Microsoft

MCITP EXAM
70-685

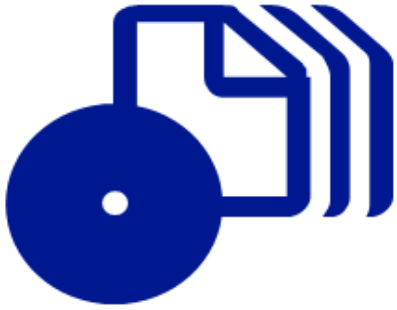
Windows® 7 Enterprise Desktop Support Technician

Tony Northrup
J.C. Mackin

SELF-PACED

Training Kit

How to access your CD files



The print edition of this book includes a CD. To access the CD files, go to http://aka.ms/627093/files, and look for the Downloads tab.

Note: Use a desktop web browser, as files may not be accessible from all ereader devices.

Questions? Please contact: mspinput@microsoft.com

Microsoft Press

Exam 70-685: Pro: Windows 7, Enterprise Desktop Support Technician

OBJECTIVE	LOCATION IN BOOK
IDENTIFYING CAUSE OF AND RESOLVING DESKTOP APPLICATION ISSUES	
Identify and resolve new software installation issues.	Chapter 9, Lesson 1
Identify and resolve software configuration issues.	Chapter 9, Lesson 2
Identify cause of and resolve software failure issues.	Chapter 9, Lesson 1
IDENTIFYING CAUSE OF AND RESOLVING NETWORKING ISSUES	
Identify and resolve logon issues.	Chapter 4, Lesson 1
Identify and resolve network connectivity issues.	Chapter 2, Lesson 1
Identify and resolve names resolution issues.	Chapter 2, Lesson 2
Identify and resolve network printer issues.	Chapter 3, Lesson 1
MANAGING AND MAINTAINING SYSTEMS THAT RUN WINDOWS 7 CLIENT	
Identify and resolve performance issues.	Chapter 8, Lessons 1 and 2
Identify and resolve hardware failure issues.	Chapter 1, Lessons 1 and 2
SUPPORTING MOBILE USERS	
Identify and resolve wireless connectivity issues.	Chapter 2, Lesson 3
Identify and resolve remote access issues.	Chapter 6, Lessons 1 and 2
IDENTIFYING CAUSE OF AND RESOLVING SECURITY ISSUES	
Identify and resolve Windows Internet Explorer security issues.	Chapter 4, Lesson 2
Identify and resolve issues due to malicious software.	Chapter 5, Lesson 1
Identify and resolve encryption issues.	Chapter 4, Lesson 3
Identify and resolve software update issues.	Chapter 7, Lesson 1

Exam Objectives The exam objectives listed here are current as of this book's publication date. Exam objectives are subject to change at any time without prior notice and at Microsoft's sole discretion. Please visit the Microsoft Learning Web site for the most current listing of exam objectives: *http://www.microsoft.com/learning/en/us/Exam.aspx?ID=70-685*.

Microsoft®

MCITP Self-Paced Training Kit (Exam 70-685): Windows® 7 Enterprise Desktop Support Technician

Tony Northrup
J.C. Mackin

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Library of Congress Control Number: 2010921440

ISBN: 978-0-7356-2709-3

Printed and bound in the United States of America.

5 6 7 8 9 10 11 12 13 QGT 7 6 5 4 3 2

Distributed in Canada by H.B. Fenn and Company Ltd.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at www.microsoft.com/mspress. Send comments to tkinput@microsoft.com.

Acquisitions Editors: Ken Jones and Martin DelRe
Developmental Editor: Maria Gargiulo
Project Editors: Denise Bankaitis and Carol Vu
Editorial Production: Christian Holdener, S4Carlisle Publishing Services
Technical Reviewer: Bob Dean; Technical Review services provided by Content Master, a member of CM Group, Ltd.
Cover: Tom Draper Design

Body Part No. X16-75082

[2012-02-10]

For my Gramma June.

—Tony Northrup

To my nieces Cassidy and Mckenna, and to my nephew Ralph.

—J.C. Mackin

Contents

Acknowledgments

This book was put together by a team of respected professionals, and we, the authors, would like to thank them all for the great job they did. At Microsoft, Ken Jones and Martin DelRe worked out our contracts, and Maria Gargiulo was our developmental editor. Denise Bankaitis, Carol Vu, and Christian Holdener were the project editors, coordinating the many other people who worked on the book. Among those, Susan McClung was our copy editor, who was responsible for making sure the book is readable and consistent, and Lindsey Valich, Paul Connelly, and Nicole Schlutt provided additional editorial proofreading.

Bob Dean and Bob Hogan provided a technical review to help make the book as accurate as possible.

Tony Northrup would also like to thank his friends for helping him relax after long days of writing, especially Eddie and Christine Mercado (for the dinners), Jose and Lucy Mercado (*por el arroz y los frijoles*), Brian and Melissa Rheaume (for the drinks), Diane Glenn (for the cake), Jose Gonzalez (for the laughs), and Madelyn Knowles (for the patience).

J.C. Mackin would like to thank all his friends and family for their support and encouragement.

It makes a huge difference when you consider the people you work with to be friends. Having a great team not only improves the quality of the book, it makes it a more enjoyable experience. Writing this book was our most enjoyable project yet, and we hope we get the chance to work with everyone again in the future.

Introduction

This training kit is designed for IT support personnel who support Windows 7 at the Tier 1 or Tier 2 level in a wide range of environments and who plan to take the Microsoft Certified Information Technology Professional (MCITP) exam 70-685. We assume that before you begin using this kit you have a solid foundation-level understanding of Microsoft Windows client operating systems and common Internet technologies. The Preparation Guide for Exam 70-685 is available at *http://www.microsoft.com/learning/en/us/exam.aspx?ID=70-685*.

By using this training kit, you will learn how to do the following:

- Identify cause of and resolve desktop application issues
- Identify cause of and resolve networking issues
- Manage and maintain systems that run Windows 7 client
- Support mobile users
- Identify cause of and resolve security issues

Refer to the objective mapping page in the front of this book to see where in the book each exam objective is covered.

Hardware Requirements

You can complete almost all the practice exercises in this book, other than those in Lesson 3 of Chapter 2 (which requires a wireless network adapter), using virtual machines rather than server hardware. The minimum and recommended hardware requirements for Windows 7 are listed in Table I-1.

TABLE I-1 Windows 7 Minimum Hardware Requirements

HARDWARE COMPONENT	MINIMUM REQUIREMENTS	RECOMMENDED
Processor	1 GHz (x86), 1.4 GHz (x64)	2 GHz or faster
RAM	1 GB	2 GB or greater
Disk Space	16 GB	40 GB or greater

You also need to be able to install Windows Server 2008 R2, which is 64-bit. Therefore, you must use hardware or virtual machine software that supports 64-bit operating systems. As of the time of this writing, Microsoft Windows Virtual PC and Microsoft Virtual Server 2005 do not

support 64-bit guests. Sun VirtualBox does support 64-bit guests and can be downloaded for free from *http://www.virtualbox.org*. Alternatively, you can use the Hyper-V feature of Windows Server 2008 R2, as described at *http://www.microsoft.com/windowsserver2008/en/us/hyperv-main.aspx*.

If you intend to implement several virtual machines on the same computer (recommended), a higher specification will enhance your user experience. In particular, a computer with 4 GB RAM and 60 GB free disk space can host all the virtual machines specified for all the practices in this book.

Practice Setup Instructions

The practice exercises in this training kit require a minimum of three computers or virtual machines, as follows:

- One server running Windows Server 2008 R2 Standard and configured as a domain controller. Name the server DC1. Name the domain nwtraders.msft.
- Two computers running Windows 7 and configured as domain members. Name the computers CLIENT1 and CLIENT2.

When installing the operating systems, accept all default settings except for the computer names listed above.

Using the Companion CD

The companion CD included with this training kit contains the following:

- **Practice tests** You can reinforce your understanding of how to support Windows 7 by using electronic practice tests that you customize to meet your needs from the pool of Lesson Review questions in this book, or you can practice for the 70-685 certification exam by using tests created from a pool of about 200 realistic exam questions, which give you many practice exams to ensure that you are prepared.
- Practice exercises Some chapters in this book include scripts that configure your test computers for the practice exercises at the end of every lesson. To install the scripts on your hard disk, run Setup.exe in the Practice Exercises folder on the companion CD. The default installation folder is \My Documents\Microsoft Press\MCITP Self-Paced Training Kit Exam 70-685.
- An eBook An electronic version (eBook) of this book is included for times when you do not want to carry the printed book with you. The eBook is in Portable Document Format (PDF), and you can view it by using Adobe Acrobat or Adobe Reader.

Digital Content for Digital Book Readers: If you bought a digital-only edition of this book, you can enjoy select content from the print edition's companion CD.
Visit **http://www.microsoftpressstore.com/title/9780735627093** to get your downloadable content. This content is always up-to-date and available to all readers.

System Requirements for the Companion CD

To use the companion CD-ROM, you need a computer running Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003, or Windows XP. The computer must meet the following minimum requirements:

- 1 GHz 32-bit (x86) or 64-bit (x64) processor
- 1 GB of system memory
- A hard disk partition with at least 1 GB of available space
- A monitor capable of at least 800 × 600 display resolution
- A keyboard
- A mouse or other pointing device
- An optical drive capable of reading CD-ROMs

The computer must also have the following software:

- A Web browser such as Microsoft Internet Explorer version 6 or later
- An application that can display PDF files, such as Adobe Acrobat Reader, which can be downloaded at *http://www.adobe.com/reader*

These requirements support use of the companion CD-ROM. To perform the practice exercises in this training kit, you will require additional hardware or software, as detailed previously.

How to Install the Practice Tests

To install the practice test software from the companion CD to your hard disk, perform the following steps:

1. Insert the companion CD into your CD drive and accept the license agreement. A CD menu appears.

> ***NOTE*** **IF THE CD MENU DOES NOT APPEAR**
>
> If the CD menu or the license agreement does not appear, AutoRun might be disabled on your computer. Refer to the Readme.txt file on the CD for alternate installation instructions.

2. Click Practice Tests and follow the instructions on the screen.

How to Use the Practice Tests

To start the practice test software, perform these steps:

1. Click Start, click All Programs, and then select Microsoft Press Training Kit Exam Prep.

   A window appears that shows all the Microsoft Press training kit exam prep suites installed on your computer.

2. Double-click the lesson review or practice test you want to use.

> ***NOTE*** **LESSON REVIEWS VERSUS PRACTICE TESTS**
>
> **Select (70-685) Windows 7, Enterprise Desktop Support Technician Lesson Review to use the questions from the "Lesson Review" sections of this book. Select Windows 7, Enterprise Desktop Support Technician Practice Test to use a pool of more than 200 questions (per exam), similar to those that appear on the 70-685 certification exam.**

Lesson Review Options

When you start a lesson review, the Custom Mode dialog box appears so that you can configure your test. You can click OK to accept the defaults, or you can customize the number of questions you want, how the practice test software works, which exam objectives you want the questions to relate to, and whether you want your lesson review to be timed. If you are retaking a test, you can select whether you want to see all the questions again or only the questions you missed or did not answer.

After you click OK, your lesson review starts as follows:

- To take the test, answer the questions and use the Next and Previous buttons to move from question to question.
- After you answer a question, if you want to see which answers are correct—along with an explanation of each correct answer—click Explanation.
- If you prefer to wait until the end of the test to see how you did, answer all the questions and then click Score Test. You will see a summary of the exam objectives you chose and the percentage of questions you got right, both overall and per objective. You can print a copy of your test, review your answers, or retake the test.

Practice Test Options

When you start a practice test, you choose whether to take the test in Certification Mode, Study Mode, or Custom Mode:

- **Certification Mode** Closely resembles the experience of taking a certification exam. The test has a set number of questions. It is timed, and you cannot pause and restart the timer.

- **Study Mode** Creates an untimed test, during which you can review the correct answers and the explanations after you answer each question.
- Custom Mode Gives you full control over the test options so that you can customize them as you like.

In all modes, the user interface when you are taking the test is basically the same but with different options enabled or disabled depending on the mode. The main options are discussed in the previous section, "Lesson Review Options."

When you review your answer to a practice test question, a "References" section is provided that lists where in the training kit you can find the information that relates to that question and provides links to other sources of information. After you click Test Results to score your entire practice test, you can click the Learning Plan tab to see a list of references for every objective.

How to Uninstall the Practice Tests

To uninstall the practice test software for a training kit, use the Uninstall A Program option in Windows Control Panel.

Microsoft Certified Professional Program

Microsoft certifications provide the best method for proving your command of current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies. Computer professionals who become Microsoft certified are recognized as experts and are sought after industry-wide. Certification brings a variety of benefits to the individual and to employers and organizations.

MORE INFO **ALL THE MICROSOFT CERTIFICATIONS**

For a full list of Microsoft certifications, go to *http://www.microsoft.com/learning/mcp/default.asp*.

Support for This Book

Every effort has been made to ensure the accuracy of this book and the contents of the companion CD. As corrections or changes are discovered, they will be added to a Microsoft Knowledge Base article accessible via the Microsoft Help and Support site. Microsoft Press provides support for books, including instructions for finding Knowledge Base articles, at the following Web site:

http://www.microsoft.com/learning/support/books/

If you have questions regarding the book that are not answered by visiting the site above or viewing a Knowledge Base article, send them to Microsoft Press via e-mail to *tkinput@microsoft.com*.

Please note that Microsoft software product support is not offered through these addresses.

We Want to Hear from You

We welcome your feedback about this book. Please share your comments and ideas via the following short survey:

http://www.microsoft.com/learning/booksurvey

Your participation will help Microsoft Press create books that better meet your needs and your standards.

NOTE **CONNECT WITH MICROSOFT PRESS**

We hope that you will give us detailed feedback via our survey. If you have questions about our publishing program, upcoming titles, or Microsoft Press in general, we encourage you to interact with us via Twitter at *http://twitter.com/MicrosoftPress*. For support issues, use only the e-mail address shown above.

CHAPTER 5

Protecting Client Systems

Any computer that is connected to the Internet faces a barrage of network-based threats in the form of malicious software attacks. These threats are growing in number and sophistication every year, and as an enterprise support technician, you are responsible for protecting client systems from these evolving dangers.

As part of your company's broad defense strategy, you need to know how to configure in Windows 7 the features whose purpose is to protect your clients. Specifically, you need to know how to minimize the risk of damage from malware by implementing User Account Control (UAC) at an appropriate level, by using Windows Defender, and by removing unwanted software if it is discovered.

Exam objective in this chapter:

- Identify and resolve issues due to malicious software.

Lesson in this chapter:

Before You Begin

To perform the exercises in this chapter, you need:

- A domain controller running Windows Server 2008 R2
- A client computer running Windows 7 that is a member of the same domain

REAL WORLD

J.C. Mackin

I often hear people repeating a number of misconceptions about viruses and other malware, and I'm convinced that these misconceptions have lulled users and administrators into a false sense of security about the dangers their systems face. Often these misconceptions are based on an accurate understanding of what *was* the state of malware threats about 10 years ago. But the nature of these threats has evolved significantly, and it continues to evolve. So in the interest of learning how best to defend ourselves today, let's deal with the most common of these misconceptions.

- **"As long as you keep Windows updated, you're fine."**

  It's certainly true that you need to keep Microsoft Windows updated, but you need to keep *all* your software updated. Security holes can be found in applications as easily as they can be found in operating systems, and the security holes in many of these can be exploited to completely compromise a system. Microsoft Office applications in particular are often targeted. Remember that your systems are not safe from exploits if you are keeping only Windows updated.

- **"As long as you aren't tricked into opening anything, you're fine."**

  A long time ago, it was true that malicious software needed user assistance to be installed on a system. Now, the situation is completely different. Merely browsing to the wrong site, for example, can lead to a secret drive-by download of malicious software. Even worse, some of the most harmful attacks come from Internet worms, which need no user involvement whatsoever. It is still essential for users to avoid opening unknown software, but this preventative measure alone is not enough to keep your systems safe from infection.

- **"As long as you keep your antivirus software up to date and scan daily, you're fine."**

  This might be the most common of all misconceptions regarding malware. While it's true that a robust anti-malware solution is one of the essential pillars of a sound client protection strategy, the sad truth is that such software has its limitations. Malware developers who are serious about exploiting computers naturally design their programs in a way that avoids detection by antivirus solutions. For example, a rootkit is a relatively new type of malware that—so far—few anti-malware applications have had good success in detecting. But even more familiar types of malware can be designed to evade detection. As a result, when your antivirus software fails to detect malware on a system, you should know that the system still could very easily be infected.

These three misconceptions all have a common thread running through them: the belief that you can protect your systems by adopting a small number of well-known defenses against malware. In truth, adequately protecting client systems requires your company to adopt a wide array of strategies that include effective software updates, antivirus software, user education, firewalls, and most important of all, effective management of these and other security features.

Lesson 1: Resolving Malware Issues

The number of new malware applications being released today actually exceeds that of new legitimate applications. As an enterprise support technician, you need to adequately protect your clients from these mounting threats and know how to handle malware infections once they are discovered.

Windows 7 includes two features that assist you in this fight against malware. User Account Control (UAC) helps prevent programs from secretly altering protected areas of the operating system, and Windows Defender scans your system for spyware and offers to remove any unwanted software that is detected.

Though you will need to use additional applications such as Microsoft Forefront and a managed anti-malware solution to protect your network, understanding how to use and configure these built-in features of Windows 7 represents part of the essential skill set you need on your job.

