Windows 7

William R. Stanek
Author and Series Editor

Administrator’s Pocket Consultant

About the Author
William R. Stanek is a Microsoft® Most Valuable Professional with 20+ years of experience in systems management and advanced programming. He is an award-winning author who's written more than 100 books, including Windows Server® 2008 Inside Out. He is the series editor for the Administrator’s Pocket Consultant line of books.

See inside cover

Windows 7
William R. Stanek
ISBN 9780735624382
• Definitive, in-depth reference
• Hundreds of timesaving solutions
• Scripts, job aids, eBook on CD

Microsoft

Recommended

More Resources for IT Professionals

Administrator’s Pocket Consultant

See inside cover

Windows 7
William R. Stanek
ISBN 9780735624382
• Definitive, in-depth reference
• Hundreds of timesaving solutions
• Scripts, job aids, eBook on CD

Windows Server 2008
Inside Out
William R. Stanek
ISBN 9780735627318
• Definitive, in-depth reference
• Hundreds of timesaving solutions
• Scripts, job aids, eBook on CD

spine = 1.63”
Cyan  Magenta   Yellow   Black
Windows® 7
Administrator’s Pocket Consultant

William R. Stanek
Contents

Introduction xix

Chapter 1 Introduction to Windows 7 Administration 1

Getting Started with Windows 7 2

Understanding 64-Bit Computing 8

Installing Windows 7 10

Preparation for Windows 7 Installation 10

Performing a Windows 7 Installation 12

Running Windows 7 15

Using Action Center and Activating Windows 17

Running Windows 7 in Groups and Domains 20

Power Plans, Sleep Modes, and Shutdown 25

Windows 7 Architecture 27

Chapter 2 Deploying Windows 7 37

Working with Windows PE 37

Understanding Windows PE 38

Configuring Windows PE 40

Preparing a Build Environment 41

Creating a Build: The Essentials 47

Creating a Bootable USB Flash Drive 55

Booting to an Image from a Hard Disk 56

Adding Windows PE Images to Windows Deployment Services 57

Working with Windows RE 58

Creating a Customized Windows RE Image 58

Creating Windows RE Recovery Media 59

What do you think of this book? We want to hear from you!
Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey
Adding Windows RE Images to Windows Deployment Services 60
Deploying Windows with a Customized Windows RE 61
Creating Windows Images for Deployment 65
Understanding Windows Imaging 65
Creating a Windows Install Image 67
Configuring and Using Windows Deployment Services 71
Setting Up Windows Deployment Services 71
Importing Images 73
Installing Windows from an Image 74
Capturing Images 75
Managing Access and Prestaging Computers 76
Customizing Windows Images 78

Chapter 3  Configuring User and Computer Policies 83
Group Policy Essentials 83
Accessing and Using Local Group Policies 85
Accessing and Using Site, Domain, and Organizational Unit Policies 88
Configuring Policies 90
Viewing Policies and Templates 90
Enabling, Disabling, and Configuring Policies 91
Adding or Removing Templates 92
Working with File and Data Management Policies 92
Configuring Disk Quota Policies 92
Configuring System Restore Policies 95
Configuring Offline File Policies 95
Working with Access and Connectivity Policies 102
Configuring Network Policies 102
Configuring Remote Assistance Policies 104
Working with Computer and User Script Policies 106
Controlling Script Behavior Through Policy 106
Assigning Computer Startup and Shutdown Scripts 108
Assigning User Logon and Logoff Scripts 109
Removing Accounts and Denying Local Access to Workstations 144

Managing Stored Credentials 144
Adding Windows or Generic Credentials 145
Adding Certificate-Based Credentials 147
Editing Windows Vault Entries 147
Backing Up and Restoring the Windows Vault 148
Removing Windows Vault Entries 149

Managing Local User Accounts and Groups 149
Creating Local User Accounts 150
Creating Local Groups for Workstations 152
Adding and Removing Local Group Members 154
Enabling or Disabling Local User Accounts 155
Creating a Secure Guest Account 156
Renaming Local User Accounts and Groups 157
Deleting Local User Accounts and Groups 158

Managing Remote Access to Workstations 159
Configuring Remote Assistance 160
Configuring Remote Desktop Access 162
Making Remote Desktop Connections 165

Chapter 6 Configuring Windows 7 Computers 167

Supporting Computers Running Windows 7 168
Working with the Computer Management Console 168
Getting Basic System and Performance Information 170
Getting Advanced System Information 175
Working with WMI Control 176

Using System Support Tools 179
Working with Disk Cleanup 180
Verifying System Files with File Signature Verification 182
Managing System Configuration, Startup, and Boot 184

Managing System Properties 190
The Computer Name Tab 190
The Hardware Tab 192
The Advanced Tab 192
Chapter 7  Customizing the Desktop and the User Interface  223

Optimizing Windows 7 Menus .................................................. 224
  Customizing the Start Menu Options 224
  Modifying Menus and Their Options 227

Working with Menus, Desktops, and Startup Applications .... 230
  Creating Shortcuts for Menus, Desktops, Startup, and More 230
  Creating Menus and Menu Options 234
  Adding and Removing Startup Applications 234

Customizing the Taskbar ...................................................... 236
  Understanding the Taskbar 236
  Pinning Shortcuts to the Taskbar 236
  Changing the Taskbar’s Size and Position 236
  Auto Hiding, Locking, and Controlling Taskbar Visibility 237
  Controlling Programs in the Notification Area 237

Optimizing Toolbars ............................................................ 239
  Displaying Toolbars 239
  Creating Personal Toolbars 239

Working with Desktop Themes ............................................. 240
  Applying and Removing Themes 240
  Tailoring and Saving Themes 241
  Deleting Custom Themes 242
Optimizing the Desktop Environment ........................................... 243
  Setting the Desktop Background ........................................... 243
  Working with the Default Desktop Icons ..................................... 244
Screen Saver Dos and Don’ts ..................................................... 246
  Configuring Screen Savers with Password Protection .................... 246
  Reducing Screen Saver Resource Usage ...................................... 248
  Setting Energy-Saving Settings for Monitors .................................. 248
Modifying Display Appearance and Video Settings ....................... 249
  Configuring Window Color and Appearance ................................ 249
  Optimizing Display Readability ............................................... 252
  Configuring Video Settings .................................................... 253
  Troubleshooting Display Problems ........................................... 260

Chapter 8  Managing Hardware Devices and Drivers ......................... 263
  Working with the Automated Help System ................................... 264
    Using Automated Help And Support ........................................ 264
    Customizing Automated Help And Support .................................. 270
  Working with Support Services ................................................ 276
    Managing Services Using Preferences ....................................... 282
  Installing and Maintaining Devices: The Essentials ..................... 283
    Installing Preexisting Devices .............................................. 284
    Installing Internal, USB, and FireWire Devices ......................... 286
    Installing Wireless, Network, and Bluetooth Devices .................. 289
    Installing Local and Network Printers ..................................... 291
  Getting Started with Device Manager ......................................... 295
  Working with Device Drivers .................................................. 297
    Device Driver Essentials ..................................................... 297
    Using Signed and Unsigned Device Drivers .................................. 298
    Tracking Driver Information .................................................. 298
    Installing and Updating Device Drivers .................................... 299
    Enabling and Disabling Types of Devices ................................... 302
    Restricting Device Installation Using Group Policy ..................... 303
    Rolling Back Drivers ......................................................... 304
    Removing Device Drivers for Removed Devices ............................ 305
    Uninstalling, Reinstalling, and Disabling Device Drivers .................. 305
Enabling and Disabling Hardware Devices 305
Troubleshooting Hardware 306

Chapter 9 Installing and Maintaining Programs 311
Managing Application Virtualization and Run Levels ............ 311
  Application Access Tokens and Location Virtualization 312
  Application Integrity and Run Levels 313
  Setting Run Levels 315
  Optimizing Virtualization and Installation Prompting for Elevation 317
Installing Programs: The Essentials ....................... 318
  Working with Autorun 319
  Application Setup and Compatibility 319
  Making Programs Available to All or Selected Users 321
Deploying Applications Through Group Policy ................. 322
Configuring Program Compatibility ......................... 324
  Special Installation Considerations for 16-Bit and MS-DOS-Based Programs 324
  Forcing Program Compatibility 325
Managing Installed and Running Programs .................... 328
  Managing Currently Running Programs 329
  Managing, Repairing, and Uninstalling Programs 330
  Designating Default Programs 331
  Managing the Command Path 332
  Managing File Extensions and File Associations 334
  Configuring AutoPlay Options 337
  Adding and Removing Windows Features 338

Chapter 10 Managing Firmware, Boot Configuration, and Startup 339
Navigating and Understanding Firmware Options .............. 339
  Firmware Interface Types and Boot Data 340
  Boot Services, Run-Time Services, and Beyond 341
  Unified EFI 342
Navigating Startup and Power States .......................... 344
  Working with Firmware Interfaces .......................... 345
  Examining Firmware Interfaces ............................. 346
  Power States and Power Management ......................... 348
Diagnosing and Resolving Startup Problems .................. 351
  Troubleshooting Startup Phase 1 ............................ 353
  Troubleshooting Startup Phase 2 ............................ 354
  Troubleshooting Startup Phase 3 ............................ 356
  Troubleshooting Startup Phase 4 ............................ 356
  Troubleshooting Startup Phase 5 ............................ 357
Managing Startup and Boot Configuration ...................... 358
  Setting Startup and Recovery Options ....................... 358
  Managing System Boot Configuration ......................... 360
  Using the BCD Editor ........................................ 362
Managing the BCD Store ........................................ 364
  Viewing BCD Entries ......................................... 364
  Creating and Identifying the BCD Store ....................... 368
  Importing and Exporting the BCD Store ....................... 368
  Creating, Copying, and Deleting BCD Entries ................ 369
  Setting BCD Entry Values .................................... 370
  Changing Data Execution Prevention and Physical Address Extension Options .......................... 376
  Changing the Operating System Display Order ................ 377
  Changing the Default Operating System Entry ................ 377
  Changing the Default Timeout ............................... 378
  Changing the Boot Sequence Temporarily ..................... 378

Chapter 11 Using TPM and BitLocker Drive Encryption ........... 379
Creating Trusted Platforms ...................................... 380
  TPM: The Essentials ........................................ 380
  Enabling and Using TPM ...................................... 381
  Initializing a TPM for First Use ............................. 383
  Turning an Initialized TPM On or Off .................... 384
  Clearing the TPM ............................................. 386
  Changing the TPM Owner Password ......................... 387
BitLocker Drive Encryption: The Essentials .......................... 387
Understanding BitLocker Drive Encryption 388
Deploying BitLocker Drive Encryption 390
Managing BitLocker Drive Encryption ................................. 393
Preparing for BitLocker Drive Encryption 394
Enabling BitLocker on Nonsystem Volumes 397
Enabling BitLocker on USB Flash Drives 399
Enabling BitLocker on System Volumes 400
Managing and Troubleshooting BitLocker 404

Chapter 12  Managing Disk Drives and File Systems 407
Disk Management Essentials ............................................ 408
Using the Computer Console ................................. 410
Using Disk Management 411
Using FSUtil and DiskPart 414
Improving Disk Performance ............................................. 414
Understanding and Using Windows ReadyBoost 414
Enabling and Configuring ReadyBoost 415
Understanding and Using Windows ReadyDrive 417
Understanding and Using Windows SuperFetch 418
Working with Basic and Dynamic Disks ............................... 420
Using Basic and Dynamic Disks ........................................... 423
Understanding Drive Designations 423
Installing and Initializing New Physical Disks 425
Changing a Disk’s Partition Table Style 426
Marking a Partition as Active 426
Converting a Basic Disk to a Dynamic Disk or Vice Versa 428
Working with Disks, Partitions, and Volumes ............................ 429
Partitioning Disks and Preparing Them for Use ........................ 431
Creating Partitions, Logical Drives, and Simple Volumes 431
Creating Spanned and Striped Volumes 434
Shrinking or Extending Volumes 436
Formatting Partitions and Volumes 438
Assigning, Changing, or Removing Drive Letters and Paths 438
Assigning, Changing, or Deleting a Volume Label 440
Deleting Partitions, Volumes, and Logical Drives 440
Converting a Volume to NTFS 441
Recovering a Failed Simple, Spanned, or Striped Volume 443

Using Disk Mirroring .............................................. 444
Creating Mirrored Volumes 444
Breaking a Mirrored Set 445
Removing a Mirrored Set 445

Moving a Dynamic Disk to a New System .................. 445

Troubleshooting Common Disk Problems .................. 447
Repairing Disk Errors and Inconsistencies 451
Checking for Disk Errors 452
Defragmenting Disks 454
Resynchronizing and Repairing a Mirrored Set 456
Repairing a Mirrored System Volume to Enable Boot 457

Working with Removable Storage Devices .................. 458

Working with Data CDs and DVDs ......................... 460
Disc Burning: The Essentials 460
Burning ISO Images to Disc 461
Burning Mastered Discs 462
Burning Discs with Live File Systems 463
Changing the Default Burning Options 464

Managing Disk Compression and File Encryption .......... 465
Compressing Drives and Data 465
Encrypting Drives and Data 467

Chapter 13 Managing File Security and Resource Sharing 473

File Security and Sharing Options ......................... 473

Controlling Access to Files and Folders with
NTFS Permissions ................................................. 478
Understanding and Using Basic Permissions 479
Assigning Special Permissions 484
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating Disk Quota Entries</td>
<td>536</td>
</tr>
<tr>
<td>Updating and Customizing Disk Quota Entries</td>
<td>537</td>
</tr>
<tr>
<td>Deleting Disk Quota Entries</td>
<td>537</td>
</tr>
<tr>
<td>Exporting and Importing Disk Quota Settings</td>
<td>538</td>
</tr>
<tr>
<td>Disabling Disk Quotas</td>
<td>539</td>
</tr>
<tr>
<td>Using Branch Caching</td>
<td>540</td>
</tr>
<tr>
<td>Chapter 15 Configuring and Troubleshooting TCP/IP Networking</td>
<td>543</td>
</tr>
<tr>
<td>Navigating Windows 7 Networking Features</td>
<td>543</td>
</tr>
<tr>
<td>Understanding Network Discovery and Network Categories</td>
<td>544</td>
</tr>
<tr>
<td>Working with Network Explorer</td>
<td>545</td>
</tr>
<tr>
<td>Working with Network And Sharing Center</td>
<td>546</td>
</tr>
<tr>
<td>Working with Network Map</td>
<td>548</td>
</tr>
<tr>
<td>Installing Networking Components</td>
<td>549</td>
</tr>
<tr>
<td>Working with TCP/IP and the Dual IP Stack</td>
<td>549</td>
</tr>
<tr>
<td>Installing Network Adapters</td>
<td>552</td>
</tr>
<tr>
<td>Installing Networking Services (TCP/IP)</td>
<td>553</td>
</tr>
<tr>
<td>Configuring Local Area Connections</td>
<td>554</td>
</tr>
<tr>
<td>Configuring Static IP Addresses</td>
<td>554</td>
</tr>
<tr>
<td>Configuring Dynamic IP Addresses and Alternate IP Addressing</td>
<td>557</td>
</tr>
<tr>
<td>Configuring Multiple Gateways</td>
<td>558</td>
</tr>
<tr>
<td>Configuring DNS Resolution</td>
<td>559</td>
</tr>
<tr>
<td>Configuring WINS Resolution</td>
<td>561</td>
</tr>
<tr>
<td>Managing Local Area Connections</td>
<td>563</td>
</tr>
<tr>
<td>Enabling and Disabling Local Area Connections</td>
<td>563</td>
</tr>
<tr>
<td>Checking the Status, Speed, and Activity for Local Area Connections</td>
<td>564</td>
</tr>
<tr>
<td>Viewing Network Configuration Information</td>
<td>565</td>
</tr>
<tr>
<td>Renaming Local Area Connections</td>
<td>566</td>
</tr>
<tr>
<td>Troubleshooting and Testing Network Settings</td>
<td>567</td>
</tr>
<tr>
<td>Diagnosing and Resolving Local Area Connection Problems</td>
<td>567</td>
</tr>
</tbody>
</table>
Chapter 16 Managing Mobile Networking and Remote Access

Configuring Networking for Laptops
Working with Windows Mobility Center
Configuring Dynamic IP Addresses
Configuring Alternate Private IP Addresses
Connecting to Networked Projectors

Understanding Mobile Networking and Remote Access

Creating Connections for Remote Access
Creating a Dial-Up Connection
Creating a Broadband Connection to the Internet
Creating a VPN Connection

Configuring Connection Properties
Configuring Automatic or Manual Connections
Configuring Proxy Settings for Mobile Connections
Configuring Connection Logon Information
Configuring Redialing Options and Automatic Disconnection
Setting a Connection to Use Dialing Rules
Configuring Primary and Alternate Phone Numbers
Configuring Identity Validation
Configuring Networking Protocols and Components
Enabling and Disabling Windows Firewall for Network Connections

Establishing Connections
Connecting with Dial-Up
Connecting with Broadband
Connecting with VPN
Wireless Networking .............................................. 608
Wireless Network Devices and Technologies 608
Wireless Security 610
Installing and Configuring a Wireless Adapter 612
Working with Wireless Networks and Wireless Connections 613
Connecting to Wireless Networks 615
Managing and Troubleshooting Wireless Networking 616

Chapter 17 Handling Maintenance and Support Tasks 617
Managing Automatic Updates ................................. 617
Windows Update: The Essentials 618
Configuring Automatic Updating 620
Checking for Updates 623
Viewing Update History and Installed Updates 623
Removing Automatic Updates to Recover from Problems 623
Hiding Available Updates 623
Restoring Declined Updates 624

Using Remote Assistance to Resolve Problems ............... 624
Understanding Remote Assistance 624
Creating Remote Assistance Invitations 626
Offering Remote Assistance or Answering a Remote Assistance Invitation 628

Detecting and Resolving Windows 7 Errors .................... 629
Using the Event Logs for Error Tracking and Diagnosis 629
Viewing and Managing the Event Logs 630

Scheduling Maintenance Tasks ................................. 631
Understanding Task Scheduling 631
Viewing and Managing Tasks on Local and Remote Systems 633
Creating Scheduled Tasks 634
Troubleshooting Scheduled Tasks 635

Backing Up and Recovering a Computer ....................... 636
Backing Up and Recovering Files and Folders Using Previous Versions 636
Recovering from a Failed Resume 636
Repairing a Computer to Enable Startup 637
Backing Up and Recovering System State Using System Restore 639
Creating and Using a Backup 642
Recovering Personal Data 645
Repairing and Recovering a Computer 645
Troubleshooting Startup and Shutdown .......................... 646
Resolving Restart or Shutdown Issues 647
Making Sense of Stop Errors 647
Index 651

What do you think of this book? We want to hear from you!
Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey
Introduction

Writing *Windows 7 Administrator’s Pocket Consultant* was a lot of fun—and a lot of work. As I set out to write this book, my initial goals were to determine how Windows 7 was different from Windows Vista and Windows XP and what new administration options were available. As with any new operating system—but especially with Windows 7—I had to do a great deal of research and a lot of digging into the operating system internals to determine exactly how things work.

When you start working with Windows 7, you’ll see at once that the operating system is different from earlier releases of Windows. What won’t be apparent, however, is just how different Windows 7 is from its predecessors—and that’s because many of the most significant changes to the operating system are below the surface. These changes affect the underlying architecture, as well as the user interfaces, and they were some of the hardest for me to research and write about.

Because Administrator’s Pocket Consultants are meant to be portable and readable—the kind of book you use to solve problems and get the job done wherever you might be—I had to carefully review my research to make sure I focused on the core aspects of Windows 7 administration. The result is the book you hold in your hands, which I hope you’ll agree is one of the best practical, portable guides to Windows 7. Toward that end, the book covers everything you need to perform the core administrative tasks for computers running Windows 7.

Because my focus is on giving you maximum value in a pocket-size guide, you don’t have to wade through hundreds of pages of extraneous information to find what you’re looking for. Instead, you’ll find exactly what you need to address a specific issue or perform a particular task. In short, the book is designed to be the one resource you turn to whenever you have questions regarding Windows 7 administration. It zeroes in on daily administration procedures, frequently used tasks, documented examples, and options that are representative while not necessarily inclusive.

One of the goals for this book is to keep its content concise so that it remains compact and easy to navigate while at the same time packing it with as much information as possible to make it a valuable resource. Instead of a hefty 1,000-page tome or a lightweight, 100-page quick reference, you get a valuable resource guide that can help you quickly and easily perform common tasks, solve problems, and implement everyday solutions for systems and users.
Who Is This Book For?

Windows 7 Administrator’s Pocket Consultant covers all editions of Windows 7. The book is designed for:

- Current Windows system administrators.
- Accomplished users who have some administrator responsibilities.
- Administrators upgrading to Windows 7 from earlier releases of Windows.
- Administrators transferring from other platforms.

To pack in as much information as possible, I had to assume that you have basic networking skills and a basic understanding of Windows operating systems. As a result, I don’t devote entire chapters to understanding Windows basics, Windows architecture, or Windows networks. I do, however, cover desktop customization, mobile networking, TCP/IP configuration, user profiles, and system optimization. The book also goes into depth on troubleshooting, and I’ve tried to ensure that each chapter, where appropriate, has troubleshooting guidelines and discussions to accompany the main text. From the start, troubleshooting advice is integrated into the book—instead of being captured in a single, catchall troubleshooting chapter inserted as an afterthought. I hope that after you read these chapters and dig into the details, you’ll be able to improve the overall experience of your users and reduce downtime.

How Is This Book Organized?

Windows 7 Administrator’s Pocket Consultant is designed to be used in daily administration, and as such, the book is organized by job-related tasks rather than by Windows 7 features. The books in the Administrator’s Pocket Consultant series are down-and-dirty, in-the-trenches books.

Speed and ease of reference are essential elements of this hands-on guide. The book has an expanded table of contents and an extensive index for finding answers to problems quickly. Many other quick reference features have been added as well. These features include step-by-step instructions, lists, tables with fast facts, and extensive cross-references.

Conventions Used in This Book

I’ve used a variety of elements to help keep the text clear and easy to follow. You’ll find code listings in monospace type, except when I tell you to actually type a command. In that case, the command appears in bold type. When I introduce and define a new term, I put it in italics.
Other conventions include the following:

**Note**  To provide additional details about a particular point that needs emphasis

**Tip**  To offer helpful hints or additional information

**Caution**  To warn you when there are potential problems you should look out for

**Real World**  To provide real-world advice when discussing advanced topics

I truly hope you find that *Windows 7 Administrator’s Pocket Consultant* provides everything you need to perform the essential administrative tasks on Windows 7 systems as quickly and efficiently as possible. You are welcome to send your thoughts to me at williamstanek@aol.com. Thank you.

### Find Additional Content Online

As new or updated material becomes available that complements this book, it will be posted online on the Microsoft Press Online Windows Server and Client Web site. The type of material you might find includes updates to book content, articles, links to companion content, errata, sample chapters, and more. This Web site is available at [http://microsoftpresssrv.libredigital.com/serverclient/](http://microsoftpresssrv.libredigital.com/serverclient/) and is updated periodically.

You’ll also find discussion about the book at [www.williamstanek.com](http://www.williamstanek.com). Follow me on Twitter at WilliamStanek.

### Support

Every effort has been made to ensure the accuracy of this book. Microsoft Press provides corrections for books through the World Wide Web at the following address:

[http://www.microsoft.com/mspress/support](http://www.microsoft.com/mspress/support)

If you have comments, questions, or ideas about this book, please send them to Microsoft Press using either of the following methods:

Postal mail:
Microsoft Press
Attn: Editor, *Windows 7 Administrator’s Pocket Consultant*
One Microsoft Way
Redmond, WA 98052-6399

E-mail:
mspinput@microsoft.com

Please note that product support isn’t offered through these addresses. For support information, visit Microsoft’s Web site at [http://support.microsoft.com/](http://support.microsoft.com/).
Understanding User and Group Accounts

Computers running Windows 7 can be configured to be members of a homegroup, a workgroup, or a domain. When a workstation is configured as a member of a homegroup or a workgroup, user access and security are configured on the workstation itself. When a workstation is configured as a member of a domain, user access and security are configured at two levels: the local system level and the domain level. User access can be configured at the local system level for a specific machine and at the domain level for multiple systems or resources throughout the current Active Directory forest. In this chapter, you’ll learn how to manage local system access and local accounts. For further discussion of configuring domain access and permissions, see Windows Server 2008 Administrator’s Pocket Consultant, Second Edition (Microsoft Press, 2010). Keep in mind that every task examined in this chapter and throughout this book can be performed through a local logon or a remote desktop connection.

Understanding User and Group Accounts

Windows 7 provides user accounts and group accounts (of which users can be members). User accounts are designed for individuals. Group accounts, usually referred to as groups, are designed to simplify the administration of multiple users. You can log on with a user account, but you can’t log on with a group account.
Two general types of user accounts are defined in Windows 7:

- **Local user accounts**  User accounts defined on a local computer are called *local user accounts*. These accounts have access to the local computer only. You add or remove local user accounts with Control Panel’s User Accounts options or with the Local Users And Groups utility. Local Users And Groups is accessible through Computer Management, a Microsoft Management Console (MMC) snap-in.

- **Domain user accounts**  User accounts defined in Active Directory are called *domain user accounts*. Through single sign-on, these accounts can access resources throughout a forest. When a computer is a member of an Active Directory domain, you can use it to create domain user accounts by using Active Directory Users And Computers. This MMC tool is available on the Administrative Tools menu when you install the Remote Server Administrator Tools on your Windows 7 computer.

Both local user accounts and domain user accounts can be configured as standard user accounts or administrator accounts. A standard user account on a local computer has limited privileges, and an administrator account on a local computer has extended privileges.

**Local User Account Essentials**

All user accounts are identified with a logon name. In Windows 7, this logon name has two parts:

- **User name**  The display text for the account

- **User computer or domain**  The computer or domain in which the user account exists

For the user Williams, whose account is created for the computer ENGPC85, the full logon name for Windows 7 is ENGPC85\Williams. With a local computer account, Williams can log on to his local workstation and access local resources but is not able to access domain resources.

When working with domains, the full logon name can be expressed in two different ways:

- The user account name and the full domain name separated by the At sign (@). For example, the full logon name for the user name Williams in the domain technology.microsoft.com would be *Williams@technology.microsoft.com*.

- The user account name and the domain separated by the backslash symbol (\). For example, the full logon name for Williams in the technology domain would be *technology\Williams*.

Although Windows 7 displays user names when describing account privileges and permissions, the key identifiers for accounts are security identifiers (SIDs). SIDs are unique identifiers generated when security principals are created. Each SID
combines a computer or domain security ID prefix with a unique relative ID for the user. Windows 7 uses these identifiers to track accounts and user names independently. SIDs serve many purposes, but the two most important are to enable you to easily change user names and to delete accounts without worrying that someone might gain access to resources simply by re-creating an account.

When you change a user name, you tell Windows 7 to map a particular SID to a new name. When you delete an account, you tell Windows 7 that a particular SID is no longer valid. Even if you create an account with the same user name later, the new account won’t have the same privileges and permissions as the previous one because the new account will have a new SID.

User accounts can also have passwords and certificates associated with them. Passwords are authentication strings for an account. Certificates combine a public and private key to identify a user. You log on with a password interactively, whereas you log on with a certificate by using its private key, which is stored on a smart card and read with a smart card reader.

When you install Windows 7, the operating system installs default user accounts. You’ll find several built-in accounts, which have purposes similar to those of accounts created in Windows domains. The key accounts are the following:

- **Administrator** Administrator is a predefined account that provides complete access to files, directories, services, and other facilities. You can’t delete or disable this account. In Active Directory, the Administrator account has domainwide access and privileges. On a local workstation, the Administrator account has access only to the local system.

- **Guest** Guest is designed for users who need one-time or occasional access. Although guests have only limited system privileges, you should be very careful about using this account because it opens the system to potential security problems. The risk is so great that the account is initially disabled when you install Windows 7.

By default, these accounts are members of various groups. Before you modify any of the built-in accounts, you should note the property settings and group memberships for the account. Group membership grants or limits the account’s access to specific system resources. For example, Administrator is a member of the Administrators group and Guest is a member of the Guests group. Being a member of a group makes it possible for the account to use the privileges and rights of the group.

In addition to the built-in accounts, Windows 7 has several pseudo-accounts that are used to perform specific types of system actions. The pseudo-accounts are available only on the local system. You can’t change the settings for these accounts with the user administration tools, and users can’t log on to a computer with these accounts. The pseudo-accounts available include the following:

- **LocalSystem** LocalSystem is used for running system processes and handling system-level tasks. This account grants the logon right Log On As
A Service. Most services run under the LocalSystem account. In some cases, these services have privileges to interact with the desktop. Services that need fewer privileges or logon rights run under the LocalService or NetworkService account. Services that run as LocalSystem include Background Intelligent Transfer Service, Computer Browser, Group Policy Client, Netlogon, Network Connections, Print Spooler, and User Profile Service.

- **LocalService**  LocalService is used for running services that need fewer privileges and logon rights on a local system. By default, services that run under this account are granted the right Log On As A Service and the privileges Adjust Memory Quotas For A Process, Change The System Time, Change The Time Zone, Generate Security Audits, and Replace A Process Level Token. Services that run as LocalService include Application Layer Gateway Service, Remote Registry, Smart Card, SSDP Discovery Service, TCP/IP NetBIOS Helper, and WebClient.

- **NetworkService**  NetworkService is used for running services that need fewer privileges and logon rights on a local system but must also access network resources. Like services that run under LocalService, services that run by default under the NetworkService account are granted the right Log On As A Service and the privileges Adjust Memory Quotas For A Process, Generate Security Audits, and Replace A Process Level Token. Services that run under NetworkService include BranchCache, Distributed Transaction Coordinator, DNS Client, Remote Desktop Services, and Remote Procedure Call (RPC). NetworkService can also authenticate to remote systems as the computer account.

