Configuring Windows Devices

Exam Ref 70-697

Andrew Bettany
Jason Kellington
Exam Ref 70-697
Configuring
Windows Devices

Andrew Bettany
Jason Kellington
Contents at a glance

Introduction xv
Preparing for the exam xix

CHAPTER 1 Manage Identity 1
CHAPTER 2 Plan desktop and device deployment 39
CHAPTER 3 Plan and implement a Microsoft Intune device management solution 81
CHAPTER 4 Configure networking 119
CHAPTER 5 Configure storage 153
CHAPTER 6 Manage data access and protection 199
CHAPTER 7 Manage Remote Access 255
CHAPTER 8 Manage apps 301
CHAPTER 9 Manage updates and recovery 329

Index 385
This page intentionally left blank
# Contents

## Introduction

Microsoft certifications .......................... xvi
Acknowledgments ................................... xvi
Free ebooks from Microsoft Press ................... xvi
Microsoft Virtual Academy ........................ xvii
Errata, updates, & book support .................... xvii
We want to hear from you .......................... xvii
Stay in touch ....................................... xvii

*Preparing for the exam* .......................... xix

## Chapter 1  Manage identity

Objective 1.1: Support Windows Store and cloud apps. ................. 1
  - Integrate Microsoft account and personalization settings 1
  - Install and manage software 5
  - Sideload apps into offline and online images 9
  - Sideload apps by using Microsoft Intune 12
  - Deep link apps using Microsoft Intune 15
  - Objective summary 16
  - Objective review 17

Objective 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

---

**What do you think of this book? We want to hear from you!**

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

Configure Windows Hello .................................................. 30
Objective summary ......................................................... 31
Objective review ............................................................ 32

Answers ................................................................................. 34
  Objective 1.1: Thought experiment .................................. 34
  Objective 1.1: Review ....................................................... 34
  Objective 1.2: Thought experiment .................................. 35
  Objective 1.2: Review ....................................................... 36

Chapter 2 Plan desktop and device deployment .......................... 39

Objective 2.1: Migrate and configure user data ....................... 39
  Configure user profiles ................................................... 40
  Configure folder location ................................................. 42
  Migrate user profiles ..................................................... 43
  Objective summary ......................................................... 46
  Objective review ............................................................ 46

Objective 2.2: Configure Hyper-V .......................................... 47
  Create and configure virtual machines ............................. 47
  Create and manage checkpoints .................................... 51
  Create and configure virtual switches .............................. 52
  Create and configure virtual disks ................................ 53
  Move virtual machine storage ....................................... 54
  Objective summary ......................................................... 56
  Objective review ............................................................ 56

Objective 2.3: Configure mobility options .............................. 57
  Configure offline file policies ......................................... 58
  Configure sync options .................................................. 59
  Configure power policies ............................................... 60
  Configure Windows To Go ............................................. 63
  Configure Wi-Fi Direct ................................................... 65
  Objective summary ......................................................... 66
  Objective review ............................................................ 67
Objective 2.4: Configure security for mobile devices ................. 68
  Configure BitLocker 68
  Configure startup key storage 72
Objective summary 73
Objective review 73

Answers .......................................................... 75
  Objective 2.1: Thought experiment 75
  Objective 2.1: Review 75
  Objective 2.2: Thought experiment 76
  Objective 2.2: Review 76
  Objective 2.3: Thought experiment 77
  Objective 2.3: Review 77
  Objective 2.4: Thought experiment 78
  Objective 2.4: Review 78

Chapter 3  Plan and implement a Microsoft Intune device management solution  81

Objective 3.1: Support mobile devices .............................. 81
  Support mobile access and data synchronization 82
  Supporting mobile access with Sync Center 83
  Support broadband connectivity 84
  Support Mobile Device Management 85
Objective summary 88
Objective review 88

Objective 3.2: Deploy software by using Microsoft Intune ............ 89
  Use reports and In-Console Monitoring to identify required updates 89
  Approve or decline updates 92
  Configure automatic approval settings 93
  Deploy third-party updates 95
Objective summary 96
Objective review 96
Chapter 4  Configure networking  119

Objective 4.1: Configure IP settings  119
   Connect to a network  119
   Configure name resolution  125
   Configure network locations  127
   Objective summary  130
   Objective review  130

Objective 4.2: Configure network settings  131
   Connect to a wireless network  131
   Manage preferred wireless networks  132
   Configure network adapters  133
   Configure location-aware printing  133
   Objective summary  135
   Objective review  136
### Objective 4.3: Configure and maintain network security

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

---

### Answers

- Objective 4.1: Thought experiment
- Objective 4.1: Review
- Objective 4.2: Thought experiment
- Objective 4.2: Review
- Objective 4.3: Thought experiment
- Objective 4.3: Review

---

### Chapter 5 Configure storage

- Objective 5.1: Support data storage
  - Distributed File System
  - Supporting Storage Spaces
  - Support OneDrive for Business
  - Objective summary
  - Objective review

- Objective 5.2: Support data security
  - Manage permissions including Sharing, NTFS and Dynamic Access Control
  - Troubleshooting Encrypting File System
  - Controlling access to removable media
  - Supporting BitLocker and BitLocker To Go
  - Understanding Microsoft BitLocker Administration and Monitoring
  - Objective summary
  - Objective review
Chapter 6  Manage data access and protection  199

Objective 6.1: Configure shared resources 199

Configure HomeGroup settings 200
Configure libraries 202
Configure shared folder permissions 205
Configure shared printers 210
Configure OneDrive 216
Objective summary 223
Objective review 224

Objective 6.2: Configure file and folder access 225

Encrypt files and folders by using Encrypting File System 225
Configure NTFS permissions 230
Configure disk quotas 238
Configure object access auditing 240
Configure authentication and authorization 244
Objective summary 250
Objective review 251

Answers 252

Objective 6.1: Thought experiment 252
Objective 6.1: Review 252
Objective 6.2: Thought experiment 253
Objective 6.2: Review 254

Chapter 7  Manage Remote Access  255

Objective 7.1: Configure remote connections 255

Configure remote authentication 256
Configure VPN connections and authentication 256
Enable VPN Reconnect 262
Configure broadband tethering 263
Chapter 8  Manage apps  301

Objective 8.1: Deploy and manage Azure RemoteApp  .......... 301
  Configure RemoteApp and Desktop Connections settings  302
  Configure Group Policy Objects for signed packages  305
  Subscribe to the Azure RemoteApp and Desktop Connections feeds  305
  Support iOS and Android  306
  Configure Remote Desktop Web access for Azure RemoteApp distribution  306
  Objective summary  307
  Objective review  307

Objective 8.2: Support desktop apps  ......................... 308
  Support desktop app compatibility by using Application Compatibility Toolkit  308
  Support desktop application co-existence  313
  Install and configure User Experience Virtualization  319
  Deploy desktop apps by using Microsoft Intune  320
  Objective summary  323
  Objective review  324
<table>
<thead>
<tr>
<th>Chapter 9</th>
<th>Manage updates and recovery</th>
<th>329</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objective 9.1: Configure system recovery</td>
<td>329</td>
<td></td>
</tr>
<tr>
<td>Configure a recovery drive</td>
<td>330</td>
<td></td>
</tr>
<tr>
<td>Configure system restore</td>
<td>332</td>
<td></td>
</tr>
<tr>
<td>Perform a refresh or recycle</td>
<td>339</td>
<td></td>
</tr>
<tr>
<td>Perform a driver rollback</td>
<td>342</td>
<td></td>
</tr>
<tr>
<td>Configure restore points</td>
<td>344</td>
<td></td>
</tr>
<tr>
<td>Objective summary</td>
<td>350</td>
<td></td>
</tr>
<tr>
<td>Objective review</td>
<td>350</td>
<td></td>
</tr>
<tr>
<td>Objective 9.2: Configure file recovery</td>
<td>351</td>
<td></td>
</tr>
<tr>
<td>Configure File History</td>
<td>352</td>
<td></td>
</tr>
<tr>
<td>Restore previous versions of files and folders</td>
<td>355</td>
<td></td>
</tr>
<tr>
<td>Recover files from OneDrive</td>
<td>357</td>
<td></td>
</tr>
<tr>
<td>Objective summary</td>
<td>360</td>
<td></td>
</tr>
<tr>
<td>Objective review</td>
<td>361</td>
<td></td>
</tr>
<tr>
<td>Objective 9.3: Configure and manage updates</td>
<td>361</td>
<td></td>
</tr>
<tr>
<td>Configure update settings</td>
<td>362</td>
<td></td>
</tr>
<tr>
<td>Configure Windows Update policies</td>
<td>366</td>
<td></td>
</tr>
<tr>
<td>Manage update history</td>
<td>370</td>
<td></td>
</tr>
<tr>
<td>Roll back updates</td>
<td>372</td>
<td></td>
</tr>
<tr>
<td>Update Windows Store apps</td>
<td>376</td>
<td></td>
</tr>
<tr>
<td>Objective summary</td>
<td>379</td>
<td></td>
</tr>
<tr>
<td>Objective review</td>
<td>380</td>
<td></td>
</tr>
</tbody>
</table>

Answers .......................................................... 326
Objective 8.1: Thought experiment 326
Objective 8.1: Review 326
Objective 8.2: Thought experiment 326
Objective 8.2: Review 327
Answers…………………………………………………………………………………381
  Objective 9.1: Thought experiment 381
  Objective 9.1: Review 381
  Objective 9.2: Thought experiment 382
  Objective 9.2: Review 382
  Objective 9.3: Thought experiment 383
  Objective 9.3: Review 384

Index 385
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 actually perform tasks relating to the exam objectives.

Prior to taking the 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. We 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 as there are always new things to learn and fresh challenges to master.

This book covers every exam objective, but it does not cover every exam question. Only the Microsoft exam team has access to the exam questions themselves 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 links you’ll find in text to find more information and take the time to research and study the topic. Great information is available on MSDN, TechNet, and in blogs and forums.
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.

Acknowledgments

I would like to thank Karen Szall for the opportunity to write for Microsoft Press again, and Jason Kellington, my co-author for the valuable insights during the early stages of the writing process. This book is dedicated to Annette and Tommy, Annette has been a rock during the summer. Mwah!

-Andrew

Many thanks to Karen Szall and the great team at Microsoft Press, and to my co-author Andrew Bettany for your tireless work and preparation of this book. It has truly been a pleasure. To my wife and boys: The pages penned herein would not be possible without your support, patience, and love. Thank you.

-Jason

Free ebooks from Microsoft Press

From technical overviews to in-depth information on special topics, the free ebooks from Microsoft Press cover a wide range of topics. These ebooks are available in PDF, EPUB, and Mobi for Kindle formats, ready for you to download at:

http://aka.ms/mspressfree

Check back often to see what is new!
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:

   http://aka.ms/ER697/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.

   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.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

   http://aka.ms/tellpress

   The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in touch

Let’s keep the conversation going! We’re on Twitter: http://twitter.com/MicrosoftPress.
Preparing for the exam

Microsoft certification exams are a great way to build your resume and let the world know about your level of expertise. Certification exams validate your on-the-job experience and product knowledge. Although there is no substitute for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam. We recommend that you augment your exam preparation plan by using a combination of available study materials and courses. For example, you might use the Exam ref and another study guide for your “at home” preparation, and take a Microsoft Official Curriculum course for the classroom experience. Choose the combination that you think works best for you.

Note that this Exam Ref is based on publicly available information about the exam and the author’s experience. To safeguard the integrity of the exam, authors do not have access to the live exam.
This page intentionally left blank
Manage identity

Identity is an important concept in Windows, and the Manage Identity objective domain will test your understanding of how identities are managed in Windows to provide users with a consistent and secure environment. You’ll also need to know how to support Windows Store and Office 365 apps, install apps into images, and support authentication and permissions mechanisms in Windows.

Objectives in this chapter:
- Objective 1.1: Support Windows Store and cloud apps
- Objective 1.2: Support authentication and authorization

Objective 1.1: Support Windows Store and cloud apps

This objective covers supporting and installing apps from a variety of sources, including Windows Store, Microsoft Office 365, and Windows Intune. You’ll see how to use a Microsoft account to synchronize app and Windows settings across multiple devices. You’ll also see how to install apps into Windows Imaging Format (WIM) images, and manage the installation and availability of apps, including sideloading and deep linking.

This objective covers how to:
- Integrate Microsoft account and personalization settings
- Install and manage software with Microsoft Office 365 and Windows Store apps
- Sideload apps into online and offline images
- Sideload apps by using Microsoft Intune
- Deep link apps by using Microsoft Intune

Integrate Microsoft account and personalization settings

Using a Microsoft account with Windows 10 is the simplest and quickest way for users to maintain a consistent environment across multiple devices. Windows 10 can use a Microsoft account to save Personalization settings to the cloud and synchronize those settings across...
devices including PCs, laptops, tablets, and smartphones. In Windows 10, you can associate a Microsoft account with two separate account types:

- **Local account**  A local account is stored in the local Security Account Manager (SAM) database on a Windows 10 computer.

- **Domain account**  A domain account is stored in the Active Directory Domain Services (AD DS) database on a domain controller. Domain accounts can be used to authenticate a user on Windows computers joined to the domain.