After this lesson, you will be able to:

- Configure User Account Control (UAC) to display notifications in a way that suits the needs of your organization.
- Configure Windows Defender settings.
- Detect and remove some malware manually in case your anti-malware applications fail.

Estimated lesson time: 30 minutes

Understanding Malware

Malware is an umbrella term for many different types of unwanted software. It's important to understand the nature of these different threats, but it's also important to recognize that many malware applications blend features from more than one of these malware types. The following list discusses the most common types of malware:

- **Virus** A *virus* is a self-replicating program that can install itself on a target computer. Viruses do not propagate over networks automatically; they need to be spread through e-mail or another means. Once installed, viruses usually alter, damage, or compromise a system in some way.
- **Worm** A *worm* is a self-replicating program that can spread automatically over a network without any help from a user or a program such as an e-mail client or Web browser. Worms vary greatly in the potential damage they can cause. Some worms simply replicate and do little other than consume network bandwidth. Others can be used to compromise a system completely.

- **Trojan horse** A Trojan horse is a program that is presented to users as a desirable application but that is intentionally written to harm a system. Unlike viruses and worms, Trojan horses do not copy themselves automatically or install themselves automatically; they rely on users to install them.
- **Spyware** *Spyware* is a type of privacy-invasive software that secretly records information about user behavior, often for the purposes of market research. Typically spyware is injected into a system when a user installs a free tool or visits a Web site with browser security settings set to a low level. The most common function of such spyware is to record the Web sites that a user visits. More rarely, some spyware, such as keyloggers (which record every keystroke), can be installed deliberately by a third party and be used to gather personal information. The biggest threat posed by most spyware is system performance degradation. All types of spyware reduce system performance by hijacking the resources of the computer for their own purposes. Unlike viruses and worms, spyware does not self-replicate.
- **Adware** Adware is similar to spyware and is often installed alongside it. The purpose of adware is to display unsolicited advertisements to the user in the form of pop-up windows or Web browser alterations. Adware can also download and install spyware.

> ***NOTE*** **SPYWARE AND ADWARE**
>
> **The term *spyware* is often used as a general term for all unwanted software that runs in the background and that gathers market research information, displays advertisements, or alters the behavior of applications such as Web browsers. Microsoft uses the phrase "spyware and potentially unwanted software" to refer to the type of software that is unwanted but is not unambiguously harmful.**

- **Backdoor** A backdoor is a program that gives a remote, unauthorized party complete control over a system by bypassing the normal authentication mechanism of that system. Backdoors have been known to be installed by worms that exploit a weakness in a well-known program. To protect your system against backdoors, it is essential to keep your applications (not just your operating system) updated.
- **Rootkit** A rootkit is a persistent type of malware that injects itself beneath the application level and that as a result, tends to be much harder to detect from within the operating system. A rootkit can alter the core functionality of the operating system, or it can install itself as its own operating system invisible to the user and to most anti-malware software. Other rootkits can operate at the firmware (BIOS) level. Typically, a rootkit is used to provide a backdoor to a system.

Although malware has been proliferating in type and number, the defenses against these threats have improved as well. When UAC is enabled in Windows 7, for example, a malware application cannot install itself easily without the user's knowledge. This next section provides an overview of UAC, which was introduced in Windows Vista and has been refined in Windows 7.

Understanding UAC

UAC is a set of security features designed to minimize the danger of running Windows as an administrator and to maximize the convenience of running Windows as a standard user. In versions of Windows before Windows Vista, the risks of logging on as an administrator were significant, yet the practice of doing so was widespread. Meanwhile, running as a standard user was generally safe, but the inconveniences prevented many from adopting the practice.

In versions of Windows before Windows Vista, malware could use the credentials of a locally logged-on administrator to damage a system. For example, if you were logged on to Windows XP as an administrator and unknowingly downloaded a Trojan horse from a network source, this malware could use your administrative privileges to reformat your hard disk drive, delete all your files, or create a hidden administrator account on the local system.

The main reason that users in previous versions of Windows often ran as administrators despite these dangers is that many common tasks, such as installing an application or adding a printer, required a user to have administrator privileges on the local machine. Because in previous versions of Windows there was no easy way to log on as a standard user and "elevate" to an administrator only when necessary, organizations whose users occasionally needed administrator privileges simply tended to configure their users as administrators on their local machines.

NOTE **WHAT IS ELEVATION?**

The term *elevation* is used when a user adopts administrator privileges to perform a task.

How Does UAC Address the Problem of Administrator Privileges?

UAC is the result of a new Windows security design in which both standard users and administrators use the limited privileges of a standard user to perform most actions. When users are logged on, UAC prompts them in different ways to confirm actions that make important changes to the computer. If an administrator is logged on, the action is performed only if he or she confirms it. If a standard user is logged on, the action is performed only if he or she can provide administrator credentials. In both cases, the elevation to administrator-level privileges is temporary and used to perform only the action required. Through this new system, UAC inhibits malware from secretly using a logged-on administrator's privileges.

Understanding UAC Notifications for Administrators

By default, UAC is configured to notify administrators only when programs request elevation. For example, administrators see UAC notification when they attempt to run a program (such as Cmd.exe) at elevated administrator privileges, as shown in Figure 5-1. According to this default setting, administrators in Windows 7 do not see a UAC notification when they adjust Windows settings that require administrator privileges.

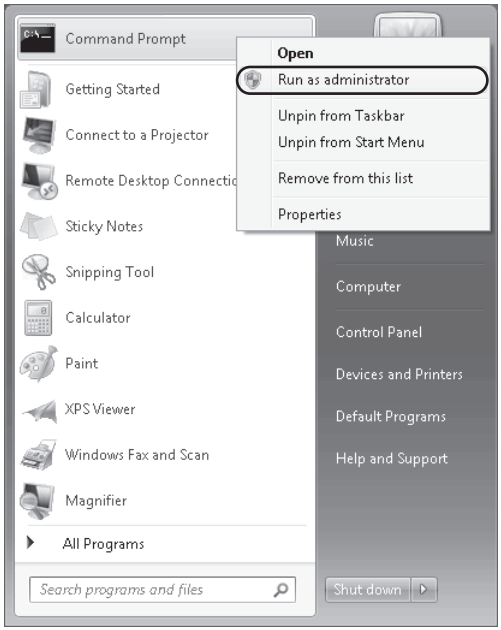


FIGURE 5-1 Opening an elevated command prompt

NOTE **CHANGES IN WINDOWS 7 UAC BEHAVIOR**

For administrators, the default behavior of UAC in Windows 7 has changed significantly from that in Windows Vista and Windows Server 2008. In those operating systems, UAC generated a prompt by default whenever any type of elevation was requested, including when an administrator attempted to change Windows settings. Administrators see UAC prompts less frequently in Windows 7.

The UAC notification that normally appears for administrators is called a *consent prompt* and is shown in Figure 5-2. Note that by default, the entire screen darkens when the notification appears and freezes until the user responds to the prompt. This feature is called the *Secure Desktop* and can be disabled.

NOTE **EDUCATE USERS ABOUT UAC PROMPTS!**

The point of UAC notifications is to alert users when malware might be harming your computer. If malware were to request elevation for a particular purpose, it too would generate a notification such as the one shown in Figures 5-2 or 5-3. Consequently, an essential factor in the ability of UAC to thwart malware is appropriate user response. You need to educate users—and gently remind your fellow administrators—that they should click No or Cancel whenever they see a UAC notification message that they did not initiate.

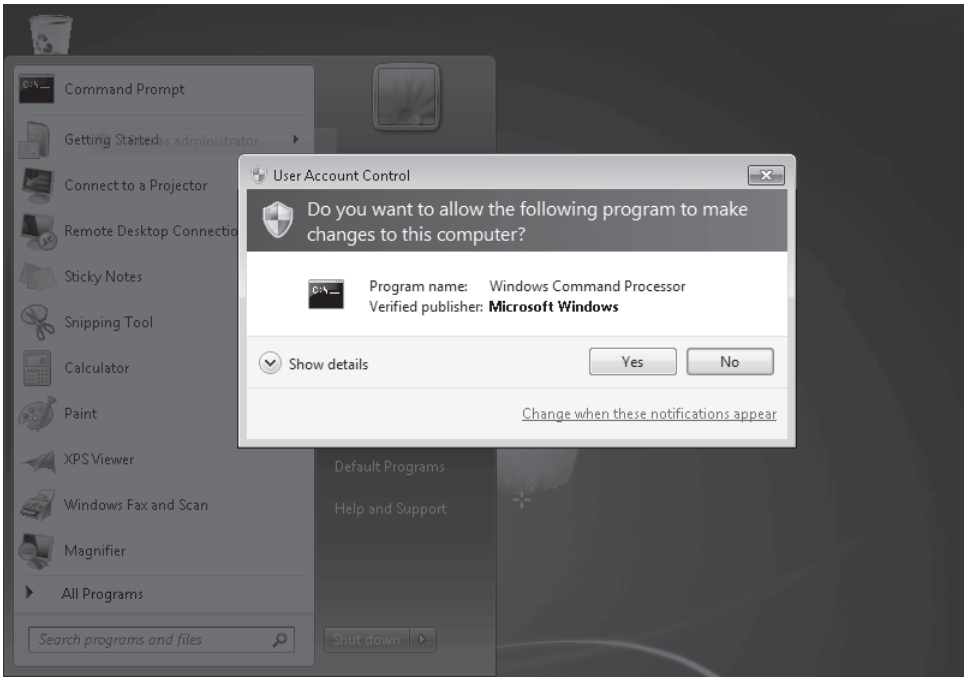


FIGURE 5-2 By default, UAC displays a consent prompt on a Secure Desktop to administrators who request to run a program with elevation.

Understanding UAC Notifications for Standard Users

The UAC notifications shown to standard users are distinct from those shown to administrators in that the notifications for standard users prompt these users to provide administrator credentials. As with administrators, standard users by default receive UAC notifications when they attempt to run a program such as a command prompt at elevated privileges, or when a program independently requests elevation. In addition, standard users by default receive UAC notifications when they attempt to make changes on the system that require administrator privileges. For example, if standard users open the System page in Control Panel and click Remote Settings, they see the credential prompt shown in Figure 5-3.

NOTE **THE DEFAULT BEHAVIOR OF UAC IS THE SAME FOR STANDARD USERS IN WINDOWS 7**

Although UAC in Windows 7 offers many notification levels that did not exist in Windows Vista or Windows Server 2008, the default behavior for standard users is the same. Whenever standard users attempt to make a change that requires administrator privileges, a credential prompt appears on a Secure Desktop.

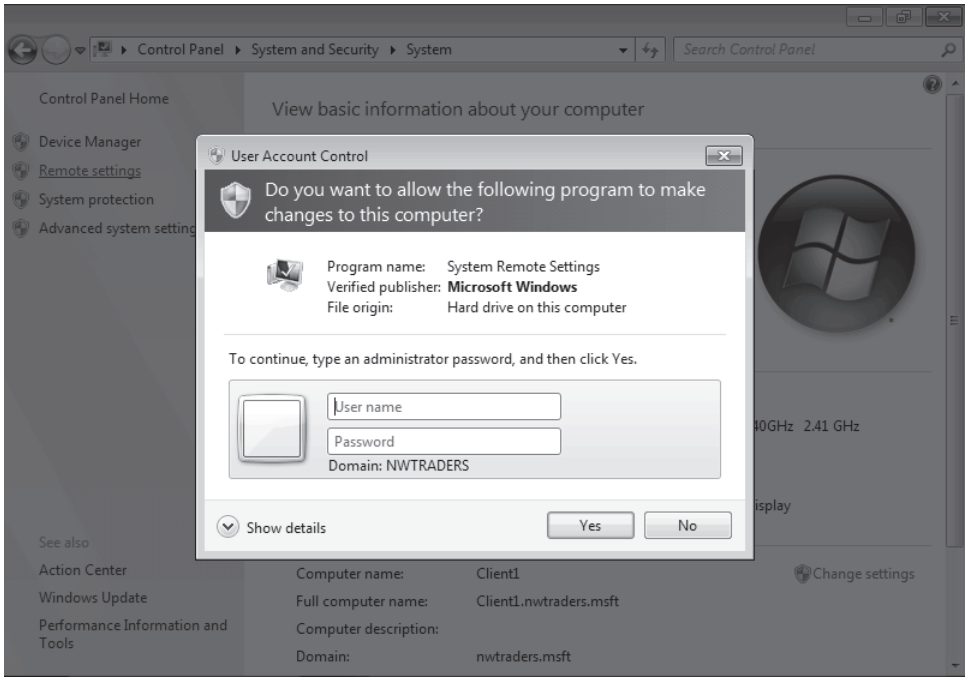


FIGURE 5-3 By default, UAC displays a credential prompt on a Secure Desktop to standard users who request elevation.

Configuring UAC in Control Panel

In a domain environment, it is recommended that UAC be controlled centrally by Group Policy instead of by configuration settings on each local machine. However, in workgroup environments or in domain environments in which Group Policy allows local UAC configuration, you can configure UAC through Control Panel.

To configure UAC in Control Panel, perform the following steps:

1. In Control Panel, click System and Security.
2. Under Action Center, click Change User Account Control Settings, as shown in Figure 5-4.

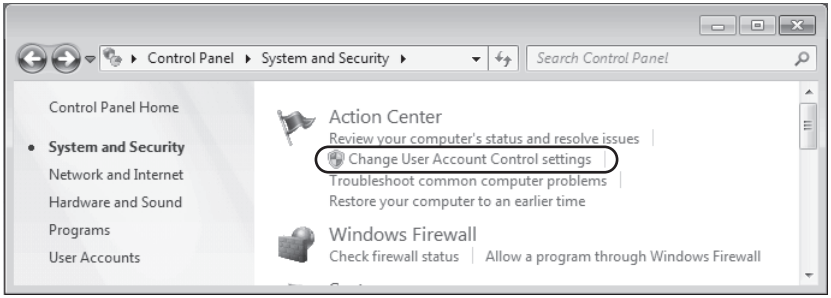


FIGURE 5-4 You can access UAC settings through the Action Center.

This step opens the User Account Settings window, one version of which is shown in Figure 5-5. Note that the set of options that appears is different for administrators and standard users, and that each user type has a different default setting.

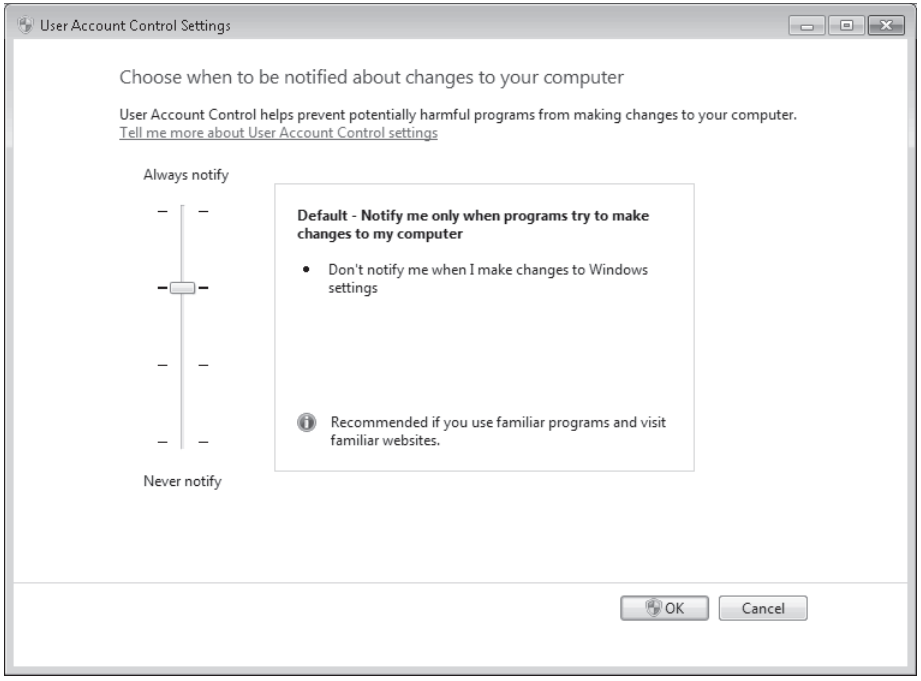


FIGURE 5-5 UAC allows you to choose among four notification levels.

3. Choose one of the following notification levels:
   - **Always Notify** This level is the default for standard users, and it configures UAC to act as it does in Windows Vista. At this level, users are notified whenever any changes that require administrator privileges are attempted on the system.
   - **Notify Me Only When Programs Try To Make Changes To My Computer** This level is the default for administrators and is not available for standard users. At this level, administrators are not notified when they make changes that require administrator privileges. However, users are notified through a consent prompt when a program requests elevation.
   - **Always Notify Me (And Do Not Dim My Desktop)** This level is not available for administrators. It is similar to the default setting for standard users, except that at this particular level, the Secure Desktop is never displayed. Disabling the Secure Desktop tends to reduce protection against malware, but it improves the user experience. This setting might be suitable for standard users who very frequently need to request elevation.

- **Notify Me Only When Programs Try To Make Changes To My Computer (Do Not Dim The Desktop)** This level is available for both standard users and administrators. At this level, the behavior is the same as with the default administrator level ("Notify me only when programs try to make changes to my computer"), but with this option the Secure Desktop is not displayed.
- **Never Notify** This level disables notifications in UAC. Users are not notified of any changes made to Windows settings or when software is installed. This option is appropriate only when you need to use programs that are incompatible with UAC.

