



# Configuring Windows Devices



SECOND EDITION

Exam Ref 70-697

Andrew Bettany  
Andrew Warren

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



# **Exam Ref 70-697**

# **Configuring Windows**

# **Devices**

## **Second Edition**

**Andrew Bettany**  
**Andrew Warren**

## **Exam Ref 70-697 Configuring Windows Devices, Second Edition**

**Published with the authorization of Microsoft Corporation by:  
Pearson Education, Inc.**

**Copyright © 2018 by Pearson Education**

All rights reserved. Printed in the United States of America. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit [www.pearsoned.com/permissions/](http://www.pearsoned.com/permissions/). No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-1-5093-0785-2

ISBN-10: 1-5093-0785-0

Library of Congress Control Number: 2018938485

1 18

### **Trademarks**

Microsoft and the trademarks listed at <https://www.microsoft.com> on the “Trademarks” webpage are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

### **Warning and Disclaimer**

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The authors, the publisher, and Microsoft Corporation 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 programs accompanying it.

### **Special Sales**

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at [corpsales@pearsoned.com](mailto:corpsales@pearsoned.com) or (800) 382-3419.

For government sales inquiries, please contact [governmentsales@pearsoned.com](mailto:governmentsales@pearsoned.com).

For questions about sales outside the U.S., please contact [intlcs@pearson.com](mailto:intlcs@pearson.com).

<b>Editor-in-Chief</b>	Greg Wiegand
<b>Senior Editor</b>	Trina MacDonald
<b>Development Editor</b>	Mark Renfrow
<b>Managing Editor</b>	Sandra Schroeder
<b>Senior Project Editor</b>	Tracey Croom
<b>Editorial Production</b>	Backstop Media
<b>Copy Editor</b>	Christina Rudloff
<b>Indexer</b>	Julie Grady
<b>Proofreader</b>	Troy Mott
<b>Technical Editor</b>	Byron Wright
<b>Cover Designer</b>	Twist Creative, Seattle

*I would like to dedicate this book to Annette and Tommy, for being so supportive and encouraging whenever I work on projects that sometimes eat into our quality time together. This book is also for the reader—having taught thousands of IT Professionals over my career, I hope this book reaches a greater audience and helps you achieve your career aspirations. Work hard and aim for the stars!.*

—ANDREW BETTANY

*Writing this book has been a team effort, and I am delighted to have been a part of that team. Aside from the folks at Pearson and my co-author, Andrew, I'd like to mention my dog, Lucy. Her enthusiasm for long walks undoubtedly helped me clear my head, and thus to deliver chapters on time to our editor, Trina Macdonald.*

—ANDREW WARREN



# Contents at a glance

	<i>Introduction</i>	<i>xvii</i>
	<i>Important: How to use this book to study for the exam</i>	<i>xxi</i>
<b>CHAPTER 1</b>	<b>Manage Identity</b>	<b>1</b>
<b>CHAPTER 2</b>	<b>Plan desktop and device deployment</b>	<b>37</b>
<b>CHAPTER 3</b>	<b>Plan and implement a Microsoft 365 solution</b>	<b>73</b>
<b>CHAPTER 4</b>	<b>Configure networking</b>	<b>133</b>
<b>CHAPTER 5</b>	<b>Configure storage</b>	<b>163</b>
<b>CHAPTER 6</b>	<b>Manage data access and protection</b>	<b>207</b>
<b>CHAPTER 7</b>	<b>Manage remote access</b>	<b>261</b>
<b>CHAPTER 8</b>	<b>Manage apps</b>	<b>307</b>
<b>CHAPTER 9</b>	<b>Manage updates and recovery</b>	<b>337</b>
	<i>Index</i>	<i>389</i>



# Contents

<b>Introduction</b>	<b>xvii</b>
Organization of this book . . . . .	xviii
Microsoft certifications . . . . .	xviii
Microsoft Virtual Academy . . . . .	xviii
Quick access to online references . . . . .	xviii
Errata, updates, & book support . . . . .	xix
Stay in touch . . . . .	xix
<i>Important: How to use this book to study for the exam</i>	<i>xxi</i>
<b>Chapter 1 Manage Identity</b>	<b>1</b>
Skill 1.1: Support Microsoft Store, Microsoft Store for Education, Microsoft Store for Business, and cloud apps . . . . .	1
Integrate Microsoft account and personalization settings	2
Install and manage software	5
Sideload apps into offline and online images	11
Sideload apps by using Microsoft Intune	14
Deep link apps using Microsoft Intune	17
Skill 1.2: Support authentication and authorization . . . . .	18
Support user authentication	19
Support workgroup, homegroup, and domain membership	23
Configure local accounts and Microsoft accounts	29
Configure Workplace Join	30
Configure Azure AD Join	30
Configure Windows Hello	33
Thought experiments . . . . .	34
Scenario 1	34
Scenario 2	34



Thought experiment answers .....	35
Scenario 1 .....	35
Scenario 2 .....	35
Chapter summary .....	35

## **Chapter 2 Plan desktop and device deployment 37**

Skill 2.1: Migrate and configure user data. ....	37
Configure user profiles .....	38
Configure folder location .....	40
Migrate user profiles .....	41
Skill 2.2: Configure Hyper-V .....	43
Create and configure virtual machines .....	44
Create and manage checkpoints .....	48
Create and configure virtual switches .....	49
Create and configure virtual disks .....	50
Move virtual machine storage .....	51
Skill 2.3: Configure mobility options .....	52
Configure offline file policies .....	53
Configure sync options .....	55
Managing Power Settings .....	56
Configure Windows To Go .....	60
Configure Wi-Fi Direct .....	63
Skill 2.4: Configure security for mobile devices .....	63
Configure BitLocker .....	64
Configure startup key storage .....	67
Thought experiments .....	68
Scenario 1 .....	68
Scenario 2 .....	68
Scenario 3 .....	69
Scenario 4 .....	69
Thought experiment answers .....	70
Scenario 1 .....	70
Scenario 2 .....	70

Scenario 3	70
Scenario 4	70
Chapter summary .....	71
<b>Chapter 3 Plan and implement a Microsoft 365 solution</b>	<b>73</b>
Skill 3.1: Support mobile devices .....	73
Support mobile device policies	74
Support mobile access and data synchronization	79
Support broadband connectivity	82
Support Mobile Device Management by using Microsoft Intune	84
Skill 3.2: Deploy software by using Microsoft Intune .....	88
Use reports and In-Console Monitoring to identify required updates	89
Approve or decline updates	91
Configure automatic approval settings	92
Configure deadlines for update installations	93
Deploy third-party updates	93
Skill 3.3: Manage devices with Microsoft 365 Solution .....	94
Provision user accounts	95
Enroll devices into Microsoft 365 Business	97
Enroll devices into Microsoft 365 Enterprise	99
View and manage all managed devices	100
Configure Microsoft Intune subscriptions	102
Configure the Microsoft Service Connection Point role	103
Manage user and computer groups	104
Configure monitoring and alerts	106
Troubleshoot Microsoft Intune	109
Manage policies	110
Manage remote computers	112
Skill 3.4: Configure information protection .....	113
Manage and configure Office 365 Data Loss Prevention	114
Windows Information Protection and BitLocker	117
Azure Information Protection	120
Microsoft Cloud App Security	123

Explore Microsoft Cloud App Security	124
Office 365 Cloud App Security	126
Thought experiments .....	128
Scenario 1	128
Scenario 2	128
Scenario 3	128
Scenario 4	129
Thought experiment answer .....	129
Scenario 1	129
Scenario 2	129
Scenario 3	129
Scenario 4	130
Chapter summary .....	130

## **Chapter 4 Configure networking 133**

Skill 4.1: Configure IP settings .....	133
Connect to a network	133
Configure name resolution	139
Configure network locations	141
Skill 4.2: Configure network settings .....	143
Connect to a wireless network	143
Manage preferred wireless networks	144
Configure network adapters	145
Configure location-aware printing	146
Skill 4.3: Configure and maintain network security .....	147
Windows Defender Security Center	148
Configure Windows Firewall	149
Configure Windows Firewall with Advanced Security	152
Configure connection security rules with IPsec	155
Configure authentication exceptions	156
Configure network discovery	157

Thought experiments.....	158
Scenario 1	158
Scenario 2	159
Scenario 3	159
Thought experiment answers .....	159
Scenario 1	159
Scenario 2	160
Scenario 3	160
Chapter summary .....	160

## **Chapter 5 Configure storage 163**

Skill 5.1: Support data storage.....	163
Distributed File System	164
Support Storage Spaces	167
Manage Storage Spaces using PowerShell	173
Support OneDrive	174
Skill 5.2: Support data security .....	179
Manage permissions including Sharing, NTFS and Dynamic Access Control	179
Support Encrypting File System	185
Troubleshoot Encrypting File System	186
Controlling access to removable media	187
Support BitLocker and BitLocker To Go	188
Configure BitLocker using command-line tools	194
Understand Microsoft BitLocker Administration and Monitoring	200
Thought experiments.....	203
Scenario 1	203
Scenario 2	203
Thought experiment answers .....	204
Scenario 1	204
Scenario 2	204
Chapter summary .....	204

<b>Chapter 6</b>	<b>Manage data access and protection</b>	<b>207</b>
	Skill 6.1: Configure shared resources .....	207
	Configure HomeGroup settings	208
	Configure libraries	210
	Configure shared folder permissions	213
	Configure shared printers	219
	Configure OneDrive	224
	Co-existence of OneDrive and OneDrive for Business	229
	Skill 6.2: Configure file and folder access .....	232
	Encrypt files and folders by using Encrypting File System	233
	Configure NTFS permissions	237
	Configure disk quotas	245
	Configure file access auditing	247
	Configure authentication and authorization	250
	Thought experiments.....	256
	Scenario 1	256
	Scenario 2	256
	Thought experiment answers .....	257
	Scenario 1	257
	Scenario 2	257
	Chapter summary .....	258
<b>Chapter 7</b>	<b>Manage remote access</b>	<b>261</b>
	Skill 7.1: Configure remote connections .....	261
	Configure remote authentication	262
	Configure VPN connections and authentication	262
	Enable VPN Reconnect	268
	Configure broadband tethering	269
	Configure Remote Desktop client for Windows 10 Mobile, iOS, and Android	272
	Configure Remote Desktop settings	275
	Enable restricted admin mode for RDP in Windows 8.1 and Windows 2012 R2	277
	Remote Desktop Connection Zoom support	280

Skill 7.2: Configure mobility options .....	281
Configure offline file policies	282
Configure power policies	285
Configure Windows To Go	290
Configure sync options	294
Configure WiFi Direct	300
Thought experiments .....	302
Scenario 1	302
Scenario 2	303
Thought experiment answers .....	303
Scenario 1	303
Scenario 2	304
Chapter summary .....	304

## **Chapter 8 Manage apps 307**

Skill 8.1: Deploy and manage RemoteApp apps .....	307
Configure RemoteApp prerequisites	308
Configure RemoteApp and Desktop Connections settings	313
Configure Group Policy Objects for signed packages	316
Subscribe to the Desktop Connections feeds	317
Support iOS and Android	317
Configure Remote Desktop Web access for distribution	318
Skill 8.2: Support desktop apps .....	319
Support desktop app compatibility by using Application Compatibility Tools	320
Support desktop application co-existence	324
Install and configure User Experience Virtualization	330
Deploy desktop apps by using Microsoft Intune	331
Thought experiments .....	333
Scenario 1	333
Scenario 2	334

Thought experiment answers .....	334
Scenario 1 .....	334
Scenario 2 .....	334
Chapter summary .....	334

## **Chapter 9 Manage updates and recovery 337**

Skill 9.1: Configure system recovery .....	337
Configure a recovery drive .....	338
Configure system restore .....	340
Perform a reset .....	347
Perform a Fresh Start .....	349
Perform a driver rollback .....	351
Configure restore points .....	353
Skill 9.2: Configure file recovery .....	357
Configure File History .....	358
Restore previous versions of files and folders .....	361
Recover files from OneDrive .....	363
Skill 9.3: Configure and manage updates .....	365
Configure update settings .....	366
Configure Windows Update policies .....	373
Manage update history .....	377
Roll back updates .....	378
Update Microsoft Store apps .....	382
Thought experiments .....	385
Scenario 1 .....	385
Scenario 2 .....	385
Scenario 3 .....	386
Thought experiment answers .....	386
Scenario 1 .....	386
Scenario 2 .....	386
Scenario 3 .....	387
Chapter summary .....	387

<i>Index</i> .....	389
--------------------	-----

# About the authors



**ANDREW BETTANY**, Microsoft Most Valuable Professional (Windows and Devices for IT), Dad, IT Geek, training mentor and consultant, entrepreneur, and author.

As a Microsoft Most Valuable Professional (MVP), Andrew is recognized for his Windows expertise, and is the author of several publications, including Windows exam certification prep, Microsoft official training materials, and an author of video training materials for LinkedIn Learning and Pluralsight.

Having managed the IT Academy at the University of York, UK for years, he now focuses his time training and writing. As a Microsoft Certified Trainer, Andrew delivers learning and consultancy to businesses on many technical areas including Microsoft 365, Azure, and Windows. He has co-founded the "IT Masterclasses" series of short intensive technical courses, [www.itmasterclasses.com](http://www.itmasterclasses.com), and is passionate about helping others learn technology. He is a frequent speaker and proctor at Microsoft Ignite conferences worldwide.

Active on social media, Andrew can be found on LinkedIn Facebook and Twitter. He lives in a village just outside of the beautiful city of York in Yorkshire (UK).



**ANDREW WARREN** has over 30 years of experience in IT and has served as subject matter expert for many Microsoft Official Curriculum courses. He is a Microsoft Certified Trainer and runs his own training consultancy in the UK.





# Introduction

---

The Configuring Windows Devices exam (70-697) is separated into nine sets of objectives.

This book contains nine chapters that clearly detail what those objectives are and the content that you can expect to see on the exam. Because each chapter covers a part of the exam, you should concentrate on one chapter at a time and complete the thought experiments and review questions. This book covers the general, high-level knowledge you need to know to answer questions regarding why and when you might perform tasks relating to the exam objectives.

Prior to taking the certification exam, you should fully prepare to the best of your ability and we assume that you have some practical experience supporting Windows devices within the workplace. You are also probably reading this book as part of your final preparations and that you feel almost ready to take the exam. In this book we have included how-to steps and walkthroughs whenever we feel that they are useful, and we hope that you will perform the tasks on your system or within a virtual machine to crystalize your knowledge. Throughout the book there are numerous notes and links to resources on the Internet, which should add even more depth to your preparation. You should expect that Windows 10 will evolve constantly, through Windows upgrades, and you should always supplement your learning with practical experience obtained by using the latest build of the operating system because there are always new things to learn and fresh challenges to master.