A Microsoft account can provide settings synchronization across local and domain accounts. For example, a user might associate his Microsoft account with a local account on his home computer and a domain account at work. With this configuration, the user can have settings like Internet Explorer favorites or app configuration settings remain consistent regardless of which computer he is signed in to.

**Associating a Microsoft account with a local or domain account**

You can associate a Microsoft account with a local or domain account from the Your Account page in the Settings app.

![ACCOUNTS](image)

**FIGURE 1-1** The Your Account page in the Settings app

To associate a Microsoft account with a local Windows account, complete the following steps:

1. From the Desktop, click the Start button, and then click Settings.
2. In the Settings app, click Accounts.
3. In the left pane of the Accounts page, click Your Account.
4. In the Your Account page, click Sign In With A Microsoft Account Instead.
5. Enter your Microsoft account user name and password, and then click Signin.
6. You will be asked to verify your identity to be able to associate the account.
7. After verification, click Switch To Start Using Your Microsoft Account to sign in to Windows.

To associate a Microsoft account with a domain account, complete the following steps:

1. When logged in with a domain account, from the Desktop, click the Start button, and then click Settings.
2. In the Settings app, click Accounts.
3. On the Accounts page, click Your Account.
4. In the Your Account box, click Sign In With A Microsoft Account.
5. On the Connect To A Microsoft Account On This PC page, select the PC settings you want to sync with the domain, and then click Next. The options are:
   - Start Screen
   - App Data
   - Appearance
   - Language Preferences
   - Desktop Personalization
   - Ease Of Access
   - Apps
   - Other Windows Settings
   - Passwords
   - Web Browser
6. Enter your Microsoft account user name and password, and then click Next.
7. You will be asked to verify your identity to continue associating the account.
8. After verification, click Connect to associate your Microsoft account with your domain account.

**Configuring Microsoft account synchronization settings**

Users can change which items they opt to synchronize by using a Microsoft account. Users can access the options in the Settings app from the Sync Your Settings section of the Accounts page (see Figure 1-2).
Configuring Microsoft account settings by using Group Policy

Network administrators can incorporate Microsoft accounts into the workplace to help users transfer what they’ve configured with their domain accounts between computers by using a Microsoft account. Network administrators can also disable the ability to associate Microsoft accounts by setting limitations in Group Policy. This section looks at the Group Policy options for controlling the association of Microsoft accounts.

The Group Policy setting used to disable Microsoft account use is named Accounts: Block Microsoft Accounts, and the setting is found in Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options (see Figure 1-3). You can choose from three different settings:

- **The policy is disabled**  If you disable or do not configure this policy, users will be able to use Microsoft accounts with Windows.

- **Users can’t add Microsoft accounts**  If you select this option, users will not be able to create new Microsoft accounts on this computer, switch a local account to a Microsoft account, or connect a domain account to a Microsoft account. This is the preferred option if you need to limit the use of Microsoft accounts in your enterprise.

- **Users can’t add or log on with Microsoft accounts**  If you select this option, existing Microsoft account users will not be able to log on to Windows. Selecting this option might make it impossible for an existing administrator on this computer to log on and manage the system.
Install and manage software

While you can install apps using conventional methods, such as choosing Add/Remove Programs in Control Panel, or removable media, you can also perform cloud-based software installation by using Windows Store or Microsoft Office 365.

Installing apps by using Microsoft Office 365

Microsoft Office 365 is Microsoft Office in the cloud, accessible via a user-based paid subscription. Because it’s cloud-based, users can access the Microsoft Office products that are licensed to them on up to five compatible devices.

Office 365 updates are applied automatically. There’s no need for software maintenance tasks, such as installing updates or upgrading versions, so enterprise administrators don’t need to worry about updating devices manually. However, they’re still in control of updates and can decide how and when these will be provided to users. Administrators can also decide where users’ data should be stored: on the on-premises data servers of a company, in private cloud-based storage, in the public cloud, or a combination of these.

Office 365 is software as a service (SaaS). With SaaS, the user is provided a software product that they can use and consume, on demand. An organization might choose a SaaS product like Office 365 to reduce maintenance and installation workloads, reduce licensing costs, or simplify the organization software portfolio. SaaS products like Office 365 also offer the benefit of access to apps and saved documents from any location or computer, provided an Internet connection is available.
MORE INFO  EXPLORING OFFICE 365
This Exam Ref focuses on installing Office 365 components. However, there is much more to Office 365, including conferencing, email, secure file sharing, and website hosting. You can learn more about Office 365 at https://products.office.com/en-ca/business/explore-office-365-for-business.

CONFIGURING OFFICE 365
You can obtain a free trial subscription to Office 365 Business Premium by visiting the following link: https://portal.office.com/SSignup?OfferId=467eb54-127b-42d3-b046-3844b860bief&dl=O365_BUSINESS_PREMIUM&culture=en-US&country=US&ali=1&olo=1&lc=1033#0. After signing up, you can perform the initial configuration steps on the Office 365 Admin Center page, pictured in Figure 1-4.

FIGURE 1-4  The Office 365 Admin Center page

After signing up, you can access the Office 365 Admin Center at https://portal.microsoftonline.com/admin/default.aspx.

INSTALLING OFFICE FROM THE OFFICE 365 PORTAL
You can configure several settings that control the ability to install Office apps from Office 365 Admin Center. From the User Software page under Service Settings in Office 365 Admin Center, you can select the applications that you will enable users to install, one of the options being Office And Skype For Business. If this option is selected, users can install Office on their computers by completing the following steps:

1. Open a web browser and navigate to https://portal.microsoftonline.
2. Sign in with the appropriate user name and password.
3. From the Office 365 portal page, click Install Now.
4. Click Run to start the installation, click Yes to continue, and click Next to start the wizard.
5. Select No Thanks to not send updates to Microsoft, and then click Accept.
6. Click Next on the Meet OneDrive page.
7. Click Next to accept defaults, select No Thanks, and then click All Done.

DEPLOYING OFFICE
You can also deploy Office in the enterprise using methods other than the self-service method explained above. The Office Deployment tool enables you to configure information about which language(s) to download, which architecture to use, where the software deployment network share is located, how updates are applied after Office is installed, and which version of the software to install. Deployment methods include Group Policy, startup scripts, or Microsoft System Center Configuration Manager.

Managing software by using Office 365
You can manage all aspects of the Office 365 environment from Office 365 Admin Center. The admin center contains configuration and management pages for all the different features that affect Office app installation:

- **Dashboard**  This page provides a view of overall service health, including Office-related components. It also contains shortcuts to administrative tasks, such as Reset User Passwords and Add New Users.
- **Users**  From this page, you can add, remove, and edit user accounts that are part of the Office 365 environment. You can also configure Active Directory synchronization and configure authentication methods and requirements.
- **Domains**  From this page, you can manage and add domains used by Office 365.
- **Service Settings**  There are several pages available under the Service Settings menu, including Updates, User Software, Passwords, Rights Management, and Mobile.
- **Tools**  This page includes several important configuration and readiness tools for Office, including:
  - Office 365 health, readiness, and connectivity checks
  - Office 365 Best Practices Analyzer
  - Microsoft Connectivity Analyzer

IMPORTANT OFFICE 365 FEATURES
There are other important features of Office 365 that you need to consider in preparation for the exam. While these topics are not covered in great detail, they might appear as supporting information for a scenario or question on the exam.

- **Click-to-Run**  You can configure a click-to-run installation of Office that enables a streamed installation process, which gives almost instant access to Office desktop ap-
lications, rather than the traditional installation method that requires the user to wait for the entire installation process to complete before using any Office applications.


### Installing apps by using the Windows Store

The Windows Store is the standard source for Windows 10 apps, and the most common method for installing those apps. The Windows Store is installed by default on all Windows 10 computers.

There are several aspects of the Windows Store that you need to be aware of for the exam:

- The Windows Store is the primary repository and source for apps that are created and made available to the public, as a free trial or paid app.
- Users must have a Microsoft account associated with their local or domain account in order to download any apps from the Windows Store.
- Windows Store apps designed for Windows 10 are universal apps. They will function on Windows 10 computers, tablets, and mobile phones or smart devices, as well as Xbox.
- Windows Store apps are limited to 10 devices per Microsoft account. A user can install an app on up to 10 devices that are associated with his or her Microsoft account.
- Apps designed for non-public use—that is, for a specific organization—can be submitted through the Windows Store and be made available only to members of the organization.
MORE INFO  WINDOWS STORE APPS VS. WINDOWS DESKTOP APPS

This objective domain covers only Windows Store apps. Desktop apps, which appear and behave much like traditional Windows programs, are covered in Chapter 8.

To install a Windows Store app, open the Windows Store while logged in to Windows with a Microsoft account. You can navigate the Windows Store by browsing the categories provided at the top of the window, or by using the Search toolbar, also at the top of the window. After you’ve located the app you want to install, click Install on the app page. The app installs in the background, and you are notified when the installation is complete. Installed apps are available from the Start menu, by clicking All Apps, or by typing the name of the app in the Search field. You can also pin apps to the Start menu or taskbar to make them easier to access.

DISABLING ACCESS TO THE WINDOWS STORE

By default, the Windows Store is accessible to all users who have a Microsoft account associated with their local or domain account. Access to the Windows Store can be disabled by using Group Policy. You might disable access for a number of reasons, including controlling apps that are available on certain computers, such as kiosk or terminal computers, satisfying legal or compliance-related requirements, or ensuring that only approved applications of your organization are installed on Windows computers.

To disable access to the Windows Store, open either the Local Group Policy Editor, or Group Policy Management on a domain controller for domain policy. Within Group Policy, navigate to the following location: Computer Configuration\Administrative Templates\Windows Components\App Package Deployment. Change the setting for Allow All Trusted Apps To Install to Disabled.

EXAM TIP

Changes to Group Policy do not take place until a Group Policy refresh occurs. By default, this is every 90 minutes. To force a refresh, you can run gpupdate /force from the command prompt.

Sideload apps into offline and online images

Organizations sometimes create their own apps. These apps have the same characteristics as the apps you find in the Windows Store (which aren’t desktop apps). As noted earlier, enterprise administrators can make these apps available publicly if they want to go through the Windows Store certification process, or they can make them available to their enterprise users through a process known as sideloading.
Enabling sideloading in Windows 10

By default, the sideloading option in Windows 10 is disabled. To enable sideloading, you need to use a Group Policy setting. To configure Group Policy so that computers can accept and install sideloaded apps that you created for your organization, navigate to Computer Configuration/ Administrative Templates/ Windows Components/ App Package Deployment. Double-click Allow All Trusted Apps To Install. When this setting is enabled, any line of business (LOB) Windows Store app, signed by a Certification Authority (CA) that the computer trusts, can be installed.

FIGURE 1-6 Group Policy setting Allow All Trusted Apps To Install

Sideloading an app

After sideloading is enabled in Group Policy, you can sideload the app using the AppX Windows PowerShell module and the associated cmdlets. To manually sideload an app for the currently logged in user, perform the following steps from a Windows PowerShell prompt:

1. Type `Import-module appx`. Press Enter.

2. Type `Add-appxpackage “path and name of the app”` to add the app. Press Enter. Table 1-1 shows the available AppX cmdlets. If you need to add app dependencies, the command should look more like this: `Add-appxpackage C:\MyApp.appx DependencyPath C:\appplus.appx`.

The app installs, and then is available to the user. This needs to be done for each user if multiple users share a single computer.
EXAM TIP

Some exam questions require you to solve a problem with more than one Windows component or tool. For example, you might be asked how you would deploy an app to all client computers in a domain and configure the app to access network resources. The answer will likely include applying a specific Group Policy Object (Allow All Trusted Apps To Install) and using a Windows PowerShell cmdlet (such as add-appxpackage).

The AppX module for Windows PowerShell includes several cmdlets that you can use to install and manage LOB Windows Store apps.

**Table 1-1** Cmdlets in the AppX module for Windows PowerShell

<table>
<thead>
<tr>
<th>Cmdlet</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add-AppxPackage</td>
<td>To add a signed app package to a single user account</td>
</tr>
<tr>
<td>Get-AppxLastError</td>
<td>To review the last error reported in the app package installation logs</td>
</tr>
<tr>
<td>Get-AppxLog</td>
<td>To review the app package installation log</td>
</tr>
<tr>
<td>Get-AppxPackage</td>
<td>To view a list of the app packages installed for a user profile</td>
</tr>
<tr>
<td>Get-AppxPackageManifest</td>
<td>To read the manifest of an app package</td>
</tr>
<tr>
<td>Remove-AppxPackage</td>
<td>To remove an app package from a user account</td>
</tr>
</tbody>
</table>

If you want to sideload the apps to multiple computers, use Deployment Image Servicing and Management (DISM) cmdlets. You can use DISM commands to manage app packages in a Windows image. When you use DISM to provision app packages, those packages are added to a Windows image, and are installed for the desired users when they next log on to their computers.

You need to be familiar with the DISM syntax when servicing a Windows image, whether a computer is offline or online. Table 1-2 lists a few cmdlets to keep in mind.