4. Click OK.

Configuring UAC Through Group Policy

You can configure UAC through Local Security Policy or Group Policy settings. To find UAC-related policy settings in a GPO, navigate to the following node:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options

This location is shown in Figure 5-6.

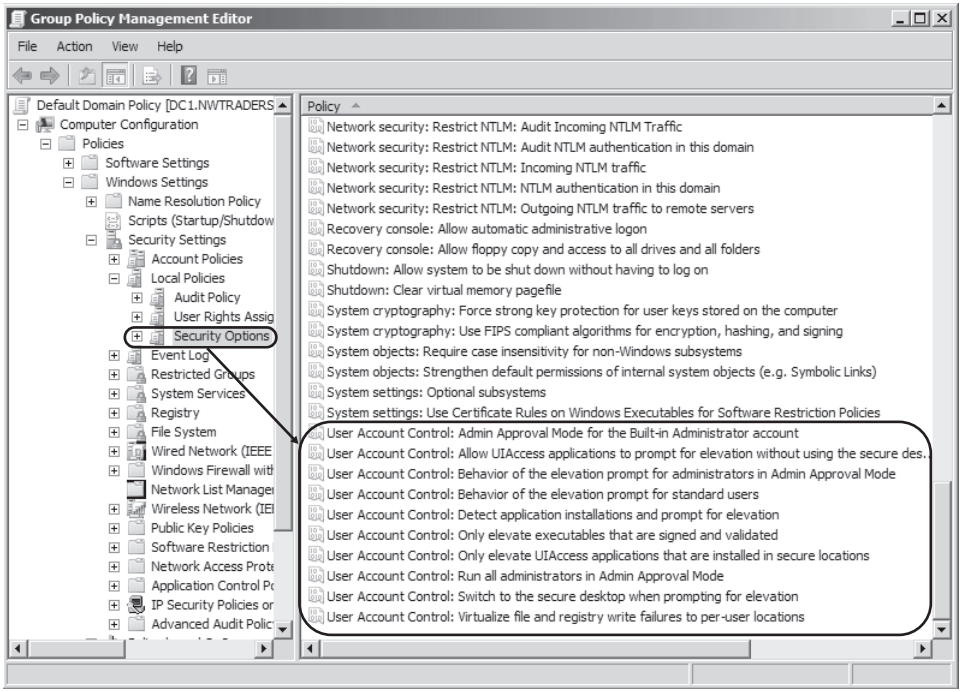


FIGURE 5-6 You can find UAC settings in Security Options in a GPO or in Local Security Policy

The following 10 UAC-related policy settings are available. The next section describes each of these configurable settings.

- **User Account Control: Admin Approval Mode For The Built-in Administrator Account** This policy applies only to the built-in Administrator account, and not to other accounts that are members of the local Administrators group. When you enable this policy setting, the built-in Administrator account sees UAC notifications just as other administrative accounts do. When you disable the setting, the built-in Administrator account behaves just like it does in Windows XP, and all processes run using Administrator privileges. This setting is disabled in Local Security Policy by default.
- **User Account Control: Allow UIAccess Applications to Prompt For Elevation Without Using The Secure Desktop** This setting controls whether user Interface Accessibility (UIAccess) programs can disable the Secure Desktop automatically. When enabled, UIAccess applications (such as Remote Assistance) automatically disable the Secure Desktop for elevation prompts. Disabling the Secure Desktop causes elevation prompts to appear on the standard desktop. By default, this setting is disabled in Local Security Policy.
- **User Account Control: Behavior Of The Elevation Prompt For Administrators In Admin Approval Mode** This policy setting controls the behavior of the elevation prompt for administrators. Six options are available:
  - **Elevate Without Prompting** With this option, administrators never see elevation prompts.
  - **Prompt For Credentials On The Secure Desktop** When this option is chosen, administrators see credential prompts on a Secure Desktop when elevation is requested.
  - **Prompt For Consent On The Secure Desktop** With this option, administrators see a consent prompt on a Secure Desktop when elevation is requested.
  - **Prompt For Credentials** When this option is selected, administrators see a credential prompt on a normal desktop when elevation is requested.
  - **Prompt For Consent** When this option is selected, administrators see a consent prompt on a normal desktop when elevation is requested.
  - **Prompt For Consent For Non-Windows Binaries** This option is the default setting in Local Security Policy. It causes a consent prompt to appear any time an application requests elevation.
- **User Account Control: Behavior Of The Elevation Prompt For Standard Users** This policy setting controls the behavior of the elevation prompt for standard users. Three options are available:
  - **Automatically Deny Elevation Requests** When this option is enforced, standard users are not able to perform tasks that require elevation.
  - **Prompt For Credentials On The Secure Desktop** With this option (the default setting in Local Security Policy), standards users see a credential prompt on the Secure Desktop when elevation is requested.
  - **Prompt For Credentials** When this option is chosen, standard users see a credential prompt on the normal desktop whenever elevation is requested.

- **User Account Control: Detect Application Installations And Prompt For Elevation** When enabled, this policy setting configures UAC to prompt for administrative credentials when the user attempts to install an application that makes changes to protected aspects of the system. When disabled, the prompt won't appear. Domain environments that use delegated installation technologies such as Group Policy Software Install (GPSI) or Microsoft Systems Management Server (SMS) can disable this feature safely because installation processes can escalate privileges automatically without user intervention. By default, this setting is enabled in Local Security Policy.
- **User Account Control: Only Elevate Executables That Are Signed And Validated** When this policy setting is enabled, Windows 7 refuses to run any executable that isn't signed with a trusted certificate, such as a certificate generated by an internal Public Key Infrastructure (PKI). When disabled, this policy setting allows users to run any executable, potentially including malware. If your environment requires all applications to be signed and validated with a trusted certificate, including internally developed applications, you can enable this policy to increase security greatly in your organization. This setting is disabled in Local Security Policy by default.
- **User Account Control: Only Elevate UIAccess Applications That Are Installed In Secure Locations** When enabled, this policy setting causes Windows 7 to grant user interface access only to those applications that are started from Program Files or subfolders, from Program Files (x86) or subfolders, or from \Windows\System32\. When disabled, the policy setting grants user interface access to applications regardless of where they are started in the file structure. This policy setting is enabled by default in Local Security Policy.
- **User Account Control: Run All Administrators In Admin Approval Mode** This policy setting, enabled by default in Local Security Policy, causes all accounts with administrator privileges *except* for the local Administrator account to see consent prompts when elevation is requested. If you disable this setting, administrators never see consent prompts and the Security Center displays a warning message.
- **User Account Control: Switch To The Secure Desktop When Prompting For Elevation** The Secure Desktop is a feature that darkens the screen and freezes all activity except for the UAC prompt. It reduces the possibility that malware can function, but some users might find that the feature slows down their work too much. When enabled, this policy setting causes the Secure Desktop to appear with a UAC prompt. When disabled, this policy setting allows UAC prompts to appear on a normal desktop. This policy setting is enabled by default in Local Security Policy.
- **User Account Control: Virtualize File And Registry Write Failures To Per-User Locations** This policy setting, enabled by default in Local Security Policy, improves compatibility with applications not developed for UAC by redirecting requests for protected resources. When disabled, this policy setting allows applications not developed for UAC to fail.

Disabling UAC Through Local or Group Policy

To force UAC to a disabled state, you can use Local Security Policy or Group Policy. First, set the User Account Control: Behavior Of The Elevation Prompt For Administrator In Admin Approval Mode setting to Elevate Without Prompting. Then, disable the User Account Control: Detect Application Installations And Prompt For Elevation and User Account Control: Run All Administrators In Admin Approval Mode settings. Finally, set User Account Control: Behavior Of The Elevation Prompt For Standard Users setting to Automatically Deny Elevation Requests. Then, restart the computers on which you want to apply the new settings.

Best Practices for Using UAC

To receive the security benefits of UAC while minimizing the costs, follow these best practices:

- Leave UAC enabled for client computers in your organization.
- Have all users—especially IT staff—log on with standard user privileges.
- Each user should have a single account with only standard user privileges. Do not give standard domain users accounts with administrator privileges to their local computers.
- Domain administrators should have two accounts: a standard user account that they use to log on to their computers, and a second administrator account that they can use to elevate privileges.
- Train users *not* to approve a UAC prompt if it appears unexpectedly. UAC prompts should appear only when the user is installing an application or starting a tool that requires elevated privileges. A UAC prompt that appears at any other time might have been initiated by malware. Rejecting the prompt helps prevent malware from making permanent changes to the computer.

Quick Check

- **Which Group Policy setting could you enable to prevent executables from running if they aren't signed with a trusted certificate?**

Quick Check Answer

- **User Account Control: Only Elevate Executables That Are Signed And Validated**

Whereas UAC is a set of features that broadly aims to protect core areas of the operating system, another Windows 7 tool—Windows Defender—has a much narrower goal of detecting and removing unwanted software.

Protecting Clients from Spyware with Windows Defender

Windows Defender is a tool in Windows 7 whose purpose is to detect and remove spyware on a client system. By default, Windows Defender is configured to download new spyware definitions regularly through Windows Update and then use these definitions to scan for

spyware on the local system. Often, you do not need to change this default configuration, though in large networks you might want to disable some Windows Defender features through Group Policy.

> ***NOTE*** **USE WINDOWS DEFENDER IN SMALL NETWORKS**
>
> **Windows Defender is a basic anti-malware program that is suitable for use in small networks or as a temporary solution before an advanced anti-malware solution is purchased. In large networks, you should use a centrally managed anti-malware solution such as Microsoft Forefront Client Security.**

To view Windows Defender, open Control Panel, select View By Large Icons, and then scroll down to click Windows Defender, as shown in Figure 5-7. (Alternatively, you can click Start, type **windows defender**, and select Windows Defender in the Start menu.)

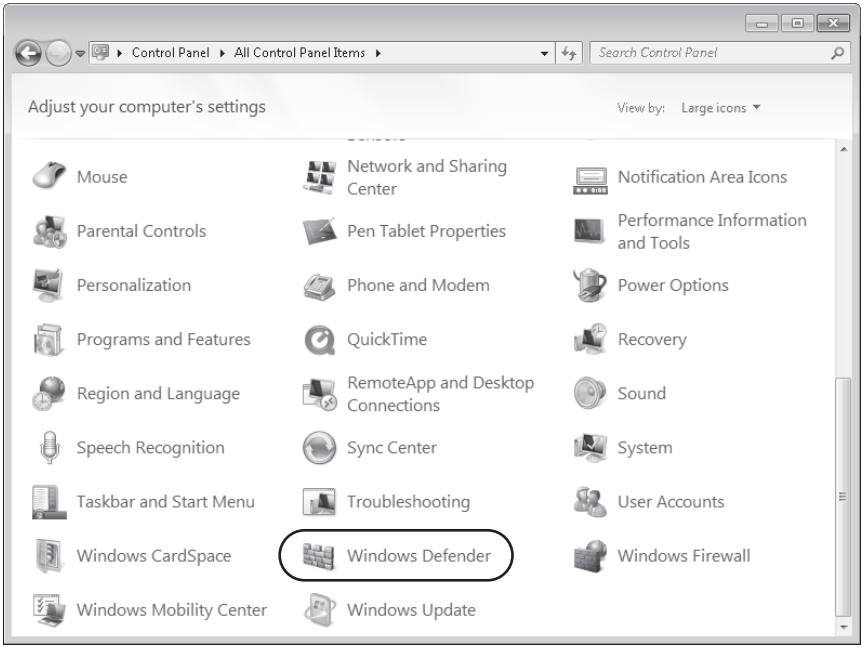


FIGURE 5-7 Opening Windows Defender

Windows Defender is shown in Figure 5-8.

By default, Windows Defender provides two types of protection:

- **Automatic scanning** Windows Defender is configured by default to download new definitions and then perform a quick scan for spyware at 2 A.M. daily.
- **Real-time protection** With this feature, Windows Defender constantly monitors computer usage in areas such as the Startup folder, the Run keys in the registry, and Windows add-ons. If an application attempts to make a change to one of these areas, Windows Defender prompts the user either to Permit (allow) or Deny (block) the change.

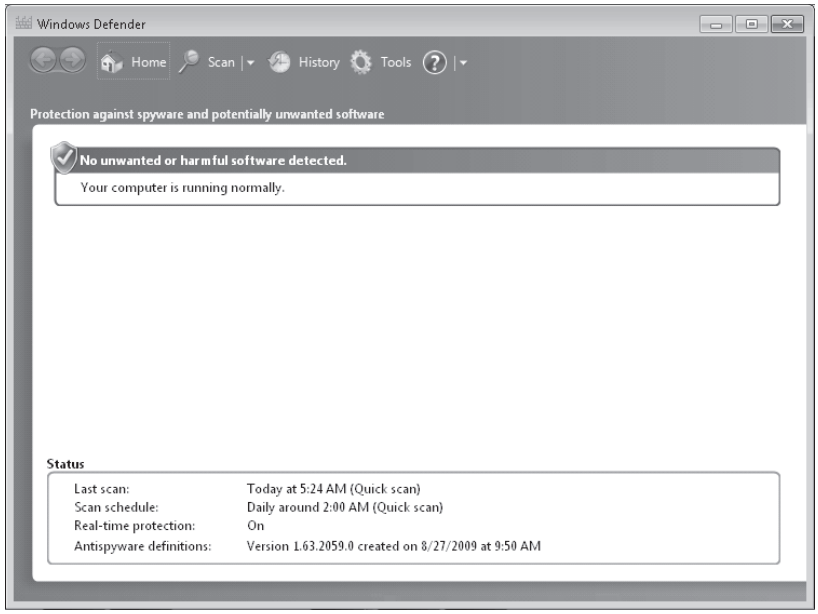


FIGURE 5-8 Windows Defender automatically checking for spyware

Besides providing this automatic functionality, Windows Defender also lets you perform a manual scan of the system. You can start a manual scan by selecting Quick Scan, Full Scan, or Custom Scan from the Scan menu, as shown in Figure 5-9.

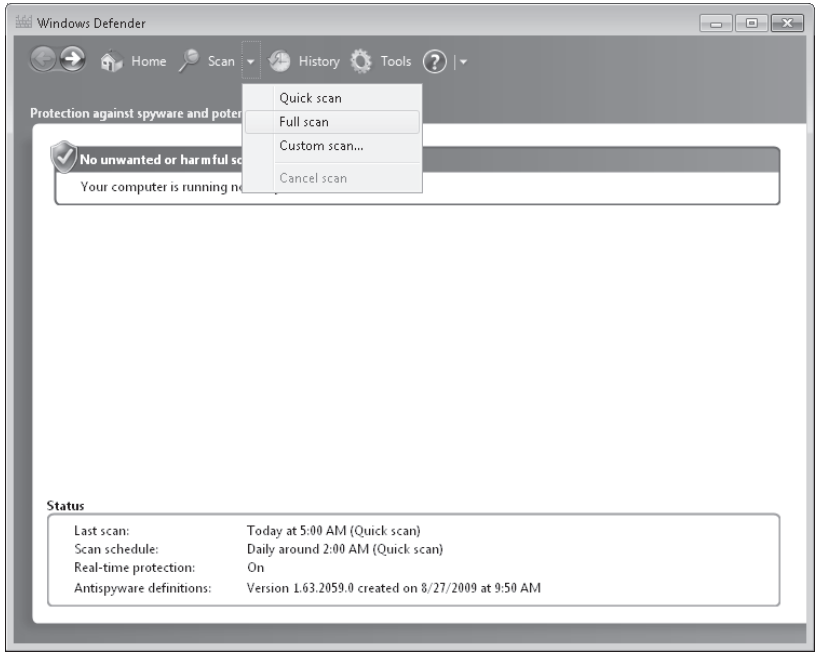


FIGURE 5-9 Performing a manual scan in Windows Defender

These three scan types are described in the following list:

- **Quick Scan** This type of scan scans only the areas of a computer most likely to be infected by spyware or other potentially unwanted software. These areas include the computer's memory and portions of the registry that link to startup applications. A quick scan is sufficient to detect most spyware.
- **Full Scan** This type of scan scans every file on the computer, including common types of file archives and applications already loaded in the computer's memory. A full scan typically takes several hours and can even take more than a day. You need to run a full scan only if you suspect that a user's computer is infected with unwanted software after the quick scan is run.
- **Custom Scan** Custom scans begin with a quick scan and then perform a detailed scan on the specific portions of a computer that you choose.

NOTE **YOU CAN WORK ON A COMPUTER WHILE A SCAN IS IN PROGRESS**

Although scans slow the computer down, a user can continue to work on the computer while a scan is in progress. Note also that scans consume battery power on mobile computers very quickly.

Handling Detected Spyware

If Windows Defender finds spyware or potentially unwanted software as a result of a scan, it displays a warning and provides you with four options for each item detected:

- **Ignore** This option allows the detected software to remain untouched on your computer and stay detectable by Windows Defender whenever the next scan is performed. This option might be appropriate when you need to research the software that Windows Defender has found before you decide to remove it.
- **Quarantine** This option isolates the detected software. When Windows Defender quarantines software, it moves it to another location on your computer and then prevents the software from running until you choose to restore it or remove it from your computer. This option is used most often when the detected software cannot be removed successfully.
- **Remove** This option deletes the detected software from your computer. You should choose this option unless you have a compelling reason not to.
- **Always Allow** The option adds the software to the Windows Defender Allowed list and allows it to run on your computer. Windows Defender stops alerting you to actions taken by the program. You should choose this option only if you trust the software and the software publisher.

