Microsoft

Microsoft® Official Academic Course

Cloud Fundamentals

Microsoft Technology Associate
EXAM 98-369

Microsoft® Official Academic Course

Cloud Fundamentals, Exam 98-369

WILEY

VICE PRESIDENT & DIRECTOR	Laurie Rosatone
SENIOR DIRECTOR	Don Fowley
EXECUTIVE EDITOR	Bryan Gambrel
DEVELOPMENT EDITOR	Jennifer Lartz
ASSISTANT	Jessy Moor
PROJECT MANAGER	Gladys Soto
PROJECT SPECIALIST	Nichole Urban
PROJECT ASSISTANT	Anna Melhorn
MARKETING MANAGER	Dan Sayre
ASSISTANT MARKETING MANAGER	Puja Katarawala
ASSOCIATE DIRECTOR, PRODUCTION	Kevin Holm
SENIOR CONTENT SPECIALIST	Nicole Repasky
PRODUCTION EDITOR	Loganathan Kandan
COVER PHOTO CREDIT	© Milosz_M/Shutterstock

This book was set in Garamond by SPi Global and printed and bound by Strategic Content Imaging.
The cover was printed by Strategic Content Imaging.

ISBN 978-1-119-23957-4

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

www.wiley.com/college/microsoft

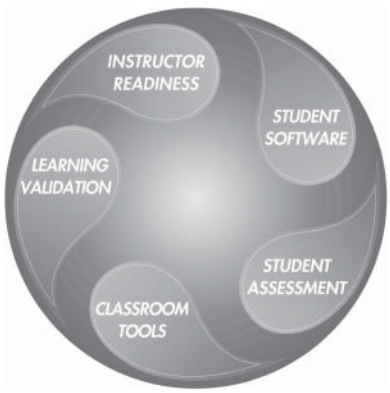
Preface

Welcome to the Microsoft Official Academic Course (MOAC) program for Cloud Fundamentals. MOAC represents the collaboration between Microsoft Learning and John Wiley & Sons, Inc. Microsoft and Wiley teamed up to produce a series of textbooks that deliver compelling and innovative teaching solutions to instructors and superior learning experiences for students. Infused and informed by in-depth knowledge from the creators of Microsoft products, and crafted by a publisher known worldwide for the pedagogical quality of its products, these textbooks maximize skills transfer in minimum time. Students are challenged to reach their potential by using their new technical skills as highly productive members of the workforce.

Because this knowledgebase comes directly from Microsoft, creator of the Microsoft Technology Associate (MTA) exams (www.microsoft.com/learning/certification), you are sure to receive the topical coverage that is most relevant to students' personal and professional success. Microsoft's direct participation not only assures you that MOAC textbook content is accurate and current; it also means that students will receive the best instruction possible to enable their success on certification exams and in the workplace.

■ The Microsoft Official Academic Course Program

The *Microsoft Official Academic Course* series is a complete program for instructors and institutions to prepare and deliver great courses on Microsoft software technologies. With MOAC, we recognize that, because of the rapid pace of change in the technology and curriculum developed by Microsoft, there is an ongoing set of needs beyond classroom instruction tools for an instructor to be ready to teach the course. The MOAC program endeavors to provide solutions for all these needs in a systematic manner in order to ensure a successful and rewarding course experience for both instructor and student—technical and curriculum training for instructor readiness with new software releases; the software itself for student use at home for building hands-on skills, assessment, and validation of skill development; and a great set of tools for delivering instruction in the classroom and lab. All are important to the smooth delivery of an interesting course on Microsoft software, and all are provided with the MOAC program. We think about the model below as a gauge for ensuring that we completely support you in your goal of teaching a great course. As you evaluate your instructional materials options, you may wish to use the model for comparison purposes with available products.



www.wiley.com/college/microsoft

■ Pedagogical Features

The MOAC textbook for Cloud Fundamentals is designed to cover all the learning objectives for MTA Exam 98-369, which are referred to as its "objective domains." The Microsoft Technology Associate (MTA) exam objectives are highlighted throughout the textbook. Many pedagogical features have been developed specifically for *Microsoft Official Academic Course* programs.

Presenting the extensive procedural information and technical concepts woven throughout the textbook raises challenges for the student and instructor alike. The Illustrated Book Tour that follows provides a guide to the rich features contributing to the *Microsoft Official Academic Course* program's pedagogical plan. Following is a list of key features in each lesson designed to prepare students for success as they continue in their IT education, on the certification exams, and in the workplace:

- Each lesson begins with an **Exam Objective Matrix**. More than a standard list of learning objectives, the Exam Objective Matrix correlates each software skill covered in the lesson to the specific exam objective domain.
- Concise and frequent **Step-by-Step** instructions teach students new features and provide an opportunity for hands-on practice. Numbered steps give detailed, step-by-step instructions to help students learn software skills.
- **Illustrations:** Screen images provide visual feedback as students work through the exercises. The images reinforce key concepts, provide visual clues about the steps, and allow students to check their progress.
- **Key Terms:** Important technical vocabulary is listed with definitions at the beginning of the lesson. When these terms are used later in the lesson, they appear in bold italic type and are defined. The Glossary contains all of the key terms and their definitions.
- Engaging point-of-use **Reader Aids**, located throughout the lessons, tell students why this topic is relevant (*The Bottom Line*), and provide students with helpful hints (*Take Note*). Reader Aids also provide additional relevant or background information that adds value to the lesson.
- **Certification Ready** features throughout the text signal students where a specific certification objective is covered. They provide students with a chance to check their understanding of that particular MTA objective and, if necessary, review the section of the lesson where it is covered. MOAC offers complete preparation for MTA certification.
- **End-of-Lesson Questions:** The Knowledge Assessment section provides a variety of multiple-choice, true-false, matching, and fill-in-the-blank questions.
- **End-of-Lesson Exercises** are projects that test students' ability to apply what they've learned in the lesson.

Conventions and Features Used in This Book

This book uses particular fonts, symbols, and heading conventions to highlight important information or to call your attention to special steps. For more information about the features in each lesson, refer to the Illustrated Book Tour section.

Convention	Meaning
THE BOTTOM LINE	This feature provides a brief summary of the material to be covered in the section that follows.
CLOSE	Words in all capital letters indicate instructions for opening, saving, or closing files or programs. They also point out items you should check or actions you should take.
CERTIFICATION READY	This feature signals the point in the text where a specific certification objective is covered. It provides you with a chance to check your understanding of that particular MTA objective and, if necessary, review the section of the lesson where it is covered.
TAKE NOTE*	Reader aids appear in shaded boxes found in your text. *Take Note* provides helpful hints related to particular tasks or topics.
XREF	These notes provide pointers to information discussed elsewhere in the textbook or describe interesting gaming development features that are not directly addressed in the current topic or exercise.
Alt + Tab	A plus sign (+) between two key names means that you must press both keys at the same time. Keys that you are instructed to press in an exercise will appear in the font shown here.
Example	Key terms appear in bold italic.

Instructor Support Program

The *Microsoft Official Academic Course* programs are accompanied by a rich array of resources that incorporate the extensive textbook visuals to form a pedagogically cohesive package. These resources provide all the materials instructors need to deploy and deliver their courses. Resources available online for download include:

- **DreamSpark Premium** is designed to provide the easiest and most inexpensive developer tools, products, and technologies available to faculty and students in labs, classrooms, and on student PCs. A free 3-year membership is available to qualified MOAC adopters.

  Note: Microsoft Visual Studio, Windows Server, and Windows Operating Systems can be downloaded from DreamSpark Premium for use by students in this course.
- The **Instructor Guide** contains Solutions to all the textbook exercises and Syllabi for various term lengths. The Instructor Guide also includes chapter summaries and lecture notes. The Instructor's Guide is available from the Book Companion site (http://www.wiley.com/college/microsoft).
- The **Test Bank** contains hundreds of questions in multiple-choice, true-false, short answer, and essay formats, and is available to download from the Instructor's Book Companion site (www.wiley.com/college/microsoft). A complete answer key is provided.
- A complete set of **PowerPoint presentations and images** is available on the Instructor's Book Companion site (http://www.wiley.com/college/microsoft) to enhance classroom presentations. Approximately 50 PowerPoint slides are provided for each lesson. Tailored to the text's topical coverage and Skills Matrix, these presentations are designed to convey key concepts addressed in the text. All images from the text are on the Instructor's Book Companion site (http://www.wiley.com/college/microsoft). You can incorporate them into your PowerPoint presentations, or create your own overhead transparencies and handouts. By using these visuals in class discussions, you can help focus students' attention on key elements of technologies covered and help them understand how to use it effectively in the workplace.

Wiley Faculty Network

- When it comes to improving the classroom experience, there is no better source of ideas and inspiration than your fellow colleagues. The **Wiley Faculty Network** connects teachers with technology, facilitates the exchange of best practices, and helps to enhance instructional efficiency and effectiveness. Faculty Network activities include technology training and tutorials, virtual seminars, peer-to-peer exchanges of experiences and ideas, personal consulting, and sharing of resources. For details visit www.WhereFacultyConnect.com.

DREAMSPARK PREMIUM—FREE 3-YEAR MEMBERSHIP AVAILABLE TO QUALIFIED ADOPTERS!

DreamSpark Premium is designed to provide the easiest and most inexpensive way for universities to make the latest Microsoft developer tools, products, and technologies available in labs, classrooms, and on student PCs. DreamSpark Premium is an annual membership program for departments teaching Science, Technology, Engineering, and Mathematics (STEM) courses. The membership provides a complete solution to keep academic labs, faculty, and students on the leading edge of technology.

Software available in the DreamSpark Premium program is provided at no charge to adopting departments through the Wiley and Microsoft publishing partnership.

Contact your Wiley rep for details.

For more information about the DreamSpark Premium program, go to:

https://www.dreamspark.com/

Note: Microsoft Visual Studio, XNA Game Studio, and Windows Operating Systems can be downloaded from DreamSpark Premium for use by students in this course.

■ Important Web Addresses and Phone Numbers

To locate the Wiley Higher Education Rep in your area, go to http://www.wiley.com/college and click on the "*Who's My Rep?*" link at the top of the page.

To learn more about becoming certified and exam availability, visit www.microsoft.com/learning/mcp/mcp.

Student Support Program

■ Additional Resources

Book Companion Website (www.wiley.com/college/microsoft)

The students' book companion site for the MOAC series includes any resources, exercise files, and Web links that will be used in conjunction with this course.

Wiley E-Text

Wiley MOAC E-Texts are innovative, electronic versions of printed textbooks. Students buy the e-text version for up to 40% off the U.S. price of the printed text, and get the added value of permanence and portability. Wiley E-Texts provide students with numerous additional benefits that are not available with other e-text solutions.