**Table 1-2** Cmdlets in the AppX module for Windows PowerShell

<table>
<thead>
<tr>
<th>Cmdlet</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISM.exe /Image:&lt;path_to_image_directory&gt; [/Online]</td>
<td>To service a Windows image with DISM</td>
</tr>
<tr>
<td>DISM.exe /Image:&lt;path_to_image_directory&gt; [/Get-ProvisionedAppxPackages</td>
<td>To service an app package (.appx or .appxbundle) for an offline image</td>
</tr>
<tr>
<td></td>
<td>/Add-ProvisionedAppxPackage</td>
</tr>
<tr>
<td>DISM.exe /Online [/Get-ProvisionedAppxPackages]</td>
<td>To service an app package (.appx or .appxbundle) for a running operating system</td>
</tr>
</tbody>
</table>
Other command-line service options include /Get-ProvisionedAppxPackages, /FolderPath, /PackagePath, /LicensePath, and /Add-ProvisionedAppxPackage. Becoming familiar with these is very important because you’ll likely be tested on them. You can learn about all available commands and options at http://technet.microsoft.com/en-US/library/HH824882.aspx. Review this article and make sure that you can make sense of commands you might come across, perhaps one that looks like:

Dism /Online /Add-ProvisionedAppxPackage /FolderPath:C:\Test\Apps\MyUnpackedApp / SkipLicense

Or it looks like this:

Dism /Image:C:\test\offline /Add-ProvisionedAppxPackage /FolderPath:c:\Test\Apps\MyUnpackedApp /CustomDataPath:c:\Test\Apps\CustomData.xml

Sideload apps by using Microsoft Intune
You can use Microsoft Intune to sideload apps via the cloud and make them available to any authorized, compatible device that’s connected to the Internet. The following list outlines the high-level steps that you need to complete to sideload an app using Microsoft Intune.

1. Add users and create groups, if applicable.
2. Upload the app to Microsoft Intune.
3. Choose the users, groups, computers, and devices that can download the app, and link them (user-to-device).
4. For the self-service model in this example, choose how to deploy the app. It can be available, or available and required.
5. Verify that the app is available in the Windows Intune Company Store, and use the Company Store to install the app on devices.

Adding a user and groups
You can add users and groups to assist you in deploying your app to the appropriate audience. In Figure 1-7, you can see the Groups page, where new users and groups can be added to Intune. If you are adding users to a group, the group must be created before the user can be added to the group.
Objective 1.1: Support Windows Store and cloud apps

CHAPTER 1

 FIGURE 1-7 The Microsoft Intune Groups page

Uploading an app to Microsoft Intune

You can upload an app from the Apps page of Microsoft Intune, as shown in Figure 1-8.

 FIGURE 1-8 Uploading to the Microsoft Intune Apps page

To upload an app, complete the following steps:

1. On the Apps page, click Add Apps.
2. In the software setup window, select Windows app package as the software installer file type.
3. Click Browse, locate the .appx or .appxbundle file to upload, and then click Open.
4. Fill out the description information for the app.
5. Specify the architecture requirements.
6. Specify any rules to deal with previously installed apps.
7. Click Upload to upload the app to Microsoft Intune.

Once uploaded, the app will be available within the administration console to assign to users or groups (see Figure 1-9).

**FIGURE 1-9** Available apps on the Apps page in the Microsoft Intune console

**Choosing the users who can install the app**

You can choose the users to whom the app is made available by selecting Manage Deployment on the Apps page, as shown in Figure 1-9. When you start the Manage Deployment Wizard, you will be prompted to choose one or more groups to which the app is assigned, as in Figure 1-10. You can choose to assign the apps to users or computers. You need to also choose the Deployment Action for the app, although there is only one option available for each group type. For computer groups, you need to choose Required Install, and for user groups, you need to choose Available Install. Once you’ve chosen your options, you can click Finish to complete the group assignment process.
Installing the app from the Company Store

To install the app, your users will navigate to the Company Store page, and select the app from the Company Store page.

Deep link apps using Microsoft Intune

You can make Windows Store apps available to Windows RT users in your company portal by using Windows Intune as well as Configuration Manager. This section focuses on Windows Intune. You'll follow the same basic process as you did when deploying an app via the Installed Software option, but this time you choose External Link in the Add Software Wizard. Before you begin, decide which Windows Store app you want to deploy. For this example, choose OneDrive for Business.

The first part of the process requires you to obtain the link to the app you want to add to your company portal. To obtain the link for OneDrive for Business, follow these steps:

1. From the Start menu, type **Store**, and then click Store.
2. Search for Word Mobile, and then click it to access the installation page.
3. On the Word Mobile page, click Share.
4. In the Share area, click Mail.
5. The email contains the link. Send this link to yourself, copy the link, and paste it into Notepad, or otherwise make the link accessible for later.

The second part of the deep-linking process involves adding the app to Windows Intune:

1. Log on to the Microsoft Intune Administrator console.
2. Click the Apps tab, and then click Add Apps.
3. Wait for the Microsoft Intune Software Publisher to install, and then enter your Microsoft Intune credentials.
4. In the Microsoft Intune Software Publisher window, click Next.
5. On the Software setup page, select External link, and then type the link you copied in step 5 of the previous task into the URL field, and then click Next.
6. Carefully input the information to describe the software. What you input can be viewed by your employees. Click Next when finished.
7. Verify that the information is correct, and then click Upload.
8. After the upload is complete, click Close.

**Thought experiment**

**Managing Microsoft Office in a small organization**

In this thought experiment, apply what you’ve learned about this objective. You can find answers to these questions in the “Answers” section at the end of this chapter.

You manage a small business that has seven employees, and each employee has multiple devices that they use to perform work. You don’t have an Active Directory domain. Sometimes the users are at the company, sometimes at home, and often in a hotel. Users don’t always have Internet access.

Users complain that they can’t always access their work documents and that when they use Microsoft Office on their devices, they get a different user experience on all of them. Their settings and preferences need to be reset repeatedly for each device as they change them. You want to resolve these problems (and others, including mandating Microsoft Office updates), but you don’t have a lot of money to spend.

1. What should you set up to resolve all these issues, all without incurring a substantial expense?
2. Where would you store the users’ data?
3. If you want to delegate some of the responsibilities for managing your solution, what types of administrator would you create to manage support tickets?

**Objective summary**

- You can integrate users’ Microsoft accounts into your organization to enable synchronization of settings between multiple devices.
- You can manage apps by using Office 365, DISM, and Microsoft Intune.
- You can configure Group Policy to manage apps, manage access to the Windows Store, and enable sideloading.
- You can sideload apps to enable LOB apps without making them available through the Windows Store.
Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the “Answers” section at the end of this chapter.

1. Where can you configure a Group Policy that restricts the use of Microsoft accounts for a specific group of users in an Active Directory domain?
   A. In the Group Policy Management Editor window, by expanding Computer Configuration/ Policies/ Windows Settings/ Security Settings/ Local Policies/ Security Options
   B. In the Group Policy Management Editor window, by expanding Computer Configuration/ Policies/ Windows Settings/ Security Settings/ Local Policies/ User Rights Assignment
   C. In the Local Group Policy Editor, by navigating to Computer Configuration/ Windows Settings/ Security Settings/ Local Policies/ Security Options
   D. In the Local Group Policy Editor, by navigating to Computer Configuration/ Windows Settings/ Security Settings/ Local Policies/ User Rights Assignment

2. Where can users associate a Microsoft account with a domain account?
   A. Users can’t do this. Only administrators can perform this task in Active Directory Users And Computers on a domain controller.
   B. In the Settings app, on the Accounts page
   C. In the Group Policy Management Editor by expanding Computer Configuration/ Policies/ Windows Settings/ Local Policies/ Security
   D. In the Settings app, on the Personalization page.

3. Which of the following can you manage in the Office 365 Admin Center?
   A. Active Directory synchronization
   B. Valid, expired, and assigned licenses
   C. User password, including resetting
   D. All of the above
   E. B and C only

4. Which of the following tools and technologies can help you sideload LOB apps for computers in your organization?
   A. DISM
   B. Windows PowerShell
   C. Configuration Manager
   D. Microsoft Intune
   E. All of the above
   F. Only C and D
5. Which Group Policy setting do you have to enable before you can sideload apps in Windows 10?
   A. None
   B. Allow All Trusted Apps To Install
   C. Allow Development Of Windows Store Apps
   D. Block Microsoft Accounts

6. True or false: You can create a required installation for an app in Microsoft Intune, which will automatically install on devices.
   A. True
   B. False

7. Which of the following describes the purpose of deep linking an app?
   A. To make specific Windows Store apps available through the company portal
   B. To force the installation of apps on Windows 10 computers
   C. To add LOB apps to the Windows Store
   D. None of the Above

Objective 1.2: Support authentication and authorization

Users need to be authenticated to access a computer or network before they can be authorized to access the resources on it. Windows 10 supports several authentication mechanisms and methods, and different ways to manage accounts. This chapter will help you to understand the important concepts needed to support Windows 10 authentication and authorization.

This objective covers how to:
- Support user authentication, including multi-factor authentication, certificates, virtual smart cards, picture passwords, and biometrics
- Support workgroup, homegroup, and domain membership, including Secure Channel, account policies, credential caching, and Credential Manager
- Know when to use a local account versus a Microsoft account
- Configure Workplace Join
- Configure Windows Hello
Support user authentication
User authentication can come in many forms in Windows 10. You need to understand the various methods for authentication as well as the different mechanisms for managing and supporting authentication.

Understanding multi-factor authentication
Multifactor authentication requires two (or more) types of authentication to gain access to a device or network. Most often, one type is a password, and the other is something else, such as a smart card, fingerprint, or digital certificate. This section focuses a little more on certificates as a means of achieving authentication, but this book has covered this topic in various places, and you need to review those entries when you can (for the most part, certificates have been associated with apps, because apps must be signed to ensure that they can be trusted).

A digital certificate is issued by a Certificate Authority (CA), such as Verisign or Active Directory Certificate Services (AD CS) in Windows Server 2012 R2. The certificate can be used to provide proof that the identity asking for authentication is trusted and true, and that the identity offering it is also trusted and authentic. Authentication with certificates involves a public key and a private key that can be matched to provide that authentication. If no match occurs, no authentication is provided. You can learn more about Certificate Authorities at http://technet.microsoft.com/en-us/library/cc732368.aspx.

AD CS can issue and manage public key infrastructure (PKI) in a domain, provide public key cryptography and the ability to create digital certificates, and offer digital signature capabilities. For the purposes here, AD CS provides authentication by associating certificate keys with computers, users, and device accounts on a network. This is called binding.

For the exam, you might be asked how to enable users to access a network resource and be given a specific scenario. A scenario that includes AD CS will note that the network has its own PKI infrastructure. You need to understand that the required certificates must be available to the computer and the user, and they need to be stored in the proper location for authentication to be granted. Client certificates are stored in the Personal certificate store for the applicable user account on the client computer. Computer accounts need trusted root certificates to be stored in the Trusted Root Certification Authorities store, again on the client computer.

You can explore many other certificate folders as well. To view these stores on a local computer, type certmgr.msc in a Run dialog box, and click OK. Open this console and review the available certificate folders before moving on. Figure 1-11 shows a local computer, not connected to a domain, and the related Personal certificates. Typically, you’ll see more certificates than those present in the example.
Understanding virtual smart cards

A virtual smart card works in the same general manner as a physical smart card does, but doesn’t require a connected or installed smart card reader. Instead, the virtual smart card works with a Trusted Platform Module (TPM) chip, which protects the virtual card information through encryption, installed on the computer. As with other more advanced security options, you’ll need a PKI domain infrastructure, complete with certificates and the ability to create and manage them, to incorporate this technology. Virtual smart cards offer the following:

- Authentication protection
- Confidentiality of the machine and its contents
- Private keys for security
- Encrypted card information that can’t be mined or removed (that is, it can’t be exported)
- Protection from rogue software that attacks at startup
- Multi-factor protection (smart card and PIN)

To use virtual smart cards, you need to meet more requirements than when you opt to use physical ones. These requirements include, but aren’t limited to the following:

- Computers must be running Windows 8 or higher and Windows Server 2012 or higher.
- A compatible TPM must be installed on those computers that adhere to TPM 1.2 or higher standards.
- A limit of ten smart cards (virtual or physical) can be used on a single computer.
The PIN and the PIN Unlock Key must be a minimum of eight characters. These can include numbers, letters, and special characters.

One very important command that you need to understand for the exam is Tpmvscmgr.exe, the command-line tool you use to configure a virtual smart card. You can use the command locally or remotely. Parameters you can use include Create and Delete. Examples include /name (the name of the smart card), /admin key (administrator key), /PIN (the PIN), /generate (to create the files in storage necessary for the card to function), and others listed at http://technet.microsoft.com/en-us/library/dn593707.aspx.

To configure a virtual smart card environment from scratch in a domain, you need to follow these steps:


   tpmvscmgr.exe create /name tpmvsc /pin default /adminkey random /generate


   MORE INFO VIRTUAL SMART CARDS

   Learn more about virtual smart cards and be sure to explore the additional links on the left side of this page at http://technet.microsoft.com/en-us/library/dn593708.aspx.

   To configure a Windows 10 virtual smart card on a stand-alone computer if you have the required technology and credentials available, follow these steps:

1. Open an elevated command prompt.

2. Type tpm.msc.

3. Verify that a compatible TPM can be found that’s at least a TPM 1.2 or later. If you receive an error instead, but are sure a compatible module is available, enable it in the system BIOS before continuing.