Configuring Windows Defender Through Group Policy

In an AD DS environment, it is recommended that you configure clients by using Group Policy instead of individually on each machine. To find the Group Policy settings for Windows Defender, open a GPO and navigate to Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender, as shown in Figure 5-10.

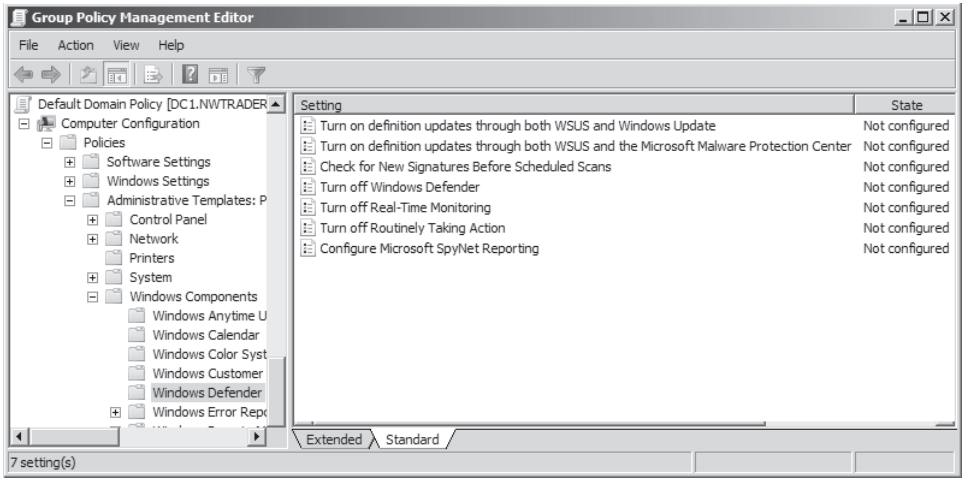


FIGURE 5-10 Group Policy settings for Windows Defender

The following seven policy settings for Windows Defender are available:

- **Turn On Definition Updates Through Both WSUS And Windows Update** If you enable or do not configure this policy setting and the Automatic Updates client is configured to point to a WSUS server, Windows Defender obtains definition updates from Windows Update if connections to that WSUS server fail. If you disable this setting, Windows Defender checks for updates only according to the setting defined for the Automatic Updates client—either by using an internal WSUS server or Windows Update.
- **Turn On Definition Updates Through Both WSUS And The Microsoft Malware Protection Center** If you enable or do not configure this policy setting and the Automatic Updates client is configured to point to a WSUS server, Windows Defender checks for definition updates from both WSUS and the Microsoft Malware Protection Center if connections to that WSUS server fail. If you disable this setting, Windows Defender checks for updates only according to the setting defined for the Automatic Updates client—either by using an internal WSUS server or Windows Update.
- **Check For New Signatures Before Scheduled Scans** If you enable this policy setting, Windows Defender always checks for new definitions before it begins a scheduled scan of the computer. When you disable or do not configure this setting, Windows Defender does not check for new definitions immediately before beginning scheduled scans.

- **Turn Off Windows Defender** If you enable this policy setting, Windows Defender no longer performs any real-time or scheduled scans. (However, users can still perform manual scans.) You should enable this setting if you have implemented a more advanced anti-spyware solution such as Microsoft Forefront Client Security. If you disable or do not configure this policy setting, Windows Defender performs both real-time scans and any scheduled scans.
- **Turn Off Real-Time Monitoring** If you enable this policy setting, Windows Defender does not automatically prompt users to allow or block activity in protected areas of the operating system. If you disable or do not configure this policy setting, by default Windows Defender prompts users to allow or block potential spyware activity on their computers.
- **Turn Off Routinely Taking Action** If you enable this policy setting, Windows Defender only prompts the user to choose how to respond to a threat but not to take any automatic action. If you disable or do not configure this policy setting, Windows Defender automatically takes action on detected threats after approximately 10 minutes.
- **Configure Microsoft SpyNet Reporting** SpyNet is an online community that pools information about threats experienced by its members. SpyNet learns from the user responses to these threats to determine which threats are benign and which are malicious.

  If you enable this policy setting and choose the "No Membership" option, SpyNet membership is disabled, and no information is sent to Microsoft. If you enable this policy setting and choose the "Advanced" option, SpyNet membership is set to Advanced, and information about detected threats and the responses to those threats is sent to Microsoft.

  If you disable or do not configure this policy setting, SpyNet membership is disabled by default, but local users can change the membership setting.

NOTE **USING A BOOTABLE ANTIVIRUS CD**

When a computer has become severely infected with malware, the computer might run so slowly that it's difficult to perform an anti-malware scan. In this case, it's a good idea to perform an offline scan from a bootable CD if you have one available. By performing the scan outside of Windows, you avoid running the malware programs that consume resources and slow down the system.

Best Practices for Using Windows Defender

To receive the security benefits of Windows Defender while minimizing the costs, follow these best practices:

- Before deploying Windows 7, test all applications with Windows Defender enabled to ensure that Windows Defender does not alert users to normal changes that the application might make. If a legitimate application does cause warnings, add the application to the Windows Defender Allowed list.

- Change the scheduled scan time to meet the needs of your business. By default, Windows Defender scans at 2 A.M. If third-shift staff uses computers overnight, you might want to find a better time to perform the scan. If users turn off their computers when they are not in the office, you should schedule the scan to occur during the day.
- Use WSUS to manage and distribute signature updates.
- Use antivirus software with Windows Defender. Alternatively, you might disable Windows Defender completely and use client-security software that provides both anti-spyware and antivirus functionality.
- Do not deploy Windows Defender in large enterprises. Instead, use Forefront or a third-party client-security suite that can be managed more easily in enterprise environments.

MORE INFO **WINDOWS DEFENDER**

For more information about Windows Defender, visit the Windows Defender Virtual Lab Express at *http://www.microsoftvirtuallabs.com/express/registration.aspx?LabId=92e04589-cdd9-4e69-8b1b-2d131d9037af*.

Determining When Your System Is Infected with Malware

As a enterprise support technician, you need to know how to recognize the symptoms of a malware infection on your client computers. Then, if your antivirus and anti-spyware are not functioning or not detecting any malware, you need to know how to remove malware manually.

Here are a few common signs of a computer being infected by a virus, worm, or Trojan horse:

- Sluggish computer performance
- Unusual error messages
- Distorted menus and dialog boxes
- Antivirus software repeatedly turning itself off
- Screen freezing
- Computer crashing
- Computer restarting
- Applications not functioning correctly
- Inaccessible disk drives, or a CD-ROM drive that automatically opens and closes
- Notification messages that an application has attempted to contact you from the Internet
- Unusual audio sounds
- Printing problems

Note that, although these are common signs of infection, these symptoms might also indicate other types of hardware or software problems that are unrelated to malware.

Signs of a spyware infection tend to be slightly different from those of other types of malware. If you see any of the following symptoms, suspect spyware:

- A new, unexpected application appears.
- Unexpected icons appear in the system tray.
- Unexpected notifications appear near the system tray.
- The Web browser home page, default search engine, or favorites change.
- New toolbars appear, especially in Web browsers.
- The mouse pointer changes.
- The Web browser displays additional advertisements when visiting a Web page, or pop-up advertisements appear when the user is not using the Web.
- When the user attempts to visit a Web page, she is redirected to a completely different Web page.
- The computer runs more slowly than usual.

Some spyware might not have any noticeable symptoms, but it still might compromise private information.

How to Resolve Malware Infections

The most important way to resolve malware infections is to prevent them in the first place by running antivirus and anti-spyware programs daily with the latest virus and spyware definitions. If malware is discovered on a system, use the application to remove the malware if possible and quarantine it if not. If it is a new malware program, you might need to run a removal tool or perform a series of steps to remove it manually.

These steps naturally apply to malware that is detected. However, as important as it is to remember to use antivirus and anti-spyware daily, it is just as important to remember that no anti-malware application is foolproof. Many malware programs are in fact written around anti-malware software so that they cannot be detected. And if even a single malicious feature remains after a scan, that remaining malware program can install other malware programs.

If you suspect a problem related to malware after running antivirus and anti-spyware applications with the latest definitions, take the following steps:

1. If you notice changes to Windows Internet Explorer, such as unwanted add-ons or a new home page, use Control Panel to look for and uninstall any unnecessary programs.
2. Use the Startup tab of the System Configuration utility (Msconfig.exe) to clear any unnecessary startup programs. Note the Registry entry associated with any of these programs. (You can use this Registry information to delete the associated Registry keys if necessary.) Use the Services tab to disable any unnecessary services.

3. Open Task Manager. Note any unusual services listed on the Services tab or unusual processes listed on the Processes tab. (Be sure to click Show Processes From All Users so you can see all running processes.) Use the Go To Process option on the Services tab and the Go To Service(s) option on the Processes tab to help learn the connection between services and processes that are unknown to you. Then, perform Web searches on services and processes that lack descriptions or that otherwise seem suspicious. If you can determine from your research that any services or processes are associated with malware, right-click them to stop them. Then, in the Services console, disable the associated service so that it cannot run again.
4. Open the Registry Editor (Regedit.exe). Navigate to HKLM\Software\Microsoft\Windows\CurrentVersion\Run. In the details pane, note any Registry values associated with unwanted started programs. Write the path names provided to the target files in the Data column, as shown in Figure 5-11, and then delete the Registry values. Then, navigate to HKCU\Software\Microsoft\Windows\CurrentVersion\Run and do the same.

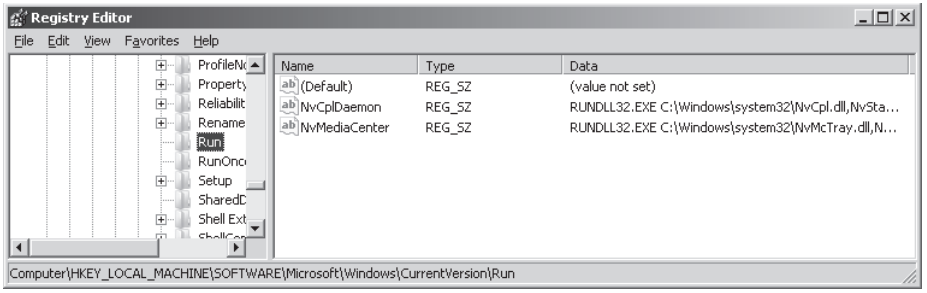


FIGURE 5-11 Copy down the path names to files associated with unwanted startup programs, and then delete the Registry values.

5. Using the path name information that you copied in step 4, visit these locations in the Windows file structure and delete the target files.
6. If you still see signs of malware, install an additional anti-spyware and antivirus application from a known and trusted vendor. Your chances of removing all traces of malware increase by using multiple applications, but you should not configure multiple applications to provide real-time protection.
7. If problems persist, shut down the computer and use the Startup Repair tool to perform a System Restore. Restore the computer to a date prior to the malware infection. System Restore typically removes any startup settings that cause malware applications to run, but it does not remove the executable files themselves. Do this only as a last resort: Although System Restore does not remove a user's personal files, it can cause problems with recently installed or configured applications.

Performing this series of steps resolves a great majority of malware problems. However, once malware has run on a computer, you can never be certain that the software is removed completely. In particular, rootkits are difficult to detect and remove. In these circumstances, if you suspect a rootkit and cannot remove it, you might be forced to reformat the hard disk, reinstall Windows, and then restore user files using a backup created prior to the infection.

PRACTICE Enforcing an Anti-Malware Policy Through Group Policy

In this practice, you use Group Policy to enforce specific settings for UAC and Windows Defender. These exercises require a domain controller running Windows Server 2008 R2 and a client running Windows 7 that is a member of the same domain.

EXERCISE 1 Enforcing UAC Settings Through Group Policy

In this exercise, you enforce new UAC default settings on computers running Windows 7 in the domain.

1. Log on to the domain controller.
2. Open Group Policy Management by clicking Start\All Programs\Administrative Tools\Group Policy Management.
3. In the Group Policy Management console tree, navigate to Group Policy Management\Forest: *Forest Name*\Domains*Domain Name*\Default Domain Policy.
4. Right-click Default Domain Policy, and then click Edit from the shortcut menu. The Group Policy Management Editor opens.
5. In the Group Policy Management Editor, navigate to Default Domain Policy\Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options.
6. In the details pane, double-click to open User Account Control: Switch To The Secure Desktop When Prompting For Elevation.
7. On the Security Settings tab, click Define This Policy Setting, select Disabled, and then Click OK.
8. In the details pane, double-click to open User Account Control: Behavior Of The Elevation Prompt For Standard Users.
9. On the Security Settings tab, click Define This Policy Setting, select Prompt For Credentials from the drop-down list, and then Click OK.

   These settings remove the Secure Desktop from all UAC prompts.
10. Click OK.
11. Switch to the client running Windows 7. Restart the client, and then log on to the domain from the client as a domain administrator.
12. Open an elevated command prompt by clicking Start\All Programs\Accessories, then right-clicking Command Prompt and clicking Run As Administrator from the shortcut menu.
13. A consent prompt appears without a Secure Desktop.
14. Log off the client, and then log on again to the domain from the client as a standard user without administrative privileges.
15. In Control Panel, beneath User Accounts, click Change Account Type. A credential prompt appears without a Secure Desktop.
16. Log off the client.

EXERCISE 2 Disabling Real-Time Monitoring for Windows Defender

A large corporate network should use a managed anti-spyware solution, which Windows Defender is not. Using Windows Defender to provide a secondary daily scan for malware on clients is a good idea, but you should not have two applications performing real-time monitoring. If your managed anti-spyware solution provides real-time monitoring, you should disable the same feature on Windows Defender by using Group Policy.

In this exercise, you use Group Policy to disable real-time monitoring for Windows Defender.

1. Log on to the domain controller.
2. Using the steps described in Exercise 1, open Group Policy Management and then choose to edit the Default Domain Policy.
3. In the Group Policy Management Editor, navigate to Default Domain Policy\Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender.
4. In the details pane, double-click to open Turn Off Real-Time Monitoring.
5. In the Turn Off Real-Time Monitoring dialog box, select Enabled, and then click OK.
6. Switch to Client1. Log on to the domain from Client1 as a domain administrator.
7. Open a command prompt and type **gpupdate**. You might see a notification bubble appear indicating that Windows Defender is turned off.
8. After the command finishes executing, click Start, type **windows defender**, and then click Windows Defender in the Start menu.
9. In Windows Defender, click Tools, and then click Options.
10. Select Real-Time Protection from the list of options.
11. The settings are dimmed. Real-time monitoring is disabled.
12. Return to the domain controller and the Default Domain Policy. Revert the Turn Off Real-Time Monitoring policy setting to Not Configured, and then click OK.
13. Rerun **gpupdate** on Client1, and then close all open windows on both computers.

Lesson Summary

- UAC helps prevent malware from secretly installing itself on Windows systems by notifying the user whenever a request is made to write to protected areas of the operating system. Users must be educated to dismiss these notifications if they have not initiated them.
- You can configure the behavior of UAC notifications. By default, administrators see consent prompts on a Secure Desktop when a program requests elevation. Standard users by default see credential prompts on a Secure Desktop whenever they or a program requests elevation.

- Windows Defender is a built-in feature of Windows 7 that provides basic spyware filtering and detection. Often Windows Defender needs no configuration, but you might want to disable it in larger networks that require a managed anti-spyware solution.
- You should how to check for and remove malware manually in case your anti-malware solution isn't functioning as desired. To do so, investigate unknown processes and services to stop and disable them if necessary, and look in the Registry for programs that are set to run automatically. Delete associated files.

Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 2, "Resolving Malware Issues." The questions are also available on the companion CD if you prefer to review them in electronic form.

> ***NOTE*** **ANSWERS**
>
> **Answers to these questions and explanations of why each answer choice is correct or incorrect are located in the "Answers" section at the end of the book.**

1. You work as an enterprise support technician in a large company. Your manager reports that some network administrators are using the built-in Administrator account for the domain and that, when logged on with this account, they are not seeing UAC notifications. She asks you to change configuration settings so that users logged on to the domain with the built-in Administrator account see UAC consent prompts. What should you do?
   - **A.** Configure Local Security Policy to set the User Account Control: Admin Approval Mode For The Built-in Administrator Account option to Enabled.
   - **B.** Configure Group Policy to set the User Account Control: Admin Approval Mode For The Built-in Administrator Account option to Enabled.
   - **C.** Configure Local Security Policy to set the User Account Control: Run All Administrators In Admin Approval Mode option to Enabled.
   - **D.** Configure Group Policy to set the User Account Control: Run All Administrators In Admin Approval Mode option to Enabled.
2. You work as an enterprise support technician in a company whose AD DS domain consists of 20 servers running Windows Server 2008 R2 and 500 client computers running Windows 7, 10 of which are portable and are used by employees who travel globally for work. These users have complained that Windows Defender tends to start a scan when the computer is operating on the battery source, and the scan quickly

consumes battery power. You want to prevent Windows Defender from consuming needed battery power without reducing the protection that it provides. What should you do?

A. Instruct the users to perform a manual scan when their computers are connected to a power source.

B. Choose the option to run a scan only when idle.

C. Instruct the users to adjust the schedule for automatic scanning.

D. Disable automatic scanning on all 10 computers.

Chapter Review

To further practice and reinforce the skills you learned in this chapter, you can perform the following tasks:

- Review the chapter summary.
- Review the list of key terms introduced in this chapter.
- Complete the case scenario. The scenario sets up a real-world situation involving the topics of this chapter and asks you to create a solution.
- Complete the suggested practices.
- Take a practice test.