### Group Account Essentials

Windows 7 also provides groups, which you use to grant permissions to similar types of users and to simplify account administration. If a user is a member of a group that has access to a resource, that user has access to the same resource. You can give a user access to various work-related resources just by making the user a member of the correct group. Although you can log on to a computer with a user account, you can’t log on to a computer with a group account. Because different Active Directory domains or local computers might have groups with the same name, groups are often referred to by *Domain\GroupName* or *Computer\GroupName* (for example, Technology\GMarketing for the GMarketing group in a domain or on a computer named Technology).

Windows 7 uses the following three types of groups:

- **Local groups**  Defined on a local computer and used on the local computer only. You create local groups with Local Users And Groups.

- **Security groups**  Can have security descriptors associated with them. You use a Windows server to define security groups in domains, using Active Directory Users And Computers.
- **Distribution groups**  Used as e-mail distribution lists. They can’t have security descriptors associated with them. You define distribution groups in domains using Active Directory Users And Computers.

As with user accounts, group accounts are tracked using unique SIDs. This means that you can’t delete a group account and re-create it and then expect that all the permissions and privileges remain the same. The new group will have a new SID, and all the permissions and privileges of the old group will be lost.

When you assign user access levels, you have the opportunity to make the user a member of the following built-in or predefined groups:

- **Administrators**  Members of this group are local administrators and have complete access to the workstation. They can create accounts, modify group membership, install printers, manage shared resources, and more. Because this account has complete access, you should be very careful about which users you add to this group.

- **Backup Operators**  Members of this group can back up and restore files and directories on the workstation. They can log on to the local computer, back up or restore files, and shut down the computer. Because of how this account is set up, its members can back up files regardless of whether the members have read/write access to the files. However, they can’t change access permissions on the files or perform other administrative tasks.

Backup Operators have privileges to perform very specific administrative tasks, such as backing up file systems. By default, no other group or user accounts are members of the operator groups. This is to ensure that you grant explicit access to the operator groups.

- **Cryptographic Operators**  Members can manage the configuration of encryption, IP Security (IPSec), digital IDs, and certificates.

- **Event Log Readers**  Members can view the event logs on the local computer.

- **Guests**  Guests are users with very limited privileges. Members can access the system and its resources remotely, but they can’t perform most other tasks.

- **Network Configuration Operators**  Members can manage network settings on the workstation. They can also configure TCP/IP settings and perform other general network configuration tasks.

- **Performance Log Users**  Members can view and manage performance counters. They can also manage performance logging.

- **Performance Monitor Users**  Members can view performance counters and performance logs.

- **Power Users**  In earlier versions of Windows, this group is used to grant additional privileges, such as the capability to modify computer settings and install programs. In Windows 7, this group is maintained only for compatibility with legacy applications.
- **Remote Desktop Users** Members can log on to the workstation remotely using Remote Desktop Services. Once members are logged on, additional groups of which they are members determine their permissions on the workstation. A user who is a member of the Administrators group is granted this privilege automatically. (However, remote logons must be enabled before an administrator can remotely log on to a workstation.)

- **Replicator** Members can manage the replication of files for the local machine. File replication is primarily used with Active Directory domains and Windows servers.

- **Users** Users are people who do most of their work on a single Windows 7 workstation. Members of the Users group have more restrictions than privileges. They can log on to a Windows 7 workstation locally, keep a local profile, lock the workstation, and shut down the workstation.

In most cases, you configure user access by using the Users or Administrators group. You can configure user and administrator access levels by setting the account type to Standard User or Administrator, respectively. While these basic tasks can be performed using Control Panel’s User Accounts page, you make a user a member of a group by using Local Users And Groups under Computer Management.

### Domain vs. Local Logon

When computers are members of a domain, you typically use domain accounts to log on to computers and the domain. All administrators in a domain have access to resources on the local workstations that are members of the domain. Users, on the other hand, can access resources only on the local workstations they are permitted to log on to. In a domain, any user with a valid domain account can by default log on to any computer that is a member of the domain. Once logged on to a computer, the user has access to any resource that his or her account or the groups to which the user’s account belongs are granted access. This includes resources on the local machine as well as resources in the domain.

You can restrict logons to specific domain workstations on a per-user basis by using Active Directory Users And Computers. In Active Directory Users And Computers, right-click the user account and then click Properties. On the Account tab of the user’s Properties dialog box, click Log On To, and then use the options in the Logon Workstations dialog box to designate the workstations to which the user is permitted to log on.

When you work with Windows 7, however, you aren’t always logging on to a domain. Computers configured in workgroups have only local accounts. You might also need to log on locally to a domain computer to administer it. Only users with a local user account can log on locally. When you log on locally, you have access to any resource on the computer that your account or the groups to which your account belongs are granted access.
Managing User Account Control and Elevation Prompts

User Account Control (UAC) represents a significant change in the way in which user accounts are used and configured. It affects which privileges standard users and administrator users have, how applications are installed and run, and much more. In this section, I’ll extend the discussion in Chapter 1, “Introduction to Windows 7 Administration,” and provide a comprehensive look at how UAC affects user and administrator accounts. This is essential information to know when managing Windows 7 systems.

**NOTE** Learning how UAC works will help you be a better administrator. To support UAC, many aspects of the Windows operating system had to be reworked. Some of the most extensive changes have to do with how applications are installed and run. In Chapter 9, “Installing and Maintaining Programs,” you’ll find a complete discussion of how the architectural changes affect programs running on Windows 7.

Redefining Standard User and Administrator User Accounts

In Windows XP and earlier versions of Windows, malicious software programs can exploit the fact that most user accounts are configured as members of the local computer’s Administrators group. Not only does this allow malicious software to install itself, but it also allows malicious software to use these elevated privileges to wreak havoc on the computer, because programs installed by administrators can write to otherwise secure areas of the registry and the file system.

To combat the growing threat of malicious software, organizations have locked down computers, required users to log on using standard user accounts, and required administrators to use the Run As command to perform administrative tasks. Unfortunately, these procedural changes can have serious negative consequences on productivity. A person logged on as a standard user under Windows XP can’t perform some of the most basic tasks, such as changing the system clock and calendar, changing the computer’s time zone, or changing the computer’s power management settings. Many software programs designed for Windows XP simply will not function properly without local administrator rights—these programs use local administrator rights to write to system locations during installation and during normal operations. Additionally, Windows XP doesn’t let you know beforehand when a task you are performing requires administrator privileges.

UAC seeks to improve usability while at the same time enhancing security by redefining how standard user and administrator user accounts are used. UAC represents a fundamental shift in computing by providing a framework that limits the scope of administrator-level access privileges and requires all applications to run in a specific user mode. In this way, UAC prevents users from making inadvertent changes to system settings and locks down the computer to prevent unauthorized applications from being installed or performing malicious actions.
Because of UAC, Windows 7 defines two levels of user accounts: standard and administrator. Windows 7 also defines two modes (run levels) for applications: standard user mode and administrator mode. Although standard user accounts can use most software and can change system settings that do not affect other users or the security of the computer, administrator user accounts have complete access to the computer and can make any changes that are needed. When an administrator user starts an application, her access token and its associated administrator privileges are applied to the application, giving her all the rights and privileges of a local computer administrator for that application. When a standard user starts an application, her access token and its associated privileges are applied to the application at run time, limiting her to the rights and privileges of a standard user for that application. Further, all applications are configured to run in a specific mode during installation. Any tasks run by standard-mode applications that require administrator privileges not only are identified during setup but require user approval to run.

In Windows 7, the set of privileges assigned to standard user accounts has changed. Tasks that standard user accounts can perform include:

- Installing fonts, viewing the system clock and calendar, and changing the time zone.
- Changing the display settings and the power management settings.
- Adding printers and other devices (when the required drivers are installed on the computer or are provided by an IT administrator).
- Downloading and installing updates (when the updates use UAC-compatible installers).
- Creating and configuring virtual private network (VPN) connections. VPN connections are used to establish secure connections to private networks over the public Internet.
- Installing Wired Equivalent Privacy (WEP) to connect to secure wireless networks. The WEP security protocol provides wireless networks with improved security.

Windows 7 also defines two run levels for applications: standard and administrator. Windows 7 determines whether a user needs elevated privileges to run a program by supplying most applications and processes with a security token. If an application has a standard token, or an application cannot be identified as an administrator application, elevated privileges are not required to run the application, and Windows 7 starts it as a standard application by default. If an application has an administrator token, elevated privileges are required to run the application, and Windows 7 prompts the user for permission or confirmation prior to running the application.

The process of getting approval prior to running an application in administrator mode and prior to performing tasks that change system configuration is known as elevation. Elevation enhances security and reduces the impact of malicious software.
by notifying users before they perform any action that could impact system settings and by preventing applications from using administrator privileges without first notifying users. Elevation also protects administrator applications from attacks by standard applications. For more information on elevation and how UAC works with applications, see Chapter 9.

By default, Windows 7 switches to the secure desktop prior to displaying the elevation prompt. The secure desktop restricts the programs and processes that have access to the desktop environment, and in this way reduces the possibility that a malicious program or user could gain access to the process being elevated. If you don’t want Windows 7 to switch to the secure desktop prior to prompting for elevation, you can choose settings that use the standard desktop rather than the secure desktop. However, this makes the computer more susceptible to malware and attack.

**Optimizing User Account Control and Admin Approval Mode**

Every computer has a built-in local Administrator account. This built-in account is not protected by UAC, and using this account for administration can put your computer at risk. To safeguard computers in environments in which you use a local Administrator account for administration, you should create a new local Administrator account and use this account for administration.

UAC can be configured or disabled for any individual user account. If you disable UAC for a user account, you lose the additional security protections UAC offers and put the computer at risk. To completely disable UAC or to reenable UAC after disabling it, the computer must be restarted for the change to take effect.

Admin Approval Mode is the key component of UAC that determines whether and how administrators are prompted when running administrator applications. The default way that Admin Approval Mode works is as follows:

- All administrators, including the built-in local Administrator account, run in and are subject to Admin Approval Mode.
- Because they are running in and subject to Admin Approval Mode, all administrators, including the built-in local Administrator account, see the elevation prompt when they run administrator applications.

If you are logged on as an administrator, you can modify the way UAC works for all users by completing the following steps:


2. On the User Account Control Settings page, shown in Figure 5-1, use the slider to choose when to be notified about changes to the computer, and then click OK. Table 5-1 summarizes the available options.
TABLE 5-1 User Account Control Settings

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
<th>WHEN TO USE</th>
<th>USES THE SECURE DESKTOP?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always Notify</td>
<td>Always notifies the current user when programs try to install software or make changes to the computer and when the user changes Windows settings.</td>
<td>Choose this option when a computer requires the highest security possible and users frequently install software and visit unfamiliar Web sites.</td>
<td>Yes</td>
</tr>
<tr>
<td>Default</td>
<td>Notifies the current user only when programs try to make changes to the computer and not when the user changes Windows settings.</td>
<td>Choose this option when a computer requires high security and you want to reduce the number of notification prompts that users see.</td>
<td>Yes</td>
</tr>
<tr>
<td>Notify Me Only When ... (Do Not Dim My Desktop)</td>
<td>Same as Default but also prevents UAC from switching to the secure desktop.</td>
<td>Choose this option when users work in a trusted environment with familiar applications and do not visit unfamiliar Web sites.</td>
<td>No</td>
</tr>
</tbody>
</table>
In Group Policy, you can manage Admin Approval Mode and elevation prompting by using settings under Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options. These security settings are:

- **User Account Control: Admin Approval Mode For The Built-In Administrator Account**  Determines whether users and processes running as the built-in local Administrator account are subject to Admin Approval Mode. By default, this feature is enabled, which means the built-in local Administrator account is subject to Admin Approval Mode and also subject to the elevation prompt behavior stipulated for administrators in Admin Approval Mode. If you disable this setting, users and processes running as the built-in local administrator are not subject to Admin Approval Mode and therefore not subject to the elevation prompt behavior stipulated for administrators in Admin Approval Mode.

- **User Account Control: Allow UIAccess Applications To Prompt For Elevation Without Using The Secure Desktop**  Determines whether User Interface Accessibility (UIAccess) programs can automatically disable the secure desktop for elevation prompts used by a standard user. If you enable this setting, UIAccess programs, including Windows Remote Assistance, can disable the secure desktop for elevation prompts.

- **User Account Control: Behavior Of The Elevation Prompt For Administrators In Admin Approval Mode**  Determines whether administrators subject to Admin Approval Mode see an elevation prompt when running administrator applications, and also determines how the elevation prompt works. By default, administrators are prompted for consent when running administrator applications on the secure desktop. You can configure this option so that administrators are prompted for consent without the secure desktop, prompted for credentials with or without the secure desktop (as is the case with standard users), or prompted for consent only for non-Windows binaries. You can also configure this option so that administrators are not prompted at all, in which case an administrator will be elevated automatically. No setting will prevent an administrator from right-clicking an application shortcut and selecting Run As Administrator.
**User Account Control: Behavior Of The Elevation Prompt For Standard Users**  Determines whether users logged on with a standard user account see an elevation prompt when running administrator applications. By default, users logged on with a standard user account are prompted for the credentials of an administrator on the secure desktop when running administrator applications or performing administrator tasks. You can also configure this option so that users are prompted for credentials on the standard desktop rather than the secure desktop, or you can deny elevation requests automatically, in which case users will not be able to elevate their privileges by supplying administrator credentials. The latter option doesn’t prevent users from right-clicking an application shortcut and selecting Run As Administrator.

**User Account Control: Run All Administrators In Admin Approval Mode**  Determines whether users logged on with an administrator account are subject to Admin Approval Mode. By default, this feature is enabled, which means administrators are subject to Admin Approval Mode and also subject to the elevation prompt behavior stipulated for administrators in Admin Approval Mode. If you disable this setting, users logged on with an administrator account are not subject to Admin Approval and therefore are not subject to the elevation prompt behavior stipulated for administrators in Admin Approval Mode.

**User Account Control: Only Elevate UIAccess Applications That Are Installed in Secure Locations**  Determines whether UIAccess programs must reside in a secure location on the file system to elevate. If enabled, UIAccess programs must reside in a secure location under %SystemRoot%\Program Files, %SystemRoot%\Program Files(x86), or %SystemRoot%\Windows\System32.

**User Account Control: Only Elevate Executables That Are Signed And Validated**  Determines whether applications must be signed and validated to elevate. If enabled, only executables that pass signature checks and have certificates in the Trusted Publisher store will elevate. Use this option only when the highest security is required and you’ve verified that all applications in use are signed and valid.

In a domain environment, you can use Active Directory–based Group Policy to apply the security configuration you want to a particular set of computers. You can also configure these settings on a per-computer basis using local security policy. To do this, follow these steps:

1. Click Start, point to All Programs, Administrative Tools, and then click Local Security Policy.
2. In the Local Security Policy console tree, under Security Settings, expand Local Policies, and then select Security Options, as shown in Figure 5-2.
3. Double-click the setting you want to work with, make any necessary changes, and then click OK. Repeat this step to modify other security settings as necessary.

Managing Local Logon

All local computer accounts should have passwords. If an account is created without a password, anyone can log on to the account, and there is no protection for the account. However, a local account without a password cannot be used to remotely access a computer.

The sections that follow discuss how to create and work with local user accounts. Every workstation computer has local computer accounts, whether the computer is a member of a homegroup, a workgroup, or a domain.

Creating Local User Accounts in a Homegroup or Workgroup

For a computer that is a member of a homegroup or a workgroup, you can create a local user account by following these steps:

1. In Control Panel, under the User Accounts heading, click Add Or Remove User Accounts. This displays the Manage Accounts page.
   
   As Figure 5-3 shows, the Manage Accounts page lists all configurable user accounts on the local computer by account type and with configuration details. If an account has a password, it is labeled Password Protected. If an account is disabled, it is listed as being off.

2. Click Create A New Account. This displays the Create New Account page.

3. Type the name of the local account. This name is displayed on the Welcome screen and Start menu.

4. Set the type of account as either Standard User or Administrator. To give the user full permissions on the local computer, select Administrator.

5. Click Create Account.
Granting Access to an Existing Domain Account to Allow Local Logon

If a user needs to be able to log on locally to a computer and has an existing domain account, you can grant the user permission to log on locally by completing the following steps:

1. In Control Panel, under the User Accounts heading, click the Change Account Type link. This displays the User Accounts dialog box. As Figure 5-4 shows, the User Accounts dialog box lists all configurable user accounts on the local computer by domain and with group membership details.
2. Click Add. This starts the Add New User wizard.

3. You are creating a local computer account for a user with an existing domain account. Type the user’s domain account name and domain in the fields provided.

4. Using the options provided, select the type of user account.

5. A standard user account is created as a member of the local Users group. To give the user the permissions of a normal user, select Standard User.

6. An administrator account is created as a member of the local Administrators group. To give the user full permissions on the local computer, select Administrator.

7. An Other account is created as a member of a group you specify. To give the user the permissions of a specific group, select Other, and then select the group.

8. Click Finish. If you need to set other permissions or add the user to other local groups, follow the steps specified in the section “Managing Local User Accounts and Groups.”

**Changing Local User Account Types**

The User Accounts utility provides an easy way to change account types for local users. You can also quickly set one of the default account types. For more advanced control, however, you need to use Local Users And Groups to assign group membership to individual accounts. (See the section “Adding and Removing Local Group Members.”)

In a homegroup or workgroup, you can change the account type for a local computer user by completing the following steps:

1. In Control Panel, under the User Accounts heading, click Add Or Remove User Accounts. This displays the Manage Accounts page.

2. Click the account you want to change, and then click Change The Account Type.

3. On the Change Account Type page, set the level of access for the user as either Standard User or Administrator, and then click Change The Account Type.

In a domain, you can change the account type for a local computer user by completing the following steps:

1. In Control Panel, click User Accounts. On the User Accounts page, click Change Account Type. This displays the User Accounts dialog box.

2. On the Users tab, click the user account you want to work with, and then click Properties.

3. In the Properties dialog box, click the Group Membership tab.
4. Set the type of account as Standard User or Administrator, or select Other and then select the group you want to use.

5. Click OK twice.

Creating Passwords for Local User Accounts

In a homegroup or workgroup configuration, local user accounts are created without passwords by default. This means that a user can log on simply by clicking his account name on the Welcome screen or by clicking OK on the classic Log On To Windows screen. To improve security, all local accounts should have passwords.

For the easiest management of local accounts, log on to each account that should have a password, and then use the User Accounts utility to assign a password to the account. If you are logged on as the user when you create a password, you don’t have to worry about losing encrypted data. If you create a password without logging on as the user, the user will lose access to his or her encrypted files, encrypted e-mail, personal certificates, and stored passwords. This occurs because the user’s master key, which is needed to access his or her personal encryption certificate and unlock this data, is encrypted with a hash that is based on an empty password. So when you create a password, the hash doesn’t match, and there’s no way to unlock the encrypted data. The only way to resolve this is to restore the original settings by removing the password from the account. The user should then be able to access his or her encrypted files. Again, this issue is related only to local user accounts for computers and not to domain user accounts.

**TIP** Only the User Accounts utility allows you to assign a password hint, which can be helpful in recovering a forgotten or lost password. Another technique for recovering a password is a password reset disk, which can be a floppy disk or a USB flash drive. It is important to note that these are the only techniques you should use to recover passwords for local user accounts unless you want to risk data loss. Why? Although you can create, reset, or remove a password from a user account, doing so deletes any personal certificates and stored passwords associated with this account. As a result, the user will no longer be able to access his or her encrypted files or private e-mail messages that have been encrypted with his or her personal key. In addition, he or she will lose stored passwords for Web sites and network resources. It is also important to note that this is an issue only for local user accounts. Administrators can change or reset passwords for domain user accounts without affecting access to encrypted data.

You can create a password for a local user account by completing the following steps:

1. Log on as the user whose password you want to create. In Control Panel, under the User Accounts heading, click Add Or Remove User Accounts. This displays the Manage Accounts page.
2. Click the account you want to work with. To prevent possible data loss, this should be the same account as the account with which you logged on. Any account that has a current password is listed as Password Protected. Any account without this label doesn’t have a password.

3. Click Create A Password. Type a password, and then confirm it, as illustrated in Figure 5-5. Afterward, type a unique password hint. The password hint is a word or phrase that can be used to obtain the password if it is lost or forgotten. This hint is visible to anyone who uses the computer.

![Figure 5-5 Create a password with a password hint.](image)

4. Click Create Password.

**Recovering Local User Account Passwords**

As discussed previously, in order to preserve access to any encrypted data and stored passwords that a user might have, it is preferable to try and recover a user password rather than change or remove the password.

Windows 7 provides two ways to recover user passwords:

- **Password hint** A hint can be accessed on the Welcome screen. Ordinarily, the Welcome screen is displayed when the computer is started and no one is logged on. If someone is logged on to the workstation, ask him or her to log off. Click the user’s name to display the Password prompt, and then click the blue enter button to display the password hint. Hopefully, the password hint will help the user remember the password. If it doesn’t, you need to use a password reset disk.
Password reset disk  Password reset disks can be created for any local user account with a password. They enable anyone to change the password of the related local account without needing to know the old password. Because anyone with access to these disks can change account passwords, you should store password reset disks in a secure location. If users are allowed to create their own password reset disks, be sure they know how important the disks are.

**NOTE**  Passwords for domain users and those for local users are managed differently. Administrators manage passwords for domain user accounts and can reset forgotten passwords using the Active Directory Users And Computers console.

Passwords for local machine accounts can be stored in a secure, encrypted file on a password reset disk, which can be a floppy disk or a USB flash device. You can create a password reset disk for the current user as discussed in “Creating and Using a Password Reset Disk” in Chapter 1. You can reset a password for a local machine account as discussed in “Resetting a User’s Password” in Chapter 1.

**Controlling Logon: Welcome Screens and Classic Logons**

By default, Windows 7 displays a Welcome screen when a computer is part of a homegroup or workgroup. Windows displays a Logon screen when a computer is part of a domain. The difference between the Welcome screen and the Logon screen is an important one.

In a homegroup or workgroup, the Welcome screen is displayed when no one is logged on or when the screen saver is activated and you attempt to log on again. On the Welcome screen, you see a list of accounts on the computer. To log on with one of these accounts, click the account and type a password if required. Contrary to what many people think, the Welcome screen doesn’t display all the accounts that have been created on the computer. Some accounts, such as Administrator, are hidden from view automatically.

The Welcome screen is convenient because it displays a list of available accounts and enables you to log on by clicking an account name. To enhance security in a homegroup or workgroup by not giving a list of accounts, you can use the Logon screen instead of the Welcome screen. In a domain, the Logon screen is displayed automatically when no one is logged on or when the screen saver is activated and you attempt to log on again. The Logon screen requires users to type a logon name rather than selecting an account from a list of available accounts.

The Logon screen has several features that you can control. By default, the name of the last user to log on is displayed in the User Name field of the Log On To Windows dialog box. Hiding the user name of the last user to log on can improve security by requiring users to know a valid account name for the computer. To do this, start the Local Security Policy tool from the Administrative Tools menu or type `secpol.msc` at an elevated command prompt. Then, under Local Policies\Security...
Options, double-click Interactive Logon: Do Not Display Last User Name. Click Enabled, and then click OK.

You can configure whether the Welcome screen is used through the Always Use Classic Logon setting in Group Policy. You have the following options:

- Enable the policy to use the Logon screen rather than the Welcome screen.
- Disable the policy to use the Welcome screen.
- Use Not Configured to use the default configuration (the Welcome screen).

In a domain environment, you can use Active Directory–based Group Policy to apply the security configuration you want to a particular set of computers. You can also configure this setting on a per-computer basis by using local security policy.

To configure a homegroup or workgroup computer to use the Logon screen rather than the Welcome screen, use the Group Policy Object Editor, which is an MMC snap-in. You can add this snap-in to an empty console and configure a computer to use the Logon screen by following these steps:

1. Click Start, type `gpedit.msc`, and then press Enter. This opens the Local Group Policy Editor with the top-level Local Group Policy object open for editing.

2. In the editor, expand Local Computer Policy, Computer Configuration, Administrative Templates, System, Logon. (See Figure 5-6.)

![Figure 5-6](image)

**FIGURE 5-6** Enable the Always Use Classic Logon setting to use the Logon screen rather than the Welcome screen.


4. Select Enabled, and then click OK.
In a domain, by default you cannot bypass the requirement to press Ctrl+Alt+Del to access the Log On To Windows dialog box. You can eliminate this requirement, but it is a poor security practice. To do so, in the Local Security Policy tool, expand Local Policies\Security Options, and then double-click Interactive Logon: Do Not Require Ctrl+Alt+Del. Click Enabled, and then click OK.

Removing Accounts and Denying Local Access to Workstations

Domain administrators are automatically granted access to local resources on workstations. Other users aren’t granted access to local resources on workstations other than to the computers to which they are permitted to log on. As workstations are moved around an organization, you might find that previous owners of a workstation still have access to its resources or that users who were granted temporary access to a workstation were never removed from the access list.

In a domain, you can control the workstations to which users can log on by using the account properties in Active Directory Users And Computers. Double-click the account to display the Properties dialog box. On the Account tab, click the Log On To button.

In a homegroup or workgroup, you can remove a user’s local account and effectively deny logon by completing these steps:

1. Log on as a user with local administrator privileges. In Control Panel, under the User Accounts heading, click Add Or Remove User Accounts. This displays the Manage Accounts page.
2. Click the account you want to remove.
3. Click Delete The Account.
4. Before deleting the account, you have the opportunity save the contents of the user’s desktop and documents folders to a folder on the current user’s desktop. To save the user’s desktop and documents, click Keep Files. To delete the files, click Delete Files.
5. Confirm the account deletion by clicking Delete Account.

Keep in mind that in a domain, unless further restrictions are in place with regard to logging on to a workstation, a user might still be able to gain access to the workstation by logging on with a domain account.

Managing Stored Credentials

In Windows 7, you can use Credential Manager to store credentials that can be used to try to automatically log on users to servers, Web sites, and programs. Credentials are stored in an electronic vault (called the Windows vault) that provides easy logon to essential resources, wherever they might be located. If you find that a user frequently has problems logging on to protected resources, such as the company
intranet or an external Internet site, you can create a stored credential for each resource that the user works with.

Credential Manager supports three types of stored credentials:

- **Windows credential** A credential that uses standard Windows authentication (NTLM or Kerberos) and includes a resource location, logon account name, and password.

- **Certificate-based credential** A credential that includes a resource location and uses a certificate saved in the Personal store in Certificate Manager for authentication.

- **Generic credential** A credential that uses basic or custom authentication techniques and includes a resource location, logon account name, and password.

The following sections examine techniques for working with stored credentials.

### Adding Windows or Generic Credentials

Each user account has a unique Windows vault. Entries in the Windows vault are stored in the user’s profile settings and contain information needed to log on to protected resources. If you are logged on to a domain account when you create a Windows vault entry, and the account has a roaming profile (instead of a local or mandatory profile), the information stored in the Windows vault entry is available when you log on to any computer in the domain. Otherwise, the information in the Windows vault entry is available only on the computer on which you create the entry.

**REAL WORLD** When your organization has computers that are in workgroups or homegroups rather than part of your domain, you’ll find that stored credentials can save everyone a lot of time. For example, if Ted uses a computer that is a member of a workgroup for his daily activities but needs to access several different servers in several different locations or domains, you can make this process easier by creating a Windows credential for each resource. Now, no matter how Ted accesses the servers, he can be authenticated automatically and without having to provide alternate credentials. For example, if Ted maps a network drive to FileServer84 and you’ve set up a credential for this server, Ted doesn’t have to select the Connect Using Different Credential option and then provide alternate credentials.

To add an entry to the current logged-on user’s Windows vault, follow these steps:

1. Log on as the user whose Windows vault entries you want to manage. In Control Panel, click User Accounts, and then click Credential Manager. On the Credential Manager page, shown in Figure 5-7, you’ll see a list of current entries by credential type (if there are any credentials).
2. Click Add A Windows Credential or Add A Generic Credential as appropriate for the type of credential you are creating. Then use the options provided to configure the credential (as shown in Figure 5-8). The available fields are as follows:

- **Internet Or Network Address**  The network or Internet resource for which you are configuring the Windows vault entry. This can be a server name, such as fileserver86; a fully qualified domain name for an Internet resource, such as www.microsoft.com; or an address containing a wildcard, such as *.microsoft.com. When you use a server name or fully qualified domain name, the entry is used for accessing a specific server or service. When you use a wildcard, the entry is used for any server in the specified domain. For example, the entry *.microsoft.com could be used to access www.microsoft.com, ftp.microsoft.com, smtp.microsoft.com, and extranet.microsoft.com.

- **User Name**  The user name required by the server, including any necessary domain qualifiers. To use the default domain for a resource, enter only the user name, such as Williams. For a nondefault domain, type the full domain and account name, such as technology\Williams. For an Internet service, type the full service account name, such as Williams@msn.com.

- **Password**  The password required by the server. One of the things most users forget is that whenever they change their password on the server or service, they must also change their password in their Windows vault. If a user forgets to change the password in the Windows vault, repeated
attempts to log on or connect to the server or service might result in the account being locked.

Figure 5-8 Create the Windows vault entry by setting the necessary logon information.

4. Click OK to save the credential.

Adding Certificate-Based Credentials

The Personal certificate store in the user’s profile stores certificates that have been issued to authenticate the user. Once you’ve added a certificate for the user, you can create a credential that uses the certificate to access a resource.

To add an entry for a certificate-based credential to the currently logged-on user’s Windows vault, follow these steps:

1. Log on as the user whose Windows vault entries you want to manage. In Control Panel, click User Accounts, and then click Credential Manager.

