RICK McDONALD

Cert Guide

Learn, prepare, and practice for exam success

CompTIA® A+

Core 1 (220-1001)
Core 2 (220-1002)

Fifth Edition

PEARSON IT CERTIFICATION

CompTIA® A+ Core 1 (220-1001) and Core 2 (220-1002) Cert Guide

Fifth Edition

Rick McDonald

Pearson

CompTIA® A+ Core 1 (220-1001) and Core 2 (220-1002) Cert Guide

Fifth Edition

Rick McDonald

Published by:
Pearson Education
221 River Street
Hoboken, NJ 07030

ISBN-13: 978-0-7897-6051-7

ISBN-10: 0-7897-6051-7

Library of Congress Control Number: 2019908201

ScoutAutomatedPrintCode

Warning and Disclaimer

This book is designed to provide information about the CompTIA Core 1 (220-1001) and Core 2 (220-1002) A+ exams. Every effort has been made to make this book as complete and accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the supplemental online content or programs accompanying it.

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose all such documents and related graphics are provided "as is" without warranty of any kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services.

The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screen shots may be viewed in full within the software version specified.

Microsoft® Windows®, and Microsoft Office® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

Editor-in-Chief
Mark Taub

Product Line Manager
Brett Bartow

Acquisitions Editor
Paul Carlstroem

Managing Editor
Sandra Schroeder

Development Editor
Christopher Cleveland

Project Editor
Mandie Frank

Copy Editor
Kitty Wilson

Technical Editors
Chris Crayton

Editorial Assistant
Cindy Teeters

Designer
Chuti Prasertsith

Composition
codeMantra

Indexer
Ken Johnson

Proofreader
Abigail Manheim

Credits

Figure Number	Attribution/Credit Line
Chapter Opener Images	Charlie Edwards/Getty Images
Figure 1-1	Rick McDonald
Figure 1-2	Rick McDonald
Figure 1-3	Rick McDonald
Figure 1-4	Rick McDonald
Figure 1-5	Rick McDonald
Figure 1-6	Rick McDonald
Figure 1-7a	Rick McDonald
Figure 1-7b	Scanrail/123RF
Figure 1-8	Rick McDonald
Figure 1-9	Rick McDonald
Figure 1-10	Rick McDonald
Figure 1-11a	Rick McDonald
Figure 1-11b	Rick McDonald
Figure 1-12	Rick McDonald
Figure 1-13	Rick McDonald
Figure 1-14	Rick McDonald
Figure 1-15	Rick McDonald
Figure 1-16	Rick McDonald
Figure 1-17	Rick McDonald
Figure 1-18	Rick McDonald
Figure 1-19	Rick McDonald
Figure 1-20	Rick McDonald
Figure 1-21	Rick McDonald
Figure 1-22	Rick McDonald
Figure 1-23	Rick McDonald
Figure 1-24	Rick McDonald
Figure 1-25	Rick McDonald
Figure 1-26	Rick McDonald
Figure 1-27	Rick McDonald
Figure 1-28a	Rick McDonald
Figure 1-28b	Rick McDonald
Figure 1-29	Rick McDonald
Figure 2-1	Rick McDonald
Figure 2-2	Rick McDonald
Figure 2-3a	Rick McDonald
Figure 2-3b	Rick McDonald
Figure 2-4	Rick McDonald
Figure 2-5	Screenshot of Microsoft Windows © Microsoft 2019
Figure 2-6	Courtesy of Cisco Systems, Inc.
Figure 2-7	Courtesy of Cisco Systems, Inc.
Figure 2-8	Screenshot of Microsoft Windows © Microsoft 2019
Figure 2-9	Es sarawuth/Shutterstock
Figure 2-13	Screenshot reprinted with permission from Apple Inc.
Figure 2-14	Screenshot of Linux © Linux Kernel Organization, Inc.

Figure 2-17	Rick McDonald
Figure 2-18	Rick McDonald
Figure 2-19	Rick McDonald
Figure 2-20	Fotosv/Shutterstock
Figure 2-21	Rick McDonald
Figure 2-22	Screenshot of inSSIDer © 2005-2019 MetaGeek, LLC.
Figure 2-23	Rick McDonald
Figure 3-1	Rick McDonald
Figure 3-2	Rick McDonald
Figure 3-3	Rick McDonald
Figure 3-3a	Rick McDonald
Figure 3-3b	Rick McDonald
Figure 3-3c	Rick McDonald
Figure 3-5	Rick McDonald
Figure 3-6	Rick McDonald
Figure 3-7	Rick McDonald
Figure 3-8	Rick McDonald
Figure 3-9	Rick McDonald
Figure 3-10	Rick McDonald
Figure 3-11	Rick McDonald
Figure 3-12	Rick McDonald
Figure 3-13	Rick McDonald
Figure 3-13a	Rick McDonald
Figure 3-14	Rick McDonald
Figure 3-15	Rick McDonald
Figure 3-16	Rick McDonald
Figure 3-17	Rick McDonald
Figure 3-18	Rick McDonald
Figure 3-19	Rick McDonald
Figure 3-20	Rick McDonald
Figure 3-21	Rick McDonald
Figure 3-22	Kaspri/Shutterstock
Figure 3-23	Rick McDonald
Figure 3-24	Rick McDonald
Figure 3-24a	Rick McDonald
Figure 3-25	Rick McDonald
Figure 3-26	Rick McDonald
Figure 3-27	Rick McDonald
Figure 3-28	Rick McDonald
Figure 3-29	Rick McDonald
Figure 3-30	Rick McDonald
Figure 3-31	JIPEN/Shutterstock
Figure 3-32	Andrush/Shutterstock
Figure 3-33	Rick McDonald
Figure 3-34	Rick McDonald
Figure 3-35	Rick McDonald
Figure 3-36	Rick McDonald
Figure 3-37	Rick McDonald
Figure 3-38	Screenshot of Microsoft Windows © Microsoft 2019
Figure 3-39	Screenshot of BIOS © 2011 American Megatrends, Inc.

Figure 3-40	Screenshot of Rapid storage technology © 2003-10 Intel Corporation
Figure 3-41	Screenshot of RAID 1 array © 2003-10 Intel Corporation
Figure 3-42	Screenshot of Microsoft Windows © Microsoft 2019
Figure 3-43	Screenshot reprinted with permission from Apple Inc.
Figure 3-44	Rick McDonald
Figure 3-45	Rick McDonald
Figure 3-46	Rick McDonald
Figure 3-47	Rick McDonald
Figure 3-49	Rick McDonald
Figure 3-49a	Rick McDonald
Figure 3-50	Rick McDonald
Figure 3-51	Rick McDonald
Figure 3-52	Rick McDonald
Figure 3-53	Rick McDonald
Figure 3-54	Rick McDonald
Figure 3-55	Rick McDonald
Figure 3-56	Rick McDonald
Figure 3-57	Rick McDonald
Figure 3-58	Rick McDonald
Figure 3-59	Rick McDonald
Figure 3-60	Screenshot of BIOS © 2011 American Megatrends, Inc.
Figure 3-61	Screenshot of BIOS © 2011 American Megatrends, Inc.
Figure 3-62	Screenshot of BIOS © 2011 American Megatrends, Inc.
Figure 3-63	Screenshot of Microsoft Windows © Microsoft 2019
Figure 3-64	Screenshot of BIOS © 2011 American Megatrends, Inc.
Figure 3-67	Screenshot Configuring network © 2016 BIOSTAR Group
Figure 3-68	Rick McDonald
Figure 3-69	Screenshot of BIOS © 2011 American Megatrends, Inc.
Figure 3-70	Screenshot of BIOS © 2011 American Megatrends, Inc.
Figure 3-71	Screenshot Configuring network © 2016 BIOSTAR Group
Figure 3-72	Screenshot of GPU-Z reports © 2019 Techpowerup
Figure 3-73a	S.Rimkuss/Shutterstock
Figure 3-73b	RMIKKA/Shutterstock
Figure 3-74	Rick McDonald
Figure 3-74a	Rick McDonald
Figure 3-76	Rick McDonald
Figure 3-77	Rick McDonald
Figure 3-77a	Rick McDonald
Figure 3-78	Rick McDonald
Figure 3-79	Rick McDonald
Figure 3-79a	Rick McDonald
Figure 3-80	Rick McDonald
Figure 3-81	Rick McDonald
Figure 3-81a	Rick McDonald
Figure 3-82	Rick McDonald
Figure 3-83	Rick McDonald
Figure 3-84	Rick McDonald
Figure 3-85	Rick McDonald
Figure 3-86	Rick McDonald
Figure 3-87	Rick McDonald

Figure 3-88	Rick McDonald
Figure 3-89	Screenshot of Bluetooth devices to computer © Microsoft 2019
Figure 3-90	Screenshot of Bluetooth devices to computer © Microsoft 2019
Figure 3-91	Screenshot of Webcam properties © Microsoft 2019
Figure 3-92	Screenshot of Audio mixers © Microsoft 2019
Figure 3-93	Rick McDonald
Figure 3-94	Rick McDonald
Figure 3-95	Rick McDonald
Figure 3-96	Rick McDonald
Figure 3-96a	Rick McDonald
Figure 3-96b	Rick McDonald
Figure 3-96c	Rick McDonald
Figure 3-97	Rick McDonald
Figure 3-97a	Rick McDonald
Figure 3-98	Rick McDonald
Figure 3-99	Rick McDonald
Figure 3-99a	Rick McDonald
Figure 3-100	Rick McDonald
Figure 3-102	Screenshot of CPU-Z © 2019 CPUID
Figure 3-103	Rick McDonald
Figure 3-104	Scanrail/123RF
Figure 3-105	Screenshot of Windows 10 © Microsoft 2019
Figure 3-106	Screenshot of print server setup dialogs © 2019 Epson America, Inc.
Figure 3-107	Screenshot reprinted with permission from Apple Inc.
Figure 3-110	Rick McDonald
Figure 3-111	Screenshot of printer properties dialog © 2019 Epson America, Inc.
Figure 3-112	Screenshot of printer properties dialog © 2019 Epson America, Inc.
Figure 3-113	Screenshot of Maintenance tab © Microsoft 2019
Figure 3-114	Rick McDonald
Figure 3-116	Rick McDonald
Figure 3-118	Rick McDonald
Figure 3-118a	Rick McDonald
Figure 3-119	asharkyu/Shutterstock
Figure 3-120	Rick McDonald
Figure 3-120a	Rick McDonald
Figure 3-121	Rick McDonald
Figure 3-122	Rick McDonald
Figure 3-123	Rick McDonald
Figure 3-124	Rick McDonald
Figure 3-125	Rick McDonald
Figure 3-125a	Rick McDonald
Figure 3-125b	Rick McDonald
Figure 3-126	Rick McDonald
Figure 3-127	Rick McDonald
Figure 3-127a	Rick McDonald
Figure 3-128	Rick McDonald
Figure 3-128a	Rick McDonald
Figure 3-129	Rick McDonald
Figure 3-130	Screenshot of Printed tab © Microsoft 2019
Figure 4-1	Zern Liew/Shutterstock

Figure 4-2	Screenshot of Google docs © 2019 Google
Figure 4-3	Screenshot of Virtual VM VirtualBox © Oracle
Figure 4-4	Screenshot of Hyper-V Manager © Microsoft 2019
Figure 4-5	Screenshot of Windows © Microsoft 2019
Unnumbered Figure 4-1	Screenshot of Virtual VM VirtualBox © Oracle
Figure 5-1	Screenshot of memory speed and timings © 2016 BIOSTAR Group
Figure 5-2	Rick McDonald
Figure 5-3	Rick McDonald
Figure 5-4	Screenshot of Startup and Recovery © Microsoft 2019
Figure 5-5	Screenshot of BIOS © 2011 American Megatrends, Inc.
Figure 5-6	Rick McDonald
Figure 5-7	Rick McDonald
Figure 5-8	Rick McDonald
Figure 5-9	Rick McDonald
Figure 5-10	Rick McDonald
Figure 5-11	Screenshot of Windows 7 © Microsoft 2019
Figure 5-12	Screenshot of Windows 8 and Windows 10 STOP error © Microsoft 2019
Figure 5-13	Screenshot reprinted with permission from Apple Inc.
Figure 5-14	Screenshot of Windows (10) Event Viewer © Microsoft 2019
Figure 5-16	Rick McDonald
Figure 5-18	Rick McDonald
Figure 5-19a	Matee Nuserm/Shutterstock
Figure 5-19b	Andrush/Shutterstock
Figure 5-20	Rick McDonald
Figure 5-21	Rick McDonald
Figure 5-22	Rick McDonald
Figure 5-23	Rick McDonald
Figure 5-24	Screenshot of Windows 7 © Microsoft 2019
Figure 5-25	Screenshot of Windows 8.1 © Microsoft 2019
Figure 5-26	Screenshot of Windows 8.1 © Microsoft 2019
Figure 5-27	Screenshot of Windows 10 © Microsoft 2019
Figure 5-28	Rick McDonald
Figure 5-29	Rick McDonald
Figure 5-30	Rick McDonald
Figure 5-31	Screenshot of Layout Advanced Graphics © Microsoft 2019
Figure 5-32	Screenshot of printer properties dialog © 2019 Epson America, Inc.
Figure 5-33	Screenshot of Maintenance tab © Microsoft 2019
Figure 5-34	Screenshot of Windows 10 © Microsoft 2019
Figure 5-35	Screenshot of Windows 10 © Microsoft 2019
Figure 5-36	Screenshot of Windows 7 © Microsoft 2019
Figure 5-37	Screenshot of Windows 7 © Microsoft 2019
Unnumbered Figure 5-1	Rick McDonald
Unnumbered Figure 5-2	Rick McDonald
Unnumbered Figure 5-3	Rick McDonald
Figure 6-1	Screenshot of File system formatting options © Microsoft 2019
Figure 6-2	Screenshot reprinted with permission from Apple Inc.
Figure 6-3	Screenshot of Mint Desktop © Linux Mint Team
Figure 6-6	Screenshot reprinted with permission from Apple Inc.
Figure 6-8	Screenshot of BIOS © 2011 American Megatrends, Inc.
Figure 6-9	Screenshot of Sysprep Tool © Microsoft 2019

Figure 6-10	Screenshot of Recovery window © Microsoft 2019
Figure 6-11	Screenshot of Windows 8.1 Installation © Microsoft 2019
Figure 6-12	Screenshot of Installation dialog © Microsoft 2019
Figure 6-13	Screenshot of A hard drive formatted © Microsoft 2019
Figure 6-14	Screenshot of Command prompt from the Windows 8/8.1 © Microsoft 2019
Figure 6-15	Screenshot of Windows 10 Command Prompt © Microsoft 2019
Figure 6-16	Screenshot of Help command © Microsoft 2019
Figure 6-17	Screenshot of Selecting Run as administrator © Microsoft 2019
Figure 6-18	Screenshot of Format menu © Microsoft 2019
Figure 6-19	Screenshot of DISKPART commands © Microsoft 2019
Figure 6-20	Screenshot of SFC /scannow reports © Microsoft 2019
Figure 6-21	Screenshot of Windows 7's Performance monitor © Microsoft 2019
Figure 6-22	Screenshot of Services dialog © Microsoft 2019
Figure 6-23	Screenshot of Services dialog © Microsoft 2019
Figure 6-24	Screenshot of Windows 7 Task Scheduler © Microsoft 2019
Figure 6-25	Screenshot of Windows 7 Task Scheduler © Microsoft 2019
Figure 6-26	Screenshot of Windows Print Management console © Microsoft 2019
Figure 6-27	Screenshot of Windows Memory Diagnostics © Microsoft 2019
Figure 6-28	Screenshot of Windows Defender Firewall © Microsoft 2019
Figure 6-29	Screenshot of Event Viewer © Microsoft 2019
Figure 6-30	Screenshot of Device Manager tabs © Microsoft 2019
Figure 6-31	Screenshot of Device Manager tabs © Microsoft 2019
Figure 6-32	Screenshot of MSCONFIG General tab © Microsoft 2019
Figure 6-33	Screenshot of MSCONFIG Boot tab © Microsoft 2019
Figure 6-34	Screenshot of MSCONFIG Tools tab © Microsoft 2019
Figure 6-35	Screenshot of Windows Task Manager's Applications tab © Microsoft 2019
Figure 6-36	Screenshot of Windows Task Manager's opening dialog © Microsoft 2019
Figure 6-37	Screenshot of Windows 8.1 version of Task Manager © Microsoft 2019
Figure 6-38	Screenshot of Task Manager © Microsoft 2019
Figure 6-39	Screenshot of Disk Management © Microsoft 2019
Figure 6-40	Screenshot of Volume wizard © Microsoft 2019
Figure 6-41	Screenshot of Volume wizard © Microsoft 2019
Figure 6-42	Screenshot of Disk Management © Microsoft 2019
Figure 6-43	Screenshot of Storage spaces © Microsoft 2019
Figure 6-44	Screenshot of REGEDIT (Windows 7) © Microsoft 2019
Figure 6-45	Screenshot of Remote Desktop Connection © Microsoft 2019
Figure 6-46	Screenshot of Windows Explorer in Windows 7 © Microsoft 2019
Figure 6-47	Screenshot of Windows 8.1 File Explorer © Microsoft 2019
Figure 6-48	Screenshot of Windows Explorer in Windows 7 © Microsoft 2019
Figure 6-49	Screenshot of System information © Microsoft 2019
Figure 6-50	Screenshot of System information © Microsoft 2019
Figure 6-51	Screenshot of DirectX Diagnostic Tool © Microsoft 2019
Figure 6-52	Screenshot of Disk Defragmenter © Microsoft 2019
Figure 6-53	Screenshot of Windows 10 © Microsoft 2019
Figure 6-54	Screenshot of Windows 8.1 Advanced Boot Options © Microsoft 2019
Figure 6-55	Screenshot of Windows 10 © Microsoft 2019
Figure 6-56	Screenshot of Control Panel © Microsoft 2019
Figure 6-57	Screenshot of Control Panel © Microsoft 2019
Unnumbered Figure 6-1	Rick McDonald
Figure 6-58	Screenshot of Windows Explorer Folder © Microsoft 2019

Figure 6-59	Screenshot of Windows 8.1 system © Microsoft 2019
Figure 6-60	Screenshot of Windows 10 System © Microsoft 2019
Figure 6-61	Screenshot of Windows 8.1 © Microsoft 2019
Figure 6-62	Screenshot of Windows 8.1 © Microsoft 2019
Figure 6-63	Screenshot of Windows 8.1 © Microsoft 2019
Figure 6-64	Screenshot of Windows 8.1 © Microsoft 2019
Figure 6-65	Screenshot of Windows 7 © Microsoft 2019
Figure 6-66	Screenshot of Windows 8.1 © Microsoft 2019
Figure 6-67	Screenshot of Windows 8.1 © Microsoft 2019
Figure 6-68	Screenshot of Map Network Drive © Microsoft 2019
Figure 6-69	Screenshot of Windows 8.1 © Microsoft 2019
Figure 6-70	Screenshot of Windows 8.1 © Microsoft 2019
Figure 6-71	Screenshot of VPN, dial-up ISP © Microsoft 2019
Figure 6-72	Screenshot of Wireless Connection © Microsoft 2019
Figure 6-73	Screenshot of Manual Proxy Servers © Microsoft 2019
Figure 6-74	Screenshot of System Properties © Microsoft 2019
Figure 6-75	Screenshot of Windows Remote Assistance © Microsoft 2019
Figure 6-76	Screenshot of Windows Remote Assistance © Microsoft 2019
Figure 6-77	Screenshot of Network Location Dialog © Microsoft 2019
Figure 6-78	Screenshot of Network and Sharing Center © Microsoft 2019
Figure 6-79	Screenshot of Windows 8.1 © Microsoft 2019
Figure 6-80	Screenshot of Windows 8.1 © Microsoft 2019
Figure 6-81	Screenshot of Windows 10 © Microsoft 2019
Figure 6-82	Screenshot of Windows Defender Firewall © Microsoft 2019
Figure 6-83	Screenshot of Windows Defender Firewall © Microsoft 2019
Figure 6-84	Screenshot of Windows 10 © Microsoft 2019
Figure 6-85	Screenshot of Windows 8.1 © Microsoft 2019
Figure 6-86	Screenshot of Alternate configuration © Microsoft 2019
Figure 6-87	Screenshot of Windows 8.1 © Microsoft 2019
Figure 6-88	Screenshot of Speed & Duplex settings © Microsoft 2019
Figure 6-89	Screenshot of Wake-on-LAN settings © Microsoft 2019
Figure 6-90	Screenshot of Crontab © Linux Kernel Organization
Figure 6-91	Screenshot reprinted with permission from Apple Inc.
Figure 6-92	Screenshot reprinted with permission from Apple Inc.
Figure 6-93	Screenshot reprinted with permission from Apple Inc.
Figure 6-94	Screenshot reprinted with permission from Apple Inc.
Figure 6-95	Screenshot reprinted with permission from Apple Inc.
Figure 6-96	Screenshot of backup job © Linux Kernel Organization
Figure 6-97	Screenshot reprinted with permission from Apple Inc.
Figure 6-98	Screenshot reprinted with permission from Apple Inc.
Figure 6-99	Screenshot reprinted with permission from Apple Inc.
Figure 6-100	Screenshot reprinted with permission from Apple Inc.
Figure 6-101	Screenshot reprinted with permission from Apple Inc.
Figure 6-102	Screenshot reprinted with permission from Apple Inc.
Figure 6-103	Screenshot reprinted with permission from Apple Inc.
Figure 6-104	Screenshot reprinted with permission from Apple Inc.
Figure 6-105	Screenshot reprinted with permission from Apple Inc.
Figure 6-106	Screenshot reprinted with permission from Apple Inc.
Figure 6-107	Screenshot of Fedora 23 Workstation © 2019 Red Hat, Inc.
Figure 6-108	Screenshot of Fedora 23 Workstation © 2019 Red Hat, Inc.