Chapter Summary

- Windows Firewall blocks all incoming connection requests by default. To allow a network program to initiate a connection with a computer running Windows 7, you need to create a firewall exception for that program.
- To combat malware, you need to educate yourself and users continually about the evolving nature of threats. You also need to manage antivirus software, anti-spyware software such as Windows Defender, and UAC effectively. Finally, you need to know how to recognize classic symptoms of an infection and how to remove an infection manually if needed.

Key Terms

Do you know what these key terms mean? You can check your answers by looking up the terms in the glossary at the end of the book.

- **Exception**
- **Malware**
- **Spyware**
- **Virus**
- **Worm**

Case Scenario

In the following case scenario, you apply what you've learned about protecting client systems. You can find answers to these questions in the "Answers" section at the end of this book.

Case Scenario 1: Resolving Malware Infections

You work as an enterprise support technician for Contoso, Ltd., a marketing research firm with 500 employees. You receive a call from the help desk to investigate a research assistant's notebook computer that is apparently running very slowly. A help desk support technician was unable to resolve the issue.

You perform some basic testing on the computer, and you discover that several toolbars associated with spyware are installed in Internet Explorer. Your company uses a combined antivirus/anti-spyware solution, and Windows Defender is disabled on the network.

You conduct interviews with the Research Assistant and the Help Desk Support Technician.

Interviews

The following is a list of company personnel interviewed and their statements:

- **Research Assistant** "The problem has been getting progressively worse for about six months. It's gotten to the point that everything takes forever. I used to take this computer home with me, but now I don't even bother."
- **Help Desk Support Technician** "I tried to run an anti-malware scan, but nothing seemed to happen."

Questions

1. You want to immediately stop any malware that might be running. How should you achieve this?
2. Your testing reveals that the anti-malware client software installed on the computer does not run when it is opened. What can you do to perform an anti-malware scan on the computer?

Suggested Practices

To help you master the exam objectives presented in this chapter, complete the following tasks.

Identify and Resolve Issues Due to Malicious Software

Perform these practices to learn about tools that help detect and remove malware.

- **Practice 1** Perform a Web search for the term "Sysinternals Suite" or visit *http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx*. Download the Sysinternals Suite and unzip the file. Within the suite, locate Autoruns. Run Autoruns to discover the programs that are configured to start up automatically on your computer. Then, locate and run Rootkitrevealer to discover any rootkits on your system.

- **Practice 2** Perform a Web search for the term "bootable anti-malware CD" and research the various bootable anti-malware CDs that are available online. Create or download a bootable anti-malware CD and then use it to perform a malware scan on your system.

Take a Practice Test

The practice tests on this book's companion CD offer many options. For example, you can test yourself on just one exam objective, or you can test yourself on all the 70-685 certification exam content. You can set up the test so that it closely simulates the experience of taking a certification exam, or you can set it up in study mode so that you can look at the correct answers and explanations after you answer each question.

MORE INFO **PRACTICE TESTS**

For details about all the practice test options available, see the section entitled "How to Use the Practice Tests," in the Introduction to this book.

CHAPTER 9

Troubleshooting Software Issues

Software errors can appear during the installation process, immediately after installation, or long afterwards. Those that appear during installation tend to result from policy or permission constraints, availability issues, or installation settings. Those that appear immediately after installation tend to be associated with policy restrictions or compatibility problems. Those that appear long after installation tend to result from configuration changes.

In this chapter, we look at the various causes of software errors and provide strategies for how to resolve them.

Exam objectives in this chapter:

- Identify and resolve new software installation issues.
- Identify and resolve software configuration issues.
- Identify cause of and resolve software failure issues.

Lessons in this chapter:

Before You Begin

To perform the exercises in this chapter, you need:

- A domain controller running Windows Server 2008 R2
- A client running Windows 7 Enterprise that is a member of the domain

Lesson 1: Understanding and Resolving Installation Failures

To troubleshoot installation failures, you need to understand the requirements of a successful installation. These requirements include—among other factors—administrator privileges, compatibility with Windows 7, availability of installation code and data, and the status of application dependencies. You also need to understand how administrative features such as Software Restriction Policies (SRP) and AppLocker can block an installation even when these requirements are met. This lesson provides an overview of issues such as these that are related both to successful and unsuccessful installations.

After this lesson, you will be able to:

- Troubleshoot software installation failures by verifying a number of well-known installation requirements.
- Understand how AppLocker can prevent software installations.
- Understand many of the feature improvements of AppLocker over Software Restriction Policies.
- Use AppLocker to block a Windows Installer program from running.

Estimated lesson time: 30 minutes

Verifying Software Installation Requirements

You can install new software on clients running Windows 7 in two general ways. First, you can push applications to clients by means of a software deployment technology such as Group Policy, Microsoft System Center Configuration Manager, or a third-party solution. The second option is to install a program manually.

Although some of the requirements for successful software installation are particular to the way in which the software is deployed, most requirements apply to all software installation methods. To begin troubleshooting a failed installation, therefore, you can verify the general requirements described in the following section.

Verifying Administrator Rights

One of the most basic requirements for a successful software installation is that the user account running the installer program needs local administrator privileges, and to have these local administrator privileges on a particular computer, the account needs to be a member of the Administrators group on that computer.

If you are not able to get past the User Account Control prompt when you attempt to install a program, therefore, you should verify that the account used for installation is granted local administrator privileges on the computer in question. Typically, having domain administrator privileges is sufficient because by default, domain administrators are members of the local

Administrators group on every computer that is a member of the same domain. However, you should perform this verification even if you are already a domain administrator because the Domain Admins group might have been removed from the local Administrators group.

To determine whether you are a member of the local Administrators group on a particular computer, you can use the Local Users And Groups console. To open this console in Windows 7, you can click Start, type **edit local users and groups**, and then press Enter. (Note that you can perform this step even if you are not already a local administrator.) Then, in the console tree of the Local Users And Groups console, select Groups, and then double-click the Administrators group in the details pane. This procedure opens the Administrators Properties dialog box, which is shown in Figure 9-1. This dialog box lists all the local administrators for that machine.

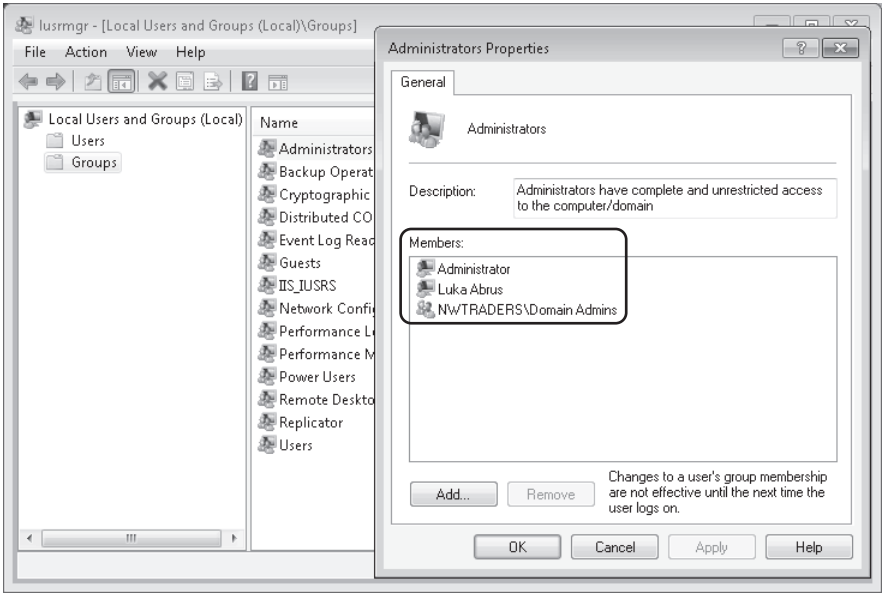


FIGURE 9-1 Viewing the local administrators

If you are a local administrator, you can then use the Add button in the Administrators Properties dialog box to add other local administrators if desired. Note, however, that in an enterprise network, it is preferable to control local group membership by using the Restricted Groups feature in Group Policy.

RUNNING AN INSTALLATION PROGRAM AS AN ADMINISTRATOR

If you can verify that you are a local administrator but you still see a message indicating that administrator rights are required to perform the installation, you should choose the option to run the installer program as an administrator. To do this, right-click the installation icon for the program, and then click Run As Administrator, as shown in Figure 9-2. If a User Account Control consent or credential prompt appears, provide confirmation or administrator credentials as needed.

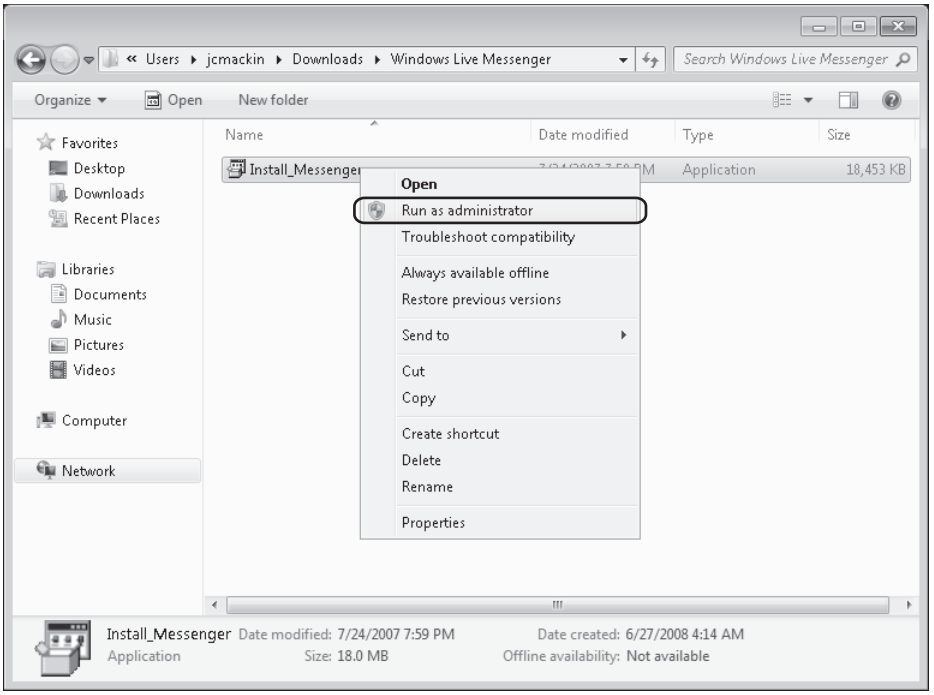


FIGURE 9-2 Running an installation with administrator privileges

Verifying Windows 7 Compatibility

If an application is known to be incompatible with Windows 7, you might receive a message informing you of this fact when you attempt to install the program. If no updated version of the software is available, you can try altering the compatibility settings on the installer program or hosting the application in a virtual environment. Handling software compatibility issues such as these is discussed in detail in Lesson 2 of this chapter, "Resolving Software Configuration and Compatibility Issues."

Verifying Trusted Publishers

When you install a new program, Windows 7 checks for a certificate and a digital signature to authenticate the publisher of the program. To verify this digital signature properly, the local computer must trust the root certification authority (CA) for the publisher certificate. Stated another way, the local computer must have installed in its Trusted Root Certification Authorities certificate store the root certificate in the certificate chain of the publisher certificate. An administrator can install this root certificate manually on a local computer or the certificate can be deployed to the Trusted Root Certification Authority certificate store on many clients through Group Policy.

If the certificate in the installer program is from a trusted publisher and the digital signature is verified, the installation proceeds normally. However, if no digital signature is present, or if the local computer is not configured to trust the publisher, you will see a warning message similar to the one shown in Figure 9-3.

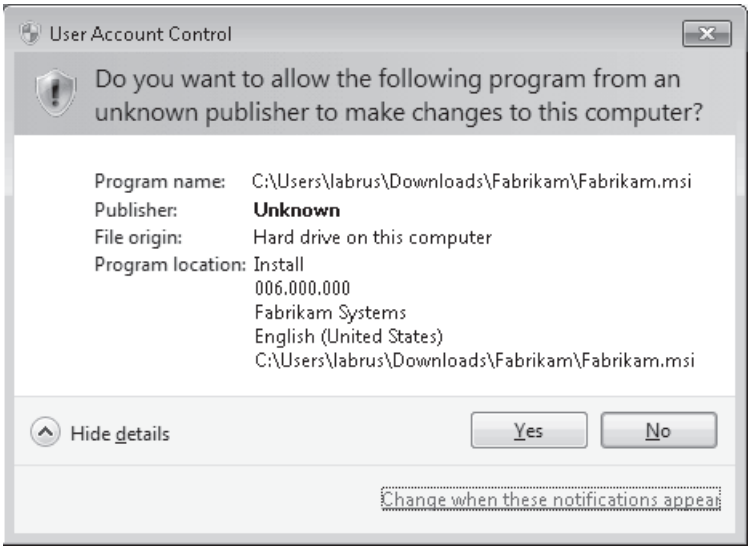


FIGURE 9-3 Avoid installing programs from untrusted publishers.

In general, you should avoid installing programs from unsigned publishers in an enterprise environment. Such programs might fail during installation, and even if they do install successfully, they could present stability problems or introduce malware into your network.

Verifying Software Logo Testing on a Client Running Windows 7

Occasionally, when you attempt to install an application, you will receive a warning that the application has not passed Windows 7 logo testing. In this case, you should avoid installing the software.

For an application to pass Windows 7 logo testing, it must meet a number of requirements, including compliance with specific anti-spyware guidelines, isolation from protected resources in Windows, a reversible installation, and a digital signature on all files.

Verifying the Installation Media Location

Before you attempt to install an application, ensure that all the files needed for installation are available in the required locations. For example, if you have copied an installer program from a network source to a local computer, be sure that you also copy all the associated secondary files that are called by the installer program when it runs. (These secondary files

can include .cab files or .ini files.) If you are installing an application from over the network, verify that any secondary files are also accessible from the local computer and that you have Read and Execute permissions on these files.

Verifying Installation Settings

When you attempt to install an application, ensure that the settings that you have chosen for the installation are configured properly; otherwise, the installation might fail. For example, if you choose to install a program on a read-only disk, the installation fails.

Verifying External Connections

Certain applications require connectivity to external sources of data. For example, the application might require a connection to a database, mainframe, Web site, license server, or other application server. In this case, verify that the installation program can reach these external connections.

Verifying Licensing and Other Application Constraints

An application might include constraints that will prevent it from installing successfully. For example, a license or product key might be required to install the application, or the application might need to be installed with a specific user account. Verify also that the application architecture is compatible with the local processor. For example, you cannot install a 64-bit application on a computer with a 32-bit CPU.

Verifying Application Dependencies

Some applications can be installed only after you first install other updates, features, service packs, or other applications. Be sure to prepare the client running Windows 7 for application installation by first installing all the necessary software dependencies.

MORE INFO **DEPLOYING APPLICATIONS**

The following Web sites are good resources for automating the installation of applications, as well as other deployment topics:

- AppDeploy.com at *http://www.appdeploy.com*

  This Web site provides information about deploying applications that are packaged using a variety of technologies.

- SourceForge at *http://unattended.sourceforge.net*

  This Web site describes how to automate the installation of many older installers.

Understanding Installation Restrictions with AppLocker

Occasionally, when you are attempting to install an application, you might receive an error such as the one shown in Figures 9-4 or 9-5.

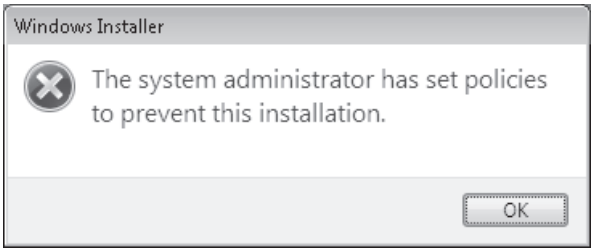


FIGURE 9-4 An installation prevented by AppLocker

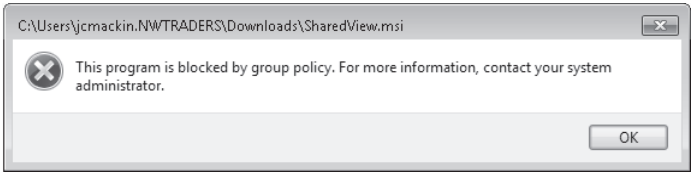


FIGURE 9-5 An installation prevented by SRP

If you see such a message, the AppLocker or SRP feature has been used to prevent the application from being installed. Both technologies are available in Windows 7 and Windows Server 2008 R2. AppLocker is essentially a new and improved version of SRP, but SRP is still included in these newer operating systems for compatibility with networks running older versions of Windows.

As with SRP, you configure AppLocker through Group Policy. To locate AppLocker, open a Group Policy Object (GPO) and navigate to Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\AppLocker, as shown in Figure 9-6. (In Local Security Policy, the path is simply Security Settings\Application Control Policies.)