2. On the Credential Manager page, you’ll see a list of current entries by credential type (if there are any credentials).

3. Click Add A Certificate-Based Credential. In the Internet Or Network Address field, enter the name of the network or Internet resource for which you are configuring the Windows vault entry. This can be a server name, a fully qualified domain name for an Internet resource, or an address containing a wildcard.

4. Click Select Certificate. In the Select Certificate dialog box, click the personal certificate that you want to use for the resource, and then click OK.

5. Click OK again to save the credential.

Editing Windows Vault Entries

You can edit Windows vault entries at any time, but keep in mind that local Windows vault entries are visible only on the computer on which they were created. This means that if you want to modify an entry, you must log on to the local
workstation where the entry was created. The only exception is for users with roaming profiles. When a user has a roaming profile, Windows vault entries can be edited from any computer where the user is logged on.

Use the following steps to edit a user’s Windows vault entries:

1. Log on as the user whose Windows vault entries you want to manage. In Control Panel, click User Accounts, and then click Credential Manager.
   On the Credential Manager page, you’ll see a list of current entries by credential type.

2. Click the credential entry that you want to edit.

3. Click Edit.

4. As necessary, specify new values for the user name and password or the certificate associated with the credential, and then click Save.

**Backing Up and Restoring the Windows Vault**

You can back up a user’s stored credentials by backing up the Windows vault. After you back up the Windows vault, you can restore the credentials or transfer them to a new computer simply by restoring the Windows vault. In most cases, you should back up the Windows vault to removable media.

To back up a user’s Windows vault, follow these steps:

1. Log on as the user whose Windows vault entries you want to manage. In Control Panel, click User Accounts, and then click Credential Manager.
   On the Credential Manager page, you’ll see a list of current entries by credential type.

2. Click Back Up Vault.

3. On the Stored User Names And Passwords page, click Browse. Use the Save Backup File As dialog box to select a save location and specify a name for the credential backup file. Credential backup files are saved with the .crd file extension. Click Save.

4. Click Next. Press Ctrl+Alt+Delete to switch to the secure desktop. When prompted, enter and confirm a password for the credential backup file.

5. Click Next, and then click Finish.

To restore a user’s Windows vault on the same or different computer, follow these steps:

1. Log on as the user whose Windows vault entries you want to manage. In Control Panel, click User Accounts, and then click Credential Manager.

2. On the Credential Manager page, click Restore Vault.
3. On the Stored User Names And Passwords page, click Browse. Use the Open Backup File As dialog box to select the location and file in which you saved the credential backup files, and then click Open.

4. Click Next. Press Ctrl+Alt+Delete to switch to the secure desktop. When prompted, enter the password for the credential backup file.

5. Click Next, and then click Finish.

Removing Windows Vault Entries

When a user no longer needs a Windows vault entry, you should remove it. To remove a user’s Windows vault entry, follow these steps:

1. Log on as the user whose Windows vault entries you want to manage. In Control Panel, click User Accounts, and then click Credential Manager.

   On the Credential Manager page, you’ll see a list of current entries by credential type.

2. Click the credential entry that you want to remove.

3. Click Remove From Vault. When prompted to confirm the action, click Yes.

   As stated previously, local Windows vault entries can be removed only on the computer on which they were created. When a user has a roaming profile, however, Windows vault entries can be deleted from any computer to which the user is logged on.

Managing Local User Accounts and Groups

Local user accounts and groups are managed much like domain accounts. You can create accounts, manage their properties, reset accounts when they are locked or disabled, and so on. In addition to being able to manage local user accounts with Control Panel, you can create local user accounts with Local Users And Groups or with policy preferences. You should:

- Use Local Users And Groups to manage local user accounts on one computer.
- Use policy preferences to manage local user accounts on multiple computers throughout a domain.

When working with policy preferences, you can manage users and groups through Computer Configuration entries or User Configuration entries. Use Computer Configuration if you want to configure preferences that should be applied to computers regardless of who logs on. Use User Configuration if you want to configure preferences that should be applied to users regardless of which computer they log on to.
Creating Local User Accounts

You can access Local Users And Groups and create a user account by completing the following steps:

1. Click Start, point to All Programs, Administrative Tools, and then click Computer Management. Alternatively, open Control Panel, click System And Security, scroll down, click Administrative Tools, and then double-click Computer Management.

2. Right-click the Computer Management entry in the console tree, and then click Connect To Another Computer on the shortcut menu. You can now select the Windows 7 workstation whose local accounts you want to manage. (Domain controllers do not have local users or groups.)

3. Under the System Tools node, double-click the Local Users And Groups node to expand it, and then select Users. In the details pane, you should see a list of the currently defined user accounts.

4. Right-click Users, and then click New User. This opens the New User dialog box, shown in Figure 5-9.

The fields in the dialog box are used as follows:

- **User Name**  The logon name for the user account. This name should follow the conventions for the local user name policy.
- **Full Name**  The full name of the user, such as William R. Stanek.
- **Description**  A description of the user. Normally, you would type the user’s job title, such as Webmaster. You could also type the user’s job title and department.
- **Password**  The password for the account. This password should follow the conventions of your password policy.
- **Confirm Password**  A field to ensure that you assign the account password correctly. Simply retype the password to confirm it.
- **User Must Change Password At Next Logon**  If this check box is selected, the user must change the password upon logon.
- **User Cannot Change Password**  If this check box is selected, the user can’t change the password.
- **Password Never Expires**  If this check box is selected, the password for this account never expires. This setting overrides the local account policy.
- **Account Is Disabled**  If this check box is selected, the account is disabled and can’t be used. Use this field to temporarily prevent anyone from using an account.
5. Click Create when you have finished configuring the new account. You can access Group Policy and use a preference item to create a user account by completing the following steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. To configure preferences for computers, expand Computer Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups. To configure preferences for users, expand User Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups.

2. Right-click the Local Users And Groups node, point to New, and then select Local User. This opens the New Local User Properties dialog box, shown in Figure 5-10.

3. In the Action list, select Create. The rest of the fields in the dialog box are used as described in the previous procedure.

4. Use the options on the Common tab to control how the preference is applied. In most cases, you’ll want to create the new account only once. If so, select Apply Once And Do Not Reapply.

5. Click OK. The next time Group Policy is refreshed, the preference item will be applied as appropriate for the Group Policy object in which you defined the preference item.
Creating Local Groups for Workstations

You create local groups with Local Users And Groups or with Group Policy. You can access Local Users And Groups and create a local group by completing the following steps:

1. Click Start, point to All Programs, Administrative Tools, and then click Computer Management. Alternatively, open Control Panel, click System And Security, scroll down, click Administrative Tools, and then double-click Computer Management.

2. Right-click the Computer Management entry in the console tree, and then click Connect To Another Computer on the shortcut menu. You can now select the Windows 7 workstation whose local accounts you want to manage. (Domain controllers do not have local users or groups.)

3. Under the System Tools node, double-click the Local Users And Groups node to expand it, and then select Groups. In the details pane, you should see a list of the currently defined group accounts.

4. Right-click Groups, and then select New Group. This opens the New Group dialog box, shown in Figure 5-11.
5. After you type a name and description for the group, click the Add button to open the Select Users dialog box and add names to the group.

6. In the Select Users dialog box, click Locations to select the computer or domain in which the user accounts you want to work with are located.

7. Type the name of a user you want to use in the Enter The Object Names To Select field, and then click Check Names. If matches are found, select the account you want to use, and then click OK. If no matches are found, update the name you entered and try searching again. Repeat this step as necessary, and then click OK when you have finished.

8. The New Group dialog box is updated to reflect your selections. If you made a mistake, select a name and remove it by clicking Remove.

9. Click Create when you have finished adding or removing group members.

You can access Group Policy and use a preference item to create a local group by completing the following steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. To configure preferences for computers, expand Computer Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups. To configure preferences for users, expand User Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups.

2. Right-click the Local Users And Groups node, point to New, and then select Local Group. This opens the New Local Group Properties dialog box, shown in Figure 5-12.
3. In the Action list, select Create. Enter a name and description for the group.

4. Specify whether the current user should be added or removed as a member of the group, or select Do Not Configure For The Current User.

5. To add members to the group, click Add. In the Local Group Member dialog box, click the browse button (the one with the three dots). Use the Select User, Computer Or Group dialog box to select a user or group to add to the local group, and then click OK twice. Repeat this step as necessary.

6. Use the options on the Common tab to control how the preference is applied. In most cases, you should create the new account only once. If so, select Apply Once And Do Not Reapply.

7. Click OK. The next time Group Policy is refreshed, the preference item will be applied as appropriate for the Group Policy object in which you defined the preference item.

**Adding and Removing Local Group Members**

You use Local Users And Groups to add or remove local group members. Complete the following steps:

1. Expand Local Users And Groups in Computer Management, and then select the Groups folder in the left pane. Double-click the group with which you want to work.
2. Click the Add button to add user accounts to the group. This opens the Select Users dialog box. In the Select Users dialog box, type the name of a user you want to use in the Enter The Object Names To Select field, and then click Check Names. If matches are found, select the account you want to use, and then click OK. If no matches are found, update the name you entered and try searching again. Repeat this step as necessary, and then click OK.

3. Use the Remove button to remove user accounts from the group. Simply select the user account you want to remove from the group, and then click Remove.

4. Click OK when you have finished.

You can access Group Policy and use a preference item to add or remove members from a local group by completing the following steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. To configure preferences for computers, expand Computer Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups. To configure preferences for users, expand User Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups.

2. Right-click the Local Users And Groups node, point to New, and then select Local Group. This opens the New Local Group Properties dialog box.

3. In the Action list, select Update to update the group’s settings, or select Replace to delete the group and then re-create it exactly as you specify. If you update a group, you can enter a new name in the Rename To box.

4. Specify whether the current user should be added or removed as a member of the group, or select Do Not Configure For The Current User.

5. Specify whether all existing member users, all existing member groups, or both should be deleted.

6. To add or remove group members, click Add. In the Local Group Member dialog box, in the Action list, select Add To This Group if you are adding a member, or select Remove From This Group if you are removing a member. Next, click the browse button (the one with the three dots). Use the Select User, Computer Or Group dialog box to select a user or group to add to the local group, and then click OK twice. Repeat this step as necessary.

7. Use the options on the Common tab to control how the preference is applied, and then click OK. The next time policy is refreshed, the preference item will be applied as appropriate for the Group Policy object in which you defined the preference item.

Enabling or Disabling Local User Accounts

Local user accounts can become disabled for several reasons. If a user forgets his password and tries to guess it, he might exceed the account policy for bad logon attempts. Another administrator could have disabled the account while a user was
on vacation. When an account is disabled or locked out, you can enable it by using the methods described here.

When an account is disabled, you can enable it on a local computer by completing the following steps:

1. Expand Local Users And Groups in Computer Management, and then select the Users folder in the left pane.
2. In the right pane, double-click the user’s account name, and then clear the Account Is Disabled check box.
3. Click OK.

When an account is locked out, you can enable it on a local computer by completing the following steps:

1. In Local Users And Groups, select the Users folder in the left pane.
2. In the right pane, double-click the user’s account name, and then clear the Account Is Locked Out check box.
3. Click OK.

You can enable or disable accounts and set other account options through policy preferences by completing the following steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. To configure preferences for computers, expand Computer Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups. To configure preferences for users, expand User Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups.
2. In the right pane, double-click the user’s account name to open the related Properties dialog box.
3. Select Update in the Action list. Make any necessary changes, and then click OK. The next time policy is refreshed, the preference item will be applied as appropriate for the Group Policy object in which you defined the preference item.

Creating a Secure Guest Account

In some environments, you might need to set up a Guest account that can be used by visitors. Most of the time, you’ll want to configure the Guest account on a specific computer or computers and carefully control how the account can be used. To create a secure Guest account, I recommend that you perform the following tasks:

- **Enable the Guest account for use.** By default, the Guest account is disabled, so you must enable it to make it available. To do this, access Local Users And Groups in Computer Management, and then select the Users folder. Double-click Guest, and then clear the Account Is Disabled check box. Click OK.
Set a secure password for the Guest account. By default, the Guest account has a blank password. To improve security on the computer, you should set a password for the account. In Local Users And Groups, right-click Guest, and then select Set Password. Click Proceed at the warning prompt. Type the new password and then confirm it. Click OK twice.

Ensure that the Guest account cannot be used over the network. The Guest account shouldn’t be accessible from other computers. If it is, users at another computer could log on over the network as a guest. To prevent this, start the Local Security Policy tool from the Administrative Tools menu, or type secpol.msc at the command prompt. Then, under Local Policies\User Rights Assignment, check that the Deny Access To This Computer From The Network policy lists Guest as a restricted account.

Prevent the Guest account from shutting down the computer. When a computer is shutting down or starting up, it is possible that a guest user (or anyone with local access) could gain unauthorized access to the computer. To help deter this, you should be sure that the Guest account doesn’t have the Shut Down The System user right. In the Local Security Policy tool, expand Local Policies\User Rights Assignment, and ensure that the Shut Down The System policy doesn’t list the Guest account.

Prevent the Guest account from viewing event logs. To help maintain the security of the system, the Guest account shouldn’t be allowed to view the event logs. To be sure this is the case, start Registry Editor by typing regedit at a command prompt, and then access the HKLM\SYSTEM\CurrentControlSet\services\Eventlog key. Here, among others, you’ll find three important subkeys: Application, Security, and System. Make sure each of these subkeys has a DWORD value named RestrictGuestAccess with a value of 1.

Renaming Local User Accounts and Groups

When you rename an account, you give it a new label. Because the SID for the account remains the same, the permissions and properties associated with the account don’t change. To rename an account while you are accessing a local computer, complete the following steps:

1. In Local Users And Groups, select the Users or Groups folder, as appropriate.

2. Right-click the account name, and then click Rename. Type the new account name, and then click a different entry.

To rename an account using Group Policy, complete the following steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. To configure preferences for computers, expand Computer Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups. To configure preferences for users, expand User Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups.
2. Do one of the following:
   - If a preference item already exists for the user or group, double-click the user or group name to open the related Properties dialog box. Select Update in the Action list. In the Rename To box, type the new account name, and then click OK.
   - If a preference item doesn’t already exist for the user or group, you need to create one using the techniques discussed previously. Because you want to rename the user or group, select Update in the Action list, and then type the new account name in the Rename To box.

Deleting Local User Accounts and Groups

Deleting an account permanently removes it. Once you delete an account, if you create another account with the same name, you can’t automatically get the same permissions because the SID for the new account won’t match the SID for the account you deleted.

Because deleting built-in accounts can have far-reaching effects on the workstation, Windows 7 doesn’t let you delete built-in user accounts or group accounts. In Local Users And Groups, you can remove other types of accounts by selecting them and pressing the Delete key or by right-clicking and then clicking Delete. When prompted, click Yes.

**NOTE** When you delete a user account using Local Users And Groups, Windows 7 doesn’t delete the user’s profile, personal files, or home directory. If you want to delete these files and directories, you have to do it manually.

To delete an account using Group Policy, complete the following steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. To configure preferences for computers, expand Computer Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups. To configure preferences for users, expand User Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups.

2. Do one of the following:
   - If a preference item already exists for the user or group, double-click the user or group name to open the related Properties dialog box. Select Delete in the Action list. On the Common tab, set the appropriate options, such as Apply Once And Do Not Reapply, and then click OK.
   - If a preference item doesn’t already exist for the user or group, you need to create one for the user or group using the techniques discussed previously. Be sure to select Delete in the Action list, and then select the appropriate options on the Common tab.
Managing Remote Access to Workstations

Windows 7 has several remote connectivity features. With Remote Assistance, users can send invitations to support technicians, enabling the technicians to service a computer remotely. With Remote Desktop, users can connect remotely to a computer and access its resources. In this section, you’ll learn how to configure Remote Assistance and Remote Desktop. Typically, neither the Remote Assistance feature nor the Remote Desktop feature is enabled, and you must enable these features manually.

Remote Assistance and Remote Desktop can function through Network Address Translation (NAT) firewalls. Remote Assistance also has built-in diagnostic tools. To allow for easier troubleshooting and escalation of support issues, two different support staff can connect to a remote computer simultaneously. When troubleshooting requires restarting the computer, Remote Assistance sessions are reestablished automatically after the computer being diagnosed reboots.

Prior to using Remote Assistance, you may want users to use the Problem Steps Recorder to create a step-by-step record of a problem they are experiencing. The Problem Steps Recorder is very easy to use. To start and use the Problem Steps Recorder, a user needs to complete the following steps:

1. To start the Problem Steps Recorder, have the user click Start, type psr, and then press Enter. Once the tool is started, the user can prepare the environment and then begin recording the problem.

2. To turn on recording, the user clicks Start Record. Once recording has started, the user can perform the action that isn’t working and click Add Comment to add comments as she works.

3. When the user experiences the problem and the related errors have been displayed, she can stop recording by clicking Stop Record.

4. When the user stops recording, the Save As dialog box is displayed. The user selects a save location and name for the Zip file that contains the record of the problem in an .mht file.

5. The user can send the Zip file to a support technician in an e-mail message or by copying it to a file share. To review the recorded problem steps, you double-click the Zip file to display its contents in Windows Explorer and then double-click the enclosed .mht file to open it in Internet Explorer.

6. You’ll then see screen captures for all the steps the user took while the problem was being recorded. After the screen captures, you’ll find additional details for each step that are generated automatically. You can use this information along with any user comments to help you troubleshoot the problem.
Configuring Remote Assistance

Remote Assistance is a useful feature for help desks, whether in-house or outsourced. A user can allow support personnel to view and take control of his or her desktop. This feature can be used to walk users through a complex process or to manage system settings while they watch the progress of the changes. The key to Remote Assistance is in the access levels you grant.

When enabled, Remote Assistance is configured by default to let support personnel view and control computers. Because users can send assistance invitations to internal and external resources, this could present a security concern for organizations. To reduce potential security problems, you might want to allow support staff to view but not control computers. A new restriction for Windows 7 is to allow connections only from computers running Windows 7 or later. This option is helpful to limit any possible compatibility issues and to ensure that any security enhancements in Windows 7 or later operating systems are available within Remote Assistance sessions.

Another key aspect of Remote Assistance you can control is the time limit for invitations. The default maximum time limit is 6 hours; the absolute maximum time limit you can assign is 30 days. Although the intent of a multiple-day invitation is to give support personnel a time window in which to respond to requests, it also means that they could use an invitation to access a computer over a period of 30 days. For instance, suppose you send an invitation with a 30-day time limit to a support person who resolves the problem the first day. That person would still have access to the computer for another 29 days, which wouldn’t be desirable for security reasons. To reduce the risk to your systems, you’ll usually want to reduce the default maximum time limit considerably—say, to 1 hour. If the problem is not solved in the allotted time period, you can issue another invitation.

To configure Remote Assistance, follow these steps:

1. In Control Panel, click System And Security, and then click System.
2. On the System page, click Remote Settings in the left pane. This opens the System Properties dialog box with the Remote tab displayed, as shown in Figure 5-13.
3. To disable Remote Assistance, clear the Allow Remote Assistance Connections To This Computer check box, and then click OK. Skip the remaining steps.
4. To enable Remote Assistance, select Allow Remote Assistance Connections To This Computer.
Figure 5-13 Use the Remote tab options to configure remote access to the computer.

5. Click Advanced. This displays the Remote Assistance Settings dialog box, shown in Figure 5-14.

Figure 5-14 The Remote Assistance Settings dialog box is used to set limits for Remote Assistance.
6. The Allow This Computer To Be Controlled Remotely option sets limits for Remote Assistance. When selected, this setting allows assistants to view and control the computer. To provide view-only access to the computer, clear this check box.

7. The Invitations options control the maximum time window for invitations. You can set a value in minutes, hours, or days, up to a maximum of 30 days. If you set a maximum limit value of 10 days, for example, a user can create an invitation with a time limit up to but not more than 10 days. The default maximum expiration limit is 6 hours.

8. Click OK twice when you have finished configuring Remote Assistance options.

In Group Policy, you can manage Remote Assistance using the policy settings shown in Table 5-2. These settings are found in the Administrative Templates policies for Computer Configuration under the paths shown.

**TABLE 5-2 Policy Settings for Managing Remote Assistance**

<table>
<thead>
<tr>
<th>SETTING</th>
<th>PATH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Only Vista Or Later Connections</td>
<td>\System\Remote Assistance</td>
</tr>
<tr>
<td>Do Not Allow Windows Messenger To Be Run</td>
<td>Windows Components\Windows Messenger</td>
</tr>
<tr>
<td>Offer Remote Assistance</td>
<td>\System\Remote Assistance</td>
</tr>
<tr>
<td>Solicited Remote Assistance</td>
<td>\System\Remote Assistance</td>
</tr>
<tr>
<td>Turn On Session Logging</td>
<td>\System\Remote Assistance</td>
</tr>
</tbody>
</table>

**Configuring Remote Desktop Access**

Unlike Remote Assistance, which provides only a view of the current user’s desktop, Remote Desktop provides several levels of access:

- If a user is logged on to the desktop locally and then tries to log on remotely, the local desktop locks, and the user can access all of the running applications just as though he or she were sitting at the keyboard. This feature is useful for users who want to work from home or other locations outside the office, enabling them to continue to work with applications and documents that they were using prior to leaving the office.

- If a user is listed on the workstation’s Remote Access list and is not otherwise logged on, he or she can initiate a new Windows session. The Windows session behaves as though the user were sitting at the keyboard. It can even be used when other users are also logged on to the computer. In this way, multiple users can share a single workstation and use its resources.
Remote Desktop is not enabled by default. You must specifically enable it to allow remote access to the workstation. When it is enabled, any member of the Administrators group can connect to the workstation. Other users must be placed on a remote access list to gain access to the workstation. To configure remote access, follow these steps:

1. In Control Panel, click System And Security, and then click System.
2. On the System page, click Remote Settings in the left pane. This opens the System Properties dialog box to the Remote tab.
3. To disable Remote Desktop, select Don’t Allow Connections To This Computer, and then click OK. Skip the remaining steps.
4. To enable Remote Desktop, you have two options. You can:
   - Select Allow Connections From Computers Running Any Version Of Remote Desktop to allow connections from any version of Windows.
   - Select Allow Connections Only From Computers Running Remote Desktop With Network Level Authentication to allow connections only from Windows 7 or later computers (and computers with secure network authentication).
5. Click Select Users. This displays the Remote Desktop Users dialog box, shown in Figure 5-15.

![Remote Desktop Users](image)

**FIGURE 5-15** Specify the additional users allowed to make Remote Desktop connections.

6. To grant Remote Desktop access to a user, click Add. This opens the Select Users dialog box. In the Select Users dialog box, click Locations to select the computer or domain in which the users you want to work with are located. Type the name of a user you want to work with in the Enter The Object Names To Select field, and then click Check Names. If matches are found, select the account you want to use and then click OK. If no matches are
found, update the name you entered and try searching again. Repeat this step as necessary, and then click OK.

7. To revoke remote access permissions for a user account, select the account and then click Remove.

8. Click OK twice when you have finished.

Windows Firewall must be configured to allow inbound Remote Desktop exceptions. You can configure this on a per-computer basis in Windows Firewall for the domain profile and the standard profile. In Group Policy, you can configure this exception and manage Remote Desktop by using the policy settings shown in Table 5-3. These settings are found in the Administrative Templates policies for Computer Configuration under the path shown.

**TABLE 5-3** Policy Settings for Managing Remote Desktop

<table>
<thead>
<tr>
<th>SETTING</th>
<th>COMPUTER CONFIGURATION PATH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow .Rdp Files From Unknown Publishers</td>
<td>\Remote Desktop Connection Client</td>
</tr>
<tr>
<td>Allow .Rdp Files From Valid Publishers And User’s Default .Rdp Settings</td>
<td>\Remote Desktop Connection Client</td>
</tr>
<tr>
<td>Always Prompt For Password Upon Connection</td>
<td>\Remote Desktop Session Host\Security</td>
</tr>
<tr>
<td>Automatic Reconnection</td>
<td>\Remote Desktop Session Host\Connections</td>
</tr>
<tr>
<td>Configure Server Authentication For Client</td>
<td>\Remote Desktop Connection Client</td>
</tr>
<tr>
<td>Deny Logoff Of An Administrator Logged In To The Console Session</td>
<td>\Remote Desktop Session Host\Connections</td>
</tr>
<tr>
<td>Do Not Allow Local Administrators To Customize Permissions</td>
<td>\Remote Desktop Session Host\Security</td>
</tr>
<tr>
<td>Do Not Allow Passwords To Be Saved</td>
<td>\Remote Desktop Connection Client</td>
</tr>
<tr>
<td>Limit Maximum Color Depth</td>
<td>\Remote Desktop Session Host\Remote Session Environment</td>
</tr>
<tr>
<td>Limit Maximum Display Resolution</td>
<td>\Remote Desktop Session Host\Remote Session Environment</td>
</tr>
<tr>
<td>Limit Maximum Number Of Monitors</td>
<td>\Remote Desktop Session Host\Remote Session Environment</td>
</tr>
</tbody>
</table>
Making Remote Desktop Connections

As an administrator, you can make Remote Desktop connections to Windows servers and workstations. With Windows 2000 Server, Remote Desktop connections are enabled by installing Terminal Services and then configuring Terminal Services in remote access mode. With Windows XP Professional and later versions, Remote Desktop is installed automatically, but it is normally not enabled until you do so as discussed in the preceding section of this chapter. Once remote access is enabled on a computer, all administrators have remote access to that computer. Other users can be granted remote access as well.

To make a Remote Desktop connection to a server or workstation, follow these steps:

1. At a command prompt, type **mstsc**, or click Start, point to All Programs, Accessories, and then click Remote Desktop Connection. Click the Options button. This displays the Remote Desktop Connection dialog box, shown in Figure 5-16.
In the Remote Desktop Connection dialog box, type the name of the computer to which you want to connect, and then click Connect.

2. In the Computer field, type the name of the computer to which you want to connect. If you don’t know the name of the computer, use the drop-down list to choose an available computer, or select Browse For More in the drop-down list to display a list of domains and computers in those domains.

3. Specify additional options as necessary. If you’ve configured stored credentials for the computer, your saved credentials will be used automatically. You can edit or delete the credentials as necessary.

4. Click Connect. If you haven’t previously stored credentials for the computer, type your credentials when prompted, and then click OK. If the connection is successful, you’ll see the Remote Desktop window on the selected computer, and you’ll be able to work with resources on the computer. In the case of a failed connection, check the information you provided and then try to connect again.

**Note** Clicking Options in the Remote Desktop Connection dialog box displays additional options for creating and saving connections. These options enable you to change the display size for the Remote Desktop, manage connections to local resources (such as printers, serial ports, and disk drives), run programs automatically on connection, and enable or disable local caching and data compression.
Administrators and support staff often install and configure applications that are used on desktop computers. You need to install and configure applications before deploying new computers, install new applications on computers when the programs are requested, and update applications when new versions become available. Also, as users install additional applications, you might be called on to help troubleshoot installation problems or to help uninstall programs. Most program installation problems are fairly easy to solve if you know what to look for. Other problems are fairly difficult to resolve and require more work than you might expect. In this chapter, you’ll learn how User Account Control (UAC) affects how you install and run applications and about techniques for installing, uninstalling, and maintaining programs.

Managing Application Virtualization and Run Levels

User Account Control (UAC) changes the way that applications are installed and run, where applications write data, and what permissions applications have. In this section, I’ll look at how UAC affects application installation, from application security tokens to file and registry virtualization to run levels. This information is essential when you are installing and maintaining applications on Windows 7.
Application Access Tokens and Location Virtualization

All applications used with Windows 7 are divided into two general categories:

- **UAC-compliant** Any application written specifically for Windows Vista or Windows 7 is considered a compliant application. Applications certified as complying with the Windows 7 architecture have the UAC-compliant logo.

- **Legacy** Any application written for Windows XP or an earlier version of Windows is considered a legacy application.

The distinction between UAC-compliant applications and legacy applications is important because of the architectural changes required to support UAC. UAC-compliant applications use UAC to reduce the attack surface of the operating system. They do this by preventing unauthorized programs from installing or running without the user’s consent and by restricting the default privileges granted to applications. These measures make it harder for malicious software to take over a computer.

**Note** The Windows 7 component responsible for UAC is the Application Information service. This service facilitates the running of interactive applications with an “administrator” access token. You can see the difference between the administrator user and standard user access tokens by opening two Command Prompt windows, running one with elevation (right-click, and then click Run As Administrator), and the other as a standard user. In each window, type `whoami /all` and compare the results. Both access tokens have the same security identifiers (SIDs), but the elevated, administrator user access token will have more privileges than the standard user access token.

All applications that run on Windows 7 derive their security context from the current user’s access token. By default, UAC turns all users into standard users even if they are members of the Administrators group. If an administrator user consents to the use of her administrator privileges, a new access token is created for the user. It contains all the user’s privileges, and this access token—rather than the user’s standard access token—is used to start an application or process.

In Windows 7, most applications can run using a standard user access token. Whether applications need to run with standard or administrator privileges depends on the actions the application performs. Applications that require administrator privileges, referred to as **administrator user applications**, differ from applications that require standard user privileges, referred to as **standard user applications**, in the following ways:

- **Administrator user applications** require elevated privileges to run and perform core tasks. Once started in elevated mode, an application with a user’s administrator access token can perform tasks that require administrator privileges and can also write to system locations of the registry and the file system.
Standard user applications do not require elevated privileges to run or to perform core tasks. Once started in standard user mode, an application with a user’s standard access token must request elevated privileges to perform administration tasks. For all other tasks, the application should not run using elevated privileges. Further, the application should write data only to nonsystem locations of the registry and the file system.