4. Close the TPM management console.

5. At the command prompt, enter:

   TpmVscMgr create /name MyVSC /pin default /adminkey random /generate

   To provide a custom PIN value when creating the virtual smart card, use /pin prompt instead.
Configuring a picture password

A picture password is a way to log on to a computer by using a series of three movements consisting of lines, circles, and/or taps. You can pick any picture you want. Picture passwords can’t be used to log on to domains; they are used to log on to stand-alone computers only. Picture password combinations are limitless because the pictures that can be used are limitless. Although picture passwords are considered more secure for stand-alone computers than typing a PIN or password, a hacker can get into a device by holding the screen up to light to see where most of the gestures are (by following the smudges on the screen). This is especially true if the user touches the screen only to input the password and rarely uses touch for anything else.

You create a picture password (or a four-digit PIN) from the Settings app:

1. Open the Settings app, and then click Accounts.
2. Click Sign-in Options.
3. Under Picture Password, click Add.
4. Input your current password, and then click Choose Picture to browse to and select the picture to use.
5. Follow the instructions in the resulting wizard to configure the picture password.

Exploring biometrics

Biometrics, like picture passwords, provides infinite possibilities for securing a computer and can be used as part of a multi-factor authentication plan (using it on its own isn’t recommended). Biometric options are generally configured by incorporating a person’s fingerprint and using a fingerprint reader (you “enroll” the user when configuring this), but you can also use a person’s face, eye, or even their voice.

Microsoft has made using biometrics easier than ever by including native support for biometrics through the Windows Biometric Framework (WBF), which includes an option in the Settings app for configuring the device on Windows 10 computers. Windows now also includes Group Policy settings related to biometrics, and you can enable or disable this feature as desired. You need to review the information at http://technet.microsoft.com/en-us/library/dn344916.aspx, and locate the available Group Policy settings, just in case. You can find Local Group Policy options here (and follow the same general path in Group Policy): Computer Configuration/ Administrative Templates/ Windows Components/ Biometrics/, as shown in Figure 1-12.
Support workgroup, homegroup, and domain membership

In this section, you'll review the differences between some similar technologies and network configurations, such as workgroup versus homegroup, workgroup versus domain, and credential caching versus Credential Manager.

Homegroups, workgroups, and domains

In almost all instances and scenarios, using a computer to complete tasks involves connecting to a network of some sort, even if it’s just to access the Internet or to back up your work someplace other than your own PC. In homes, networked computers are often configured as homegroups. In a small business, the configuration is generally a workgroup. The purpose of both of these types of networks is frequently to share an Internet connection as well as files, folders, printers, and other resources. Domains are used in larger enterprises, which require more control and good protection of resource access. Domains are the only one of these three that employ AD DS to manage users, computers, and resources.

UNDERSTANDING HOMEGROUPS

A homegroup lets home users easily share documents, printers, and media with others on their private local network. This is the simplest kind of network sharing and is limited in what permissions and restrictions can be placed on the data shared. By default, all users that join a homegroup (only one per network) have read-only access to what’s already shared by others. Users can reconfigure this, however, enabling both read and write access, if desired. When opting for a homegroup, users can:

- Create or join a homegroup from the prompt offered by Windows, assuming the network is configured as Private.
Create or join a homegroup from the Network And Sharing Center, assuming the computers that want to join are running Windows 7, Windows 8, or Windows 10. Work through the applicable homegroup wizard to create or join a homegroup. Windows generates a random password other users will need to use to join.

- Share files from their original locations and their default libraries.
- Grant read-only or read/write access to the data they’ve shared.
- Limit access to only those network users who also have an account and password on their computers.
- Configure the same permissions for all network users, or set different permissions for individual users.

**MORE INFO UNABLE TO CREATE A HOMEGROUP?**

Creating a homegroup requires IPv6 to be installed on all of the computers in the homegroup. Computers within a homegroup must also be within 5 minutes of each other’s system time in order for the homegroup to function properly. If you have problems with a homegroup, check for these two potential issues.

Because you can create and join a homegroup using a wizard, detailing the steps in this text isn’t really necessary. However, you need to create a homegroup on your own local network and let other computers join it, just so that you are familiar with the process. Note that users might already be joined to a homegroup because Windows detects and will prompt you to join existing homegroups automatically during setup.

**Understanding workgroups**

In businesses where a little more control is required and a homegroup isn’t the ideal configuration, a workgroup is used. A workgroup is a manual grouping of computers (almost any operating system will do, including Windows RT) that doesn’t include an Active Directory domain controller, but still offers security options. A workgroup exists on a single network segment. Securing data here is a distributed concept similar to a homegroup; each user decides what to share, how to share it, and with whom to share. Note that Windows doesn’t create a password for joining the workgroup, nothing is shared automatically by default (except possibly the Public folders), and users join the workgroup from the System Properties dialog box under the Computer Name tab (see Figure 1-13). Click Change in the System Properties dialog box, and then enter the workgroup name in the Computer Name/Domain Changes dialog box.
Because this section is about authorization, you need to consider that concept with regard to a workgroup. Users decide what to share, and then share it. The person who wants access to shared items must have an account on the sharing computer (or be given one). Accounts are stored in the Security Account Manager (SAM) database in the sharing computer. Because each computer maintains its own local database, users who need to access resources on multiple workgroup computers must be authenticated on each. The problem with this is that as the network grows, so does the amount of work required to maintain and manage these accounts.

Here is an overview of how authorization works:

1. The first time a user tries to access a shared resource, he or she is asked for a user name and password.
2. The user name and password that are entered must be from an approved account on the sharing computer and must be listed in the SAM database. The user can opt to have Windows remember the password for the next time.
3. The Local Security Authority (LSA) looks to the SAM database to see whether the account that was entered is valid.
4. If the account is valid, the user is granted access.
5. The same user who wants to access another shared resource on the same computer during the same session can do so without re-entering the password.
6. If this same user wants to access a shared resource on another computer in the workgroup, the process must be repeated.
UNDERSTANDING DOMAINS

Companies and enterprises configure networks as domains. You couldn’t successfully manage 100 computers by using a homegroup or workgroup, so a domain is an obvious choice for enterprise networks.

Domains are configured with at least one AD DS domain controller that authenticates users centrally and secures network resources. These larger networks can contain additional servers that manage data storage, email, faxes, and printers; maintain database replications, and so on. Managing all resources as a whole is important to keeping everything secure and available for users, and enables a simpler management solution for administrators. A large enterprise can have more than one domain. When multiple domains exist, a Global Catalog is used to locate objects in other domains. Authentication in a domain is handled by AD DS, a database that contains objects, such as user accounts, computers, groups, and so on. In this case, a network administrator creates user accounts, almost always puts those accounts into groups, and then assigns the desired permissions to the group. This makes managing users simpler than trying to manage users one at a time, and it enables administrators to deal with newly hired or recently fired employees. The authentication process includes and uses the Kerberos v5 authentication protocol to identify the user or the host. The Kerberos Key Distribution Center (KDC) uses the domain-specific AD DS as its security account database. AD DS is required for default Kerberos implementations within the domain or forest. If you aren’t familiar with Kerberos v5, the TechNet article “Kerberos Authentication Overview” at http://technet.microsoft.com/en-us/library/hh831553.aspx provides a good explanation of how this works and offers links to additional resources.

UNDERSTANDING COMPUTER AND USER AUTHENTICATION

The previous section discusses AD DS and authentication with regard to user accounts. Network administrators create these accounts, users input their account credentials to log on to the domain, and authentication is handled by the applicable AD DS server and Kerberos v5. Computers that join domains acquire a computer account automatically. Like user accounts, computer accounts are used to authenticate the computer to enable it to access network and domain resources. Each computer account must be unique. A user doesn’t have to do anything to cause the computer to be authenticated. Note that computers have passwords that are automatically managed, and if a computer password on a client is out of sync with AD DS, then the computer can’t authenticate.

Computer accounts are necessary for auditing, for control, and for grouping purposes. You can apply changes to computer accounts that affect whoever logs on to the computer, and not the individual users. For instance, you can force policies regarding the desktop appearance, how updates are applied, and so on, and those policies will affect the computer and anyone who uses it.

Administrators can manage computer accounts in the same way they can user accounts—by adding, deleting, resetting, and disabling them in the Active Directory Users And Computers snap-in.
UNDERSTANDING SECURE CHANNEL

When applications need network or Internet access, you have to ensure that the connection is secure. This is especially true if you are transmitting data over an untrusted network. You can use Transport Layer Security (TLS)/Secure Sockets Layer (SSL) security to authenticate servers and client computers, and then use that to encrypt messages between them. These two protocols are included in the Secure Channel set of security protocols. TLS and SSL aren’t interchangeable and SSL is the predecessor to TLS, but both protect against tampering and eavesdropping.

Secure Channel can authenticate an identity as well as provide a secure and private connection to another host by using encryption. It’s also called Schannel and is mostly used for applications that require secure HTTP communications. Schannel is a Security Support Provider (SSP), and the TLS/SSL protocol uses a client/server model that’s based on certificate authentication. This means you need to also have a PKI configured and available.

MORE INFO DISCOVERING SECURE CHANNEL


EXPLORING ACCOUNT POLICIES

The weakest link when protecting computers that use a password as part of the authentication process is most often the password itself. The password could be nonexistent (not likely, especially with the advent of the Microsoft account for stand-alone computers), too short, too simple, too predictable, or the user might simply never change it. Often, users create and use the same password for multiple user IDs. This is a secondary weak link. To protect authentication in both workgroups and domains, you can create local policies and Group Policy Objects (GPOs) defining how passwords should be created, how often they can or must be changed, and what happens when a user fails to log on after attempting a specific number of times that you set. You can configure account policies in the Local Security Policy for a stand-alone computer or for computers in a workgroup, and in Group Policy for domains. In Local Security Policy, Account Policies is listed first. Click Account Policies, and then click Account Lockout Policy to see the options.

You can configure three account lockout policies, and in most instances they must be configured together:

- **Account Lockout Duration** If you’ve configured an account lockout threshold and if that threshold is met, this setting defines how long (in minutes) the user will be locked out of the computer. A setting of 5 to 15 minutes is common.

- **Account Lockout Threshold** You need to configure this to use the other options. This setting defines how many times a user can try to log on to the computer and fail, before being locked out.
- **Reset Account Counter After**  This setting defines the number of minutes that must pass after a failed logon attempt before the failed logon attempt counter is reset to zero. If an account lockout threshold is defined, this must be less than or equal to the number of minutes set there.

**EXPLORING CREDENTIAL MANAGER**

Using user names and passwords is a common way to authenticate users. Windows 10 includes Credential Manager to help manage and maintain those passwords. Credential Manager saves the credentials that users enter when they use their own computers to access network servers and resources on local networks (Windows credentials), and can be used to back up and restore them. When prompted, users have to check the box Remember My Credentials, or else the credentials won’t be saved. Credential Manager also offers Credential Locker, which saves user names and passwords associated with websites and Windows apps (Web Credentials). It saves all of these in an area called the Windows Vault.

---

**NOTE  SAVING CREDENTIALS**

Credentials are saved in encrypted folders on the computer under the user’s profile. Applications that support this feature, such as web browsers and Windows apps, can automatically offer up the correct credentials to other computers and websites during the sign-in process.

If the user name or password has been changed since the last time it was saved and access is unsuccessful, the user is prompted to type the new credentials. When access to the resource or website is successful, Credential Manager and Credential Locker overwrite what was there.

The saved user names and passwords follow users when they move from one computer to another in a workgroup or homegroup, presuming they log on with their Microsoft accounts. However, this feature isn’t enabled on domains for security reasons. You can open Credential Manager from Control Panel. Figure 1-14 shows Credential Manager.

Here are a few more points to understand about Credential Manager:

- You can program Windows Store apps to use Credential Locker.
- Credential roaming requires the Microsoft account for synchronization.
- Credential roaming is enabled by default on non-domain joined computers, and it is disabled on domain-joined computers.
- Credential Locker supports seamless sign in by using Windows Store apps that use Web Authentication Broker and remember passwords for services, such as Twitter and LinkedIn.
CHAPTER 1

Configure local accounts and Microsoft accounts

The Microsoft account enables users to sync settings to the cloud and to other computers that they log on to using that same Microsoft account. With a Microsoft account, users can also access their own cloud storage, called OneDrive. Windows 10 comes with the OneDrive app, which can be accessed from compatible applications, various web browsers, and File Explorer.

Users are prompted to create a Microsoft account when they set up their Windows 10-based computers. They can opt to do that, or they can decline and create a local account instead. A user might also create a local account if the computer can’t access the Internet during setup (because they can’t create or confirm the Microsoft account if no Internet access is available). Users generally opt to create a Microsoft account later, even if they start with a local account, because many apps are inaccessible if the user is logged on with a local account. Users also can’t get apps from the Store without a Microsoft account.

After a Microsoft account is created, users don’t need to be connected to the Internet to log on during subsequent sessions. The account information is cached locally. If an Internet connection isn’t available, the last saved settings are also applied because they are also cached locally. You can switch from a local account to a Microsoft account from the Settings app.