Figure 6-109	Screenshot of Fedora 23 Workstation © 2019 Red Hat, Inc.
Figure 6-110	Screenshot of Ubuntu © 2019 Canonical Ltd.
Figure 6-111	Screenshot of Ubuntu © 2019 Canonical Ltd.
Figure 6-112	Screenshot of Ubuntu © 2019 Canonical Ltd.
Figure 6-113	Screenshot of Fedora 23 Workstation © 2019 Red Hat, Inc.
Figure 7-1	Rick McDonald
Figure 7-2	Rick McDonald
Figure 7-3	Screenshot of Certificate Manager © Microsoft 2019
Figure 7-4	Screenshot of Dialog Purports © Microsoft 2019
Figure 7-5	Screenshot of Windows 10 Recovery Options © Microsoft 2019
Figure 7-6	Screenshot of Windows 10 Recovery Options © Microsoft 2019
Figure 7-7	Screenshot reprinted with permission from Apple Inc.
Figure 7-8	Screenshot reprinted with permission from Apple Inc.
Figure 7-9	Screenshot reprinted with permission from Apple Inc.
Figure 7-10	Screenshot of SND server address © Microsoft 2019
Figure 7-11	Screenshot of Message Purports © Microsoft 2019
Figure 7-12	Screenshot of Windows 10 © Microsoft 2019
Figure 7-13	Screenshot of EFS Encryption © Microsoft 2019
Figure 7-14	Screenshot of Local Group Policy Editor © Microsoft 2019
Figure 7-15	Screenshot of Active Directory Users and Computers © Microsoft 2019
Figure 7-16	Screenshot of Active Directory Users and Computers © Microsoft 2019
Figure 7-17	Screenshot of Active Directory Users and Computers © Microsoft 2019
Figure 7-18	Screenshot of Active Directory Users and Computers © Microsoft 2019
Figure 7-19	Screenshot of Windows 10 © Microsoft 2019
Figure 7-20	Screenshot of Local Group Policy Editor © Microsoft 2019
Figure 7-21	Screenshot of Encrypting Files © Microsoft 2019
Figure 7-22	Screenshot of Linksys © 2018 Belkin International, Inc.
Figure 7-23	Screenshot of Linksys © 2018 Belkin International, Inc.
Figure 7-24	Screenshot of Linksys © 2018 Belkin International, Inc.
Figure 7-25	Screenshot of Windows 10 © Microsoft 2019
Figure 8-1	Screenshot of Windows Recovery © Microsoft 2019
Figure 8-2	Screenshot of Ubuntu © 2019 Canonical Ltd.
Figure 8-3	Screenshot of Ubuntu © 2019 Canonical Ltd.
Figure 8-4	Screenshot of Ubuntu © 2019 Canonical Ltd.
Unnumbered Figure 8-1	Screenshot of Windows 7 © Microsoft 2019
Unnumbered Figure 8-2	Screenshot reprinted with permission from Apple Inc.
Figure 9-3	Screenshot of Windows 10 © Microsoft 2019
Figure 9-4	Screenshot reprinted with permission from Apple Inc.
Figure 9-5	Screenshot reprinted with permission from Apple Inc.
Figure 9-6	Jason Kolenda/Shutterstock
Figure 9-7	Rick McDonald
Figure 9-8	Rick McDonald
Figure 9-9	Rick McDonald
Figure 9-10	Rick McDonald
Figure 9-11	Rick McDonald
Figure 9-12	Screenshot of Windows PowerShell © Microsoft 2019
Unnumbered Figure 9-1	Rick McDonald
Unnumbered Figure 9-2	Rick McDonald
Cover Credit information	Bunyiam/Shutterstock

Contents at a Glance

Table of Contents

About the Author

Rick McDonald is a professor in the IT Specialist program at the University of Alaska in Fairbanks, Alaska. He holds degrees and certificates from Gonzaga University in Spokane, Washington, and University of Illinois Springfield. After several years in the airline industry, he returned to full-time teaching in North Carolina and then in Ketchikan, Alaska. Previous publication projects include CCNA Companion Guides and technical editing of various certification textbooks. He is currently teaching A+, CCNA, and AWS certification classes in Fairbanks and across Alaska via the Web.

About the Technical Reviewer

Chris Crayton (MCSE) is an author, technical consultant, and trainer. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several of the leading publishing companies. He holds numerous industry certifications, has been recognized with many professional teaching awards, and has served as a state-level SkillsUSA competition judge.

Dedication

I would like to dedicate this book to my wife, Becky, whose unending patience allowed deadlines be met. And to my mother, Frances McDonald, who taught me that learning is a life-long adventure.

I also dedicate this book to my two young grandsons, Hank and Walt. Considering the changes in the past 10 years in IT, it is fun to wonder what this book will hold when you are ready for your own copy.

Acknowledgments

This book is a result of concerted efforts of many dedicated people, without whom this book would not be a reality. I wish like to thank the technical reviewer, Chris Crayton, whose efforts and patience made this a better book for all to use, and to the development editor, Chris Cleveland, who helped me navigate the adjustments to a new CompTIA A+ version. Thanks also to Kitty Wilson, Copy Editor, whose thorough work makes this book much more approachable.

Thanks also to Paul Carlstroem, portfolio manager, for his help and continuous support during the development of this book. I wish to also express my appreciation to Mary Beth Ray, executive editor at Pearson/Cisco Press, for her confidence in me throughout years of working on book projects. Thank you and best to you in your new adventures.

I also wish to thank Professors Josh Peter and Mel Denning, and Ivan Gallagher, Ken Moneymaker, David Mattice, and Cheri Renson, my colleagues and friends at the Community and Technical College at the University of Alaska. Their patience and support as ideas and details were discussed and parsed are greatly appreciated. I learned much from their generous sharing of IT experiences.

It has been a huge undertaking to pull all the pieces of this project together. It is due to the dedication of those mentioned above that this book is not only large in scope but high in quality. It is my sincerest hope that our combined efforts will help you, the readers and users of this book, achieve your goals in an IT career.

Introduction

CompTIA A+ certification is widely recognized as the first certification you should receive in an information technology (IT) career. Whether you are planning to specialize in PC or mobile device hardware, operating systems management, security, or network management, the CompTIA A+ certification exams measure the baseline skills you need to master to begin your journey toward greater responsibilities and achievements in IT.

CompTIA A+ certification is based on a vendor-neutral exam that measures your knowledge of industry-standard technology.

Goals and Methods

The number-one goal of this book is a simple one: to help you pass the CompTIA A+ certification Core 1 (220-1001) and Core 2 (220-1002) exams.

Because CompTIA A+ certification exams now stress problem-solving abilities and reasoning more than memorization of terms and facts, our goal is to help you master and understand the required objectives for each exam.

To aid you in mastering and understanding the A+ certification objectives, this book uses the following methods:

- The beginning of each chapter defines the topics to be covered in the chapter; it also lists the corresponding CompTIA A+ objective numbers.
- The body of the chapter explains the topics from hands-on and theory-based standpoints. Each chapter includes in-depth descriptions, tables, and figures that are geared toward building your knowledge so that you can pass the exam. The chapters are broken down into several topics each.
- The key topics indicate important figures, tables, and lists of information that you should know for the exam. They are interspersed throughout the chapter and are listed in table format at the end of the chapter.
- You can find memory tables online in Appendix C, "Memory Tables," and Appendix D, "Answer Key to Memory Tables." Use them to help memorize important information.
- Key terms without definitions are listed at the end of each chapter. Write down the definition of each term and check your work against the key terms in the glossary.

How the Book Is Organized

Each chapter in this book maps one-to-one with the domains of the A+ Core 1 (220-1001) and Core 2 (220-1002) exam domains:

Chapter	Core 1 (220-1001) Domain Covered	Percentage of Exam
Chapter 1, Mobile Devices	1.0 Mobile Devices	14%
Chapter 2	2.0 Networking	20%
Chapter 3	3.0 Hardware	27%
Chapter 4	4.0 Virtualization and Cloud Computing	12%
Chapter 5	5.0 Hardware and Network Troubleshooting	27%
Chapter	**Core 2 (220-1002) Domain Covered**	
Chapter 6	1.0 Operating Systems	27%
Chapter 7	2.0 Security	24%
Chapter 8	3.0 Software Troubleshooting	26%
Chapter 9	4.0 Operational Procedures	23%

Book Features

To help you customize your study time using this book, the core chapters have several features that help you make the best use of your time:

- **Foundation Topics:** These are the core sections of each chapter. They explain the concepts for the topics in each chapter.
- **Exam Preparation Tasks:** After the "Foundation Topics" section of each chapter, the "Exam Preparation Tasks" section lists a series of study activities that you should do at the end of the chapter.
- **Review All Key Topics:** The Key Topic icon appears next to the most important items in the "Foundation Topics" section of the chapter. The Review All Key Topics activity lists the key topics from the chapter, along with their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know all the information highlighted with Key Topic icons, so you should review this activity.

- **Define Key Terms:** This section lists the most important terms from the chapter. To ensure that you know them, write a short definition of each and compare your answer to the glossary at the end of the book.
- **Review Questions:** Confirm that you understand the content that you just covered by answering these questions and reading the answer explanations.
- **Web-based practice exam:** The companion website includes the Pearson Cert Practice Test engine, which allows you to answer practice exam questions. Use it to prepare with a sample exam and to pinpoint areas where you need more study.

What's New?

You'll find plenty that's new and improved in this edition, including:

- Increased content concerning the troubleshooting of computer hardware and software
- Addition of Windows 10 content
- Addition of Chrome OS content
- A large increase in operational procedures content
- Addition of basic scripting
- Addition of remote access technologies
- Increased virtualization concepts
- Addition of cloud computing concepts
- Reorganized text to minimize duplication of coverage between objectives
- New coverage of Linux and OS X features and troubleshooting
- New coverage of MacBook features, such as Thunderbolt 2
- Updated processor coverage
- Updated BIOS dialogs, including more UEFI/BIOS examples
- USB 3.1 and USB-Type C
- mSATA and M.2 SSDs
- Improved photos and illustrations

- Enhanced laptop teardown and subassembly replacement procedures
- Updated memory coverage (DDR4 DIMMs and UniDIMMs)
- Updated coverage of mobile devices, including teardown tips
- Enhanced coverage of desktop and laptop upgrades, including Thunderbolt and the miniPCIe card
- Updated coverage of docking stations and video cable adapters
- Updated power supply and cooling system information
- Improved coverage of network hardware and cabling
- Enhanced coverage of device troubleshooting, teardown, and upgrades
- New coverage related to dealing with prohibited content/activity
- Enhanced coverage of Windows features
- Enhanced discussion of Windows upgrade paths and methods
- New Windows 8/8.1/10 features
- Enhanced coverage of ESD protection issues
- Enhanced coverage of Windows OS troubleshooting
- Enhanced Control Panel discussion
- Enhanced coverage of iOS and Android devices
- Enhanced coverage of security issues (physical, digital, wireless network, wired network, workgroup, and homegroup folders)
- New coverage of network and cloud computing concepts
- Enhanced coverage of security issues
- New coverage of Linux and OS X OS troubleshooting

Who Should Read This Book?

The CompTIA A+ exams measure the necessary competencies for an entry-level IT professional with knowledge equivalent to what you would learn in 6 to 12 months of hands-on experience in a lab or in the field. This book is written for people who have that amount of experience working with desktop PCs, laptops, and mobile devices. Average readers will have attempted in the past to replace a hardware component within a PC or mobile device; they should also understand how to navigate through Windows, access the Internet, and have (or be willing to learn) a basic knowledge of OS X and Linux features.

Readers will range from people who are attempting to attain a position in the IT field to people who want to keep their skills sharp or perhaps retain their job due to a company policy that mandates that they take the new exams.

This book is also aimed at readers who want to acquire additional certifications beyond the A+ certification (Network+, Security+, and so on). The book is designed to provide an easy transition to future certification studies.

Strategies for Exam Preparation

Strategies for exam preparation vary depending on your existing skills and knowledge, as well as the equipment you have available. Of course, the ideal exam preparation would consist of building a PC from scratch and installing and configuring the operating systems covered.

Chapter 1 contains lists of the tools, software, and operating systems recommended by CompTIA for exam study and preparation and how to track down the best deals.

The next best step you can take is to read through the chapters in this book, jotting down notes about key concepts or configurations in a dedicated notepad. Each chapter contains a quiz that you can use to test your knowledge of the chapter's topics. It's located near the end of the chapter.

After you have read through the book, take a look at the current exam objectives for the CompTIA A+ certification exams listed at https://certification.comptia.org/certifications/a. If there are any areas shown in the certification exam outline that you would still like to study, find those sections in the book and review them.

When you feel confident in your skills, attempt the practice exams included on the companion website with this book. As you work through the practice exam, note the areas where you lack confidence and review those concepts or configurations in the book. After you have reviewed the areas, work through the practice exam a second time and rate your skills. Keep in mind that the more you work through the practice exam, the more familiar the questions will become.

After you have worked through the practice exam a second time and feel confident with your skills, schedule the real CompTIA A+ Core 1 (220-1001) and Core 2 (220-1002) exams through Pearson VUE (www.vue.com). To prevent the information from evaporating out of your mind, you should typically take the exam within a week of when you consider yourself ready to take the exam.

Security

The most important asset most companies own is their data. Data has become so important to business success that it is what most thieves seek. Because of the interconnected nature of the Internet, a security breach of a single device or network can lead to data theft, including the theft of client financial data that can greatly affect the lives of millions. Large-scale data breaches have brought large companies to bankruptcy, so data security is among the top concerns of business leadership. In this chapter, you learn about the multifaceted threats to security in the modern computing environment and how to mitigate them through the study of these CompTIA A+ Core 2 objectives. This chapter covers the following topics:

- **Physical security measures:** Physical security practices and their implementation.
- **Logical security concepts:** Software-based security measures.
- **Wireless security protocols and authentication:** Types of wireless security and authentication.
- **Malware removal and prevention:** Methods and protocols for detection and prevention.
- **Social engineering threats and vulnerabilities:** The various types of threats.
- **Microsoft Windows OS security settings:** The important Microsoft security settings.
- **Security best practices to secure a workstation:** Implementation of best practices.
- **Securing mobile devices:** Implementation methods for securing devices.
- **Data destruction and disposal:** Methods and techniques for safely and securely disposing of hardware.
- **Configuring security on SOHO networks:** Methods for configuring SOHO security.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read the entire chapter. Table 7-1 lists the major headings in this chapter and the "Do I Know This Already?" quiz questions covering the material in those headings so you can assess your knowledge of these specific areas. The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Review Question Sections."

Table 7-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Physical Security Measures	1
Logical Security Concepts	2
Wireless Security Protocols and Authentication	3–4
Social Engineering Threats and Vulnerabilities	5
Microsoft Windows OS Security Settings	6
Security Best Practices to Secure a Workstation	7
Securing Mobile Devices	8
Data Destruction and Disposal	9
Configuring Security on SOHO Networks	10

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. What kind of security breach is a mantrap designed to foil?
   - **a.** Biometric
   - **b.** Tailgating
   - **c.** Sleeping guard
   - **d.** Shoulder surfing

2. Say that you have been asked to improve security by adding a system to examine network packets to determine whether they should be forwarded or blocked. What is the function you would be most likely to add?
   a. MAC address filtering
   b. MAC address cloning
   c. Software firewall
   d. Multifactor authentication

3. Which of the following is the most secure wireless protocol in use today?
   a. WEP
   b. WEP3
   c. TKIP
   d. WPA2

4. A user has unwittingly downloaded malware while also downloading a free application on a gaming site. What general term describes the unintentionally downloaded file?
   a. Worm
   b. Trojan
   c. Ransomware
   d. Botnet

5. Several computers on a network have been commandeered to launch an attack on a server on the Web. Which term best describes this situation?
   a. Phishing
   b. DoS
   c. Spoofing
   d. DDoS

6. Which setting allows the user the most privileges on a Windows network?
   a. Modify
   b. Read and Execute
   c. Ultimate Use
   d. Write

7. Which is the best example of a strong password?
   a. dr0wssap
   b. Password9
   c. Pa5SwoRd5
   d. pA55wrds

8. Which of the following is not an example of biometric authentication?
   a. Entering a password and answering a secret question
   b. Apple FACE ID
   c. Windows Hello
   d. Touch ID

9. Which method erases storage media but leaves the device intact?
   a. Data shredding
   b. Degaussing
   c. BitLocking
   d. Incineration

10. To help hide the identity of a wireless router, what should be changed from the default setting?
    a. Private IP address
    b. MAC address filter
    c. IP default gateway
    d. Service set identifier

Foundation Topics

Physical Security Measures

220-1002: Objective 2.1: Summarize the importance of physical security measures.

220-1002 Exam

Physical security of IT equipment is a fundamental first factor in a secure network. As mentioned earlier, data is typically the most valuable asset in a company, and leaving it in an unlocked area is dangerous in two ways. First, computer equipment is valuable, and a thief may want it for its face value, not caring about the valuable data it may contain or harm its release may do to customers. Second, an unlocked door is an invitation for someone to install sniffing equipment and gain access to company network assets well beyond the physical room left unattended. In the realm of physical security, there are several measures an IT professional must understand and practice.

Mantrap

Some secure areas include what is known as a ***mantrap***, which is an area with two locking doors. A person might get past a first door by way of tailgating but might have difficulty getting past the second door, especially if there is a guard in between the two doors. A mantrap essentially slows down the entry process in hopes that people sneaking in behind others will be thwarted before gaining entry to the secure area. If the person doesn't have proper authentication, he will be stranded in the mantrap until authorities arrive.

Badge Reader

Badge readers are devices that can interpret the data on a certain type of ID. While photo IDs are still best assessed by humans, other types of IDs add extra security that can be read by badge readers.

ID badges and readers can use a variety of physical security methods, including the following:

- **Photos:** If the bearer of the card doesn't look like the person on the card, the bearer might be using someone else's card and should be detained.
- **Barcodes and magnetic strips:** The codes embedded on these cards enable the cards to carry a range of information about the bearers and can limit individuals' access to only authorized areas of buildings. These cards can be read quickly by a barcode scanner or swipe device.

- ***RFID technology*:** Like barcoded badges, cards with radio-frequency identification (RFID) chips can be used to open only doors that are matched to the RFID chip. They can also track movement within a building and provide other access data required by a security officer.

To prevent undetected tampering, ID badges should be coated with a tamper-evident outer layer.