Applications not written for Windows 7 run with a user’s standard access token by default. To support the UAC architecture, these applications run in a special compatibility mode and use file system and registry virtualization to provide “virtualized” views of file and registry locations. When an application attempts to write to a system location, Windows 7 gives the application a private copy of the file or registry value. Any changes are then written to the private copy, and this private copy is then stored in the user’s profile data. If the application attempts to read or write to this system location again, it is given the private copy from the user’s profile to work with. By default, if an error occurs when the application is working with virtualized data, the error notification and logging information show the virtualized location rather than the actual location that the application was trying to work with.

Application Integrity and Run Levels

The focus on standard user and administrator privileges also changes the general permissions required to install and run applications. In Windows XP and earlier versions of Windows, the Power Users group gave users specific administrator privileges to perform basic system tasks when installing and running applications. Applications written for Windows 7 do not require the use of the Power Users group. Windows 7 maintains it only for legacy application compatibility.

As part of UAC, Windows 7 by default detects application installations and prompts users for elevation to continue the installation. Installation packages for UAC-compliant applications use application manifests that contain run-level designations to help track required privileges. Application manifests define the application’s privileges as one of the following:

- **RunAsInvoker** Run the application with the same privileges as the user. Any user can run the application. For a standard user or a user who is a member of the Administrators group, the application runs with a standard access token. The application runs with higher privileges only if the parent process from which it is started has an administrator access token. For example, if you open an elevated Command Prompt window and then launch an application from this window, the application runs with an administrator access token.

- **RunAsHighest** Run the application with the highest privileges of the user. The application can be run by both administrator users and standard users. The tasks the application can perform depend on the user’s privileges. For a standard user, the application runs with a standard access token. For a user who is a member of a group with additional privileges, such as the Backup
Operators, Server Operators, or Account Operators group, the application runs with a partial administrator access token that contains only the privileges the user has been granted. For a user who is a member of the Administrators group, the application runs with a full administrator access token.

- **RunAsAdmin** Run the application with administrator privileges. Only administrators can run the application. For a standard user or a user who is a member of a group with additional privileges, the application runs only if the user can be prompted for credentials required to run in elevated mode or if the application is started from an elevated process, such as an elevated Command Prompt window. For a user who is a member of the Administrators group, the application runs with an administrator access token.

To protect application processes, Windows 7 labels them with integrity levels ranging from high to low. Applications that modify system data, such as Disk Management, are considered high integrity. Applications performing tasks that could compromise the operating system, such as Windows Internet Explorer 8 in Windows 7, are considered low integrity. Applications with lower integrity levels cannot modify data in applications with higher integrity levels.

Windows 7 identifies the publisher of any application that attempts to run with an administrator’s full access token. Then, depending on that publisher, Windows 7 marks the application as belonging to one of the following three categories:

- Windows Vista / Windows 7
- Publisher verified (signed)
- Publisher not verified (unsigned)

To help you quickly identify the potential security risk of installing or running the application, a color-coded elevation prompt displays a particular message depending on the category to which the application belongs:

- If the application is from a blocked publisher or is blocked by Group Policy, the elevation prompt has a red background and displays the message “The application is blocked from running.”
- If the application is administrative (such as Computer Management), the elevation prompt has a blue-green background and displays the message “Windows needs your permission to continue.”
- If the application has been signed by Authenticode and is trusted by the local computer, the elevation prompt has a gray background and displays the message “A program needs your permission to continue.”
- If the application is unsigned (or is signed but not yet trusted), the elevation prompt has a yellow background and red shield icon and displays the message “An unidentified program wants access to your computer.”

Prompting on the secure desktop can be used to further secure the elevation process. The secure desktop safeguards the elevation process by preventing spoofing of the elevation prompt. The secure desktop is enabled by default in Group...
Policy, as discussed in the section “Optimizing User Account Control and Admin Approval Mode” in Chapter 5.

**Setting Run Levels**

By default, only applications running with a user’s administrator access token run in elevated mode. Sometimes, you’ll want an application running with a user’s standard access token to be in elevated mode. For example, you might want to start the Command Prompt window in elevated mode so that you can perform administration tasks.

In addition to application manifests (discussed in the previous section), Windows 7 provides two different ways to set the run level for applications:

- Run an application once as an administrator.
- Always run an application as an administrator.

To run an application once as an administrator, right-click the application’s shortcut or menu item, and then click Run As Administrator. If you are using a standard account and prompting is enabled, you are prompted for consent before the application is started. If you are using a standard user account and prompting is disabled, the application will fail to run. If you are using an administrator account and prompting for consent is enabled, you are prompted for consent before the application is started.

Windows 7 also enables you to mark an application so that it always runs with administrator privileges. This approach is useful for resolving compatibility issues with legacy applications that require administrator privileges. It is also useful for UAC-compliant applications that normally run in standard mode but that you use to perform administration tasks. As examples, consider the following:

- A standard application written for Windows 7 is routinely run in elevated mode and used for administration tasks. To eliminate the need to right-click the application shortcut and choose Run As Administrator before running the application, you can mark it to always run as an administrator.

- An application written for Windows XP or an earlier version of Windows requires administrator privileges. Because this program is configured to use standard mode by default under Windows 7, the program isn’t running properly and is generating numerous errors. To resolve the compatibility problem, you could create an application compatibility shim using the Windows Application Compatibility Toolkit (ACT) version 5.5 or later. As a temporary solution, you can mark the application to always run as an administrator.

**NOTE** You cannot mark system applications or processes to always run with administrator privileges. Only nonsystem applications and processes can be marked to always run at this level.
The Windows Application Compatibility Toolkit (ACT) is a solution for administrators that requires no reprogramming of an application. ACT can help you resolve common compatibility problems. For example, some programs run only on a specific operating system or when the user is an administrator. Using ACT, you can create a shim that responds to the application inquiry about the operating system or user level with a True statement, which allows the application to run. ACT also can help you create more in-depth solutions for applications that try to write to protected areas of the operating system or use elevated privileges when they don’t need to. ACT can be downloaded from the Microsoft Download Center (http://download.microsoft.com).

You can mark an application to always run as an administrator by following these steps:

1. On the Start menu, locate the program that you want to always run as an administrator.
2. Right-click the application’s shortcut, and then click Properties.
3. In the Properties dialog box, click the Compatibility tab, shown in Figure 9-1.

![FIGURE 9-1 Access the Compatibility tab.]

4. Do one of the following:
   - To apply the setting to the currently logged-on user, select the Run This Program As An Administrator check box, and then click OK.
   - To apply the setting to all users on the computer and regardless of which shortcut is used to start the application, click Change Setting For All Users to display the Properties dialog box for the application’s .exe file, select the Run This Program As An Administrator check box, and then click OK twice.
**NOTE** If the Run This Program As An Administrator option is unavailable, it means that the application is blocked from always running at an elevated level, the application does not require administrator credentials to run, or you are not logged on as an administrator.

The application will now always run using an administrator access token. Keep in mind that if you are using a standard account and prompting is disabled, the application will fail to run.

**Optimizing Virtualization and Installation Prompting for Elevation**

With regard to applications, two areas of User Account Control can be customized:

- Automatic installation detection and prompting
- Virtualization of write failures

In Group Policy, you can configure these features by using the Administrative Templates policies for Computer Configuration under Windows Settings\Security Settings\Local Policies\Security Options. The security settings are as follows:

- **User Account Control: Detect Application Installations And Prompt For Elevation**  
  Determines whether Windows 7 automatically detects application installation and prompts for elevation or consent. (This setting is enabled by default in Windows 7.) If you disable this setting, users are not prompted, in which case, the users will not be able to elevate permissions by supplying administrator credentials.

- **User Account Control: Virtualize File And Registry Write Failures To Per-User Locations**  
  Determines whether file and registry virtualization is on or off. Because this setting is enabled by default, error notifications and error logging related to virtualized files and registry values are written to the virtualized location rather than the actual location to which the application was trying to write. If you disable this setting, the application will silently fail when trying to write to protected folders or protected areas of the registry.

In a domain environment, you can use Active Directory–based Group Policy to apply the security configuration you want to a particular set of computers. You can also configure these settings on a per-computer basis by using local security policy. To do this, follow these steps:

1. Click Start, point to All Programs, Administrative Tools, and then click Local Security Policy. This starts the Local Security Policy console.
2. In the console tree, under Security Settings, expand Local Policies, and then select Security Options.
3. Double-click the setting you want to work with, make any necessary changes, and then click OK.
Installing Programs: The Essentials

Program installation is fairly straightforward. Not so straightforward are troubleshooting the many things that can go wrong and fixing problems. To solve problems that might occur, you first need to understand the installation process. In many cases, the typical installation process starts when Autorun is triggered. Autorun in turn invokes a setup program. Once the setup program starts, the installation process can begin. Part of the installation process involves checking the user’s credentials to ensure that he or she has the appropriate privileges to install the program and prompting for consent if the user doesn’t. As part of installing a program, you might also need to make the program available to all or only some users on a computer.

Occasionally, Windows might not be successful in detecting the required installation permissions. This can occur if the installation manifest for the program has an embedded RequestedExecutionLevel setting that has a value set as RequireAdministrator. Because the RequestedExecutionLevel setting overrides what the installer detects in Windows, the installation process fails any time you run the installer with standard user permissions. To solve this problem, back out of the failed installation by exiting, canceling the installation, or taking another appropriate action. Next, locate the executable file for the installer. Right-click this file, and then click Run As Administrator to restart the installation process with administrator privileges.

Additionally, it is important to understand that in Windows 7 and Windows Server 2008 Release 2, Application Control policies replace Software Restriction policies. Software Restriction policies control the applications that users can install and run on Windows 2000, Windows XP, and Windows Vista. Application Control policies control the applications that users can install and run on Windows 7 and Windows Server 2008 Release 2. Keep the following in mind:

- When you are editing a Group Policy object (GPO), you can create and manage Software Restriction policies by using settings for computers under Computer Configuration\Policies\Windows Settings\Security Settings\Software Restriction Policies and settings for users under User Configuration\Policies\Windows Settings\Security Settings\Software Restriction Policies. Enforcement settings control how restrictions are applied. Designated file types determine what is and what is not considered an executable program.

- When you are editing a GPO, you can create and manage Application Control policies by using settings for computers under Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies. You can now create separate rules for executable files, Windows installer files, and script files. Rules can be applied by publisher, file path, or file hash. A publisher rule gives you the most flexibility, enabling you to specify which products and versions to allow. For example, you could allow Microsoft Word 2003 or later.
Working with Autorun

When you insert an application CD or DVD into a CD or DVD drive, Windows 7 checks for a file named Autorun.inf. If present, Autorun.inf specifies the action that the operating system should take and might also define other installation parameters. Autorun.inf is a text-based file that can be opened in any standard text editor. If you were to examine the contents of one, you’d see something similar to the following code:

```
[autorun]
OPEN=SETUP.EXE AUTORUN=1
ICON=SETUP.EXE,4
SHELL=OPEN
DisplayName=Microsoft Digital Image Suite 9
ShortName=PIS
PISETUP=PIP\pisetup.exe
```

This Autorun.inf file opens a file named Setup.exe when the CD or DVD is inserted into the CD or DVD drive. Because Setup.exe is an actual program, this program is invoked. The Autorun.inf file also specifies an icon to use, the status of the shell, the program display name, the program’s short name, and an additional parameter, which in this case is the location of another setup program to run.

The file that Autorun.inf specifies to open won’t always be a program. Consider the following example:

```
[autorun]
OPEN=Autorun\ShelExec default.htm
```

This Autorun.inf file executes via the shell and opens a file named Default.htm in the computer’s Web browser. It’s important to note that even in this case, the document opened in the Web browser contains links that point to a setup program.

**TIP** With an application CD or DVD in a drive, you can restart the Autorun process at any time. Simply open and then close the drive bay.

Application Setup and Compatibility

Most applications have a setup program that uses InstallShield, Wise Install, or Microsoft Windows Installer. When you start the setup program, the installer helps track the installation process and should also make it possible to easily uninstall the program when you need to. If you are installing an older application, the setup program might use an older version of one of these installers, and this might mean the uninstall process won’t completely uninstall the program.

Even if you are absolutely certain that a program has a current installer, you should consider the possibility that you will need to recover the system if something goes wrong with the installation. To help ensure that you can recover your system, check that System Restore is enabled for the drive on which you are installing.
the program so that System Restore can create an automatic checkpoint before installing the program.

While the installers for most current programs automatically trigger the creation of a restore point before making any changes to a computer, the installers for older programs might not. You can manually create a restore point as discussed in Chapter 17, “Handling Maintenance and Support Tasks.” Then, if you run into problems, you can try to uninstall the program or use System Restore to recover the system to the state it was in prior to the program’s installation.

Before installing any application, you should check to see whether it is compatible with Windows 7. To determine compatibility, you can do the following:

- Check the software packaging, which should specify whether the program is compatible. Look for the Windows 7 logo.
- Check the software developer’s Web site for a list of compatible operating systems.

**NOTE** As part of the compatibility check, look for updates or patches for the program. If any are available, install them after installing the program.

Windows 7 attempts to recognize potential compatibility problems before you install applications. If it detects one, you might see a Program Compatibility Assistant dialog box after you start a program’s installer. Often, this dialog box contains information about the known compatibility issues with the program, and in many cases it displays a possible solution. For example, you might be advised to install the latest service pack for the program before running the program on the computer. In some cases, the Program Compatibility Assistant might display the message “This program is blocked due to compatibility issues.” Here, the program is blocked because it causes a known stability issue with Windows, and you can’t create an immediate fix to work around the problem. Your only options are to click the Check For Solutions Online button or click Cancel. If you check for solutions online, the typical solution requires you to purchase an updated version of the program. If you cancel, you stop the installation process without checking for possible solutions.

If the installation continues but fails for any reason before it is fully complete (or to properly notify the operating system regarding completion), you’ll also see a Program Compatibility Assistant dialog box. In this case, if the program installed correctly, click This Program Installed Correctly. If the program didn’t install correctly, click Reinstall Using Recommended Settings to allow the Program Compatibility Assistant to apply one or more compatibility fixes, and then try again to run the installer.

When you start programs, Windows 7 uses the Program Compatibility Assistant to automatically make changes for known compatibility issues as well. If the Program Compatibility Assistant detects a known compatibility issue when you run an application, it notifies you about the problem and provides possible solutions for resolving the problem automatically. You can then allow the Program Compatibility
Assistant to reconfigure the application for you, or you can manually configure compatibility as discussed in the section “Configuring Program Compatibility” later in this chapter.

For legacy applications, you can also use the Compatibility Administrator (Compatadmin.exe), provided in the Windows Application Compatibility Toolkit, to create an application manifest that sets the application’s run level. The Compatibility Administrator can also help identify other types of compatibility issues with legacy applications. The Windows Application Compatibility Toolkit (ACT) can be downloaded from the Microsoft Download Center (http://download.microsoft.com).

Making Programs Available to All or Selected Users

Usually when you install a program, the program is available to all users on a computer. This occurs because the program’s shortcuts are placed in the Start Menu\Programs folder (%SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs) for all users so that any user who logs on to the system has access to the program. Some programs prompt you during installation to choose whether you want to install the program for all users or only for the currently logged-on user. Other programs simply install themselves only for the current user.

If setup installs a program so that it is available only to the currently logged-on user and you want other users to have access to the program, you need to take one of the following actions:

- Log on to the computer with each user account that should have access to the program, and then rerun setup to make the program available to these users. You also need to run setup again when a new user account is added to the computer and that user needs access to the program.

- For programs that don’t require per-user settings to be added to the registry before running, you can in some cases make the program available to all users on a computer by adding the appropriate shortcuts to the Start Menu\Programs folder for all users. Copy or move the program shortcuts from the currently logged-on user’s profile to the Start Menu\Programs folder for all users.

If you want to make a program available to all users on a computer, you can copy or move a program’s shortcuts by completing the following steps:

1. Right-click the Start button, and then click Open Windows Explorer. In Windows Explorer, navigate to the currently logged on user’s Programs folder. This is a hidden folder under %UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu.

2. In the Programs folder, right-click the folder for the program group or the shortcut you want to work with, and then click Copy or Cut on the shortcut menu.
3. Next, navigate to the all-users Start Menu\Programs folder. This hidden folder is under %SystemDrive%\ProgramData\Microsoft\Windows\Start Menu.

4. In the Programs folder, right-click an open space, and then click Paste. The program group or shortcut should now be available to all users of the computer.

**NOTE** In the %SystemDrive%\Users folder, you’ll find a folder called All Users. If you are aware of this folder, you might wonder why you didn’t copy the program’s shortcut for all users to a subfolder of this folder. Well, the reason is that %SystemDrive%\Users\All Users is a symbolic link to %SystemDrive%\ProgramData. A symbolic link is a pointer to where a folder actually exists. When you are working with the command prompt (Cmd.exe), you can view symbolic links and reparse points (junctions) in the current directory by entering `dir /al`.

If you want to make a program available only to the currently logged-on user rather than all users on a computer, you can move a program’s shortcuts by completing the following steps:

1. Right-click the Start button, and then click Open Windows Explorer. In Windows Explorer, navigate to the all-users Start Menu folder. This hidden folder is under %SystemDrive%\ProgramData\Microsoft\Windows\Start Menu.

2. In the Programs folder, right-click the folder for a program group or the program shortcut that you want to work with, and then click Cut.

3. In Windows Explorer, navigate to the currently logged-on user’s Programs folder. This is a hidden folder under %UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu.

4. In the Programs folder, right-click an open space, and then click Paste. The program group or shortcut should now be available only to the currently logged-on user.

**NOTE** Moving a program group or shortcut hides the fact that the program is available on the computer—it doesn’t prevent other users from running the program by using the Run dialog box or Windows Explorer.

### Deploying Applications Through Group Policy

You can make applications available to users over the network through Group Policy. When you use Group Policy to deploy applications, you have two distribution options:

- The first option is to assign the application to users or computers. When an application is assigned to a computer, it is installed the next time the
computer is started and is available to all users of that computer the next time users log on. When an application is assigned to a user, it is installed the next time the user logs on to the network. An assigned application can also be configured to be installed on first use. In this configuration, the application is made available through shortcuts on the user’s desktop or Start menu. When install-on-first-use configured, the application is installed when the user clicks a shortcut to launch the application.

The second option is to publish the application and make it available for installation. When you publish an application, the application can be made available through extension activation. With extension activation configured, the program is installed when a user opens any file with an extension associated with the application. For example, if a user double-clicks a file with a .doc or .docx extension, Microsoft Word could be installed automatically.

You deploy applications for computers using a Microsoft Windows Installer Package (.msi file) and policies under Computer Configuration\Policies\Software Settings\Software Installation You deploy applications for users using a Windows Installer Package (.msi file) and policies under User Configuration\Policies\Software Settings\Software Installation. The basic steps required to deploy applications through Group Policy are as follows:

1. For clients to access the Windows Installer Package, it must be located on a network share. As necessary, copy the Windows Installer Package (.msi file) to a network share that is accessible by the appropriate users.

2. In the Group Policy Management Editor, open the Group Policy object (GPO) from which you want to deploy the application. After it is deployed, the application is available to all clients to which the GPO applies. This means the application is available to computers and users in the related domain, site, or organizational unit (OU).

3. Expand Computer Configuration\Policies\Software Settings or User Configuration\Policies\Software Settings, right-click Software Installation, point to New, and then click Package.

4. Use the Open dialog box to locate the Windows Installer Package (.msi file) for the application, and then click Open. You are then given the choice to select the deployment method: Published, Assigned, or Advanced.

5. To publish or assign the program, select Published or Assigned, and then click OK. If you are configuring computer policy, the program is available the next time a computer affected by the GPO is started. If you are configuring user policy, the program is available to users in the domain, site, or OU the next time users log on. Currently logged-on users need to log off and then log on.

6. To configure additional deployment options for the program, select Advanced. You can then set additional deployment options as necessary.
Configuring Program Compatibility

If you want to install 16-bit or MS-DOS-based programs, you might need to make special considerations. Additionally, to get older programs to run, you might sometimes need to adjust compatibility options. Techniques for handling these situations are discussed in the following sections.

Special Installation Considerations for 16-Bit and MS-DOS-Based Programs

Many 16-bit and MS-DOS-based programs that don’t require direct access to hardware can be installed and run on Windows 7 without any problems. However, most 16-bit and MS-DOS-based programs do not support long file names. To help ensure compatibility with these programs, Windows 7 maps long and short file names as necessary. This ensures that long file names are protected when they are modified by a 16-bit or an MS-DOS-based program. Additionally, it is important to note that some 16-bit and MS-DOS-based programs require 16-bit drivers, which are not supported on Windows 7. As a result, these programs won’t run.

Most existing 16-bit and MS-DOS-based programs were originally written for Windows 3.0 or Windows 3.1. Windows 7 runs these older programs using a virtual machine that mimics the 386-enhanced mode used by Windows 3.0 and Windows 3.1. Unlike on other recent releases of Windows, on Windows 7 each 16-bit and MS-DOS-based application runs as a thread within a single virtual machine. This means that if you run multiple 16-bit and MS-DOS-based applications, they all share a common memory space. Unfortunately, if one of these applications hangs or crashes, it usually means the others will as well.

You can help prevent one 16-bit or MS-DOS-based application from causing others to hang or crash by running it in a separate memory space. To do this, follow these steps.

1. Right-click the program’s shortcut icon, and then click Properties. If the program doesn’t have a shortcut, create one, and then open the shortcut’s Properties dialog box.

2. On the Shortcut tab, click the Advanced button. This displays the Advanced Properties dialog box.

3. Select the Run In Separate Memory Space check box.

4. Click OK twice to close all open dialog boxes and save the changes.

*NOTE* Running a program in a separate memory space uses additional memory. However, you’ll usually find that the program is more responsive. Another added benefit is that you are able to run multiple instances of the program—as long as all the instances are running in separate memory spaces.
**TIP** The Windows 7 command prompt (Cmd.exe) is a 32-bit command prompt. If you want to invoke a 16-bit MS-DOS command prompt, you can use Command.com. Type `command` in the Run dialog box.

**Forcing Program Compatibility**

Some programs won’t install or run on Windows 7 even if they work on previous versions of the Windows operating system. If you try to install a program that has known compatibility problems, Windows 7 should display a warning prompt telling you about the compatibility issue. In most cases, you should not continue installing or running a program with known compatibility problems, especially if the program is a system utility such as an antivirus program or a disk partitioning program, because running an incompatible system utility can cause serious problems. Running other types of incompatible programs can also cause problems, especially if they write to system locations on disk.

That said, if a program will not install or run on Windows 7, you might be able to run the program by adjusting its compatibility settings. Windows 7 provides two mechanisms for managing compatibility settings. You can use the Program Compatibility wizard, or you can edit the program’s compatibility settings directly by using the program’s Properties dialog box. Both techniques work the same way. However, the Program Compatibility wizard is the only way you can change compatibility settings for programs that are on shared network drives, CD or DVD drives, or other types of removable media drives. As a result, you can sometimes use the Program Compatibility wizard to install and run programs that would not otherwise install and run.

**Using the Program Compatibility Wizard**

You can only configure compatibility settings for programs you’ve installed. You can’t configure compatibility settings for programs included with the operating system. To try to automatically detect compatibility issues using the Program Compatibility wizard, follow these steps.

1. Locate the program shortcut by navigating the menus under Start, All Programs. Right-click the program shortcut, and then click Troubleshoot Compatibility. This starts the Program Compatibility wizard, shown in Figure 9-2.
2. The wizard automatically tries to detect compatibility issues. To try to run the program you are troubleshooting with the recommended fixes, click Try Recommended Settings. Next, review the settings that will be applied, and then click Start The Program.

3. After running the program, click Next, and then do one of the following:
   - Click Yes, Save These Settings For This Program if the compatibility settings resolved the problem and you want to keep the settings.
   - Click No, Try Again Using Different Settings if the compatibility settings didn’t resolve the problem and you want to repeat this process from the beginning.
   - Click No, Report The Problem To Microsoft And Check Online For A Solution if the compatibility settings didn’t resolve the problem and you’d like to check for an online solution.
   - Click Cancel if you want to discard the compatibility settings and exit the wizard.

To perform advanced troubleshooting and use the Program Compatibility wizard to specify the compatibility settings to use, follow these steps:

1. Locate the program shortcut by navigating the menus under Start, All Programs. Right-click the program shortcut, and then click Troubleshoot Compatibility. This starts the Program Compatibility wizard.

2. Click Troubleshoot Program. On the What Problems Do You Notice? page, you can specify information about problems you’ve seen. The selections you make determine the wizard pages you see when you click Next. They include the following:
   - **The Program Worked On Earlier Versions Of Windows But Won’t Install Or Run Now**  If you select this option, you are prompted on one of the subsequent wizard pages to specify which version. Because your
choice sets the compatibility mode, choose the operating system for which the program was designed. When running the program, Windows 7 simulates the environment for the specified operating system.

- **The Program Opens But Doesn’t Display Correctly** If you are trying to run a game, an educational program, or any other program that requires specific display settings, such as a program designed for Windows 98, you can select this option and then choose the type of display problem you are seeing. Your selections restrict the video display: when you use 256 colors, 640 × 480 screen resolution, or both, Windows restricts the video display. This can help with programs that have problems running at higher screen resolutions and greater color depths. Your selections can also disable themes, desktop compositing (which prevents special visual effects on the desktop), and display scaling of high dots-per-inch (DPI) settings.

- **The Program Requires Additional Permissions** If you choose this option, the program will be configured to run with administrator privileges.

- **I Don’t See My Problem Listed** If you choose this option, the wizard displays optional pages for operating system and display issue selection. The wizard also sets the program to run as an administrator. Ultimately, choosing this option has the same effect as if you had selected all three of the previous options.

3. Review the compatibility settings that will be applied. If you don’t want to apply these settings, click Cancel and repeat this procedure to select different options. If you want to apply these settings, click Start The Program, and the wizard runs the program with the compatibility settings you specified.

4. After running the program, click Next to continue. When you continue, you are prompted to confirm whether the changes fixed the problem. Do one of the following:

- If the compatibility settings resolved the problem and you want to keep the settings, click Yes, Save These Settings For This Program.

- If the compatibility settings didn’t resolve the problem and you want to repeat this process from the beginning, click No, Try Again Using Different Settings.

- If the compatibility settings didn’t resolve the problem and you’d like to check for an online solution, click No, Report The Problem To Microsoft And Check Online For A Solution.

- If you want to discard the compatibility settings and exit the wizard, click Cancel.

**NOTE** If you’ve configured alternate display settings for an application, the application will run in the alternate display mode whenever you start it. To restore the original display settings, simply exit the program.
Setting Compatibility Options Directly
If a program you have already installed won’t run correctly, you might want to edit the compatibility settings directly rather than through the wizard. To do this, follow these steps.

1. Right-click the program’s shortcut icon, and then click Properties.

2. In the Properties dialog box, click the Compatibility tab. Any option you select is applied to the currently logged-on user for the application shortcut. To apply the setting to all users on the computer and regardless of which shortcut is used to start the application, click Change Setting For All Users to display the Properties dialog box for the application’s .exe file, and then select the compatibility settings that you want to use for all users who log on to the computer.

3. Select the Run This Program In Compatibility Mode For check box, and then use the selection menu to choose the operating system for which the program was designed.

4. If necessary, use the options in the Settings panel to restrict the video display settings for the program. Select 256 colors, 640 × 480 screen resolution, or both, as required.

5. If necessary, you can also disable visual themes, desktop compositing, and display scaling of high DPI settings.

6. Click OK. Double-click the shortcut to run the program and test the compatibility settings. If you still have problems running the program, you might need to modify the compatibility settings again.

Managing Installed and Running Programs
Windows 7 provides several management tools for working with programs. These tools include:

- **Task Manager** Provides options for viewing and managing running programs as well as options for viewing resource usage and performance
- **Programs** Provides tasks for viewing installed programs, adding and removing programs, viewing installed updates, and more
- **Default Programs** Helps you track and configure global default programs for the computer, personal default programs for individual users, AutoPlay settings for multimedia, and file associations for programs
- **Windows Features**  Helps you view and manage the Windows components installed on a computer
- **Assoc**  Helps you view and manage file type associations
- **Ftype**  Helps you view and manage file type definitions

These tools and related configuration options are discussed in the sections that follow.

**Managing Currently Running Programs**

In Windows 7, you can view and work with a computer’s currently running programs and processes by using Task Manager. You can open Task Manager by pressing Ctrl+Alt+Delete and then selecting Start Task Manager. As Figure 9-3 shows, Task Manager has two tabs for working with running programs:

- **Applications**  Lists applications that are currently running in the foreground by name and status (such as Running or Not Responding). To exit a program, which might be necessary when it is not responding, click the program in the Task list, and then click End Task.

- **Processes**  Lists all background and foreground applications running on the computer by image name, user name, and resource usage. To stop a process, click the process, and then click End Process.

![Figure 9-3](image)

While the details for process count, CPU usage, and physical memory usage are for the computer as a whole, the processes are only listed for the currently logged-on user and the operating system by default. To see running processes for all users, you must click Show Processes From All Users.
TIP  On the Processes tab, you can manage processes in additional ways by right-clicking a process and selecting from an extended list of options. The options include Open File Location, which opens the folder containing the executable file for the process in Windows Explorer; End Process Tree, which stops the process and all dependent processes; Create Dump File, which creates a memory dump file for the selected process; and Properties, which opens the Properties dialog box for the executable file.

Managing, Repairing, and Uninstalling Programs

Windows 7 considers any program you’ve installed on a computer or made available for a network installation to be an installed program. In Windows XP and earlier versions, you use the Add Or Remove Programs utility to install and manage applications. In Windows 7, you use the setup program that comes with the application to install applications, and you use the Installed Programs page in Control Panel to manage applications.