This book covers every major topic area found on the exam, but it does not cover every exam question. Only the Microsoft exam team has access to the exam questions, and Microsoft regularly adds new questions to the exam, making it impossible to cover specific questions. You should consider this book a supplement to your relevant real-world experience and other study materials. If you encounter a topic in this book that you do not feel completely comfortable with, use the “Need more review?” links you’ll find in the text to find more information and take the time to research and study the topic. Great information is available on <https://docs.microsoft.com> and in blogs and forums.

## Organization of this book

---

This book is organized by the “Skills measured” list published for the exam. The “Skills measured” list is available for each exam on the Microsoft Learning website: <http://aka.ms/examlist>. Each chapter in this book corresponds to a major topic area in the list, and the technical tasks in each topic area determine a chapter’s organization. If an exam covers six major topic areas, for example, the book will contain six chapters.

## Microsoft certifications

---

Microsoft certifications distinguish you by proving your command of a broad set of skills and experience with current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies both on-premises and in the cloud. Certification brings a variety of benefits to the individual and to employers and organizations.

### **MORE INFO** ALL MICROSOFT CERTIFICATIONS

For information about Microsoft certifications, including a full list of available certifications, go to <http://www.microsoft.com/learning>.

## Microsoft Virtual Academy

---

Build your knowledge of Microsoft technologies with free expert-led online training from Microsoft Virtual Academy (MVA). MVA offers a comprehensive library of videos, live events, and more to help you learn the latest technologies and prepare for certification exams. You’ll find what you need here:

<http://www.microsoftvirtualacademy.com>

## Errata, updates, & book support

---

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

*<https://aka.ms/examref697ed2/errata>*

If you discover an error that is not already listed, please submit it to us at the same page.

If you need additional support, email Microsoft Press Book Support at *[mspinput@microsoft.com](mailto:mspinput@microsoft.com)*.

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to *<http://support.microsoft.com>*.

## Stay in touch

---

Let's keep the conversation going! We're on Twitter: *<http://twitter.com/MicrosoftPress>*.



## **Important: How to use this book to study for the exam**

Certification exams validate your on-the-job experience and product knowledge. To gauge your readiness to take an exam, use this Exam Ref to help you check your understanding of the skills tested by the exam. Determine the topics you know well and the areas in which you need more experience. To help you refresh your skills in specific areas, we have also provided “Need more review?” pointers, which direct you to more in-depth information outside the book.

The Exam Ref is not a substitute for hands-on experience. This book is not designed to teach you new skills.

We recommend that you round out your exam preparation by using a combination of available study materials and courses. Learn more about available classroom training at <http://www.microsoft.com/learning>. Microsoft Official Practice Tests are available for many exams at <http://aka.ms/practicetests>. You can also find free online courses and live events from Microsoft Virtual Academy at <http://www.microsoftvirtualacademy.com>.

This book is organized by the “Skills measured” list published for the exam. The “Skills measured” list for each exam is available on the Microsoft Learning website: <http://aka.ms/examlist>.

Note that this Exam Ref is based on this publicly available information and the author’s experience. To safeguard the integrity of the exam, authors do not have access to the exam questions.



# Configure networking

It is important to understand the fundamentals of networking in Windows 10 to pass the 70-697, Configuring Windows Devices exam. Network connectivity is an almost universal assumption in typical Windows 10 operation, so understanding how Windows networking works will help you in many areas of the exam. This chapter will cover the basics of main networking components of Windows 10, along with how to configure each of them.

## Skills in this chapter:

- Skill 4.1: Configure IP settings
- Skill 4.2: Configure network settings
- Skill 4.3: Configure and maintain network security

## Skill 4.1: Configure IP settings

---

The IP address is the most widely used point of contact for a Windows 10 computer that is connected to the network. A computer's IP address uniquely identifies it on the local network segment, and it serves as the functional component for most of the ways that computers communicate on a network, including name resolution and file transfer.

### This section covers how to:

- Connect to a network
- Configure name resolution
- Configure network locations

## Connect to a network

Networks are groups of computers and other resources. When connected, each resource that is connected (computer, network printer, server, or other host) must acquire, or have previously been assigned an exclusive address that will define it on that network. These addresses are unique, and you can't have two hosts on the same network with the same address. This makes addressing a very important part of configuring and connecting to networks.



## Understanding IP address requirements

Each host on a network must have a unique Internet Protocol (IP) address. This address, when it's configured as an IPv4 address, is a 32-bit number that is styled as four sets of decimal numbers. For example: 192.168.4.20. Each host is also assigned a subnet mask, which determines which part of the IP address defines the network and which part defines the host. Together, the IP address and the subnet mask define the network within which a host can communicate. If the host requires communication outside of the local network segment, a gateway must be specified, which typically represents a network router that can provide network paths to other networks and the Internet. The IP address, subnet mask and default gateway together provide the full definition of IP connectivity for a network host. There are two ways to get an address to a resource: You can define it manually, or it can be assigned by a Dynamic Host Configuration Protocol (DHCP) server.

When an address can't be assigned this way, Windows will assign its own IP address using a technology called Automatic Private IP Addressing (APIPA). APIPA addresses fall in the 169.254.x.x address range.



---

### **EXAM TIP**

Make sure to review the IP address ranges for Class A, B, and C to have an idea of how many networks and hosts each offers. Know their default subnet masks, too. Beyond that, know the private addresses available for local networks (192.x.x.x, 172.x.x.x, and 10.x.x.x for Class C, B, and A, respectively).

---

## Understanding network terminology

Make sure that you are familiar with the following terms before continuing:

- **APIPA** This is a link-local (IP) address that is assigned by Windows when no other addressing mechanism can be found. This enables the host to function on the local network segment. Routers do not forward packets from these kinds of addresses.
- **Default gateway** This hardware or software device lets hosts connect to other networks. Often that network is the Internet, but it could also be another network segment in an enterprise domain.
- **DHCP** This is a networking protocol that dynamically configures IP addresses for hosts on a network. A DHCP server assigns these addresses. These IP addresses are generally granted for a specified interval and must be renewed when the interval is up. If specific static addresses are required for clients, DHCP can be configured to allow reservations for those clients.
- **DHCP Scope** A DHCP scope is a consecutive range of possible IP addresses that can be offered to hosts on a subnet (part of a network).

- **DNS** Domain Name Service (DNS) is a service that enables users to type the name of the host to which they want to connect to instead of its IP address. A DNS server resolves the name.
- **IPv4** This is an IP address that consists of 32 bits, notated by four 8-bit octets. It has two parts: the network ID and the host ID. The network ID describes the network, and the host ID defines the specific device on it. IPv4 addresses can be Unicast, Broadcast, or Multicast.
- **Subnet mask** This 32-bit number, notated by four 8-bit octets that consist of a set of 1s followed by a set of 0s, is used to define which part of the IPv4 address is the network ID and which part is the host ID. The 1s denote the network; the 0s denote the host. The default subnet masks are in the form 255.0.0.0 for Class A addresses, 255.255.0.0 for Class B addresses, and 255.255.255.0 for Class C addresses. Translated to binary, 255.0.0.0 looks like this: 11111111 00000000 00000000 00000000.
- **IPv6** The available IPv4 address combinations are dwindling, thus the need for a better option. IPv6 is that option. Instead of a 32-bit space, it's a 128-bit space with 16-bit boundaries. This allows for many more addresses. An IPv6 address typically looks like this: 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A.

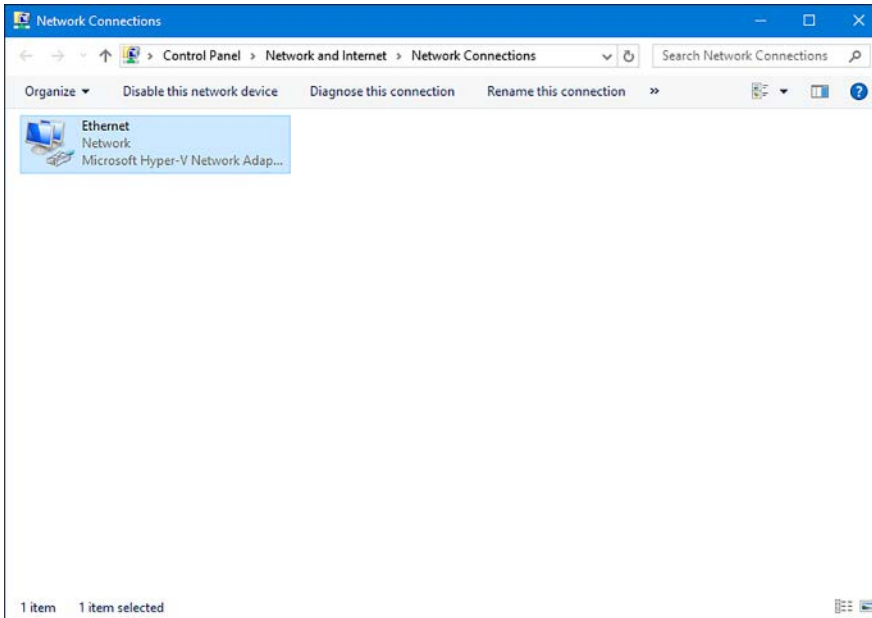
#### **MORE INFO IP ADDRESSING**

For more information on how IP addresses are defined and how they function, visit: <https://technet.microsoft.com/en-us/library/cc958829.aspx>.

## Configuring IP settings

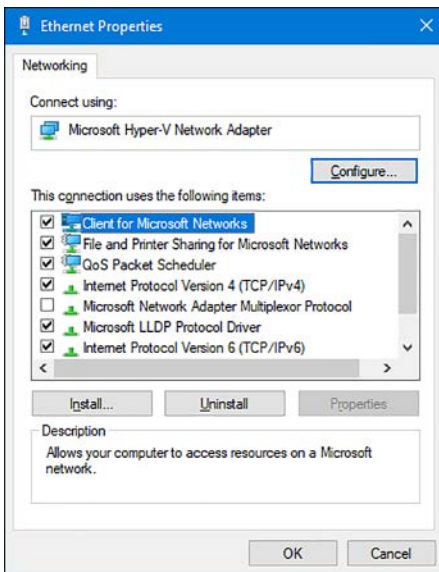
You can configure IP settings on a Windows 10 computer by accessing the Properties page for the network adapter. To open the Properties page, perform the following steps:

1. From the desktop, right-click the Start button, and then click Network Connections.
2. In Settings, click Change Adapter Options.
3. In the Network Connections window, shown in Figure 4-1, right-click the appropriate network adapter, and then click Properties.



**FIGURE 4-1** Configuring network connections

4. In the Ethernet Properties dialog box shown in Figure 4-2, select Internet Protocol Version 4 (TCP/IP4), and then click Properties.



**FIGURE 4-2** Configuring a network connection's properties

5. In the Internet Protocol Version 4 Properties dialog box shown in Figure 4-3, select the appropriate configuration options and specify addresses, if necessary. You can choose to either obtain the IP address and DNS server addresses automatically (from a DHCP server), or specify the addresses manually. You must, at a minimum, supply an IP address and a subnet mask.

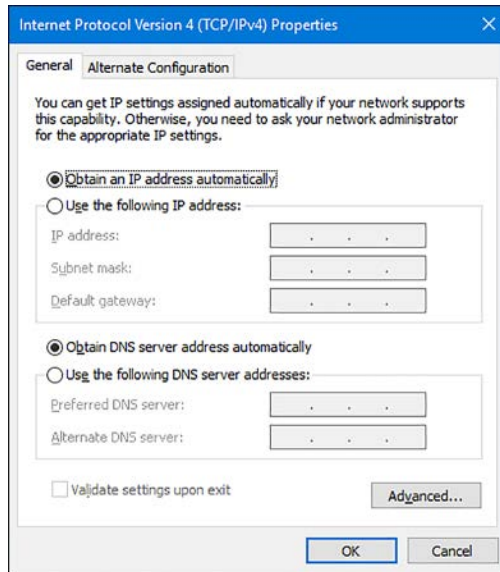


FIGURE 4-3 Configuring the TCP/IPv4 properties for a network adapter



#### EXAM TIP

You might be asked how to configure IPv4 or IPv6 addresses from the command line. The command to do this is Netsh. Make sure you understand the options associated with this command. You might be asked to select the proper command to apply a static address for a host, among other things. That command would look like this: `netsh interface ipv4 set address 'Ethernet' static 192.168.5.12 255.255.255.0 192.168.1.10`. If you want the address to come from a DHCP server, the command would look more like this: `netsh interface ipv4 set address name="Ethernet" source=dhcp`.

## Connecting to a network

The first time you connect to a local network, you are prompted to choose from one of these options:

- **No, Don't Turn On Sharing Or Connect To Devices** This option is intended for public networks and hot spots (libraries, coffee shops). The user's computer can't be seen or accessed by others, and the user can't see other computers also accessing the network.

- **Yes, Turn On Sharing And Connect To Devices** This option is intended for private, trusted networks (home, work) and homegroups. Computers sit behind a trusted router and do not connect to the Internet directly.

These two options do not appear when you connect to an Active Directory Domain Services domain. However, when they do appear and when you choose an option, settings are configured automatically for network discovery, file and printer sharing, the state of the firewall, apps that can accept incoming connections, and so on. (Computers configured as Private or Domain have network discovery enabled; Public networks do not.)

## Resolving connectivity issues

When a host can't reach a network, that host has connectivity issues. The issue might be isolated to only that device; perhaps the computer's Ethernet cable has come unplugged or the computer's wireless features have been disabled. Maybe there is an IP address conflict on the network and the user's IP address needs to be released and renewed. Often, using the troubleshooting tools in the Network And Sharing Center can expose the problem and offer a solution. If the issue isn't isolated though, you have larger problems. A network server, gateway, or other necessary resource might be down, a network segment or physical backbone might be damaged, or there could be an issue that is caused by the Internet service provider (ISP), cloud services, or other technologies that are out of your control.

### **NOTE VIEWING CONNECTION STATUS**

To view the status of any connection, open the Network And Sharing Center, then click Change Adapter Settings. Double-click the icon that represents the connected network and click Details. In the dialog box that appears, you can view the physical address, DHCP information, and IP addresses. You can even see the IP address of the DNS server, default gateway, and DHCP server, along with when the DHCP lease was obtained and when it must be renewed. You can also run the `ipconfig /all` command from the command line.

## NETWORK AND SHARING CENTER

The Network And Sharing Center enables you to view the status of your active networks. If there's a problem, you can click Troubleshoot Problems to see if the Network And Sharing Center can resolve it. It can be resolved by releasing and renewing the IP address, resetting adapter settings, or uncovering a simple problem such as a disconnected Ethernet cable (which you can then reconnect).

If a problem exists, but can't be resolved automatically, you can choose from a list of troubleshooting options that include: solving problems connecting to websites, accessing shared folders, finding computers or files in a homegroup, finding and fixing problems with wireless adapters, and troubleshooting incoming connections. When you select any option and start the troubleshooter, it generally finds the problem and performs the repair or prompts you to authorize the repair. It might also require you to do something first, like insert an ethernet cable into the ethernet port on the computer.