A Microsoft account can be used in a domain, if it isn’t restricted through Group Policy. If possible at your place of business, when connected, users will see the same desktop background, app settings, browser history, and so on that they see on their main computers at home (or in another office). Again, you can make the change through the Settings app. There, you’ll opt to connect your Microsoft account and work through the setup process.
Configure Workplace Join

Personal devices have become part of the enterprise landscape, and if you don’t already, at some point you need to be able to enable users to access network resources from them. This is how Workplace Join came about. Workplace Join enables users to have a single sign-on (SSO) experience and enables them to get to the resources they need. You can also manage and secure the devices. In Windows Server 2012 R2, you can use Workplace Join with Windows 8.1, Windows 10, and iOS devices.

Workplace Join uses the Device Registration Service (DRS), part of the Active Directory Federation Services (ADFS) role in Windows Server 2012 R2, to create a device object in AD DS and use a certificate to identify the device in the future. If you add Web Application Proxy, users can join your enterprise from any Internet-enabled location.

Various walkthrough guides are available on TechNet to help you use this technology to join devices. Here are two of those:


Configure Windows Hello

Windows Hello enables you to use a combination of optical recognition and fingerprint data to sign in to a Windows 10 computer, and authenticate to apps, enterprise content, and online authentication providers. Windows Hello is designed to be a user-friendly interface for configuring biometric authentication in Windows 10.

You can configure Windows Hello from the Settings app, in the Sign-in Options section of the Accounts page.
Thought experiment
Creating and configuring authentication solutions

In this thought experiment, apply what you’ve learned about this objective. You can find answers to these questions in the “Answers” section at the end of this chapter.

You’ve been asked to create and configure a multi-factor authentication solution that can be used to validate users in an enterprise domain. You’ve also been instructed to include digital certificates in that solution. Your client doesn’t want to rely on a third party CA, and instead wants to use the Active Directory Certificate Services (AD CS) in Windows Server 2012 R2. Answer the following questions regarding this task.

1. The network currently doesn’t include a PKI infrastructure. Will you need to add it?
2. Where will the client certificates you create be stored?
3. Where will the trusted root certificates you create be stored?
4. What command can you run, from a Run dialog box, on a client computer to view the certificates stored on that machine?

Objective summary

- Multi-factor authentication lets you further secure the authentication process with certificates, virtual smart cards, picture passwords, and biometrics, by requiring more than one method of authentication before access is granted.
- Different networks exist for different needs. Homegroups enable simple sharing for home networks; workgroups let you share and manage shared data in a non-domain setting; and domains are used by larger enterprises and include Active Directory Domain Services (AD DS) to secure and manage authentication.
- You can further secure authentication by including Secure Channel, account policies, credential caching, and Credential Manager to help control access and manage logon credentials.
- Local accounts are good for homegroups and workgroups, but now even those networks rely on Microsoft accounts for authorization management. Microsoft accounts can also be incorporated into domains to sync settings, such as desktop backgrounds.
- Workplace Join enables you to enroll and control mobile devices on your domain for the purpose of letting your users bring their own devices to work.
- Windows Hello enables configuration of facial and fingerprint recognition for use with the Windows 10 authentication process.
Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the “Answers” section at the end of this chapter.

1. Which two of the following Windows PowerShell commands can you use to manage a CA database?
   A. Backup-CARoleService
   B. Restore-CARoleService
   C. Backup-CACertStore
   D. Restore-CACertStore

2. Which two of the following technologies offer authentication protection, confidentiality of the machine and its contents, private keys for security, and encrypted card information that can’t be mined or removed?
   A. Physical smart card
   B. A compatible TPM chip
   C. Virtual smart card
   D. A biometric fingerprint reader
   E. BitLocker Drive Encryption

3. You create a homegroup on one computer and join it from another. This process goes smoothly. However, when you try to access data shared with the homegroup from the second computer, you can’t. What’s most likely the problem?
   A. You aren’t connected to the network.
   B. You aren’t using BitLocker Drive Encryption.
   C. The time is configured incorrectly on the second computer.
   D. You aren’t running a compatible version of Windows.

4. Which of the following network types is a distributed concept, in which users manage their own data sharing?
   A. Workgroup
   B. Homegroup
   C. Domain
   D. Workgroup or domain
5. You want to secure communications over an untrusted network for applications that need Internet access. You want to use TLS and SSL to achieve this. Which of the following technologies offers this? Must the solution include a PKI infrastructure?

A. VPN
B. Remote Desktop Services
C. Microsoft Application Virtualization (App-V)
D. Secure Channel

6. You are trying to configure Group Policy to set an account lockout duration when users try and fail to authenticate their computers after a specific number of events. The options are grayed out. Why?

A. You must first configure the policy Account Lockout Threshold.
B. You must first configure the policy Reset Account Counter After.
C. You are trying to configure the policy for a workgroup computer, but these policies are available only in domains.
D. You are in the Group Security Policy console, but need to be in the Group Policy Editor.

7. Can Credential Manager and Credential Locker be used to store passwords for Windows Store apps? Can Credential Manager and Credential Locker be used to store passwords saved for local network resources?

A. Yes
B. No
C. Yes
D. No

8. You want to enable your domain users to access the same desktop background, app settings, browser history, and so on that they see on their main computers at home (or in another office). What should you do?

A. A Microsoft account would be optimal, but can’t be used in a domain.
B. Let the users associate their Microsoft accounts with their domain accounts.
C. Use Workplace Join.
D. Incorporate a Web Application Proxy server into your network.
Answers

This section contains the solutions to the thought experiments and answers to the objective review questions in this chapter.

Objective 1.1: Thought experiment

1. Office 365
2. Most likely using the cloud, with options that enable the user to sync that data even when they aren’t online
3. Billing; Global; Password; Service; User Management

Objective 1.1: Review

1. Correct answer: A
   
   A. Correct: Options to restrict the use of Microsoft accounts for a group of users in a domain are in the Group Policy Management Editor window. Expand Computer Configuration/ Policies/ Windows Settings/ Security Settings/ Local Policies/ Security Options.

   B. Incorrect: The User Rights Assignment node doesn’t provide options for restricting Microsoft accounts.

   C. Incorrect: To restrict a group of users in an Active Directory domain, you need to access Group Policy, not Local Group Policy.

   D. Incorrect: To restrict a group of users in an Active Directory domain, you need to access Group Policy, not Local Group Policy. Also, User Rights doesn’t offer the options you need.

2. Correct answer: B
   
   A. Incorrect: Users can do this from their local computers.

   B. Correct: This is the correct answer; from their local computers, in the Settings app, from the Accounts page.

   C. Incorrect: You can’t connect a Microsoft account using Group Policy.

   D. Incorrect: This is achieved in the Settings app, but not from the Personalization page.

3. Correct answer: D
   
   A. Incorrect: Active Directory synchronization is one of the things you can manage in the Office 365 Admin Center, but others are correct here.

   B. Incorrect: Valid, expired, and assigned licenses are some of the things you can manage in the Office 365 Admin Center, but others are correct here.

   C. Incorrect: User passwords, including resetting, is one of the things you can manage in the Office 365 Admin Center, but others are correct here.
D. **Correct:** All of the above can be configured in the Office 365 Admin Center.
E. **Incorrect:** All the answers are correct, not just B and C.

4. **Correct answer:** E
   - A. **Incorrect:** DISM is only one of the correct options listed.
   - B. **Incorrect:** Windows PowerShell is only one of the correct options listed.
   - C. **Incorrect:** Configuration Manager is only one of the correct options listed.
   - D. **Incorrect:** Windows Intune is only one of the correct options listed.
   - E. **Correct:** All of the above
   - F. **Incorrect:** “Only C and D” isn’t correct because A and B are correct also.

5. **Correct answer:** B
   - A. **Incorrect:** Special Group Policies are required.
   - B. **Correct:** Allow All Trusted Apps To Install is the required Group Policy setting that must be enabled.
   - C. **Incorrect:** Allow Development Of Windows Store Apps isn’t the correct Group Policy setting to enable.
   - D. **Incorrect:** You should not block Microsoft accounts; you need to enable the Group Policy setting listed for answer B.

6. **Correct answer:** B
   - A. **Incorrect:** You cannot make sideloaded apps mandatory and force their installation on clients by applying the applicable settings in Windows Intune.
   - B. **Correct:** This statement is false.

7. **Correct answer:** A
   - A. **Correct:** You deep link apps to make Windows Store apps available through the company portal.
   - B. **Incorrect:** You do not use deep linking to force the installation of apps on Windows 10 computers.
   - C. **Incorrect:** You don’t use deep linking to add LOB apps to the Windows Store. It’s used to make Windows Store apps available through the company portal.
   - D. **Incorrect:** “None of the above” isn’t correct. A is correct.

**Objective 1.2: Thought experiment**

1. Yes. AC CS in Windows Server 2012 requires an existing PKI infrastructure.
2. Client certificates are stored in the Personal certificate store for the applicable user account on the client computer.
3. Trusted root certificates are stored in the Trusted Root Certification Authorities store on the client computer.
4. Certmgr.msc can be used to open the Certmgr window.
Objective 1.2: Review

1. **Correct answers:** A and B
   - A. **Correct:** Backup-CARoleService is the correct command for backing up the CA database.
   - B. **Correct:** Restore-CARoleService is the correct command for restoring the CA database.
   - C. **Incorrect:** This isn’t a valid Windows PowerShell command.
   - D. **Incorrect:** This isn’t a valid Windows PowerShell command.

2. **Correct answers:** B and C
   - A. **Incorrect:** A physical smart card can be removed.
   - B. **Correct:** The solution here requires a compatible TPM chip and a virtual smart card.
   - C. **Correct:** The solution here requires a compatible TPM chip and a virtual smart card.
   - D. **Incorrect:** A biometric fingerprint reader doesn’t offer private keys for security.
   - E. **Incorrect:** BitLocker Drive Encryption is used to protect data on the drive and isn’t for authentication purposes.

3. **Correct answer:** C
   - A. **Incorrect:** If you’ve joined the homegroup, you are connected to the network.
   - B. **Incorrect:** BitLocker Drive Encryption isn’t required to join a homegroup.
   - C. **Correct:** The time is configured incorrectly on the second computer.
   - D. **Incorrect:** If you have joined the homegroup, you are running a compatible version of Windows.

4. **Correct answers:** A and B
   - A. **Correct:** A workgroup uses a distributed method for sharing data.
   - B. **Correct:** A homegroup uses a distributed method for sharing data.
   - C. **Incorrect:** A domain uses a centralized method of sharing and managing data and uses AD DS for authentication and user access.
   - D. **Incorrect:** Although a workgroup is a distributed sharing method, a domain isn’t.
5. **Correct answer**: D
   A. **Incorrect**: A VPN enables users to access your local network when they are away from the office. VPNs might use PPTP or L2TP to secure the connection.
   B. **Incorrect**: Remote Desktop Services enables users to access session-based desktops, virtual machine-based desktops, or applications from both within a network and from the Internet.
   C. **Incorrect**: App-V enables the application to run in a virtualized environment without having to install or configure it on the local machine.
   D. **Correct**: Secure Channel is a Security Support Provider (SSP), and the TLS/SSL protocol uses a client/server model that's based on certificate authentication. It does require a PKI infrastructure.

6. **Correct answer**: A
   A. **Correct**: You need to first configure the policy Account Lockout Threshold to state how many times a user can try to authenticate before additional measures are taken.
   B. **Incorrect**: The policy Reset Account Counter After is optional.
   C. **Incorrect**: These policies are available in both workgroups and domains.
   D. **Incorrect**: The Group Security Policy console is the appropriate place to create these policies.

7. **Correct answer**: C
   A. **Incorrect**: Credential Manager can store Windows Store passwords as well as local ones.
   B. **Incorrect**: Credential Manager can store Windows Store passwords as well as those input for local resources.
   C. **Correct**: Credential Manager can store Windows Store passwords as well as passwords for local resources.
   D. **Incorrect**: Credential Manager can store both Windows Store passwords and local user passwords.