Wiley E-Texts are NOT subscriptions; students download the Wiley E-Text to their computer desktops. Students own the content they buy to keep for as long as they want. Once a Wiley E-Text is downloaded to the computer desktop, students have instant access to all of the content without being online. Students can also print out the sections they prefer to read in hard copy. Students also have access to fully integrated resources within their Wiley E-Text. From highlighting their e-text to taking and sharing notes, students can easily personalize their Wiley E-Text as they are reading or following along in class.

■ About the Microsoft Technology Associate (MTA) Certification

Preparing Tomorrow's Technology Workforce

Technology plays a role in virtually every business around the world. Possessing the fundamental knowledge of how technology works and understanding its impact on today's academic and workplace environment is increasingly important—particularly for students interested in exploring professions involving technology. That's why Microsoft created the Microsoft Technology Associate (MTA) certification—a new entry-level credential that validates fundamental technology knowledge among students seeking to build a career in technology.

The Microsoft Technology Associate (MTA) certification is the ideal and preferred path to Microsoft's world-renowned technology certification programs. MTA is positioned to become the premier credential for individuals seeking to explore and pursue a career in technology, or augment related pursuits such as business or any other field where technology is pervasive.

MTA Candidate Profile

The MTA certification program is designed specifically for secondary and post-secondary students interested in exploring academic and career options in a technology field. It offers

students a certification in basic IT and development. As the new recommended entry point for Microsoft technology certifications, MTA is designed especially for students new to IT and software development. It is available exclusively in educational settings and easily integrates into the curricula of existing computer classes.

MTA Empowers Educators and Motivates Students

MTA provides a new standard for measuring and validating fundamental technology knowledge right in the classroom while keeping your budget and teaching resources intact. MTA helps institutions stand out as innovative providers of high-demand industry credentials and is easily deployed with a simple, convenient, and affordable suite of entry-level technology certification exams. MTA enables students to explore career paths in technology without requiring a big investment of time and resources, while providing a career foundation and the confidence to succeed in advanced studies and future vocational endeavors.

In addition to giving students an entry-level Microsoft certification, MTA is designed to be a stepping stone to other, more advanced Microsoft technology certifications.

To learn more about becoming a Microsoft Technology Associate and exam availability, visit www.microsoft.com/learning/mta.

Acknowledgments

■ MOAC MTA Technology Fundamentals Reviewers

We'd like to thank the many reviewers who pored over the manuscript and provided invaluable feedback in the service of quality instructional materials:

Yuke Wang, University of Texas at Dallas
Palaniappan Vairavan, Bellevue College
Harold "Buz" Lamson, ITT Technical Institute
Colin Archibald, Valencia Community College
Catherine Bradfield, DeVry University Online
Robert Nelson, Blinn College
Kalpana Viswanathan, Bellevue College
Bob Becker, Vatterott College
Carol Torkko, Bellevue College
Bharat Kandel, Missouri Tech
Linda Cohen, Forsyth Technical Community College
Candice Lambert, Metro Technology Centers
Susan Mahon, Collin College
Mark Aruda, Hillsborough Community College
Claude Russo, Brevard Community College
Heith Hennel, Valencia College
Adrian Genesir, Western Governors University
Zeshan Sattar, Zenos
Douglas Tabbutt, Blackhawk Technical College
David Koppy, Baker College
Sharon Moran, Hillsborough Community College
Keith Hoell, Briarcliffe College and Queens College—CUNY
Mark Hufnagel, Lee County School District
Rachelle Hall, Glendale Community College
Scott Elliott, Christie Digital Systems, Inc.
Gralan Gilliam, Kaplan
Steve Strom, Butler Community College
John Crowley, Bucks County Community College
Margaret Leary, Northern Virginia Community College
Sue Miner, Lehigh Carbon Community College
Gary Rollinson, Cabrillo College
Al Kelly, University of Advancing Technology
Katherine James, Seneca College
David Kidd, Western Governors University
Bob Treichel, Lake Havasu Unified School District & Mohave Community College

Contents

Lesson 5: Supporting Cloud Users 146

Understanding the Cloud

LESSON 1

OBJECTIVE DOMAIN MATRIX

Technology Skill	Objective Domain Description	Objective Domain Number
Understanding Cloud Principles and Delivery Mechanism • Differentiating Between Various Funding Models • Using Cloud Services to Expand Capacity Scalability, Redundancy, and Availability • Differentiating Between Cloud Services and On-Premises Services	Describe cloud principles and delivery mechanisms	1.1
Understanding Cloud Security Requirements and Policies • Understanding How Cloud Services Manage Privacy • Understanding How Compliance Goals are Met • Understanding How Data is Secured at Rest or On-the-Wire • Understanding How Data and Operations Transparency Requirements are Met	Describe cloud security requirements and policies	1.2
Understanding How a Cloud Service Stays Up to Date and Available • Understanding the Service/Feature Improvement Process • Monitoring Service Health, Service Maintenance, and Future Roadmap Publishing • Understanding Guarantees, Service-Level Agreements (SLAs), and Capping of Liability of the Cloud Service Provider	Describe how a cloud service stays up to date and available	1.3
Understanding the Different Types of Cloud Services • Differentiating Between the Types of Cloud Services and Their Characteristics • Integrating the Cloud with On-premises Services in Hybrid Scenarios	Describe the different types of cloud services	1.4

KEY TERMS

asymmetric key
Capital Expenditure (CapEx)
cloud
Communication as a Services (CaaS)
communications services
decryption
dedicated public cloud
Desktop as a Service (DaaS)
downtime
elasticity
encryption
Enterprise Mobility Suite (EMS)
high availability
hosted private cloud
hybrid cloud
Infrastructure as a Service (IaaS)
Microsoft Azure Active Directory (Azure AD/AAD)
Microsoft Azure Rights Management (Azure RMS)
Microsoft Intune
Monitoring as a Service (MaaS)
multi-tenancy
Network as a Service (NaaS)
Operating Expense (OpEx)
pay-as-you-go
Platform as a Service (PaaS)
private cloud
productivity services
public cloud
public-key cryptography
scalability
search services
Secure Socket Layer (SSL)
service-level agreements (SLAs)
shared public cloud
Software as a Service (SaaS)
storage services
subscription
symmetric encryption
System Center 2012 R2/2016 Operations Manager
System Center Global Service Monitor
transparency
Transport Layer Security (TLS)
Virtual Private Network (VPN)

You work as an IT administrator for the Contoso Corporation and you are looking to expand your server infrastructure by expanding onto the cloud. Since you are new to the cloud, you need to develop a thorough understanding of what the cloud can do for your organization as well as how to use the cloud to supplement your current infrastructure.

■ Understanding Cloud Principles and Delivery Mechanisms

THE BOTTOM LINE

The ***cloud*** is a network of servers, and each server in the network has a different function. Some servers run applications or deliver a service. By using the cloud, you don't have to have the individual application or services running on the user's computers. In addition, the cloud allows you to share resources and technology so that they can be accessed by multiple users. From the standpoint of the user, the cloud is a black box that the user accesses. However, the user is not concerned with what happens inside the black box. When choosing to use the cloud, you are shifting certain responsibilities to the cloud so that you can focus on other things—such as your business—and less on the underlying technologies.

CERTIFICATION READY
Describe cloud principles and delivery mechanisms
1.1

Early data centers could consist of hundreds of physical servers, with each server being assigned a workload (such as specific application or service). Unfortunately, most of the resources on an individual sever were often wasted. Eventually, data centers started to consolidate many physical servers to a single server running multiple virtual machines or virtual servers using Microsoft Hyper-V or VMware ESX/ESXi. As a result, there was a significant increase in resource use while reducing overall cost and power consumption.

Cloud computing takes the next step; instead of virtualizing servers, it virtualizes datacenters. It uses a single resource pool containing an infrastructure that delivers infinite computer, network, and storage resources for important services. The cloud is more easily accessible to

IT teams and has more accountability features that can be used to figure out cost center-based chargeback billing.

The advantages in cloud computing are:

- **A virtualized datacenter:** Allows you to access computer services without regard to where, exactly, the data center is located and the hardware that the services are running on. However, you do want to select a data center that is in close proximity to users.
- **Reduced operational costs:** Similar to using virtual machines, cloud computing uses resources more efficiently. In addition, inconsistent availability and high operational costs are reduced by providing pooled resources, elasticity, and virtualization technology.
- **Datacenter/Server consolidation:** A virtual infrastructure helps consolidate servers by hosting multiple virtual machines on a virtualization host. Although the cloud uses a virtual infrastructure, the cloud goes one step further by helping consolidate data centers by moving servers from your current data center to the cloud. In fact, the cloud can also be used to expand current datacenters.
- You can consolidate servers by hosting multiple virtual machines on a virtualization host.
- **Improved resilience and agility:** With the correct applications, the cloud-computing model improves resiliency and agility.

When looking at the cloud, you should understand the following terms:

- ***Communication as a Service (CaaS)*:** Allows the deployment of communications services through cloud computing without the need to purchase their own equipment. It can include Voice over IP (VoIP), VPN services, and business telephone service that you would find on a private branch exchange (PBX) such as phone menus and voice mails.
- ***Desktop as a Service (DaaS)*:** Provides a desktop or work environment to run applications, access emails, or back up data.
- ***Infrastructure as a Service (IaaS)*:** Provides the infrastructure that the cloud runs on, such as servers, switches, routers, storage area networks, firewalls, and other equipment.
- ***Monitoring as a Service (MaaS)*:** Allows you to monitor software applications so that the correct personnel are notified when it is down or not fully performing as needed.
- ***Network as a Service (NaaS)*:** Offers network services such as network infrastructure/IIAS and Communication services/CaaS.
- ***Platform as a Service (PaaS)*:** Allows you to buy, develop, test, deploy, and manage software applications so that users can access the applications.
- ***Software as a Service (SaaS)*:** Allows the development and provisioning of software for the user, including providing servers on which the software runs on. Typically, SaaS runs on demand through the remote desktop services or through a web browser. Often, the cloud provider owns the software licenses and charges a fee to subscribers.

The cloud can provide your organization with the following services:

- **Productivity services:** Allows users to work and collaborate. An example of productivity services is Office 365, which allows users to create and share documents.
- **Storage services:** Provides a storage platform for data. By storing data on the cloud, the data can be accessed by any user or device. An example of storage services is Azure Storage.
- **Communications services:** Provides communications between users. Examples of communication services include Exchange Online and Skype for Business Online. Exchange Online provides email, calendar, and contact sharing and Skype for Business Online provides instant messaging, computer-to-computer audio and video calls, and screen sharing.
- **Search services:** Provides search functionality into custom applications. In addition, it can provide a search engine and storage of data that can be accessed on an Application Programming Interface (API). An example of search services is Azure Search.