Smart Card

A smart card is a credit card–sized card that contains stored information and might also contain a simple microprocessor or an RFID chip. Smart cards can be used to store identification information for use in security applications and to store values for use in prepaid telephone or debit card services, hotel guest room access, and many other functions. Smart cards are available in contact and contactless form factors.

Contactless cards are also known as *proximity cards*. Readers for these cards are usually wall mounted so users can scan their cards within 6 inches of a reader.

A ***smart card***–based security system includes smart cards, card readers that are designed to work with smart cards, and a back-end system that contains a database that stores a list of approved smart cards for each secured location. Smart card–based security systems can also be used to secure individual personal computers.

To further enhance security, smart card security systems can also be multifactor, requiring the user to input a PIN or security password as well as provide the smart card at secured checkpoints, such as the entrance to a computer room.

Security Guard

Even the best security plans can be foiled by a determined and skillful thief. The best way to deter a thief is to use a mix of technical barriers and human interaction. Guards can be deployed in different ways. When employees enter the work area in the presence of a guard, it is more likely that best practices will be followed and everyone will scan in and be authenticated. Without a guard, it is more common for people to hold the door for people who are recognized but say they have misplaced their IDs. Knowing that someone is watching carefully keeps honest people honest and those who are dishonest away from the door.

Another way to deploy guards is to have them watch several areas via security cameras that record access into and out of the buildings. While this method is not

as effective as posting a guard at each door, it makes it possible for fewer security guards to scan different areas for traffic behaviors that warrant further attention.

Door Lock

Of course, the easiest way to secure an area is to lock doors. While this seems an obvious statement, it is surprisingly common for people to get to unauthorized areas by just wandering in. Some organizations have written policies explaining how, when, and where to lock doors. Aside from main entrances, you should also always lock server rooms, wiring closets, labs, and other technical rooms when not in use.

Physical door locks might seem low tech, but they can't be taken over by hackers. Other precautions to take include documenting who has keys to server rooms and wiring closets and periodically changing locks and keys. Cipher locks that use punch codes also enhance security. Using a combination of these methods provides for greater protection.

Biometric Locks

Biometric security refers to the use of a person's biological information—through fingerprint scanning, retina scanning, or facial recognition, for example—to authenticate potential users of a secure area. The most common type of biometric security system for PCs is fingerprint based, but other methods include voice measurements, facial recognition, and scans of the eye's retina or iris. Newer versions of device security that use fingerprint and facial recognition are Microsoft's Hello (available in Windows 10) and Apple Face ID on newer iPhones.

Tokens

Any physical device that a user must carry to gain access to a specific system can be called a ***token***. Examples are smart cards, RFID cards, USB tokens, and key fobs. (Key fob hardware tokens are explained later in this section.)

Laptop and Cable Locks

Most desktops, laptops, and many other mobile devices such as projectors and docking stations feature a security slot. On a laptop, the slot is typically located near a rear corner (see Figure 7-1).

1. Security slot

FIGURE 7-1 A Security Slot on a Laptop

This slot is used with a laptop ***cable lock***, such as the one shown in Figure 7-2. Laptop locks use a combination or keyed lock and are designed to lock a laptop (or other secured device) to a fixed location such as a table.

FIGURE 7-2 A Combination Laptop Security Lock

Server Locks

Even with building security in place, it may be necessary to have more granular security in place in areas like server rooms. A data center might contain equipment from several different companies, and non-employees may need access to server areas. Of course, not all threats are external, and some employees who have access to equipment areas should also have access to server equipment in the data center.

Rack-level security involves locking down equipment in a server rack. This can be done with cabinets or cages with secure biometric locks or perhaps keycards that can be changed often. Security cameras are appropriate in data centers as well. Rack cabinets can be quite sophisticated, with alarms that indicate access and improperly closed doors.

Examples of rack level security can be seen at https://tzsmartcabinets.net.

USB Locks

It is possible for someone to remove a USB cable from a computer and insert another USB device (or simply plug into an empty USB port), making it possible for a thief to then move data from the computer. ***USB locks*** can be used to secure USB cables into the computer and to securely plug empty USB ports. One manufacturer of these specialty port locks is PadJack (http://www.padjack.com/usb-cable-lock-seal/).

Privacy Screen

Privacy issues are important to any company that handles confidential data, and when such data is being used on a workstation screen or mobile device, it needs to be protected from unintentional viewing. Data on a computer screen can be easily protected by installing a ***privacy screen***, which is a transparent cover for a PC monitor or laptop display. It reduces the cone of vision, usually to about 30 degrees, so that only the person directly in front of the screen can see the content. Many of these screens are also antiglare, helping to reduce the user's eye strain.

Key Fobs

Key fobs can be used with a variety of security devices. They can contain RFID chips, and many key fobs are used as part of a two-step authentication protocol that works as follows:

- The user carries a key fob that generates a code every 30 to 60 seconds. Every time the code changes on the fob, it is also matched in the authentication server. In some cases, the user must also log into the fob to see the access code for an extra layer of security.
- The user then logs into the system or restricted area, using the randomly generated access code displayed on the key fob's LCD display. The authentication server matches the current code and allows access.

A key fob used in this way is often referred to as a hardware token.

Entry Control Roster

An ***entry control roster***, which is a list of individuals or representatives who are authorized to enter a secured area, can be used with a variety of security systems. Potential entrants can be looked up on an entry control roster and granted access if their credentials match those listed. A keypad lock on an entrance to a secure area can store a list of authorized PINs. Only users with recognized PINs can enter the secure area. Logs are usually kept to record who entered and exited a room at different times.

Logical Security Concepts

220-1002 Exam

220-1002: Objective 2.2: Explain logical security concepts.

Because a computer is a combination of physical and logical systems, security practices must address both of these sides of computing. The physical components of security addressed in the previous section are only part of a good security plan and will be ineffective if the security policies stop there. Addressing software (logical) security practices is essential as well.

Active Directory

Active Directory is a Microsoft solution for managing users, computers, and information access in a network. It is based on a database of all resources and users that will be managed within the network. The information in the database determines what people can see and do within the network. Complete understanding of Active Directory is beyond the scope of this course, but every IT support person should know the basics of what it is and how it works. Here are the basics:

Key Topic

- ***Login script*:** When a user logs onto the network, Active Directory knows who that user is and runs a login script to make the assigned resources available. Examples of login tasks include virus updates, drive mapping, and printer assignments.
- ***Domain*:** The domain is a computer network or group of computer networks under one administration. Users log into the Active Directory domain to access network resources within the domain.
- ***Group Policy*:** This is a set of rules and instructions defining what a user or group of users can or cannot do when logged into the domain. You may see the term Group Policy Object (GPO), which is a set of instructions assigned to a group of users or to certain machines on the network.

- ***Organizational Unit (OU)*:** OUs are logical groups that help organize users and computers so that GPOs can be assigned to them. For example, a team of accountants may be assigned to an OU, and their GPO may give them special access to financial records.
- ***Home folder*:** This folder, which is accessible to the network administrator, is where the user's data and files are kept locally.
- ***Folder redirection*:** This allows for the work done by an OU to be saved on a common folder in the domain as directed by the administrator instead of the user. For example, a policy may indicate that all work must be kept in a common folder so all members of a team can see the latest work and updates.

Software Tokens

Like key fobs, mentioned in the previous section for physical security, ***software tokens*** are part of a multifactor authentication process. The difference is that software tokens exist in software and are commonly stored on devices.

An example of a software token is Google Authenticator, an app that is downloaded to a device and provides a shared secret key. The user logs in with his or her username and password, and the app runs an authenticating algorithm. This multifactor authentication is more secure than earlier versions of software tokens, which could be stolen.

MDM Policies

Organizations that have many mobile devices need to administer them such that all devices and users comply with the security practices in place. This is usually done with a suite of software known as ***mobile device management (MDM)***. The MDM marketplace is quite competitive, and several solutions are available from companies such as VMware (AirWatch), Citrix (XenMobile), and SOTI MobiControl. These products push updates and allow an administrator to configure many mobile devices from a central location. Good MDM software secures, monitors, manages, and supports multiple different mobile devices across the enterprise.

Port Security

Disabling ports refers to using a firewall appliance or software firewall to prevent specified UDP or TCP ports from being used by a service, an application, a specific device, or all devices. Turning off unused ports makes it harder for hackers to find stealthy access into a machine.

MAC Address Filtering

Every network adapter, whether it's built into a PC, is an add-on card, or is built into a specialized device such as a media adapter or a networked printer, has a unique identifier known as the media access control address, or ***MAC address***. The MAC address (sometimes known as the physical address) is a list of six two-digit hexadecimal numbers. For example, a typical PC MAC address is FA-15-B7-89-6C-24. (MAC addresses are sometimes listed as 12 digits rather than in six groups of 2 digits.)

A MAC address is usually found on a label on the side of a network adapter. If an adapter is already installed, enter **ipconfig /all** at a command prompt to display the MAC address.

Because MAC addresses are unique, it is possible to control access to most wireless networks by allowing only certain addresses in. The practice of allowing only certain devices is sometimes called ***whitelisting***. Some routers can also be configured to block a list of specified MAC addresses from accessing the wired network.

MAC address filtering can be a useful way to block casual hackers from gaining access to a small wireless (or wired) network, but it can be troublesome for a large network with many different devices coming into and going out of the system as each needs to be entered separately. MAC address filtering is discussed in further detail in Chapter 2, "Networking."

It is possible to use software to change the MAC address of a network device (a feature sometimes referred to as ***MAC address cloning***). Also, MAC addresses are not encrypted and can be detected by software used to hack networks. Thus, MAC address filtering alone should not be relied on to stop serious attacks.

Certificates

Apps can sometimes hold viruses or other bugs that can cause trouble on a network. It is important to be sure all apps installed come from reliable sources and have been approved by the operating system vendor. App stores for iOS, Android, Windows 8 and later, macOS, and many Linux distros are examples of trusted sources of software.

However, not all software for an operating system comes from an app store. Digital ***certificates*** included in software are used to identify the publisher, and most operating systems display warning messages when an app without a digital certificate is being installed. Some settings block the installation of any app that does not have a digital certificate.

In Windows 10 the Certificate Manager keeps track of and check certificates. Figure 7-3 shows the Windows Certificate Manager with specific certificates listed in the right pane. To access Certificate Manager in Windows 10, click the **Start** button, type **certmgr.msc** in the search field, and press **Enter**.

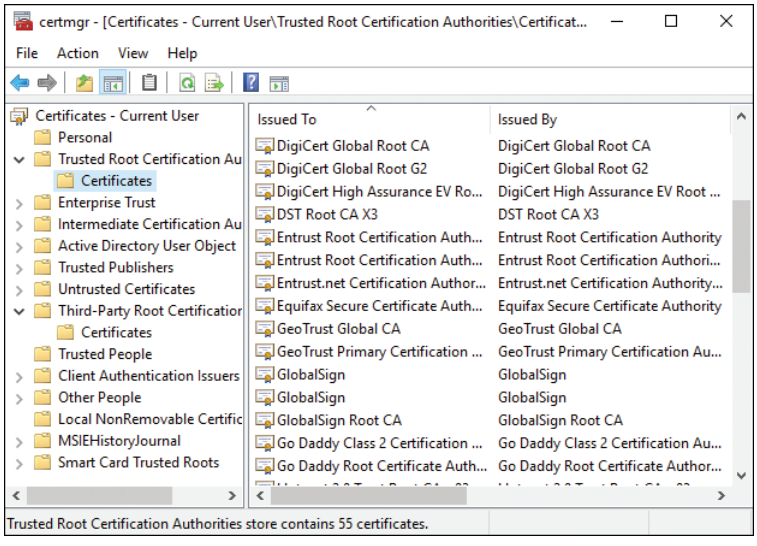


FIGURE 7-3 Certificate Manager

Antivirus/Anti-malware

Just as there is antivirus software for PCs, there is also ***antivirus/anti-malware software*** for mobile devices. These are third-party applications that need to be paid for, downloaded, and installed to the mobile device. Some common examples of reliable companies offering antivirus and anti-malware products include McAfee, Norton, and Trend, though many companies offer such products.

iOS works a bit differently from the other mobile operating systems. iOS is a tightly controlled operating system. One of the benefits of being a closed-source OS is that it can be more difficult to write viruses for it, making it somewhat more difficult to compromise. But there is no OS that can't be compromised, and as Apple's success has grown, efforts to write viruses for Apple machines have increased. McAfee, Norton, Trend Micro, and others have well-respected iOS protection products.

Firewalls

A ***firewall*** is a physical device or a software program that examines data packets on a network to determine whether to forward them to their destination or block them. A firewall can be a one-way firewall, which means it is used to protect against inbound threats only, or it can be a ***two-way firewall***, which protects against both unauthorized inbound and outbound traffic. Most third-party firewall programs, such as ZoneAlarm, are two-way firewalls. A software firewall can be configured to permit traffic between specified IP addresses and to block traffic to and from the Internet except when permitted on a per-program basis.

A corporate network may use a proxy server with a firewall as the sole direct connection between the Internet and the corporate network and use a firewall in the proxy server to protect the corporate network against threats.

Physical firewalls are specialized computers whose software is designed to quickly analyze network traffic and make forwarding decisions based on rules set by the administrator. Over time, that task has been incorporated more and more into software on the computers and into the OS design. An example is Windows Defender Firewall in Windows 10, which is discussed later in the chapter.

Most current operating systems have some sort of firewall built in:

- As initially configured, the standard firewall in Windows is a one-way firewall. However, it can be configured to work as a two-way firewall. For more information about how it works, see the section "Firewall Settings," later in this chapter.
- macOS includes an application firewall. In OS X 10.6 and newer, the application firewall offers additional customization options.
- Linux, starting with distros based on kernel 2.4.x and later, includes iptables to configure netfilter, its packet-filtering framework. To learn more, see www.netfilter.org. Many distros and third-party Linux apps are available to help make iptables and netfilter easier to configure.

User Authentication/Strong Passwords

Authenticating users means making sure those who are logging in are truly who they say they are. Requiring passwords for user authentication can make systems more secure, but humans have proven pretty lax at voluntarily practicing security. To solve this problem, administrators should mandate strong passwords in their ***authentication*** settings.

Strong passwords that foil casual hackers have the following characteristics:

- They are at least eight characters long; every character added to this minimum makes the password exponentially safer.
- They include a variety of uppercase and lowercase letters, numbers, and symbols.
- They do not include real names and words.

Multifactor Authentication

The best type of authentication system is one that uses two or more authentication methods. This is known as ***multifactor authentication***. An example of this would be a person using a smart card and typing a username and password to gain access to a system. The combination of the password and the physical token makes it very difficult for imposters to gain access to a system.

Directory Permissions

Directory permissions is the term used in macOS and Linux for configuring the access levels a user has to a directory (folder) and individual files. In Windows, the equivalent term is ***file and folder permissions***.

In Linux and macOS, directory permissions include:

- Read (opens file but no changes)
- Write (able to read and change file)
- Execute (runs executable file or opens directory)

The chmod command is used in Linux to change directory permissions. In macOS, the Get Info menu's Sharing & Permissions submenu is used to change directory permissions.

In Windows, file and folder permissions on an NTFS drive include:

- Full control
- Modify
- Read & Execute
- List folder contents (applies to folders only)
- Read
- Write

These settings are configured through the Security tab of the file or folder's properties sheet. The chmod command and output are discussed in further detail in Chapter 6, "Operating Systems."

VPN

A ***virtual private network (VPN)*** is a private and secure network connection that is carried by an insecure public network, such as the Internet. A VPN connection requires a VPN server at the remote site and a VPN client at the client site. VPN traffic between client and server is encrypted and encapsulated into packets suitable for transmission over the network. VPNs can be used in place of leased lines for connections between locations and for telecommuting workers.

The most common types of VPNs use Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP/IPsec). Tunneling refers to the practice of using encryption to shield traffic between the client and server from other traffic. PPTP uses 128-bit encryption, and L2TP combined with IPsec (L2TP/IPsec) uses 256-bit encryption. VPNs are discussed further in Chapter 2.

DLP

Data loss/leakage prevention (DLP) involves preventing confidential information from being viewed or stolen by unauthorized parties. DLP goes beyond normal digital security methods such as firewalls and antivirus software by observing and analyzing unusual patterns of data access, email, and instant messaging, whether the data is going into or out of an organization's network.

Access Control Lists

Access control lists (ACLs) are lists of permissions or restriction rules for access to an object such as a file or folder. ACLs control which users or groups can perform specific operations on specified files or folders.

Smart Card

Smart cards can be used to enable logins to a network, encrypt or decrypt drives, and provide digital signatures when supported by the network server.

Email Filtering

Email filtering can be used to organize email into folders automatically, but from a security standpoint, its most important function is to block spam and potentially dangerous messages.

Email filtering can be performed at the point of entry to a network with a specialized email filtering server or appliance as well as by enabling the spam and threat detection features that are built into email clients or security software.

Spam or suspicious emails can be discarded or quarantined by the user, and false positives that are actually legitimate messages can be retrieved from the spam folder and placed back into the normal inbox.

Trusted/Untrusted Software Sources

As mentioned previously concerning certificates, app stores for iOS, Android, Windows, macOS, and many Linux distros are examples of trusted sources of software. Apps installed from these sources have been approved by the operating system vendor and awarded certificates.

But not all software for an operating system comes from an app store. Digital certificates included in software are used to identify the publisher, and most operating systems display warning messages when an app without a digital certificate is being installed. Some operating systems block the installation of any app that does not have a digital certificate. It is ultimately up to the user to determine the trustworthiness of a software source.

Principle of Least Privilege

Applying the ***principle of least privilege*** means giving a user access to only what is required to do his or her job. Most users in a business environment do not need administrative access to computers and should be restricted from functions that could compromise security.

While the principle of least privilege appears to be basic common sense, it should not be taken lightly. When user accounts are created locally on a computer—and especially on a domain—great care should be taken in assigning users to groups. Also, many programs, when installed, ask who can use and make modifications to the program; often the default is "all users." Some technicians just accept the defaults when hastily installing programs without realizing that they are giving users full control of the program. It is an important practice to give clients all they need but limit their access to only what they need.

Wireless Security Protocols and Authentication

220-1002: Objective 2.3: Compare and contrast wireless security protocols and authentication methods.

220-1002 Exam

Wireless security has evolved over the past few years to adapt to the increasingly available tools that can hack into a wireless network. An administrator cannot safely

install a wireless network using the default settings. The following sections describe the security options available on a wireless network.

Protocols and Encryption

Key Topic

An encrypted wireless network relies on the exchange of a passphrase between the client and the wireless access point (WAP) or router before the client can connect to the network. There are several standards for encryption:

- **WEP:** ***Wired Equivalent Privacy (WEP)*** was the original encryption standard for wireless Ethernet (WiFi) networks. WEP encryption has aged, however, and is no longer strong enough to resist attacks from hackers. This is because the encryption keys are short, and some of the transmissions for the handshaking process are unencrypted. WEP encryption should not be considered secure for a wireless network.
- **WPA versions:** As a replacement to WEP, ***WiFi Protected Access (WPA)*** was developed in 2003. It is available in three strengths:
  - WPA uses the ***Temporal Key Integrity Protocol (TKIP)*** encryption, which was designed to provide better encryption than WEP.
  - WPA2 was released in 2004 and uses ***Advanced Encryption Standard (AES)*** encryption. WPA2's AES encryption is much stronger than WPA's; it uses 128-bit blocks and supports variable key lengths of 128, 192, and 256 bits. It allows up to 63 alphanumeric characters (including punctuation marks and other characters) or 64 hexadecimal characters. WPA2 also supports the use of a RADIUS authentication server in corporate environments.
  - WPA3, which was released in January 2018, uses 128-bit encryption (192-bit in an enterprise version) and has a different method for sharing security keys than the other types of encryption. WPA3 is designed to add better privacy and protection against attacks on public WiFi networks. WPA3 is not currently part of the A+ 220-1002 exam objectives, but its use is expanding as new hardware supporting it becomes common.

TKIP and AES encryption are quite different. TKIP is somewhat like WEP in design so that it can operate on legacy hardware lacking computing power. TKIP is no longer considered secure. AES is much more secure and has been adopted by the U.S. government as the encryption standard.

Authentication

There are four different authentication methods for access to a wireless network: single-factor, multifactor, RADIUS, and TACACS. These methods also apply to wired networks.