8. **Correct answer**: B
   A. **Incorrect**: A Microsoft account can be used in a domain if it isn’t restricted through Group Policy.
   B. **Correct**: Enable the user to associate their own Microsoft account to achieve this.
   C. **Incorrect**: Workplace Join enables users to connect to your domain with their own personal devices.
   D. **Incorrect**: If you add Web Application Proxy, users can join your enterprise from any Internet-enabled location by using a device you’ve allowed using Workplace Join.
This page intentionally left blank
Index

A

AAD. See Azure Active Directory (AAD)
access. See data access
access-based enumeration (ABE) 209–210
Access Control Entries (ACEs) 173, 207, 231
Access Control List (ACL) 207, 230
account lockout policies 27–28
Accounts: Block Microsoft Accounts setting 4–5
Accounts page 3–4
ACEs. See Access Control Entries (ACEs)
ACT. See Application Compatibility Toolkit (ACT)
Active Directory Certificate Services (AD CS) 19
Active Directory Domain Services (AD DS) 2, 26, 41, 173
synchronizing user accounts with 99–100
Active Directory Federation Services (ADFS) 30, 99
Add-AppxPackage cmdlet 11
Add A VPN Connection Wizard 259
Add/Remove Programs Control Panel applet 5
administrative templates 369
administrative users 244–245, 247–249
Administrator Properties dialog box 41
Advanced Encryption Standard (AES) 227
advanced troubleshooting mode 336–339
alerts
   categories of 109
   notification rules 109
   using 108–109
Allow All Trusted Apps To Install setting 9
Allow permissions 237
Always Offline Mode 58–59, 275
Always On feature 261
Android clients 306–307
anti-malware protection 329, 338
Any folder sharing 199, 200, 207–208
Anywhere Working 255. See also remote access
APIP 120
Application Compatibility Toolkit (ACT) 308, 308–313
Compatibility Administrator 313
fixing problems 312–313
inventory collector packages
   creating 309
   deployment 310–311
reviewing report data 312–313
runtime-analysis packages
   creating 310–311
   deployment 311
tools 309–310
apps
   allowing through Windows Firewall 138
Azure RemoteApp 301–308
configuration 302–305
Group Policy Objects 305
Remote Desktop Web Access (RD Web Access) 306
subscribing to feeds 305
choosing users who can install 14–15
deep linking, using Microsoft Intune 15
desktop 9, 308–326
   App-V 316–319
   co-existence support 313–318
   compatibility support, using ACT 308–313
deploying using Microsoft Intune 320–322
   User Experience Virtualization (UE-V) 319–321
identifying affected, for System Restore 334–335
installing
   Add/Remove Programs Control Panel applet for 5
   from Company Store 15
   using Windows Store 8–9
   with Microsoft Office 365 5–8
noncompliant apps reports 108
Remote Desktop Connection app 306–307
sequencing 318–319
sideloading 9–14
supporting 1–19
uploading to Microsoft Intune 13–14
virtualization 316–319
app-triggered VPNs

Windows 10  8–9
Windows Store
  reinstalling after system restore  341–342
  updating  376–379
app-triggered VPNs  262
App-V  316–319
App-V Sequencer  317
AppX Windows PowerShell module
cmdlets  11
  sideloading apps using  10–12
Assessment and Deployment Toolkit (ADK)  44
Assessment Platform  309
auditing
  object access  240–244
Audit Object Access GPO  241–242
authentication
  account policies and  27–29
  biometrics for  22
BitLocker Drive Encryption  70–71
  computer  26
  configuration  244–249
  digital certificates for  19–20
  in domains  26
  Kerberos v5 authentication protocol  26
  multi-factor  19–20, 68
  passwords for  19, 27
  picture passwords for  22
  remote  256–260
Secure Channel  27
  support for  18–23
  understanding  26
  virtual smart cards for  20–21
Windows Hello for  30
authentication exceptions
  configuration  145
authorization
  configuration  244–249
  homegroups and  23–24
  Secure Channel  27
  workgroups and  24–26
automatic approval rules  93–94
AutomaticBackup task  345
Automatic Private IP Addressing (APIPA)  120
automatic restart  338
Azure Active Directory (AAD)  99
Azure Active Directory Synchronization Tool (DirSync)  99
Azure RemoteApp  301–308
  client
    installation and configuration  302–305
    configuration  302–305
Group Policy Objects for signed packages  305
Remote Desktop Web Access (RD Web Access)  306
  subscribing to feeds  305
  supporting iOS and Android  306–307
Azure RemoteApp and Desktop Connections
  configuration  302–305
  subscribing to feeds  305
B
background file synchronization  275, 276
Backup And Restore (Windows 7) tool  344–345, 348–349, 356
backups  345–346
  File History  355
  scheduling  345
battery life  277
Battery Saver mode  277
BCDboot command-line tool  65
Bcdboot.exe  286
biometrics  22
BitLocker Drive Encryption  68–71, 168, 177–190, 355
  authentication methods  70–71
  computer upgrades and  180–181
  configuration  178–179
    using command-line tools  181–183
  Control Panel configuration  70–71
  data recovery  186–187
  Manage-bde tool for  71–72
  Microsoft BitLocker Administration
    and Monitoring  187–190
  moving drive to another computer  181
  password  72–73
  PIN for  72
  recovery key  72, 187–188
  startup key  70, 72–73
  startup key storage and recovery options  185–186
  Suspend Protection option  181
  using  177–180
  Windows To Go and  282
BitLocker Network Unlock feature  185
BitLocker To Go  168, 177
  configuration  184–186
  data recovery  186–187
Block Inheritance dialog box 235
Bluetooth 293
boot logging mode 337
BranchCache 271
broadband connectivity 84
broadband tethering
configuration 263–267
bulletin boards 256

C

cache
clearing 126
DNS resolver 127
cached files 274
certificate compliance reports 108
Certificate Authorities (CAs) 19
Certificate Import Wizard 228
certificates
EFS 229
Certificates MMC (CertMgr.msc) 228
certifications
for authentication 19–20
Certmgr console 20
certmgr.msc 19
Challenge-Handshake Authentication Protocol (CHAP) 258, 260
Checkpoint-Computer cmdlet 333
checkpoints
creating 51–52
for virtual machines 51–52
restoring 52
Cipher.exe 227, 228
Clear-DnsClientCache 126
Click-to-Run feature 7
cloud
saving Personalization settings to 1–4
cloud apps
supporting 1–19
cloud-based applications 163
collaboration. See also sharing
command line
folder sharing from 208
command-line tools
for configuring BitLocker 181–183
for connectivity issues 125
command prompt 336
comma separated value (CSV) file
importing users from 99
Company Store
installing apps from 15
Compatibility Administrator 313
Component Store 373–375
computer accounts 26
computer authentication 26
computer groups
managing, in Microsoft Intune 105–107
computer inventory reports 108
Computer Management MMC 207–208
Computer Name tab 24
configuration
account policies 27–28
account settings, using Group Policy 4–5
authentication 244–249
authentication exceptions 145
authorization 244–249
Azure RemoteApp 302–305
BitLocker 178–179, 181–183
BitLocker Drive Encryption 68–71
BitLocker To Go 184–186
broadband tethering 263–267
connection security rules 143–144
Connector site role 105–106
data storage 153–198
Desktop Connections 302–305
disk quotas 238–240
file and folder access 225–251
File History 352–355
file recovery 351–362
folder location 42–43
folder permissions 205–210
HomeGroups settings 200–202
Hyper-V 47–57
IP settings 119–130, 121–123
libraries 202–205
local accounts 29
location-aware printing 133–134
MDM 86–87
Microsoft accounts 29
Microsoft Intune subscriptions 102–104
mobile device security 68–73
mobility options 57–66, 273–297
name resolution 125–127
network adapters 133–134
Network Discovery 146–147
networking 119–152
network locations 127–129
network security 137–148
network settings 131–135
NTFS permissions 230–238
Office 365 6
offline file policies 58–59, 274–277
OneDrive 216–223
policies 111–113
power options 277–282
power policies 60–63
recovery drive 330–332
remote connections 255–274
Remote Desktop 266–271
restore points 344–348
shared printers 210–216
shared resources 199–224
startup key storage 72–73
Storage Spaces 157, 158–161
sync options 59–60, 286–292
system recovery 329–350
System Restore 332–339
update settings 362–364
user profiles 40–42
virtual disks 53–54
virtual machines 50–51
virtual smart cards 21–22
virtual switches 52–53
Wi-Fi Direct 65, 293–294
Windows Firewall 137–142
Windows Firewall with Advanced Security 139–142
Windows To Go 63–65, 282–287
Work Folders 83
Configuration Manager 15
Config.xml 44, 45
connection security rules
configuration, with IPsec 143–144
firewall rules and 144
types of 144
connection status
viewing 124
connectivity issues 124–125
connectors. See also receive connectors;
See also send connectors
Connector site role
configuration 105–106
Control Panel
BitLocker configuration from 70–71
configuring Work Folders in 83
Control Panel Sync Center applet 288
Convert Inherited Permissions Into Explicit Permissions
On This Object 235
Cost-Aware Synchronization 58
Create A Windows To Go Workspace Wizard 64–65
Creator Owner special identity 173
Credential Locker 28
Credential Manager 28, 229
Credential Roaming 229
CSV file
importing users from 99
C:\Users folder 40

D

DAC. See Data Access Control (DAC)
data
encryption. See encryption
redundancy 158–159
shared. See shared resources
data access 169–170
access-based enumeration (ABE) 209–210
configuring file and folder access 225–251
Dynamic Access Control (DAC) 173, 209
Effective Access 236–237
management 199
object access auditing 240–244
removable media 176–177
User Account Control 244–245
Data Encryption Standard (DES) 258
data recovery
BitLocker 186–187
Data Recovery Agent (DRA) 174, 225, 227
data security 168–193
BitLocker Drive Encryption 177–190
defensive layering 240–241
Encrypting File System (EFS) 173–175, 225–230
permissions 168–173
removable media 176–177
Secure Desktop 249
data storage
configuration 153–198
disk quotas for 238–240
Distributed Files System (DFS) 154–157
OneDrive for Business 162–166, 216–223
removable 168, 176–177
Storage Spaces 157–162
support 153–167
data synchronization  82
mobile devices  82
OneDrive  218, 220–221
scheduling, in Sync Center  84
debugging mode  337
decryption  226
deep linking
    apps, using Microsoft Intune  15
default gateway  120
Defer Upgrades  365
deleted files
    recovering  357–359
Deny permissions  170, 237
deployment
    Azure RemoteApp  301–308
    choosing groups for  14–15
desktop apps
    using Microsoft Intune  320
    inventory collector packages  310–311
of Office  7
planning for  39–80
policies  112–113
runtime-analysis packages  311
software, using Microsoft Intune  89–96
virtual application packages  318
Windows Store apps  15
Deployment Image Servicing and Management (DISM)  286, 374–375
Deployment Image Servicing and Management (DISM) cmdlets  11
Deployment Image Servicing and Management (DISM) tools  65
desktop apps  9, 308–326
    App-V  316–319
    co-existence support  313–318
    compatibility support, using ACT  308–313
    deploying using Microsoft Intune  320–322
    User Experience Virtualization (UE-V)  319–321
device drivers
    resolving problem  372–373
    rollback of  342–344
device enrollment manager account  100
device groups
    creating  106–107
device history reports  108
device management
    enabling network discovery  206
    enrolling devices  100–101
    group management  105–107
monitoring and alerts  107–109
    policies  109–112
    reports  107–108
    viewing and managing devices  101
    with Microsoft Intune  81–118
Device Registration Service (DRS)  30
DFR Namespaces (DFSN or DFS-N)  155, 156
DFR Replication (DFSR or DFS-R)  155, 156
DFS. See Distributed File System (DFS)
Dfscmd.exe  156
Dfsdiag.exe  156
DFS-R  154
Dfsradmin.exe  156
Dfsutil.exe  156
DHCP  120
DHCP scope  120
dial-up connections  256, 257
digital certificates  19–20
DirectAccess  58, 271
directory synchronization  99–100
DirSync  99
    with Password Sync  99
    with Single Sign-on  99
Disable-ComputerRestore cmdlet  333
Disable-PnpDevice cmdlet  343
discretionary access control list (DAACL)  231
disk drive space  330
disk quotas  238–240
DISM. See Deployment Image Servicing and Management (DISM)
Distributed File System (DFS)  153, 154–157
dns resolver cache  127
document version history  359–360
domain account  2
    associating Microsoft account with  2–3
Domain Name Service (DNS)  121
domain networks  127
domains
    authentication in  26
    Microsoft accounts in  29
    use of  23–24
DRA. See Data Recovery Agent (DRA)
driver files  342
driver rollback  342–344
driver signature enforcement  338
Driver Store  342
Dynamic Access Control (DAC)  168, 173, 209
dynamic display scaling  269
Dynamic Host Configuration Protocol (DHCP)  120
E

EAP-MS-CHApv2  260–261
Effective Access  236–237
Effective Access tool  171

effective permissions  170–171
EFS. See Encrypting File System (EFS)
electronic point of sale (EPOS)  256
Electronic Software Distribution (ESD)  318
Enable Always Offline Mode setting  275
Enable-ComputerRestore cmdlet  333
Enable File Synchronization On Costed Networks policy
setting  59
Enable File Synchronization On Costed Networks setting  275
Enable-PnpDevice cmdlet  343
Encrypting File System (EFS)  168, 225–230, 355
backup and recovery  228–229
Credential Roaming  229
troubleshooting  173–175
encryption
Advanced Encryption Standard (AES)  227
BitLocker Drive Encryption  177–190, 355
Encrypting File System (EFS)  173–175, 225–230, 355
File History support for  355
Perfect Forward Secrecy  163
enterprise remote technologies  271
ESD. See Electronic Software Distribution (ESD)
ESRA. See EdgeSync replication account (ESRA)
Extensible Authentication Protocol-Transport Layer Secu-
ritv (EAP-TLS)  258
external virtual switches  52

F

factory settings
restoring  341
Federal Information Processing Standard (FIPS)  189
File Explorer
Encrypt Contents To Secure Data option  227
file sharing using  207
Quick Access  204–205
File History
backup location  355
configuration  352–355
ciphering support  355
Previous Versions feature and  356
restore points  354, 355
turning off  355

file recovery
configuration  351–362
File History  352–355
from OneDrive  357–360
of previous versions  355–357
files
access configuration  225–251
access to  169–170
auditing  240–244
backup and recovery of EFS-protected  228–229
cached  274
driver  342
efficiency of  225–230
fetching from PC, using OneDrive  221–222
identifying affected, for System Restore  334–335
libraries  202–205
locally cached  42
maximum size, in OneDrive  218
NTFS permissions  230–238
offline policies  58–59, 274–277, 288
recovering, from OneDrive  164–166
shared. See shared resources
showing hidden  40
File Server Resource Manager (FSRM)  240
file systems
NTFS  168–171
types of  168
File Transfer Protocol (FTP)  137
filtering  137
firewalls
Remote Desktop and  268
rules  144
settings  206
Windows Firewall  137–142
folders
access configuration  225–251
Any folder sharing  207–208
auditing  240–244
configuring location of  42–43
efficiency of  225–230
libraries  202–205
moving or copying  235–236
offline versions of  42
permissions
configuration  205–210
NTFS  230–238
privacy settings  205
Public  206
restoring previous versions of  355–357
internet service providers

sharing
  access-based enumeration 209–210
  from command line 208
  in HomeGroups 201–202
  using Windows PowerShell 208–209
Work Folders 291–293
fully-qualified domain name (FQDN) 126