You can use the Installed Programs page to view, add, remove, or repair installed programs by following these steps:

1. Click Start, and then click Control Panel. In Control Panel, click Programs.
2. Click Programs And Features. You should see a list of installed programs.
3. In the Name list, right-click the program you want to work with, and then click one of the following commands:
   - **Uninstall** to uninstall the program
   - **Change** to modify the program’s configuration
   - **Repair** to repair the program’s installation

When you are uninstalling programs, keep the following in mind:

- Windows warns you if you try to uninstall a program while other users are logged on. Generally, you should be sure that other users are logged off before uninstalling programs. Otherwise, you might cause other users to lose data or experience other problems.
- Windows will allow you to remove only those programs that were installed with a Windows-compatible setup program. Although most applications have a setup program that uses InstallShield, Wise Install, or Microsoft Windows Installer, older programs might have a separate uninstall utility. Some older programs work by copying their data files to a program folder. In this case, you uninstall the program by deleting the related folder.
- Many uninstall programs leave behind data either inadvertently or by design. As a result, you often find folders for these applications within the Program Files folder. You could delete these folders, but they might contain important data files or custom user settings that could be used again if you reinstall the program.
Sometimes, the uninstall process fails. Often, you can resolve any problem simply by rerunning the uninstaller for the program. Occasionally, you might need to clean up after the uninstall process. This might require removing program files and deleting remnants of the program in the Windows registry. A program called the Windows Installer Cleanup utility can help you clean up the registry. For more information on the utility and to download the software, see the article on the Microsoft support Website at http://support.microsoft.com/kb/290301.

Designating Default Programs

Default programs determine which programs are used with which types of files and how Windows handles files on CDs, DVDs, and portable devices. You configure default programs based on the types of files those programs support, either globally for all users of a computer or only for the current user. Individual user defaults override global defaults. For example, you could select Windows Media Player as the global default for all types of files it supports, and then all users of the computer would use Windows Media Player to play the sound, audio, and video files it supports. If a specific user wanted to use Apple iTunes instead as the default player for sound and audio files, you could configure iTunes to be that user’s default player for the types of media files it supports.

You can configure global default programs for all the users of a computer by following these steps:

1. Click Start, and then click Control Panel. In Control Panel, click Programs.
2. Click Default Programs, and then click Set Program Access And Computer Defaults. You’ll see the dialog box shown in Figure 9-4.

![Set Program Access and Computer Defaults](image)

**FIGURE 9-4** Choose a global default configuration.
3. Choose a configuration from one of the following options:
   - **Microsoft Windows**  Sets the currently installed Windows programs as the default programs for browsing the Web, sending e-mail, playing media files, and so on.
   - **Non-Microsoft**  Sets the currently installed programs as the default programs for browsing the Web, sending e-mail, playing media files, and so on.
   - **Custom**  Enables you to choose programs as the defaults for browsing the Web, sending e-mail, playing media files, and so on.

4. Click OK to save the settings.

To override global defaults, you can set default programs for individual users. You can configure default programs for the current user by following these steps:
1. Click Start, and then click Control Panel. In Control Panel, click Programs.
2. Click Default Programs, and then click Set Your Default Programs.
3. Select a program you want to work with in the Programs list.
4. If you want the program to be the default for all the file types and protocols it supports, click Set This Program As Default.
5. If you want the program to be the default for specific file types and protocols, click Choose Defaults For This Program. Select the file extensions for which the program should be the default, and then click Save.

### Managing the Command Path

Windows uses the command path to locate executables. You can view the current command path for executables by using the PATH command. In a command shell, type `path` on a line by itself, and then press Enter. In a Windows PowerShell console, type `$env:path` on a line by itself, and then press Enter. In the output, observe that Windows uses a semicolon (;) to separate individual paths, marking where one file path ends and another begins.

The command path is set during logon by using system and user environment variables. The path defined in the PATH system variable sets the base path. The path defined in the PATH user variable adds to the base path by using the following syntax:

```
%PATH%;AdditionalPaths
```

Here, `%PATH%` tells Windows to insert the current system paths, and `AdditionalPaths` designates the additional user-specific paths to use.

**CAUTION** An improperly set path can cause severe problems. You should always test any command path change before using it in a live environment. The command path is set during logon. Therefore, you must log off and then log on again to see the effects of the revised path.
Don’t forget about the search order that Windows uses. Paths are searched in order, with the last path in the PATH user variable being the last one searched. This can sometimes slow the execution of your programs and scripts. To help Windows find your programs and scripts faster, you should consider placing a required path earlier in the search order.

Be careful when setting the command path. It is easy to overwrite all path information accidentally. For example, if you don’t specify %PATH% when setting the user path, you will delete all other path information. One way to ensure that you can easily re-create the command path is to keep a copy of the command path in a file.

■ When you are working with the command prompt, you can write the current command path to a file by entering `path > orig_path.txt`. Keep in mind that if you are using a standard command prompt rather than an administrator command prompt, you won’t be able to write to secure system locations. In this case, you can write to a subdirectory to which you have access or to your personal profile. To write the command path to the command-shell window, type `path`.

■ When you are working with the PowerShell console, you can write the current command path to a file by entering `$env:path > orig_path.txt`. If you are using a standard console rather than an administrator console, you won’t be able to write to secure system locations. In this case, you can write to a subdirectory to which you have access or to your personal profile. To write the command path to the PowerShell window, type `$env:path`.

At the command prompt or in the PowerShell window, you can modify the command path by using the `setx.exe` utility. You also can edit the command path by completing the following steps:

1. In Control Panel, click System And Security, and then click System.
2. In the System console, click Change Settings, or click Advanced System Settings in the left pane.
3. On the Advanced tab in the System Properties dialog box, click the Environment Variables button.
4. Select the PATH variable in the System Variables list. Under System Variables, click Edit.
5. By default, the path value is selected. Without pressing any other key, press the Right Arrow key. This should remove the selection highlight and place the insertion point at the end of the variable value.
6. Type a semicolon, and then enter a path to insert. Repeat as necessary, and then click OK three times.

In Group Policy, you can use a preference item to modify the command path. Follow these steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. To configure preferences for computers, expand Computer
Configuration\Preferences\Windows Settings, and then select Environment. To configure preferences for users, expand User Configuration\Preferences\Windows Settings, and then select Environment.

2. Right-click the Environment node, point to New, and then click Environment Variable. This opens the New Environment Properties dialog box.

3. In the Action list, select Update to update the path variable, or select Replace to delete and then re-create the path variable. Next, select User Variable to work with user variables.

4. In the Name field, type Path. In the Value field, type the variable value. Typically, you’ll enter %PATH%; followed by the paths you want to add, using a semicolon to separate each path. If the affected computers have existing PATH user variable definitions, you must provide the related paths to ensure that these paths are retained.

5. Use the options on the Common tab to control how the preference is applied. In most cases, you’ll want to create the PATH variable only once (rather than have Group Policy re-create the variable each time policy is refreshed). If so, select Apply Once And Do Not Reapply.

6. Click OK. The next time policy is refreshed, the preference item will be applied as appropriate for the GPO in which you defined the preference item.

**CAUTION** Incorrectly setting the path can cause serious problems. Before deploying an updated path to multiple computers, you should test the configuration. One way to do this is to create a GPO in Active Directory that applies only to an isolated test computer. Next, create a preference item for this GPO, and then wait for a policy to refresh or apply policy using GPUpdate. If you are logged on to the computer, you need to log off and then log back on before you can confirm the results.

**Managing File Extensions and File Associations**

File extensions and file associations also are important for determining how programs run. The types of files that Windows considers to be executables are determined by the file extensions for executables. File extensions allow users to execute a command by using just the command name. File associations are what allow users to double-click a file and open the file automatically in a related application. Two types of file extensions are used:

- **File extensions for executables** Executable files are defined with the %PATH% environment variable and can be set using the Environment Variables dialog box or with Group Policy preference items in much the same way as the PATH variable. You can view the current settings by typing `set pathext` at the command line or by typing `$env:pathext` at a PowerShell prompt. The default setting is `PATH=COM;EXE;BAT;CMD;VBS;VBE;JS;JSE;WSF;WSH;MSC`. With this setting, the command line knows which files
are executable and which files are not, so you don’t have to specify the file extension at the command line.

- **File extensions for applications**  File extensions for applications are referred to as file associations. File associations are what enable you to pass arguments to executables and to open documents, worksheets, or other application files by double-clicking their file icons. Each known extension on a system has a file association that you can view at a command prompt by typing `assoc` followed by the extension, such as `assoc .doc` or `assoc .docx`. Each file association in turn specifies the file type for the file extension. This can be viewed at a command prompt by typing `ftype` followed by the file association, such as `ftype Word.Document.8` or `ftype Word.Document.12`.

**NOTE**  Assoc and Ftype are internal commands for the command shell (Cmd.exe).

To use the Assoc command in PowerShell, enter `cmd /c assoc` followed by the extension, such as `cmd /c assoc .doc`. To use the Ftype command in PowerShell, enter `cmd /c ftype` followed by the file association, such as `cmd /c ftype Word.Document.8`.

With executables, the order of file extensions in the `%PATHEXT%` variable sets the search order used by the command line on a per-directory basis. Thus, if a particular directory in the command path has multiple executables that match the command name provided, a .com file would be executed before an .exe file and so on.

Every known file extension on a system has a corresponding file association and file type—even extensions for executables. In some cases, the file type is the extension text without the period followed by the keyword file, such as cmdfile, exefile, or batfile, and the file association specifies that the first parameter passed is the command name and that other parameters should be passed on to the application. For example, if you type `assoc .exe` to see the file associations for .exe executables, you then type `ftype exefile`. You’ll see the file association is set to the following:

```
exefile="%1" %*
```

Thus, when you run an .exe file, Windows knows the first value is the command that you want to run and anything else provided is a parameter to pass along.

File associations and types are maintained in the Windows registry and can be set using the Assoc and Ftype commands, respectively. To create the file association at the command line, type `assoc` followed by the extension setting, such as `assoc .pl=perlfile`. To create the file type at the command line, set the file-type mapping, including how to use parameters supplied with the command name, such as `ftype perlfile=C:\Perl\Bin\Perl.exe "%1" %*`.

You also can associate a file type or protocol with a specific program by completing the following steps:

1. Click Start, and then click Control Panel. In Control Panel, click Programs.
2. Click Default Programs, and then click Associate A File Type Or Protocol With A Program.
3. On the Set Associations page, current file associations are listed by file extension and the current default for that extension. To change the file association for an extension, click the file extension, and then click Change Program.

4. Do one of the following:
   - The Recommended Programs list shows programs that are registered in the operating system as supporting files with the selected extension. Click a recommended program to set it as the default for the selected extension, and then click OK.
   - The Other Programs list shows programs that might also support the selected extension. Click a program to set it as the default for the selected extension, and then click OK. Alternatively, click Browse to locate another program to use as the default.

In Group Policy, you can use a preference item to create new file types and file associations. To create a preference item for a new file type, follow these steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. Expand Computer Configuration\Preferences\Control Panel Settings, and then select Folder Options.
2. Right-click the Folder Options node, point to New, and then click File Type. This opens the New File Type Properties dialog box.
3. In the Action list, select Create, Update, Replace, or Delete.
4. In the File Name Extension field, type the extension of the file type without the period, such as `pl`.
5. In the Associated Class list, select a registered class to associate with the file type.
6. Use the options on the Common tab to control how the preference is applied. In most cases, you’ll want to create the new variable only once. If so, select Apply Once And Do Not Reapply.
7. Click OK. The next time policy is refreshed, the preference item will be applied as appropriate for the GPO in which you defined the preference item.

To create a preference item for a new file association, follow these steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. Expand User Configuration\Preferences\Control Panel Settings, and then select Folder Options.
2. Right-click the Folder Options node, point to New, and then click Open With. This opens the New Open With Properties dialog box.
3. In the Action list, select Create, Update, Replace, or Delete.
4. In the File Name Extension field, type the extension of the file type without the period, such as `pl`. 
5. Click the Browse (…) button to the right of the Associated Program field, and then use the Open dialog box to select the program to associate with the file type.

6. Optionally, select Set As Default to make the associated program the default for files with the previously specified file extension.

7. Use the options on the Common tab to control how the preference is applied. In most cases, you’ll want to create the new variable only once. If so, select Apply Once And Do Not Reapply.

8. Click OK. The next time policy is refreshed, the preference item will be applied as appropriate for the GPO in which you defined the preference item.

Configuring AutoPlay Options

In Windows 7, AutoPlay options determine how Windows handles files on CDs, DVDs, and portable devices. You can configure separate AutoPlay options for each type of CD, DVD, and media your computer can handle by following these steps:

1. Click Start, and then click Control Panel. In Control Panel, click Programs.

2. Click Default Programs, and then click Change AutoPlay Settings. This displays the AutoPlay page in Control Panel.

3. As shown in Figure 9-5, use the media selection list to set the default AutoPlay option for each media type.

4. Click Save to save your settings.
Adding and Removing Windows Features

In Windows XP and earlier versions of Windows, you use the Add/Remove Windows Components option of the Add Or Remove Programs utility to add or remove operating system components. In Windows Vista and Windows 7, operating system components are considered Windows features that can be turned on or off rather than added or removed.

You can turn on or off Windows features by following these steps:

1. Click Start, and then click Control Panel. In Control Panel, click Programs.
2. Under Programs And Features, click Turn Windows Features On Or Off. This displays the Windows Features dialog box.
3. As shown in Figure 9-6, select the check boxes for features to turn them on, or clear the check boxes for features to turn them off.
4. Click OK, and Windows 7 reconfigures components for any changes you made.

![Figure 9-6 Add or remove operating system components.](image-url)
Symbols and Numbers
* (asterisk), 571, 597
$ (dollar sign), 504
128-bit addresses, 549
1394 debugging, 371–372
16-bit applications, 324
16-bit architecture, 340
16-bit drivers, 324
32- and 64-bit driver stores, 297
32-bit addresses, 549
32-bit architecture, 3, 5, 13, 42, 342
386-enhanced mode, 324
64-bit architecture
design and implications, 8–9
EFI and, 342
installing Windows PE, 42
MBR and GPT partition styles, 410
separate distribution media for, 5
UEFI and, 342
Windows 7 and, 3, 13
802.11.
See IEEE 802.11

A
access. See also permissions
access permissions, 474
BitLocker, 387–393
decrypted files, 471
denying, on workstations, 144
deployment of permissions, 478
file ownership, 488
file sharing auditing, 508–511
file sharing options, 473–478, 501–504
file sharing permissions, 478–494
local logons, 137–144
network connection access types, 547
network shares, 495
offline files, 520–531
policy settings, 102–105, 372
principle of least privilege, 483
Public folder sharing, 507–508
remote. See remote access
Remote Desktop, 162–165
stored credentials, 144–149
TPM features, 380–387
types of accounts, 125
UAC and, 131–137
user and group accounts, 125–128, 149–158
Windows Explorer, 513–520
wireless. See wireless networks
access control list (ACL), 480
access control test, 35
access points (wireless), 608.
See also wireless networks
access policies, 102–105, 372
access tokens, 132, 312
accounts. See also specific types of accounts
credentials, 144–149
local user accounts, 20
locked-out, 156
logon names, 126
passwords, 23–25
pseudo-accounts, 127
removing and denying access, 144
roaming profiles, 145
SIDs (security identifiers), 126
Welcome screen, 142
ACL (access control list), 480
ACPI (Advanced Configuration and Power Interface), 341, 343, 348, 423
ACT (Windows Application Compatibility Toolkit), 315, 321
Action Center
archiving solutions, 267
failed applications and drivers, 33
hardware error messages, 306–310
hiding icon, 275
notification area, 237
notifications, 265–274
problem detection, 266
reliability reports, 268
resolving problems in, 267
scripted diagnostics and, 32
starting, 17–19
actions (tasks), 632, 635
activating Windows, 19, 67, 171
Active Directory domains, 10, 126, 190, 392–393
Active Directory Users And Computers console, 24, 126, 130
Active Directory–based Group Policy
Common tab options, 121
configuring preferences, 115–119
creating and editing preference items, 120
described, 84
devices, tasks, and services, 119
editing states, 117
logon screens, 143
management actions, 115
out-of-scope preferences, 122
processing order, 120
security configuration, 136
site, domain, and OU policies, 88–90
targeting items, 123
types of policy preferences, 113–115
active networks, 547
active partitions, 11, 356, 394, 423, 426, 441–442
Active status (removable media), 424
active volumes, 423, 441
ad hoc mode (wireless), 612
adapters, 283. See also graphics adapters; network adapters; wireless adapters
Add Hardware wizard, 299
Add New User wizard, 139
Add Or Remove Programs utility, 338
Add Printer wizard, 292–293
Add Recovery Agent Wizard, 471
Address bar, 236, 239
Address Resolution Protocol Service Binding Protocol (ARPSBP), 344
ADM files, 90
Admin Approval Mode, 133–137
ADMIN$ share, 501, 505
administrative shares, 504
administrative template files. See ADMX files (administrative template files)
Administrative Tools menu, 229–230
administrative user applications, 314
administratively assigned folders and files, 97, 99
administrator access tokens, 312, 315
administrator accounts, 127, 133–137
administrator mode, 132
administrator user accounts, 20, 22, 131–133
administrative user applications, 312
Administrators group, 127, 129, 478–494, 533
ADMX files (administrative template files), 90, 92. See also policy settings
Advanced Boot Options menu, 358, 637, 645
Advanced Configuration and Power Interface. See ACPI (Advanced Configuration and Power Interface)
Advanced Encryption Standard (AES), 611
Advanced Encryption Standard 128-bit Cyclical Bit Check (AES-128-CBC), 468
Advanced Folder Options policies, 115
Advanced Power Management (APM), 423
Advanced Programmable Interrupt Controller (APIC), 374–376
advanced sharing, 496–497
Advanced tab (System Properties dialog box), 192
Advanced Tools (performance), 173
advanced Windows OS Loader options, 374
Aero Peek feature, 237
Aero user interface, 3, 17, 249, 252, 272
AES (Advanced Encryption Standard), 611
AES-128–CBC (Advanced Encryption Standard 128-bit Cyclical Bit Check), 468
alarms (power warnings), 220
alerts, 17–19, 135, 270–274, 306–310
All Programs menu, 228–229
alternate IP addresses, 554, 557, 578
alternate shells, 375
always run as administrator applications, 315
AMD Opteron (AMD64) processors, 8, 196, 350
AMX (associated component manifest files), 297
analog modems, 581, 588
Anonymous Logon identity, 482
answer files, 10, 65
API (Advanced Programmable Interrupt Controller), 374–376
APIPA (Automatic Private IP Addressing), 569, 578
APM (Advanced Power Management), 423
Appearance And Personalization troubleshooting, 33
appending data, 43, 485
Application Control policies, 318
application entries (BCD), 369
Application Layer Gateway Service, 128
Application Management service, 277
applications
32-bit vs. 64-bit, 9
access tokens, 132, 312
administrator accounts and, 131
administrator user vs. standard user, 312
assigning, 322
AutoPlay feature, 337
Autorun features, 319
cleaning up program files, 180
command paths and, 332–334
compatibility, 30, 273, 324–328
currently running, 329
default, 331
DEP and, 196
device issues, 310
display issues, 260
elevation, 132
environment information, 176
event logs, 629
event sounds, 242
failures in, 276
file extensions and associations, 334–337
Group Policy settings, 90
highlighting, 225
installing, 318–322
integrity levels, 314
legacy, 260, 313
nonresponsive, 265, 647
offline use, 523
performance settings, 193
permissions, 485
pinning to taskbar, 236
policy preferences, 114
prioritizing and preloading, 419
privileges, 312–313
problem reporting, 271
publishing, 323
recently changed or added, 648
recently used, 225
reinstalling, 10
Remote Desktop connections, 166
repairing, 330
restore points and, 639
run levels, 315–317
run lists, 110–111
run modes, 132
running at logon, 110–111
setup programs, 319
signed, 136, 182
sorting names in menus, 225
standard and administrator mode, 132
startup applications, 188, 230, 232, 234–235
troubleshooting, 30, 33, 273
UAC-compliant, 312
uninstalling, 330
validated, 136
virtualization, 313, 317
window arrangements, 243
Windows PE, 51
working directories, 234
Applications policies, 114, 116
area codes, 585–586
ARP protocol, 344
ARPSBP (Address Resolution Protocol Service Binding Protocol), 344
assistance invitations, 160
Assoc tool, 335
associated component manifest files, 297
asterisks (*), 571, 597
audio controllers, 344
audit mode, 63
auditing events, 629
auditing file sharing, 508–511
Authenticated Users identity, 482
authentication
BitLocker policies, 392
credentials, 145
logon screens, 110
remote access, 601
Remote Desktop sessions, 164
startup process, 352
TPM methods, 396
Authenticode, 314
Auto Hide feature, 237
Automated Help and Support features
Action Center notifications, 265–270
configuring services, 278
customizing, 270–276
detecting problems, 264
reliability reports, 268
Restart Manager, 265
support services, 276–279
troubleshooters, 272–274
automated installation, 10, 65
automatic backups, 642
Automatic Black Hole Router Detection feature, 550
Automatic Dead Gateway Retry feature, 550
automatic defragmentation, 455
automatic network connections, 593
Automatic Private IP Addressing (APIPA), 569, 578
automatic reconnections, 164
automatic restarts, 375, 638
automatic synchronization, 521, 526–527
automatic unlocking, encrypted drives, 398
automatic updates, 620–622, 640
AutoPlay feature, 337, 400
Autorun feature, 318–319
auto-tuning monitors, 261

B
background desktop images, 211, 240, 242–243
Background Intelligent Transfer Service (BITS), 128, 277, 540
background logon display, 110
background processes, 418–419
background synchronization, 96, 100
backing up. See also Backup And Restore Center
BCD store data, 364
BitLocker recovery information, 393
configuring backups, 642
creating backups, 642–645
disabling, 644
displaying settings, 643
personal data, 642
recovering personal data, 645
system images, 642
System Restore tool, 639–641
TPM and, 384, 393
troubleshooting backups, 644
Windows vault, 148
WMI repository, 178
Backup And Restore Center, 636, 642–645
Backup Operators group, 129, 488
Backup tool, 179
Balanced power plan, 25, 210
base video option, 186
basic disks
characteristics, 420–429
converting to dynamic, 408, 412, 428–429
described, 420
Disk Management tool, 411
extending, 436
functions, 408–414
laptops and, 423
partitions on, 11, 408–414
shrinking, 436
spanning or striping, 435
volumes, 423–425
basic permissions, 479–484
basic sharing, 496
batteries
firmware configuration details, 345
hybrid drives and, 417
power alerts, 220
power plan options, 211
sleep mode and, 25
status, 576
total battery life, 221
baud rates, 371–373
BCD Editor and BCD store
additional operating system entries, 367
backing up data, 364
boot entries for mirrored disks, 457
copying or creating entries, 363, 369
creating stores, 368
default operating system entry, 377
default timeouts, 378
deleting entries, 369
DEP and, 376
entry properties, 365–366
entry values, 370–376
exporting contents, 363
functions and commands, 362–364
GUIDs and, 366–367
importing and exporting stores, 368
legacy operating system entries, 367
operating system order, 377
PAE configuration, 376
restoring, 364
startup and, 340, 344
system and nonsystem, 364, 368
temporary boot sequence changes, 378
troubleshooting, 353
viewing store entries, 364–368
BCD registry file, 41, 341
BCDBoot tool, 38
BIND, dynamic DNS updates and, 561
binding (TPM), 380
BIOS (basic input/output system), 8, 11, 340–341, 356
BIS (Boot Integrity Services), 343
BitLocker Drive Encryption. See also BitLocker To Go configuring, 394
deleting, 390–393
deploying, 390–393
disabling or turning off, 406
functions, 388–390
installing software, 394
moving disks and, 446
nonsystem volumes, 397
partitions needed, 401
PIN numbers, 403
policy settings, 392
preparing to deploy, 394–397
recovery data, 405
recovery passwords, 397
recovery policies, 470
removable media boot settings, 351
saving backup information, 393
status of, 404
system volumes, 401–403
TPM and, 381
troubleshooting, 404–406
unlocking computers, 405
USB flash drive installation, 399
versions of, 391
Windows 7 edition, 3
BitLocker Drive Encryption Recovery console, 405
BitLocker To Go, 24, 387, 400, 417
BitLocker To Go reader, 400
BITS (Background Intelligent Transfer Service), 540, 619
black hole router detection, 550
blocked applications, 314
blocked disk I/O operations, 264
blocked drive access, 520
blocked network discovery, 545
blocked publishers, 314
blocked TPM commands, 392
Bluetooth devices, 289–291, 293–295
Blu-ray support, 460
Boolean values, BCD store entries, 370
boot applications, 372–373
boot configuration
  BCD Editor, 362–364
  BCD store management, 364–368
boot options, 185–187
  managing, 360–362
  multiple bootable operating systems, 201
booting
  automatic rebooting, 202
dual booting, 397
  firmware boot settings, 351
from media, 15
keyboard shortcuts, 341
mirrored disk problems, 457
performance diagnostics, 30
screen display, 375
services and, 189
startup applications and, 188
startup process and, 344, 351
  troubleshooting, 353–358, 372
Windows PE and, 40
Bootmgr file. See boot manager
Bootsect tool, 38, 56
Bootsector (Windows Boot Sector Application), 362, 369
branch caching, 540–542
breaking mirrored sets, 445
broadband connections
  automatic or manual connections, 593
  creating, 590
described, 581
establishing, 606
identity validation, 601
logon configuration, 597
network protocols and components, 602–604
proxy settings, 594–597
troubleshooting, 606
Windows Firewall and, 604
Bug check analysis, 35
build environments, 41–47
build images, 53–54
Built-In Diagnostics tool, 179
Burn A Disc Wizard, 460, 462, 464
burning discs, 460–463
test-code signing certificates, 373
bypassing proxy servers, 596
CA (certificate authority), 471
certificate authority (CA), 471
certificate servers, 582
certificates
  certificate-based credentials, 145, 147
data-recovery agents, 390
  encryption certificates, 468
  passwords and, 140
  recovery certificates, 471
  Remote Desktop, 165
  remote logon configuration, 598
  test-code signing certificates, 373
  user accounts, 127
  wireless connections, 613
certified drivers, 297, 640
CHAP (Challenge Handshake Authentication Protocol), 601
characters in volume labels, 440
chat windows (Remote Assistance), 628
Check Disk tool, 447, 451–454, 647
child OU policies, 84
Chkdsk.exe. See Check Disk tool
colons in IP addresses, 550

colors
  color depth, 253, 259
  color quality, 258
  encrypted or compressed file display, 515
  intensity and transparency, 251
Remote Desktop settings, 164
  spots on displays, 260
window interface, 249–252