Based on the cloud solution that you select, you can also perform self-service and provide multi-tenancy. Self-service provides the ability for an organization end-user to acquire and

manage servers, storage, or other resources without going through the IT operations teams. Users can go to their portals and add more licenses, renew contracts, and reduce the numbers.

Multi-tenancy allows several companies to use the same cloud products. For example, for an application, multi-tenancy means that different customers can use the same codebase. However, to keep customers separated from other customers, their configuration and data are stored in separate containers. Multi-tenancy offers the following benefits:

- Lower costs through economies of scale
- A shared infrastructure or servers lowers costs
- End users don't have to pay costly maintenance fees to perform ongoing maintenance and updates
- Configuring can be done without touching the underlying codebase

Recently, Microsoft developed the ***Enterprise Mobility Suite (EMS)***, which is a comprehensive suite of cloud services that addresses the use of and managing of mobile devices in a corporate environment, including corporate devices and personal devices used on corporate networks. The EMS consists of the following cloud components:

- **Microsoft Azure Active Directory (Azure AD/AAD):** Delivers access management from the cloud and existing on-premises deployment.
- **Microsoft Intune:** Provides advanced device management, including management of Windows, Windows Phones, IOS devices, and Androids. It allows the deployment of policies and software and provides inventory of hardware and software.
- **Microsoft Azure Rights Management (Azure RMS):** Provides protection for company assets with security, compliance, and regulatory requirements by using encryption, identity, and authorization to secure files and email.

Differentiating Between Various Funding Models

Cloud computing is intended to save costs because of the pay-as-you-go model and because of the economies of scale (because cloud computing offers scalability as long as you are willing to pay for the growing resources).

In a traditional, on-premises data center, you will need to pay for the following:

- **Server costs:** All hardware components and the cost of hardware support. Of course, when purchasing servers, don't forget to design fault tolerance and redundancy, such as clustering of servers, redundant power supplies, and uninterruptable power supplies.
- **Storage costs:** All hardware components and the cost of hardware support. Based on the application and level of fault tolerance, centralized storage can be very expensive. For larger organizations, you can create tiers of storage where more expensive fault-tolerant storage is used for critical applications and lower priorities use a cheaper form of storage.
- **Network costs:** All hardware components, including cabling, switches, access points, and routers. It also includes WAN connections and Internet connections.
- **Backup and archive costs:** The cost to back up, copy, or archive data to the cloud or data center. Options might include backing up to the cloud or backing up from the cloud.
- **Business continuity and disaster recovery costs:** Along with server fault tolerance and redundancy, you have to think about how to recover from disaster and continue operating should the worst scenario occur. This should consist of creating a data recovery (DR) site. It could also include backup generators.
- **Data center infrastructure costs:** Costs for electricity, floor space, cooling, and building maintenance.
- **Technical personnel:** Based on the technology used, you will need technical expertise and manpower to install, deploy, and manage the systems at the data center.

When using the cloud, many of these costs are shifted to the cloud provider. However, you need to ensure that you have enough bandwidth available for users to connect to the cloud and use the required applications. If you are connecting a data center to the cloud or connecting two clouds together, you have to see how much data needs to be transferred so that you can determine the bandwidth needed. Don't forget to plan for backup traffic to or from the cloud and replication between data centers or the cloud for data-recovery purposes.

The ***subscription*** or ***pay-as-you-go*** model is a computing billing method that is aimed at organizations and end-users. The organization or user is billed for the services used, typically on a recurring basis. You can scale, customize, and provision computing resources, including software, storage and development platforms. For example, when using a dedicated cloud service, you could pay based on server power and usage. When using software on a SaaS—covered later in this lesson—you lease the software and customized features.

When you use the pay-as-you-go mode, you have to actively manage your subscriptions. You must ensure that users do not misuse the cloud; make sure accounts that are provisioned are actually being used and not wasted. When resources are being provisioned by the provider, billing starts. It is the responsibility of the client to deprovision the resources when they are not in use, so that you can manage costs.

Capital Expenditures (CapEx) are funds used by an organization to acquire or upgrade physical assets, such as servers, networking equipment, and storage. It also includes real estate such as buildings or data center space. Typically, the physical resources are amortized over several years, whereby instead of deducting the full cost of the equipment in the first year, you deduct a smaller portion of it each year.

Operating Expenses (OpEx) are the expenditures that an organization incurs while performing its normal business operations, including the amount of electricity consumed, the cost of employees to manage and support systems, office space, and Internet connections. Management is responsible for minimizing operating expenses without significantly affecting the firm's operations and its ability to compete in the marketplace. OpEx is expensed each year because you pay for and use the product or service.

When a server needs to be replaced, or a server needs to be added to a data center, you need to use CapEx to pay for the computer. It will affect immediate cash flow because you have to pay for the server up front. Fortunately, however, you can amortize the cost over several years. The expense of running the server and the staff to run the server is an OpEx.

If you lease a server or use the cloud, the cost is based on the pay-as-you-go model. For accounting purposes, the costs are considered an OpEx.

Using Cloud Services to Expand Capacity Scalability, Redundancy, and Availability

The advantage of cloud services is that they provide a dynamic infrastructure that allows you to change the services provided based on the changing levels of demand. When planning for any service, including the cloud, you need to plan for capacity, scalability, redundancy, and availability.

Most organizations will face growth. If you are purchasing a server, you would have to purchase a server that can handle the current demand as well as the demand determined by growth over the next three to five years. The current demand could be based on:

- Total number of log-ins per hour
- Page response time
- Transaction and process completion time
- Initial load time

- Amount of website traffic and user load based on the average and maximum number of users, peak load, and maximum number of transactions per second (TPS)
- Seasonal trends

When planning capacity, you will must consider memory, CPU (speed and number of core), disks (speed and capacity), and databases (response times and capacity). You will need to perform the following steps:

1. Conduct a demand analysis.
2. Conduct a current capacity analysis.
3. Conduct future capacity planning.

Demand analysis is used to gather all information about the current demand, workload, and trends from all aspects of the infrastructure. Current capacity analysis establishes the threshold and benchmark values so that you can determine when a resource is over utilized or underutilized.

Scalability is the ability of a computer application or product to continue to function as the application or product changes in size or volume in order to meet user need. Since the cloud is based on virtual technology, the ability to scale on demand is the biggest advantage of cloud computers. That could be as simple as increasing or reducing the amount of memory or number of CPU cores or adding another server to a cluster.

Elasticity is the degree in which a system can adapt to workload changes by provisioning or deprovisioning resources automatically. Of course, elastic computing is the dynamic provisioning and deprovisioning of computer resources to meet the varying workload. By offering elasticity, you can increase and decrease cost, quality, and resources.

When a server or service goes down, it most likely causes your organization to lose money. If your network contains an external website or database that controls your sales, ordering, inventory, or production, server downtime can be detrimental to these business needs. If it is an internal server or service, it might not allow your users to perform their jobs. In either case, your company sustains losses in revenue or productivity—and, in some cases, both.

For any service, you need to minimize downtime by identifying potential failures and then taking steps to avoid those failures and to reduce their effects. ***High availability*** is a combination of technology, protocols, and redundant hardware that ensures a certain degree of operational continuity during a given measurement period while resisting disaster and failure. Generally, the term ***downtime*** is used to refer to periods when a system is unavailable. Availability is usually expressed as a percentage of uptime in a given year, as shown in Table 1-1.

Table 1-1
Availability Guidelines

Availability %	Downtime Per Year	Downtime Per Month
99% ("two nines")	3.65 days	7.20 hours
99.9% ("three nines")	8.76 hours	43.8 minutes
99.99% ("four nines")	52.6 minutes	4.32 minutes
99.999% ("five nines")	5.26 minutes	25.9 seconds
99.9999% ("six nines")	31.5 seconds	2.59 seconds

When designing servers and the services they provide, they are often assigned ***service-level agreements (SLAs)***, which state the level of availability those servers or services must maintain. Of course, a server design that can support five or six nines is much more expensive than supporting an availability of 99%. Of course, six nines is going to cost a lot more than two or even three nines.

If there is miscommunication about service-level expectations between the hosting company and an organization, it could lead to poor business decisions, unsuitable investments,

unsuitable service levels, or customer dissatisfaction. Therefore, you need to express availability requirements clearly so that there are no misunderstandings about the implications.

Typically, to make a server more fault tolerant, you should first consider what components are most likely to fail and then implement technology to make a system less likely to fail. Some of the components that are made redundant within a system are usually the following:

- **Disks:** Use some form of RAID and hot spares.
- **Power supplies:** Use redundant power supplies.
- **Network cards:** Use redundant network cards.

Although you can make these components fault tolerant, the entire server still won't be fault tolerant. Instead, you can use a cluster to provide server redundancy. By using the cloud, you don't have to worry about these details because these details will be handled by the hosting company. When using the cloud, you will need to look at the provided SLAs.

While a hosting company provides six nines for the services it provides, unforeseen disasters could still hinder the availability of those services. Therefore, to provide business continuity in these cases, you should use cloud services that can be accessed from two or more sites. Therefore, if a disaster or mishap impacts the delivery of your agreed services, the necessary services can be provided by the other site or sites.

The cloud can also be used as a DR site for an organization. For example, without establishing a physical DR site, you can deploy backup servers to the cloud. If the primary data center goes down, you can ramp up or switch to the DR site to provide the necessary services.

Differentiating Between Cloud Services and On-Premises Services

When you have a service running from a server placed on-premises, you have full control of the server and the surrounding infrastructure. You can install any desired software on the server and configure the server and infrastructure as you see fit. When you move services to the cloud, some of the services might run a dedicated server that you control. In other cases, you are paying for only a specific service. In either case, some or much of the infrastructure is built and managed by the hosting company and in some situations, parts of the server are managed by the hosting company. As you choose the level of service provided by the cloud hosting company, you need to determine which services need to be provided by the hosting company and which level of control or management capabilities you need.

On-premises services allow you to configure the following so that you adapt to the needs of an organization:

- Software
- Resources
- Topology
- Access

In a scenario whereby you notice that a system is running a little slow, you can then increase the amount of memory and number of processor cores. If you need more bandwidth, you can increase the speed of the network links. You have complete control over who can use the service provided and who can administer the server and services.

One of the advantages of using the cloud is that the organization does not have to concern itself with the infrastructure that the services run on. Therefore, you typically do not have direct access to the servers that the services run on. However, most of these services still provide you with some degree of customization.

■ Understanding Cloud Security Requirements and Policies

THE BOTTOM LINE

When you select a cloud deployment model, you will select a public cloud, a private cloud, a hosted private cloud, or a hybrid cloud (which is based on whether you want the cloud to be shared or dedicated or if you want it to be hosted internally or externally). When you select one of these methods, you will base your decision on cost, control, and scalability.