Single-Factor

Single-factor authentication is basic username and password access to a computer or network. For years, this was sufficient—and it is still used in many environments. But the rise of online banking and shopping drew more advanced hacking methods, and single-factor authentication is now rare in online commerce.

Multifactor

A ***multifactor authentication*** system uses two or more authentication methods and is far more secure than single-factor authentication. An example of this would be a person using a digital code from a fob and typing a username and password to gain access to a system. The combination of the password and the digital token makes it very difficult for imposters to gain access to a system.

As mentioned earlier in the chapter, Google Authenticator is an app that is downloaded to a device and provides a shared secret key. The user can log in with his or her username and password, and the app runs an authenticating algorithm as well. This multifactor authentication is more secure than earlier versions of software tokens, which could be stolen.

RADIUS

Remote Authentication Dial-In User Service (RADIUS) dates back to the days of dial-up modem access to networks in the early 1990s. It has been widely distributed and has been updated over the years and is still in use. A user who wants to access a network or an online service can contact a RADIUS server and enter username and password information when requested. The server authenticates (or declines) the user and advises the network or service to allow the client in (or not).

TACACS

Terminal Access Controller Access Control System (TACACS) solved a problem that occurred as network use expanded in the 1980s. While the name and acronym seem convoluted, it does describe the function and process pretty well. In early network computing, when a user logged into a network, each time he or she accessed a different resource or host on that network, the user had to re-authenticate. Dial-up

was slow, and logging in was a time-consuming process. With TACACS, a user who was already authenticated into the network was automatically logged into other resources in the system as well. The user's terminal access was taken care of by the network's access control system.

TACACS in its original form is quite insecure, but it has been updated and re-released in proprietary form by Cisco Systems as TACACS+.

Malware Removal and Prevention

220-1002 Exam

220-1002: Objective 2.4: Given a scenario, detect, remove, and prevent malware using appropriate tools and methods.

Wireless security has evolved over the past few years to adapt to the increasingly available tools that can be used to hack into a wireless network. An administrator cannot safely install a wireless network using the default settings. The following sections describe the security options available on a wireless network.

Malware

Key Topic

Malicious software, or malware, is software designed to infiltrate a computer system and possibly damage it without the user's knowledge or consent. Malware is a broad term used by computer professionals to include viruses, worms, Trojan horses, spyware, rootkits, keyloggers, adware, and other types of undesirable software. The sections that follow describe some types of malware in more detail.

Ransomware

Ransomware uses malware to encrypt the targeted computer's files. The ransom demand might be presented after you call a bogus technical support number displayed by a fake error message coming from the ransomware, or the ransom demand might be displayed onscreen. The ransom must be paid within a specified amount of time, or the files will not be decrypted.

The most famous example of ransomware is the WannaCry virus, which spread throughout the world in 2017. It impacted Windows machines that had not been updated with security patches that would have prevented the spread of the attack.

Trojan

Trojan malware, also known as a Trojan horse, is a malware program disguised as a "gift"—usually popular videos or website links—that trick the user into downloading a virus that might be used to trap keystrokes or transmit sensitive information.

Trojans are aptly named for the famous story of the wooden Trojan horse—an apparent gift that hid invading soldiers and allowed them to sneak inside the city gates of Troy.

Keylogger

Keylogger viruses are especially dangerous because they track keystrokes and can capture usernames and passwords of unwitting users. A keylogger can be delivered via a Trojan horse, phishing, or a fake email attachment that the user opens. One way to foil these attacks is to require multifactor authentication because the second authentication factor changes, rendering the stolen password invalid.

Rootkit

A ***rootkit*** is a set of hacking tools that makes its way deep into the computer's operating system or applications and sets up shop to take over the computer. Some rootkits do keylogging, some listen for banking information, and more complex ones can take over a computer completely. A rootkit is a complex type of malware that is difficult to detect and remove with standard malware antivirus software. Sometimes wiping the drive and reinstalling the operating system is the only certain solution.

Virus

Just as biological viruses can infect humans and cause all sorts of different illnesses, computer viruses can infect and damage computers. ***Virus*** is a generic term for any malicious software that can spread to other computers and cause trouble. Some are more malicious than others, but all need to be guarded against with antivirus updates. Most virus attacks are spread with human assistance when users fall prey to phishing and carelessly open attachments. (Phishing is discussed later in the chapter.)

Botnet

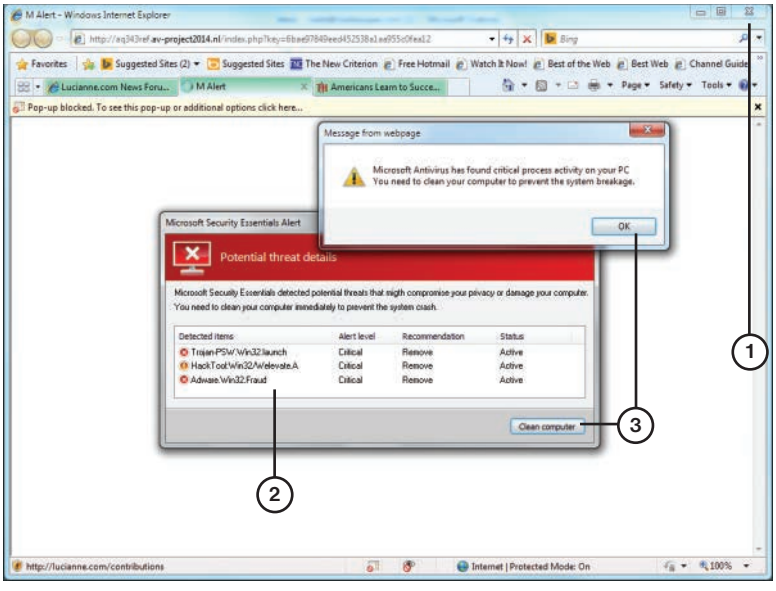
One danger in not protecting a computer from virus attacks is that it may be taken over and become a "bot"—or robot on a network of infected computers. Hackers can infect multiple computers to form a ***botnet*** and then use the infected machines to work together to cause trouble, such as by mounting denial of service attacks or spreading spam. Hackers who install networks of bots sometimes sell access to them to other hackers.

Worm

Worms are different from other viruses in that they are able to self-replicate on computers and push themselves out to other computers. Phishing and other human errors are not required for worms to thrive.

Spyware

Spyware is software that spies on system activities and transmits details of web searches or other activities to remote computers. Getting multiple unwanted pop-up windows when browsing the Internet is a good indicator of spyware. Some of the pop-up windows may show fake security alerts (as shown in Figure 7-4) in the hopes that the user will click on something and then purchase rogue or fake antivirus software or just download more malware. Spyware can possibly cause slow system performance.



1. The only safe place to click is the close browser button.
2. Fictitious threats.
3. Clicking either of these buttons might launch malware or spyware.

FIGURE 7-4 A Fake Security Alert That Purports to Be from Microsoft

Tools and Methods

The antivirus/anti-malware industry has worked hard to keep pace with the menace of hackers and ever-more-sophisticated viruses. The following sections discuss some of the tools and methods that are used to thwart the hackers.

Antivirus/Anti-malware

Protection against viruses and malware is necessary for every type of computing device, from mobile devices to servers. Computer protection suites that include antivirus, anti-malware, anti-adware, and anti-phishing protection are available from many vendors, but some users prefer a "best of breed" approach and choose the best available product in each category.

Antivirus/anti-malware programs can use some or all of the following techniques to protect users and systems:

- Real-time protection to block infection
- Periodic scans for known and suspected threats
- Automatic updating on a frequent (usually daily) basis
- Renewable subscriptions to obtain updated threat signatures
- Links to virus and threat encyclopedias
- Inoculation of system files
- Permissions-based access to the Internet
- Scanning of downloaded files and sent/received emails

When attempting to protect against viruses and malware, the most important thing to remember is to keep your anti-malware application up to date. The second most important item is to watch out for is unknown data, whether it comes via email, USB flash drive, mobile device, or some other mechanism.

Recovery Console

The ***Recovery Console*** allows you to reset your PC or boot from a recovery disk. If resetting the PC is not sufficient, you can boot from a recovery disk to remove some infected files and restore your original files. Access the recovery tools in Windows 10 by going to **Settings > Update & Security > Recovery**. Figure 7-5 shows the recovery tools page in Windows 10.

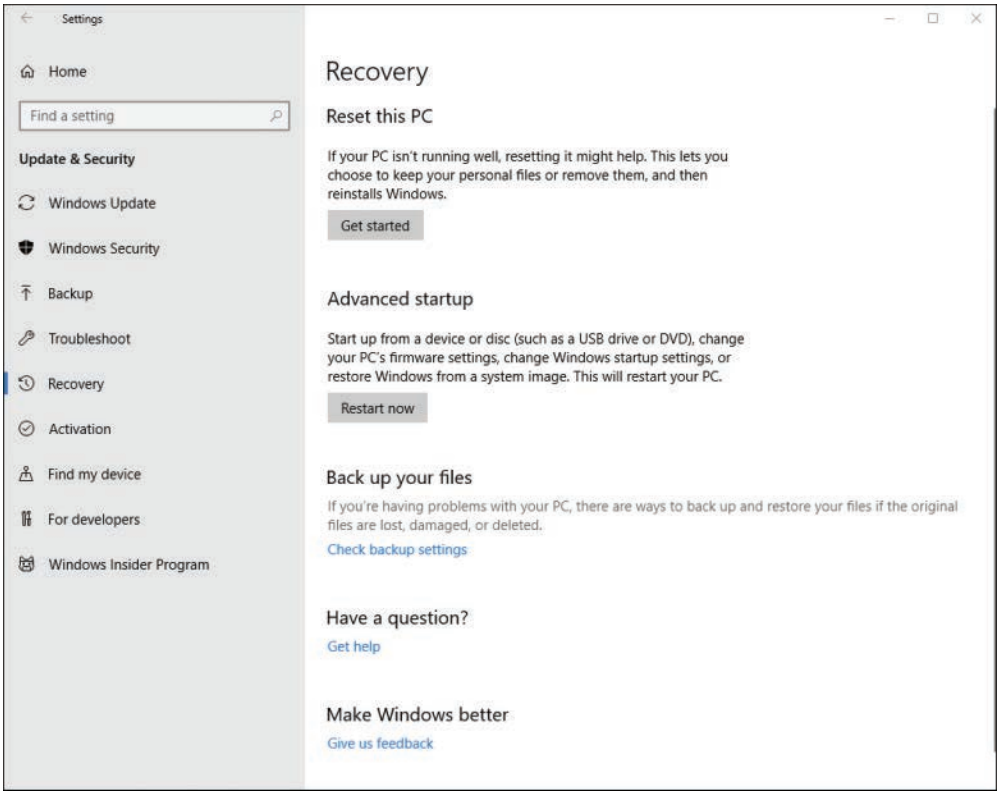


FIGURE 7-5 Windows 10 Recovery Options

Backup/Restore

Key Topic

Troubleshooting an infected PC can be done from a recovery drive. This is a drive that is created and put aside in case it is needed. The drive allows you to boot into a minimal Safe mode that does not install all applications or services. From this mode, you can remove infected files and reboot the computer to normal condition. Figure 7-6 shows the Windows 10 Backup options, which you access by going to **Settings > Update & Security > Backup**.

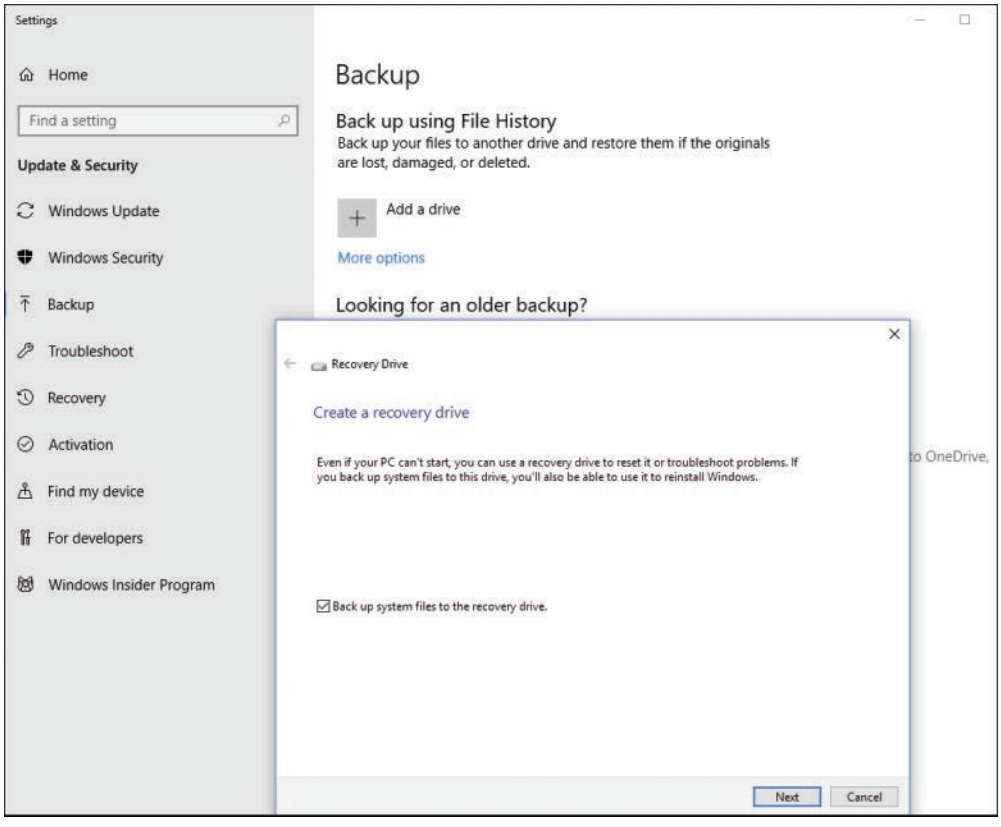


FIGURE 7-6 Tools for Creating a Recovery Drive in Windows 10

Backup/Time Machine

Some Linux distros already have a backup utility installed, and others rely on third-party software. Backing up in Linux can be done by creating a TAR (tape archive) file. macOS includes the Time Machine backup application. Both Linux and macOS must have their backup utilities configured and running in order to be useful in the event that data is lost.

macOS includes Time Machine, a backup utility that can be set up to automatically create daily backups and maintain weekly and monthly versions. To enable and configure Time Machine:

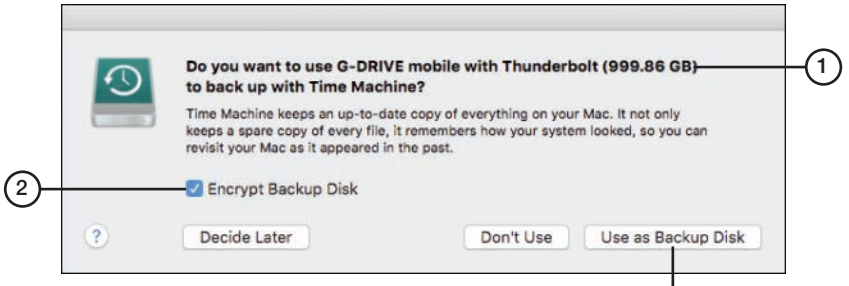
Step 1. Connect a suitable external disk to a macOS system.

Step 2. When prompted, click **Use as Backup Disk**. You can also check the Encrypt Backup Disk box to protect the backup (see Figure 7-7).

Key Topic

Step 3. If you selected the option to encrypt your backup in Step 2, enter a password, confirm it, and enter a password hint. Click **Encrypt Disk** (see Figure 7-8).

Step 4. Make sure Time Machine is turned on. After the selected disk is encrypted, the backup starts (see Figure 7-9).

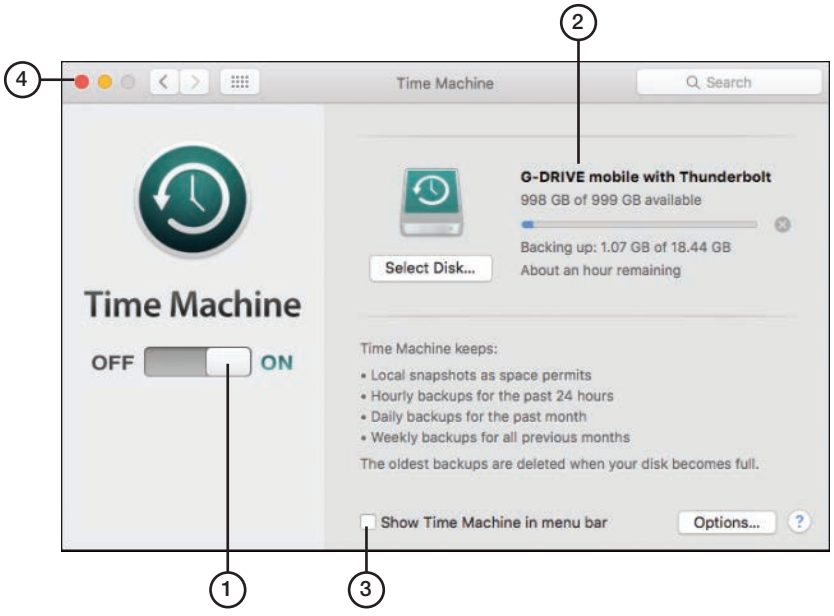


1. Newly-attached external drive
2. Check this box to encrypt backup drive
3. Click to use this drive with Time Machine

FIGURE 7-7 Selecting an External Disk for Use with Time Machine

1. Create and confirm password for encrypted Time Machine drive
2. Enter a password hint
3. Click to start encryption of Time Machine drive

FIGURE 7-8 Encrypting the Time Machine Disk



1. Time Machine turned on
2. Progress bar and backup disk information
3. Check box to put Time Machine on menu bar at top of screen
4. Click to close (Red) or minimize (Yellow) Time Machine menu

FIGURE 7-9 Creating a Backup with Time Machine

Time Machine is designed to back up user files automatically. However, to create a disk image that can be restored in case of disaster, use Disk Utility.

User Education/AUP (Acceptable Use Policy)

Regardless of the sophistication of physical or digital security measures, the lack of user education and an ***acceptable use policy (AUP)*** can lead to security issues. Some elements of a good AUP include the following:

Key Topic

- Have users ask for an ID when approached in person by somebody claiming to be from the help desk, the phone company, or a service company.
- Have users ask for a name and supervisor name when contacted by phone by someone claiming to be from the help desk, the phone company, or a service company.
- Provide contact information for the help desk, phone company, and authorized service companies and ask users to call the authorized contact person to verify that a service call or phone request for information is legitimate.

- Ask users to log into systems and then provide the tech the computer rather than giving the tech login information.
- Have users change passwords immediately after service calls.
- Ask users to report any potential social engineering calls or in-person contacts, even if no information was exchanged. Social engineering experts can gather innocuous-sounding information from several users and use it to create a convincing story to gain access to restricted systems.

Users should be educated in how to do the following:

- Keep antivirus, antispyware, and anti-malware programs updated.
- Scan systems for viruses, spyware, and malware.
- Understand major malware types and techniques.
- Scan removable media drives (such as optical discs and USB drives) for viruses and malware.
- Disable autorun (as described later in this chapter).
- Configure scanning programs for scheduled operation.
- Respond to notifications that viruses, spyware, or malware have been detected.
- Quarantine suspect files.
- Report suspect files to the help desk.
- Remove malware.
- Disable antivirus software when needed (such as during software installations) and know when to reenable antivirus software.
- Avoid opening attachments from unknown senders.
- Use anti-phishing features in web browsers and email clients.

Firewalls

Firewalls are used to prevent unauthorized communication into or out of a device or network. Android does not include a firewall, and third-party apps, such as NetGuard, NetStop Firewall, or AFWall+, must be used to provide protection against unwanted Internet traffic. Google Play offers many free firewall apps.

Apple does not include a firewall because the design of iOS uses a feature called "sandboxing" that runs apps in separate protected space.

Windows 10 has incorporated Windows Defender Firewall into the OS. When it is enabled to default settings, Windows Defender Firewall prevents the most common types of malicious traffic into the computer, and the user can customize the settings as needed. Windows Defender is discussed in much greater detail in Chapter 6.