## COMMAND-LINE TOOLS

When the Network And Sharing Center and the Action Center can't help resolve a connectivity problem, it's likely a more complex issue. Perhaps a domain's (or network segment's) gateway is offline or a router failed. Perhaps the DNS server isn't available or has been incorrectly configured on the host, or the unique, corporate, IP address of the computer has been changed to an APIPA address because of a currently unresolved network issue.

When these kinds of problems exist, you can use command-line tools to resolve them. Here are some of the tools you can use:

- **Ping** This tool verifies IP-level connectivity to another TCP/IP computer. To do this, it sends Internet Control Message Protocol (ICMP) Echo Request messages to the recipient. The receipt of these messages is displayed, along with round-trip times, if the connection is successful. Ping is the primary command used to troubleshoot connectivity, reachability, and name resolution.
- **Ipconfig and Ipconfig /all** This displays all current TCP/IP network configuration values. It can also refresh DHCP and DNS settings. Used without the /all parameter, Ipconfig displays IPv4 and IPv6 addresses, the subnet mask, and the default gateway for all adapters installed on the host. Common parameters are /release, /renew, and /flushdns.
- **Tracert** This tool determines the path taken to a destination and shows information about each hop a packet takes to get to where it's going. A hop is a pass through a router. You can use this information to see where the transmission fails.
- **Netstat** This displays a list of active TCP connections and the ports on which the computer is listening. It also displays Ethernet statistics, the IP routing table, and IPv4 and IPv6 statistics.
- **Netsh** This enables you to make changes to the network configuration of the current computer at the command line.
- **Nslookup** This tool displays information that you can use to diagnose problems with DNS.

## Configure name resolution

Computers are represented by their unique IP address, and you can communicate with them using that address if you like. One way to communicate with an IP address is to do so at a command line. For instance, you can type something like **ping 192.168.4.5** to troubleshoot connectivity to another host on a local area network segment. Communicating this way however, is cumbersome.

DNS enables users to type names instead of numbers; this process is called *name resolution*. DNS servers store information about the names and addresses of Internet computers, and the lists they maintain are distributed among thousands of DNS servers available on the Internet, which are placed all over the world. The name resolution request is forwarded to one of these

servers. If the name can't be resolved server, it's passed to another server and another, until it is resolved.

In many cases, your DHCP server will provide DNS server addresses for your client computers to use for name resolution. This occurs if Obtain DNS Server Address Automatically is selected. You can also manually configure a host to use a specific DNS server in the connection's Properties dialog box (shown in Figure 4-3). On a domain with a unique DNS server that the host is required to use, this is necessary. It might also be necessary in a virtual private network (VPN) or in a virtual machine.

Depending on the configuration, Windows 10 resolves host names by performing the following actions:

1. Checking whether the host name is the same as the local host name.
2. Searching the DNS resolver cache, which is populated from the local Hosts file.
3. Sending a DNS request to its configured DNS servers.

## Troubleshooting name resolution

The primary tools for troubleshooting host name resolution are *IPConfig* and *NSLookup*, and their Windows PowerShell equivalents *Get-NetIPAddress*, *Get-NetIPv4Protocol*, and *Resolve-dnsname*.

If you cannot connect to a remote host, and if you suspect a name resolution problem, you can troubleshoot name resolution by using the following procedure:

1. Open an elevated command prompt, and then clear the DNS resolver cache by typing the following command:

```
IPConfig /flushdns
```

Or, you can use the Windows PowerShell cmdlet `Clear-DnsClientCache`.

2. Attempt to verify connectivity to a remote host by using its IP address. This helps you identify whether the issue is due to name resolution. You can use the `Ping` command or the `Test-Connection` Windows PowerShell cmdlet. If the `Ping` command succeeds with the IP address, but fails by the host name, the problem is with name resolution.
3. Attempt to verify connectivity to the remote host by its host name by using the fully-qualified domain name (FQDN) followed by a period. For example, type the following command at a Windows PowerShell command prompt:

```
Test-connection LON-c11.adatum.com
```

You can also use the `ping` command.

4. If the test is successful, the problem is likely unrelated to name resolution.
5. If the test is unsuccessful, edit the `C:\Windows\System32\Drivers\Etc\hosts.txt` text file, and then add the appropriate entry to the end of the file. For example, add this line and then save the file:

```
172.16.0.51          LON-c11.adatum.com
```

6. Perform the test-by-host-name procedure again. The name resolution should now be successful.
7. Examine the DNS resolver cache to verify that the name resolved correctly. To examine the DNS resolver cache, type the following command at a command prompt:

```
IPConfig /displaydns
```

You can also use the Windows PowerShell cmdlet `Get-DnsClientCache`.

8. Remove the entry that you added to the hosts file, and then clear the resolver cache once more. At the command prompt, type the following command, and then examine the contents of the filename.txt file to identify the failed stage in name resolution:

```
NSLookup.exe -d2 LON-c11.adatum.com > filename.txt
```

The Windows PowerShell equivalent command is:

```
Resolve-dnsname lon-c11.adatum.com > filename.txt
```

## Configure network locations

The first time that you connect a computer to a network, you must select whether you trust the network. This sets appropriate firewall and security settings automatically. When you connect to networks in different locations, you can ensure that your computer is set to an appropriate security level at all times by choosing a network location.

Windows 10 uses network location awareness to uniquely identify networks to which a computer is connected. Network location awareness collects information from networks, including IP address and media access control (MAC) address data from important network components, like routers and gateways, to identify a specific network.

There are three network location types:

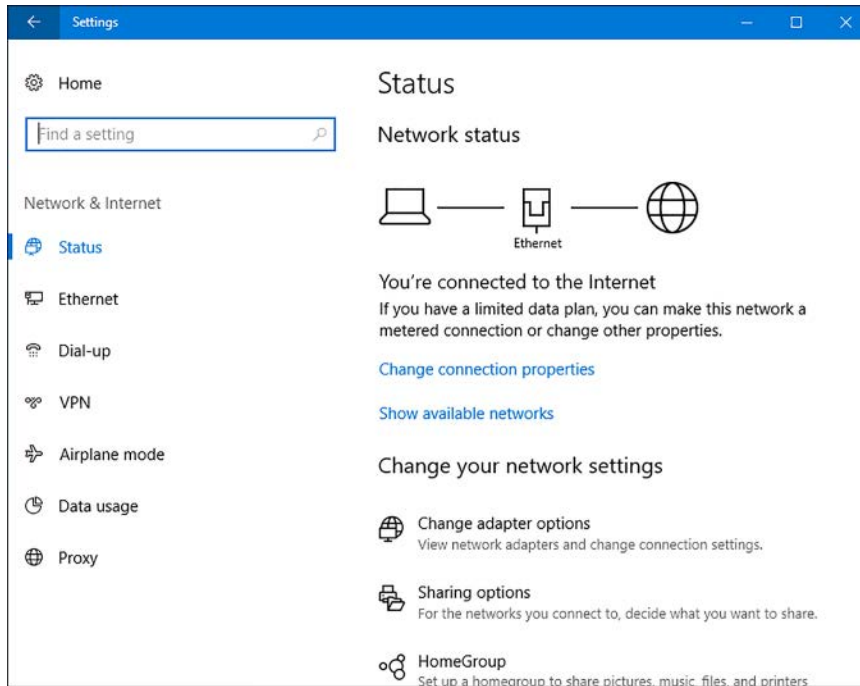
- **Domain networks** These are workplace networks that attach to a domain. Use this option for any network that allows communication with a domain controller. Network discovery is on by default, and you cannot create or join a homegroup.
- **Private networks** These are networks at home or work where you know and trust the people and devices on the network. When you select home or work (private) networks, this turns on network discovery. Computers on a home network can belong to a homegroup.
- **Guest or public networks** These are networks in public places. This location keeps the computer from being visible to other computers. When you select the Public place network location, homegroup is not available and network discovery is turned off.

The Public networks location blocks certain programs and services from running, which protects a computer from unauthorized access. If you connect to a Public network and Windows Firewall is on, some programs or services might ask you to allow them to communicate through the firewall so that they can work properly.



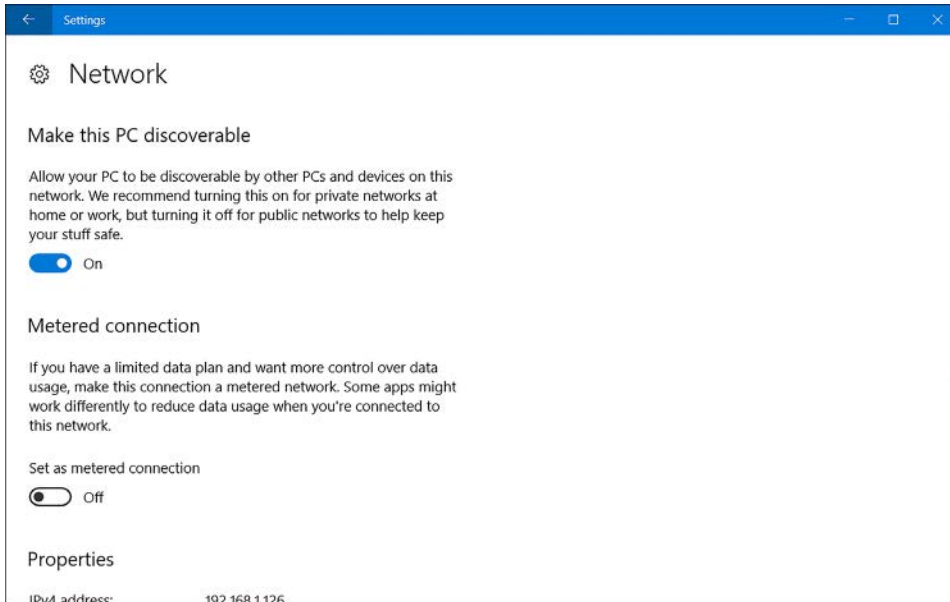
To make changes to the network location, if that location is a homegroup, you can run the Homegroup Troubleshooter. This might never happen in a homegroup, but it's worth noting that the Homegroup Troubleshooter is an option. If the location is a local network in a workgroup, you can make changes in the Settings app as follows:

1. In the Settings app, click Network & Internet.
2. On the Network & Internet page shown in Figure 4-4, click Ethernet, and then click the adapter for which you'd like to configure the network location (Ethernet, in this case).



**FIGURE 4-4** Viewing network status

3. On the Network page, under Make this PC discoverable heading, shown in Figure 4-5, change the toggle switch to Off (do not find devices, which is recommended for a public network location) or On (find devices, which is recommended for a private network location). When you choose Off, the network location profile is Public, and when you choose On, the network location profile is changed to Private. You can verify this change by clicking Sharing options on the Status tab.



**FIGURE 4-5** Changing the network location profile

## Skill 4.2: Configure network settings

There are many networking settings that you can configure. You can connect to wireless and broadband networks, and manage the list of wireless networks to which you've previously connected. You can configure location-aware printing to enable users to print to the desired local printer automatically. You can configure network adapters to reconfigure default settings and tweak performance.

### This section covers how to:

- Connect to a wireless network
- Manage preferred wireless networks
- Configure network adapters
- Configure location-aware printing

## Connect to a wireless network

An increasing number of devices use wireless connections as the primary method for accessing corporate intranets and the Internet. Additionally, many users have come to expect a wireless infrastructure in a corporate workplace. As a result, a good working knowledge of wireless

connectivity is a requirement for today's networking environment. In Windows 10, you can connect to a network from the network icon on the taskbar by following these steps:

1. From the Desktop, click the Network icon on the taskbar, as shown in Figure 4-6.



**FIGURE 4-6** Connecting to a wireless network

2. Click the appropriate wireless network name in the list.
3. Optionally, select the Connect automatically check box. This option will save the network security key so you do not have to enter it each time you connect to the network.
4. Click Connect. If the network is secure, you will be asked to enter the network security key.

## Manage preferred wireless networks

Windows 10 keeps track of all networks to which you connect and prioritizes them automatically. When you have more than one connection option, Windows 10 determines which type it will connect to in this order: Ethernet, Wi-Fi, and then mobile broadband. For example, if a Windows 10 computer has all three network types available, Ethernet will be its chosen first; otherwise, Wi-Fi is chosen. If both become unavailable, then broadband will be chosen (and will be chosen automatically if you've configured it to). When choosing from wireless networks

to which you've connected in the past, when more than one of those is available at a given time, Windows 10 connects to the last one you used.

If you're connected to a network automatically, but want to choose another, click it from the list of networks. You can access this list by clicking the Network icon in the taskbar's system tray.

In Windows 10, you can manage preferred networks in one of two ways. First, you can use the Wi-Fi page in the Network Setting section of the Settings app:

1. Open the Settings app.
2. Click Network & Internet, and then click Wi-Fi.
3. On the Wi-Fi page, click Manage Known Networks.
4. At the bottom of the page, beneath Manage Known Networks, click the network you want to manage.
5. To configure the network, click Properties. You can configure the following properties:
  - Connect automatically when in range.
  - Make this PC discoverable.
  - Set as metered connection.
6. To remove the network, click Forget.

You can also manage wireless networks by using Netsh. To use Netsh to remove networks, perform the following steps:

1. From the command prompt, type the following:

```
Netsh wlan show profiles
```
2. Locate the profile you want to remove, and use it in the following command:

```
Netsh wlan delete profile name=<profile name>
```

## Configure network adapters

When you right-click a network adapter in the Network Connections window, you can do any of the following:

- Enable or disable the adapter. (This can help you solve connection problems or keep wireless adapters from searching for networks when you don't need them to.)
- Connect to or disconnect from the associated network.
- See the status of the adapter or connection. (You can use this to view the number of bytes sent and received, to diagnose connection problems, to view signal quality and speed, and to view the service set identifier (SSID).)
- Diagnose problems with the adapter or connection. (You can use this to run an automated tool that can assist in diagnosing connection problems.)

- Bridge two or more connections. (You must select two connections that are LAN or High Speed Internet connections that are not being used by Internet Connection Sharing. A network bridge is a network device that connects to multiple network segments.)
- Create a shortcut to the adapter for easier access.
- Delete the entry, if the option is available.
- Rename the adapter.
- View the adapter's properties. (You'll see the Properties dialog box you learned about earlier in this chapter. From there, you can see the type of connection the adapter uses and install or uninstall protocols, Hyper-V Extensible Virtual Switch, Microsoft LLDP Protocol Driver, and more. When you select an option, you can view additional properties.)

Explore the options available from the adapters on a computer you have access to. Make sure to click Configure in any Wi-Fi Properties dialog box to view the advanced options. You can configure the computer to turn off that device to conserve power or to allow the device to wake up the computer (on the Power Management tab). You can also view events (Events tab), see adapter and driver details (Details, Driver, and General tabs), and view advanced configuration options (Advanced tab).