CERTIFICATION READY
Describe cloud security requirements and policies
1.2

Public cloud services provide a way to access information from anywhere at any time. Microsoft defines a ***public cloud*** as a web-based service that is hosted outside of your organization. This means the information technology infrastructure (hardware, servers, software, and so on) is located somewhere other than your office and is managed by a third party (such as when it is hosted). If you use mobile banking—accessing web-based email or storing your photos online in one of the many services provided—you are interacting with "the cloud."

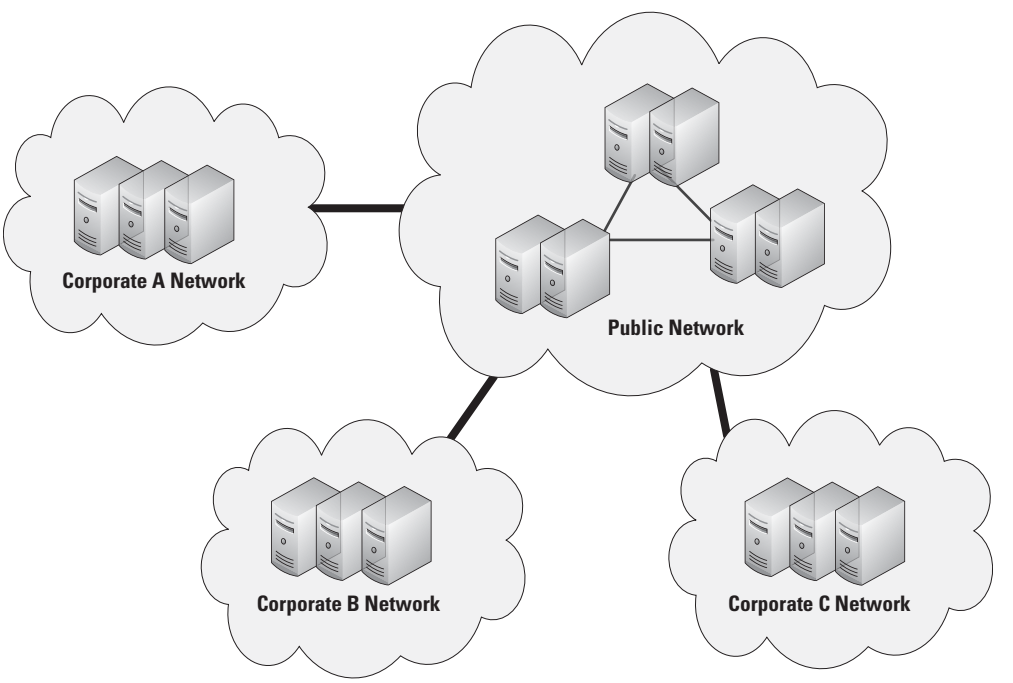
With the public cloud, you pay only for the resources you consume. For example, with IaaS, you can increase the number of processors, the amount of memory, the amount of network throughput, or the amount of data transfer. With SaaS, you pay for the number of licenses based on the number of users who need to use the services. In addition, the public cloud offers quick deployment, rapid capacity scaling, and all services are delivered with consistent availability, resiliency, security, and manageability.

Using public cloud services such as OneDrive and Office 365 enable you to take advantage of hosted solutions. This means users have the ability to access their information from anywhere at any time across multiple devices. By using cloud-based services, users can collaborate via calendars, email, and through document sharing. From an administrative perspective, it means you gain access to services and programs without the additional overhead of maintenance and software upgrades.

The public cloud can be organized according to:

- **The *shared public cloud*:** As shown in Figure 1-1, the shared public cloud is used by multiple organizations and is hosted on an infrastructure, where the architecture, customization, and some of the security are designed and managed by the provider.

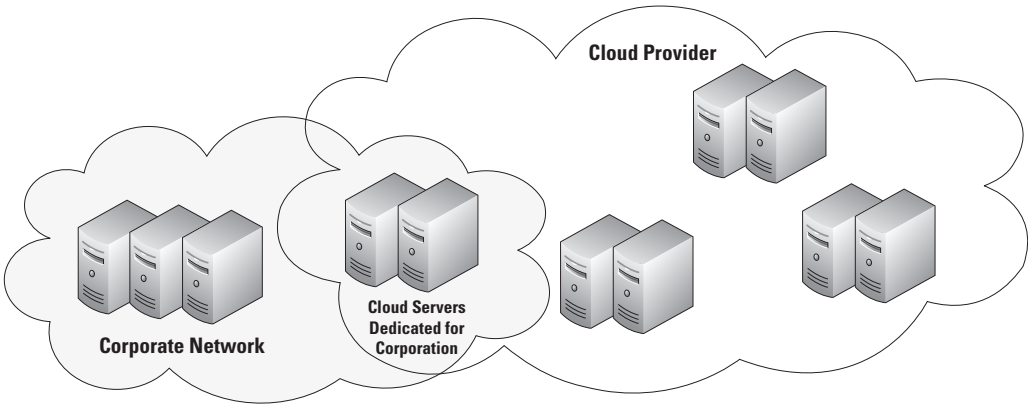
Figure 1-1
A shared public cloud is used by multiple organizations



- **The *dedicated public cloud*:** It's similar to the shared public cloud, but the cloud is delivered on a dedicated physical infrastructure (see Figure 1-2). While cost might be higher than that of the shared public cloud, the dedicated public cloud might offer better security, performance, and customization.

Figure 1-2

A dedicated public cloud is used by one organization



A ***private cloud*** offers the same features and benefits of a public cloud, but is contained within the corporate network and is controlled by the corporate IT department. The private cloud offers more security and privacy and allows for more control of its resources and data. Newer versions of Microsoft Hyper-V and VMware ESXi support creating and maintaining a private cloud.

A ***hosted private cloud*** is provided by a third-party company but is accessible only by users within a specific organization. In other words, the resources are leased or owned by the organization but are managed and located away from the organization. However, the hosted private cloud tends to be cheaper than the private cloud because some of the cost for the building, power, and personnel is distributed across several companies.

A ***hybrid cloud*** is a cloud-computing environment in which the organization provides and manages some of the resources in-house and a third party provides the hosted servers for the organization externally. In other words, it utilizes both a public cloud and a private cloud.

When you decide to use the cloud, you need to make sure that your use of the cloud is secure. This includes establishing privacy and compliance and determining how your data is secured.

Understanding How Cloud Services Manage Privacy

When you depend on online service providers, you are relying on online service providers to keep your data safe from loss, and theft as well as misuse from the third parties, other customers, employees of the hosting company, and even users within your own organization.

As more and more customers are relying on online service providers to keep their data safe from loss, theft, or misuse by third parties, other customers, or even the provider's employees, cloud services raise unique privacy questions for businesses. Organizations have legal obligations to ensure the privacy of their employees, customers, and clients.

Laws prohibit some data from being used for a reason other than the purpose for which the data was originally collected. In addition, when you collect and store data in the cloud, you are subject to legal requirements, such as the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act (GLBA), just as if you were storing data on premise. If you deal with European companies or customers, you will must adhere to EU privacy laws.

Before using the cloud, you should always read the privacy notices that specify how data is accessed by users and how it can be deleted or modified. In addition, you need to know where data is actually kept, how data is backed up, how often data is backed up, and where the backups are stored. In some instances, you might have data that cannot leave the country that it is intended for or cross the borders of other countries.

As previously mentioned, you need to consider how the hosting company handles disaster recovery and business continuity. You must ensure that backups are being done on a regular basis, data is being replicated to another site, and that the services are duplicated on another site.

You also must consider how the hosting company handles security breaches. You should read the cloud provider's disclosure policy and how quickly they will disclose the breach to you. In addition, there are laws that require you to ensure that you are informed promptly of any breaches.

Understanding How Compliance Goals are Met

Many organizations have regulations and policies that they must comply with to operate businesses in various industries. For example, when working in the health industry, you have to follow HIPAA. These policies can be quite complex based on the industry, the geographical location of the organization, as well as company-based policies. Further complicating matters is the fact that legal and regulatory bodies might change the responsibilities of both the cloud computing tenants and providers.

An organization that does not protect its data may be subject to a fine by one or more government or industry regulatory bodies. Some of these fines can be substantial, crippling a small or mid-sized business.

Laws or regulations typically specify who within an organization should be held responsible for data accuracy and security. For example, the Sarbanes–Oxley Act designates the CFO and CEO as having joint responsibility for the financial data, while the Gramm–Leach–Bliley Act specifies the responsibility for security lies within the entire board of directors. The United States Federal Trade Commission (FTC) requires a specific individual to be accountable for the information security program within a company.

If you store any of your data in the cloud, you must ensure that the cloud service provider follows all legal and regulatory requirements. Although the cloud is hosted by another company, it is still your responsibility to ensure these requirements are met. Before you sign any contract, you need to evaluate the specific needs and requirements. Then after the contract is signed, you need to take steps to ensure that compliance is maintained.

Understanding How Data is Secured at Rest or On-the-Wire

When running services and storing data on the cloud, you should follow the standard best practices for security as you would on any on-premise network. You should always use strong passwords you should ensure the passwords are changed regularly. You should always set rights and permissions for only what is needed and they should be reviewed on a regular basis. However, since data consists of confidential information, you should consider using encryption. You also need to perform auditing and monitoring.

Encryption is the process of converting data into a format that cannot be read by another user. Once a user has encrypted a file, it automatically remains encrypted when the file is stored on disk. ***Decryption*** is the process of converting data from encrypted format back to its original format. To help protect files on a computer, you can use encryption.

Symmetric encryption uses a single key to encrypt and decrypt data. Therefore, it is also referred to as secret-key, single-key, shared-key, and private-key encryption. To use symmetric key algorithms, you need to initially send or provide the secret key to both the sender and the receiver.

Asymmetric key, also known as ***public-key cryptography***, uses two mathematically related keys. One key is used to encrypt the data and the second key is used to decrypt the data. Unlike symmetric key algorithms, an asymmetric key does not require a secure initial exchange of one or more secret keys to both the sender and the receiver. Instead, you can make the public key known to anyone and use the other key to encrypt or decrypt the data. The public key can be sent to someone or it can be published within a digital certificate via a certificate authority (CA). Secure Socket Layer (SSL)/Transport Layer Security (TLS) and Pretty Good Privacy (PGP) use asymmetric keys.

For example, consider a scenario in which you want a partner to send you data. You send the partner the public key and the partner then encrypts the data with the key and sends you the encrypted message. You then use the private key to decrypt the message. If the public key is used by another user, that user still cannot decrypt the message because the user does not have the private key.