DNS Configuration

Domain Name Service (DNS) involves a database containing public IP addresses and their associated domain names. The purpose of DNS is to translate domain names used in web page requests into IP addresses. Domain name server functions are included in SOHO routers, and in larger networks, a separate domain name server can be used. Domain name servers communicate with other, larger, domain name servers if the requested addresses are not in their databases.

Hackers like to capture DNS information because it provides links between domain names (such as company.com) and IP addresses. With DNS records, a hacker can create false DNS information that can point victims to fake websites and get them to download malware or viruses. Third-party software can provide DNS Security (DNSSEC) that secures a system's domain name server.

Configuring DNS is covered in Chapter 2, and here we review how the DNS settings are entered when configuring the NIC IPv4 properties. Domain name server addresses can be obtained automatically from the ISP, or they can be statically assigned. Figure 7-10 shows a statically assigned domain name server address and a backup alternative address.

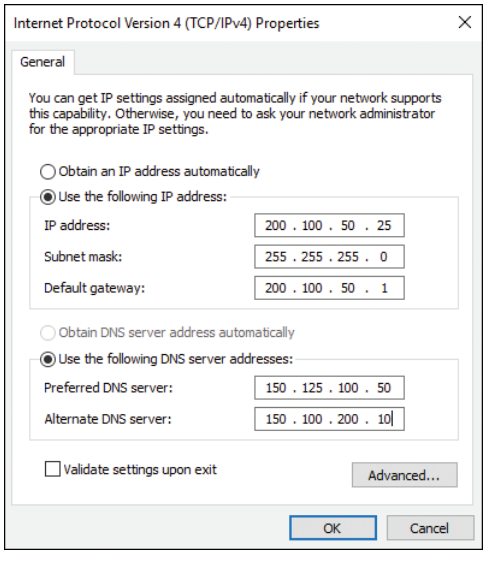


FIGURE 7-10 DNS Addressing Under NIC Properties

Social Engineering Threats and Vulnerabilities

220-1002 Exam

220-1002: Objective 2.5: Compare and contrast social engineering, threats, and vulnerabilities.

Botnets have made hacking so easy that any network can be tested by hackers thousands of times per day. Updated antivirus/anti-malware software and other software does the heavy lifting in protecting networks and devices. But another constant threat to a computer network is users being manipulated or tricked into doing hackers' work for them. This hacking technique is known as social engineering. The following sections describe social engineering and other threats and vulnerabilities to networks.

Social Engineering

Key Topic

Six common ***social engineering*** techniques that all employees in an organization should know about are phishing, spear phishing, impersonation, shoulder surfing, tailgating, and dumpster diving. The sections that follow describe each of these social engineering techniques.

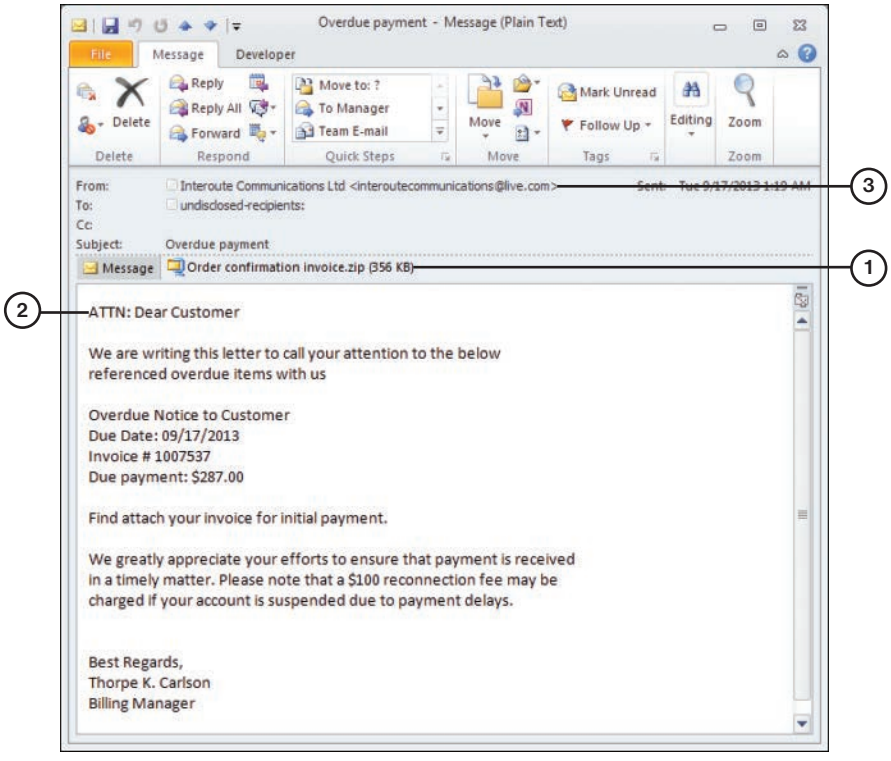
The key to mitigating these social engineering threats is a combination of ensuring employee awareness, implementing policies and protocols for handling sensitive internal information, and, whenever possible, using cybersecurity tools.

Phishing

Phishing involves creating bogus websites or sending fraudulent emails that trick users into providing personal, bank, or credit card information. A variation, phone phishing, uses an interactive voice response (IVR) system that the user has been tricked into calling to dupe the user into revealing information.

Phishing is a constant threat that can be addressed with awareness warnings from administrators that give examples of the latest threats and education for employees about using judgment to identify suspicious messages.

Figure 7-11 illustrates a typical phishing email.



1. **Zip archive files are frequently used by malware; open the file and your system is infected**
2. **Genuine emails from a company you work with will be addressed to a person or account number**
3. **Live.com is typically used by personal email, not company email**

FIGURE 7-11 A Message That Purports to Be About an Overdue Payment but Shows Classic Signs of a Phishing Attack

Spear Phishing

Spear phishing involves sending spoof messages that appear to come from an internal source requesting confidential information, such as payroll or tax information. These attacks typically target a specific person, organization, or business. The best protection against spear phishing is implementing security software that identifies spear phishing mail and educating users about how to handle sensitive information within the organization.

Impersonation

Impersonation is a type of social engineering similar to phishing in which a hacker sends an email pretending to be someone the victim trusts. It can take time and research for the impersonator to figure out how to gain the target's trust. Impersonation, also known as business email compromise (BEC), is not restricted to email but can happen on the phone or in person. Common sense and strict policies on how to communicate sensitive information can help prevent impersonation attacks.

Shoulder Surfing

Shoulder surfing is the attempt to view physical documents on a user's desk or electronic documents displayed on a monitor by looking over the user's shoulder. Shoulder surfers sometimes watch the keyboard to see passwords being entered. Shoulder surfers either act covertly, looking around corners, using mirrors or binoculars, or introduce themselves to the user and make conversation in the hopes that the user will let his or her guard down.

A common protection against shoulder surfing is a special privacy screen that limits the viewing range of a display. Employees should be trained to be aware of others being able to see their screens and to leave screens locked when away from their workstations.

Tailgating

Tailgating occurs when an unauthorized person attempts to accompany an authorized person into a secure area by following that person closely and grabbing the door before it shuts. This is usually done without the authorized person's consent, and sometimes the authorized person is tricked into believing the thief is authorized. If the authorized person is knowingly involved, it is known as ***piggybacking***. Mantraps, mentioned earlier, are designed to thwart tailgating.

Dumpster Diving

Going through the trash seeking information about a network—or a person with access to the network—is called ***dumpster diving***. This type of activity doesn't have to involve an actual dumpster, of course—just someone searching for any information that will help him or her socially engineer a way into a network. To limit the prospects of a dumpster diver, paper shredders or shredding services should be employed to keep available data limited.

DDoS

A ***distributed denial of service (DDoS)*** attack occurs when several (up to thousands) of computers have been compromised with special malware that turns them into bots. The bots then get directions from their new master to attack with thousands of requests to a network site. The traffic is so overwhelming that the site is unreachable by normal traffic and is effectively shut down.

DoS

A ***denial of service (DoS)*** attack involves one computer attacking a specific target with an overwhelming number of service requests. This is very similar to a DDoS attack but without the bots. The messages coming from one source can still take down a network, at great cost to a business.

Zero-Day

When legitimate software is sold and distributed, it may have security vulnerabilities that are unknown. When the flaws are discovered, the users may put out alerts while the software company who made the software creates a patch. Sometimes hackers watch for those alerts and exploit the vulnerabilities before the patch is installed, hence the term ***zero day***.

Man-in-the-Middle

A ***man-in-the-middle (MiTM)*** attack involves the attacker intercepting a connection while fooling the endpoints into thinking they are communicating directly with each other. Essentially, the attacker becomes an unauthorized and undetected proxy or relay point and the attacker uses this position to capture confidential data or transmit altered information to one or both ends of the original connection.

Brute Force

A ***brute force attack*** involves cracking passwords by calculating and using every possible combination of characters until the correct password is discovered. The longer the password used, and the greater the number of possible characters in a password, the longer brute forcing will take. One way an administrator can block brute forcing is to set authentication systems to lock after a specified number of incorrect passwords are offered. Longer passwords also aid in the fight against brute force attacks.

Dictionary Attacks

Dictionary attacks involve attempting to crack passwords by trying all the words in a list, such as a dictionary. A simple list might include commonly used passwords such as "12345678" and "password." Dictionary attacks can be blocked by locking systems after a specified number of incorrect passwords are offered. Requiring more sophisticated passwords that do not include identifiable information such as birthdays or family names is also a strategy that can be employed.

Rainbow Table

A ***rainbow table*** is used in an attack in much the same manner as in a brute force attack, but it is more mathematically sophisticated and takes less time. Rainbow tables are precomputed tables that can speed calculations when cracking hashes.

Spoofing

Spoofing is a general term for malware attacks that purport to come from a trustworthy source. Phishing, spear phishing, and rogue antivirus programs are three examples of spoofing.

Non-Compliant Systems

Non-compliant systems are systems that are tagged by a configuration manager application (for example, Microsoft's System Center Configuration Manager) for not having the most up-to-date security patches installed. Systems that don't have the most up-to-date security patches are especially vulnerable to attacks. An example of this would be a user attempting to log on to a corporate network with a personal computer that has not been updated to network standards that comply with the corporations specifications.

Zombie/Botnet

A ***zombie***/botnet is a computer on the Internet that has been taken over by a hostile program so it can be used for malware distribution or distributed denial of service (DDoS) or other attacks without notification to the regular users of the computer. Many malware attacks attempt to turn targeted computers into zombies on a hostile botnet.

Microsoft Windows OS Security Settings

220-1002: Objective 2.6: Compare and contrast the differences of basic Microsoft Windows OS security settings.

220-1002 Exam

Microsoft has made several security settings and tools available in the Windows OS. These settings and tools allow users and administrators to control access to files, folders, printers, and physical locations.

The sections that follow discuss the purposes and principles of ***access control*** through:

Key Topic

- Users and groups
- NTFS vs. share permissions
- Shared files and folders
- System files and folders
- User authentication
- Run as administrator vs. standard user
- BitLocker
- BitLocker To Go
- EFS

Users and Groups

Users in Windows can be assigned to different groups, each with different permissions. The Local Policy settings (for local PCs) and Group Policy settings (for networked PCs connected to a domain controller running Active Directory) can restrict PC features by group or by PC. The 220-1002 exam covers some of the differences between the accounts. There are three standard account levels in Windows:

- **Standard user:** Standard accounts have permission to perform routine tasks. However, these accounts are blocked from performing tasks that involve systemwide changes, such as installing hardware or software, unless they can provide an administrator password when prompted by User Account Control (UAC).
- **Administrator:** Users with an administrator account can perform any and all tasks.

- **Guest:** The guest account level is the most limited. A guest account cannot install software or hardware or run already-existing applications and cannot access files in shared document folders or the Guest profile. The Guest account is disabled by default. If it is enabled for a user to gain access to the computer, that access should be temporary, and the account should be disabled again when the user no longer requires access.

NOTE When a user is created using the Users applet in Windows, the user must be assigned a standard or administrator account. Guest accounts are used for visitors.

In Windows versions up to 8.1, the power users account is a specific account type that has more permissions than standard users but fewer than administrators. In those versions, power users have the same rights and permissions as standard users, but a custom security template can be created if the Power Users group needs specific permissions, such as for the operation of legacy programs.

In Windows 10 the Power Users group has been discontinued, but it is available to assign for backward compatibility.

NTFS vs. Share Permissions

Microsoft introduced ***New Technology File System (NTFS)*** as an improved way to store files on disks over the FAT system of Windows 95. The changes in storage systems allowed for implementing file security in the form of permissions. Permissions control both local and network access to files and can be set for individual users or groups.

Allow vs. Deny

Each permission has two settings: Allow or Deny. Generally, if you want a user to have access to a folder, you add that user to the list and select **Allow** for the appropriate permission. If you don't want to allow a user access, normally you simply don't add the user to a list. In some cases, an administrator must issue an explicit denial if the user is part of a larger group that already has access to a parent folder but needs to be kept out of a particular subfolder.

Moving and Copying Folders and Files

Moving and copying folders and files have different results depending on permissions. For example, when you copy a folder or file to a different volume, the folder

or file inherits the permissions of the parent folder it was copied to (the target directory). When you move a folder or file to a different location on the same volume, the folder or file retains its original permissions.

File Attributes

File attributes are used in Windows to indicate how files can be treated. They can be used to specify which files should be backed up, which should be hidden from the normal GUI or command-line file listings, whether a file is compressed or encrypted, and so on, depending on the operating system.

To view file attributes in Windows, right-click a file in File Explorer or Windows Explorer and select **Properties**. To view file attributes from the Windows command line, use the **Attrib** command.

Shared Files and Folders

Key Topic

Shared files and folders have their permissions assigned via the Security tab of the object's properties sheet. Folder and file permissions vary by user type or group and can include the following:

- **Full control:** Complete access to the contents of the file or folder. When Full Control is selected, all of the following are selected and enabled automatically.
- **Modify:** Change file or folder contents.
- **Read & Execute:** Access file or folder contents and run programs.
- **List Folder Contents:** Display folder contents.
- **Read:** Access a file or folder.
- **Write:** Add a new file or folder.

Administrative Shares vs. Local Shares

Local shares are normally configured on a folder or library basis in Windows. However, Windows sets up special ***administrative shares*** that are available across a network for each local drive. For example, the administrative share for the C: drive on a system called MARK-PC is \\MARK-PC\C$.

To connect to the administrative share, a user must provide a username and password for an account on that system.

Permission Inheritance and Propagation

Permission propagation and inheritance describe how files and folders receive permissions.

If you create a folder, the default action is for the folder to inherit permissions from the parent folder—that is, any permissions that you set in the parent will be inherited by any subfolder of the parent. To view an example of this, locate any folder within an NTFS volume (besides the root folder), right-click it and select **Properties**, access the **Security** tab, and then click the **Advanced** button. In Windows 8/8.1/10, the Advanced Security Settings dialog offers these buttons: Add, Remove, View, and Disable Inheritance.

You can also propagate permission changes to subfolders that are not inheriting from the current folder. To do so, select **Replace All Child Object Permissions with Inheritable Permissions from This Object**. Remember that folders automatically inherit from the parent unless you turn off inheritance, and you can propagate permission entries to subfolders at any time by selecting the **Replace** option.

System Files and Folders

System files and folders are files and folders with the system(s) attribute. They are normally not displayed in File Explorer to help protect them from deletion.

To make these files and folders visible in Windows 10:

Step 1. Open **File Explorer**.

Step 2. In the top left select the **View** tab.

Step 3. Uncheck the boxes that are hidden that need to be viewed.

Figure 7-12 depicts the File Explorer boxes that hide files.

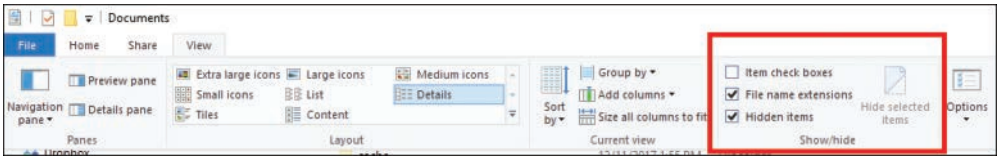


FIGURE 7-12 Showing Hidden Files in Windows 10

User Authentication

Authentication is the process of securely determining that authorized persons accessing computers or network are who they say they are. Windows includes a

variety of authentication protocols that can be used on a corporate network, including Kerberos, TLS/SSL, PKU2U, and NTLM.

Apple, Microsoft, and Google use mutual authentication for multiple services (also known as ***SSO*** or ***Single Sign-on***) to enable a single login that provides access to multiple services. For example, a single Microsoft Account login provides access to Outlook email, the Microsoft Store, and OneDrive. To make SSO possible in Windows, client IP addresses are mapped to usernames in Windows Active Directory. Similarly, a single Apple login provides access to iTunes, iCloud, and other services. A single Google login provides access to Gmail, Google Drive, and other services.

Key Topic

BitLocker and BitLocker To Go

To encrypt an entire drive, you need some kind of full disk encryption software. Several options are currently available on the market; one option developed for business-oriented versions of Windows by Microsoft is called ***BitLocker***. This software can encrypt the entire disk, which, after completed, is transparent to the user. However, there are some requirements for this, including:

- A ***Trusted Platform Module (TPM)*** chip, which is a chip residing on the motherboard that actually stores the encrypted keys.

Key Topic

or

- An external USB key to store the encrypted keys. Using BitLocker without a TPM chip requires changes to Group Policy settings.

and

- A hard drive with two volumes, preferably created during the installation of Windows. One volume is for the operating system (most likely C:), and it will be encrypted; the other is the active volume, and it remains unencrypted so that the computer can boot. If a second volume needs to be created, the BitLocker Drive Preparation Tool can be of assistance; it can be downloaded from the Microsoft Download Center.

BitLocker software is based on Advanced Encryption Standard (AES) and uses a 128-bit encryption key.

Since Windows Vista SP1, it has been possible to use BitLocker to encrypt internal hard disk volumes other than the system drive. For example, if a hard disk is partitioned as C: and D: drives, BitLocker can encrypt both drives.

Windows 10 has several enhancements that allow BitLocker to be more user friendly, but the essentials of BitLocker are the same as in Windows 7.

BitLocker To Go

In Windows 7 and later versions, BitLocker functionality is extended to removable drives and external USB drives (including flash drives) with ***BitLocker To Go***.

To enable BitLocker on Windows 10, go to the **Control Panel > System and Security > BitLocker Drive Encryption**. For external drives, simply right-click the drive to encrypt and select **Enable BitLocker** to start the encryption process. During the process, you are prompted to specify a password or a smart card for credentials to access the drive's contents.

EFS

Business-oriented editions of Windows include support for ***Encrypting File System (EFS)***. EFS can be used to protect sensitive data files and temporary files and can be applied to individual files or folders. (When EFS is applied to folders, all files in an encrypted folder are also encrypted.)

EFS files can be opened only by the user who encrypted them, by an administrator, or by EFS keyholders (users who have been provided with the EFS certificate key for another user's account). Thus, they are protected against access by hackers.

Files encrypted with EFS are listed with green filenames when viewed in Windows Explorer or File Explorer. Only files stored on a drive that uses NTFS can be encrypted.

Key Topic

To encrypt a file in Windows 10, follow this process:

Step 1. Right-click the file in File Explorer and select **Properties**.

Step 2. Click the **Advanced** button on the General tab.

Step 3. Click the empty **Encrypt Contents to Secure Data** check box. Figure 7-13 shows the steps for EFS encryption.

Step 4. Click **OK**.

Step 5. Click **Apply**. When prompted, select the option to encrypt the file and parent folder or only the file as desired and click **OK**.

Step 6. Click **OK** to close the properties sheet.

To decrypt the file, follow the same procedure but clear the **Encrypt Contents to Secure Data** check box in Step 3.

NOTE To enable the recovery of EFS encrypted files in the event that Windows cannot start, you should export the user's EFS certificate key. For details, see the Microsoft TechNet article "Data Recovery and Encrypting File System (EFS)" at https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc512680(v=technet.10).