G

Get-Acl cmdlet 233
Get-AppxLastError cmdlet 11
Get-AppxLog cmdlet 11
Get-AppxPackage cmdlet 11
Get-AppxPackageManifest cmdlet 11
Get-ComputerRestorePoint cmdlet 333
Get-DnsClientCache cmdlet 127
Get-NetIPAddress 126
Get-NetIPv4Protocol 126
Get-PnpDevice cmdlet 343
Get-PnpDeviceProperty cmdlet 343
Get-SmbShare cmdlet 209
Global Catalog 26
Group Policy
  biometrics settings 22
  BitLocker management 68
  BitLocker settings in 178
  configuring account settings using 4–5
  disabling access to Windows Store using 9
  disk quotas using 239–240
  enabling sideloading with 10–11
  Local Group Policy Editor 9
  offline file policies 275–276
  power policy configuration using 279, 281–282
  power policy creation using 62–63
  print management with 214
  restricting data access with 176
  shared folder permissions using 206
  update policies in 366–369
  Windows To Go settings 64
  Work Folders configuration using 83, 291–292
Group Policy Management 9
Group Policy Objects 173
Group Policy Objects (GPOs) 27
  Audit Object Access 241–242
  for signed packages 305
  inventory collector packages 310–311
  Windows Store 378
  Windows Update 366–369

H

Hibernate 63
hibernation 283
hidden files
  showing 40
HKEY_CURRENT_USER registry 40
Homegroups 23–24
  creating 200
  joining 201
  settings 200–202
  sharing 199
Homegroup Troubleshooter 128
HTTPS (HTTP Secure) 137
hygiene. See message hygiene
Hypertext Transfer Protocol (HTTP) 137
Hyper-V 314–315
  configuration of 47–57
  enabling 48
  minimum requirements for 47
  Windows PowerShell Direct 51
Hyper-V Manager 48–50, 53, 54

I

ICACLS.exe 233
identity management 1–38
  app support and 1–19
  authentication and authorization 18–31
In-Console Monitoring
  installation
    apps 5–16
    Office 365 6–7
internal virtual switches 52
Internet Key Exchange (IKE) 258
Internet Key Exchange, version 2 (IKEv2) 258
Internet Protocol (IP) address. See IP address
internet service providers (ISPs) 85
Intune Administration console

Intune Administration console 92–93
inventory collector packages
   creating 309
development 310–311
iOS clients 306–307
IP address 119
   assignment of 120
   communication via 125
   conflicts 124
   filtering 137
   name resolution 125–127
   requirements 120
Ipconfig 125
IPconfig 126
Ipconfig /all 125
IPsec
   configuring connection security rules with 143–144
   functionality 143
IP settings
   address requirements 120
   configuration 119–130, 121–123
IPv4 121
IPv4 configuration dialog box 123
IPv6 121
isolation rules 144

K

Kerberos Key Distribution Center (KDC) 26
Kerberos v5 authentication protocol 26

L

Last Known Good Configuration 339
Layer 2 Tunneling Protocol (L2TP) 258
legal hold. See litigation hold
libraries
   configuration 202–205
   creating 203
license installation reports 108
license purchase reports 108
Link Layer Topology Discovery (LLTD) protocol 206
link-local (IP) address 120
link referral 155
Link Target 155
LLTD Mapper (LLTDIO) 206
loadState.exe 44, 45
local accounts 2
   associating Microsoft account with 2–3
   configuration of 29
Local Group Policy Editor 9
local profiles 40
Local Security Authority (LSA) 25
local Security Policy 27
location-aware printing
   configuration 133–134
LockDown VPN 262
Logical Unit Number (LUN) 157
Long Term Servicing Branch (LTSB) 365–366
low-resolution video mode 337
Lync Online. See Skype for Business

M

malware 329
malware attacks 244–245
Manage-bde.exe 181–182
Manage-bde tool 71–72
Manage Default Printers dialog box 134
Manage Deployment Wizard 14
Manage Identity objective 1–38
   app support and 1–19
   authentication and authorization 18–31
   mandatory profiles 42
   master boot record (MBR) disk 286
MDM. See Mobile Device Management (MDM)
MDOP. See Microsoft Desktop Optimization Pack (MDOP)
media access control (MAC) address 127
message transport. See transport
Microsoft accounts
   associating with local or domain account 2–3
   configuration of 29
   using Group Policy 4–5
   integration of 1–4
   synchronization settings 3–4
Microsoft Application Compatibility Manager 309
Microsoft BitLocker Administration and Monitoring (MBAM) 177, 187–190
Microsoft Compatibility Exchange 311
Microsoft Desktop Optimization Pack (MDOP) 177, 188, 316–317, 317
Microsoft Intune 81–118, 308
adding users and groups 12
Administrator Console 322
automatic approval rules 93–94
Connector site role 105–106
deep linking apps using 15
deploying desktop apps using 320–322
device management 97–112
  enrolling devices 100–101
  monitoring and alerts 107–109
viewing and managing devices 101
group management 105–107
Groups page 13
Licenses page 103
MDM configuration for 86–87
mobile device support 81–88
policies
  configuration 111–113
  creating 111–112
  deployment 112–113
  managing 109–112
provisioning user accounts 98–99
reports 107–108
sideloading apps using 12–15
software deployment using 89–96
subscriptions 102–104
third-party updates 95
Updates page 89–93
uploading apps to 13–14
Microsoft Intune Software Publisher 322–323
Microsoft Management Console (MMC) 207
Microsoft Office 365
  Admin Center 7–8
  as SaaS 5
  Business Premium 6
configuration of 6
deployment of 7
free trial of 6
important features of 7–8
installing 6–7
installing apps using 5–8
software management using 7–9
updates 5
Microsoft Services Agreement 163–164
Microsoft Software Assurance 177, 188
Microsoft Volume Licensing 188
MigApp.xml 44, 45
MigDocs.xml 44, 45

migration
  of user data 39–43
  of user profiles 43–45
User State Migration Tool (USMT) 44–45
MigUser.xml 44, 45
Mobile Device Management (MDM) 85–87
mobile devices
  access 82
    with Sync Center 83
    with Work Folders 82–83
battery life 277
broadband connectivity 84
broadband tethering 263–267
configuration of 57–66
data synchronization 82
enrolling, in MDM 87
inventory reports 108
management. See device management
Mobile Device Management (MDM) 85–87
near field communication and 215–216
policies 109–112
power policies 60–63
remote connectivity for 58
rolling back updates on 376
security configuration for 68–73
  BitLocker 68–71
supporting 81–88
sync options 59–60
Wi-Fi Direct and 65
Work Folders for 82–83
mobile hot spots 263–267
Mobility and Multihoming (MOBIKE) protocol 258
mobility options
  configuration 273–297
  offline file policies 274–277
  power options 277–282
  sync options 286–292
  Wi-Fi Direct 293–294
  Windows To Go 282–287
  Work Folders 291–293
Modify permissions 236
MRM. See Messaging Records Management
MS-CHAP v2 260
Mstsc.exe 268
multi-factor authentication 19–20, 68
name resolution

configuration 125–127
troubleshooting 126–127
NAT. See network address translation (NAT)
near field communication (NFC) 210, 215–216
netsh 125
Netsh 65
Net Share 208
netstat 125
network adapters 122, 131
configuration 133–134
Network And Sharing Center 124
network discovery
enabling 206
Network Discovery
configuration 146–147
network locations 127–129
network settings
configuration 131–135
network sharing
homegroups for 23
workgroups for 24–29
networks/networking
broadband connectivity 84
configuration 119–152
connecting to 119–124, 123–124
defined 119
domain 127
identifying 127–129
IP address requirements 120
IP settings 119–130
location-aware printing 133–134
name resolution 125–127
network adapters
configuration 133–134
network locations, configuring 127–129
private 127
public (guest) 127
resolving connectivity issues 124–125
security 137–148
authentication exceptions 145–146
connection security rules 143–144
Network Discovery 146
Windows Firewall 137–142
settings for 131–135
terminology 120–121

Wi-Fi 84
wireless
connections 131–132
enabling printing on 135–136
managing preferred 132–133
Network Unlock 185
New Connection Security Rule Wizard 144
NICs. See network interface cards (NICs)
noncompliant apps reports 108
notification rules 109
NSLookup 125, 126
NTFS permissions 168–171, 172, 225
basic and advanced 232
configuration 230–238
Effective Access 236–237
inheritance 234–236
moving or copying folders and 235–236
resource ownership 238
shared folders and 234–235
states 233
types of 231
NTUSER.DAT file 40, 42

object access auditing 240–244
Office 365. See Microsoft Office 365
Office 365 Admin Center 7–8
Office 365.com Service Health 164
Office Deployment tool 7
Office Telemetry. See telemetry
offline file policies 58–59, 288
Offline Files 83
Offline Files feature 58–59
Offline Files Synchronization Schedule Wizard 289
OneDrive 29
OneDrive for Business 154, 162–166
configuration 216–223
deleting personal settings 288–289
document version history 359–360
fetching files on PC using 221–222
file access 216
file recovery 164–166, 357–360
help for 163
limitations of 218
options 219–220
Recycle Bin 218, 357–359
service availability 163–164
personal settings
   deleting from cloud  288–289
PFS. See Perfect Forward Secrecy (PFS)
picture passwords  22
PIN
   BitLocker  72, 185
Ping command  125, 126
platform-as-a-service. See PaaS
Pnutil.exe  211, 343
Point-to-Point Protocol (PPP)  257
Point-to-Point Tunneling Protocol (PPTP)  257
policies
   deployment  112–113
   Microsoft Intune  109–112
   port 21  137
   port 25  137
   port 53  137
   port 80  137
   port 443  137
   port numbers  137
   port rules  141
   PostScript  211
   powercfg.exe  61–62
   powercfg.exe  280–282
   Power Management Group Policy settings  281–282
   power options  277–282
   Power Options applet  278
   Power Options Control Panel  278
   power policies
      configuration of  60–63
      creating  62–63
   Power & Sleep Settings  277–278
   Previous Versions  355–357
   print drivers  211
      Type 4  211–212
   Printer Control Language  211
   printer ports  211
   printers
      permissions  213
      shared  210–216
      Type 4 print drivers  211–212
   printing
      location-aware  133–134
      near field communication and  215–216
      print management  212–213
   Print Management MMC console  213
   print servers  212–213
   properties, managing  213–214

P
page description language (PDL)  211
PAP protocol  260
parity  158
Password Authentication Protocol (PAP)  258, 260
passwords  19
   BitLocker  185
   BitLocker Drive Encryption  72–73
   computer  26
   Credential Manager for  28
   picture  22
   policies for  27–28
   recovery  185
   weaknesses of  27
   Wi-Fi  264
pen support  270
Perfect Forward Secrecy (PFS) encryption  163
permissions
   administrative  247–249
   combining NTFS and Share  172
   data access and  169–170
   Deny  170
   Dynamic Access Control (DAC)  173
   effective  170–171
   Effective Access  236–237
   inheritance  234–236
   managing  168–173
   NTFS  168–171, 172, 205, 225, 230–238
   printers  213
   Read  205
   resource ownership  238
   Share  171–173, 205, 207
   shared folder  205–210
   Show Advanced Permissions  242–243
   user-effective  170
Personal certificates  19
personal devices
   Workplace Join for  30
Personalization settings  1–4

supported device platforms  222
sync settings  220–221
operating system failures
   recovery from  329–351
out-of-box experience (OOBE)  220, 341
OWA. See Outlook Web App (OWA)
privacy
OneDrive and 218
privacy settings
Folder Options 205
private keys 19–20, 226
private networks 127
private virtual switches 52
profilePath attribute 41
program rules 141
Protected Extensible Authentication Protocol (PEAP) 258
Public folders
sharing 199, 206
public key infrastructure (PKI) 19
Public Key Infrastructure (PKI) 226
public keys 19–20, 226
public networks 127