For data that is at rest (sitting on a disk somewhere on the cloud), you should encrypt the disks or files on the disks. If the system is running Windows, you can use EFS to encrypt individual files and folders or you can use BitLocker to encrypt an entire volume. By encrypting the data, you will limit access to only those who have the correct keys to unlock the files. It will also help protect the data if the system is compromised or if the system is being disposed of and the disks will no longer be needed.

For the encryption to be effective, however, you need to use longer keys (2,048 bits minimum, but 4,096 bits would be better). You should also keep your own keys and store the keys off the cloud provider's premises. Therefore, if the cloud systems are compromised, they will still not have access to the keys. In addition, by using encryption and not providing the keys to the cloud, providers will prevent the cloud provider from accessing the data. Lastly, a cloud provider managing your keys could be compelled to give up your key—if ordered by a government body, court, or law enforcement agency without your knowledge.

When you browse the web, there are times when you need to transmit important data (such as credit card numbers, social security numbers, and so on). You should do so using SSL over http (https), which encrypts the data. By convention, URLs that require an SSL connection start with https instead of http.

Secure Socket Layer (SSL) uses a cryptographic system that uses two keys to encrypt data: a public key known to everyone and a private or secret key known only to the recipient of the message. The public key is published in a digital certificate, which also confirms the identity of the web server.

When you connect to a site that is secured using SSL using Internet Explorer 11, clicking the lock icon displays more information about the site, including the identity of the CA that issued the certificate (see Figure 1-3). For even more information, you can click the View Certificates link to open the Certificate dialog box.

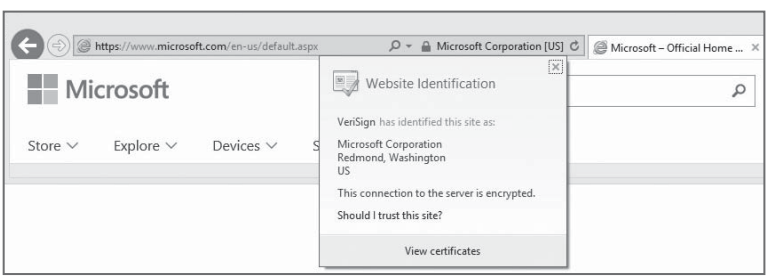


Figure 1-3

Viewing the SSL website identification in Internet Explorer 11

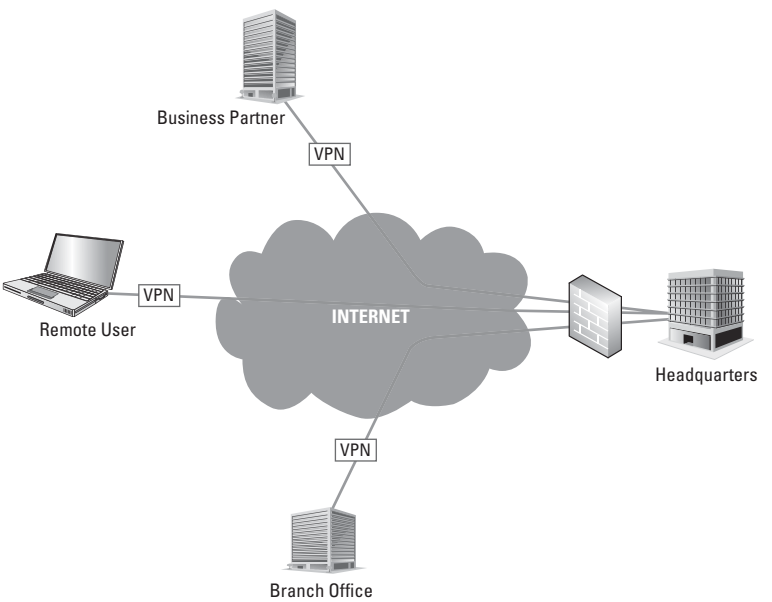
When visiting certain websites, Internet Explorer might find problems with the digital certificate (such as that the certificate has expired, it is corrupted, it has been revoked, or it does not match the name of the website). When this happens, Internet Explorer blocks access to the site and displays a warning stating that there is a problem with the certificate. You then have a chance to close the browser window or ignore the warning and continue on to the site. Of course, if you chose to ignore the warning, make sure you trust the website and you believe that you are communicating with the correct server.

Transport Layer Security (TLS) is an extension of SSL, which is supported by the Internet Engineering Task Force (IETF) so that it could be an open, community-supported standard that could then be expanded with other Internet standards. While TLS is often referred to as SSL 3.0, it does not interoperate with SSL. While TLS is usually default for most browsers, it has a downgrade feature that allows SSL 3.0 to run as needed.

Virtual Private Network (VPN) is a technology that uses encrypted tunnels to create secure connections across public networks like the Internet. There are a variety of uses for this technology, but three of the most common are shown in Figure 1-4.

Figure 1-4

Uses for VPN technology



VPNs are commonly used by remote employees for access to internal networks; VPNs create secure network-to-network connections for branch offices or business partner connections. A fourth use is to create secure host-to-host connections for additional security and isolation on an internal network. VPNs utilize encryption and authentication to provide confidentiality, integrity, and privacy protection for data. VPN tunnels can be used to connect an organization's data center to the cloud, or to connect one cloud to another.

Of course, when looking at security, you still need to follow the basics. Therefore, you need to consider the following:

- Perimeter security
- Hypervisor security
- Storage security
- Configuration and change management

This includes assessing the security of firewalls and the security of the operating system running the virtual servers. You also need to look at what can connect to a storage logical unit number (LUN), which are the storage units that are used by the virtual machines to create virtual disks. If a program or service has direct access to the LUNs, the program or service also has access to the data stored on the LUNs. Lastly, you need to ensure that you control and

review changes to the system by using configuration and change management so that changes do not negatively affect the services.

While you have encryption to help protect the data, you need to establish an audit policy and enable auditing so that when data (individual files and database records) is accessed, a record is created in the logs. You can then review the logs whenever necessary to determine whether data was accessed improperly or without your knowledge.

Lastly, you should analyze data access patterns, looking for anomalies. For example, if you have large amounts of data being pulled at night or weekends (when data traffic should be light), it might indicate that someone has compromised your system and is downloading content. In addition, you should look for network packets that don't belong; it might indicate that someone has accessed your system or is attempting to access your system.

Understanding How Data and Operations Transparency Requirements are Met

When moving to the cloud, you must also ensure transparency from your cloud provider regarding security and compliance measures that the provider users to protect your sensitive information and intellectual property. ***Transparency*** deals with honesty, openness, and accountability. You must know how individual virtual machines are segregated from other tenant virtual machines. In addition, you must know how the data is protected and how networks are secured.

When dealing with transparency, you should assess the following:

- Where does your data actually reside?
- Who has access to your data?
- Do you have visibility to the actual availability of your servers and services, including where there are changes to your service?
- How is the uptime guaranteed?

As part of assessing transparency, you need to know where your data is located. If you have confidential or intellectual property, you may require that data remains within the country. You should also check to see how backups are performed and where those backups are located.

As you recall, a public cloud is used to service multiple customers who are referred to as tenants. Therefore, if the cloud provider has a physical server with 10 different virtual servers for 10 different customers, you need to ensure that one customer cannot access other virtual machines and the data that resides on those virtual machines.

You also need to know if the data is accessible to the cloud provider's employees. For example, the provider might encrypt all data in its cloud environment, which ensures that its employees cannot access the data. Of course, you should also be concerned with how the employees of the provider are screened.

With any cloud technology, you need insurance that the server and services will be available at least 99.9% of the time. Therefore, you should see what tools the provider provides to its tenants to monitor the servers and services on the cloud. One such tool is NewRelic, which can show performance over a period of time (which can be valuable in diagnosing performance issues). To help ensure availability, you might need to use your monitoring tools so that you can be immediately notified when a server or service is not available.

The cloud provider should be transparent regarding service disruptions or poor performance and you must have clear SLAs, including an SLA for availability/uptime, application response time, application throughput, incident-response time, and problem-resolution time. The cloud provider should also provide access to logging and root-cause analysis of service problems at no additional cost. The provider should also have an easy method by which it can escalate issues when problems are found.

■ Understanding How a Cloud Service Stays Up to Date and Available

THE BOTTOM LINE

Just like any server or services that you operate, the server and services hosted on the cloud have a lot in common. You need to keep the system up-to-date so that security patches and other critical updates are applied, keeping the system secure and running smoothly. You should also understand that from time to time, you will want to upgrade or improve the server or service that is running. Because updates or improvements can create downtime, you need to develop a plan to accommodate these updates and improvements and avoid or minimize downtime.

CERTIFICATION READY
Describe how a cloud service stays up to date and available
1.3

Although the cloud has been available for some time and the cloud capabilities are still growing, there have been some significant outages from big cloud providers. Therefore, you need to thoroughly review the agreement between your organization and the cloud provider.

Understanding the Service/Feature Improvement Process

As with services and applications that run on on-premise networks and servers, there will come a time that the infrastructure, server, or application on the cloud will have to be upgraded or a feature will have to be added. If a service or feature is being upgraded by the host provider, you need to understand how the SLA addresses those improvements.

There are two types of service and feature improvements. In one scenario, the service and feature improvement is completed by the cloud provider. When this occurs, you should be notified before the service and feature is upgraded or improved so that you have an opportunity to review what is being done. You then evaluate those changes so that you can determine whether the changes will adversely impact any of the functionality of the service that you are hosting with the provider. Ideally, you should have a test/dev environment that can be upgraded first, so that you can thoroughly test the changes before they are implemented in a production environment. Of course, if something goes wrong, be sure you know how you can report it immediately to the hosting provider.

In the second scenario, the provider is providing an infrastructure or a server and you are upgrading or improving the service and feature. You need to perform the upgrades on a test/dev server so that you can test the changes before applying those updates to production. As part of the upgrade plan, you need to have a plan in place to quickly roll back those changes should something not function as expected.

Monitoring Service Health, Service Maintenance, and Future Roadmap Publishing

As with any network and/or servers that provide critical and important services, you need to determine the health of the services or servers located on the cloud. Some cloud providers will have a web-based console that will allow you to review the status of the server or service that is hosted on the cloud. However, since the customer is responsible for the service or service, you should also place other monitoring tools, such as System Center 2012 R2/2016 Operations Manager and System Center Global Service Monitor.

System Center 2012 R2/2016 Operations Manager is the part of the System Center suite that is the primary tool for monitoring an enterprise environment. You can monitor multiple computers, devices, services, and applications using the Operations Manager console. However, if you want to monitor the health of a server, you might need to have a VPN connection to the cloud so that Operations Manager can communicate fully with the server.

Operations Manager enables you to check the health, performance, and availability of all monitored objects and helps you identify and resolve problems. In addition, it records the events, availability, and performance so that you can look at a system's history and identify trends. Since it can monitor Windows machines, UNIX machines, Linux machines, and network equipment, it is considered a cross-platform monitoring and alerting solution.