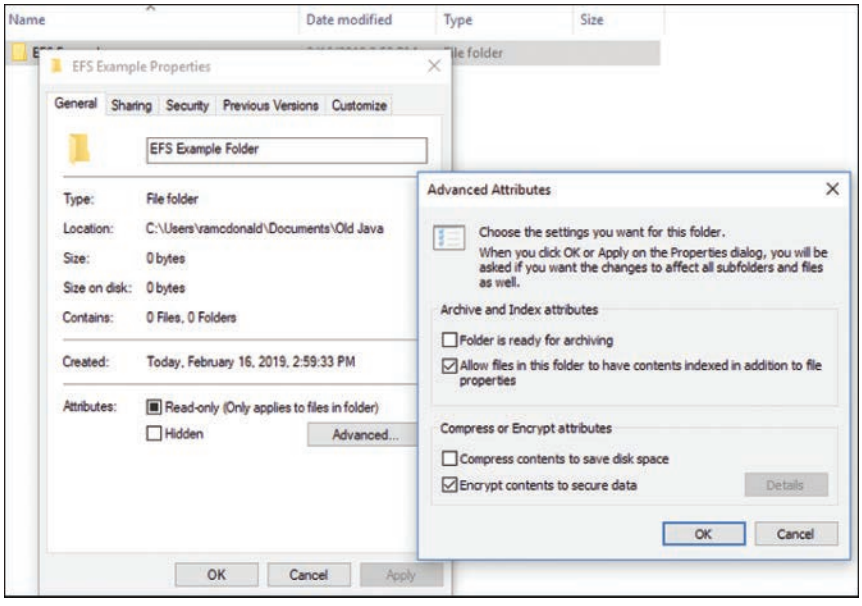


FIGURE 7-13 EFS Encryption Steps

Security Best Practices to Secure a Workstation

220-1002: Objective 2.7: Given a scenario, implement security best practices to secure a workstation.

220-1002 Exam

Secure workstations are the foundation of secure networks. If an outside hacker or thief can access a workstation, the whole network may be compromised. The following sections cover use of passwords, account management, and other methods to make workstations secure.

Password Best Practices

Key Topic

Not all passwords are equally secure, and some are very easy to hack. It is important that administrators use stringent security policy settings to require users to follow strict guidelines for password they use to access the network. The guidelines in the following sections reflect password best practices.

Setting Strong Passwords

Guidelines for setting strong passwords should include requirements for minimum length and a mixture of alphanumeric and symbol characters. Every extra character in a password makes it much harder to hack. Using a password generator can make the creation of strong passwords easier. For example, the Norton Identity Safe Password Generator (https://identitysafe.norton.com/password-generator) offers highly customizable random passwords and can generate multiple passwords at the same time.

Password Expiration

No matter how strong a password is, it becomes less secure over time. The longer it is in use, the more susceptible it is to social engineering, brute forcing, or other attacks. The risk of password discovery by unauthorized users is minimized by the use of a password expiration policy under which passwords expire after a particular length of time and must be reset.

Screensaver Required Password

To help protect computers from unauthorized use, users can be required to enter their password to return to the desktop after the screensaver appears. Users should also be required to lock their workstations so that a logon is required to return to the desktop. (See "Timeout/Screen Lock," later in this chapter, for details.)

In Windows, the screensaver required password setting (**On Resume, Display Logon Screen** check box) is located in the Screen Saver Settings window, which can be accessed from **Settings > Personalization** in Windows 10. In macOS, use the **Desktop & Screen Saver** menu to choose a screen saver and **Security & Privacy** to require a password to unlock the system.

BIOS/UEFI Passwords

BIOS/UEFI passwords prevent unauthorized users from changing settings. Note that they can be removed by resetting the CMOS. Some motherboards feature a jumper block or a push button to reset the CMOS. If this feature is not present, the CMOS can be reset by removing the CMOS battery for several minutes. Configuration of BIOS/UEFI security settings is covered in more detail in Chapter 3, "Hardware."

Requiring Passwords

PC users should be trained to use passwords to secure their user accounts. Administrators can require this through the Local Security Policy and Group Policy in Windows.

Passwords can be set up to require users to do the following:

- Change passwords periodically to keep them fresh and secure.
- Be informed in advance that passwords are about to expire so that users can change passwords early and prevent being locked out at an inconvenient time.
- Enforce a minimum password length to keep passwords strong.
- Require complex passwords that include a mixture of letters, numbers, and special characters.
- Prevent old passwords from being reused continually by tracking past passwords and not allowing them.
- Wait a certain number of minutes after a specified number of unsuccessful logins has taken place before being able to log in again.

To create a password or adjust password settings in Windows 10, go to **Settings > Accounts > Sign-in Options**. To change or enforce password policy settings, go to the following location by using the Group Policy Management Console: **Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy**. Figure 7-14 shows the path to these settings.

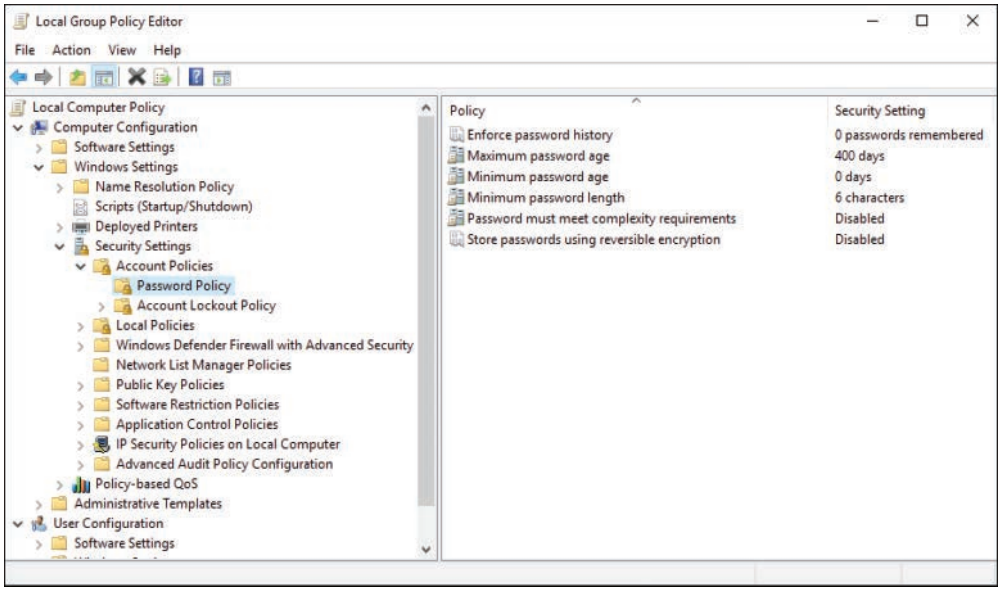


FIGURE 7-14 Password Policy Settings

Account Management

User account settings, when combined with workstation security settings, help prevent unauthorized access to the network. The account management settings described in the sections that follow can enhance security.

Restricting User Permissions

User permissions for standard users prevent systemwide changes, but additional restrictions can be set with Group Policy or Local Security Policy.

Login Time Restrictions

To prevent a user account from being used after hours or before the start of business, login time restrictions can be used to specify when an account can be used.

Disabling Guest Account

The guest account in Windows is a potential security risk, so it should be disabled. If visitors need Internet access, a guest wireless network that doesn't connect to the business network is a good replacement.

Failed Attempts Lockout

Password policy should specify that a user should be locked out after a specified number of failed attempts to log into an account. A lockout policy can also incorporate a timeout policy, which specifies how long the user must wait after an unsuccessful login before attempting to log in again.

Timeout/Screen Lock

Automatic screen locking can be configured to take effect after a specified amount of idle time, which can help safeguard a system if a user forgets to lock the system manually. Before screen locking can be used, accounts must have the screen lock feature enabled. In Windows 10, go to **Settings > Personalization > Lock Screen**.

In Windows, users can lock their screens manually by pressing **Windows+L** on the keyboard or pressing **Ctrl+Alt+Del** and selecting **Lock Computer**. In Linux, the keys to use vary by desktop environment. In macOS, use **Ctrl+Shift+Eject** or **Ctrl+Shift+Power** (for keyboards without the Eject key).

Changing Default Usernames and Passwords

Default usernames and passwords for SOHO routers or other devices or services that have default passwords should be changed. Default usernames and passwords are available in documentation for these devices, so it is easy for an attacker to find the defaults and use them to take over routers or other devices that are still set to the default passwords.

Basic Active Directory Functions

Active Directory (AD) functions occur in the Windows Server environment, not on local workstations. A full discussion of Active Directory is well beyond the scope of the CompTIA A+ exam, but understanding the essentials of user accounts is necessary because user access issues are a common for support personnel. If a support technician has access to Active Directory, basic user account functions can be performed in the Microsoft Management Console (MMC) or by navigating to the Active Directory Users and Computers folder. This second method is used in Figure 7-12, which shows an account being created.

Creating, Deleting, Resetting/Unlocking, and Disabling an Account

To create an account, select **Action > New > User** (or right-click the **Users** folder), as shown in Figure 7-15. Windows opens a dialog where you now enter the new user's account information, as shown in Figure 7-16.

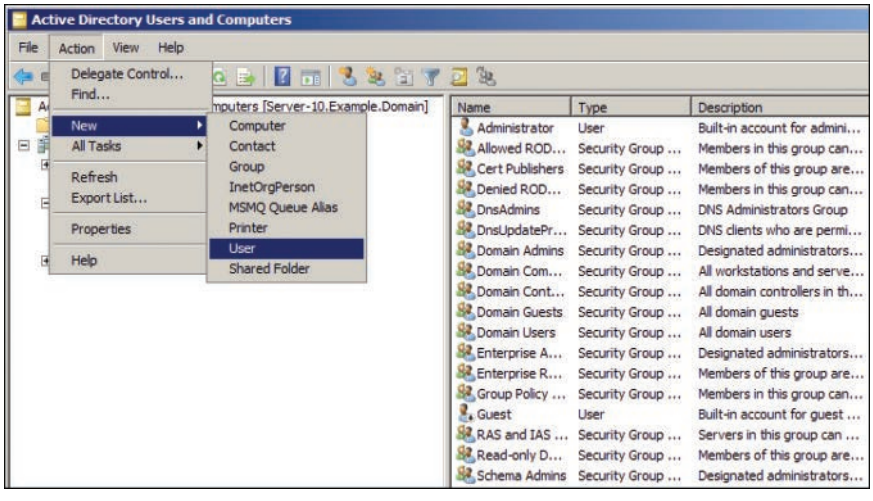


FIGURE 7-15 Creating a New User Account in Active Directory Users and Computers

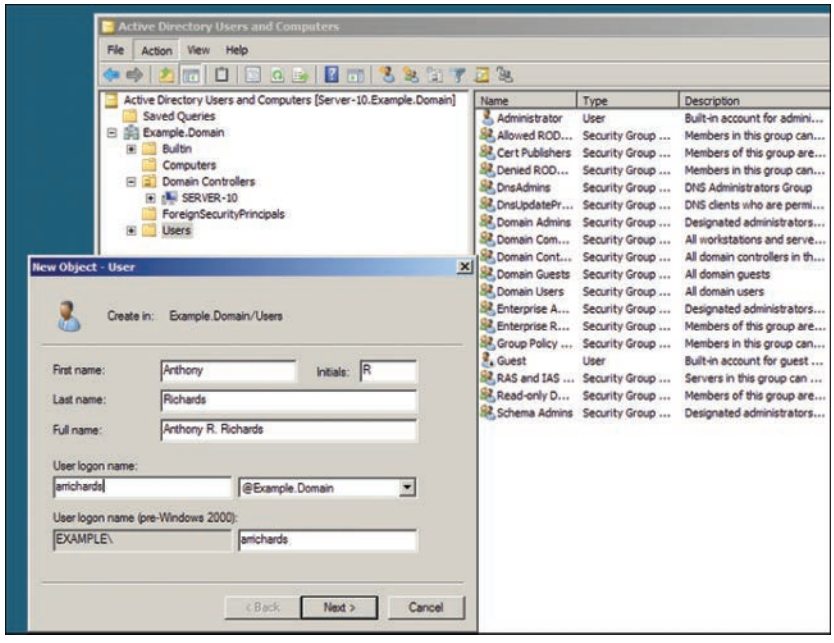


FIGURE 7-16 New User Account

Click the **Next** button, and an initial password dialog box appears. Figure 7-17 shows this dialog for a new account; note that this dialog allows you to set a password and indicate how the password will be managed by Active Directory.

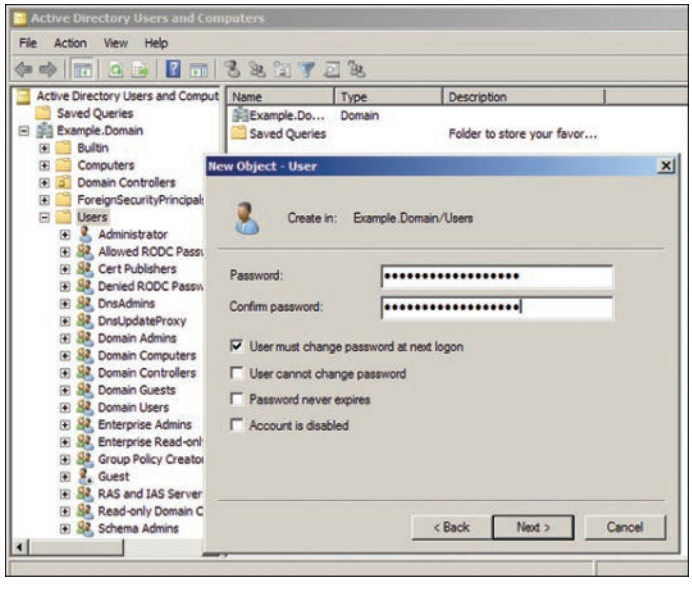


FIGURE 7-17 Initial Password Dialog Box

Click the **Next** button to create the user.

After a user is created, a technician might need to perform a few common tasks:

- **Account deletion:** A technician might need to completely remove a user from Active Directory.
- **Password reset/unlock:** This may need to be done when a user has forgotten a password or failed to authenticate.
- **Disable account:** It is possible to deactivate a user but keep the account and its records.

These tasks can all be performed by right-clicking on a user's name. Note that commands for all three of these functions—Delete, Reset Password, and Disable account—appear in the menu in Figure 7-18.

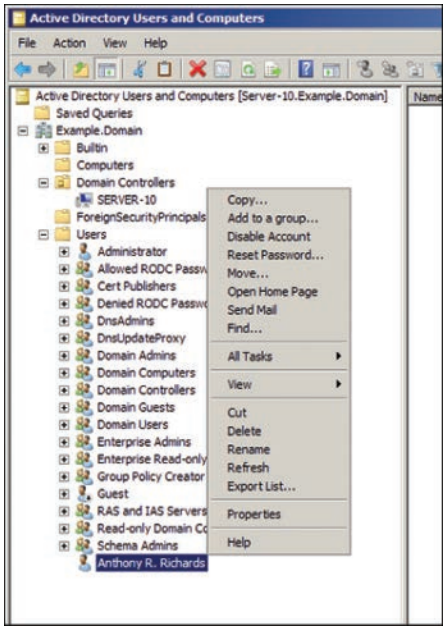


FIGURE 7-18 User options in Active Directory

Disabling Autorun/AutoPlay

Autorun is a feature that enables programs to start automatically when a CD or USB drive or flashcard is connected to a computer. AutoPlay is a similar feature with enhanced options in a Windows environment. Both Autorun and AutoPlay allow the user to be selective in what kinds of programs, updates, and syncs can take place. When you disable autorun, an optical disc or USB drive won't automatically start its autorun application (if it has one), and any embedded malware won't have a chance

to infect the system before you scan the media. AutoPlay is a similar feature that pops up a menu of apps to use for the media on an optical drive or USB flash drive.

The easiest way to turn off AutoPlay in Windows 10 is to open the AutoPlay applet in **Settings > Devices > AutoPlay** and toggle the button off. Figure 7-19 shows the AutoPlay Settings window in Windows 10. Figure 7-20 shows how to turn off AutoPlay from the Group Policy settings.

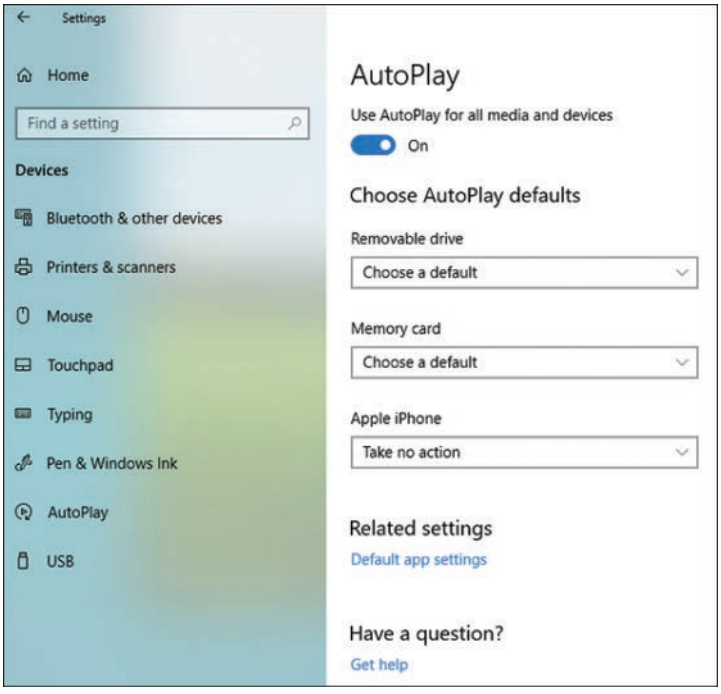


FIGURE 7-19 AutoPlay Settings in Windows 10

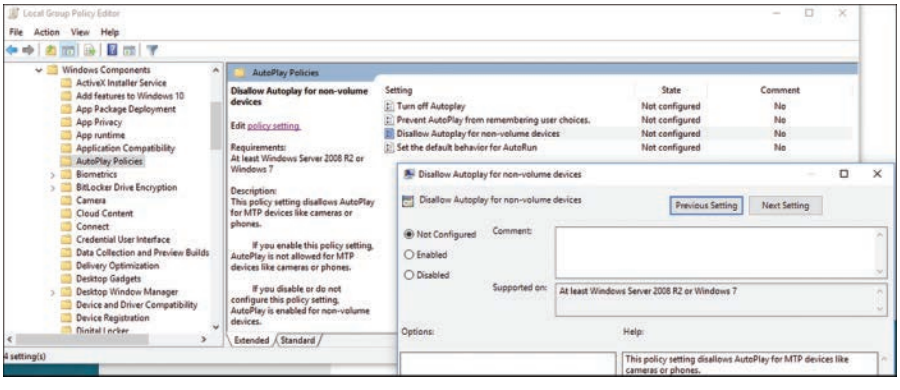


FIGURE 7-20 Disabling Autoplay in the Group Policy Settings

To disable autorun in Windows by using Local Group Policy, complete the following steps:

Step 1. Click **Start** and in the search field type **gpedit.msc** to open the Local Group Policy Editor.

Step 2. Navigate to **Computer Configuration > Administrative Templates > Windows Components > AutoPlay Policies**.

Step 3. Double-click the **Turn Off AutoPlay** setting to display the Turn Off AutoPlay configuration window.

Step 4. Click the **Enabled** radio button and then click **OK** to enable the policy named Turn off AutoPlay.

NOTE Laptops that do presentations might require AutoPlay.

For security reasons, macOS does not support any type of autorun feature, but it is possible to select apps you want to run on startup. To edit this list, select **Apple menu > System Preferences > Users and Groups > Login Items**.

In Linux, you can disable autorun on systems that use the Nautilus file manager by changing the properties on the Media tab to enable **Never Prompt or Start Programs on Media Insertion** and disable **Browse Media When Inserted**.

Using Data Encryption

Data encryption should be used on laptops and other systems that might be used outside the more secure corporate network environment. Laptops containing unencrypted sensitive data have led to many data breaches. To encrypt folders or drives, use the following steps:

Step 1. Right-click the folder or drive to be secured and select **Properties**.

Step 2. Click the **Advanced** button at the bottom of the General tab.

Step 3. In the Advanced Attributes dialog, select the **Encrypt Contents to Secure Data** check box and click **OK**.