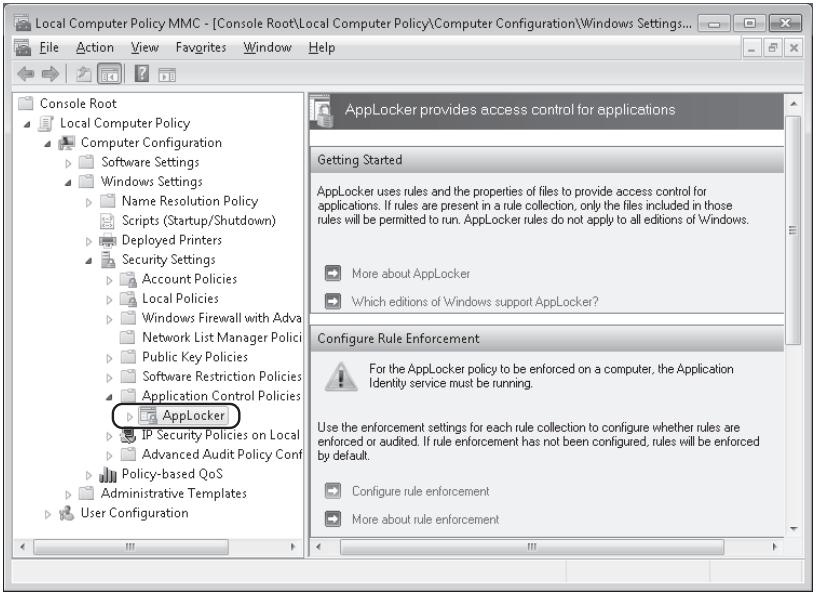


FIGURE 9-6 AppLocker is configured in a GPO.

You can see that the container for AppLocker (Application Control Policies) is found immediately below SRP.

The next section introduces AppLocker and describes the differences between it and SRP.

OVERVIEW OF APPLOCKER

AppLocker is a new feature in Windows 7 and Windows Server 2008 R2. It allows administrators to restrict the programs that users can run or install in your organization.

AppLocker resembles SRP in a number of ways. First, you configure both AppLocker and SRP in a GPO. Also like SRP, AppLocker allows you to create rules specifying an application to which you want to allow or deny access. Finally, as in SRP, in AppLocker you can define a program by specifying—among other methods—a hash of or a path to its file.

AppLocker, however, provides the following important improvements over SRP:

- Publisher rule condition

  In AppLocker, you can specify a program by extracting information from its digital signature, as shown in Figure 9-7. You can then use part of or all of this publisher information to define the programs you want to allow or deny. This publisher condition essentially replaces Certificate Rules in SRP.

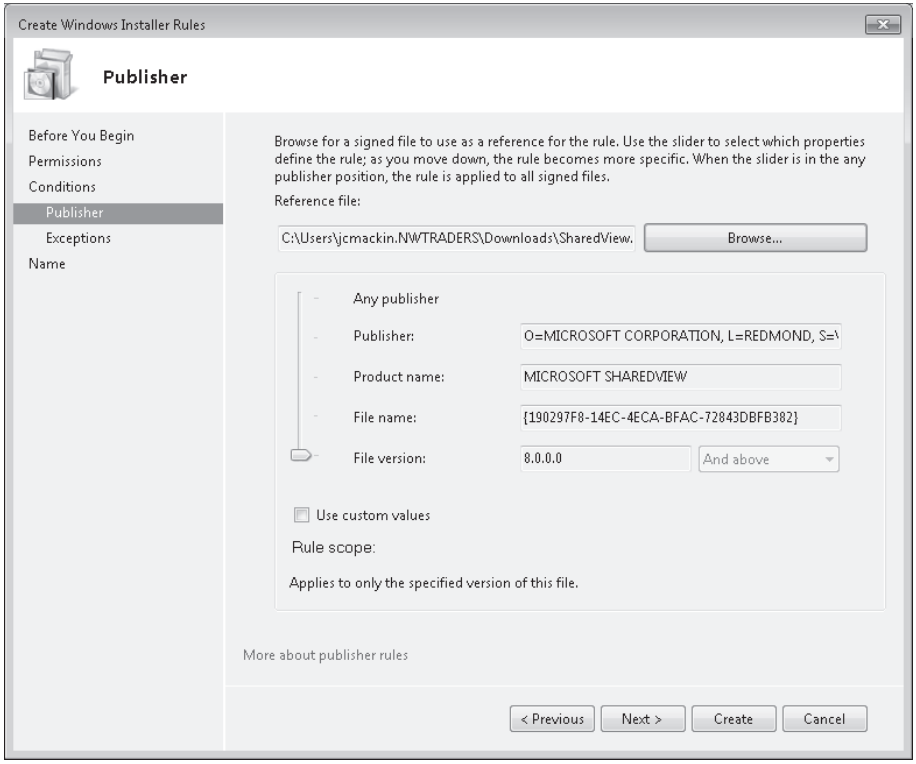


FIGURE 9-7 With AppLocker, you can specify an application by digital signature.

Using publisher information from a digital signature is by far the best way to specify an application in AppLocker. First, you can use this publisher information to create rules at various levels of specificity: You can make the rule apply to the publisher in general, to any version of the particular application, or to specific versions of the application (including all previous or future versions). Second, the publisher condition solves a key problem with SRP: In SRP, there is no comparable way to restrict access to an application through multiple updates. If you specify a path to an application that you want to restrict, users can simply move the program to a new path to avoid the restriction. If you specify a hash for the application, you have to create a new rule every time the application is updated.

- AppLocker blocks all programs that are not specifically allowed

  In SRP, rules by default are used to block access to chosen applications. However, within any company network, the number of applications that you want to block typically far exceeds the number that you want to allow. AppLocker accounts for this disparity by locking all applications that are not allowed. More specifically, AppLocker rules are enabled for one of four file type (executables, Windows Installer programs, scripts, or DLL files) when you first create a rule for that file type. Then, when AppLocker is enabled, all applications of that file type are locked if they are not allowed by a rule. To prevent system lockouts, AppLocker provides the Create Default Rules and Automatically Create Rules options. These options create allow-type rules for most applications. You can then create additional rules to change this default configuration.

- Assign Rules to Specific Users and Groups

  In AppLocker, you can create rules that apply to everyone or only to specific users and groups. In SRP, you can create only rules that apply to everyone.

- Exceptions

  AppLocker enables you to create a rule with an exception. For example, you can create a rule that allows any application to run except a specific .exe file. This feature is not available in SRP.

- Audit-only mode

  Unlike SRP, AppLocker includes an audit-only mode. Through auditing, you can test your configuration without enforcing AppLocker rules. When you configure AppLocker to audit AppLocker rules for a chosen file type (such Windows Installer programs), events are written to the event log when AppLocker would normally block access to that application.

  Audit mode is configured in the properties of the AppLocker node in a GPO, as shown in Figure 9-8. Audit events as they appear in Event Viewer are shown in Figure 9-9.

- Import and export rules

  In AppLocker, you can export and import rules to and from other computers, which allows administrators to copy and edit rules easily.

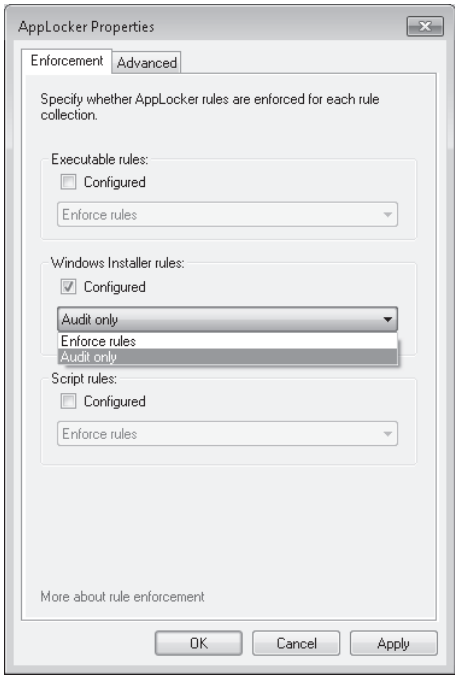


FIGURE 9-8 Configuring AppLocker rules for audit only

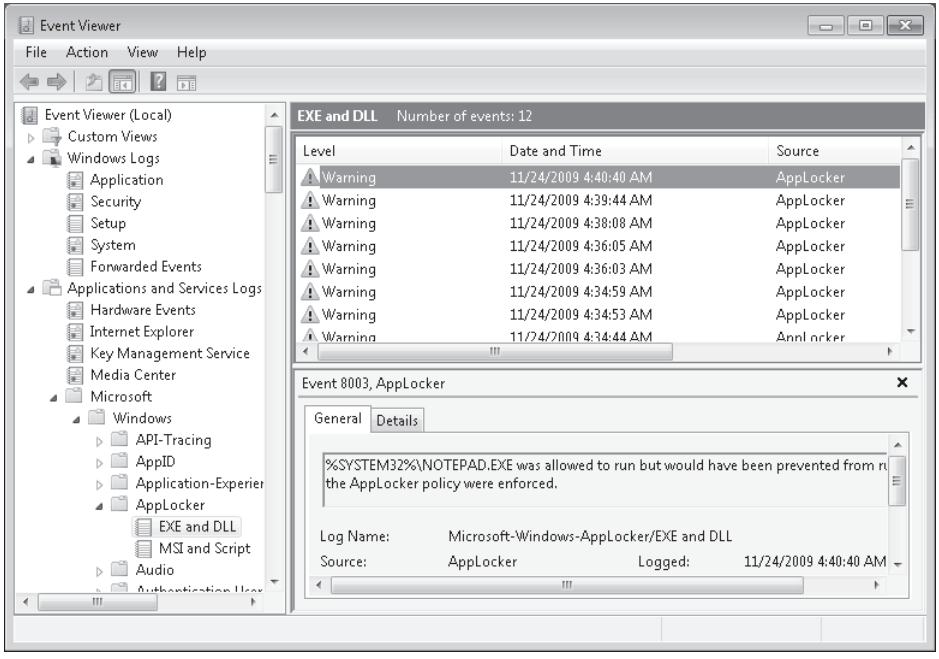


FIGURE 9-9 Audit-only events for AppLocker

REAL WORLD

J.C. Mackin

AppLocker is a great feature in many ways, but I don't believe it sufficiently warns administrators about the dangers of configuring it incorrectly. If you create a new rule without also creating the default rules, for example, you can easily lock yourself and everyone else out of your computer.

I actually experienced this problem firsthand when I originally saw AppLocker in a Windows 7 beta. I simply made a rule in Local Security Policy denying access to Notepad.exe, and I ignored the messages prompting me to create the default rules. Immediately afterwards, I was dismayed to see that Windows could not start. What I didn't know at the time was that AppLocker is enabled when you create the first rule. After you create that first rule, all programs of the same type—executables, in this case—are denied if you have not allowed them.

Luckily for me, this was only a virtual environment, and I had made a data snapshot of the computer before making any changes. It was easy for me to return the computer to the previous state. But I thought—what if this were a real environment? It's not unusual for administrators to explore new features on their own machines. Few people would suspect that the punishment for incorrectly configuring such a feature would be locking themselves out of their computer indefinitely. Worse yet, what if someone actually applied such a policy to the entire domain, and the domain controllers themselves were rendered unusable? It could be a disastrous situation.

What you should remember is always to create the default rules first in AppLocker and then create additional rules to modify the behavior of those default rules. When creating new rules, always test your results first in audit-only mode or use a virtual machine environment so that you can easily revert to a previous state if necessary.

Quick Check

- How do you find messages related to AppLocker in Event Viewer?

Quick Check Answer

- In the Event Viewer console tree, navigate to Event Viewer (Local)\Applications and Services Logs\Microsoft\Windows\AppLocker.

APPLOCKER AVAILABILITY AND COMPATIBILITY

AppLocker rules are enforced on computers running only Windows Server 2008 R2, Windows 7 Ultimate, and Windows 7 Enterprise. AppLocker rules are not enforced on computers running other versions of Windows, such as Windows Server 2008, Windows 7 Professional, or Windows Vista.

In a GPO containing only SRP rules, the rules are enforced on all computers running Windows, including those running Windows Server 2008 R2, Windows 7 Ultimate, and Windows 7 Professional. However, if a GPO contains both SRP rules and AppLocker rules, these same three operating systems read only the AppLocker rules. The SRP rules are applied to computers running other Windows operating systems.

APPLOCKER RELIES ON THE APPLICATION IDENTITY SERVICE

AppLocker rules are enforced on eligible clients only when those clients are running the Application Identity Service. By default, this service is not configured to start automatically on computers running Windows 7. If you want to enforce AppLocker rules, therefore, you should use Group Policy to set the Startup Type parameter to Automatic for the Application Identity Service.

PRACTICE Preventing Software Installation with AppLocker

In this practice, you download an .msi file from the Microsoft Web site and then prevent installation of that .msi file through AppLocker.

EXERCISE 1 Obtaining an .msi File

In this exercise, you download the file SharedView.msi from the Microsoft Download Center. You then begin a new installation to test its functionality.

1. Log on to the domain from the client running Windows 7 (Computer1) as a domain administrator.
2. In Windows Internet Explorer, visit the Microsoft Download Center at *http://download.microsoft.com*. Search for the file "SharedView.msi," and save it to your Downloads folder on Computer1. (If you do not have Internet access from Computer1, you can download the file from another computer and copy it to Computer1.)

> ***NOTE*** **YOU CAN USE ANY .MSI FILE**
>
> **Although we will use the file SharedView.msi in this exercise, you can replace this file with any other that you can locate and copy to the Downloads folder on Computer1.**

3. Share the Downloads folder by granting Read access to Everyone. To perform this step, right-click the Downloads folder, choose Share With on the shortcut menu, and then click Specific People. In the File Sharing window, type **Everyone**, click Share, and then click Done.

4. Open the Downloads folder and double-click SharedView.msi to begin the installation.
5. If an Open File-Security Warning message box appears and asks if you want to run the file, click Run.
6. The first page of the Microsoft SharedView Setup wizard appears. The fact that the wizard has started indicates that the .msi file is not blocked.
7. Click Cancel and then Yes to close the Microsoft SharedView Setup wizard.

EXERCISE 2 Configuring AppLocker to Block an .msi

In this exercise, you create a GPO, and then, in the new GPO, you create the default rules for AppLocker in the Windows Installer rule collection. Finally, you create a new Windows Installer rule that denies SharedView.msi.

1. Switch to the domain controller (DC1), and log on as a domain administrator.
2. Open Group Policy Management, which is available through the Start menu in the Administrative Tools folder.
3. In the Group Policy Management console tree, locate and expand the Domains container, and then select the domain (Nwtraders.msft) node.
4. Right-click the Nwtraders.msft node, and then click Create A GPO In This Domain, And Link It Here in the shortcut menu.
5. In the New GPO dialog box, type **AppLocker Block SharedView.msi**, and then click OK.
6. In the Group Policy Management console, in the details pane, right-click the AppLocker Block SharedView.msi GPO, and then click Edit. The Group Policy Management Editor opens.
7. In the Group Policy Management Editor console tree, navigate to Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\AppLocker\Windows Installer Rules.
8. Select and then right-click the Windows Installer Rules node, and then click Create Default Rules from the shortcut menu.

   In the details pane, three new rules appear. These rules allow everyone to run all digitally signed Windows Installer files, everyone to run all Windows Installer files (signed or not) in the %Systemdrive%\Windows\Installer directory, and administrators to run all Windows Installer files without exception.
9. Right-click the Windows Installer Rules node, and then click Create New Rule on the shortcut menu. The Before You Begin page of the Create Windows Installer Rules wizard opens.
10. Read all of the text on the page, and then click Next.
11. On the Permissions page, click Deny, and then click Next.
12. On the Conditions page, leave the default selection of Publisher, and then click Next.
13. On the Publisher page, click Browse.

14. In the Open window, in the File Name field, type **\\computer1\users*username*\Downloads\SharedView.msi**, and then click Open. For the variable *username*, specify the name of the account that you used in Exercise 1 to copy SharedView.msi to the Downloads folder. On the Publisher page, the information from the digital signature in the .msi file has populated the gray fields next to the slider.
15. Raise the slider two notches so that it is positioned next to Product Name. Next to the slider, MICROSOFT SHAREDVIEW still appears in the associated field, but the two fields beneath contain only an asterisk ("*").
16. Click Next.
17. On the Exceptions page, click Next.
18. On the Name And Description page, type **Block SharedView.msi** in the Name text box, and then click Create. The new Deny rule now appears in the details pane.
19. In the Group Policy Management Editor console tree, navigate to Computer Configuration\Policies\Windows Settings\Security Settings\System Services.
20. In the details pane, double-click to open the Application Identity service. The Application Identity Properties dialog box opens.
21. In the Application Identity Properties dialog box, check Define This Policy Setting, click Automatic, and then click OK. Clients need to run this service for AppLocker to work.
22. Close the Group Policy Management Editor console and the Group Policy Management console.
23. Switch to Computer1, and then restart Computer1.

EXERCISE 3 Testing the Configuration

In this exercise, you test the results of implementing the new GPO that you created in the last exercise.

1. After Computer1 has finished restarting, log on to the domain from Computer1 as a domain administrator.
2. Open your Downloads folder, and then double-click SharedView.msi.
3. If an Open File-Security Warning message box appears and asks if you want to run the file, click Run.
4. A Windows Installer warning message appears, indicating that the system administrator has set policies to prevent this installation.
5. Click OK to close the message.
6. Return to DC1. In the Group Policy Management console tree, locate the GPO named AppLocker Block SharedView.msi.
7. Right-click the AppLocker Block SharedView.msi GPO, and clear Link Enabled on the shortcut menu. This step effectively disables the policy.
8. Log off both computers.