## Configure location-aware printing

Users are not always working at the same desk, day after day. Instead, many people move around and work at different desks, and often in different offices. This means that they'll almost certainly need to access printers in various locations.

Printers can be available on any kind of network, including a network at home, at the office, or even at a company kiosk. Having to choose a printer every time they connect to a new network can annoy users, thus the need for location-aware printing. With location-aware printing, a default printer can be set for each location from which the user prints. This also keeps the user from accidentally printing to the wrong printer, which poses a potential security risk if the printed data is confidential.




---

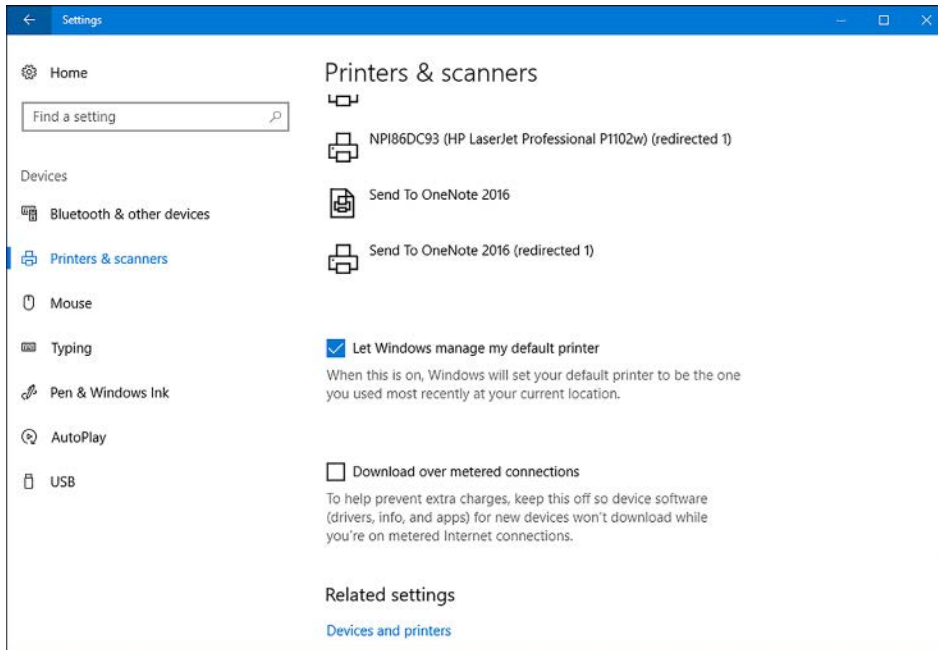
### **EXAM TIP**

**Location-aware printing uses the Network Location Awareness service and the Network List service to determine the network location. The former collects and maintains network configuration information, and the latter identifies the network to which the computer is connected. If this feature doesn't work, be aware that you need to check to make sure these services are running.**

---

To configure location-aware printing, follow these steps:

1. In Settings, click Devices and then click Printers & scanners.
2. Scroll down the list of printers, and as shown in Figure 4-7, select the Let Windows manage my default printer check box.



**FIGURE 4-7** Enabling the Let Windows manage my default printer option

## Skill 4.3: Configure and maintain network security

A computer that is running Windows 10 is more likely to face threats that originate from the network than from anywhere else. This is because attacks from the network can target a large number of computers and malicious users perform them remotely, whereas other forms of attacks require physical access to the computer. In this Skill, you will learn about common network-related security threats and the steps that you can take to mitigate them.

### This section covers how to:

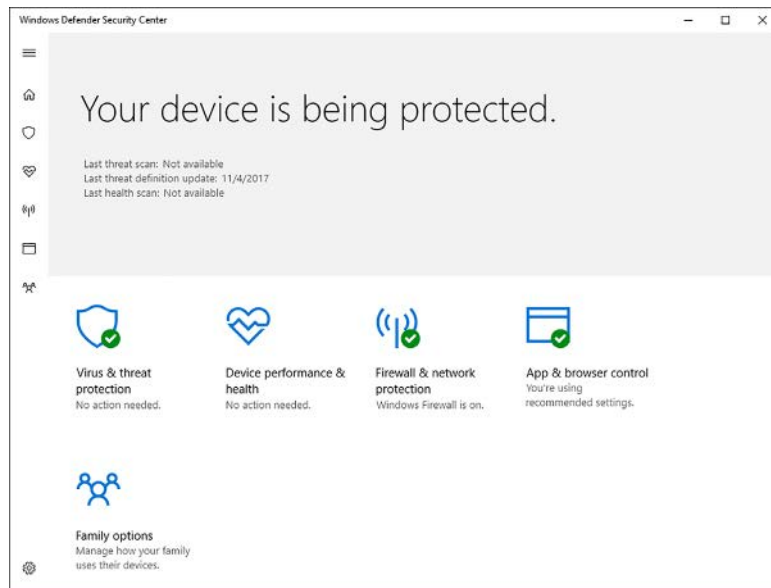
- Configure Windows Firewall
- Configure Windows Firewall with Advanced Security
- Configure connection security rules with IPsec
- Configure authentication exceptions
- Configure network discovery

# Windows Defender Security Center

Windows 10 1703 introduces the Windows Defender Security Center. This Microsoft Store app consolidates a number of network-related security components:

- Virus & threat protection
- Device performance & health
- Firewall & network protection
- App & browser control
- Family options

To access Windows Firewall settings, open Windows Defender Security Center, and on the home tab, shown in Figure 4-8, click Firewall & network protection.



**FIGURE 4-8** Windows Defender Security Center

On the Firewall & network protection page, shown in Figure 4-9, you can view the current Windows Firewall status and access links to enable you to configure firewall behavior.

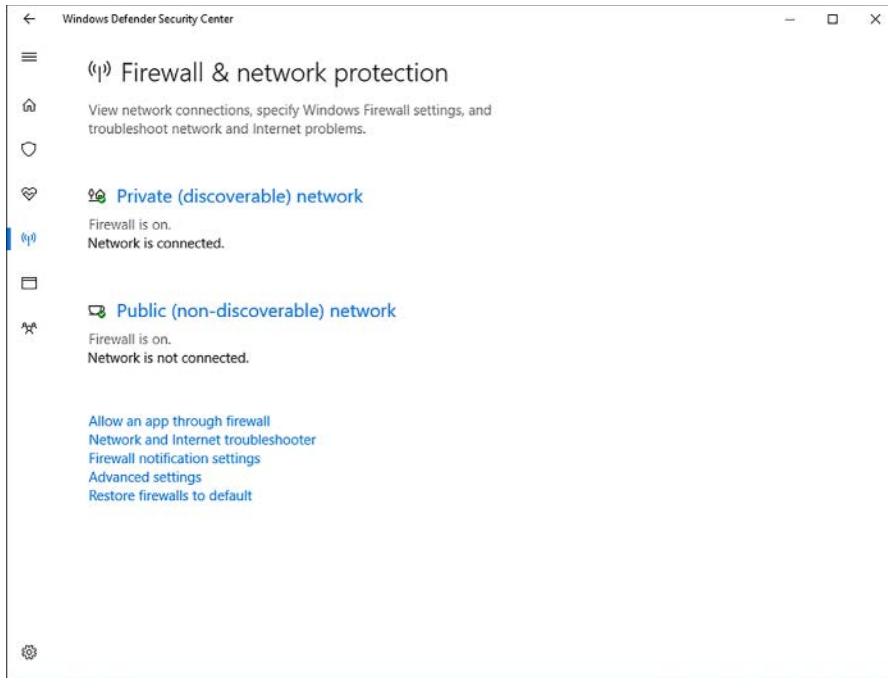


FIGURE 4-9 Firewall settings

## Configure Windows Firewall

Windows Firewall is a software solution that comes with Windows 10 that creates a virtual barrier between a computer and the network to which it is connected for the purpose of protecting the computer from unwanted incoming traffic and protecting the network from unwanted outgoing traffic. The firewall allows specific types of data to enter and exit the computer and blocks others; settings are configured by default (but they can be changed). This type of protection is called filtering. The filters are generally based on IP addresses, ports, and protocols.

- IP addresses are assigned to every computer and network resource connected directly to the network. The firewall can block or allow traffic based on an IP address of a resource (or a scope of addresses).
- Port numbers identify the application that is running on the computer. For example, port 21 is associated with the File Transfer Protocol (FTP), port 25 is associated with Simple Mail Transfer Protocol (SMTP), port 53 is associated with DNS, port 80 is associated with Hypertext Transfer Protocol (HTTP), and port 443 is associated with HTTPS (HTTP Secure).
- Protocol Protocols are used to define the type of packet being sent or received. Common protocols are TCP, Telnet, FTP, HTTP, Post Office Protocol 3 (POP3), Internet

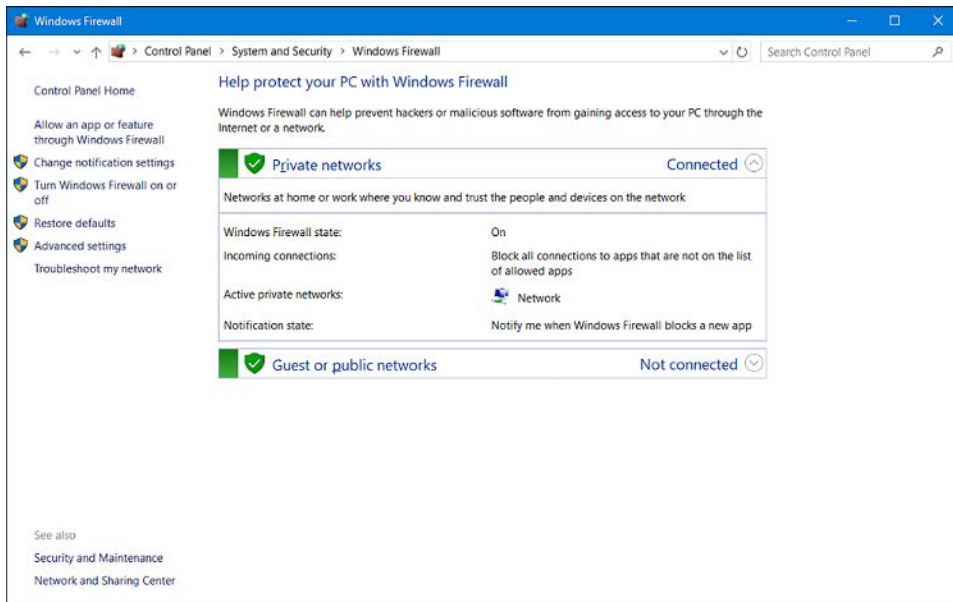


Message Access Protocol (IMAP), HTTPS, and User Datagram Protocol (UDP). (You should be familiar with the most common protocols before taking the exam.)

Although there are many rules already configured for the firewall, you can create your own inbound and outbound rules based on ports, protocols, programs, and more to configure the firewall to suit your exact needs. You'll learn how later in this chapter.

## Monitor the Windows Firewall

You can monitor the state of the Windows Firewall from Windows Defender Security Center. It's easy to tell from here if the firewall is on or off, and which is the active network. However, for more information, including how you are notified when the firewall takes action, open Control Panel, click System and Security, and then click Windows Firewall, as shown in Figure 4-10.



**FIGURE 4-10** Viewing Windows Firewall settings

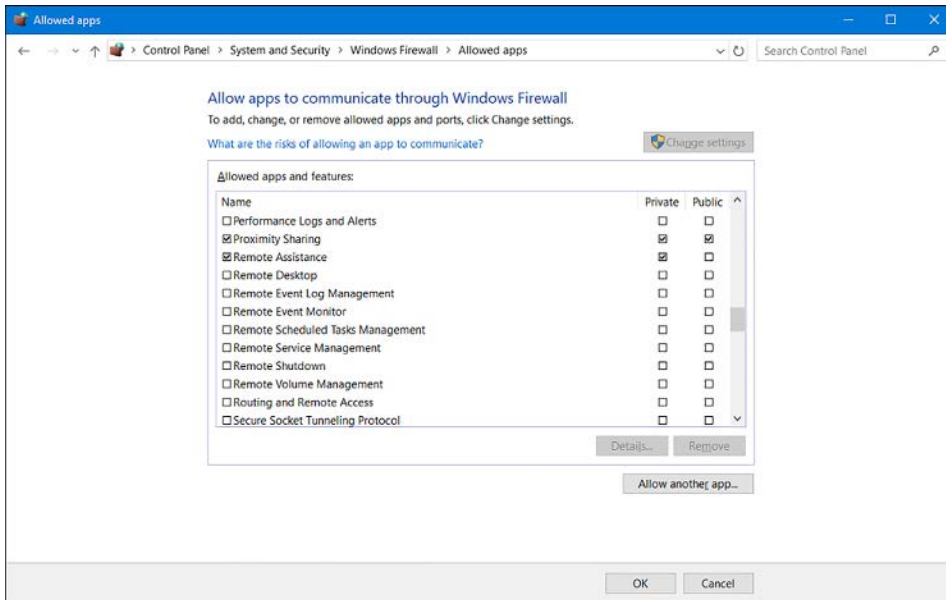
To make basic changes to the state of the firewall, in the left pane click Turn Windows Firewall On Or Off. From there you can change settings for both private and public networks. There are two options for each:

- Turn On Windows Firewall (this is selected by default).
  - Block All Incoming Connections, Including Those In The List Of Allowed Apps.
  - Notify Me When Windows Firewall Blocks A New App (This is selected by default).
- Turn Off Windows Firewall (not recommended).

What you'll be most interested in as a network administrator, are the options available in the left pane. Specifically, you'll use the Allow An App Or Feature Through Windows Firewall and Advanced Settings options. You'll learn about the Advanced Settings in the next section, but here we discuss allowing an app through the firewall that is blocked by default.

## Allow an app through the Windows Firewall

Some data generated with and by specific apps is already allowed to pass through the Windows Firewall. You can see which apps are allowed by clicking Allow An App Or Feature Through Windows Firewall in the left pane of the Windows Firewall window in Control Panel. As you scroll through the list, you'll see many apps you recognize, including Bing Food & Drink, Games, Maps, Music, and Windows Media Player. See Figure 4-11. (Once you click Change Settings and give administrator approval, the Change Settings option will appear unavailable and the options in this list will be editable, as you see here.) You will also notice that some apps are not enabled by default, including Windows Media Player Network Sharing Service (Internet), Windows Remote Management, and Remote Shutdown.