These steps are shown in Figure 7-21, where a folder named A+ is being encrypted.

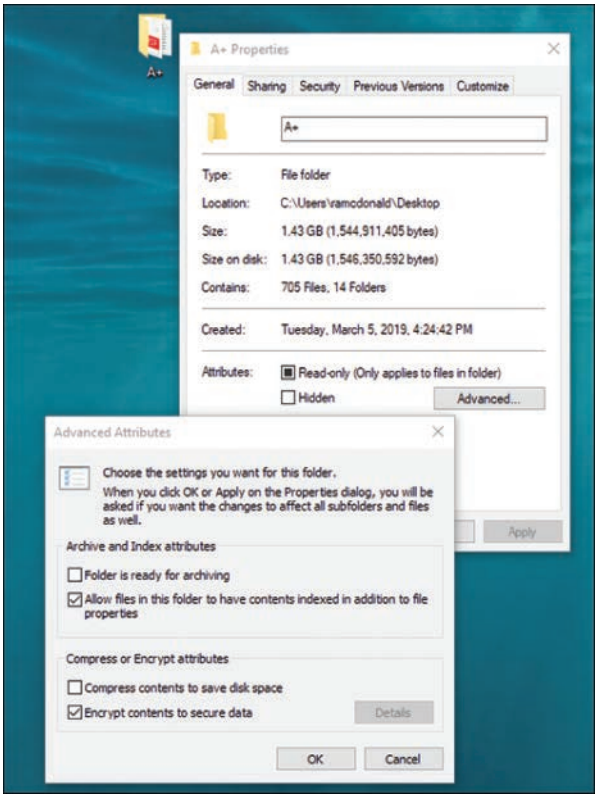


FIGURE 7-21 Encrypting Files or Drives

Patch/Update Management

Patches and updates to operating systems and applications should be managed centrally to prevent systems from falling out of compliance. Microsoft's Windows Server Update Services (WSUS) can be used for OS and application patches and updates for Microsoft products. macOS Server's Software Update service provides the same role for macOS machines. Linux distributions use various programs to manage updates.

Securing Mobile Devices

220-1002 Exam

220-1002: Objective 2.8: Given a scenario, implement methods for securing mobile devices.

Mobile devices have evolved to the point that they can hold as much valuable data as any workstation. Add to this their compact and easy-to-conceal design and the high

cost of the devices, and it becomes clear why mobile devices pose a serious security threat. The following sections cover methods and practices that can mitigate mobile device threats.

NOTE For the 220-1002 exam, be familiar with:

Key Topic

- Screen locks
- Remote wipes
- Locator applications
- Remote backup applications
- Failed login attempt restrictions
- Antivirus/anti-malware
- Patching/OS updates
- Biometric authentication
- Full device encryption
- Multifactor authentication
- Authenticator applications
- Trusted sources vs. untrusted sources
- Firewalls
- Policies and procedures

Screen Locks

The first step in securing a mobile device is setting a numeric passcode or another type of ***screen lock***. Such a passcode locks the device, making it inaccessible to everyone except those who know the passcode and experienced hackers. A screen lock can be a pattern that is drawn on the display, a PIN (passcode lock), or a password. A very strong password is usually the strongest form of screen lock. The screen lock setting can be accessed on an Android device by going to **Settings > Security**. On iPhone 6, go to **Settings > Touch ID > Passcode** (requires entering current passcode). On iPhone 7 go to **Settings > General > Passcode**. On iPhone X and later, go to **Settings > FaceID & Passcode**. While the navigation will vary between Android and iPhone versions, the settings here apply to both types of phones unless noted.

You can select how long the phone waits after inactivity to lock; this is usually set to three or five minutes, but in a confidential environment, it may be appropriate to set this to **Immediate**. To enable Auto-Lock, go to **Settings > General > Auto-Lock** and select a number of minutes. If this is set to **Never**, the device will never sleep,

negating the security of the passcode and using valuable battery power. The default setting is two minutes. On an iPhone, Auto Lock is under the Display Settings area.

In addition to the default timeout, devices can also be locked by pressing the power button quickly. If configured, the passcode must be supplied whenever a mobile device comes out of a sleep or lock state and whenever it is first booted.

Some devices support other types of screen locking, including ***fingerprint lock*** (where the user's fingerprint is matched against a list of authorized user fingerprints) and ***face lock*** (where the user's face is matched against a list of authorized user faces). Windows Hello, a Windows 10 feature supported on some devices, is an example of a face lock. Face ID is the Apple version that is supported on newer versions of iPhone and iPad Pro.

A ***swipe lock*** app immediately locks a device when the user swipes the display to one side.

The next option on the Security screen is Visible Passwords. If this option is checked, the device shows the current letter of the password being typed by the user. This type of setting is vulnerable to shoulder surfers (people looking over your shoulder to find out your password) and should be deselected so that only asterisks (*) are shown when the user types a password.

There is also a Credential Storage option. By default, secure credentials are dropped after a session is over. (An exception to this rule is a Gmail or other similar login.) However, if Use Secure Credentials is checked, and a user accesses a website or an application that requires a secure certificate, the credentials are stored on the device. A user can set a password here so that only he or she can view or clear credentials or install credentials from a memory card. The use of secure credentials is usually configured only if a user needs access to confidential company information on the Internet.

Passcode locking can be accessed on iPad and iPhone devices by going to **Settings > Passcode** and tapping **Passcode Lock** to display the Passcode Lock screen. Tap **Turn Passcode On** to set a passcode.

Remote Wipes

A lost or missing mobile device is a serious security threat. A hacker can get past passcodes and other screen locks. It's just a matter of time before the hacker has access to the data. So, an organization with confidential information should consider enabling a ***remote wipe*** program of a device. As long as the mobile device still has access to the Internet, the remote wipe program can be initiated from a desktop computer to delete all the contents of the remote mobile device.

Some devices (such as the iPhone) have a setting that causes the device to be erased after a certain number of incorrect password attempts (10 in the case of the iPhone). There are also third-party apps available for download for most mobile devices that can wipe the data after a specified number of attempts. Some apps configure a device to automatically take a picture after three failed attempts and email the picture to the device owner. Examples of software that can accomplish this include Google Sync, Google Apps Device Policy, Apple's Data Protection, and third-party apps such as Mobile Defense. In some cases, such as with Apple's Data Protection, the command that starts the remote wipe must be issued from an Exchange server or mobile device management (MDM) server. Of course, you should have a backup plan in place as well so that data on the mobile device is backed up to a secure location at regular intervals. This way, if the data needs to be wiped, you know that most or all of the data can be recovered. The type of remote wipe program, backup program, and policies regarding how these are implemented can vary from one organization to the next.

Locator Applications

By installing or enabling a ***locator application*** or service such as Android Device Manager, Lookout for iOS or Android, or Find My iPhone, a user can track down a lost device. These apps can be operated from any other phone that has a similar app installed as long as the power is on and geolocation is working.

Remote Backup Applications

There are two ways to back up a mobile device: via a USB connection to a desktop or laptop computer or to the cloud by using a ***remote backup application***.

Apple's iCloud offers free cloud backup service for a limited amount of data (currently 5GB), with more space available by subscription. iTunes, which can be used for USB-based backup, enables the entire device to be backed up to a hard drive at no additional cost.

Android users have free backup for email, contacts, and other information via Google Cloud. However, backing up photos, music, and other content and documents must either be performed manually via USB or file sync to the cloud, using a service such as Dropbox or another third-party app.

Both iOS and Android users can use popular third-party cloud-based backups that are also supported for macOS and Windows, such as Carbonite (carbonite.com) and iDrive (idrive.com).

Failed Login Attempts Restrictions

Most mobile devices include failed login attempt restrictions. If a person fails to enter the correct passcode after a certain number of attempts, the device locks temporarily, and the person has to wait a certain amount of time before attempting the passcode again. If the person fails to enter the correct passcode again, on most devices the timeout increases. As mentioned earlier, multiple failed logins may result in a remote wipe of the hard drive.

Antivirus/Anti-malware

Just as there is antivirus software for PCs, there is also antivirus/anti-malware software for mobile devices. These are third-party applications that need to be paid for, downloaded, and installed to the mobile device. Some common examples for Android include McAfee's VirusScan Mobile, AVG, Lookout, Dr. Web, and NetQin.

iOS works a bit differently than Android. iOS is a tightly controlled operating system. One of the benefits of being a closed-source OS is that it can be more difficult to write viruses for it, making it somewhat more difficult to compromise. But there is no OS that can't be compromised. For the longest time there was no antivirus software for iOS, but Apple now allows the download of previously unavailable applications and software not authorized by Apple.

Patching/OS Updates

Patching/OS updates help protect mobile devices from the latest vulnerabilities and threats. By default, you are notified automatically about available updates on Android and iOS-based devices. However, you should know where to go to manually update these devices as well:

- For Android, go to **Settings > General > About Device > Software Update** or **Settings > System > About Device > Software Update > Check for Updates**.
- For iOS, go to **Settings > General > Software Update**.

When it comes to large organizations that have many mobile devices, a mobile device management (MDM) suite should be used. McAfee and many other companies have MDM software suites that can take care of pushing updates and configuring many mobile devices from a central location. Decent-quality MDM software secures, monitors, manages, and supports multiple different mobile devices across the enterprise.

Biometric Authentication

Both current and older Android and iOS devices can use ***biometric authentication*** through the use of add-on fingerprint readers or iris readers.

Recent and current iOS devices have built-in support for fingerprint reading with all Touch ID feature enabled phones and iPad versions.

Face locks, like Microsoft's Windows Hello and Apple's Face ID, are also considered a type of biometric authentication.

Full Device Encryption

With ***full device encryption***, your data is not accessible to would-be thieves unless they know the passcode. Apple's iOS devices feature full device encryption that is activated when a passcode is assigned to the device. To learn more about this and other iOS security, Apple provides an iOS Security guide at https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

Android 5 and later supports full disk encryption, and Android 7 and later supports file-based encryption. File-based encryption is encryption on individual files, meaning each file has a separate encryption key, so all the phone resources do not have to be tied up in the encryption process.

Multifactor Authentication

Any authentication method for email, e-banking, or other tasks that requires two forms of authentication is considered multifactor authentication. For example, websites and apps might require authentication of both the account information (name and password) and the device being used to access the account. Typically, this is done by sending an SMS text message or making a robocall to the pre-registered mobile phone of the account holder. The account holder must enter the code received when prompted by the website or app before the app can run or the website opens. Unless the app is deleted or cookies are deleted from the browser, the device is an approved device for that account.

Authenticator Applications

An ***authenticator application*** is used to receive or generate authentication codes for one or more apps or services.

Google Authenticator from the Google Play app store enables a user to receive or generate multifactor codes with Android, iOS, and BlackBerry devices. It supports options to add or remove trusted computers and devices and works with the Security

Key USB device. There are several other authenticator apps for mobile devices, but before selecting one, be sure to determine which websites and services it supports.

Trusted Sources vs. Untrusted Sources

The Apple Store (apps for iOS), Google Play (Android), and Microsoft Store (Windows 10 Mobile) are trusted sources for apps for mobile devices. Apps downloaded from other locations are considered untrusted and should not be used if at all possible. Jailbreaking the phone is usually required to run untrusted apps, and jailbreaking removes security measures built into the phones.

Firewalls

Android does not include a firewall, so third-party apps must be used to provide protection against unwanted Internet traffic. Google Play offers many free firewall apps for Android.

Apple does not include a firewall because the design of iOS uses a feature called "sandboxing" that runs apps in separate protected space.

Policies and Procedures

Many individually owned mobile devices are now being used on corporate networks. Because these devices were not configured by the corporation, they could potentially present security threats. To prevent security threats, organizations need to address these issues in their policies and procedures.

BYOD vs. Corporate-Owned Devices

Benefits of ***bring your own device (BYOD)*** policies include:

- No hardware cost to the organization
- Higher usage due to employee satisfaction with their selected device
- Greater productivity

Potential drawbacks include:

- Hidden costs of management and security
- Possibility that some employees will not want to buy their own devices

Profile Security Requirements

Whether an organization uses corporate-owned mobile devices, BYOD, or a mixture, setting and following profile security requirements are very important to

achieving increased productivity without incurring significant risks. Issues involved include specifying approved devices and operating system versions, requiring passwords and lock screens, requiring device encryption, support issues, and when and how to remove company information when an employee leaves the organization.

Data Destruction and Disposal

220-1002: Objective 2.9: Given a scenario, implement appropriate data destruction and disposal methods.

220-1002 Exam

Even after computers, mobile devices, and even some types of printers have reached the end of their useful lives, the hard drives inside contain potential security risks. Risks also lie in flash drives, external drives, and optical media. To prevent confidential company or client information from being accessed from a computer or another device that is being disposed of for resale, recycling, or deconstruction for parts, the methods in the following sections should be used.

NOTE For the 220-1002 exam, the importance of these methods should be well understood.

- Physical destruction methods
- Recycling or repurposing best practices

Physical Destruction Methods

Physical destruction renders a mass storage device into small pieces that cannot be reconstructed, making the data inside unrecoverable. Methods include the following:

Key Topic

- **Shredder:** Some office-grade shredders can be used to destroy optical media. Electronics recyclers use heavy-duty shredders made for hard disks and mass storage devices to reduce storage devices, tape, or other types of media into small bits.
- **Drill/Hammer:** Remove the hard disks and destroy their platters with a drill, hammer, or other device; then recycle the scrap.
- **Electromagnetic (degaussing):** Other tools such as electromagnetic degaussers and permanent magnet degaussers can also be used to permanently purge information from a disk. The drive is physically intact, but all data, formatting, and control track data is missing. Use this type of physical destruction if you want to use a drive for display purposes.
- **Incineration:** Incineration of tape, floppy, and other types of magnetic and optical media is allowed in some areas and available from various companies.

Data-recycling companies that destroy hard drives or other storage devices can provide a certificate of destruction to prove compliance with local laws or institutional policies.

Recycling or Repurposing Best Practices

As long as the data on a hard drive or other mass storage device can be rendered unrecoverable, it is not necessary to destroy the media itself. The following are some best practices for recycling and repurposing:

Key Topic

- **Low-level format vs. standard format:** The standard format used in operating systems is a quick format. This type of format clears only the root folder. The remainder of the data on the disk can be recovered until it is overwritten. A long format rewrites the disk surface. However, data recovery programs available from many third-party firms can recover data from a formatted drive. A low-level format that creates the physical infrastructure where data will be stored on a disk is performed by the drive manufacturer before the drive is shipped and cannot be performed in the field.
- **Overwrite:** Some disk maintenance programs from mass storage vendors include options to ***overwrite*** a hard disk's or SSD's data area with zeros. Data recovery programs can often recover data that has been overwritten in this fashion.
- **Drive wipe:** To ensure the complete destruction of retrievable data on a storage device, it must be overwritten with a program that meets or exceeds recognized data-destruction standards, such as the U.S. Department of Defense (DoD) 5220.22-M (which requires 7 passes) or Peter Gutman's 35-pass maximum-security method. These programs, referred to as ***drive wipes***, destroy existing data and partition information in such a way as to prevent data recovery or drive forensic analysis. Use this method when maintaining the storage device as a working device is important for repurposing (such as for donation or resale). A variety of commercial and freeware programs can be used for this task, which is also known as disk scrubbing or disk wiping.

Configuring Security on SOHO Networks

220-1002 Exam

220-1002: Objective 2.10: Given a scenario, configure security on SOHO wireless and wired networks.

Both wireless and wired small office/home office (SOHO) networks are important to businesses of all sizes as well as individual users. However, they also represent significant vulnerabilities if they are not properly secured. The following sections explain how the different encryption methods work and the additional steps that must be taken to completely secure a wireless network.

NOTE For the 220-1002 exam, be familiar with the following tasks:

- Wireless-specific security settings
- Changing default usernames and passwords
- Enabling MAC filtering
- Assigning static IP addresses
- Firewall settings
- Port forwarding/mapping
- Disabling ports
- Content filtering/parental controls
- Updating firmware
- Physical security

Wireless-Specific Security

The default settings for a wireless network should be changed to provide security. The following sections discuss these issues.

Key Topic

Changing Default SSID

The ***service set identifier (SSID)*** can provide a great deal of useful information to a potential hacker of a wireless network. Every wireless network must have an SSID, and by default, WAPs and wireless routers typically use the manufacturer's name or the device's model number as the default SSID. If a ***default SSID*** is broadcast by a wireless network, a hacker can look up the documentation for a specific router or the most common models of a particular brand and determine the default IP address range, the default administrator username and password, and other information that would make it easy to attack the network.

To help "hide" the details of your network and location, a replacement SSID for a secure wireless network should not include any of the following:

- Your name
- Your company name
- Your location
- Any other easily identifiable information

An SSID that includes obscure information (such as the name of your first pet) would be a suitable replacement.

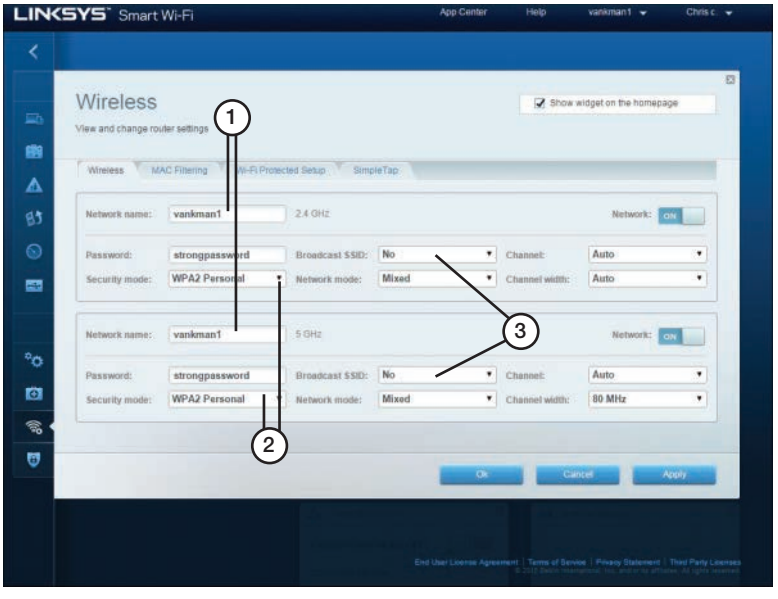
Setting Encryption

The importance of setting encryption to the latest possible standards is covered earlier in this chapter, in the section "Wireless Security Protocols and Authentication." The information there applies to SOHO networks as well, as a SOHO may be set up as an extension of a business. In such a case, all security policies from the business should apply at the SOHO extension as well.

Disabling SSID Broadcast

Disabling SSID broadcast is widely believed to be an effective way to prevent a wireless network from being detected and is so regarded by the A+ certification exams. But that is not always enough. Even though disabling SSID broadcast prevents casual bandwidth snoopers from finding your wireless network, Microsoft does not recommend disabling SSID broadcasting as a security measure because there are methods serious hackers can use to discover networks.

Figure 7-22 illustrates a Linksys router configuration dialog in which several of these security recommendations have been implemented.



1. User-assigned SSID in place of factory default
2. WPA2 Personal security mode selected
3. SSID broadcast disabled

FIGURE 7-22 Configuring a Router with Alternative SSIDs, WPA2 Encryption Enabled, and SSID Broadcast Disabled

Antenna and Access Point Placement

When configuring and/or troubleshooting wireless connections, think about the wireless access point's (WAP's) location. The placement of the access point plays a big part in a strong signal. Generally, it should be placed in the middle of an office to offer the greatest coverage while reducing the chance of outsiders being able to connect to the device. The antennas on the access point should be set at a 90-degree angle to each other. Keep the device away from any forms of electrical interference, such as other wireless devices, speakers, and any devices that use a lot of electricity.

Radio Power Levels

Some wireless routers and access points have adjustable radio power levels. When they are set too low, clients at the perimeter of the building will not be able to gain access. When they are set too high, computers located in neighboring businesses will be able to attempt access. If a wireless signal is too weak, regardless of the router location and radio power levels, and the router is older, consider replacing it with a new wireless router.