Q
Quick Access 204–205

R
radio frequency identification (RFID) 215
RAID technology 157
RD Connection Broker 315
RD Gateway 315
RD Licensing 315
RDS. See Remote Desktop Services (RDS)
RD Session Host 315
RD Virtualization Host 315
RD Web Access 315
Read permissions 205
recovering files 164–166
recovery 329
file 351–362
system 329–351
recovery drive
configuration 330–332
USB 330
Recovery Environment (RE) 330
recovery key 72
BitLocker 187–188
recovery partitions 330, 331
recovery password 185
Recycle Bin 164, 165–166, 218, 357–359
recycle option 339–341
redundancy
types of, with Storage Spaces 158–159
referral 155
referral cache 155
refresh option 339–341
reliability 329
remote access 255–300
configuring remote connections 255–274
mobility options 273–297
RemoteApp 315–316
RemoteApp and Desktop Connections 302–305
remote connections
authentication 256–260
authentication of remote users 259–260
broadband tethering 263–267
configuration 255–274
enterprise remote technologies 271
Remote Desktop 266–271
VPN connections
creating 260–262
VPN Reconnect 262–263
Wi-Fi Sense 264–266
remote connectivity 58
Remote Desktop
command-line parameters for connection 268–269
firewall port 268
pen support 270
scaling 270
settings configuration 266–271
troubleshooting connections 268–269
Zoom support 269–270
Remote Desktop Connection app 306–307
Remote Desktop Connection Manager (RDCMan) 271–272
Remote Desktop Protocol 256
Remote Desktop Services (RDS) 315–316
Remote Desktop Web Access (RD Web Access) 306
Remote Differential Compression (RDC) 155
Remote Server Administration Tools (RSAT) 155
removable media
BitLocker to Go for 184
BitLocker To Go for 177
security 168
Remove All Inherited Permissions From This Object 235
Remove-AppxPackage cmdlet 11
reports
application compatibility 312–313
creating 108

396
Simple Mail Transfer Protocol (SMTP)

BitLocker Drive Encryption 68–71
network 137–148
authentication exceptions 145–146
connection security rules 143–144
Network Discovery 146
Windows Firewall 137–142
Perfect Forward Secrecy (PFS) encryption 163
permissions 168–173
removable media 176–177
Secure Desktop 249
threats 329
Wi-Fi Sense password 264
Security Account Manager (SAM) database 2, 25
security protocols 27
Security Support Provider (SSP) 27
self-service deployment. See user-driven client deployments
Server Message Block (SMB) 205
server-to-server rules 144
service availability
OneDrive 163–164
service set identifier (SSID) 133
Set Up Work Folders Wizard 291
shared resources
configuration 199–224
folder permissions 205–210
HomeGroups settings 200–202
libraries 202–205
NTFS permissions and 234–235
OneDrive 216–223
printers 210–216
Share permissions 168, 171–173, 205, 207
SharePoint Online 154
sharing. See also collaboration
external. See external users
Shim Infrastructure 312–313
shims 313–314
Show hidden files option 40
tsideloding
apps 9–14
enabling, in Windows 10 10–11
using Microsoft Intune 12–15
Simple Mail Transfer Protocol (SMTP) 137

S
Safe Mode 337, 344
Safe Mode with Command Prompt 338
Safe Mode with Networking 338
Sarbanes-Oxley Act 240
ScanState.exe 44, 45
Schannel 27
screen brightness 277, 279
Second Level Address Translation (SLAT) 47
Secure Channel 27
Secure Desktop 249
Secure Digital High-Capacity (SDHC) memory cards 332
Secure Digital (SD) cards 177
Secure Sockets Layer (SSL) protocol 258
Secure Sockets Layer (SSL) security 27
Secure Socket Tunneling Protocol (SSTP) 258
security
BitLocker Drive Encryption 177–190
data 168–193
defensive layering 240–241
Encrypting File System (EFS) 173–175, 225–230
firewall settings 206
for mobile devices 68–73
single sign-on (SSO) 30
SIP addresses. See Session Initiation Protocol (SIP) addresses
Slow-link Mode 277
smart cards
virtual 20–21
SmbShare 208–209
SMTP. See Single Mail Transfer Protocol (SMTP) software as a service (SaaS) 5
Software Assurance (SA) 317–318
software deployment
using Microsoft Intune 89–96
software reports 108
software updates
approving or declining 92–93
configuring automatic approval settings 93–94
reports 107
third-party 95
using reports to identify required 89–93
software management
using Office 365 7–8
Solid State Drive (SSD) 238
SPF. See send policy framework (SPF) records
startup key
for BitLocker 70, 72–73, 185–186
storage configuration 72–73
Startup Repair 336
Startup Settings 336, 337, 339
storage
configuration of 153–198
disk quotas for 238–240
Distributed Files System (DFS) 154–157
OneDrive for Business 162–166, 216–223
pools 157, 160–161
removable 168, 176–177
Storage Spaces 157–162
support 153–167
virtual machines 54–55
Storage Area Network (SAN) devices 157
Storage Area Network (SAN) technology 238
Storage Spaces 153, 157–162, 329
configuration 157, 158–161
types of redundancy with 158–159
subnet mask 120, 121
subscriptions
configuring Microsoft Intune 102–104
Sync Center 59–60, 83, 288–290
synchronization
background file 275, 276
directory 99–100
OneDrive 218, 220–221
options configuration 286–292
scheduling, in Sync Center 84
sync options
configuration of 59–60
sync partnerships 84
synchronization settings 3–4
sync shares 291–293
Sync Your Settings 287–288
Sync Your Settings section 3–4
System Center Configuration Manager (SCCM) 366
system image
creation of 345–346
System Image Recovery 336, 346–348
system instability 329
System Properties dialog box 24
System Protection 334
system recovery 329–351
configuration 329–350
driver rollback 342–344
performing refresh or recycle 339–341
recovery drive configuration 330–332
restore points 344–348
System Image Recovery 346–348
system repair disk creation 348–349
System Restore 332–339
system repair disk
creation of 348–349
System Restore
configuration 332–339
identifying affected apps and files 334–335
modifying task schedule 336
within Windows RE 335
System Restore Wizard 334
systems access control list (SACL) 231
T
task schedule
modifying default 336
Task Scheduler 336, 345, 374
technology advances 255
terms and conditions reports 108
Test-Connection cmdlet 126
third-party updates 95
three-way mirror 158
Time to Live (TTL) 155
TPM. See Trusted Platform Module (TPM)
Tpmvscmgr.exe 21
tracert 125
traffic filters 262
Transport Layer Security (TLS) 27
Triple DES (3DES) 258
troubleshooting mode 336–339
Trusted Platform Module (TPM) 63, 68, 177, 178–179, 179, 282
Trusted Platform Module (TPM) chips 20
Trusted Root Certification Authorities store 19
tunnel rules 144
two-way mirror 158
type 4 print drivers 210, 211–212

U

UAC. See User Account Control (UAC)
Undo feature 164–165
unified extensible firmware interface (UEFI) 337
Unified Extensible Firmware Interface (UEFI) 63
Unified Extensible Firmware Interface (UEFI) settings 179
Uniform Naming Convention (UNC) 155
Universal Naming Convention (UNC) address 209
Universal Serial Bus (USB) recovery drive 330
update reports 107
updates 329, 361–381
automatic 362
deferring upgrades 365
delivery optimization 363–364
disabling automatic, in Windows Store 377–379
for enterprise customers 365–366
history management 370–371
missing 371
policies configuration 366–369
resolving problem 372–373
rolling back 372–376
settings configuration 362–364
Windows Server Update Services (WSUS) 369
Windows Store apps 376–379
Updates page 89–93
USB flash drive
running Windows 10 from 63–65
USB flash drives
BitLocker To Go for 177, 184
controlling access to 176–177
User Account Control (UAC) 111–112, 225, 244–245
changing settings 248
elevation prompts 247–249
Secure Desktop 249
user accounts
administrators 244–245, 247–249
configuration of 29
importing from CSV file 99
manual creation of 98
policies for 27–29
provisioning 98–99
synchronizing with AD DS 99–100
user authentication
account policies and 27–29
biometrics for 22
digital certificates for 19–20
in domains 26
multi-factor 19–20
passwords for 19
picture passwords for 22
support for 18–23
understanding 26
virtual smart cards for 20–21
Windows Hello for 30
user data
configuration of 39–43
folder location for 42–43
migration of 43–45
user-effective permissions 170
User Experience Virtualization (UE-V) 308, 319–321
user groups
creating 106–107
managing, in Microsoft Intune 105–107
user profiles
configuration of 40–42
local profiles 40
mandatory profiles 42
migration of 43–45
modifying, with Windpws PowerShell 42
roaming profiles 41–42
users
adding, to Intune 12
User State Migration Tool (USMT) 44–45
UsmtUtils.exe 44
V
Verisign 19
VHDX format 53
View Update Reports 90
virtual hard disks (VHDs) 52, 53–54
virtual hard disk (.vhdx) file format 346
virtualization tools 315–316
App-V 316–319
User Experience Virtualization (UE-V) 319–321
virtualized application packages 318–319
virtual machines 47–57, 126
checkpoints 51–52
configuration of 50–51
creating 48–50
importing 54–55
moving storage 54–55
virtual disks for 53–54
virtual switches for 52–53
virtual private networks (VPNs) 58, 126, 256
connections
creating 260–262
connections and authentication 256–262
features of 261
protocols 257–259
security properties 261
VPN Reconnect 262–263
virtual smart cards 20–21
virtual switches 52–53
Virtual Switch Manager 53
volume-level resiliency 157
Volume Shadow Copy Service (VSS) 334, 346
VPN protocols 257–259
VPN Reconnect 262–263
VSS. See Volume Shadow Copy Service (VSS)
W
WDS. See Windows Deployment Services (WDS)
Web Application Proxy 30
Wi-Fi Direct
configuration 293–294
configuration of 65
Wi-Fi hotspots 263
Wi-Fi networks 84
Wi-Fi Properties dialog box 133
Wi-Fi Sense 264–266
WIM. See Windows Imaging Format (WIM)
Windows 10
advanced troubleshooting mode 336–339
Assessment and Deployment Toolkit (ADK) 44
authentication and authorization 18–31
enabling sideloading in 10–11
mobile device support in 81–88
reliability 329
rolling back 375–376
running from USB flash drive 63–65
system recovery 329–350
using Microsoft account with 1–4
wireless connectivity and 132–133
Windows 10 apps 8–9
Windows 10 devices
deployment planning for 39–80
Windows Assessment and Deployment Toolkit (Windows ADK) 308
Windows Assessment Console 309
Windows Biometric Framework (WBF) 22, 215
Windows Deployment Services (WDS) 154
Windows Deployment Services (Windows DS) 340
Windows Firewall
allowing app through 138
configuration 137–142
connection security rules 140
custom rules 141
inbound rules 140, 141, 145
monitoring 138
outbound rules 140, 141
port rules 141
predefined rules 141
program rules 141
turning on/off 138
with Advanced Security 139–142, 144
Windows Hello 30
Windows Imaging Format (WIM) 1
Windows PowerShell 8
AppX module for 10–12
BitLocker cmdlets 182–183
creating Windows to Go workspace using 65
driver rollback using 343
modifying users with 42
permissions management in 233
sharing folders using 208–209
System Restore configuration using 333
to manage DFS-R 155–156
troubleshooting name resolution with 126
virtual machine configuration using 51
workspace creation with 286–287
Windows PowerShell Direct 51
Windows Preinstallation Environment (Windows PE) 44–45
Windows Recovery Environment 63
Windows Recovery Environment (Windows RE) 334
launching 336–339
System Restore within 335
Windows Server Update Services (WSUS) 366, 369
Windows Store
disabling access to 9
installing apps using 8–9
Windows Store apps
deploying, using Microsoft Intune 15
reinstalling after system restore 341–342
supporting 1–19
updating 376–379
Windows To Go
certified drives 284–285
configuration 282–287
configuration of 63–65
features 282–283
hardware considerations 283
roaming with 283
workspace creation 64–65, 285–287
Windows To Go Workspace Wizard 285–286
Windows Update Delivery Optimization 363
Windows Updates 361–381
deferring upgrades 365
delivery optimization 363–364
for enterprise customers 365–366
policies configuration 366–369
resolving problematic 372–373
settings configuration 362–364
Windows Vault 28, 229
WinStoreUI files 378
WinSxS storage folder 373
wireless networks
connecting to 131–132
enabling printing on 135–136
managing preferred 132–133
Work Folders 291–293
configuration
in Control Panel 83
mobile access with 82–83
workgroups 23, 24–26
Workplace Join 30
workspaces
Windows To Go 64–65
Write-DfsrHealthReport cmdlet 155
Write permissions 236
WSUS. See Windows Server Update Services (WSUS)
XML Paper Specification (XPS) 211
Zoom option 269–270
Zoom option
This page intentionally left blank
About the authors

ANDREW BETTANY is a Microsoft Most Valuable Professional (MVP), recognized for his Windows expertise, and author of several publications including Windows exam certification prep and Microsoft official training materials. As leader of the IT Academy at the University of York, UK and Microsoft Certified Trainer, Andrew delivers learning and consultancy to businesses on a number of technical areas including Windows deployment and troubleshooting. He has created and manages the “IT Masterclasses” series of short intensive technical courses, www.itmasterclasses.com and is passionate about helping others learn technology. He is a frequent speaker and proctor at TechEd and Ignite conferences worldwide. In 2011 and 2013 he delivered classes in earthquake-hit Haiti to help the community rebuild their technology skills. Very active on social media, having co-founded Queuedit.com, as Social Media Management tool, 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).

JASON KELLINGTON MCT, MCSE, MCITP, MCTS, is a consultant, trainer, and author living in beautiful, cold northern Canada with his wife and two boys. Jason has spent time as an engineer, developer, administrator, and educator during his 15+ years in IT. His consulting and training practice specialize in enterprise infrastructure deployment as well as data management and business intelligence. He has assisted in the development of several projects with Microsoft Press and Microsoft Learning.