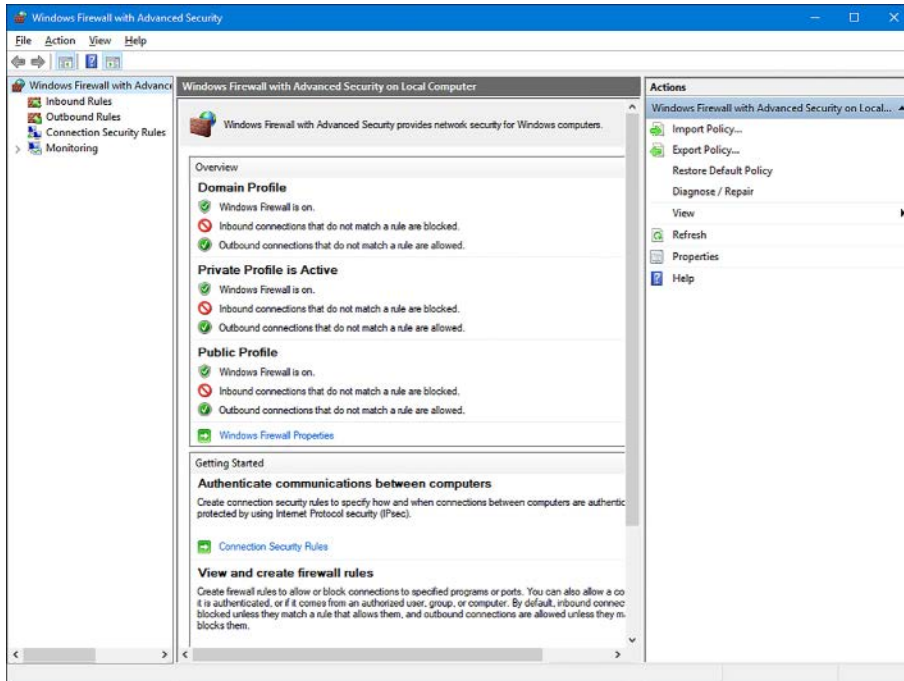


**FIGURE 4-11** Allowing an app through Windows Firewall

To allow an app through the firewall or stop one from getting through, select the check box under the appropriate network profile for which it should be configured. As shown in Figure 4-11, there are two options for each: Private and Public. If you don't see the app you want to allow or block, click Allow Another App. You can then select the desired app from the Add An App dialog box.

# Configure Windows Firewall with Advanced Security

Although you can configure a few options in the main Windows Firewall window, most configuration tasks are performed within Windows Firewall With Advanced Security. You can open this window by clicking Advanced Settings in the Windows Firewall window as shown in Figure 4-12.



**FIGURE 4-12** Windows Firewall with Advanced Security

Once opened, there are several options and terms with which you need to be familiar.

- In the left pane, your selection determines which items appear in the middle and right panes.
  - **Inbound Rules** Lists all configured inbound rules and enables you to double-click any item in the list and reconfigure it as desired. Some app rules are predefined and can't be modified, although they can be disabled. Explore the other nodes as time allows. You can also right-click Inbound Rules in the left pane and create your own custom rule. Rule types include Program, Port, Predefined, and Custom. They are detailed later in this section.
  - **Outbound Rules** Offers the same options as Inbound Rules, but these apply to outgoing data. You can also right-click Outbound Rules in the left pane and create your own custom rule.

- **Connection Security Rules** Connection security rules establish how computers must authenticate before any data can be sent. IP Security (IPsec) standards define how data is secured while it is in transit over a TCP/IP network, and you can require a connection use this type of authentication before computers can send data. You'll learn more about connection security rules in the next section.
- **Monitoring** Offers information about the active firewall status, state, and general settings for both the private and public profile types.
- In the right pane, you'll see the options that correspond to your selection in the left pane.
  - **Import/Export/Restore/Diagnose/Repair Policies** Enables you to manage the settings you've configured for your firewall. Policies use the WFW extension.
  - **New Rules** Enables you to start the applicable Rule Wizard to create a new rule. You can also do this from the Action menu.
  - **Filter By** Enables you to filter rules by Domain Profile, Private Profile, or Public Profile. You can also filter by state: Enabled or Disabled. Use this to narrow the rules listed to only those you want to view.
  - **View** Enables you to customize how and what you view in the middle pane of the Windows Firewall With Advanced Security window.

When you opt to create your own inbound or outbound rule, you can choose from four rule types. A wizard walks you through the process, and the process changes depending on the type of rule you want to create. The rules are as follows:

- **Program** A program rule sets firewall behavior for a specific program you choose or for all programs that match the rule properties you set. You can't control apps, but you can configure traditional EXE. Once you've selected the program for which to create the rule, you can allow the connection, allow only if the connection is secure and has been authenticated using IPsec, or block the connection. You can also choose the profiles to which the rule will be applied (domain, private, public) and name the rule.
- **Port** A port rule sets firewall behavior for TCP and UDP port types and specifies which ports are allowed or blocked. You can apply the rule to all ports or only ports you specify. As with other rules, you can allow the connection, allow only if the connection is secured with IPsec, or block the connection. You can also choose the profiles to which the rule will be applied (domain, private, public) and name the rule.

#### **MORE INFO CONNECTIVITY AND SECURITY**

When you create inbound and outbound rules, and when you opt to allow the connection only if the connection is secured by authenticating the connection with IPsec, the connection will be secured using the settings in the IPsec properties and applicable rules in the Connection Security Rules node. The next section covers how to create connection security rules.

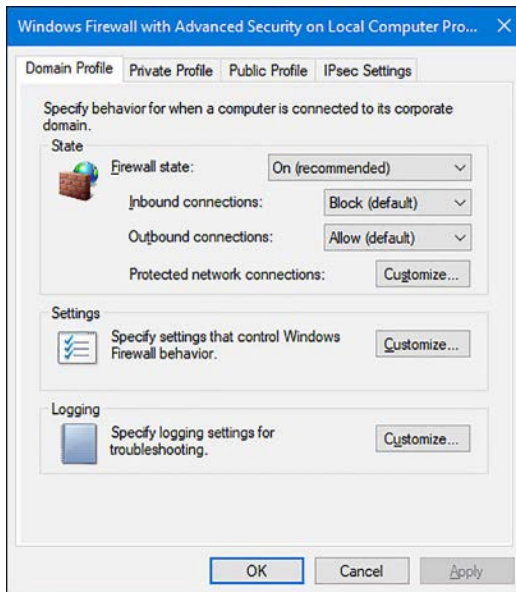
- **Predefined** Sets firewall behavior for a program or service that you select from a list of rules that are already defined by Windows.
- **Custom** A rule you create from scratch, defining every aspect of the rule. Use this if the first three rule types don't offer the kind of rule you need.



#### EXAM TIP

You might encounter questions regarding how to create a rule on the exam. Therefore, you should spend a few minutes working through the wizard a few times, selecting different rule types each time to become familiar with the process.

With Windows Firewall With Advanced Security selected in the left pane and using the Overview section of the middle pane, click Windows Firewall Properties to see the dialog box shown in Figure 4-13. From there you can make changes to the firewall and the profiles, even if you aren't connected to the type of network you want to configure.



**FIGURE 4-13** Viewing the Windows Firewall properties

In Figure 4-13, the Domain Profile tab is selected. If you want to, you can configure the firewall to be turned off when connected to a domain network. Additionally, you can strengthen the settings for the Public profile and customize settings for the Private profile. Finally, you can customize IPsec defaults, exemptions, and tunnel authorization on the IPsec Settings tab. Make sure to explore all areas of this dialog box and research any terms you are not familiar with.

## Configure connection security rules with IPsec

You can use IPsec to ensure confidentiality, integrity, and authentication in data transport across channels that are not secure. Though its original purpose was to secure traffic across public networks, many organizations have chosen to implement IPsec to address perceived weaknesses in their own private networks that might be susceptible to exploitation.

If you implement IPsec properly, it provides a private channel for sending and exchanging potentially sensitive or vulnerable data, whether it is email, FTP traffic, news feeds, partner and supply-chain data, medical records, or any other type of TCP/IP-based data. IPsec provides the following functionality:

- Offers mutual authentication before and during communications.
- Forces both parties to identify themselves during the communication process.
- Enables confidentiality through IP traffic encryption and digital-packet authentication.

### Exploring connection security rules

A connection security rule forces authentication between two peer computers before they can establish a connection and transmit secure information. Windows Firewall with Advanced Security uses IPsec to enforce the following configurable rules:

- **Isolation** An isolation rule isolates computers by restricting connections based on credentials, such as domain membership or health status. Isolation rules allow you to implement an isolation strategy for servers or domains.
- **Authentication exemption** You can use an authentication exemption to designate connections that do not require authentication. You can designate computers by a specific IP address, an IP address range, a subnet, or a predefined group such as a gateway.
- **Server-to-server** This type of rule usually protects connections between servers. When you create the rule, you specify the network endpoints between which communications are protected. You then designate requirements and the authentication that you want to use.
- **Tunnel** This rule allows you to protect connections between gateway computers. It is typically used when you are connecting across the Internet between two security gateways.
- **Custom** There might be situations in which you cannot configure the authentication rules that you need by using the rules available in the New Connection Security Rule Wizard. However, you can use a custom rule to authenticate connections between two endpoints.

## Firewall rules and connection security rules

Firewall rules allow traffic through a firewall, but do not secure that traffic. To secure traffic with IPsec, you can create connection security rules. However, when you create a connection security rule, this does not allow the traffic through the firewall. You must create a firewall rule to do this if the firewall's default behavior does not allow traffic. Connection security rules do not apply to programs and services. They apply only between the computers that are the two endpoints.



---

### **EXAM TIP**

Connection security rules specify how and when authentication occurs, but they do not allow those connections. To allow a connection, you must create an inbound or outbound rule. During the inbound or outbound rule creation, you choose the required conditions for the connection, including requiring that the connections have been authenticated by using IPsec. When you do, connections will be secured using the settings in the IPsec properties and rules in the Connection Security Rule node.

---

## Configure authentication exceptions

When you configure a rule to allow traffic only when the connection between the communicating computers is secured using IPsec, you are creating an authenticated exception. You configure this option from the application Action page of the Rule Wizard when creating an inbound or outbound rule. When you choose the Allow The Connection If It Is Secure option on the Action page, you are configuring the rule to allow the connection using the settings in IPsec properties and rules in the Connection Security Rule node.

To create an inbound rule that applies to a single TCP port (Telnet, port 23) and create an authenticated exception for it, follow these steps:

1. In Windows Firewall With Advanced Security, select and then right-click Inbound Rules.
2. Click New Rule.
3. For the rule type, click Port, and then click Next.
4. On the Protocol And Ports page, leave TCP selected and in the Specific Local Ports box, type 23. Click Next.
5. For the action to take, select Allow The Connection If It Is Secure, and click Next.
6. To configure authorized users or authorized exceptions, select the applicable check box, click Add, and use the Select Users Or Groups dialog box to add the applicable entries.
7. Repeat step 6 for authorized computers and exceptions. Click Next.
8. Choose the profiles to which the rules should apply. Click Next. Name the rule. Click Finish.

### **IMPORTANT PREPARING FOR THE EXAM**

This book covers the Skills presented in the list of Skills for the exam. However, the Microsoft certification page for this exam clearly states, “Please note that the questions may test on, but will not be limited to, the topics described in the bulleted text.”

This means that you’ll see questions on items that aren’t addressed here, and we can’t even guess what those might be. However, to provide an example, you might see questions that ask you about the different types of Wi-Fi authentication, including Temporal Key Integrity Protocol (TKIP), Advanced Encryption System (AES), and the various Wi-Fi Protected Access (WPA) options. Likewise, you might be faced with questions that require you to know a specific file extension, such as WFW, which is the file type used when you export a Windows Firewall policy. You might be expected to know a little about Branch Cache or Direct Access, too.

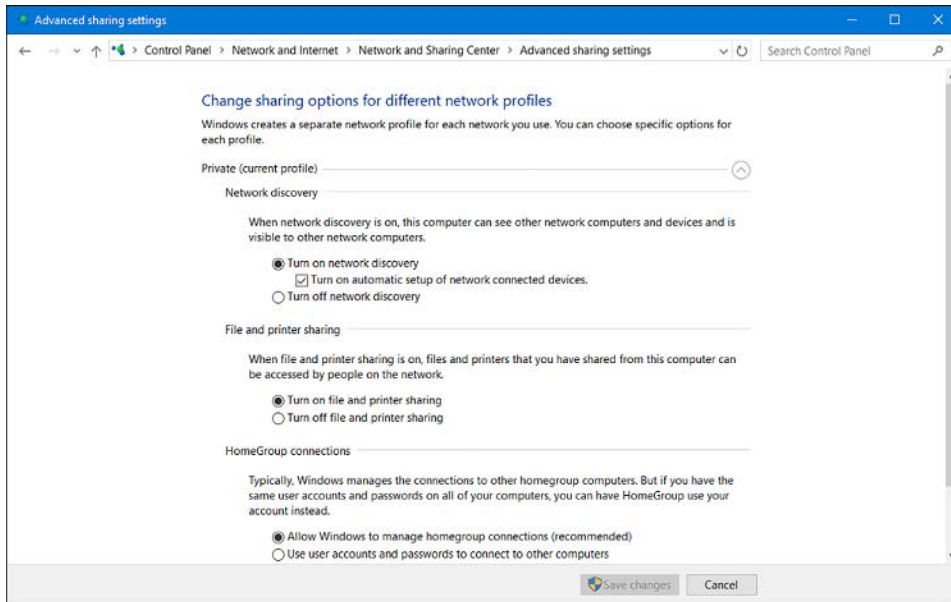
## **Configure network discovery**

By default, Network Discovery is enabled for private and domain networks and disabled for public ones. Network Discovery enables a computer to locate other computers on a network and allows computers on the network to see it as well. This is fine when the network is trusted, but it isn’t a good idea when the network is not. By having these settings and others already configured for the various network types, along with the applicable settings for ports and protocols, the network administrator does not have to configure every aspect of a connection manually. There is one caveat; even if Network Discovery is disabled, a Windows 10 computer can still access network resources if the user knows the names and locations of those resources (because they can’t be discovered by browsing).

It’s possible to make changes to how Network Discovery is configured. You do this from the Network And Sharing Center by following this procedure:

1. Open the Network And Sharing Center.
2. In the left pane, click Change Advanced Sharing Settings.
3. Click the down arrow, if applicable, beside the network type to change the settings: *Private* or *Guest Or Public*.
4. Make the desired change for Network Discovery Settings. Note the other options. See Figure 4-14.
5. Click Save Changes.





**FIGURE 4-14** Advanced sharing settings

## Thought experiments

---

In these thought experiments, demonstrate your skills and knowledge of the topics covered in this chapter. You can find the answers to these thought experiments in the next section.

### Scenario 1

You are troubleshooting connectivity problems on a new laptop that has been added to a local, small business network that already includes eight other computers. Three of these eight are laptops that have always connected without issues. The new laptop can connect when plugged in directly to the router with an Ethernet cable, but it cannot connect wirelessly.

Answer the following questions related to how you would troubleshoot this issue:

1. What do you suspect is causing this problem?
2. Do you think that the troubleshooter in the Network And Sharing Center can resolve this problem?
3. If the Internet Connection troubleshooter uncovers the issue but can't resolve it, where would you turn next and why?