COM (Component Object Model), 9, 275
command path, 332–334
command prompts, 14, 38, 325
command-shell batch scripts, 106, 631
Common tab (hardware), 121
Compact utility, 467
CompactFlash cards, 415, 424
compatibility
  16-bit and MS-DOS-based programs, 324
  Compatibility Administrator, 321
display issues, 260
driver issues, 275
error messages, 308, 310
forcing, 325
legacy applications and, 313
manual settings, 328
program compatibility, 276
Program Compatibility Assistant, 30, 320
Program Compatibility wizard, 325–327
task scheduling, 632
turning off compatibility database, 276
virtualization, 313
Web compatibility lists, 620
Windows Application Compatibility Toolkit, 315
Compatibility Administrator, 321
Complete PC Backup feature, 3
Component Object Model (COM), 9, 275
components, 176. See also specific component types
Compound TCP feature, 550
compression
  enabling, 433
  encryption and, 469
  expanding compressed drives, 466
  files and directories, 465–467
RDP data, 165
Remote Desktop sessions and, 166
UEFI support, 343
Windows Explorer display options, 515
Computer icon, 245
Computer Management console
  administrative shares, 504
  configuring services, 278
  enabling offline file features, 522
  file sharing settings, 498–500
  functions of, 168
  network shares, 496, 504
  remote computer management, 170
  stopping, starting, or pausing services, 279
  viewing event logs, 630
Computer Name tab (System Properties dialog box), 190
computers
  64-bit support, 9
  administrative policies for, 91
  assigning file ownership, 489
  assigning scripts, 108
  automatic problem detection, 266
  automatic updates, 620
domain membership, 125
  event log entries, 630
  file and data management policies, 92–102
  Group Policy settings, 89
  homegroups and, 125
  logon and startup policies, 109–111
  names, 171
  network access types, 547
  network policies, 102–103
  offline file policies, 95–102
  policy preferences, 113–115, 120
  policy settings, 84
  problem reporting settings, 271
  registry changes for Group Policy, 90
  reliability and stability reports, 268
  remote access, 159–166
  repairing, 645
  script policies, 106–109
  special permissions, 486
  Windows Experience Index rating, 172
workgroups and, 125
conditions (tasks), 632, 635
configuration
  advanced system information, 175
  application performance, 193
  automated Help system, 264–283
  Computer Management console, 168
current OS identifier, 366
DEP (Data Execution Prevention), 196
Device Manager, 295
firmware, 346–348
hardware, 192
last known good configuration, 357
manual jumper or firmware settings, 308
names and addresses of computers, 190
OS information, 171
performance options, 192
policy settings, 90–92
power management, 207–222
recovery options, 202, 639
Startup And Recovery dialog box options, 358
startup options, 200
system and environment variables, 198–200
system and performance information, 170–174
System Configuration utility, 184–190
system failure and debugging, 202
System Properties dialog box, 190–207
System Restore settings, 203–207
system support tools, 168, 179–188
virtual memory, 194–196
Windows PE files, 40
WMI Control, 176–178
configuration flags, 374
configuration scripts, 38, 595
conflict resolution (offline files), 521, 528
conflicts
  error messages, 309
policy settings, 84–85
Connect To A Network Projector wizard, 575, 580
connections
  devices, 296
  See network connections
connectivity settings, 102–105
console support (UEFI), 343
context menus, 225, 518
Control Panel Settings policies, 114
Convert utility, 441
  converting
disks to basic or dynamic, 412, 428–429
FAT drives to NTFS, 441
converting
  disks to basic or dynamic, 412, 428–429
  FAT drives to NTFS, 441
  BCD store entries, 369
  BitLocker PINs or keys, 404
  command path, 333
  encrypted files, 470
  files to CDs or DVDs, 460
  Public folder and, 474
corrupted file recovery, 31
crash dump partitions, 425
crash dump volumes, 425
crashes, 265, 339, 648.
  See also troubleshooting
  CRC (cyclic redundancy checking), 343
critical battery alarms, 221–222
critical updates, 618
cryptographic operators group, 129
current registry value, 357
cursor themes, 242
customer experience improvement program, 18, 275
cyclic redundancy checking (CRC), 343
Data Execution Prevention (DEP), 196, 376
Data Incomplete volume status, 449
data management policies, 92–102
data not redundant volume status, 449
data partitions, 11
  data recovery agents, 390, 393
Data Sources policies, 114, 116
data volumes, 394, 406
datagram transmission, 476
dates, 526
DCOM (Remote Assistance requirements), 624
debugging
  BCD store entries, 371
  boot options, 187
  enabling, 360, 363
  global debugger parameters, 366
  kernel, 374
  online crash analysis feature, 648
  private debugger transport, 374
  Stop errors, 647–649
  writing debugging information, 202
decompressing data, 466
decrypting files, 406, 468, 471–472
default applications, 331
default boot partition, 185
default boot timeouts, 378
default gateways, 556, 558, 566, 570, 580
default operating system entry, 377
Default registry value, 357
defragmenting disks, 179, 454–456
degaussing monitors, 261
deployment
  applications, 322
  automating, 66
  BitLocker, 390–393
  creating Windows Images for, 65–67
  DISM, 5–7
  master computers, 67
  scripts, 67
  WIM files and, 65
  Windows PE and, 37–57
  Windows RE and, 58–65
Deployment Image Servicing and Management tool. See DISM (Deployment Image Servicing and Management tool)
Deployment Tools command prompt, 48
deprecated COM objects, 275
deprecated DLLs, 276
desktop
  background images, 242–243
  customizing, 223, 243–246
  extending across monitors, 258
  files and folders on, 243
  icons, 244
  secure vs. standard, 133
  sharing, 507
  shortcuts on, 230–234
  start button, 26
  taskbar, 236–239
  toolbar, 239
desktop deployment tools, 3
desktop folder, 232
desktop images (power plan), 211
detecting devices, 284–285

data execution prevention, 441
copying
  BCD store entries, 369
  BitLocker PINs or keys, 404
  command path, 333
  encrypted files, 470
  files to CDs or DVDs, 460
  Public folder and, 474
corrupted file recovery, 31
crash dump partitions, 425
crash dump volumes, 425
crashes, 265, 339, 648. See also troubleshooting
CRC (cyclic redundancy checking), 343
critical battery alarms, 221–222
critical updates, 618
Cryptographic Operators group, 129
Current registry value, 357
cursor themes, 242
Customer Experience Improvement Program, 18, 275
Cyclic redundancy checking (CRC), 343
Data Execution Prevention (DEP), 196, 376
Data Incomplete volume status, 449
Data management policies, 92–102
Data Not Redundant volume status, 449
data partitions, 11
data recovery agents, 390, 393
Data Sources policies, 114, 116
data volumes, 394, 406
datagram transmission, 476
dates, 526
DCOM (Remote Assistance requirements), 624
debugging
  BCD store entries, 371
  boot options, 187
  enabling, 360, 363
  global debugger parameters, 366
  kernel, 374
  Online Crash Analysis feature, 648
  private debugger transport, 374
  Stop errors, 647–649
  writing debugging information, 202
decompressing data, 466
decrypting files, 406, 468, 471–472
default applications, 331
default boot partition, 185
default boot timeouts, 378
default gateways, 556, 558, 566, 570, 580
default operating system entry, 377
Default registry value, 357
defragmenting disks, 179, 454–456
degaussing monitors, 261
deployment
  applications, 322
  automating, 66
  BitLocker, 390–393
  creating Windows Images for, 65–67
  DISM, 5–7
  master computers, 67
  scripts, 67
  WIM files and, 65
  Windows PE and, 37–57
  Windows RE and, 58–65
Deployment Image Servicing and Management tool. See DISM (Deployment Image Servicing and Management tool)
Deployment Tools command prompt, 48
deprecated COM objects, 275
deprecated DLLs, 276
desktop
  background images, 242–243
  customizing, 223, 243–246
  extending across monitors, 258
  files and folders on, 243
  icons, 244
  secure vs. standard, 133
  sharing, 507
  shortcuts on, 230–234
  start button, 26
  taskbar, 236–239
  toolbar, 239
desktop deployment tools, 3
desktop folder, 232
desktop images (power plan), 211
detecting devices, 284–285

device class GUIDs, 303
device drivers
32- and 64-bit driver stores, 297
adding to Windows PE, 51
automated Help system, 264–283
enabling or disabling, 302, 305
error message list, 306–310
file information, 298
finding, 299
installing, 284–288, 299–302
internal, USB, or FireWire, 286–288
load failure policies, 374
power requests, 208
preexisting hardware, 284–285
pre-update restore points, 288
printers, 291
reinstalling, 305
removing drivers, 305
restore points and, 640
restricting installation, 303
rolling back, 304
signed and unsigned, 298
startup failures, 356
startup process, 352, 637
Stop errors and, 648
test environments, 300
troubleshooting, 260, 353, 637
uninstalling, 305
updating, 288, 299–302
video and monitor, 253–257, 260
wireless, network, and Bluetooth, 289–291
Device Manager, 170, 295, 306–310
devices. See also specific types of devices
account privileges, 132
automated Help system, 264–283
deleting drivers, 305
device drivers, 297–310
duplicate, 309
enabling and disabling, 302, 305
error detection, 35
error message list, 306–310
firmware interface controls, 345
hidden, 296
installing preexisting, 284–285
internal, USB, or FireWire, 286–288
legacy, 307
policy preferences, 114, 119
power information, 208
restricting installation, 303
safe removal, 310
system root on, 375
types of, 283
unplugging, 26
wireless, network, and Bluetooth, 289–291
Devices policies, 114
DFS (distributed file system), 518
DHCP (Dynamic Host Configuration Protocol)
alternate settings, 575
configuring WINS and, 562
default network setting, 604
DHCPv4, DHCPv6, and service binding, 344
displaying configuration, 566
DNS server addresses, 559
dynamic IP addresses, 554
functions of, 543
mobile computing settings, 577
releasing and renewing, 570
wireless networks, 613
DHCPv6-Capable DHCP Client feature, 552
diagnostic startup, 184, 360
diagnostic tools. See also troubleshooters; troubleshooting
disk cleanup, 447
Disk Defragmenter, 179
Disk Management snap-in
accessing, 170
active partitions, 11
basic and dynamic disks, 428–429
compressing drives, 465
defragmenting disks, 454–456
deleting partitions or volumes, 440
disk quotas, 534–539
drive letters and drive paths, 438
formatting partitions and volumes, 438
redialing and disconnection, 598
troubleshooting, 605
Windows Firewall and, 604
work network connections, 588–589
Dial-Up Connections policies, 114
Dialup identity, 483
digital hashes, 542
digital modems, 581
digital signatures, 182, 297, 638
Digital Video Interface (DVI), 257
digital-to-analog converters, 588
direct memory access (DMA), 175
DirectAccess feature, 29, 103, 582, 602
direct-dial connections. See dial-up connections
DirectX 9 graphics processors, 13, 249
DirectX Diagnostics Tool, 179
Disable Driver Signature Enforcement mode, 341, 638
Disabled Group Policy state, 91–92
disc mastering, 461
disconnecting
disk cleanup, 447
Disk Defragmenter, 179, 447, 454–456
disk drives. See hard disk drives; removable media drives
disk error repairs, 451–454
disk failure diagnosis test, 34
disk formats. See file systems
disk I/O subsystem, 422
Disk Management snap-in
accessing, 170
active partitions, 11
basic and dynamic disks, 428–429
compressing drives, 465
defragmenting disks, 454–456
deleting partitions or volumes, 440
disk quotas, 534–539
drive letters and drive paths, 438
formatting partitions and volumes, 438
Disk Management snap-in, continued
functions and displays, 411
initializing disks, 425
MBR and GPT disks, 426
mirroring disks, 444–445
moving disks, 445
partitions, logical drives, and simple volumes, 431–434
recovering volumes, 443
shrinking or extending volumes, 436–438
spanned and striped volumes, 434
status messages, 447–449
virtual hard drives, 167
volume labels, 440
volume status messages, 449–451
Disk Part tool, 15, 431
disk quotas
administration, 532
creating entries, 536
customizing, 536–537
deleting, 537
disabling, 539
enabling, 533
enforcing, 532
exporting settings, 538
limits, 532
updating, 537
viewing entries, 535
warning levels, 532, 534
disk signatures, 425
disk space
backups and, 643
disk quota policies, 92–94
free space and performance, 173
Stop errors and, 649
storage devices, 411
System Restore and, 95, 204
Windows 7 requirements, 13
disk spanning. See spanned volumes
disk striping. See striped volumes
DiskPart tool
active partitions, 427
bootable USB flash drives, 55
described, 38, 414
listing disks, 57
MBR and GPT disks, 426
virtual hard drives, 167
DISM (Deployment Image Servicing and Management tool)
custom builds, 47–55
subcommands, 6–7
Windows editions, 5
Windows PE, 38
displaying
boot screen display, 375
disk quota entries, 535
event logs, 630
file extensions, 515
files by keystroke, 516
hidden files, 513
hidden tasks, 633
inherited permissions, 491
menu bars, 517
notification area icons, 238
permissions and, 479–480, 486
sync partnerships, 525
system files, 513
toolbars, 239
update and installation history, 623
users working with share resources, 505
DisplayPort adapters, 257
disable drivers, 254–257
drive checking, 253
color and appearance, 249–252
color quality, 258
degaussing, 261
extending screen display, 258
external, 576
failures during startup, 353
firmware and, 345
flickering or spotty, 260
legacy application problems, 327
multiple monitor support, 258
power settings, 248
powering down, 211
readability adjustments, 252
refresh rates, 253, 259
Remote Desktop settings, 164
resolution, 252, 258, 638
switching monitors, 257
troubleshooting, 260, 638
types of, 257
user privileges, 132
Windows PE and, 39
distributed caches, 540
distributed file system (DFS), 518
Distribution Transaction Coordinator, 128
distribution groups, 128
DLLs (dynamic link libraries), 9, 276, 297
DMA (direct memory access), 175
DNS (Domain Name System)
adding IP addresses, 560
checking settings, 191
configuring, 559–561
DHCP releasing and renewing, 570
displaying configuration, 566
dynamic updates, 561
flushing cache, 572
functions of, 543
network shares, 506
obtaining address automatically, 557
pinging, 568
PowerShell and, 7
primary DNS suffix, 191
printers, 294
private IPv4 addresses, 580
registering addresses, 561, 572
static IP addresses and, 556
suffixes, 560
docking taskbar, 236
dollar sign ($), 504
Domain Administrators group, 533
domain Group Policy objects, 85, 88–90
Domain Name System. See DNS (Domain Name System)
domains
color membership in, 125, 190
dial-up connections, 589
domain user accounts, 126
encryption recovery policies, 470
file and data policies, 92–102
file sharing options, 475
information about, 171
local account logon vs.
domain, 130
local logons, 138
logging on, 22
logon names, 126
logon screens, 143
network connection policies, 102
passwords, 23, 142
policy settings, 84
recovery agents, 469
remote access, 597
removing accounts and denying access, 144
security configuration, 136
shares, 495–500
eSATA devices and ports

UAC and, 21
update servers, 622
VPN connections, 591
Welcome screens, 143
Windows 7 editions and, 2
DOS applications, 324
double-colon notation, 550
downloading
Public Downloads folder, 507
themes, 240
trusted peers and, 619
updates, 13, 617–619
user privileges, 132
Windows AIK, 41
DPI (dots per inch), 252
drive designators, 429
drive letters
assigning, 412, 429, 438
in-use or reserved, 440
mapping to shares, 501, 503
moved disks and, 447
Windows Explorer and, 515
Windows PE and, 40
Drive Maps policies, 114, 116
drive paths, 412, 430, 438
driver model boot services,
driver stores, 342
drivers.
See device drivers
Drivers folder, 297
DriverStore folder, 297
dropped connections, 599
Drvload tool, 38
DSL routers, 581
dual booting, 397
dual IP-layer architecture, 549
Dual Link DVI, 257
dual processor support, 3
dump files, 202, 330, 648
duplicate devices, 309
duration of connections, 564
DVDs and DVD drives
AutoPlay feature, 337
backup devices, 642
bootable image files, 54
data DVDs, 460–464
opening files on, 331
share designations, 505
Windows RE bootable drives, 59
DVI, DVI-I, DVI-A, DVI-D (Digital Video Interface), 257
dynamic disks and volumes
characteristics, 420–429
converting to basic, 408, 412, 428–429
described, 420
Disk Management tool, 411
error correction, 421
extending, 436
external hard drives, 423
functions, 408–414
laptops and, 423
mirrored disks, 420
moving to new systems, 445
partitions on, 11, 408–414
removable media and, 422
shrinking, 436
spanned disks, 420, 435
striped disks, 420, 435
volumes on, 408, 423–425
Dynamic Host Configuration Protocol. See DHCP
(Dynamic Host Configuration Protocol)
dynamic IP addresses, 554,
557, 570, 575, 577, 613
dynamic link libraries, 9, 276, 297
E
E$ share, 505
EAP (Extensible Authentication Protocol), 601, 611
Ease Of Access theme, 251
Easy Connect invitations, 625, 627
echo requests, 476
editing states, 117, 123
EEPROM RAM, 353
effective permissions, 493
EFI (Extensible Firmware Interface), 8, 11, 340, 356, 364
EFI byte code virtual machine support, 343
EFI system partition (ESP), 9, 11, 409
EFS (Encrypting File System), 3, 380, 467–468, 470
EIST (Enhanced Intel SpeedStep Technology), 350
electromagnetic interference, 260, 290, 616
elevation
Admin Approval Mode, 135
administrator accounts and, 22
administrator applications and, 312
application privileges, 313
described, 132
malicious software and, 131
policy settings and, 102
security and notification, 135, 314
spoofing prompts, 314
e-mail Remote Assistance invitations, 105, 625–626
Emergency Management Services. See EMS (Emergency Management Services)
empty drives, 515
EMS (Emergency Management Services), 363, 366, 371–374
Enabled Group Policy state, 90, 92
Encrypting File System. See EFS
(Encrypting File System) encryption. See also EFS
(Encrypting File System) BitLocker, 387–393, 400
branch caching and, 541
Cipher utility, 472
decrypted files, 471
decrypting data, 472
file sharing and, 477
file systems and, 390
Group Policy, 468
L2TP and PPTP, 582
Next Generation TCP/IP, 552
offline files, 96, 101, 531
passwords and encrypted files, 140
recovering passwords and data, 141
Remote Assistance invitations, 104
Remote Desktop sessions, 165
TPM process, 380
validation techniques, 601
VPN connections, 592
Windows Explorer display, 515
wireless networks and, 610
encryption keys, 467
Energy-Report.html file, 209
enforcing
disk quotas, 532, 534
preferences, 114
Enhanced Intel SpeedStep Technology (EIST), 350
Enterprise mode WPA, 611
environment policies, 114, 116
environment variables
command path, 333
configuring, 198–200
error messages, 310
folder paths and, 500
resolving, 500
startup process, 352, 357
syntax for, 16
EPIC (Explicitly Parallel Instruction Computing), 8
error messages, 382, 528, 644, 647–649
error reporting, 264, 276, 278
errors, 35, 629
eSATA devices and ports, 26, 423
ESP (EFI system partition), 9, 11, 409
Ethernet protocols, 602
event log diagnosis test, 35
Event Log Readers group, 129
event logs, 629–630, 648
event services (UEFI), 342
Event Viewer, 169
events, 527, 629–630, 632, 639
Everyone group, 475
Everyone identity, 483
executables. See applications
execution protection, 196
exFAT file system, 421–422, 458, 470
expanded caching, 523
expanding compressed drives, 466
expansion cards, 344
Explicitly Parallel Instruction Computing (EPIC), 8
Explorer Favorites folder, 232
Explorer Links folder, 232
Explorer shell, 233, 638
exporting
BCD store entries, 363
disk quota settings, 538
scheduled tasks, 633
Extend Volume Wizard, 437
extended attributes, 485
extended FAT file system (exFAT), 421–422, 458, 470
extended memory, 416
extended partitions or volumes
basic disks, 420, 428
creating, 431, 436–438
deleting, 441
described, 408
Disk Management tool, 411
dynamic disks, 420, 428
limitations, 436
MBR drives, 409
moving disks to new systems and, 446
simple and spanned volumes, 434
extended screen display, 258
Extended Selective Acknowledgments feature, 550
Extensible Authentication Protocol (EAP), 601
Extensible Firmware Interface. See EFI (Extensible Firmware Interface)
external devices, 284, 423, 459, 576
external IP addresses, 552
external support services, 31

F
Failed drive status, 443
failed file accesses, 510
Failed Redundancy status, 456
Failed registry value, 357
Failed volume status, 450
fallback diagnosis, 35
fan speed, 213
fast user switching, 23
FAT, FAT16, and FAT32 file systems
BitLocker and, 390, 397
bits, 408
cluster sizes, 421–422
comparisons, 421
converting to NTFS, 441
described, 430
EFI shell and, 12
encryption and, 470
file security and sharing, 473
removable media drives, 458
volume labels, 440
fatal system errors, 202
fault tolerance (disks and volumes), 434, 444, 449
fault-tolerant heap, 31
favorite links, 232
Favorites menu, 232
FAX$ share, 501
Federal Information Processing Standard (FIPS), 393, 612
file allocation tables, 408
File And Printer Sharing exception, 476, 506
File And Printer Sharing For Microsoft Networks component, 602
file associations, 334–337
file extensions
activation, 323
default programs, 331
displaying, 515
file associations and, 334–337
file caching and, 96, 101
offline use and, 97
file management policies, 92–102
File menu, removing, 518
file names, 324, 485
file paths, 332–334
file sharing
accessing resources, 501–504
administrative shares, 504
auditing and tracking, 508–511
changing or disabling, 476, 497
Computer Management and, 498–500
decrypted files, 471
enabling network sharing, 476, 494, 516
encryption, 477
Group Policy and, 500
network shares, 495
NTFS permissions, 478–494
offline use of files, 499, 522–524
passwords, 477
preventing, 477
Public folder, 507–508
removable media, 459
security and, 473–478
troubleshooting, 506–507
types of, 474, 494
Windows 7 edition differences, 3
File Sharing wizard, 475, 496, 516
File Signature Verification Utility, 179
File System Object shortcuts, 233
file system test. See Check Disk tool
types of file systems. See also specific
types of file systems, i.e., FAT, NTFS
basic disks, 408
BitLocker and, 390
clusters, 421–422
converting to NTFS, 441
cryptographic hard disks, 430, 438
decompressing hard drives, 458
repairing errors, 454
security and sharing options, 473
selecting, 433
File Transfer Protocol (FTP), 597
File Type policies, 115
file types. See file extensions
files
associations, 334–337
attributes, 485
disk allocation, 277
burning to CDs or DVDs, 460, 464
corrupted files, 31
default programs for, 331
deleting, 517
descriptions, 515
desktop location, 243
device drivers, 297–298
Disk Cleanup, 180
encryption, 467–472
expanding compressed, 467
extensions. See file extensions
hidden, 513
in-use files and updates, 264, 618
network permissions, 495
NTFS permissions, 478–494
offline files. See offline files and folders
ownership, 488
policy preferences, 114–115
previews, 516
Public folder and, 507
recovering corrupted, 31
recovering previous versions, 206, 636
Remote Assistance invitations, 625, 627
sending via Remote Assistance, 628
sharing. See file sharing
shortcuts for, 232
signature verification, 182
size, 515
special permissions, 487
uninstalled program leftovers, 330
versions of, 203, 521
Windows Explorer configuration, 513–520
Files policies, 114, 117
Filter Manager, 419
finding. See searching
FIPS (Federal Information Processing Standard), 393, 612
firewalls
Action Center alerts, 18
configuring connections and, 604
devices and, 290
multiple network features, 28
network discovery and, 544
policies, 102
Remote Assistance and, 626
Remote Desktop feature and, 164
shares and, 506
status, 266
wireless networks and, 610
FireWire devices
Active status, 424
disconnecting, 411
dynamic disks and, 423
file systems and formats, 458
installing, 286–288
No Media drive status, 449
unplugging, 26
Unreadable status, 448
versions of, 458
firmware and firmware interfaces
64-bit architecture, 8
boot services, 341
boot settings in, 351
booting process, 344
configuration details, 345
configuring boot options, 354
described, 340
elements of, 346–348
failures during startup, 354
firmware interface
abstraction, 27
identifier, 366
interface types, 340
keyboard shortcuts, 348
manual configuration, 308
motherboard-chipsets, 340
passwords for, 346
power states and management, 348
run-time services, 341
startup process, 345, 351
TCG-compatible, 380
TPM-compatible, 380
troubleshooting, 339, 353
UEFI overview, 342–344
updating, 340, 346
versions of, 345
Firmware Boot Manager, 362
first megabyte policy, 373
Fixed Drive policies, 392
flash devices. See USB flash devices
flash memory, 353, 417
flickering displays, 260
floppy disks, 24, 142
floppy drives, 520
flushing DNS caches, 572
Folder Options dialog box, 514, 518
folders
arranging on screen, 243
attributes, 485
compressing, 465
created by Windows PE, 41
created during installation, 15
desktop location, 243
cracks, 203, 472
disk cloning, 521
encrypting, 467
expanding compressed, 467
ghosting, 521
hidden, 229
network permissions, 495
NTFS permissions, 478–494
offline. See offline files and folders
ownership, 488
policy preferences, 114–115
preventing display of contents, 520
public folder sharing, 474
recovering previous versions, 206, 636
shortcuts in, 231–232
special permissions, 487
standard folder sharing, 474
Start Menu and Programs folders, 227–230
symbolic links, 16, 322
tools for, 239
uninstalled program leftovers, 330
Windows Explorer configuration, 513–520
Folders policies, 114, 117, 234
fonts, 52, 132, 251–252
Fonts folder, 232
foreign disks, 448–449, 451
forests, 88
forgotten passwords, 24
Format tool, 431
disk space
formatting
partitions and volumes, 433, 438
Quick Format feature, 433
removable media drives, 458
status messages, 450
storage devices, 412, 430
forward lookups, 572
Found New Hardware wizard, 299
fragmentation, 443
free disk space
backups and, 643
basic and dynamic disks and, 428
displaying, 411
offline files, 530
performance ratings and, 173
recommended amount, 13
Stop errors and, 649
troubleshooting and, 447
FSUtil tool, 414
FTP (File Transfer Protocol), 597
Ftype tool, 335
disk space
full synchronization, 100
function keys, 406
Gaming graphics, 173, 211
Gateway metrics, 558
Gateways configuring, 558
dead gateways, 550
DHCP releasing and renewing, 570
displaying, 566
static IP addresses, 556
wireless. See wireless networks
generic credentials, 145
ghosting unavailable files, 521
global debugger parameters, 363, 366
GPMC (Group Policy Management Console), 88, 90
GPOs (Group Policy objects) administrative templates, 91
creating, 86
editing, 86, 120
errors processing, 122
GPO links vs. GPOs, 88
links compared to objects, 88
local Group Policy, 85–88
removing items, 122
site, domain, and OU Group Policy, 88–90
GPT (GUID partition table) capacity of partitions, 409
EFI and, 342
Itanium computers, 8
partition data storage, 409
partition styles, 409
required partitions, 409
switching to MBR, 410, 426
UEFI and, 342
Windows RE and, 61–62
GPUs (graphics processing units), 249
graphic enhancements, 192, 250
graphics adapters changing drivers, 254–257
checking drivers, 253
color capabilities, 259
power plans, 211
ratings, 173
refresh rates, 259
startup process, 344
troubleshooting, 260
Windows 7 requirements, 12
graphics mode, 357, 373

graphics processing units (GPUs), 249
group accounts. See groups
group keys, 611
Group Policy. See also policies; policy preferences; policy settings
Active-Directory–based Group Policy, 84
Common tab items, 121
computer and user scripts, 106–109
configuring, 90–92
conflicts, 84
deleting applications, 322
local Group Policy, 84–88
order of application, 84
policy settings and preferences, 83
processing preferences, 120
Group Policy Management Console (GPMC), 88, 90
Group Policy Management Editor, 86, 89–91, 120
Group Policy Modeling Wizard, 88
Group Policy Object Editor, 86
Group Policy Results Wizard, 88
groups. See also homegroups; workgroups; domains
adding members to, 154
basic permissions, 478–494
computer membership, 190
default accounts in, 127
deleting, 158
features of, 128–130
file ownership, 489
local groups, 152–154
network permissions, 495
permission assignments and, 483
policy preferences, 115
renaming, 157
scheduling updates, 622
SIDs, 129
special permissions, 486
types of, 20, 128–130
Guest accounts, 127, 156
Guests group, 127, 129
GUID partition table. See GPT (GUID partition table)
GUIDs (BCD store identifiers), 366–368
GUIDs (device classes), 303
Hacking, prevention, 380, 388
HAL (hardware abstraction layer), 297, 352–353, 356, 374
hard disks
basic vs. dynamic, 11, 420–429
booting from, 351
compression, 465–467
Computer console, 410
configuration tools, 410–414
converting to NTFS, 441
defragmenting, 454–456
deleting volumes or partitions, 440
disk failure diagnosis test, 34
Disk Management tool, 411
disk space requirements, 13
DiskPart tool, 414
drive letters and paths, 438
empty, 515
encryption, 391–392, 467–472
error detection, 35
extending volumes, 436–438
failures during startup, 354
firmware interface controls, 345
foreign, 448
formats and file systems, 429
free space on, 447
FSUtil tool, 414
GPT partitions, 342, 426
hiding, 517, 520
hybrid, 417
installing and initializing, 425
internal and external, 283
logical, 431–434
MBR vs. GPT, 426
mirrored, 355, 444–445
moving to new systems, 445
paging files on, 195
partitions, 408–414, 431–434
PE images on, 56
performance, 414–419
powering down, 211
preventing access to, 517
problems selecting for installation, 15
quotas, 532–539
ratings, 173
recovering, 443, 639
Remote Desktop connections, 166
removable media. See removable media drives
help desks, 160–162
hibernation, 208, 213, 348–351, 370, 622, 636
Hibernation File Cleaner, 180
hidden devices, 296
hidden files, 513
hidden folders, 229
hidden scripts, 107
hidden shares, 504
hidden tasks, 632–633
help desk configurations, 192
device drivers, 297–310
Device Manager, 295
error detection, 35
error message list, 306–310
event logs, 629
failures during startup, 353
help system, 264–283
printers, 291–295
ratings, 173
recently changed or added, 648
system diagnostic reports, 174
system information, 175
troubleshooting, 33, 638
Windows 7 requirements, 12
wireless, network, and Bluetooth, 289–291
hardware abstraction layer. See HAL (hardware abstraction layer)
Hardware And Device troubleshooter, 273
Hardware And Sound troubleshooter, 33
Hardware tab (System Properties dialog box), 192, 518
Hardware Update wizard, 296
HDMI (High-Definition Multimedia Interface), 257
Healthy (At Risk) volume status, 450
Healthy (Unknown Partition) volume status, 450
Healthy volume status, 450
heap, fault-tolerant, 31
help. See Automated Help and Support features
help desks, 160–162
hibernation, 208, 213, 348–351, 370, 622, 636
Hibernation File Cleaner, 180
hidden devices, 296
hidden files, 513
hidden folders, 229
hidden scripts, 107
hidden shares, 504
hidden tasks, 632–633
hidden folder contents, 520
hard drives, 517, 520
icons, 246
logon names, 142
notification icons, 238
shares, 520
taskbar, 237
toolbars, 239
updates, 623
High Performance power plan, 211
High-Definition Multimedia Interface (HDMI), 257
high-priority I/O, 418
hints, password, 140–141
history feature, 236, 268, 623
home networks, 544, 575
HomeGroup Networking troubleshooter, 273
computer membership in, 125
file sharing and, 475
information about, 171
local user accounts in, 137
passwords, 140
recovery policies, 470
stored credentials, 145
UAC and, 20
workgroups vs., 20
host caches, 540
hotkey sequences, 232–234
HTML support, 52
HTTP (Hypertext Transfer Protocol), 597
hubs (USB), 458
Human Interface Infrastructure support, 343
hybrid sleep, 208, 213
hypervisor binaries, 374
hypervisor debugging settings, 371
hypervisor launch type, 374
hypervisor parameters, 363, 367
IEEE 1394 devices. See FireWire devices
IEEE 802.11, 609
IEEE 802.11a, 609
IEEE 802.11b, 609
IEEE 802.11g, 609
IEEE 802.11i, 609, 611
IEEE 802.11n, 609
IGMPv3 (Internet Group Management Protocol version 3), 552
IKE (Internet Key Exchange), 552
image files, 243
image services, 342
ImageX tool, 38, 43–48, 53, 66
Immediate Task policies, 115
immediate update installation, 621
importing disk quota settings, 538
indexed file data, 518
indexing settings, 173
INF files (Setup Information), 297, 319
informational events, 629
infrastructure mode (wireless), 612
inherited permissions, 479, 481, 483, 489–493, 511
INI Files policies, 115
initialization logging, 374
physical disks, 425
startup failures, 354
startup process, 351
TPM, 381, 383
troubleshooting, 353
volumes, 450
initialization files, 27
Initialize And Convert Disk Wizard, 425
Initialize The TPM Security Hardware wizard, 382–383
Initializing volume status, 450
input/output (I/O). See I/O problems
installation restore points