Lesson Summary

- The successful installation of software depends on many requirements. These requirements include local administrator privileges, Windows 7 compatibility, proper installation settings, and other factors. To troubleshoot problems with an installation, you should verify that all of these requirements are met.
- A Windows Installer program can also be blocked by SRP or AppLocker.
- AppLocker is an improved version of SRP that is new to Windows 7 and Windows Server 2008 R2. Improvements in AppLocker include the publisher rule condition, the ability to assign rules to specific users and groups, and audit-only mode.

Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 1, "Understanding and Resolving Installation Failures." The questions are also available on the companion CD if you prefer to review them in electronic form.

> ***NOTE*** **ANSWERS**
>
> **Answers to these questions and explanations of why each answer choice is correct or incorrect are located in the "Answers" section at the end of the book.**

1. You work for Fabrikam, Inc., a firm whose network consists of a single Active Directory Domain Services (AD DS) domain.

   Fabrikam's development team periodically tests new software tools for various departments. Recently the team has been testing a tool created by another company, a new partner named Contoso.com. Whenever authorized users attempt to install the program, however, they receive a warning informing them that the program is from an unknown publisher.

   You want to allow authorized users to install applications made by Contoso without receiving a warning. What should you do?

   A. Ensure that all authorized users are administrators of the computers on which they are installing the software.

   B. Provide authorized users with the credentials of a domain administrator and instruct them to provide these credentials at the User Account Control prompt when they attempt to install the software.

   C. Use Group Policy to deploy the public certificate provided with the software to the Trusted Publishers certificate store on all required computers.

   D. Use Group Policy to deploy the root certificate for Contoso.com to the Trusted Root Certification Authorities certificate store on all required computers.

2. You want to use AppLocker to prevent users from running a file named NewApp.msi for versions 7.0 and earlier. You have already created the default rules. How can you achieve this objective?

   A. Create a new Executable rule with the Publisher rule condition.

   B. Create a new Executable rule with the File Hash rule condition.

   C. Create a new Windows Installer rule with the Publisher rule condition.

   D. Create a new Windows Installer rule with the File Hash rule condition.

Lesson 2: Resolving Software Configuration and Compatibility Issues

If a program that fails is known to be compatible with Windows 7, the failure is typically the result of a faulty configuration. In this case, resolving the issue requires you to review the program settings to pinpoint the configuration error causing the problems experienced. If on the other hand a program that fails is not fully compatible with Windows 7, you can often resolve the issue by adjusting compatibility settings or finding an alternate host for the application.

After this lesson, you will be able to:

- Understand strategies and features used to resolve software configuration errors.
- Understand the features in Windows 7 that are most likely to create an application compatibility problem.
- Configure an application to run with settings compatible with an older version of Windows.
- Understand Group Policy settings that can affect compatibility handling and reporting.

Estimated lesson time: 30 minutes

Resolving Software Configuration Issues

Installed applications that have been working properly sometimes malfunction or fail unexpectedly for an unknown reason. Application errors such as these often result from changes in configuration settings that are specific to the application, but there are some general guidelines that can help you in your efforts to resolve these issues.

The following list includes general strategies and features to use in troubleshooting software configuration problems.

- **Review application settings** If an application suddenly fails, it is often the result of a configuration change. If you can open the application, proceed systematically through the available menus and configuration areas of the interface to see if any settings have been set improperly. If an application relies on a database or specific type of file (such as Microsoft Outlook, which relies on .pst files), then make sure that the database or file in question is accessible and not corrupted. If the application relies on a network resource, check network settings and ensure that the network resource is both accessible and available.

  During this phase of troubleshooting, you should also perform research on the Web about the issue experienced and contact the application manufacturer if necessary.

- **Using Event Viewer** As part of your troubleshooting process, you should use Event Viewer to find error messages related to the application you are troubleshooting. Event Viewer can help you determine when errors related to the application started appearing and ultimately help you determine the cause of failure. Pay special attention to the Application log and any logs that are specific to the application in question. Use the Filter Current Log function to locate only Critical, Warning, and Error messages. If you find errors that seem relevant, perform Web searches on these errors to learn more about them if necessary.
- **Using Event Forwarding** Troubleshooting a network-wide application issue might require you to review logs on multiple computers. To simplify this procedure, you can use *Event Forwarding*, a feature in which multiple computers are configured to forward a particular event to a collecting computer. Using the Event Forwarding feature requires that you configure both the forwarding computers, called the *source computers,* and the collecting computer, called the *collector*.

  To configure event forwarding, perform the following steps:

  1. On each source computer, type the following at an elevated command prompt:

     ```
     winrm quickconfig
     ```

  2. On the collector computer, type the following at an elevated command prompt:

     ```
     wecutil qc
     ```

  3. Add the computer account of the collector computer to the local Administrators group on each of the source computers.
  4. In Event Viewer on the collector computer, choose Create Subscription, and then follow the prompts to specify both the event you want to collect and the source computers on which you want to collect them.

> ***NOTE*** **EVENT FORWARDING REQUIRES CERTAIN SERVICES TO BE RUNNING**
>
> **Event forwarding depends on the Windows Remote Management (WinRM) service and the Windows Event Collector (Wecsvc) service. Both of these services must be running on computers participating in the forwarding and collecting process.**

- **System Restore** An application can fail because of changes to the operating system. If an application stops functioning after you install an update or make a system change, consider using the System Restore feature to revert the computer's configuration to a time when the application functioned properly. Although this feature does not remove or change user files such as documents or e-mail, it will remove any applications, updates, or system changes that have occurred since the system restore point.

> ***NOTE*** **OPENING SYSTEM RESTORE**
>
> **To start the System Restore Wizard, click Start, type system restore, and then press Enter.**

- **Repairing or reinstalling software** If software stops functioning but you cannot revert to an earlier state manually or automatically, you should attempt to repair the software in question. A repair option, if available, essentially reinstalls the application while preserving user files and settings for that application. If no such repair option is available, you can back up the user files and simply reinstall the software. To perform a fresh installation, you might need to uninstall the software first.
- **Restoring from backup** If a critical application fails but you cannot repair it by using any of the methods listed previously, you should restore the entire system from a backup of the last functioning version of the computer. Before doing so, be sure to perform a backup of the user's personal files and folders.

Understanding Application Compatibility

Each release of Windows includes new features and capabilities that affect how applications run. Before making adjustments to improve application compatibility, you should gain some understanding of the particular features in Windows 7 that are most likely to cause application compatibility problems. These particular features can generally be classified as security enhancements and operating system changes.

Security Enhancements Affecting Application Compatibility

Many organizations deploying Windows 7 will be replacing Windows XP on their clients, not Windows Vista. Compared to Windows XP, the Windows 7 environment offers a number of important security-related enhancements. The following security features are the ones most likely to lead to compatibility problems with third-party applications:

- **User Account Control** Introduced in Windows Vista, User Account Control (UAC) separates standard user privileges from administrator privileges in a way that helps reduce the effect of malware, unauthorized software installation, and unapproved system changes. If you are logged on as an administrator, UAC by default prompts you to confirm some tasks that you want to perform that require administrator privileges. If you are logged on as a standard user and attempt to perform a task that requires administrator privileges, UAC gives you an opportunity to enter administrator credentials instead of denying you the right to perform the task outright.

  UAC can introduce problems in applications that are not compliant with this technology enhancement. For this reason, it is important to test applications with UAC enabled before you deploy them.
- **Windows Resource Protection (also called File and Registry Virtualization)** *Windows Resource Protection* is a feature in Windows Vista and Windows 7 that intercepts any application requests to write to protected system files or registry locations and then redirects these requests to safe and temporary locations. Although most applications can handle this redirection without generating an error, some applications require full access to the protected areas and cannot handle the redirection process.

- **Internet Explorer Protected Mode** *Protected Mode* is a feature of Windows Internet Explorer 8 that protects computers from malware by restricting the browser's access within the registry and file system. Although Protected Mode helps maintain the integrity of client computers, it can affect the proper operation of older applications, ActiveX controls, and other script code.
- **Operating system and Internet Explorer versioning** Many applications check the version of the operating system and behave differently or fail to run when an unexpected version number is detected. You can resolve this issue by setting appropriate compatibility modes or applying versioning shims (application-compatibility fixes).

Operating System Changes Affecting Application Compatibility

Of the many operating system changes introduced by Windows 7, the following features are most likely to lead to application compatibility difficulties:

- **New system Application Programming Interfaces (APIs)** APIs expose layers of the Windows 7 operating system differently than they did in previous versions of Windows. Antivirus and firewall software are examples of applications that rely on these new APIs to monitor and protect Windows 7.

  Applications that relied on outdated APIs will need to be upgraded or replaced for Windows 7.
- **Windows 7 64-bit** Neither 16-bit applications nor 32-bit drivers are supported in the Windows 7 64-bit environment. The automatic registry and system file redirection that allows some older applications to function in the 32-bit version of Windows 7 are not available for the 64-bit environment. For these reasons, new 64-bit applications must comply fully with Windows 7 application standards.
- **Operating system version** Many older applications check for a specific version of Windows and stop responding when they fail to find this specific version. Features built into Windows 7 such as the Program Compatibility Assistant (discussed in the next section) can usually resolve this type of issue automatically.
- **New folder locations** User folders, My Documents folders, and folders with localization have changed since Windows XP. Applications with hard-coded paths may fail.

Using Windows 7 Built-in Compatibility Tools

Although you should perform extensive application compatibility testing before you deploy Windows 7, compatibility problems may unexpectedly appear or persist after deployment. To help you improve the compatibility of older programs after deployment, Windows 7 provides three tools: the Program Compatibility Assistant (PCA), the Program Compatibility Troubleshooter, and the Compatibility tab in a program's Properties dialog box.

- **PCA** The PCA is a tool that automatically appears when Windows 7 detects known compatibility issues in older programs. When it does appear, the PCA can offer to fix the problem. For example, the PCA can resolve conflicts with UAC, or it can run the program in a mode that simulates earlier versions of Windows. If you agree to the changes PCA proposes, these changes are then performed automatically. Alternatively,

if the compatibility issue detected is serious, the PCA can warn you or block the program from running.

When the PCA recognizes a problem but cannot offer a fix, it will give you an option to check online for possible solutions, as shown in Figure 9-10.

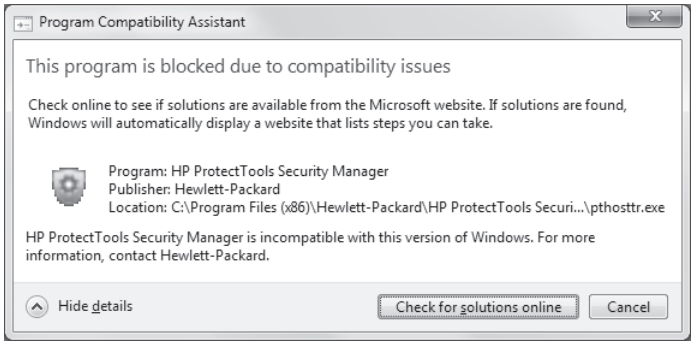


FIGURE 9-10 The PCA triggers a message when a program incompatibility is found.

- **Program Compatibility Troubleshooter** The Program Compatibility Troubleshooter is a Control Panel program that you can use to configure the compatibility settings for an older program if you notice that the program is not running smoothly. For example, you can configure the program to run in a simulated environment of a previous version of Windows, to run with specific display settings, or to run with Administrator privileges.

  To start the wizard, in Control Panel, first click Programs, and then, in the Programs and Features category, click Run Programs Made For Previous Versions Of Windows. You can also start the Program Compatibility Troubleshooter by right-clicking an application and selecting Troubleshoot Compatibility from the shortcut menu, as shown in Figure 9-11.

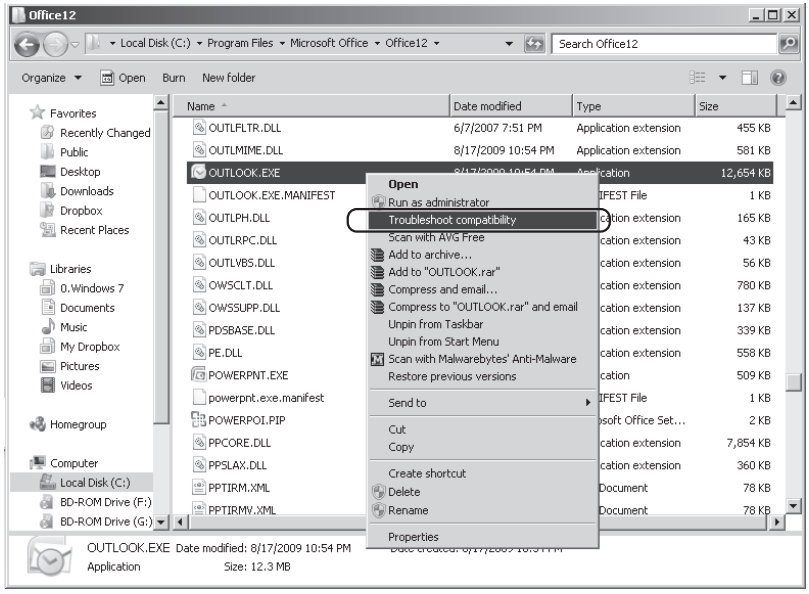


FIGURE 9-11 Launching the Program Compatibility Troubleshooter

A page of the Program Compatibility Troubleshooter is shown in Figure 9-12.

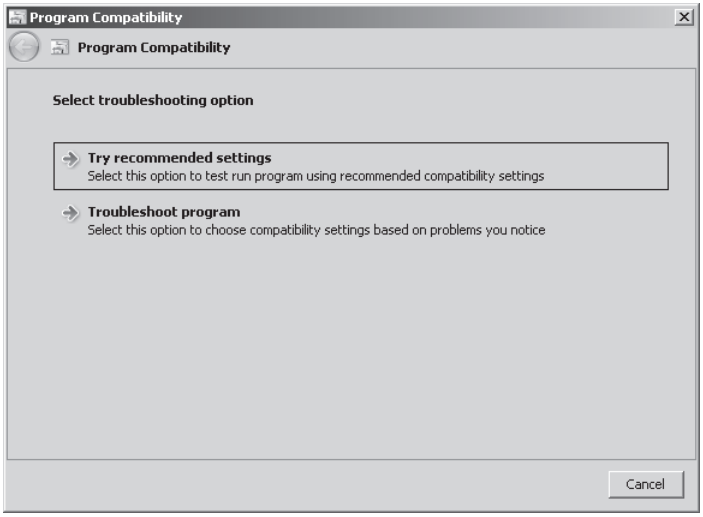


FIGURE 9-12 The Program Compatibility Troubleshooter

- **Compatibility Tab** As an alternative to running the Program Compatibility Troubleshooter, you can simply configure compatibility settings on the Compatibility tab within the Properties sheet of any given program. The options provided on this tab are the same as those you can configure through the Program Compatibility Troubleshooter. The Compatibility Tab is shown in Figure 9-13.

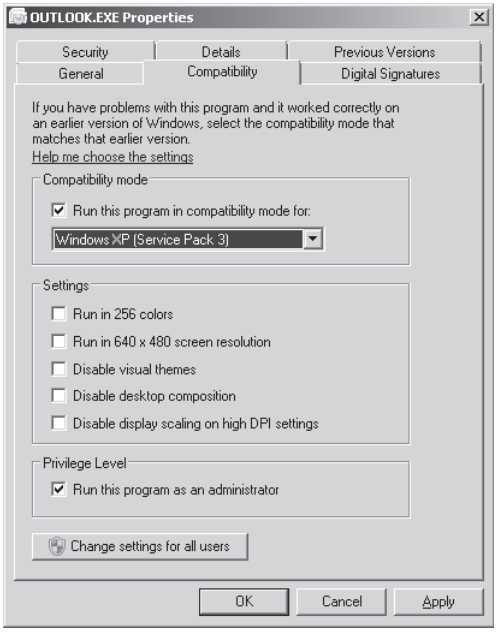


FIGURE 9-13 The Compatibility tab of an application

Note that adjusting the compatibility settings of a program does not always fix the problem. If issues persist, you should attempt alternate hosting or obtain an updated version of the program.

Alternate Hosting for Application Compatibility

In some cases, your organization will need to support an application whose compatibility issues with Windows 7 cannot be resolved immediately. For example, if you are running a 64-bit version of Windows 7, you cannot run 16-bit applications by merely adjusting the compatibility settings of the program. Until a newer, more compatible version of the application appears (or until your organization finds an alternate application), you must find a temporary fix for the application compatibility problem.

The most common temporary fix for unresolved application compatibility problems such as this is simply to run the program within the old operating system in a virtual machine, on a remote server that can be accessed through Remote Desktop, or both.

The following list describes various options of hosting an older application on an older operating system:

- **Microsoft Virtual PC 2007** You can use Virtual PC to run applications that function properly only with older versions of Windows. For example, if your organization needs to support a 16-bit application within a 64-bit version of Windows 7, you can use Virtual PC 2007 to run the program within a virtual machine running a previous version of Windows. Although virtual machine software such as Virtual PC is required to run 16-bit applications in 64-bit versions of Windows 7, the use of Virtual PC need not be reserved only for this purpose. Virtual PC also lets users keep a previous version of Windows until upgraded versions of older applications are developed. Whenever you need to support an older application that does not run smoothly in Windows 7 and that cannot be upgraded, you should consider running the application inside a virtual machine.
- **Windows XP Mode** *Windows XP Mode* is essentially a downloadable enhancement to Virtual PC that is available in Windows 7 Professional, Enterprise, and Ultimate. Windows XP Mode also requires special virtualization technology. Specifically, Windows XP Mode requires a CPU with Intel-VT or AMD-V technology, and this technology must be enabled in the BIOS.