## Scenario 2

You support multiple mobile users who connect to a dozen wireless networks a month and print to the printers on those networks regularly. Users complain that they have to choose their printers manually when using those networks and that sometimes they choose the wrong ones. Not only is this annoying, but because they print sensitive documents, it's also a security issue for your company.

Beyond that, users have connected to wireless networks they'd rather have their laptops forget. The list of networks is quite long and they want you to remove entries for networks they'll never use again (or networks that offered poor connectivity, such as one they have connected to in the past at a hotel or conference center). In the case of networks with poor connections, they'd rather default to broadband.

Regarding this scenario, answer the following questions:

1. What feature do you enable on the users' Windows 10 laptops to enable the network connection to define the printer to which the users will print by default, and what two services does this feature rely on?
2. When a user is in a hotel where she's stayed before, and that user has also connected to the hotel's free Wi-Fi, what must you do to forget that network so that the user can default to broadband when she stays there next time?

## Scenario 3

A client has a large library of media that contains thousands of music files. He wants to share that media in such a way as to be able to access it over the Internet from another computer he owns and keeps at his office. He's enabled the appropriate options in Media Player on both computers. However, he can't get sharing to work.

1. What do you need to do regarding the firewall so that this client can allow Media Player to share music files over the Internet?
2. Will you perform the required task in Windows Firewall or Windows Firewall with Advanced Security?
3. Will you need to be logged on as an Administrator to do this?

## Thought experiment answers

---

This section provides the solutions for the tasks included in the thought experiment.

### Scenario 1

1. There is probably something wrong with the wireless adapter. Maybe it isn't enabled or needs an updated driver to work.

2. Probably. The Network And Sharing Center Internet Connection troubleshooter can discover that the Wi-Fi adapter is disabled, although it might not know why. If the adapter is functional, it can enable it with administrator approval.
3. You can try the Action Center to see if a new driver is available for the Wi-Fi adapter. If not, you can try to locate one using Device Manager. You can also refer to the manufacturer's website to find out how to enable the Wi-Fi adapter, if that is the problem.

## Scenario 2

1. Location-aware printing. This feature enables default printers to be configured based on the network the user is connected to. Location-aware printing uses the Network Location Awareness service and the Network List service to determine the network location.
2. Use the Netsh command to show the list of wireless profiles and then use this command to forget specific networks: Type **netsh wlan delete profile name=<profile name>**.

## Scenario 3

1. You need to create an exception for the Media Player Network Sharing Server (Internet) in Windows Firewall.
2. You can perform this task in Windows Firewall. You will create an app exception.
3. Yes. You must be able to input Administrator credentials or be logged on as an Administrator to enable Change Settings in Windows Firewall.

## Chapter summary

---

- After you connect to a network, your computer is given a unique IP address on that network segment. Every host connected to a network must have an IP address. You can use several troubleshooting tools to diagnose connection problems, if necessary.
- Name resolution enables network nodes to use friendly names to identify each other on the network rather than just an IP address.
- A network location determines the different types of network traffic that are enabled for a network adapter.
- There are several ways to connect to a wireless network including using Control Panel and the Network icon in the desktop's taskbar.
- There is a default priority for networks to which the user has previously connected: Ethernet, Wi-Fi, and mobile broadband. When there are two or more wireless connections available, Windows defaults to the last one used. You can manage networks by using the Settings app or the Netsh command.

- Each network adapter has options available for configuration. You can access these by right-clicking the network adapter in Network Connections and selecting an option from the shortcut menu.
- Location-aware printing lets users configure a default printer for each network they connect to.
- In Windows Firewall you can view the settings for private and public networks and make basic changes to the settings there. You can also disable the firewall there.
- In Windows Firewall, apps are either allowed through the firewall or not. You can create exceptions to configure specific apps to be able to get through the firewall.
- Windows Firewall with Advanced Security offers many more options for administrators, including configuring their own inbound, outbound, and connection security rules, configuring authenticated exceptions, and making changes to existing firewall settings.
- You can make changes to how Network Discovery is configured for the available public and private profiles using the Advanced Sharing Settings in the Network And Sharing Center.



# Index

## A

- access. *See also* remote access
  - authentication and authorization 250–256
  - Dynamic Access Control 217
  - Effective Access 244–245, 245
  - Effective Access tool 182
  - file access auditing 247–250
  - file and folder 232–256
  - mobile devices 81–82
  - removable storage 187–188
  - troubleshooting 184
- access-based enumeration (ABE) 217–218
- Access Control Entry (ACE) 215, 238
- Access Control List (ACL) 215, 238, 240
- account lockout policies 27–28
- Accounts: Block Microsoft Accounts 4–5
- Active Directory Certificate Services (AD CS) 19
- Active Directory Domain Services (AD DS) 26, 39
  - synchronizing user accounts with 95–97
- Active Directory Domain Services (AD DS) database 2
- Active Directory Federation Services (AD FS) 30, 96
- Add-AppxPackage cmdlet 12
- Add-PhysicalDisk cmdlet 174
- administrative users 253
- Advanced Security Settings dialog box 245
- alerts
  - Cloud App Security 125
  - notification rules 108
  - using 108–109
- Allow permissions 244
- Always Offline Mode 53, 54, 283–284
- Android
  - RemoteApp apps 317–318
- Android devices
  - Remote Desktop on 274
- Any folder sharing 215–216
- APIPA. *See* Automatic Private IP Addressing
- Application Compatibility Tools 319, 320–324
- application settings 78
- application virtualization 327–330
- apps
  - Cloud App Security 123–127
  - compatibility modes for 323
  - deep linking 17–18
  - desktop 9
  - installation 5–8
    - choosing users for 16
    - from Company Store 17
    - using Microsoft Office 365 5–7
    - using Microsoft Store 8–10
  - line-of-business (LOB) 10
  - management 307–336
    - desktop 319–333
    - RemoteApp 307–319
  - sequencing 328–329
  - sideloading 11–17
  - System Restore and 342–343
  - updating 382–385
  - virtualization 327–330
- App-V 327–330
  - MDOP and 327–328
  - requirements 327–328
  - sequencing apps 328–329
- App-V Sequencer 328–329
- AppX Windows PowerShell module 12–13
- assigned groups 105
- Attach Task To This Event option 250
- auditing
  - file access 247–250

## authentication

- authentication 18–33
  - account policies to protect 27–28
  - Azure AD 30–33
  - biometrics 22–23, 33
  - BitLocker 65–66, 189
  - computer accounts 26
  - configuration 250–256
  - Credential Manager 28
  - digital certificates for 19
  - domains 26
  - exceptions, configuring 156–157
  - Kerberos 265
  - Kerberos v5 26
  - multifactor 19, 33, 189
  - picture passwords 22
  - remote 262–268
  - Secure Channel 27
  - user accounts 26
  - virtual smart cards 20–22
- authorization
  - administrative users 253
  - Azure AD 30–33
  - configuration 250–256
  - personal devices 30
  - standard users 251–253
  - User Account Control 250–256
  - workgroups 25
- Automatic Private IP Addressing (APIPA) 134
- Azure Active Directory (AAD) 95
- Azure Active Directory (AD) Connect tool 96–97
- Azure Active Directory (Azure AD)
  - joining devices in 30–33
- Azure Information Protection 120–123
  - activation of 121
  - client installation 122–123
  - configuration 120
  - labels 120
  - policies 121–122
- Azure portal
  - Intune policies configuration in 111–112
- Azure Rights Management (Azure RMS) 120

## B

- Backup And Restore (Windows 7) tool 353–357, 361, 362
- backups
  - creating 354–355
  - of EFS-protected files 235–237
  - scheduling 354

- battery settings 57
- biometrics 22–23, 33
- BitLocker 63–68, 117–118, 185, 188, 233
  - authentication methods 189
  - configuration 64–67, 190–191, 194–196
  - data recovery 197–200
  - Microsoft BitLocker Administration and Monitoring 200–203
  - moving encrypted drive to another computer 193
  - recovery keys 65
  - startup key storage 67–68, 197–198
  - support for 188–193
  - suspending 193
  - terminology 197–198
  - upgrading 192–193
  - using 189–192
  - without TPM 65
- BitLocker Network Unlock 198
- BitLocker Recovery Password Viewer 200
- BitLocker To Go
  - configuration 196–197
  - data recovery 198–200
  - support for 188–193
- Bluetooth 223
- boot troubleshooting 345–346
- bring your own device (BYOD) 74
- Bring Your Own Device (BYOD) 294
- broadband connectivity
  - mobile devices 82–84
- broadband tethering
  - configuration 269–272

## C

- Certificate Authority (CA) 19
- certificate compliance reports 107
- certificates
  - digital 19
  - EFS 236, 237
  - Remote Desktop Session Host 316
- certmgr.msc 19–20
- Challenge-Handshake Authentication Protocol (CHAP)
  - 264, 266
- Checkpoint-Computer cmdlet 341
- checkpoints
  - creating 48
  - restoring 49
- choose your own device (CYOD) 74
- Cipher.exe 236

- Clear-DnsClientCache cmdlet 140
- click-to-run installation 8
- client certificates 19
- Cloud App Security (CAS) 123–127
  - accessing and exploring 124–125
  - alerts 125
  - General Dashboard 125
  - layers of 123–124
  - Office 365 126–127
- Cloud Discovery 123, 124
- cloud settings 78
- cloud storage 29
- command-line tools
  - BitLocker configuration using 194–196
  - for connectivity issues 139
  - for sharing folders 216
- comma separated value (CSV) files 96
- Company Store
  - installing apps from 17
- Compatibility Administrator 320, 321–324
- Component Store 380–381
- computer accounts
  - authentication 26
- computer groups
  - management of 104–106
- computer inventory reports 106
- Computer Management Intune Policies 76–77
- Computer Management MMC snap-in 215–216
- configuration
  - authentication and authorization 250–256
  - authentication exceptions 156–157
  - Azure Information Protection 120
  - BitLocker 64–67, 190–191, 194–196
  - BitLocker To Go 196–197
  - broadband tethering 269–272
  - connection security rules 155–156
  - DAC 184
  - disk quotas 245–247
  - file and folder access 232–256
  - file recovery 357–365
  - folder location 40–41
  - folder permissions 213–218
  - HomeGroup 208–210
  - Hyper-V 43–52
  - information protection 113–127
  - libraries 210–213
  - local accounts 29
  - location-aware printing 146–147
  - Microsoft account 29
    - using Group Policy 4–5
  - Microsoft Intune subscriptions 102–103
  - Microsoft Office 365 6
  - Mobile Device Management 86–87
  - mobile devices 73–88
  - mobility options 52–63, 281–302
  - Network Discovery 157–158
  - networking 133–162
    - IP settings 133–143
    - name resolution 139–141
    - network adapters 145–146
    - network locations 141–143
    - network settings 143–148
  - network security 147–158
  - NTFS permissions 238
  - offline file policies 282–285
  - OneDrive 224–229
  - picture passwords 22
  - power plans 57–58
  - power policies 285–290
  - printers 219–224
  - RemoteApp apps 313–316
  - remote connections 261–281
  - Remote Desktop 272–279
  - restore points 353–357
  - security
    - for mobile devices 63–68
  - startup key storage 67–68
  - storage 163–206
  - Sync Center 81–82
  - synchronization settings 3–4
  - sync options 55–56, 294–300
  - system recovery 337–357
  - System Restore 340–347
  - user data 37–41
  - user profiles 38–40
  - virtual machines 46–48
  - virtual smart cards 21
  - Wi-Fi Direct 63
  - WiFi Direct 300–302
  - Windows Firewall 149–154
  - Windows Hello 33
  - Windows To Go 290–294
  - Windows Update 366–370, 373–377
  - Work Folders 80–81
  - Workplace Join 30
- connection security rules 153, 155–156
- connectivity issues 138–139, 153



## Control Panel

### Control Panel

- BitLocker configuration in 65–66
- Work Folders configuration in 80
- Cost-Aware Synchronization 53
- Credential Locker 28
- Credential Manager 28–29, 237
- credential roaming 237

## D

### data

- user
  - configuration 37–41
  - migration 41–43
- data access. *See* access
- data encryption
  - BitLocker 64–68, 118–119, 185, 188–202, 233
  - Encrypting File System 185–187, 233–237
  - File History support for 361
- Data Encryption Standard (DES) 264
- data loss prevention (DLP) policy 114–116
- data recovery
  - BitLocker 197–200
- Data Recovery Agent (DRA) 185–186, 233, 234, 235
- data security 179–203. *See* information protection;  
    *See* security
  - BitLocker 188–202
  - Dynamic Access Control 184–185
  - Encrypting File System 185–187
  - permissions management 179–185
  - removable storage 187–188
- data storage
  - cloud-based 29
  - configuration 163–206
  - Distributed File System 164–167
  - OneDrive 174–178, 224–232
  - removable 187–188
  - Storage Spaces 167–174
  - support for 163–178
  - user data 6
- data synchronization 79–82
  - sync options 294–300
- default gateway 134
- defensive layering 247–248
- Deny permissions 244
- Deny Write Access To Drives Not Protected By
  - BitLocker 188

- Deployment Image Servicing and Management (DISM)  
    294, 381
- Deployment Image Servicing and Management (DISM)  
    cmdlets 12–13
- desktop apps 9, 319–333
  - App-V and 327–330
  - co-existence support 324–330
  - compatibility issues 319, 320–324
  - compatibility modes for 323
  - deployment using Microsoft Intune 331–333
  - Hyper-V and 324–326
  - RemoteApp and 326–327
  - User Experience Virtualization and 330–331
- Desktop Connections fee 317
- detected software reports 106
- device capabilities settings 78
- device deployment 37–72
  - mobility options 52–63
  - security configuration 63–68
  - user data 37–43
  - virtual machines 43–52
- device drivers
  - resolving problem 378–379
  - rollback of 351–353
  - signed 351
  - uninstalling 378
- Device Enrollment Manager (DEM) 99–100
- device history reports 107
- device management 94–113. *See also* remote access
  - Microsoft 365 Business enrollment 97–99
  - Microsoft 365 Enterprise enrollment 99–100
  - Microsoft Intune subscriptions 102–103
  - Microsoft Service Connection Point role 103–104
  - monitoring and alerts 106–109
  - policy management 110–112
  - remote computers 112–113
  - troubleshooting Microsoft Intune 109
  - user account provisioning 95–97
  - user and computer groups 104–106
  - view and manage devices 100–102
- device registration
  - in Azure AD 30–33
- Device Registration Service (DRS) 30
- DFS. *See* Distributed File System
- DFS Namespaces (DFSN or DFS-N) 165
- DFS Namespace service (Dfssvc.exe) 166
- DFS Replication (DFSR or DFS-R) 164–167