204, 639

Installed Programs (Control Panel), 330

installing hardware
device drivers, 299–302
internal, USB, or FireWire, 286–288
network adapters, 552, 612
network components, 549–554
preexisting devices, 284–285
printers, 291–295
restore points and, 639
restricting with Group Policy, 303
wireless, network, and Bluetooth, 289–291

installing software
Admin Approval Mode settings, 134
all users vs. selected users, 321
application installation, 318–322
Autorun, 318–319
BitLocker, 391, 394, 400
compatibility checks, 320
failure notifications, 265
group Policy deployments, 322
install-on-first-use, 322
network components, 549–554
privileges, 313
problems with, 318
restore points and, 639
setup programs, 319
TCP/IP, 553
updates, 617–619, 623
video drivers, 255
Windows PE, 39, 41

installing Windows 7. See also deployment
activating, 19
automated installation, 65
clean installations vs. upgrades, 10
command prompts, 14
interactive vs. automated, 10
performing installation, 12–15
preparations, 10–12
prior versions, 180
product keys, 14
troubleshooting, 15
Windows PE and, 38

InstallShield, 319, 330

Intel processor power settings, 350

Intel Quick Resume Technology Driver (QRTD), 350

Intel Xeon processors, 8
Interactive identity, 483
interactive installation, 10, 13–15
interfaces, firmware. See firmware and firmware interfaces
interference in wireless networks, 616
internal drives, 283, 286–288, 520, 642
internal IP addresses, 552
Internal state check, 35

Internet
connection policies, 117
installing software from, 319
Network And Internet troubleshooter, 33
routing policies, 582
security, 18, 266
shortcuts to resources, 232

Internet Connection Firewall feature, 102
Internet Connection Sharing feature, 102
Internet Connectivity troubleshooter, 273

Internet Group Management Protocol version 3 (IGMPv3), 552

Internet Key Exchange (IKE), 552
Internet service providers (ISPs), 583, 587
interrupt requests (IRQs), 175
invitations, 104, 160, 162, 625–628

IP addresses
adding, 560
alternate, 557
checking, 191
DHCP releasing and renewing, 570
displaying configuration, 566
dynamic IP addresses, 557
internal and external mapping, 552
IPv4 and IPv6 addressing, 549
mobile computing settings, 577
network devices and, 291
pinging, 568
PowerShell remote management and, 7
printers, 294
private and public addressing, 552
proxy servers, 597
resolving problems, 569
static, 554
VPN connections, 591

IPSec (IP Security), 541, 582, 602
IPv4 and IPv6 protocols
dynamic or alternate IP addresses, 557
installing, 554
mobile computing settings, 577
Next Generation DHCP, 552
private IPv4 addresses, 555
resolving problems, 569
scanning for addresses, 552
static IP addresses, 555–556
VPN connections, 591
Windows PE support, 40
wireless networks, 613
IPv6 over IPSec protocol, 602
IPv6 over Point-to-Point Protocol (PPPv6) feature, 552
IRPs (interrupt requests), 175
ISA interrupts, 308
iSCSI support, 343
ISO files, 43, 54, 59, 460–461
ISPs (Internet service providers), 583, 587
Itanium-based systems. See IA64 processors (Itanium)
item-level targeting, 123

J

JScript, 106
jump lists, 226
junctions (reparse points), 322

K

Kerberos authentication, 145
kernel, 202, 352–353, 356, 363, 374
Kernel Transaction Manager (KTM), 451
keyboard failures, 353
KTM (Kernel Transaction Manager), 451
L

L2TP (Layer 2 Tunneling Protocol), 581, 602
labels for volumes and partitions, 433, 440
LAN networks, 103, 540
language support, 4, 53
laptops and tablet PCs
alternate IP addresses, 578
automatic or manual connections, 593
battery information, 209
broadband connections, 590
dial-up connections, 583–589, 593, 599
disconnections, 598
dynamic disks and, 422
dynamic IP addresses, 577
firmware configuration, 345
identity validation, 601
lid power options, 212
logon configuration, 597
network access policies and, 103
network connections, 575–580, 593, 604–608
network projectors and, 580
network protocols and components, 602–604
offline files and, 520
Power icon, 210
power management, 207, 248
proxy settings, 594–597
remote access connections, 583–592
sleep mode, 25
VPN connections, 591
Windows 7 edition differences, 4
Windows Firewall and, 604
Windows Mobility Center, 576
Windows ReadyDrive, 417
wireless adapters, 608
wireless connections. See wireless networks

last known good configuration, 374, 638
LastKnownGood registry value, 357
Layer 2 Tunneling Protocol (L2TP), 581, 602
leases (DHCP), 566
legacy applications, 312, 321, 324
legacy device interrupts, 308
legacy devices, 307

legacy OS BCD store entries, 41, 362, 367
legacy run–list applications, 110–111
legacy scripts, 107
legacy setup packages, 52
libraries, 16, 475
licensing, 4, 19
link shortcuts, 232–233
Link-Local Multicast Name Resolution (LLMNR), 552
links on menus, 224
Links toolbar, 239
live file system CDs and DVDs, 461, 463
LLMNR (Link-Local Multicast Name Resolution), 552
LLTDIO driver, 549
LMHOSTS files, 562–563
local accounts. See also local user accounts
credentials, 144–149
deleting, 158
domain logon vs., 130
group accounts, 149–158
local administrator accounts, 133–137
local logon, 137–144
local user accounts, 149–158
logon and welcome screens, 142
passwords, 137
recovery agents, 469
remote access, 159–166
removing and denying access, 144
renaming, 157
local administrator accounts, 133–137
local area connections, 554–564, 566–573
local Group Policy, 84–88, 90
local groups, 128, 152–154
local printers, 115, 291–293
Local Security Authority, 352, 358
Local Security Policy console, 136, 142, 157, 390
local user accounts
Admin Approval Mode, 133–137
creating, 150–151
deleting, 158
domain accounts vs., 130
enabling or disabling, 155
features of, 126–128
Guest accounts, 156
local logon, 137–144
logon names, 126
optimizing UAC, 133–137
passwords, 140
remote access, 159–166
removing and denying access, 144
renaming, 157
types of, 20, 139
UAC and elevation, 131–137
Local Users And Groups policies, 115
Local Users And Groups utility accessing, 170
adding and removing group members, 154
changing account types, 139
creating local groups, 152
deleting accounts, 158
enabling or disabling accounts, 156
managing user accounts, 126, 149
renaming accounts, 157
LocalService account, 128, 277
LocalSystem account, 127, 277, 280, 631
locations
dial-up connections, 584, 586
shortcuts, 233
users, 482
locked accounts, 156
locked computers, 526
locked files, 492
locked taskbar, 237
logging off
Remote Desktop sessions, 164
script policies, 106–108
services for, 278
synchronizing offline files and, 96, 98, 527
uninstalling software and, 330
logging on
classic vs. simple, 110
domain accounts, 130, 138
local logons, 130
logon screens, 142
policies, 109–111
remote access, 597
Remote Desktop and, 162
script policies, 106–108
service logons, 280
services for, 278
synchronizing offline files and, 98, 526–527
task scheduling and, 632, 635
user accounts and, 22

logical drives
active partitions and, 426
basic disks, 420
creating, 431–434
deleting, 440
Disk Management tool, 411
logical drives, continued
drive letters and paths, 438
file system management, 422
switching between basic and dynamic, 428
viewing list of, 412
logs
boot logs, 186
disk quota entries, 535
disk quota limits, 93–94
file sharing activity, 508–511
Group Policy, 84
offline file events, 97
performance data, 375
Remote Assistance sessions, 162
services for, 278
system failures, 202
troubleshooting and, 629
verified file signatures, 182
warning levels, 629
WMI errors, 177
MAC (machine address), 549, 566, 582
maintenance
Action Center, 17–19, 266
automatic updates, 617–624
backing up, 642–645
Maintenance troubleshooter, 273
task scheduling, 631–635
malicious software, 131, 266, 312, 376
Manage item (Windows Explorer), 517
Manage The TPM Security
Hardware wizard, 384, 386
Manage Wireless Networks tool, 616
Managed Network Protocol (MNP), 343
Managed Network Service Binding Protocol (MNSBP), 343
managed settings. See policy settings
management action policies, 115
manual backups, 643
manual network connections, 593
manual restore points, 204, 640
mapping
networks, 548
ports, 552
preventing drive mapping, 517
shares, 501
summary network maps, 547
master boot code, 409
master boot record. See MBR
(master boot record)
master file table (MFT), 430
master keys, 140
Mbps rates, 458
MBR (master boot record)
active partitions or volumes, 423
BIOS and, 342
boot partitions or volumes, 424
capacity of volumes, 409
crash dump partitions or volumes, 425
failures during startup, 356
hard disk capabilities, 409
installing Windows RE and, 61
number of partitions, 409
page file partitions or volumes, 424
partition style, 409
switching drives to GPT, 410, 426
system partitions or volumes, 424
types of partitions, 409
x86 architecture and, 8
media state of connections, 564
media streaming, 477
media support, 343
memory
adding, 284
BCD store entries, 370, 372
boot options, 187
buffers, 551
DEP, 196, 376
diagnostics, 35, 367, 646
diagnostic details, 345
graphics, 250
information about, 171
legacy applications and, 324
large memory usage, 375
memory leaks, 31
nonexecutable portions, 196, 376
optimizing, 418
overwriting, 392
physical memory addresses, 373
prioritization, 418–419
ratings, 173
reducing, 375
relocating, 373
screen savers and, 247
specifying, 361
startup process, 344, 352
Stop errors and, 649
troubleshooting, 264, 353
Windows 7 requirements, 12
Windows PE requirements, 50
Windows ReadyBoost, 414–417
memory allocation services, 342
memory-use prioritization, 418–419
menu bar display, 517
menus
adding and editing, 228
Administrative Tools
menu, 230
customizing, 223–230
deleting items on, 229
deleting menus, 228, 518
policy preferences for, 234
rearranging and adding items, 227–230
shortcuts for items, 230–234
sorting applications in, 225
Windows Explorer
customizing, 514
message signaled interrupts (MSI), 375
MFT (master file table), 430, 443
microchips (TPM), 380
Microsoft
product updates, 620
sending dump files to, 648
Microsoft .NET Framework, 40
Microsoft Backup tool, 640
Microsoft Certificate Services, 582
Microsoft Data Access Component support, 52
Microsoft JScript, 106
Microsoft Knowledge Base, 630, 648
Microsoft Office temporary files, 180
Microsoft Remote Control Incident files, 625
Microsoft reserved partition (MSR), 11, 409
Microsoft Support Diagnostic Tool (MSDT), 31
Microsoft Visual Basic Scripting Edition, 106
Microsoft Windows 7. See Windows 7
Microsoft Windows Installer, 319, 330
Microsoft Windows Installer files (MSI), 323
mirroring BCD entries, 364
Missing drive status, 443
Mklink utility, 16
MLDv2 (Multicast Listener Discovery version 2), 552
MNP (Managed Network Protocol), 343
MNSBP (Managed Network Service Binding Protocol), 343
mobile computers. See laptops and tablet PCs
mobile networking. See also laptops and tablet PCs
automatic or manual connections, 593
broadband connections, 590, 606
dialing rules, 599
dial-up connections, 581, 583–589, 604–606
identity validation, 601
laptop configuration, 575–580
logon configuration, 597
network protocols and components, 602–604
phone numbers, 600
proxy settings, 594–597
redialing and disconnection, 598
remote access connections, 583–592
Remote Assistance, 626
Remote Desktop, 165
types of connections, 581
VPN connections, 591, 607
Windows Firewall and, 604
wireless networks, 615–616
modem pools, 581
modems, 581, 584–587, 590
Modified Fast Recovery Algorithm feature, 551
modifier keys, 232–234
monitors. See displays
motherboard-chipsets, 340, 344
mounting images, 43–47, 50, 53
mouse devices, 242, 353
mouse pointer themes, 242
moving
dynamic disks to new systems, 445
encrypted files, 470
files after disk quota deletion, 537
menu items, 229
taskbar, 236
MS-CHAP version 2, 601
MS-DOS, 37, 324
MSDT (Microsoft Support Diagnostic Tool), 31
MSI (message signaled interrupts), 375
MSI files (Windows Installer), 31, 323
MSR (Microsoft reserved partition), 11, 409
MsRcIncident files, 625
multiboot entry files, 55
Multicast Listener Discovery version 2 (MLDv2) feature, 552
multimedia power settings, 212
multiple monitor support, 258
multiple processors, 187, 308
N
name resolution, 476, 543, 559–563. See also DHCP (Dynamic Host Configuration Protocol); DNS (Domain Name System); WINS (Windows Internet Naming Service)
named pipes, 505
names
computers, 190
logon, 126
shortcuts, 233
SIDs and, 126
namespaces, 177
NAT (Network Address Translation), 159, 626
Neighbor Unreachability Detection for IPv4 feature, 551
.NET Framework, 40
Net Share command, 495, 504
Net tool, 38
NetBIOS names, 7, 476,
561–563, 568
Netcfg tool, 38
NETLOGON share, 501
Network Access Protection client, 3, 266
network adapters, 273, 289–291, 549, 552, 565, 608, 612
Network Address Translation (NAT), 159, 626
network addressing protocol support, 344
Network And Internet troubleshooter, 33
Network And Sharing Center connection status, 29
creating connections, 583
functions of, 544, 546
troubleshooting sharing, 506
Windows 7 edition differences, 4
Windows Collaboration and, 519
network awareness, 28
Network Bridge, 102
Network Configuration Operators group, 129
network connections
access types, 547
broadband, 590, 606
configuration, 565
dial-up, 583–589, 604–606
establishing, 604–608
laptops, 575–580
local area, 554–556
remote access, 583–592
Remote Assistance, 626
Remote Desktop, 165
renaming, 566
speed, 605
troubleshooting, 567–573
types of, 581
VPN, 591, 607
warning icons, 547
wireless, 615–616
Network console notification area, 237
Network Diagnostics, 544
Network Diagnostics Framework feature, 551
network discovery, 28, 291, 476, 544–545, 569
network drives, 411
Network Explorer, 543, 545, 568
Network icon, 245
Network identity, 483
network keys, 613
Network Location Awareness, 84
Network Map, 544
network printers, 291, 293–295
network projectors, 575, 580
network protocols, 343, 602–604
network shares. See shares
Network Shares policies, 115, 117
networks
active, 547
awareness and discovery, 28, 544
backup storage, 642
networks, continued
boots from, 351
branch caching, 540
connection types, 602–604
diagnostic tools, 29
DirectAccess feature, 29
domain networks, 544
enabling sharing, 476
file sharing, 459, 494
file shortcuts, 232
firewalls, 266
homegroups, 20, 544
identifying, 29
installing components, 549–554
latency, 100, 541
local area connections, 554–566
location type, 20
mapping, 547, 549
mobile access. See mobile networking
Network And Internet troubleshooter, 33
Network And Sharing Center, 546
Network Explorer, 545
Network Map, 548
offline files and, 520–531
policies, 102–105, 114–115
public networks, 544
remote access, 583–592
removable media devices, 459
speed, 563–566
troubleshooting, 33, 567–573
UEFI support, 343
VPN connections, 29, 115
waiting for at startup/logon, 110
Windows 7 features and tools, 543
wireless. See wireless networks
work networks, 544
NetworkService account, 128
New Mirrored Volume Wizard, 444
New Simple Volume Wizard, 431
Next Generation TCP/IP stack, 550–552
No GUI Boot option, 186, 360
No Media drive status, 449
Nobody sharing option, 475
no-execute page-protection (NX) processor feature, 196, 309, 367, 375–376
nonexecutable memory, 376
non-system BCD stores, 364, 368
nonsystem volumes, 397
nonuniform memory access (NUMA), 373
nonvolatile memory, 353
non-Windows operating systems, 426, 449
normal startup, 184, 360
Not Configured Group Policy state, 90, 92
Not Initialized disk status, 449
notices
Action Center, 17–19
Admin Approval Mode, 135
battery alerts, 220
customizing, 237, 270–274
described, 430
disk quotas, 93, 532–539
described, 430
disk quotas, 93, 532–539
described, 430
disk quotas, 93, 532–539
encryption and, 470
file security and sharing, 473
permissions, 484–488, 493
permissions, 484–488, 493
removable media drives, 458
self-healing NTFS, 451
system labels, 440
volume labels, 440
Windows RE and, 61
Ntldr (Windows Legacy OS Loader)
BCD store entries, 367, 371
booting earlier Windows versions, 362, 426
identifier, 367
startup process, 344
Windows 7 and, 167
NTLM authentication, 145
NUMA (nonuniform memory access), 373
NX (no-execute page-protection processor feature), 196, 309, 367, 375–376
octets, 549
OEM partitions, 409
Offer Remote Assistance tool, 179, 628
Offline drive status, 443, 448
offline files and folders
opening files, 334–337
operating system configuration. See configuration; operating systems
Operating System Drive policies, 392
operating system folders, 505
operating systems
64-bit support, 9
BitLocker policies, 392
boot order, 377
default, 377
described, 421–422
converting FAT drives to, 441
described, 430
disk quotas, 93, 532–539
encryption and, 470
file ownership, 488
file security and sharing, 473
permissions, 484–488, 493
removable media drives, 458
self-healing NTFS, 451
system labels, 440
volume labels, 440
Windows RE and, 61
offline drive status, 443
Online (Errors) disk status, 457
Online (Errors) drive status, 443, 448
Online Crash Analysis feature, 648
Online drive status, 448
Open Network And Sharing utility, 20
organizational units (OUs), 84, 88–90, 92–102
OS Boot Information option, 187
Oscdimg tool, 38, 43, 54
Osloder entry, 362, 369
OUs. See organizational units (OUs)
out-of-scope preferences, 122
ownership, 382–383, 386, 480, 486, 488, 537
packages in Windows PE, 52
PAE (Physical Address Extension) mode, 196, 370, 375–376
page file partitions or volumes, 424
Play Sound troubleshooter, 273
Plug and Play devices, 39, 175
PNP devices, 39, 175
PNRP (Peer Name Resolution Protocol), 625–626
point and print driver updates, 620
point of presence (POP), 587
pointer themes, 242
pointing devices, 353
Point-to-Point Protocol (PPP), 602
Point-to-Point Tunneling Protocol (PPTP), 581, 602
Policies. See also Group Policy; policy preferences; policy settings
access, 102–105
accounts, 156–158
Application Control, 318
BitLocker, 390, 392–393, 395
branch caching, 541
command paths, 333
Common tab display, 121
connectivity, 102–105
device drivers, 299
devices, 119, 302–303
dial-up connections, 589
DirectAccess, 582
disk quotas, 533
domains, 88–90
cryptography, 468
environment variables, 199
file and data management, 92–102
file sharing, 477, 500, 508
file type and associations, 336
folder views, 516–519
function keys, 118
groups, 153, 155
local printers, 292
logon, 109–111, 143
menus, 234
network mapping, 502, 549
offline files, 526
OUs, 88–90
power management, 219
power plan, 216, 218
printers, 294
Remote Assistance, 162
Remote Desktop, 164
scripts, 106–109
services, 119, 282
sites, 88–90
Software Restriction, 318
Start menu, 226
startup, 109–111, 143
startup applications, 235
tasks, 119
TPM, 393
troubleshooting and diagnostics, 274–276
UAC application, 317
unsigned drivers, 298
upgrades, 619, 621–622
user accounts, 149, 151
VPN connections, 592
Windows Explorer, 516–519
policy preferences
configuration, 115–119, 121
creating items, 120
description, 83
editing items, 120
editing states, 117
extensions, 122
management actions, 115
out-of-scope, 122
processing order, 120
shortcuts, 123
targets, 123
types, 113–115
policy settings
application order, 84
configuration, 90–92
conflicts, 84–85
description, 83
disabled settings, 90–91
enabled, 90–91
local settings, 85–88
not configured, 90–91
Power-based Quality of Service feature, 4
POP (point of presence), 587
portable computers. See laptops and tablet PCs
portable media drives. See removable media drives
ports
debugger ports, 371
devices and, 284
EMS ports, 371
file sharing and open ports, 476
HTTP, SSL, FTP, or Socks, 597
mapping, 552
network shares and, 506
printer configuration, 291
proxy servers, 597
Remote Assistance and, 624
POST (power-on self test), 351, 353
power button, 26, 212, 218, 224, 351
Power Configuration, 208–210
Power Efficiency Diagnostics report, 209
power management
ACPI power states, 348–351
alarms and warnings, 220
command-line options, 208–210
displays, 248
Group Policy settings, 219
laptops, 207
password protection, 218
power plans, 210–214, 217
power states, 348–351
screen savers and, 247–248
troubleshooter, 273
updates and, 622
user privileges, 132
Power Options policies, 115
power plans
active plans, 208
configuring, 210–214
creating, 217
deleting, 208
listing, 208
policies, 115, 117
selecting and optimizing, 214–217
settings, 173
types of, 210
Windows 7 options, 25–27
power states, 348–351
Power troubleshooter, 273
Power Users group, 129, 313
power-on self test, 351, 353
PowerShell 2.0, 7, 106, 272, 278
PPP (Point-to-Point Protocol), 602
PPPoE (PPP over Ethernet), 552, 590, 602
PPPV6 (IPv6 over Point-to-Point Protocol), 552
PPTP (Point-to-Point Tunneling Protocol), 581, 602
Preboot Execution Environment (PXE), 343
preference extensions, 122
preferences. See policy preferences
prefetching data, 277, 419
preloading applications, 419
presentation settings, 576, 580
primary partitions, 408–409
print driver updates, 620
printer sharing, 3, 476, 494, 505
printers, 115, 132, 166, 291–295
Printers, 291–295
Preboot Execution Environment (PXE), 343
primary partitions, 408–409
print driver updates, 620
printer sharing, 3, 476, 494, 505
printer troubleshooter, 273
primary DNS suffix, 191
principle of least privilege, 483
previews of files, 516
previous versions of data, 206, 636
primary partitions, 408–409
print driver updates, 620
printer sharing, 3, 476, 494, 505
Printer troubleshooter, 273
preferences.
See policy preferences
primary DNS suffix, 191
principle of least privilege, 483
print driver updates, 620
printer sharing, 3, 476, 494, 505
Printer troubleshooter, 273
primary partitions, 408–409
print driver updates, 620
printer sharing, 3, 476, 494, 505
Printer troubleshooter, 273
primary partitions, 408–409
print driver updates, 620
printer sharing, 3, 476, 494, 505
Printer troubleshooter, 273
primary partitions, 408–409
print driver updates, 620
printer sharing, 3, 476, 494, 505
Printer troubleshooter, 273
printing recovery keys, 398, 400, 405
resolution of, 252
TPM passwords, 384
prioritizing applications, 419
private debugger transport, 374
private hypervisor binaries, 374
private IPv4 addresses, 555, 578
private kernels, 374
private keys, 127
private networks. See VPN connections privileges, 84, 132. See also permissions
Problem Devices node, 176
problem reporting, 18, 270
Problem Reports And Solutions feature, 277, 306, 629
Problem Steps Recorder, 159
processes event logs, 629
new windows as, 515
stopping or starting, 329
SuperFetch utility and, 418–419
Task Manager list, 329
processors APIC clusters, 374
boot options, 187
firmware configuration, 345
firmware interface controls, 345
information about, 171
multiple, 375
number of, 360, 374–375
power options, 212
ratings, 173
screen savers and, 247
startup process, 344
Windows 7 requirements, 12
processor-scheduling caching, 193
product keys, 5, 14, 19
profiling, 49–50, 54
Program Compatibility Assistant. See PCA (Program Compatibility Assistant)
Program Compatibility troubleshooter, 273
Program Compatibility wizard, 325–327
Program Files folder, 330
Programs folder, 227, 232, 321
Programs menu, 232
Programs troubleshooter, 33
projectors, 575, 580
prompting after updates, 622
Properties dialog box (applications), 325, 328
Properties dialog box (policy preferences), 120
properties of BCD entries, 365–366
proxy server settings, 594–597
pseudo-accounts, 127
Public folder, 474, 477–478, 494, 507–508
public keys, 127, 467
public networks, 506, 544
publisher not verified (unsigned) applications, 314
publisher verified (signed) applications, 314
publishing applications, 323
PXE (Preboot Execution Environment), 343
Q
QRDT (Intel Quick Resume Technology Driver), 350
queued tasks, 635
Quick Format feature, 433
Quick Launch toolbar, 236
Quick Resume mode, 350
Quick Sleep mode, 350
quick synchronization, 100
quota limits, 92–94, 532–539
R
RAID controllers, 355, 421
RAM adding, 284
defects in, 366
disk options, 367
hybrid drives, 417
loading Windows PE into, 39, 56
Stop errors and, 649
virtual memory and, 194
Windows 7 requirements, 3, 13
Random Interface IDs feature, 552
range of wireless devices, 609
ratings, 172
RDP files, 164
reactivating mirrored disks, 457
Read permission, 480
readability adjustments, 252
read-only files, 469
ReadyBoost, 414–417
reboot configuration, 202
Receive Window Auto Tuning feature, 551
receive windows, 551
receivers (wireless or Bluetooth), 289
Recent folder, 232
recentsky used documents, 232, 517
recommended updates, 620
reconnecting to shares, 502–503
Record Sound troubleshooter, 273
recording problem steps, 159
recovering passwords, 141
personal data, 645
restarting services, 281
restore points and, 641
system files, 645
system images, 646
System Restore tool, 639–641
volumes, 443
recycle agents, 468, 471
recovery certificates, 397, 471
Recovery control panel, 58
recovery extensions, 393
recovery keys, 388, 391, 393, 398–399, 402, 404–405
Recovery mode, 388, 405
Recovery objects, 393
recovery partitions, 61
recovery passwords, 392, 397
recovery sequences, 373
recovery tools, 12, 38
Recycle Bin, 181, 244, 517, 519
redialing connection options, 598
refresh rates, 253, 259
Regenerating disk status, 457
region settings, 585–586
Regional Options policies, 115, 117
registering DNS addresses, 561, 572
registry, 40, 90, 111, 115, 307, 309, 313, 317, 335
Registry Editor, 304
registry hives, 35, 352, 356
Registry policies, 115, 117
reinstalling device drivers, 305
Windows 7, 646
releasing DHCP settings, 570
reliability reports, 268
remote access automatic or manual connections, 593
branch caching and, 541
broadband connections, 590
connection types, 581
dial-up connections, 583–589, 598–599
establishing connections, 604–608
data sharing settings, 498–500
identity validation, 601
logon configuration, 597
Remote Assistance feature

file systems and formats, 458
No Media drive status, 449
opening files on, 331
performance, 414–419
removing. See deleting; ejecting
device
renaming
encrypted files, 470
folders and shortcuts, 229
network connections, 566
renewing DHCP settings, 570
Repair Your Computer mode, 637, 646
repairing
applications, 330
computers, 637, 645–646
disk errors, 451–454
mirrored disks, 456–457
reparse points (junctions), 322
repeating synchronization, 526
Replicator group, 130
reporting problems. See problem reporting
reports
Action Center links, 266
Disk Cleanup tool, 180
Power Efficiency Diagnostics report, 209
power issues, 208
reliability reports, 268
report queue configuration, 276
signature verification utility, 183
system diagnostic reports, 174
repositories (WMI statistics), 177
re-recordable discs, 461
rescanning discs, 443
rescheduling updates, 622
reserve battery alarm, 221–222
reserved drive letters, 440
Reset Password Wizard, 25
resetting
computers, 343
passwords, 25
TPM, 383
resizing
dialog box and window elements, 251
icons on menus, 225
taskbar, 236
volumes and partitions, 436
resolution
changing, 258
driver details, 253
graphics display, 373
printing and, 252
readability and, 252
troubleshooting, 253
resolving
sync conflicts, 529
variables, 500
resource allocation, 296, 308
resource exhaustion, 32, 307
Resource Manager, 174
responsiveness, 32, 174, 194, 581
Restart Manager, 33, 265
restarting
automatic restart, 375
BitLocker and, 390
delaying after updates, 621
disabling automatic, 638
limiting after updates, 618
safe mode and other options, 637
services, 280–281
Windows PE automatic, 40
Restore Files window, 645
restore operations, 640
Restore Operators group, 488
restore points, 319, 639–641
restoring
BCD store, 364
computers, 639–641
desktop themes, 241
files or folders, 206
inherited permissions, 492
personal data, 645
previous versions of files, 203
Start menu, 226
Windows vault, 148
WMI repository, 178
Resume (Windows Resume Loader), 362, 369
Resume From Hibernate entry, 370
resuming
performance of, 32
services, 280
Windows Resume Loader, 636
resynching mirrored disks, 450, 456
retransmission timeouts, 551
reverse lookups, 572
right-click menus, 225, 518
roaming profiles, 145, 468
Robust Security Network (RSN), 612
root folders, 489
rotating encryption keys, 611
routers, 550, 558, 590
Routing Compartments feature, 551
routing costs, 558
routing policies, 582
routing tables, 551
RPC (Remote Procedure Call), 128
RSA public key encryption, 468
RSAT (Remote Server Administration Tools), 88
RSN (Robust Security Network), 612
RSPNDR driver, 549
run levels for applications, 315–317
run-list applications, 110–111
running application privileges, 313
applications, 329
DISM, 6
run-once application run level, 315
run-once lists, 110–111
run-time services, 341, 343
S
S0–S5 power states, 348–351
SACK-Based Loss Recovery feature, 551
SACKs (Selective Acknowledgments), 550
Safe Boot option, 186, 360, 375
Safe Mode option, 341, 637
Safe Mode With Command Prompt option, 638
Safe Mode With Networking option, 637–638
Safe Removal application, 310
SAL (system abstraction layer), 342
saving branch caching and, 541
optimized build profiles, 54
recovery keys, 398, 405
sync schedules, 526
themes, 241
scanning hardware changes, 296, 309
IPv6 addresses, 552
scheduled backups, 4, 643–644
scheduled defragmentation, 455
scheduled maintenance, 32
scheduled offline file sync, 526
Scheduled Task policies, 115
scheduled tasks. See task scheduling
scheduled updates, 621
Schtasks tool, 631
scratch space, 49–50
screen displays. See displays
screen savers, 242, 246–248
scripted diagnostics, 32
scripts assigning, 108–109
computer and user policies, 106–109
deleting, 108
deployment scripts, 67
DiskPart tool, 414
proxy server settings, 595
Read permission and, 480
types of policies, 106
types of scripts, 106
Windows PE configuration scripts, 38
SCSI support, 343
SD cards (Secure Digital), 415
sealing keys, 380
searching command path order, 333
file association order, 335
for device drivers, 299
indexed file data and, 518
search policy settings, 519
sectors, 454
secure desktop, 133–134
Secure Digital cards (SD), 415
Secure Sockets Layer (SSL), 468
security Action Center, 17–19, 266
Admin Approval Mode, 135
application access tokens, 312
BitLocker, 387–393
disabling services, 281
domain settings, 136
file ownership, 488
file sharing, 473–511
Guest accounts, 156
IEEE 802.11i and, 609
Internet routing policies, 582
local logons, 137–144
policy preferences, 122
principle of least privilege, 483
Public folders, 507–508
remote access, 159–166, 601
Remote Assistance, 160
Remote Desktop, 162–165
scheduled tasks, 634
signed and unsigned applications, 314
stored credentials, 144–149
System And Security troubleshooter, 33
TPM features, 380–387
UAC and elevation, 131–137
user and group accounts, 125–128, 149–158
Web Browsing Safety troubleshooter, 273
Windows logs, 629
Windows Updates, 618
wireless networks, 610–612
WMI control and, 177
security groups, 128
security keys, 615
Security tab (Properties dialog box), 518
security updates, 618
Selective Acknowledgments.
See SACKs (Selective Acknowledgments)
selective startup, 184, 360
selective suspend options, 214
self-healing NTFS, 451
Send To menu, 232
sending information to Microsoft, 266, 276
SendTo folder, 232
SERIAL debugging, 371–372
Serial Line Internet Protocol (SLIP), 602
serial ports, 166, 291, 372
Server Message Block (SMB), 476
servers, 52, 97, 99, 540, 570, 581
service accounts, 486, 489
service packs, 297, 320, 618
services configuring, 278
device error messages, 308
disabling, 189, 281, 361
enabling, 189
event logs, 629
halting devices, 310
loading, 184
LocalSystem account, 127
logon, 280
policy preferences, 115, 119, 282
recovery policies, 264
responsiveness and, 194
restarting and recovery, 281
startup configuration, 280
startup failures, 356
startup process, 352
stopping, starting, or pausing, 279
support services, 276–279
troubleshooting, 353, 637
Services Control Manager, 352, 358
Services for System Management BIOS (SMBIOS), 342
Services policies, 115
Services tool, 170
session keys, 611
Session Manager, 352–353, 357
Set Up A Connection Or Network Wizard, 587–588, 590–591
settings. See policy settings
Setup Information files (INF), 297
setup packages, 52, 319, 330
setup state check, 35
SHA-1 hashing