System Center Global Service Monitor is a cloud service that extends the capabilities of System Center 2012 R2/2016 by monitoring external web-based applications from multiple locations around the world. It is designed to show you what the customer experiences when running your web applications. It does not focus on the Internet or network problem; it focuses on the application or service performance and any problems.

To use Global Service Monitor, you must have System Center 2012 (or higher) Operations Manager installed. To test Web Application Availability Monitoring, you define the URL and specify the number of locations throughout the world you want to test from, the number of tests that you want to perform, and how often to perform the tests.

There are two kinds of monitoring types:

- Web Application Availability Monitoring (see Table 1-2) performs a test on one URL from one location.
- Visual Studio Web Tests (see Table 1-3) runs tests from the 15 external locations provided by Microsoft as part of the subscription.

Table 1-2

Test Parameters for Web Application Availability Monitoring

Test parameters	Description
Total tests	This provides the number of tests multiplied by the number of locations
Trial subscription	A trial subscription limits the total tests to 25 per subscription and 10 tests for each location
Paid subscription	A paid subscription allows up to five subscriptions per tenant, but the total number of tests is limited to 25 per subscription and 10 tests for each location
Minimum interval per test	Greater than or equal to five minutes
Global test timeout	30 seconds

When looking at the cloud provider's agreement, you need to also understand the provider's maintenance window, whereby the company may perform maintenance tasks, updates, and patching that may or may not temporarily take down your service.

Lastly, you should always review the cloud provider's future plans so that you are aware of any new technologies or features that you might be able to use in the future, and more importantly, you might be able to identify changes that could affect your systems and services.

Table 1-3

Test Parameters for Visual Studio Web Tests

Test parameters	Description
Total tests	This provides the number of .webtest files multiplied by the number of locations
Trial subscription	A trial subscription limits the total number of tests to 25 per subscription and a maximum of three tests for each POP location
Paid subscription	A paid subscription allows up to five subscriptions per tenant, but the total tests are limited to 25 per subscription and a maximum of three tests for each POP location
Minimum interval per test	Greater than or equal to five minutes
Maximum number of requests per web test	100
Maximum web test file size	100 KB
Download/response size limit per request	500 KB

Understanding Guarantees, Service-Level Agreements (SLAs), and Capping of Liability of the Cloud Service Provider

Although the cloud has much to offer, it's not unlike any other network, server, or on-premise service. An unforeseen problem or disaster can cause the service to be unavailable. Therefore, before you start using the cloud, you must take to time to thoroughly review the agreement between your organization and the cloud provider, particular when it comes to guarantees, SLAs, and capping of liability.

Cloud computing agreements are non-negotiable forms executed by the customer and the cloud provider. Cloud providers can argue that tailoring their service agreements to individual customers adversely affects the biggest advantages of cloud computing, but you have to review the agreement to understand guarantees, SLAs, and capping of liability and to make changes where needed. Many clients might be surprised to learn that a multi-day outage does not violate the applicable SLA of a cloud provider. While a hosting company advertises 99.9% uptime (meaning 8.76 hours of down time per year), you need to read the entire service agreement to see what the actual SLAs are.

When reviewing the agreement, you must assess the following:

- How does the cloud provider determine whether service levels are being achieved?
- Who is responsible for measurement?
- What exceptions apply to service-level performance?
- When the SLA is not met, what is the remedy for the deficiencies?
- What happens when maintenance (both scheduled and emergency) is performed?
- What happens when a third party targets your organization or the infrastructure that your organization is running on, which results in downtime?
- What happens when third-party system failures or services are not under the vendor's control?
- What happens when the service is brought down by acts of ware or natural disasters, such as earthquakes, floods, storms, tornadoes, or hurricanes?

For example, an SLA could set forth an uptime of 99.9%, so when you have an outage of three days, the cloud provider issues a credit of three days.

You should also look at indemnities that will help share the limitation of liability. For example, the agreement might limit the provider's indemnification responsibility for intellectual property infringement, violation of laws, gross negligence, theft or fraud, other intentional misconduct, death, personal injury and property damage (including data loss). Often these agreements have loopholes that will totally absolve the provider of any liability.

Remember, the SLA is designed to protect the service provider, not the customer. Some cloud providers will not release details of their SLAs without a signed non-disclosure agreement (NDA) in effect. For Office 365 and Azure, SLAs can be found on the Microsoft website.

■ Understanding the Different Types of Cloud Services

THE BOTTOM LINE

When defining the cloud, you need to think of cloud computing as a service-oriented model instead of a server-oriented mode. The cloud can provide three primary service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

CERTIFICATION READY
Describe the different types of cloud services
1.4

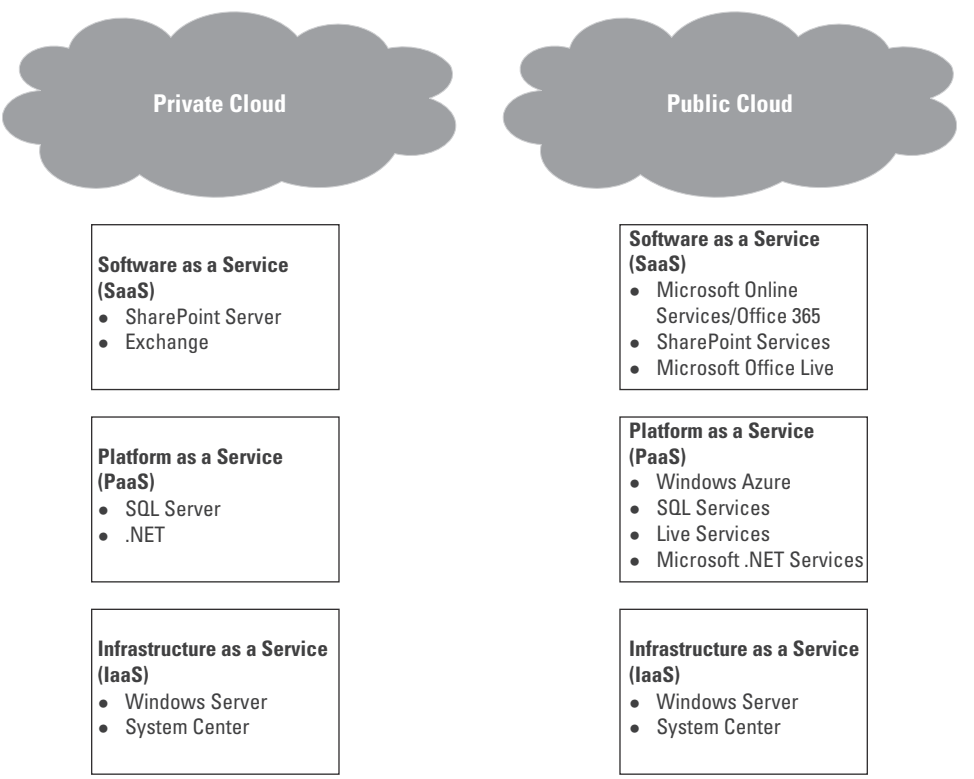
When you move to the cloud, you will need to determine which type of cloud deployment you want to use (public, private, or a hybrid cloud) and which service model that you want to implement (SaaS, PaaS, or IaaS).

Differentiating Between the Types of Cloud Services and Their Characteristics

The three primary types of cloud computing are SaaS, PaaS, and IaaS, which are made possible through virtualization. While SaaS is geared toward the end users of your organization, IaaS provides full access to virtual servers without having to maintain the equipment that they are running. PaaS lies between SaaS and IaaS (see Figure 1-5).

Figure 1-5

Comparing SaaS, PaaS, and IaaS



Software as a Service (SaaS) is the most basic form of cloud computing. It provides software and associated data (such as databases or user documents) that is hosted on the cloud. It is typically accessed by an application (such as a web browser) over the Internet. The users do not manage or control the cloud infrastructure, including network, servers, or storage. They may not even control the individual application's capabilities unless you are using a provider-defined, user-specific application. SaaS is sometimes referred to as on-demand software. The cost of SaaS is typically based on a usage-based model, where the consumer pays an agreed amount based on the use of the service or a monthly or yearly flat fee per user. Examples of SaaS include Hotmail, Gmail, Office 365, and Dropbox.

Platform as a Service (PaaS) goes one step further than SaaS. Instead of providing the applications, it provides the computing platform (such as networks, servers, and storage) on which the organization can host its own applications. PaaS allows the organization to focus on the developing and improving of the application without worrying about the infrastructure that it runs on. The two primary program languages for PaaS are Java and .NET. The cost of PaaS is typically based on usage of the platform, operating costs of the platform, and the agreed SLA. Examples of PaaS include Microsoft Azure, Amazon Web Services, and Google App Engine.

The Infrastructure as a Service (IaaS) service model provides the hardware for servers, storage, and networking—usually in the form of a standardized virtual server environment—and provides a foundation for PaaS and SaaS. The organization manages the guest operating system, the software, and the database application/servers. Cost is based on an agreed service level. While the hosting company mitigates the risks to the infrastructure, the organization assumes the responsibility for uptime of the cloud. Examples of IaaS include Amazon EC2, Microsoft Azure, Rackspace, and Google Compute Engine.

Integrating the Cloud with On-premises Services in Hybrid Scenarios

A hybrid cloud consists of a private cloud and a public cloud bound together. With the hybrid cloud, you can connect collocations such as an organization data center (private cloud) with a public cloud or by combining two public clouds. For example, you can store sensitive client data on the organization data center but host applications on a public cloud that will access the data center. Adopting the hybrid cloud requires consideration of a number of factors, such as data security and compliance requirements, level of control needed over data, and the application an organization uses.

Based on your requirements, the cloud can meet the following requirements:

- It can connect a private data center to a public or private cloud environment. By using a connection between the two, you can extend or scale the private data center into the cloud by moving specific workloads from the data center to the cloud (such as when demand for resources suddenly spikes).
- It can connect resources between clouds. By signing up for a SaaS to provide one service, you might need access to resources in another SaaS. For example, you can use customer relationship management product needs to connect to a human resource system or a back-office accounting system.
- It can implement a service that is hosted or controlled by a partner, such as when an organization needs to connect to a partner that is also using cloud-based service.
- Although the public clouds offer scalability, you might choose to use the private cloud because you want greater management and control.
- You might want to perform development and testing on one public cloud because of the support and options that it offers, but deploy it on a less expensive public cloud or a public cloud that is more reliable.

- It provides a solution when an organization does not want to become too reliant on one vendor or cloud provider. Therefore, you use another cloud provider to provide service redundancy.