Dfsutil.exe 166  
 DHCP. *See* Dynamic Host Configuration Protocol  
 DHCP scope 134  
 dial-up 262, 263  
 differencing disks 49  
 digital certificates 19  
 DirectAccess 53  
 DirSync 96  
 Disable-ComputerRestore cmdlet 341  
 discretionary access control list (DACL) 238  
 Disk Cleanup 381  
 disk drives  
   kepping together 171  
 disk quotas 232  
   configuration 245–247  
   policies 246–247  
 disk space 172  
 disk usage 172  
 Dism.exe 380  
 Distributed File System (DFS) 163, 164–167  
 DNS. *See* Domain Name Service  
 document version history 365  
 domain accounts 2  
   associating Microsoft account with 2–3  
 domain controllers 26  
 Domain Name Service (DNS) 135  
 domain networks 141  
 domains 23, 26  
 DRA. *See* Data Recovery Agent  
 driver rollback 351–353  
 Driver Roll Back feature 352–353  
 Driver Store 351  
 DVDs 187  
 Dynamic Access Control (DAC) 184–185, 217  
 dynamic groups 105  
 Dynamic Host Configuration Protocol (DHCP) 134

## E

EAP-MS-CHAPv2 265  
 Echo Request messages 139  
 Effective Access 244–245, 245  
 Effective Access tool 182  
 EFS. *See* Encrypting File System (EFS)  
 electronic point of sale (EPOS) 262  
 Electronic Software Distribution (ESD) 329  
 elevation prompts, UAC 253–256

Enable-ComputerRestore cmdlet 341  
 Encrypting File System (EFS) 185–187, 232, 233–237, 361  
   backup and recovery 235–237  
   credential roaming 237  
   Windows Public Key Infrastructure and 234  
 encryption  
   BitLocker 64–68, 118–119, 185, 188–202, 233  
   Encrypting File System 185–187, 233–237  
   File History support for 361  
   Perfect Forward Secrecy 174  
   settings 78  
 Endpoint Protection 76–77, 108  
 enhanced PINs 197  
 environmental variables 39  
 Extensible Authentication Protocol (EAP) 265  
 Extensible Authentication Protocol-Transport  
   Layer Security (EAP-TLS) 264

## F

FAT volume 243  
 federation  
   Azure AD Connect and 96  
 File Explorer  
   accessing OneDrive from 225  
   History 213  
   Quick Access feature 212–213  
   sharing indicator 218  
 File History  
   configuration 358–361  
   encryption support 361  
   file recovery 360–361  
   Previous Versions and 361–363  
   restore points 360  
   turning off 361  
 file recovery  
   configuration 357–365  
   File History 358–361  
   OneDrive 363–365  
   Previous Versions 361–363  
 files  
   access  
     auditing 247–250  
     configuring 232–256  
   copying 243  
   deleting from library 212  
   encrypting 233–237

## File Server Resource Manager (FSRM)

- fetching, using OneDrive 230–231
- moving 243
- Offline Files 53–54, 81, 282–285, 296–298
- OneDrive 226
- permissions. *See* permissions management
- recovery of 177–178
- restoring previous versions of 361–363
- synchronization 282–284, 296–298
- System Restore and 342–343
- File Server Resource Manager (FSRM) 232, 247
- file systems 179–180
- filtering 149
- firewalls
  - rules 156
  - Windows Firewall 149–154
  - Windows Firewall Settings template 77
- flash drives 187–188
- folder location
  - configuration 40–41
- folders
  - access, configuring 232–256
  - Any folder sharing 215–216
  - copying 243
  - deleting from library 212
  - encrypting 233–237
  - moving 243
  - OneDrive 226
  - permissions 213–218
  - Public 214
  - renamed 216
  - restoring previous versions of 361–363
  - shared 213–218, 241–242
  - sharing from command line 216
  - sharing using Windows PowerShell 216–217
  - Work Folders 298–300
- folder structure 181
- Fresh Start 349–350

## G

- Get-AppxLastError cmdlet 12
- Get-AppxLog cmdlet 12
- Get-AppxPackage cmdlet 12
- Get-AppxPackageManifest cmdlet 12
- Get-ComputerRestorePoint cmdlet 341
- Get-DnsClientCache cmdlet 141
- Get-NetIPAddress cmdlet 140

- Get-NetIPv4Protocol cmdlet 140
- Get-SmbShare cmdlet 217
- Get-StoragePool cmdlet 174
- Get-VirtualDisk cmdlet 174
- Global Catalog 26
- Global Policy 121–122
- /grant switch 241
- graphical user interface (GUI) 283
- Graphical User Interface (GUI) 173
- group memberships 104–105
- Group Policy 74
  - accessing 4
  - biometrics settings 22–23
  - disabling Microsoft Store access with 10
  - enabling sideloading using 11–12
  - for BitLocker 190, 199
  - for Windows to Go 61
  - Microsoft account configuration using 4–5
  - offline file policies 54
  - power policies 59–60
  - power policy configuration using 287, 289
  - removable media management using 187–188
  - Work Folders configuration using 81, 299–300
- Group Policy Objects 184
- Group Policy Objects (GPOs) 27
  - auditing 248, 250
  - disk quota 246
  - for Microsoft Store functionality 384
  - for signed packages 316–317
  - for Windows Update 373–377
- groups
  - adding, to Microsoft Intune 14
  - assigned 105
  - dynamic 105
  - homegroups 23–24
  - HomeGroups 208–210
  - managing 104–106
  - workgroups 23, 24–25
- guest networks 141

## H

- Health Insurance Portability and Accountability Act (HIPAA) 114
- Hibernate 61
- HKEY\_CURRENT\_USER registry 38
- homegroups 23–24

HomeGroups  
 configuration 208–210  
 creating 208–209  
 file and folder sharing 210  
 joining 209  
 troubleshooting 209

Hotspot 2.0 networks 271–272

hotspots 83, 269–272

Hyper-V 324–326  
 checkpoints 48–49  
 configuration 43–52  
 configuring virtual machines in 46–48  
 creating virtual machines in 45–46  
 enabling 44  
 installation 325  
 moving virtual machines 51–52  
 requirements 325  
 virtual switches 49–50

**I**

ICACLS.exe 241

identity management 1–36  
 authentication and authorization 18–33  
 support and install apps 1–18

inbound rules 152, 153, 156

information protection  
 Azure 120–123  
 BitLocker 117–118  
 Cloud App Security 123–127  
 configuration 113–127  
 data loss prevention (DLP) policy 114–116  
 key pillars of 117–118  
 Windows Information Protection (WIP) 117–119

inheritance  
 permissions 242–243

installation  
 apps  
   from Company Store 17  
   with Microsoft Office 365 5–8  
   with Microsoft Store 8–10  
 click-to-run 8  
 Microsoft Office 365 7

Internet Control Message Protocol (ICMP) 139

Internet Key Exchange, Version 2 (IKEv2) 264

Internet Service Providers (ISPs) 82

Intune. *See* Microsoft Intune

Intune App Protection 98

iOS  
 RemoteApp apps 317–318  
 Remote Desktop on 275

IP addresses 133  
 conflicts 138  
 filtering 149  
 name resolution 139–141  
 requirements for 134

Ipconfig 139

Ipconfig /all 139

IPsec 155–156

IP settings  
 configuration 133–143

IPv4 addresses 135, 137

IPv6 addresses 135, 137

## K

Kerberos 265

Kerberos Key Distribution Center (KDC) 26

Kerberos v5 authentication protocol 26

## L

Last Known Good Configuration 347

Layer 2 Tunneling Protocol (L2TP) 264

libraries  
 adding locations 211  
 configuration 210–213  
 creating 211  
 deleting files from 212

license installation reports 106

license purchase reports 106

licenses  
 Microsoft 365 99, 103  
 user 95

line-of-business (LOB) apps 10

Link Layer Topology Discovery (LLTD) protocol 214

LLTD Mapper (LLTDIO) 214

local accounts 2  
 associating Microsoft account with 2–3  
 configuration 29

local cache 53

local profiles 38

Local Security Policy 27

location-aware printing 146–147

LockDown VPN profile 268

lockout policies 27–28

## Logical Unit Number

Logical Unit Number (LUN) 168  
Long Term Servicing Channel (LTSC) 372

## M

### Mac computers

Remote Desktop on 275

malware 108, 251, 256

malware settings 78

Manage-bde.exe 65, 66–67, 194

Manage Storage Spaces console 171

mandatory profiles 40

MDM. *See* Mobile Device Management

metered networks 83–85

### Microsoft 365

about 73

Admin Center 95

device management 94–113

information protection 113–127

licenses 103

mobile device support in 73–88

software deployment 88–94

user licenses 95

### Microsoft 365 Business

device enrollment in 97–99

view and manage devices 100–101

### Microsoft 365 Enterprise

device enrollment in 99–100

view and manage devices 101–102

### Microsoft account

associating with local or domain account 2–3

configuration 29

synchronization settings 3–4

using Group Policy 4–5

disabling 4–5

integration of 2–5

personalization settings 2–5

### Microsoft BitLocker Administration and Monitoring (MBAM) 119, 200–203

### Microsoft Desktop Optimization Pack (MDOP) 201, 327–328

### Microsoft Intune

adding users and groups 14

Administrator Console 332

Connection Point role 103–104

deep link apps using 17–18

desktop app deployment with 331–333

Device Enrollment Manager 99–100

group management 104–106

Mobile Device Management and 84–88

monitoring and alerts 106–109

policies

classic 110–111

computer management 76–77

configuring in Azure portal 111–112

deployment 111–112

managing 110–112

mobile devices 74–79

policy templates 75–76

remote computer management 112–113

sideloading apps using 13–16

software deployment using 88–94

subscriptions configuration 102–103

troubleshooting 109–110

updates information in 89–90

WIP policy in 118–119

Microsoft Intune Agent Settings template 76–77

Microsoft Intune Center Settings template 77

Microsoft Intune Policy page 110

### Microsoft Office 365

about 5–6

Admin Center 6–7

app installation with 5–7

configuration 6

deployment 7–8

features 8

installation 7

updates 5

Microsoft Online Services 175–176

Microsoft Remote Desktop Assistant 274

Microsoft Service Connection Point role 103–104

Microsoft Services Agreement 175

### Microsoft Store

about 9

apps installation using 8–10

disabling access to 10

### Microsoft Store apps

updating 382–385

Microsoft Store for Business 10

Microsoft Store for Education 10

migration

user data 41–43

Miracast over Infrastructure 300

mobile device inventory reports 106

- Mobile Device Management (MDM) 74, 84–88
    - annual certificate renewal 88
    - configuration 86–87
    - enrolling devices 87–88
  - mobile devices 261–306. *See also* remote access
    - access 81–82
    - broadband connectivity 82–84
    - broadband tethering 269–272
    - data synchronization 79–81
    - managing remote 84–88
    - mobility options for 52–63
    - offline file policies 53–54
    - policies 74–79
    - power policies 285–290
    - power settings 56–60
    - remote connectivity 53
    - security for 63–68
    - security policies 78–79
    - sync options 55–56
    - Wi-Fi Direct 63
    - Windows To Go 60–63
  - Mobile Device Security Policy template 78–79
  - mobile hotspots 83
  - Mobility and Multi-homing (MOBIKE) protocol 264
  - mobility options 52–63
    - configuration 281–302
    - offline file policies 282–285
    - power policies 285–290
    - sync options 294–300
    - WiFi Direct 300–302
    - Windows To Go 290–294
  - Modify permission 244
  - monitoring
    - managed devices 106–109
  - MS-CHAP v2 266
  - Mstsc.exe 275
  - multifactor authentication 19, 33, 189
- ## N
- name resolution
    - configuration 139–141
  - namespaces
    - DFS 166
  - near field communication (NFC) 219, 223–224
  - Netsh 63
  - Net Share 216
  - Netsh tool 139, 145
  - Netstat tool 139
  - network adapters
    - configuration 145–146
  - Network And Sharing Center 138, 209, 214
  - network discovery 214
  - Network Discovery 157–158
  - Network Discovery settings 214
  - networking
    - configuration 133–162
      - IP settings 133–143
      - name resolution 139–141
      - network settings 143–148
    - connectivity issues 138–139
    - IP addresses 134
    - virtual private 262–268
  - network locations 141–143
    - for folders 40–41
  - networks 23
    - broadband connectivity 82–84
    - connecting to 133–139
    - connection status, viewing 138
    - domain 141
    - domains 26
    - guest 141
    - Hotspot 2.0 271–272
    - metered 83–85
    - private 141
    - public 137, 141
    - terminology 134–135
    - wireless
      - connecting to 143–144
      - managing preferred 144–145
  - network security
    - configuration 147–158
  - network sharing 23–26
  - New-StoragePool cmdlet 174
  - New Technology File System (NTFS) 179–184, 213, 362
    - auditing 247–250
    - disk quotas 245–247
    - permissions 238–245
    - shared folders and 241–242
  - New-VirtualDisk cmdlet 174
  - noncompliant apps reports 107
  - Non-Volatile Memory Express (NVMe) 245
  - notification rules 108
  - Nslookup tool 139
  - NTUSER.DAT 38

## O

Office 365. *See* Microsoft Office 365

Cloud App Security 126–127

data loss prevention (DLP) policy 114–116

Office 365 Security & Compliance Center 114–116

offline file policies 53–54, 81, 282–285

Offline Files 282–285

syncing 296–298

OneDrive 29

configuration 224–229

deleting personal settings from 296

document version history 365

fetching files using 230–231

file recovery from 363–365

files and folders 226

help for 174–175

limitations of 226

mapping drive to 227

OneDrive for Business and 229–232

options 227–228

pricing plans 225

recovering files from 177–178

Recycle Bin 177–178, 226, 363–365

service availability 175–176

support for 174–178

synchronization 226

sync settings 228–229

usage policy 226

using on other devices 232

OneDrive for Business 178, 229–232

operating system

rolling back 381–382

Optimize-StoragePool cmdlet 174

outbound rules 152, 153

out-of-box experience (OOBE) 229

## P

page description language (PDL) 219

parity 168

parity volume mirroring 169

Password Authentication Protocol (PAP) 264, 266

passwords 19

Credential Manager for 28

picture 22

policies 27

recovery 67, 189, 197

recovery key 67

saving 28

weak 27

Patch Tuesday 366

Perfect Forward Secrecy (PFS) 174

permissions management 179–185

combining NTFS and Share 183–184

NTFS permissions 179–182, 213, 238

permissions inheritance 242–243

shared folders 213–218

Share permissions 183–184, 213, 215

troubleshooting 183, 184

Personal certificate store 19

personal devices

configuring access for 30

personalization settings 2–5

personally identifiable information (PII) 114–115

picture passwords 22

Ping tool 139

PINs 68, 197

PKI. *See* public key infrastructure

Pnputil.exe 219, 351–352

Point-to-Point Tunneling Protocol (PPTP) 263–264

port numbers 149

port rules 153

powercfg.exe 58–59, 288–290

power plans 57–58

power policies 59–60, 285–290

power settings 56–60

powercfg.exe 58–59

power plans 57–58

Settings app 56–57

PowerShell. *See* Windows PowerShell

Power & Sleep Settings option 285–286

Premium OneDrive 225

Previous Versions 361–363

printer drivers 219

printer ports 219

printers

key terms 219

near field communication 223–224

print management 220–222

print server properties 222–223

shared, configuring 219–224

Type 4 printer drivers 219–220

printing

location-aware printing 146–147

Print Management console 222  
 private networks 141  
 program rules 153  
 protocols 149  
 Public folders 214  
 public key infrastructure (PKI) 19  
 public networks 137, 141