SHA-1 thumbprints, 165

Share permissions, 474, 478, 495

Shared Folders tool, 169

Shared keys, 610

Shared Printer policies, 115

Shared printers, 115, 292

shares access to, 495

administrative or special, 504

auditing and tracking, 508–511

basic and advanced, 496

Computer Management, 498–500

creating, 495–500

deleting, 501

Group Policy, 500

hidden, 504, 520

mapping, 501

naming, 497

offline use of files, 499

preventing mapped paths to, 517

system shares, 501

troubleshooting, 506–507

UNC paths, 497

upgrading, 501

user sessions with, 505

shell extensions, 517

Shell Object shortcuts, 233

short file names, 324

shortcut menus, 518

shortcuts (interface), 115, 225, 228, 230–234

shortcuts (techniques)

accessing boot options, 341

displaying files by keystroke, 516

firmware shortcuts, 348

hotkeys, 232, 234

policy preferences, 118

updates, 234

Shortcuts policies, 115, 117, 230

shutting down

ACPI power states, 348–351

clearing paging files, 196

device-related errors, 310

hard shutdowns, 647

performance during, 32

script policies, 106–108

troubleshooting, 646

Windows 7 options, 25–27

SIDs (security identifiers), 126, 129, 157, 533

signal strength, 613

signature verification, 182

signed applications, 136, 314

signed device drivers, 298, 307, 640

Simple Network Protocol (SNP), 343

simple volumes, 408, 428, 431–434, 436–438, 443

site policies, 84, 88–90, 92–102

sleep mode

ACPI power states, 348–351

hybrid sleep, 208, 213

passwords, 213

settings, 213

timing, 211

troubleshooting, 636

types of, 208

Windows 7 options, 25–27

slide shows, 211. See also projectors

SLIP (Serial Line Internet Protocol), 602

slow-link mode, 100

slow-link policies, 96

small memory dumps, 202

smart cards

administration of, 391

certificates, 389

dial-up connections, 589

encryption and, 392, 398–399, 405, 601

user accounts, 127

wireless connections, 613

SMB (Server Message Block), 476, 541

SMBIOS (Services for System Management BIOS), 342

SNP (Simple Network Protocol), 343

Socks protocol, 597

software. See applications; installing software

Software Assurance, 4

Software install log diagnosis, 35

Software Quality Management (SQM), 31

Software Restriction policies. See Application Control policies

Solicited Remote Assistance policy, 162

soliciting remote assistance, 104

solutions (Action Center), 17, 266, 275

sorting files by keystroke, 516

programs on menus, 228

sound, 33, 221, 240, 242, 577

source files (SYS), 297

sources in event logs, 630

spanned volumes

creating, 434

Data Incomplete status, 449

deleting, 440

described, 170, 408

dynamic disks, 420

moving disks to new systems and, 446

recovering, 443

shrinking or extending, 436–438

switching between basic and dynamic, 428

special identities, 482–484, 494

special permissions, 486

special shares, 504

speed

local area connections, 564

ReadyBoost devices, 417

startup, 358

wireless devices, 609, 615

SpeedStep, 350

split ImageX command, 46

split WIM files (SWM), 46

spoofing elevation prompts, 314

Spurious Retransmission Time-out Detection feature, 551

SQM (Software Quality Management), 31

SRK (Storage Root Key), 380

SSIDs (network secure identifiers), 615

SSL (Secure Sockets Layer), 468, 597

staging files, 178

Stale Data volume status, 451

standard application mode, 132

standard desktop, 133

standard folder sharing, 474, 478, 494

standard tasks, 632

standard user access tokens, 312

standard user accounts, 20, 131–133, 136

standard user applications, 312

standard user mode, 132

standby performance, 32

Start button, 26

Start menu

customizing, 224–227

pinned items on, 227

rearranging and adding items, 227–230

shortcuts on, 229, 232

starting services, 279

StartMenu folder, 232

startup applications. See startup applications

automatic reboot, 202

booting process, 344
configuring, 200, 360–362
firmware interfaces, 345
modes, 184, 341, 358
policies, 109–111
power states and management, 348
repairing, 646
sequence, 351
services, 280
speeding up, 358
troubleshooting, 184, 353–358, 637–639, 646
types of, 360

Startup And Recovery dialog box, 200–202, 358
Startup applications
adding and removing, 234–235
BCD store entries, 369
disabling, 188, 362
enabling, 188
folder location, 232
shortcuts for, 230–234
specifying for users, 232
Startup folder, 229, 232, 234–235
startup keys, 389, 391, 396, 402, 404
Startup Repair tool (Str), 12, 35, 427, 637–639
static IP addresses, 554–556, 562, 570, 575, 604, 613
Static Root of Trust Measurement, 380
status messages, 598
Stop errors, 202, 339, 358, 647–649
stopping
file sharing, 497
inherited permissions, 491
services, 279
storage devices. See also hard disks; removable media drives
backup devices, 642
CD and DVD devices, 460–464
Computer console, 410
defragmenting, 454–456
Disk Management tool, 411
DiskPart tool, 414
drive letters and paths, 438
encryption, 467–472
extending or shrinking volumes, 436–438
file systems, 429
firmware configuration, 345
formatting, 429, 431
FSUtil tool, 414
hybrid drives, 417
installing and initializing, 425
MBR and GPT, 426
mirrored disks, 444–445
partitions or volumes, 423–425, 431–434
performance, 414–419
quotas, 532–539
spanned volumes, 443
status messages, 447–449
striped volumes, 434
troubleshooting, 447–458
types of, 407
Storage Root Key (SRK), 380
streaming media, 477
subfolders, 97, 466, 480, 485, 487
submenus, 224–225
subnet masks, 554, 566, 579
subnets, 290, 556, 570
SuperFetch utility, 418–419
support. See Automated Help and Support features;
system support tools
support services, list of, 276–279
suspend events, 98
suspend mode, 350
switching, fast user, 23
SWM files (split WIM), 46
symbolic links, 16, 322
Symmetric Network Address Translators feature, 552
Sync Center and synchroni-
zation
automatic synchroniza-
tion, 526–527
background, 100
configuring policies, 96, 100
details, errors, and warn-
ings, 528
disk space settings, 530
encrypting files, 531
full synchronization vs. quick, 100
laptop settings, 576
logging off or on and, 98
managing synchronization, 100, 521
manual synchronization, 525
offline files, 100, 521
permissions for, 480, 486
resolving conflicts, 528
suspend events and, 98
Sync partnerships, 524–525
SYS files (source files), 297
System abstraction layer (SAL), 342
System And Security troubleshoot-
er, 33
system applications, 315
system BCD stores, 364
system boot log diagnosis
test, 35
system cache, 414
system checkpoints, 204, 639
system components, 629
System Configuration, 179, 184–189, 360–362
System console, 170–173
System Data Sources policies, 114
system disk test, 34
system environment variables, 198
system files
displaying, 513
ciphering, 469
repairing, 646
signature verification, 182
Stop errors and, 649
System Restore and, 207
troubleshooting startup, 637–639
system hive, 310
System Image Recovery tool, 12
system images, 12, 642, 646
System Information, 175
system partitions, 11, 424, 442
System Properties dialog box, 172, 190, 203–207, 641
System Protection tab (System Properties dialog box), 203–207, 641
System Restore tool
collection, 203–207
described, 12, 179
enabling or disabling, 95
normal or safe mode
usage, 640
policy settings, 95
preinstallation restore
points, 319
recovering systems, 641
restore points, 639–641
troubleshooting, 641
system root, 375
system services, 352
system shares, 501
system support tools
Computer Management, 168
Disk Cleanup, 180
File Signature Verifica-
tion, 182
list of, 179
system support tools, continued
Performance Information And Tools, 173–174
System Configuration, 184–190
System Console, 170–173
System Information, 175
WMI Control, 176–178
system tray notifications, 237
System Variable policies, 114
system volumes, 394, 401–403, 406, 420, 424, 439, 457
SystemDrive environmental variable, 16
SYSVOL share, 501
tablet PCs. See laptops and Tablet PCs
tampering. See hacking, prevention
target OS test, 34
target paths, 50, 233
Targeting Editor, 123
Task Manager, 173, 329, 647
task priority services, 342
Task Scheduler, 32, 169, 631, 633
task scheduling

event logs, 630
functions and customizing, 631–635
managing tasks, 633
policy preferences, 115, 119
Task Scheduler and Schtasks, 631
troubleshooting, 635
types of tasks, 632
taskbar, 236–239
TCG (Trusted Computing Group), 380
TCP Extended Statistics feature, 551
TCP ports, 476
TCP/IP configuration
default configuration, 602
filtering architecture, 551
installing components, 549–554
local area connections, 554–563
mobile computing settings, 577
Network And Sharing Center, 546
network discovery, 544
Network Explorer, 545
Network Map, 548
network shares and, 506
Next Generation TCP/IP, 550–552
policies, 103
troubleshooting, 567–573
Windows 7 features and tools, 543
wireless networks, 613
TCP/IP NetBIOS Helper, 128
TCP/IP Printer policies, 115
technical support. See Automated Help and Support features
television, 507
templates. See ADMX files (administrative template files)
Temporal Key Integrity Protocol (TKIP), 612
temporary boot sequence changes, 378
temporary files, 180, 462, 530
Teredo, 626
Terminal Services, 165
test-code signing certificates, 373
testing local area connections, 567–573
text prompts, 221
text readability adjustments, 252
themes, 17, 240–242
Themes folder, 242
third-party drivers, 51
throughput, 388, 417, 551
thumbnails, 181, 514, 518
ticket times, 104
time limits
invitations, 104, 160, 627
scripts, 106
time synchronization, 278
Time to Live (TTL), 572
time zones, 132
timetouts, 186, 359, 364, 378
timer wakeup settings, 213
times (synchronization), 526
TKIP (Temporal Key Integrity Protocol), 612
TLS (Transport Layer Security) encryption, 468
tone dialing, 585–586
toolbars, 239
TPM (Trusted Platform Module Services)
authentication methods, 396
BitLocker and, 388, 394
functions and implementation, 380–387
policies, 392
saving backup information, 393
tools (tpm.msc), 382
TPM Platform Validation profiles, 392
trace logging, 84
tracking file sharing, 508–511
Transactionable NTFS, 451
transfer rates (removable media), 458
transmission frequency (wireless), 609
transparency, 242, 250
Transport Layer Security (TLS) encryption, 468
triggers, 632, 635
Triple DES encryption, 468
troubleshooters, 272–274
troubleshooting
Action Center, 17–19, 266
Aero performance, 252
backing up and recovering, 206, 443, 636, 642–645
BitLocker, 404–406
Bluetooth, 289
boot process, 187, 360, 457
broadband connections, 606
built-in tools for, 28, 30–35, 272–274
burning files, 463
compatibility issues, 325–327
device drivers, 304
dial-up connections, 605
disk drives, 447–458
disk errors, 451–454
display resolution and, 253
displays and video adapters, 260
drive letters or paths, 439
event logs and, 629
file sharing, 506–507
Group Policy, 84, 274–276
hibernation, 209, 636
installation, 15
Microsoft Knowledge Base and, 630
mirrored disks, 445, 457
network connections, 29, 290, 551, 567–573
partitions, 427
permissions, 493
power issue reports, 208
previous versions of files, 206
printer connections, 294
problem reporting, 18
Problem Steps Recorder, 159
ReadyBoost, 415
Remote Assistance, 160–162, 624–629
services, 189
shutdown, 646
sleep mode, 26, 209, 636
startup, 353–358, 637–639, 646
Stop errors, 647–649
SuperFetch, 419
system diagnostic reports, 174
System Restore, 639–641
task scheduling, 635
TPM, 382
troubleshooting tools, 33–35
updates, 623
user-specific settings, 272
volume status messages, 449–451
VPN connections, 607
Windows 7 errors, 629–630
Windows PE and, 38
wireless connections, 614, 616
wireless devices, 289
Troubleshooting window tools, 33–35, 273
trusted applications, 314
Trusted Computing Group (TCG), 380
trusted peers, 619
Trusted Platform Module Services. See TPM (Trusted Platform Module Services)
TTL (Time to Live), 572

U
UAC (User Account Control) access tokens, 312
Admin Approval Mode, 133–137
alerts, 18
elevating privileges, 313
homegroups, workgroups, and domains, 20–22
installation detection, 317
legacy applications and, 313
managing user accounts, 126
modifying settings, 19
optimizing, 133–137
passwords, 140
security settings, 135
status, 266
UAC-compliant applications, 312
virtualization of write failures, 317
UDF (Universal Disc Format), 55, 461, 464
UDP ports, 476, 506
UEFI (Unified Extensible Firmware Interface) 64-bit architecture, 8
boot processes and, 340
functions and services, 342–344
recovery partitions and, 62
startup process, 345
UEFI standard, 340
UIAccess programs, 136
unallocated space, 428, 436
Unattend.xml file, 40–41, 65
unattended answer files, 10, 65
unavailable files, ghosting, 521
UNC (Universal Naming Convention) paths, 97, 497
unenforced disk quotas, 532
Unified Extensible Firmware Interface. See UEFI (Unified Extensible Firmware Interface)
uninstalling applications, 330
device drivers, 305
devices, 296
incomplete uninstalls, 319
System Restore and, 640
Universal Disc Format (UDF). See UDF (Universal Disc Format)
Universal Naming Convention (UNC), 97, 497
UNIX application support, 4
UNIX servers, 602
Unknown volume status, 451
unlocked drives, 397
unlocking computers, 405, 526
unmanaged settings. See policy preferences
unmounting base images, 53
unpinning items, 228
unplugging components, 26
Unreadable drive status, 443
Unrecognized disk status, 449
unsealing keys, 381
unsigned applications, 314
unsigned device drivers, 298, 640
unverified applications, 314
Update Driver Software Wizard, 256, 299–300
update sequence number (USN) journaling, 452
upgrading Windows, 5, 10, 13
UPnP (Remote Assistance requirements), 626
URL shortcuts, 232–234
USB card readers, 424, 448–449
USB debugging, 371, 373
USB devices
backup devices, 642
BitLocker, 387, 389, 399, 406
booting and, 351, 354
decrypting, 406
dynamic disks and, 423
ejecting, 411
encryption, 389
file systems and formatting, 458
hub devices, 458
installing, 286–288
network adapters, 549
password reset disks, 24, 142
printers, 291
ReadyBoost, 414–417
recovery keys on, 398
selective suspend options, 214
UEFI support, 343
unplugging, 26
versions of, 458
Windows PE bootable drives, 55
Windows RE bootable drives, 59
wireless adapters, 608, 612
firmware, 340, 346
hiding updates, 623
installation choices, 619
marking in-use files, 264
modules and, 65
offline files, 522, 525–529
policy settings for, 621–622
prioritizing updates, 618
removing updates after installation, 623
restore points and, 288, 640
roll-ups, 618
services for, 278
shares, 501
shortcuts for, 234
troubleshooting tools, 274
trusted peers and, 619
types of updates, 618, 620
update servers, 622
user account privileges and, 132
video drivers, 255
Web compatibility lists and, 620
Windows Update, 617–619
upgrading Windows, 5, 10, 13
USB flash devices
backup devices, 642
BitLocker, 387, 389
boot order, 354
ejecting, 411
password reset disks, 24, 142
ReadyBoost, 414–417
recovery keys on, 398
Windows PE bootable drives, 55
Windows RE bootable drives, 59
USB hub devices, 458
User Account Control. See UAC (User Account Control)
user accounts
adding, 137
changing type, 139
default accounts, 127
deleting, 158
enabling or disabling, 155
fast user switching, 23
group accounts, 128–130
Guest accounts, 156
local user accounts, 126–128
logging on, 22
logon names, 126
new accounts, 150
password hints, 140
passwords, 23–25, 127, 140
remote access, 159–166
removing and denying access, 144
renaming, 157
scheduled tasks and, 634
UAC and, 131–133
User Accounts utility, 140
user certificates, 471
User Data Sources policies, 114
user environment variables, 198, 358
user names, 597, 605–606
user processes, 418–419
user profiles, 192, 468
User Variable policies, 114
user-mode exceptions, 373
UserName environmental variable, 16
users. See also user accounts
Add New User wizard, 139
adding to groups, 154
administrative policies for, 91
basic permissions, 478–494
credentials, 144–149
customized Help and Support features, 270
disk quotas, 532, 535
event log entries, 630
file ownership, 489
file sharing, 475
Group Policy settings, 89–90
installing applications for, 321
local user accounts, 20
logon and startup policies, 109–111
network policies, 102–103
new accounts, 150
offline file policies, 95–102
permissions list, 481
personal folders, 15
personal libraries, 16
policy preferences, 113–115, 120
policy settings, 84
profiles, 192, 468
remote access, 159–166
Remote Desktop list, 163
script assignments, 109
script policies, 106–109
special permissions, 486
update installation, 620
Users folder, 235
Users group, 130, 475
Users identity, 483
user-specific local Group Policy objects, 85
USN journaling, 452
valid signatures, 449
validated executables, 136
values (BCD store), 370–376
variable-length subnetting, 556
variables, 198–200, 500
vaults, 144, 147–148
VBScript, 106
verbose output, 187, 364
verified applications, 314
versions of files, 521, 529, 636
VES A (Video Electronics Standards Association), 373
VGA displays, 257, 376
VGA settings, 186, 376
VHD files, 6, 167. See also virtual machines
video chipsets, 345
Video Electronics Standards Association (VESA), 373
video settings. See VGA displays; VGA settings
video settings. See displays
videos, 212, 477, 507
viewing. See displaying
Viiv-based computers, 350
virtual address space, 374
virtual hard disk files (VHD), 6, 167
virtual hard drives, 167
virtual machines, 4–5
virtual memory, 32, 194–196
virtual private networks. See VPN connections
virtual tunneling, 581, 602
virtual volumes, 400
virtualization, 313, 317, 324
virus programs, 18, 266
viruses, 451
visible scripts, 107
Visual Basic scripts, 106
visual effects, 173, 192–193
volume (sound), 577
volume content check, 34
volume licensing keys, 4, 19
volumes. See also partitions
activation, 67
active volumes, 423, 426
basic disks, 420
BitLocker, 387
boot volumes, 424
crash dump volumes, 425
deleting, 428, 440
Disk Management, 411
disk quotas, 532
disk types, 422
drive letters and drive paths, 438
dynamic disks and, 408
extending, 411, 436–438
formatting, 433, 438
labels, 433, 440
mirrored disks, 445
page file volumes, 425
recovering, 443
shrinking, 436–438
simple volumes, 431–434
size of, 431
spanned volumes, 434
status messages, 449–451
striped volumes, 434
switching between basic and dynamic, 428
system volumes, 424
viewing list of, 412
volume images, 43–47
VPN Connection policies, 115
VPN connections
automatic or manual connections, 593
creating, 591
described, 581
DirectAccess, 29
establishing, 607
identity validation, 601
logon configuration, 597
network protocols and components, 602–604
policy preferences, 115
proxy settings, 594–597
troubleshooting, 607
user account privileges, 132
Windows Firewall and, 604
clean installations vs. upgrades, 10
configuration. See configuration
diagnostic and troubleshooting tools, 28,
30–32, 264
editions, 2–5, 171
Group Policy settings, 90
hardware independence,
27
hardware requirements,
12
installing, 12–15
modularization of, 28
networking tools, 543
power plans and, 25–27
preparing for installation,
10–12
reinstalling, 646
Remote Desktop sessions,
162
troubleshooting errors,
629–630
version information, 171
Windows Explorer set-
tings and, 519
Windows 7 Basic theme, 17,
251
Windows 7 Enterprise, 2–5,
387, 582, 642
Windows 7 for Itanium-Based
Systems, 5
Windows 7 Home Basic, 2–5,
620
Windows 7 Home Premium,
2–5
Windows 7 Professional, 2–5,
620, 642
Windows 7 Starter, 2–5
Windows 7 Ultimate, 2–5, 387,
620, 642
Windows Activation Wizard, 19
Windows Aero. See Aero user
interface
Windows AIK, 39
Windows Anytime Upgrade, 5
Windows Application Compat-
ibility Toolkit (ACT), 315, 321
Windows Authentication,
601, 603
Windows Automated Installation
Kit, 39, 66
Windows Backup, 18, 266
Windows Boot Loader
BCD store entries, 362,
364–366, 372–373
boot options, 185–187
configuring startup, 200
functions of, 341
safe mode and other
options, 637
settings, 366
startup failures, 356
startup process, 344
Windows 7 booting, 27
Windows PE and, 40
Windows Boot Sector Application,
362
Windows BranchCache,
540–542
Windows Classic theme, 17
Windows Collaboration, 519
Windows credentials, 145
Windows Defender, 632
Windows Deployment Ser-
dvices, 10, 52, 57, 60
Windows Easy Transfer, 10
Windows Experience Index
rating, 172
Windows Explorer, 352, 496,
513–519, 568
Windows Fax And Scan, 4
Windows Filtering Platform
feature, 551
Windows Firewall. See also
firewalls
File And Printer Sharing
exception, 476
multiple network fea-
tures, 28
network connections, 604
network discovery and,
291, 544
policies, 102
Remote Assistance fea-
ture and, 624, 626
Remote Desktop feature
and, 164–165
Windows Hardware Quality
Lab, 298
Windows Images files. See
WIM (Windows Imaging
Format)
Windows Installer Cleanup
utility, 331
Windows Internet Naming
Service. See WINS (Windows
Internet Naming Service)
Windows Legacy OS Loader.
See Ntldr (Windows Legacy
OS Loader)
Windows Logon Manager,
352, 358
Windows Management Instru-
mentation (WMI), 52, 170,
176–178, 278
Windows Media Center, 4
Windows Media troubleshooter, 273
Windows Memory Diagnostics tool, 12, 35, 365, 370, 372–373, 646
Windows Memory Tester entry, 370
Windows Messenger, 162
Windows Network Diagnostics, 29, 548, 567
Windows OEM Preinstallation Kit, 39
Windows OPK, 39
Windows OS Loader, 372–376
Windows PE (Windows Preinstallation Environment) adding applications to, 51 bootable flash drives, 55 booting from hard disks, 56 build environments, 41–47 capturing builds, 53 command-line tools, 38 component and subsystem support, 39 configuring, 40 custom builds, 47–55 disabling booting to, 376 functions of, 38–40 installing, 41 memory requirements, 50 packages in, 52 requirements, 39 restarts, 40 Windows Deployment Services, 57 Windows PowerShell. See PowerShell 2.0
Windows Preinstallation Environment. See Windows PE (Windows Preinstallation Environment)
Windows prompt, booting to, 186
Windows RE (Windows Recovery Environment) functions and customization, 58–65 installation package, 52 partitions for, 391, 645 relocating during BitLocker installation, 401 tools in, 12
Windows ReadyBoost, 414–417
Windows ReadyDrive, 417
Windows Recovery Environment. See Windows RE (Windows Recovery Environment)
Windows Remote Assistance wizard, 625, 628 Windows Resume Loader, 362, 369, 372–373, 636
Windows Script Host (WSH), 52, 106, 631
Windows scripts, 106
Windows Server 2003, 41, 100
Windows Server 2008, 318, 340, 540, 582
Windows Settings policies, 114
Windows Setup, 11, 319, 629
Windows SuperFetch, 418–419
Windows System Image Manager, 10, 41, 66
Windows Update alerts, 18 checking for updates, 623 configuring updates, 617–619 hiding updates, 623 history and installation status, 623 notifications, 266 prioritizing updates, 618 removing automatic updates, 623 restoring declined updates, 624
Windows Upgrade, 180
Windows vault, 146–148
Windows Vista, 10, 162, 318, 340, 367, 519
Windows Vista/Windows 7 applications, 314
Windows XP, 10, 41, 99–100, 131, 315, 318
Windows.old folder, 13–14
WINS (Windows Internet Naming Service), 543, 561–563, 566, 568, 570, 580
Wired Equivalent Privacy. See WEP (Wired Equivalent Privacy)
Wired for Management Baseline (WMB), 342
SSIDs, 615 transmission standards, 609 troubleshooting, 614, 616 Windows 7 edition and, 4
Wireless Protected Setup (WPS), 289
Wise Install, 319, 330
WMB (Wired for Management Baseline), 342
WMI (Windows Management Instrumentation), 52, 176–178, 278
WMI Control access, 170
work networks, 544, 583, 588–589
workgroups accounts and, 130 computer membership in, 125 creating shares for, 495–500 file sharing options, 475 homegroups vs., 20 information about, 171 local user accounts in, 137 logging on, 22 passwords, 140 recovery policies, 470 stored credentials, 145 UAC and, 20 working directories, 234 workstations. See computers WOW (Windows x64 emulation layer), 9, 40
WPA (Wi-Fi Protected Access), 611, 613
WPA2 (Wi-Fi Protected Access Version 2), 610–611, 613
wpeinit tool, 38
WPS (Wireless Protected Setup), 289
wrapping (TPM), 380 write access, 392–393, 480
WSH (Windows Script Host), 52, 106, 631
WS-Management protocol, 278
x64 architecture, 8, 342, 410
x86 architecture, 8, 11, 340, 410

X
WILLIAM R. STANEK (www.williamstanek.com/) has more than 20 years of hands-on experience with advanced computer programming and software development. He is a leading technology expert, an award-winning author, and a pretty-darn-good instructional trainer. Over the years, his practical advice has helped millions of programmers, developers, and network engineers all over the world. He has written more than 100 books. His recent books include Active Directory Administrator's Pocket Consultant, Windows Group Policy Administrator's Pocket Consultant, Windows PowerShell 2.0 Administrator's Pocket Consultant, and Windows Server 2008 Inside Out (all from Microsoft Press).

William has been involved in the commercial Internet community since 1991. His core business and technology experience comes from more than 11 years of military service. He has substantial experience in developing server technology, encryption, and Internet solutions. He has written many technical white papers and training courses on a wide variety of topics. He frequently serves as a subject matter expert and consultant.

William has a BS in computer science, magna cum laude, and an MS with distinction in information systems. He is proud to have served in the Persian Gulf War as a combat crewmember on an electronic warfare aircraft. He flew on numerous combat missions into Iraq and was awarded nine medals for his wartime service, including one of the United States of America's highest flying honors, the Air Force Distinguished Flying Cross. Currently, he resides in the Pacific Northwest with his wife and children.

Follow William on Twitter at WilliamStanek.