When you are determining whether to implement a public or private cloud, you need to understand the cost associated with changing from the data center to the cloud:

- **Management:** By extending a data center to the cloud, you need to manage multiple environments: the on-premises data center and the cloud.
- **Data transfer:** The costs to transfer data to or from the cloud. If you have large amounts of data, you might need higher bandwidth to the cloud. In addition, some cloud services might charge based on bandwidth usage.
- **Customization and integration costs:** You might need to pay for the customization of an application so that it can work in the hybrid environment. Some of the applications might need to be rewritten.
- **Storage costs:** You will need to consider long-term storage costs needed locally and on the cloud.
- **Platform costs:** The cost of licensing for middleware or for software that provides services to software applications. Middleware may include web servers, application servers, and content management severs. You also need to consider how information will be accessed, such as accessing through Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), Web services, SOA, Web 2.0 infrastructure, and Lightweight Directory Access Protocol (LDAP).
- **Software maintenance costs:** The costs for licensing and support of software. Some licensing may be under a global usage deal while others may require a second set of licenses for systems on the cloud.
- **Compliance costs:** The costs to audit cloud services, including checking security and recovery procedures.
- **Server costs:** When you expand to the cloud, you might not significantly reduce the number of servers in your organization's data center (unless you move several servers to the cloud). However, while you might not reduce the number of servers, expanding to the cloud might allow your organization to avoid purchasing new servers for the data center.
- **Data center infrastructure costs:** When you remove a few servers, you still will not reduce the cost of the floor space used on the data center and will most likely not reduce costs for electricity and cooling.
- **Operational support personnel costs:** Costs can be reduced when you no longer have to pay for personnel because those duties are now being handled by the cloud provider.

To assist in calculating costs, some cloud providers will provide cost calculators to estimate charges and to calculate the total cost of ownership (TCO). Before moving to the cloud, you should determine whether you will actually save money by replacing your existing system or save money by not upgrading or adding to your current systems.

When you integrate a data center with the cloud or from one cloud to another, you might need to use:

- **Cloud-based tools:** Cloud-based tools might provide an application or web page that allows you to connect specific applications. For example, you might need database connectivity or you might need to transform data to or from a database or from one database to another.
- **Cloud-based solutions:** Cloud-based solutions can be used for data replication or to copy data from one source to another. Cloud-based solutions can also be used for backups to and from the cloud.

When you are considering a move to the cloud, you should follow these steps:

1. Assess your current IT strategy.
2. Consider your future technology needs.
3. Explore the different cloud computing options, best practices, and vendors.
4. Create a hybrid cloud strategy plan.
5. Plan for implementation.

When you evaluate your current IT strategy, you need to review the servers and services you are currently using and their respective loads. You also need to consider current limitations. You also need to evaluate your recent and current growth trends and assess where your technology needs over the next 3 to 5 years. By knowing where you are today and where you are headed tomorrow, you will be able to determine whether your current system is a good investment.

The next task is to research what is available to you. Evaluate several vendors so that you can compare options, costs, SLAs, and reputations. You should then be ready to design and implement a hybrid cloud strategy.

When working on these steps, be sure to include your business objectives. You should create a task force that includes your organization's IT and management leaders. You should also consider your ultimate objectives with cloud technology and how you will measure the services hosted in the cloud. Lastly, don't rush into the cloud—it's an important decision that must be evaluated and implemented with the greatest of care.

SUMMARY SKILL MATRIX

In this lesson you learned:

- The cloud is a network of services, and each server has different function.
- The cloud is a network of servers, and each server in the network has a different function. Some servers run applications or deliver a service.
- Capital Expenditures (CapEx) are funds used by an organization to acquire or upgrade physical assets such as servers, networking equipment, and storage. It also includes real estate such as buildings or data center space.
- Operating Expenses (OpEx) are the expenditures that an organization incurs while performing its normal business operations, including the amount of electricity consumed, the cost of employees to manage and support systems, office space, and Internet connections.
- The advantage of cloud services is that they provide a dynamic infrastructure that allows you to change the services provided based on the changing levels of demand. When planning for any service, including the cloud, you need to plan for capacity, scalability, redundancy, and availability.
- When you select a cloud deployment model, you will select a public cloud, a private cloud, a hosted private cloud, or a hybrid cloud (which is based on whether you want the cloud to be shared or dedicated or if you want it to be hosted internally or externally). When you select one of these methods, you will base your decision on cost, control, and scalability.
- Transparency deals with honesty, openness, and accountability. You must know how individual virtual machines are segregated from other tenant virtual machines. In addition, you must know how the data is protected and how networks are secured.
- When defining the cloud, you need to think of cloud computing as a service-oriented model instead of a server-oriented mode. The cloud can provide three primary service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

■ Knowledge Assessment

Fill in the Blank

Complete the following sentences by writing the correct word or words in the blanks provided.

1. The _____ provides services accessible from the Internet, such as a network application or server.
2. The subscription funding model is the same as _____.
3. The _____ between your corporation and the cloud provider will specify the level of availability for the provided services or services.
4. The _____ is provided by a third-party company that is accessible only by users within a specific organization.
5. When using a PKI to deploy digital certificates, you are using _____.
6. _____ deals with honesty, openness, and accountability when using the cloud.
7. If you want to monitor your cloud applications from multiple locations, you should use the _____.
8. The _____ service model provides the hardware for servers, storage, and networking—usually in the form of a standardized virtual server environment.
9. _____ allows several companies to use the same cloud products.
10. To protect an application running on the cloud that is accessible using a web browser, you should use _____ to encrypt data that is sent over the network.

Multiple Choice

Circle the letter that corresponds to the best answer.

1. Your corporation's data center has reached its capacity. Where should you temporarily run a new corporate application that requires several virtual machines?
   a. The cloud
   b. On a user workstation
   c. On four newly purchased servers
   d. Your data recovery site
2. Which cloud service should be used to run an application that is accessed using a web browser?
   a. SaaS
   b. PaaS
   c. IaaS
   d. NaaS
3. Which type of cloud service is Office 365?
   a. Storage services
   b. Productivity services
   c. Communications services
   d. Search services
4. Which type of cloud service is provided by Office 365?
   a. SaaS
   b. PaaS
   c. IaaS
   d. NaaS

5. Which pay model should be used with Office 365?
   a. Pay as you go
   b. Deferred
   c. Upfront CapEx/OpEx
   d. MaaS

6. You need to purchase several servers. Which funding model should be used for your corporation?
   a. Subscription
   b. Pay as you go
   c. OpEx
   d. CapEx

7. Which of the following allows you to change the cloud resources based on the required workload?
   a. Scalability
   b. Elasticity
   c. Availability
   d. Redundancy

8. You want to deploy an application to the cloud but you want to ensure that the actual data is stored in-house. Which type of cloud should be used?
   a. dedicated public cloud
   b. private cloud
   c. hosted private cloud
   d. hybrid cloud

9. Which of the following are advantages of cloud computing? (Choose all that apply)
   a. Improved resilience and agility
   b. Better control
   c. Server consolidation
   d. Reduced operational costs

10. Which type of cloud is delivered on a physical infrastructure that is used by a single organization?
    a. Hybrid cloud
    b. Shared public cloud
    c. Dedicated public cloud
    d. Floating public cloud

True / False

Circle T if the statement is true or F if the statement is false.

T | F **1.** The cloud is always less expensive than hosting an application or server yourself.

T | F **2.** When subscribing to Office 365, the costs will be classified as OpEx.

T | F **3.** Microsoft OneDrive is a PaaS.

T | F **4.** If you are hosting a private cloud via Microsoft Hyper-V, you should use System Center 2012 R2/2016 Operations Manager.

T | F **5.** The SLA will specify the limitation of liability for a cloud provider.

■ Case Projects

Scenario 1-1: Choosing a Type of Cloud

You are an administrator for the Contoso Corporation and your data center has reached its capacity. Your corporation is interested in using the cloud. You decide you want to expand your data center so that you can install additional servers to the cloud. Which kind of cloud (public or private, dedicated or shared, or hybrid) should be used to extend your data center and why?

Scenario 1-2: Choosing Types of Cloud Services

You are an administrator for the Contoso Corporation and you want to create a data recovery (DR) site on the cloud. Which type of cloud server should be used? Which features would you be looking to support for a DR site that can run your company applications and services if the primary site is not available?

Scenario 1-3: Comparing Costs

You are administrator for the Contoso Corporation and your data center has several servers running Hyper-V. Unfortunately, these servers are running at full capacity. Your corporation just formed a partnership with Litware.com and you need to deploy several virtual machines to run a corporate application that will be accessed by Litware. This partnership will be around for 8 months. You need to determine whether you want to run the servers on the cloud or within your data center. Describe how to determine which is the most cost effective method.

Scenario 1-4: Planning Your Cloud Deployment

You are an administrator for the Contoso Corporation and you are considering deploying a data recovery (DR) site to the cloud. If you do decide to use the cloud, you want to make sure that you plan and implement the cloud effectively. Describe the general steps you should take before you perform the implementation as well as what you should specify in the contract between your organization and the cloud provider.

2 LESSON

Enabling Microsoft Cloud Services

OBJECTIVE DOMAIN MATRIX

Technology Skill	Objective Domain Description	Objective Domain Number
Enabling Office 365 • Identifying the requirements and dependencies for using Office 365 • Selecting a cloud service plan for Office 365 • Signing Up for Cloud Services for Office 365 • Setting Up the Initial Configuration of Cloud Services for Office 365	Identify the requirements and dependencies for using Office 365 Select a cloud service plan (for Office 365) Sign up for cloud services (for Office 365) Set up the initial configuration of cloud services (for Office 365)	2.1 2.2 2.3 2.4
Enabling Microsoft Intune • Identifying the Requirements and Dependencies for Using Microsoft Intune • Selecting a Cloud Service Plan for Microsoft Intune • Signing Up for Cloud Services for Microsoft Intune • Setting Up the Initial Configuration of Cloud Services for Microsoft Intune	Identify the requirements and dependencies for using Microsoft Intune Select a cloud service plan (for Microsoft Intune) Sign up for cloud services (for Microsoft Intune) Set up the initial configuration of cloud services (for Microsoft Intune)	2.1 2.2 2.3 2.4
Understanding Microsoft Azure • Understanding Virtual Machines • Understanding Azure Services • Understanding Azure Disaster Recovery, High Availability, Redundancy, and Fault Tolerance	(None)	(None)

KEY TERMS

domain name
Domain Name System (DNS)
host
hypervisor
Microsoft Azure
Microsoft Azure Active Directory (Azure AD or AAD)

Microsoft Azure Fabric Controller (FC)
Microsoft Azure Site Recovery
Microsoft Intune
Microsoft Office 365
Microsoft Office 2016
Multi-Factor Authentication (MFA)
Office Web Apps
partition
resource record (RR)
second-level domains
top-level domains
virtual machine
Virtual Machine Manager (VMM)

You are the administrator for the Contoso Corporation, which has decided to implement both Office 365 and Microsoft Intune. Office 365 will be used to replace older versions of Office on your client computers. Microsoft Intune will help you manage several client computers that are used in homes and offices.