## Q

Quick Access 212–213

## R

radio frequency identification (RFID) 223  
 RD Session Host role service 308–310  
 Read permission 244  
 recovery  
   file 357–365  
   of EFS-protected files 235–237  
   system 337–357  
 recovery drives 338–340  
 Recovery Environment (RE) 338  
 recovery keys 65, 67, 189, 191, 197, 199  
 recovery passwords 67, 189, 197  
 Recycle Bin 177–178, 226, 363–365  
 redundancy 168  
 referral cache 165  
 remote access 261–306  
   broadband tethering 269–272  
   mobility options 281–302  
   remote connections 261–281  
 RemoteApp And Desktop Connections 313–316, 317  
 RemoteApp apps 307–319, 326–327  
   advantages of 307  
   configuration 313–316  
   distribution 318–319  
   GPOs for signed packages 316–317  
   installation 310–313  
   iOS and Android support 317–318  
   prerequisites 308–313  
 remote computers  
   managing 112–113  
 remote connections 261–281  
   broadband tethering 269–272  
   configuring PC for 273–274  
   remote authentication 262–268  
   Remote Desktop 272–281  
   VPN 262–268  
   WiFi Direct 300–302  
 Remote Desktop  
   configuration 272–279  
   deployment of 309–310  
   on Android 274  
   on iOS and Mac 275  
   on Windows 10 274  
   pen support 280–281  
   Restricted Admin mode 277–279  
   settings 275–277  
   troubleshooting 279  
   Zoom support 280  
 Remote Desktop Connection Manager (RDCMan) 281  
 Remote Desktop Protocol 261–281  
 Remote Desktop Services (RDS) 326–327  
 Remote Desktop Session Host 310, 316  
 Remote Desktop Web Access (RD Web Access) 318–319  
 Remote Differential Compression (RDC) 165  
 Remote Server Administration Tools (RSAT) 166, 200  
 removable storage 179, 196–197  
   controlling access to 187–188  
 Remove-AppxPackage cmdlet 12  
 Remove-PhysicalDisk cmdlet 174  
 Remove-StoragePool cmdlet 174  
 Repair-VirtualDisk cmdlet 174  
 reports  
   creating 107  
   on software updates 89–90  
   types of 106–107  
   using 106–107  
 reset 347–349  
 Reset This PC option 347–349  
 Resilient File System (ReFS) 168, 172, 247  
 Restricted Admin mode  
   Remote Desktop 277–279  
 Resolve-dnsname cmdlet 140  
 resources ownership 245–246  
 Responder (RSPNDR) 214  
 restore points 353–357, 360, 362  
 roaming profiles 39–40  
 Robocopy 164  
 Robust File Copy for Windows (Robocopy) 164  
 root certificates 19



## S

- SaaS. *See* software as a service
- safe mode 343, 345, 353
- Sarbanes-Oxley Act 247
- Schannel 27
- scheduling
  - backups 354
  - synchronization 82
- Secure Channel 27
- Secure Desktop 256
- Secure Digital High-Capacity (SDHC) memory cards 339
- Secure Sockets Layer (SSL) protocol 264
- Secure Socket Tunneling Protocol (SSTP) 264
- security. *See also* authentication
  - account policies 27–28
  - alerts 108–109
  - authentication exceptions 156–157
  - BitLocker 188–202
  - Cloud App Security 123–127
  - connection security rules 155–156
  - connectivity and 153
  - data 179–203
  - Dynamic Access Control 184–185
  - Encrypting File System 185–187
  - for mobile devices 63–68
  - information protection 113–127
  - mobile device policies 78–79
  - network 147–158
  - Network Discovery 157–158
  - permissions management 179–185
  - personal devices 30
  - removable storage 187–188
  - TLS/SSL 27
  - Windows Defender Security Center 148–149
  - Windows Firewall 149–154
- Security Account Manager (SAM) 2, 25
- Security & Compliance Center 114–116
- Security log 249
- Security Support Provider (SSP) 27
- Semi-Annual Channel 371
- Server Message Block (SMB) 213
- service set identifier (SSID) 145
- Set-PhysicalDisk cmdlet 174
- Set-StoragePool cmdlet 174
- Settings app 3–4, 11, 29, 56–57
  - Network Setting 145
- shared resources 207–232
  - access-based enumeration 217–218
  - folder permissions 213–218, 241–242
  - HomeGroup 208–210
  - libraries 210–213
  - OneDrive 224–232
  - printers 219–224
  - Public folders 214
- Share permissions 183–184, 213, 215
- Shim Infrastructure 320–321
- shims 320–321
- sideloading
  - apps 11–17
  - enabling 11–12
  - using Microsoft Intune 13–16
- single sign-on (SSO) 30
- Slow-link Mode 285
- smart cards
  - virtual 20–22
- SmbShare module 217–218
- software
  - installation 5–16
  - software as a service (SaaS) 6
  - Software Assurance (SA) 328
  - software deployment
    - using Microsoft Intune 88–94
  - software updates
    - approving or declining 91–92
    - automatic approval settings 92–93
    - deadlines for installations 93
    - identifying required 89–90
    - third-party 93–94
- Solid State Drive (SSD) 245
- SSO. *See* single sign-on
- Standard User Analyzer 320
- standard users 251–253
- StartComponentCleanup task 380
- startup keys 197–198
- startup key storage 67–68
- Startup Settings 345–346
- storage
  - cloud 29
  - cmdlets 174
  - configuration 163–206
  - Distributed File System 164–167
  - OneDrive 174–178, 224–232
  - removable 179, 187–188, 196–197

- startup keys 197–198
- startup key storage 67–68
- viewing usage 172–173
- Storage Area Network (SAN) 167, 245
- storage pools 167–168, 169–171
- Storage Spaces 163
  - configuration 168–173
  - Manage Storage Spaces console 171
  - managing 173–174
  - redundancy types 168
  - size of 171
  - support for 167–173
- subnet masks 134, 135
- Sync Center 55, 81–82, 296–298
- synchronization
  - background file 282–284, 283
  - OneDrive 226, 228–229
  - options configuration 294–300
  - scheduling options 297–298
  - UE-V and 330–331
  - Work Folders 298–300
- synchronization settings 3–4
- sync options 55–56
- sync shares 298–300
- system access control list (SACL) 239
- System Center Configuration Manager 103–104, 198
- System Center Configuration Manager (SCCM) 373
- system crash 337–338
- system image
  - creating 354–355
- System Image Recovery 355–356
- System Properties dialog box 24
- system recovery
  - configuration 337–357
  - driver rollback 351–353
  - Fresh Start 349–350
  - recovery drives 338–340
  - reset 347–349
  - restore points 353–357
  - System Image Recovery 355–356
  - system repair disks 356–357
  - System Restore 340–347
  - troubleshooting 344–346
- system repair disks
  - creating 356–357
- System Restore 340–347
  - identifying affected apps and files 342–343

- task schedule modification 343
  - Windows RE and 343–347
  - within Windows RE 343
- System Restore Wizard 342
- system settings 78

## T

- Task Scheduler 343, 354, 380
- templates
  - computer management 76–77
  - DLP policy 115–117
  - Intune policies 75–76
- terms and conditions reports 106
- tethering
  - broadband 83, 269–272
- third-party software
  - updates of 93–94
- three-way mirroring 168
- Time to Live (TTL) 165
- TPM Lockout 198
- Tpmvscmgr.exe 21
- Tracert tool 139
- Transport Layer Security (TLS)/Secure Sockets Layer (SSL)
  - security 27
- Triple DES (3DES) algorithm 264
- troubleshooting
  - access 184
  - boot 345–346
  - connectivity issues 138–139
  - Encrypting File System 186–187
  - HomeGroups 209
  - Microsoft Intune 109–110
  - name resolution 140–141
  - permissions 184
  - Remote Desktop 279
  - system recovery 344–346
  - updates 378–379
- Trusted Platform Module (TPM) 61, 64, 188, 191, 290
  - BitLocker and 119
- Trusted Platform Module (TPM) chip 20
- Trusted Root Certification Authorities store 19
- two-way mirroring 168
- Type 3 print drivers 219
- Type 4 print drivers 219, 219–220

## Undo feature

# U

- Undo feature 177
- unified extensible firmware interface (UEFI) 344
- Unified Extensible Firmware Interface (UEFI) 191
- Universal Naming Convention (UNC) 166
- Universal Naming Convention (UNC) address 217
- update reports 106
- updates 365–385
  - Component Store 380–381
  - deferring 371
  - delivery optimization for 368–370, 376–377
  - disabling automatic 367–368
  - for enterprise customers 371–373
  - history management 377–378
  - Microsoft Store apps 382–385
  - pausing 367
  - policy configuration 373–377
  - release of 366
  - resolving problem 378–379
  - rolling back 378–382
  - settings configuration 366–370
- Updates page 89–90
- Update-StoragePool cmdlet 174
- USB 2.0 ports 291
- USB 3.0 ports 291
- USB flash drives 187–188
- User Account Control (UAC) 233
  - administrative users 253
  - configuration 250–251
  - elevation prompts 253–256
  - Secure Desktop 256
  - settings 254–255
  - standard users 251–253
- user accounts
  - authentication 26
  - creating from CSV file 96–97
  - manual creation of 95
  - provisioning 95–97
  - roaming profiles 39–40
  - synchronizing with AD DS 95–97
- user credentials
  - saving 28
- user data
  - configuration 37–41
  - migration 41–43
- user-effective permissions 181
- User Experience Virtualization (UE-V) 330–331

- user groups
  - management of 104–106
- user licenses 95
- user names
  - saving 28
- user profiles
  - configuration 38–40
  - local 38
  - mandatory 40
  - migration 41–43
  - roaming 39–40
- users
  - adding, to Microsoft Intune 14
  - administrative 253
  - authentication 18–33
    - remote, authentication of 265–266
    - standard 251–253
- User State Migration Tool (USMT) 41–43
- ut-of-box experience (OOBE) 348–349

# V

- variables
  - environmental 39
- Verisign 19
- VHDX format 50–51
- virtual hard disks (VHDs) 50–51, 168
- virtual hard drives (VHDs) 49
- virtual machines (VMs) 43
  - checkpoints 48–49
  - creating and configuring 44–48
  - Hyper-V and 324–326
  - importing 52
  - moving 51–52
  - virtual disks 50–51
  - virtual switches 49–50
- virtual private networking (VPN) 262
  - authentication and 262–268
  - creating connection 265, 266–268
  - features 267–268
  - protocols 263–264
  - security properties 267
  - VPN Reconnect 268–269
- virtual private networks (VPNs) 53
- virtual smart cards 20–22
- virtual switches 49–50
  - creating 49–50
  - types of 49

Virtual Switch Manager 50  
 volume-level resiliency 168  
 Volume Shadow Copy Service (VSS) 341, 355, 362  
 VPN Reconnect 268–269

## W

Wake-on-LAN (WoL) 198  
 Wbadmin.exe 355  
 WBF. *See* Windows Biometric Framework  
 WiFi Alliance 302  
 Wi-Fi Direct 63  
 WiFi Direct  
   configuration 300–302  
 WiFi hotspots 269–272  
 Wi-Fi networks 82–84  
 WiFi Services 270–271  
 Windows 8 283  
 Windows 10  
   Advanced Troubleshooting Mode 344–346  
   authentication 18–33  
   authentication and authorization 250–256  
   device deployment 37–72  
   device setup 97–98  
   enabling sideloading in 11–12  
   GUI changes 283  
   integration of Microsoft Account with 2–5  
   mobile device support in 73–88  
   mobility options 281–302  
   OneDrive synchronization 226  
   printing capabilities 219–224  
   Remote Desktop app on 274  
   rolling back 381–382  
   shared resources in 207–232  
   Startup Settings 345–346  
   sync options 294–300  
   system recovery 337–357  
   upgrades, deferring 371  
 Windows 10 Anniversary Update 117  
 Windows 10 Enterprise 99  
 Windows 10 Pro 97  
 Windows ADK 42  
 Windows Assessment and Deployment Toolkit (Windows ADK) 320  
 Windows Biometric Framework (WBF) 22, 224  
 Windows Credential Manager 237  
 Windows Defender Credential Guard 237  
 Windows Defender Remote Credential Guard 276–277  
 Windows Defender Security Center 148–149, 150  
 Windows Deployment Services (WDS) 164  
 Windows Deployment Services (Windows DS) 347  
 Windows Firewall  
   allowing app through 151  
   configuration 149–154  
   monitoring 150–151  
   security settings 214  
 Windows Firewall Settings template 77  
 Windows Firewall With Advanced Security 152–154  
 Windows Health Attestation Service 117  
 Windows Hello 33  
 Windows Information Protection (WIP) 117–119  
 Windows Insider Program 372  
 Windows Intune 373  
 Windows Mobility Center 286–287  
 Windows PowerShell  
   AppX module 12–13  
   BitLocker cmdlets 194–195  
   managing Officer 365 with 8  
   managing Storage Spaces using 173–174  
   modifying domain users with 40  
   sharing folders using 216–217  
   System Restore configuration using 341  
   virtual machine configuration in 47–48  
   Windows To Go workspace creation with 62  
   Windows To Go workspace creation with 293–294  
 Windows PowerShell Direct 48  
 Windows Preinstallation Environment (Windows PE) 42–43  
 Windows Public Key Infrastructure (PKI) 234  
 Windows Recovery Environment 61  
 Windows Recovery Environment (Windows RE) 343  
   launching 343–347  
 Windows Server 2012 283  
 Windows Server Update Services (WSUS) 373  
 Windows Software Update Services (WSUS) 220  
 Windows Store. *See* Microsoft Store  
 Windows To Go 60–63  
   certified drives 292  
   configuration 290–294  
   features 61, 290–291  
   hardware considerations 291  
   limitations and requirements 60–61  
   roaming with 291  
   workspace creation 62–63, 292–294  
 Windows To Go Workspace Wizard 292–293  
 Windows Update

## Zero-Day updates

- Advanced Options 366–367
- delivery optimization for 368–370, 376–377
- for enterprise customers 371–373
- history management 377–378
- policy configuration 373–377
- rolling back 378–382
- settings configuration 366–370
- Windows Vault 237
- wireless networks
  - connecting to 143–144
  - managing preferred 144–145
- Work Folders 79–81, 298–300
- workgroups 23, 24–25
- Work Offline button 53
- Workplace Join 30
- workspaces
  - Windows To Go 292–294
- Write-DfsrHealthReport cmdlet 165

## Y

- Your Info tab 2

## Z

- Zero-Day updates 366