WiFi Protected Setup (WPS)

Using WiFi Protected Setup (WPS) is an easy way to configure a secure wireless network with a SOHO router, provided that all devices on the network support WPS. There are several ways that WPS can be configured. The most common ways include:

- **PIN:** A personal identification number (PIN) marked on the router may be entered into each new device added to the network. This is the default method.
- **Push button:** The router or WAP may have a push button, and each new device may also have a physical push button or (more often) a software push button in the setup program. Both the button on the WAP or router and the button on the other device must be pushed within a short period of time to make the connection.

A security flaw with the PIN method was discovered, and many professionals recommend against WPS on this basis. But it really depends on the features available on the router. Some routers let you disable the PIN and allow the push-button method, but many do not. Some routers allow you to disable WPS altogether. These settings are worth investigating when looking to install or replace a WAP. Figure 7-23 depicts WiFi Protected Setup options.

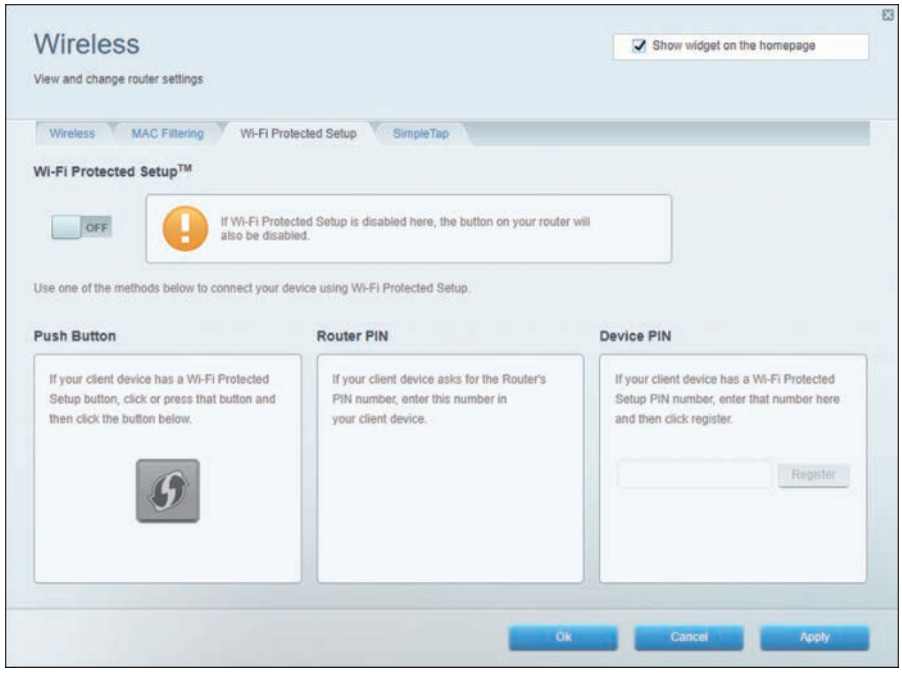


FIGURE 7-23 WiFi Protected Setup Options

Change Default Usernames and Passwords

As mentioned previously, the documentation for almost all WAPs and wireless routers lists the default administrator password, and the documentation can be readily downloaded in PDF or HTML form from vendor websites. Because an attacker could use this information to "take over" the device, it is essential to change the default to a private password. Most routers use the Administration or Management dialog for the password and other security settings.

TIP To further secure a router or WAP, configure the device so it can be managed only with a wired Ethernet connection.

Enable MAC Filtering

As mentioned earlier in this chapter, every device on a network has a MAC address. All devices on a SOHO network, including phones and tablets, have MAC addresses as well, and they need to be managed with filtering. Refer to the section "Physical Security Measures," earlier in this chapter, for details about software used to hack networks. MAC filtering is described in more detail in Chapter 2.

Assign Static IP Addresses

The DHCP server built into a router hands out IP addresses to all computers connected to it. This is convenient, but if you want to limit access to the Internet for certain computers or log activity for computers by IP address, the DHCP setting should be disabled, and a static IP address should be assigned to each computer. This way, outside devices will not be assigned IP addresses and be able to access the network.

Firewall Settings

By default, most WAPs and wireless routers use a feature called ***Network Address Translation (NAT)*** to act as simple firewalls. NAT prevents traffic from the Internet from determining the private IP addresses used by computers on the network. However, many WAPs and wireless routers offer additional firewall features that can be enabled, including:

- Access logs
- Filtering of specific types of traffic
- Enhanced support for VPNs

See the router manufacturer's documentation for more information about advanced security features. Figure 7-24 shows an example of firewall settings.

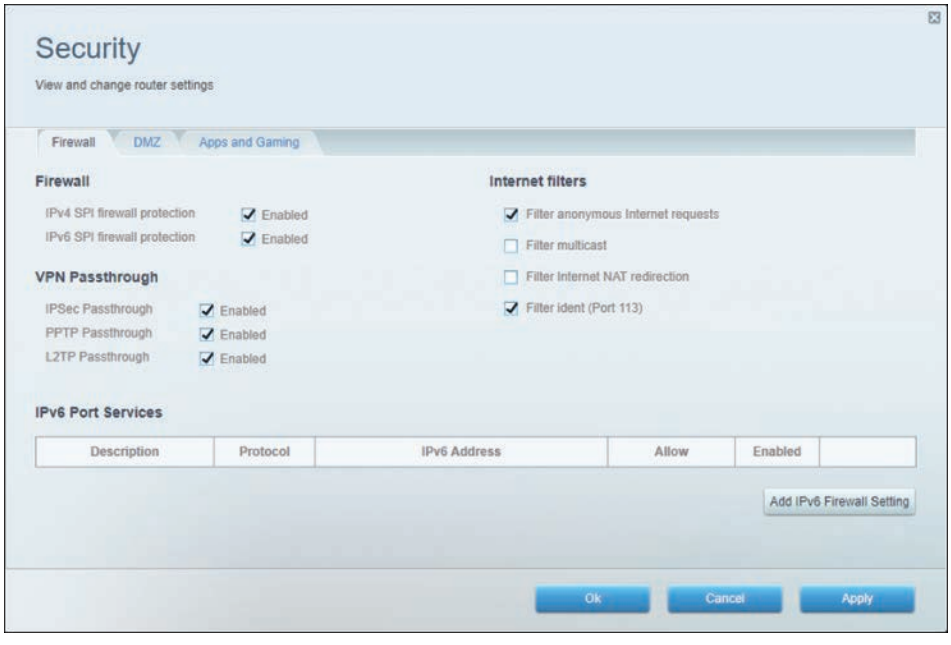


FIGURE 7-24 Firewall Settings

Port Forwarding/Mapping

Use ***port forwarding*** (also known as ***port mapping***) to allow inbound traffic on a particular TCP or UDP port or range to go to a particular IP address rather than to all devices on a network. A basic example would be an FTP server internal to a LAN. The FTP server might have the IP address 192.168.0.250 and have port 21 open and ready to accept file transactions (or a different inbound port could be used). Clients on the Internet that want to connect to the FTP server would have to know the IP address of the router, so the clients might connect with an FTP client using the IP address 68.54.127.95 and port 21. If there is an appropriate port-forwarding rule, the router sees these packets and forwards them to 192.168.0.250:21, or whatever port is chosen. Many ISPs block this type of activity, but port forwarding is a common and important method in larger networks.

Disabling Ports

Blocking TCP and UDP ports, also known as disabling ports, is performed with a firewall app such as Windows Defender Firewall with Advanced Security. Hackers take advantage of unused ports sitting idle on a network, and disabling unnecessary ports makes it harder to access your domain.

Content Filtering/Parental Controls

Windows Defender is Microsoft's anti-spyware tool that has evolved over the Windows releases. Windows 8 combined Windows Defender with other tools so that Windows was equipped to fight off virus attacks without any additional software. In Windows 10, the same Windows Defender protection is in place, and it has been combined with other tools and put into the Settings menu as an app. Figure 7-25 depicts the Windows Defender Security Center options. Windows Defender includes the following sections:

- **Virus & Threat Protection:** Allows tracking of Windows Defender and third-party antivirus software
- **Account Protection:** Includes Windows Hello and Dynamic Lock features
- **Firewall & Network Protection:** Contains access control rules and other network and domain security settings
- **App & Browser Control:** Contains filter controls for browsers and apps
- **Device Security:** Tests device security and sets core security
- **Device Performance & Health:** Scans devices and apps to report on status

- **Family Options:** Provides parental controls and family device management options

Spending time getting to know the settings in the Windows Defender Security Center is a must for any technical support professional.

Apple has parental controls in macOS versions. They can be found by selecting the **Apple menu > System Preferences > Parental Controls**.

Linux distros do not include parental controls, but many third-party apps are available.

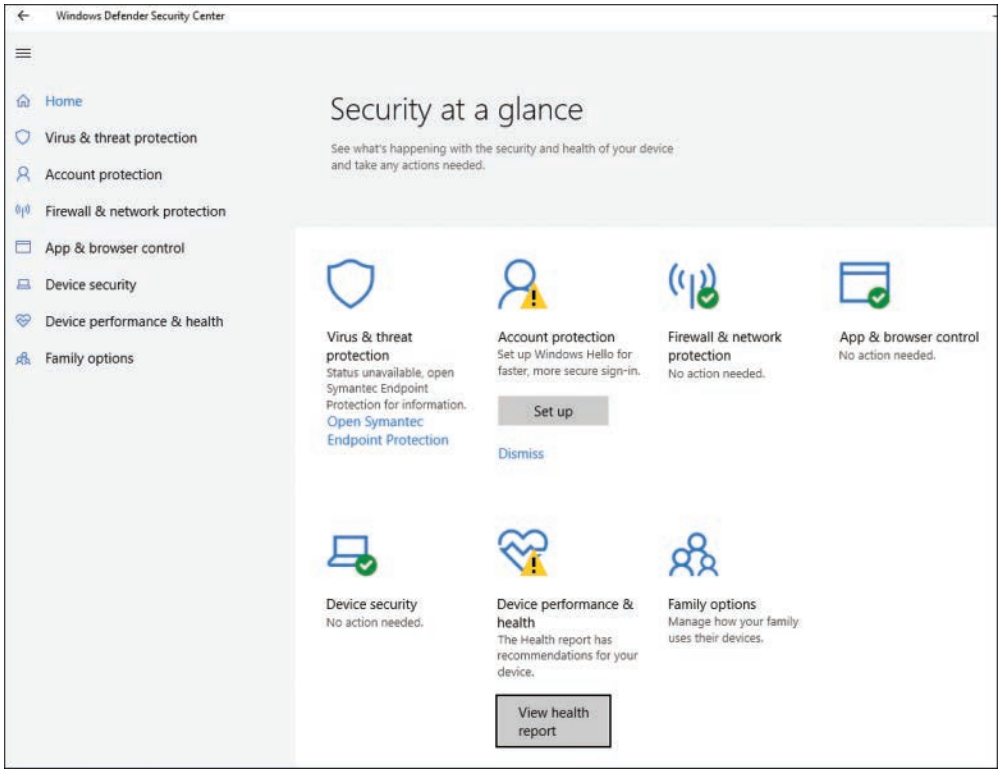


FIGURE 7-25 Windows Defender Settings in Windows 10

Update Firmware

Most SOHO router vendors issue at least one firmware update during the life span of each model of WAP and wireless router. Updates can solve operational problems and might add features that enhance WiFi interoperability, security, and ease of use. To determine whether a WAP or wireless router has a firmware update available, follow these steps:

Key Topic

Step 1. View the device's configuration dialogs to record the current firmware version. Also note the router's model number and revision from the back or bottom of the device.

Step 2. Visit the device vendor's website to see whether a newer version of the firmware is available.

Step 3. Download the firmware update to a PC that can be connected to the device with an Ethernet cable.

Step 4. Connect the PC to the device with an Ethernet cable.

Step 5. Navigate to the device's firmware update dialog.

Step 6. Follow the instructions to update firmware.

Physical Security

In a SOHO network environment, physical security refers to preventing unauthorized use of the network. The same basics of physical security apply in a SOHO network in a large office environment:

Key Topic

- Secure the network equipment in a locked wiring closet or room.
- Disable any unused wall Ethernet jacks by either disabling their switch ports or unplugging the patch panels in the wiring closet.
- Route network cables out of sight, in the walls and above the ceiling. Having them out of sight cuts down on the chances of someone tapping into the network.
- Lock doors when leaving.
- If possible, dedicate a lockable room as a workspace in a home office to protect company devices and other resources from the hazards of daily family life, such as children and pets.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple choices for exam preparation: the exercises here, Chapter 10, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All the Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. Table 7-2 lists these key topics and the page numbers on which each is found.

Table 7-2 Key Topics for Chapter 7

Key Topic

Key Topic Element	Description	Page Number
List	Active Directory Service basics	694
List	Built-in OS firewalls	698
List	Strong password characteristics	699
Section	Directory Permissions	699
Section	Wireless protocols and encryption types	702
Section	Malware Types	704
List	Antivirus/anti-malware protection techniques	707
Section	Backup/Restore	708
Steps	Enabling/configuring Time Machine	709
List	Characteristics of an acceptable use policy (AUP)	711
Paragraphs	Firewalls/DNS	712
Section	Social Engineering/Attack Types	714
Section	Windows OS Security Settings	719
Section	Shared Files and Folders	721
Paragraph	Single Sign-on (SSO)	723
List	Drive encryption requirements	723
Steps	Encrypting files	724
Section	Password Best Practice	725
Section	Account Management	728

Key Topic Element	Description	Page Number
List	Securing mobile devices	735
List	Physical destruction methods	741
List	Recycling/repurposing best practices	742
Section	Wireless-Specific Security	743
Steps	Updating SOHO router firmware	750
List	Physical security best practices in a SOHO network environment	750

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

mantrap, RFID technology, smart card, biometric security, token, cable lock, USB lock, privacy screen, key fob, entry control roster, Active Directory Service, login script, domain, Group Policy, Organizational Unit (OU), home folder, folder redirection, software token, mobile device management (MDM), MAC address, whitelisting, MAC address filtering, MAC address cloning, certificate, antivirus/anti-malware software, firewall, two-way firewall, authentication, multifactor authentication, directory permissions, file and folder permissions, virtual private network (VPN), data loss/leakage prevention (DLP), access control list, email filtering, principle of least privilege, Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA), Temporal Key Integrity Protocol (TKIP), Advanced Encryption Standard (AES), single-factor authentication, multifactor authentication, Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access Control System (TACACS), ransomware, Trojan, keylogger, rootkit, virus, botnet, worm, spyware, Recovery Console, acceptable use policy (AUP), Domain Name Service (DNS), social engineering, phishing, spear phishing, impersonation, shoulder surfing, tailgating, piggybacking, dumpster diving, distributed denial of service (DDoS), denial of service (DoS), zero day, man-in-the-middle (MiTM), brute force attack, dictionary attack, rainbow table, spoofing, non-compliant systems, zombie, access control, NT File System (NTFS), file attributes, local shares, administrative shares, system files and folders, SSO, Single Sign-on, BitLocker, Trusted Platform Module (TPM), BitLocker To Go, Encrypting File System (EFS), autorun, screen lock, fingerprint lock, face lock, swipe lock, passcode locking, remote wipe, locator application, remote backup application, patching/OS updates, biometric authentication, full device encryption, authenticator application, bring your own device (BYOD), overwrite, drive wipe, service set identifier (SSID), default SSID, Network Address Translation (NAT), port forwarding, port mapping

Answer Review Questions

1. Andre was running late for work and left his security badge in his car. Rather than take the time to return to his car and be late, he waited by the outer door and walked in behind another employee. The other employee was unsure of who Andre was and was irritated with him for following so closely, so she didn't allow Andre to follow her through the inner door to work. He had to return to his car for the badge. What two security concepts were involved in this scenario? (Choose two.)
   a. Security guard
   b. Tailgating
   c. Mantrap
   d. Shoulder surfing

2. Alexa was working her shift in the server room when an alarm went off on a server belonging to a vendor from another company. She was unable to get to the reset button on the server. What likely prevented her from accessing the server whose alarm was going off?
   a. Lack of a key fob
   b. Rack-level security
   c. Lack of authentication
   d. Privacy screen

3. Match the type of malware to its description.

Description	Type of Malware
1. Infects and rewrites files. Replicates automatically with no user intervention.	
2. A method of hiding malware from detection programs.	
3. Tracks web browsing; uses pop-ups to attract a user's attention.	
4. Encrypts target files and then demands payment to unencrypt files.	
5. Infects and rewrites files. Replicates itself if a user executes the file.	

Answer options:

a. Spyware

b. Virus

c. Worm

d. Rootkit

e. Ransomware

4. As an IT professional, you should be sure to employ security best practices. Which of the following is not a best practice?

   a. Strong passwords for user accounts

   b. Antivirus/malware protection

   c. Changing the default password on a WAP

   d. WEP encryption

5. Which of the following is generally the most difficult form of security for a malicious hacker to overcome?

   a. Firewall

   b. Encryption

   c. Biometrics

   d. Physical lock and key

6. Biometrics includes the use of which of the following? (Choose all that apply.)

   a. Fingerprint scan

   b. RFID

   c. Retinal scan

   d. Token

7. Which of the following is not a type of token?

   a. Key fob

   b. Cable lock

   c. RFID card

   d. Smart card

8. Which of the following is a program that either blocks or allows data packets to be delivered to network addresses?
   a. DHCP server
   b. Key fob
   c. Firewall
   d. Network server

9. Which of the following is a characteristic of a strong password? (Choose all that apply.)
   a. No more than six characters
   b. Lowercase only
   c. Use of symbols
   d. Use of numbers

10. Mike was called to a workstation that was running slowly. After interviewing the user and asking about recent activity, Mike determined that the user had opened a fake email and reset his password. Which of the following was the user most likely involved in?
    a. Tailgating
    b. Dumpster diving
    c. Phishing
    d. Shoulder surfing

11. Fred determined that encryption was the best solution for keeping his USB flash drive safe while on the road. Which security product would satisfy this need?
    a. Recovery Console
    b. Single Sign-on (SSO)
    c. BitLocker To Go
    d. USB 3 Lockup

12. Ellen, who works at home as an accountant, noticed her wireless network slowing and wondered if neighbors had started using her network for streaming. Which security practices can she employ to ensure that neighbors don't gain access to her network and that her clients' files are protected? (Choose two.)
    a. Change the default IP address on the default gateway.
    b. Change the network name and disable the SSID broadcast.
    c. Use MAC address filtering.
    d. Change the Netflix password.

13. Jen has been tasked with repurposing laptops used by the human resources department. What can she do to make sure important personnel information cannot be compromised?
    a. Overwrite
    b. Low-level format
    c. Standard format
    d. Drive wipe

14. Hiro is able to log into his account at work but can't see the work his team is doing for an advertising client. He didn't have any trouble before he went on vacation. What is a reasonable explanation for this problem?
    a. Share permissions were updated while he was gone.
    b. Hiro was locked out due to inactivity
    c. It took Hiro three tries to log into his computer, and his permissions were suspended after the second attempt.
    d. The boss thought Hiro was leaving the company, so his account was disabled.

15. Victoria was updating a computer from another office and realized she needed to change the UEFI settings. Unfortunately, the UEFI BIOS was password protected, and the motherboard had no reset buttons or jumpers, as she was used to seeing. What should she do?
    a. Scrap the motherboard because control of the BIOS/UEFI is essential.
    b. Unplug the computer overnight.
    c. Remove the CMOS battery, go to lunch, and replace the batter after eating.
    d. Change the CPU jumpers.

This page intentionally left blank

This chapter covers the five A+ 220-1002 exam objectives related to troubleshooting Microsoft Windows OS, PC security, malware removal, mobile OS and application operational and security issues, and related topics. These objectives may comprise 26% of the exam questions:

- **Core 2 (220-1002): Objective 3.1:** Given a scenario, troubleshoot Microsoft Windows OS problems.
- **Core 2 (220-1002): Objective 3.2:** Given a scenario, troubleshoot and resolve PC security issues.
- **Core 2 (220-1002): Objective 3.3:** Given a scenario, use best practice procedures for malware removal.
- **Core 2 (220-1002): Objective 3.4:** Given a scenario, troubleshoot mobile OS and application issues.
- **Core 2 (220-1002): Objective 3.5:** Given a scenario, troubleshoot mobile OS and application security issues.

Index

Numbers

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X - Y

Z