  For eligible computers, Windows XP Mode enables you to access through the Start menu in Windows 7 any applications installed in a Windows XP guest virtual machine in Virtual PC. You then interact with these applications exactly as if they were installed natively in Windows 7. Windows XP Mode also provides an enormous performance advantage: It gives the Windows XP guest operating system direct access to the system hardware, so performance is much better than it is in Virtual PC alone.

  To install Windows XP Mode is easy: First download and install Virtual PC, and then download and install Windows XP Mode. You can perform both tasks from the Virtual PC Web site at *http://www.microsoft.com/windows/virtual-pc/download.aspx*. (Both Virtual PC and Windows XP Mode are free.)

MORE INFO **WINDOWS XP MODE**

For step-by-step instructions on using Windows XP Mode, including installing and using applications, visit *http://www.microsoft.com/windows/virtual-pc/support/default.aspx*. You can also view a five-minute introduction to Windows XP Mode at *http://windows.microsoft.com/en-us/windows7/help/videos/using-windows-xp-mode*.

- **Hyper-V on Windows Server 2008** Hyper-V is a high-performance virtualization environment available in Windows Server 2008. It allows you to create guest virtual machines with direct access to the hardware. On the virtual machines, you can install any version of Windows.

  If you choose to host an application on a virtual machine inside Hyper-V, clients running Windows 7 or other operating systems can then connect remotely to this application from over the network.

  Hyper-V requires a 64-bit processor with virtualization technology (Intel-VT or AMD-V).
- **Remote Desktop Services for Hosting Applications** Hosting older applications on Remote Desktop Services lets you deliver Windows-based applications or the Windows desktop itself to virtually any computer device on your network. Clients running Windows 7 can connect to these application-hosting environments through Remote Desktop.

✔ Quick Check

- **Which CPU technology must be available to use Windows XP Mode on a client running Windows 7?**

Quick Check Answer

- **Intel-VT or AMD-V**

Understanding the Application Compatibility Toolkit (ACT)

The Application Compatibility Toolkit (ACT) is a tool you can use to identify application compatibility issues before Windows 7 deployment.

The following are some of the major components that make up the ACT solution:

- **Application Compatibility Manager** A tool that enables you to collect and analyze your data so that you can identify any issues prior to deploying a new operating system or deploying a Windows update in your organization. You use this program heavily during the initial phases of an application migration project. Consider this tool as the primary user interface for ACT.

- **Application Compatibility Toolkit Data Collector** The Application Compatibility Toolkit Data Collector is distributed to each computer. It then performs scans by using compatibility evaluators. Data is collected and stored in the central compatibility database.
- **Setup Analysis Tool (SAT)** The SAT automates the running of application installations while monitoring the actions taken by each application's installer.
- **Standard User Analyzer (SUA)** The SUA determines the possible issues for applications running as a standard user in Windows 7.

ACT is an important tool for testing applications across a wide variety of computers and operating systems within your organization.

Configuring Application Compatibility Diagnostics Through Group Policy

Windows Server 2008 includes a set of policy options related to application compatibility diagnostics. To browse these settings in a GPO, browse to Computer Configuration\Policies\Administrative Templates\System\Troubleshooting And Diagnostics\Application Compatibility Diagnostics.

The Application Compatibility Diagnostics container includes the following six policies:

- **Notify Blocked Drivers** This policy setting determines whether the PCA will notify the user if drivers are blocked because of compatibility issues. If you enable this policy setting, the PCA notifies the user of blocked driver issues and provides the user with an option to check the Microsoft Web site for solutions. (This behavior is also the default behavior in Windows 7.) If you disable this policy setting, the PCA does not notify the user of blocked driver issues. Note that if this policy setting is configured as disabled, the user is not presented with solutions to blocked drivers.
- **Detect Application Failures Caused By Deprecated Windows COM Objects** This policy setting determines whether the PCA will notify the user when a COM object creation failure is detected in an application. If you enable this policy setting, the PCA detects programs creating older COM objects that are removed in this version of Windows. (This behavior is also the default behavior in Windows 7.) When this failure is detected, after the program is terminated, PCA notifies the user about this problem and provides an option to check the Microsoft Web site for solutions. If you disable this policy setting, the PCA does not detect programs creating older COM objects.
- **Detect Application Failures Caused By Deprecated Windows DLLs** This policy setting determines whether the PCA will notify the user when a DLL load failure is detected in an application. If you enable this policy setting, the PCA detects programs trying to load older Microsoft Windows DLLs that are removed in this version of Windows. (This behavior is also the default behavior in Windows 7.) When this failure is detected, PCA notifies the user about this problem after the program is terminated and provides an option to check the Microsoft Web site for solutions. If you disable this policy setting, the PCA does not detect programs trying to load older Windows DLLs.

- **Detect Application Install Failures** This policy setting configures the PCA to notify the user when an application installation has failed. If you enable this policy setting, the PCA detects application installation failures and provides the user with an option to restart the installer in Windows XP compatibility mode. (This behavior is also the default behavior in Windows 7.) If you disable this policy setting, the PCA does not detect program installation failures.
- **Detect Application Installers That Need To Be Run As Administrator** This policy setting determines whether the PCA will notify the user when application installations have failed because they need to be run as an administrator. If you enable this policy setting, the PCA detects such installation failures and provides the user with an option to restart the installer programs as an administrator. (This behavior is also the default behavior in Windows 7.) If you disable this policy setting, the PCA does not notify users when installer program failures have occurred for this reason.
- **Detect Applications Unable To Launch Installers Under UAC** This policy setting configures the PCA to notify the user when UAC is preventing an application from launching an installer (typically an updater program). If you enable this policy setting, the PCA detects programs that fail to start installers and grants administrator privileges that allow this task to be performed the next time the program is run. (This behavior is also the default behavior in Windows 7.) If you disable this policy setting, the PCA does not detect applications that fail to launch installers run under UAC.

EXAM TIP

You need to understand these application compatibility diagnostics Group Policy settings for the 70-685 exam.

PRACTICE Configuring Application Compatibility Diagnostics

In this exercise, you configure application compatibility settings in Group Policy.

EXERCISE Creating a Policy for Application Compatibility Settings

In this exercise, you create a new GPO named Application Compatibility Diagnostics Policy. In the GPO, you enable two settings that enable particular behaviors in the PCA.

1. Log on to the domain controller as a domain administrator.
2. Click Start, type **Group Policy Management**, and then click OK. The Group Policy Management console opens.
3. In the Group Policy Management console tree, expand Forest: nwtraders.msft and then Domains.
4. Beneath the Domains container, select and right-click the Nwtraders.msft icon, and then click the option to Create A GPO In This Domain, And Link It Here. The New GPO dialog box opens.

5. In the New GPO dialog box, type **Application Compatibility Diagnostics Policy**, and then click OK.
6. In the Details pane of the Group Policy Management console, ensure that the Linked Group Policy Objects tab is selected. Then, in the list of GPOs, right-click Application Compatibility Diagnostics Policy, and then click Edit. A Group Policy Management Editor window opens.
7. In the console tree of the Group Policy Management Editor, navigate to Computer Configuration\Policies\Administrative Templates\System\Troubleshooting and Diagnostics\Application Compatibility Diagnostics.
8. In the details pane of the Group Policy Management Editor, double-click the policy named Detect Application Failures Caused By Deprecated Windows DLLs. The associated policy setting Properties dialog box opens.
9. Read the description of the policy setting. Note that the Diagnostic Policy Service and the Program Compatibility Assistant Service must be running on Windows 7 for the Program Compatibility Assistant to execute. These services run by default on domain-joined computers running Windows 7.
10. Click Enabled.
11. In the Scenario Execution Level drop-down list box, ensure that Detection, Troubleshooting, And Resolution is selected.
12. Click OK. In the details pane of the Group Policy Management Editor, the policy setting should now appear as Enabled.
13. In the details pane of the Group Policy Management Editor, double-click the policy setting named Detect Application Install Failures. The associated policy setting Properties dialog box opens.
14. Read the description of the policy setting, and then click Enabled.
15. Click OK. In the details pane of the Group Policy Management Editor, the policy setting should now appear as Enabled.
16. Close all open windows.

Lesson Summary

- If an application malfunctions after it has been working correctly, the problem is usually a result of a configuration error or a system change. To discover or undo the error, you should use a variety of strategies, such as reviewing application settings, reviewing event logs, using System Restore, repairing or reinstalling the application, and restoring the system from backup.
- Each new release of Windows introduces features that affect the functionality of programs written for earlier operating systems. With Windows 7, the features most likely to affect application compatibility include UAC, Windows Resource Protection, and new system APIs.

- Windows 7 includes tools that help detect and mitigate compatibility problems for older applications. The PCA automatically appears when Windows 7 detects known compatibility issues. The Program Compatibility Troubleshooter is a wizard that enables you to run an older program with settings used in a previous version of Windows. You can configure these same compatibility settings on the Compatibility Tab of the program.
- If you need to support an application that is not compatible with Windows 7, you can run the program in a compatible operating system within a virtual machine. Alternatively, you can use a Remote Desktop connection to a computer running the application and a compatible operating system.
- Windows 7 includes several Group Policy settings that allow you to determine how the PCA will diagnose and troubleshoot application compatibility problems.

Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 2, "Resolving Software Configuration and Compatibility Issues." The questions are also available on the companion CD if you prefer to review them in electronic form.

NOTE **ANSWERS**

Answers to these questions and explanations of why each answer choice is correct or incorrect are located in the "Answers" section at the end of the book.

1. You receive a call from the help desk about a user who is experiencing problems with an application on a computer running Windows 7. The application was functioning well until the user installed an optional update to Windows. She has made no other changes to the system since. Now, however, she is unable to start the application. Unfortunately, neither she nor the help desk staff has been able to return the application to its original functioning state.

   Which of the following steps should you take to solve the problem?

   A. Use the System Restore feature to return the computer to the point in time just before the user installed the optional update to Windows.

   B. Restore her user files from the latest backup.

   C. Configure Event Forwarding to forward messages in the application log to your computer.

   D. Uninstall and reinstall the application.

2. After upgrading the client computers in your organization from Windows XP to Windows Vista, you discover that a certain application installs without error but no longer runs properly in the new operating system. How can you ensure that users will receive any possible notifications telling them why the application has failed?

   A. In Group Policy, enable the Detect Application Failures Caused By Deprecated Windows DLLs Or COM Objects policy.

   B. In Group Policy, enable the Notify Blocked Drivers policy.

   C. In Group Policy, enable the Detect Application Install Failures policy.

   D. In Group Policy, enable the Detect Application Installers That Need To Be Run As Administrator policy.

3. Which of the following applications is least likely to run on the 32-bit version of Windows 7 without a software update?

   A. A 16-bit application written for Microsoft Windows 2000

   B. A 32-bit application written for Windows XP that requires administrative privileges to run properly

   C. An application written for Windows 2000 that writes to a protected area of the registry

   D. An application written for Windows XP that writes to protected system files

Chapter Review

To further practice and reinforce the skills you learned in this chapter, you can perform the following tasks:

- Review the chapter summary.
- Review the list of key terms introduced in this chapter.
- Complete the case scenarios. These scenarios set up real-world situations involving the topics of this chapter and ask you to create a solution.
- Complete the suggested practices.
- Take a practice test.

Chapter Summary

- To troubleshoot installation issues, verify administrator rights, Windows 7 compatibility, installation settings, application constraints and dependencies, resource availability, and any policy restrictions set in SRP or AppLocker.
- Applications can fail because of an improper configuration or because of a fundamental compatibility issue with Windows 7. For configuration issues, first attempt to identify and fix the problem manually, but if necessary, you can use System Restore, software repair, or system backups to resolve the issue. For compatibility issues, you can modify the program's compatibility settings, find a remote or virtual older host for the application, or simply upgrade your software to a newer version that is compatible with Windows 7.

Key Terms

Do you know what these key terms mean? You can check your answers by looking up the terms in the glossary at the end of the book.

- **Event Forwarding** A feature in which multiple source computers on a network are configured to forward particular events to a single collector computer.
- **Windows Resource Protection** A feature of Windows Vista and Windows 7 in which requests by programs to write to protected areas of the operating system are intercepted and redirected to safe areas.
- **Windows XP Mode** In Windows 7, a downloadable enhancement to Virtual PC in which you can access and interact with programs transparently in a guest Windows XP virtual machine. Windows XP Mode requires a CPU with Intel-VT or AMD-V technology.

Case Scenarios

In the following case scenarios, you apply what you've learned about protecting client systems. You can find answers to these questions in the "Answers" section at the end of this book.

Case Scenario 1: Restricting Software with AppLocker

You work as an enterprise support technician in a large company whose network consists of a single AD DS domain. All the clients in the company are running Windows 7, and all the domain controllers are running Windows Server 2008 R2.

You want to use AppLocker to allow users to run Windows Installer programs from Microsoft. You also want to prevent them from running Windows Installer programs from other companies. You begin by creating a new GPO and linking it to the domain.

With this scenario in mind, answer the following questions:

1. You are creating a Windows Installer rule in the new GPO. What kind of rule condition should you specify if you want to allow Windows Installer programs from Microsoft to be run?
2. You successfully create a Windows Installer rule that allows everyone to run .msi files from Microsoft. You have not created any default rules. If the GPO is enforced without making further changes, will users be able to run Windows Installer programs created by other companies? Why or why not?

Case Scenario 2: Configuring Application Compatibility Settings

You work as an enterprise support technician for Contoso, Inc. The Contoso network includes 20 computers running Windows Server 2008 R2, 150 client computers running Windows XP Professional, and 100 client computers on which Windows 7 Professional has been installed recently.

You currently are handling issues related to application compatibility on the clients running Windows 7.

With this scenario in mind, answer the following questions:

1. A certain application used infrequently by the Advertising department was written for Windows XP. Users report that the application is unstable in Windows 7. Assuming that no updates for the application are yet available, what is the first remedy that you should investigate?
2. Users report that sometimes applications fail to install, but that they receive no notification about the failure. What can you do to ensure that users receive notification when applications fail to install?

Suggested Practices

To help you master the exam objectives presented in this chapter, complete the following tasks.

Identify and Resolve New Software Installation Issues

Perform the following activities to learn to resolve common installation issues:

- **Practice 1** Attempt to install on Windows 7 an older program that was written for Windows XP or Windows 2000. If the installation fails, run the installation as an administrator and see if it succeeds.
- **Practice 2** In a test domain, obtain a certificate from a third-party software publisher. Use Group Policy to deploy that certificate to the Trusted Publishers certificate store on all clients in the domain.

Identify and Resolve Software Configuration Issues

Perform the following activity to learn to troubleshoot many computers on a network:

- **Practice 1** In a test domain, enable Event Forwarding on multiple source computers. Enable Event Forwarding on the collector computer, and then specify a common error to collect in order to test the results.

Identify Cause of and Resolve Software Failure Issues

Perform the following activity to learn one way to resolve an application compatibility issue:

- **Practice 1** On a computer whose CPU includes Intel-VT or AMD-V technology, enable that feature in the BIOS. Then, download and install Virtual PC, and then download and install Windows XP Mode. Use Windows XP Mode to access applications installed in a virtual machine from the Start menu of Windows 7.

Take a Practice Test

The practice tests on this book's companion CD offer many options. For example, you can test yourself on just one exam objective, or you can test yourself on all the 70-685 certification exam content. You can set up the test so that it closely simulates the experience of taking a certification exam, or you can set it up in study mode so that you can look at the correct answers and explanations after you answer each question.

MORE INFO **PRACTICE TESTS**

For details about all the practice test options available, see the section entitled "How to Use the Practice Tests," in the Introduction to this book.

Index

Symbols and Numbers

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

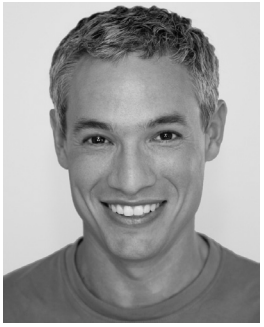
T

U

V

W

About the Authors



TONY NORTHRUP, MVP, MCSE, MCTS, and CISSP, is a Microsoft Windows consultant and author living in New London, Connecticut. Tony started programming before Microsoft Windows 1.0 was released, but he has focused on Windows administration and development for the last 15 years. He has written about 25 books covering Windows development, networking, and security. Among other titles, Tony is coauthor of *Windows 7 Resource Kit, Windows Vista Resource Kit,* and *Windows Server 2008 Networking and Network Access Protection (NAP)*.

When he's not writing, Tony enjoys photography and travel. Tony lives with his girlfriend, Chelsea, her daughter, Madelyn, and three dogs. You can learn more about Tony by visiting his personal Web site at *http://www.northrup.org* and his technical blog at *http://www.vistaclues.com*.

J.C. MACKIN, MCITP, MCTS, MCSE, MCDST, and MCT, is a consultant, trainer, and writer who has been working with Microsoft networks since Microsoft Windows NT 4.0. He is author or coauthor of many Microsoft Press Self-Paced Training Kits (including those for exams 70-291, 70-642, and 70-643) and of the *Windows Essential Business Server 2008 Administrator's Companion*. When he's not working with computers, J.C. can be found with a camera wandering the streets of small medieval towns in Europe.