■ Enabling Microsoft Office 365

THE BOTTOM LINE

By deploying cloud computing services such as Microsoft Office 365, you can reduce the workload on your IT staff. You can also improve the collaboration between your team members.

Microsoft Office 365 is a Microsoft subscription-based software service that enables users to access their documents and collaborate with others from anywhere using their computers, the Internet, or their smart devices. Office 365 moves the traditional Office suite to the cloud. The service includes Office 365 apps (Word, Excel, PowerPoint, Outlook, OneNote, Access, and Publisher), Exchange Online, SharePoint Online, and Skype for Business Online. By using Office 365, you can offload many of the administrative tasks normally handled by your IT department. These tasks include managing software updates, patches, and service packs as well as purchasing additional server hardware to support company growth.

Administration is handled through a web portal/dashboard in which you can create/manage user accounts and oversee the health of all services. Microsoft also provides tools to migrate from your existing on-premise Exchange Server to Office 365.

The service can be used in combination with the desktop version of Office and also works even if you don't have Office installed on your computers.

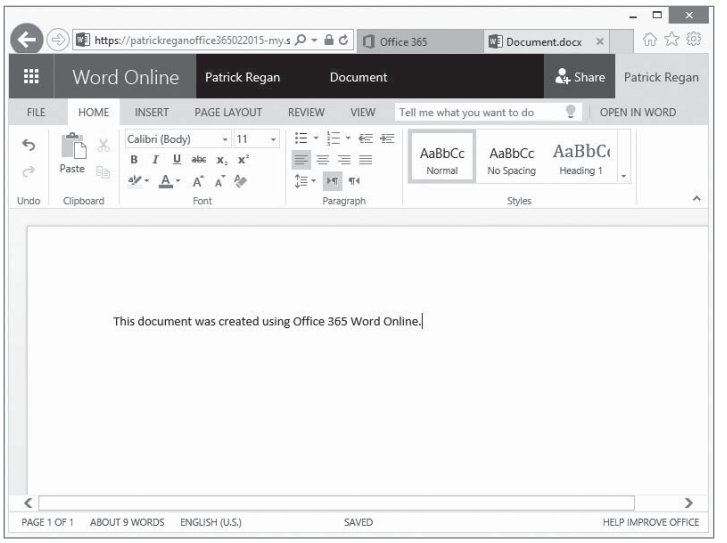
Office 365 is available in a number of different plans designed to meet different segments of the market. Each plan uses a per-user/month charge and provides access to either the entire service or only subsets of Office 365.

The following are features available with Microsoft Office 365:

- Users can access email, calendars, and contacts using the Microsoft Exchange service. The applications can be delivered to Outlook or Outlook Web Access.
- Users can create, edit, and store documents they create with ***Office Web Apps***, which are browser-based versions of the standard Office suite (Word Online, PowerPoint Online, and Excel Online), as shown in Figure 2-1. These documents are fully compatible with the desktop versions of Office.
- Users can set up and maintain a company website.
- Users can connect immediately with their co-workers via instant messaging by using Skype for Business.

- Users can set up and conduct online meetings (audio, video, and web conferencing), including the ability to share desktops, files, and presentations online.
- Users can share documents inside and outside of the organization and collaborate with their colleagues by using Microsoft SharePoint.

Figure 2-1
Using Word Online



From an administrative perspective, Office 365 offers several benefits:

- **Maintenance:** Microsoft performs the administrative tasks, so you do not have to manage backups, patches, and software updates for Office Online. However, if you install Office on the local computer, you will still have to manage backups, patches, and software updates.
- **Software upgrades:** Office 365 includes upgrades with the subscription price.
- **Hardware:** Because Office 365 runs in the cloud, you don't have to purchase and maintain expensive server hardware. You can migrate Exchange Server over to Office 365 while at the same time increasing the mailbox storage for users.
- **Collaboration on projects:** Using SharePoint as a document repository and collaboration workspace, you can connect and work with a geographically dispersed workforce. By using team sites, you can share a portfolio of company projects, enable employees to access project information, share documents, and collaborate on project documents.

Identifying the Requirements and Dependencies for Using Office 365

Office 365 is designed to work with the current or immediately previous versions of Internet Explorer or Firefox or the latest versions of Chrome or Safari. It also designed to work with any version of Microsoft Office in mainstream support. Of course, Microsoft always recommends that you use the latest browsers, Office clients, and apps. You should also install any Windows, Office, and browser updates.

CERTIFICATION READY
Identify the requirements and dependencies for using Office 365
2.1

Office 365 primarily uses IPv4. Although Office 365 does support IPv6, not all Office 365 features are fully enabled using IPv6. Some organizations restrict the client computers from connecting to the Internet. Since Office 365 is used over the Internet, you can open Office 365 help to get a list of what URLs or IP addresses that will need to be available for your users to use Office 365. Since the IP addresses assigned to a domain might change, it is recommended that

you use root domain names, such as the following partial list of domains, instead of IPv4 or IPv6 addresses:

- *.outlook.com
- *.microsoftOnline.com
- *.sharePoint.com
- *.office365.com
- *.office.com
- *.portal.office.com
- *.live.com

When configuring the corporate firewalls, clients, and on-premises services (such as Active Directory Federation Services), you should have access to the most up-to-date Root Certificate Authorities.

All connections to Office 365 are done over the Internet and are secured by SSL as appropriate. You will need the following ports open at your firewalls to access Office 365:

- **TCP 443:** AD FS (federation server role), AD FS (proxy server role), Office 365 portal, Office 365 My Company Portal, Outlook 2010 and Office Outlook 2007, Microsoft Entourage 2008 for Mac Exchange Web Services/Outlook for Mac 2011, Outlook Web App, and SharePoint Online
- **TCP 25:** Mail routing
- **TCP 587:** Simple Mail Transfer Protocol (SMTP) relay, which is used by SMTP Relay with Exchange Online
- **TCP 143/993:** Simple IMAP4 migration tool
- **TCP 995:** POP3, which is used with Exchange Online
- **TCP 80 and 443:** Used by Azure Active Directory Sync tool, Simple Exchange Migration Tool, Simple IMAP Migration Tool, Staged Exchange Migration Tool, Exchange Management Console, Exchange Management Shell, and Office 365 ProPlus

Office 365 does not have an operating system requirements. However, you should only use operating systems that include mainstream support. While Microsoft does not block Office 365 to operate with older operating systems, functionality might be diminished or might not operate as expected. In addition, based on the Microsoft Service Pack Lifecycle Support Policy, you should install Office Service Packs within 12 months of release.

Using Office 365 will most likely increase your organization's Internet traffic. Email traffic, directory synchronization, and Exchange hybrid deployments will have the most impact on bandwidth. As with any cloud product, you will need to consider the following when estimating network traffic:

- The Office 365 service offerings being used
- The number of client accessing Office 365 at one time
- The type of task each client computer is performing
- The client's network connections and current traffic patterns
- The organization's network topology
- The capacity of network links and network hardware

To help you prepare for an Office 365 deployment, you can use the following tools:

- **Exchange Client Network Bandwidth Calculator:** Used predict the network bandwidth requirements for a specific set of clients.
- **OneDrive for Business Synchronization Calculator:** A calculator used to estimate the bandwidth that a OneDrive for Business client deployment will require.

- **Office 365 Network Analysis Tool:** Helps analyze network-related issues prior to deploying Office 365 services.

Lastly, to access the Office 365 services over the Internet, client computers will have to use DNS to translate IP addresses. However, for efficiency and higher security, clients can use local DNS servers, which will then perform queries over the Internet.

Selecting a Cloud Service Plan for Office 365

Office 365 offers several plans designed for small, midsize, and enterprise-level businesses. The Office 365 Business (300 users) plan and the Office 365 Enterprise E3 and E4 (unlimited users) plan includes a subscription for Office 2016 for up to five PCs/Macs.

CERTIFICATION READY
Select a cloud service plan (for Office 365)
2.2

Microsoft Office 2016 includes desktop versions of the following applications:

- Access 2016
- OneNote 2016
- Excel 2016
- Word 2016
- Outlook 2016
- PowerPoint 2016
- Publisher 2016
- OneDrive Pro 2016
- Skype for Business Online

Unfortunately, if you want to install an older version of Office, Office 365 does not provide for a downgrade installation.

Based on the plan that you choose, you can get some or all of these.

Some of the Office 365 licensing plans include the following:

- **Personal:** Includes Word, Excel, PowerPoint, OneNote, Outlook, Publisher, and Access for home/non-commercial use on one computer (PC or Mac) plus access to premium features on one tablet or phone. It also gives 1 TB of additional OneDrive storage and 60 minutes of Skype international calls per month.
- **Home:** Targeted for mainstream consumers and families. It has the same features as Personal except that it can be used on as many as five devices by up to five users.
- **ProPlus:** Offers access to the Office 2016 Professional Plus applications for up to 25 users on up to five devices per user.
- **Business Essentials:** Targeted for small businesses. It offers access to hosted Exchange, SharePoint, and Skype for Business Online services only.
- **Business:** Offers desktop apps for both Macs and PCs for as many as five computers per users.
- **Business Premium:** Combines Business Essentials and Business to include hosted Exchange, SharePoint and Skype for Business Online services, with desktop apps for Macs and PCs.
- **Enterprise (E3):** Offers access to all Office applications, hosted Exchange, and SharePoint, with enterprise-specific legal compliance features and support.
- **Enterprise (E4):** Offers everything that E3 offers as well as Enterprise voice/enterprise calling capabilities.

Office 365 manages the licenses for Office 2016 through an online portal by indicating which Office 365 users have the ability to install the program during the setup of the user's account.

In the Office 365 portal, you can delete a user to free up a licenses, remove a license from a user if his job changes, or assign a license for a user after the account is set up. You can also review which licenses are assigned to a user and purchase more if necessary.

Signing up for Cloud Services for Office 365

CERTIFICATION READY
Sign up for cloud services (for Office 365)
2.3

A ***domain name*** represents the online identity of companies or individuals. You can use your domain name in Office 365 with your emails, public websites, and SharePoint sites.

When you sign up with the service, you start with two initial domains: the onmicrosoft.com domain and a SharePoint Online domain. The <domainname>.onmicrosoft.com domain, such as contoso.onmicrosoft.com, will be used with most Office 365 services, including your Office 365 email addresses and team sites. You cannot rename your initial domains after sign-up, but you can add domains to your Office 365 account.

When you sign up for Office 365, you have to define a user ID, such as JSmith@contoso.onmicrosoft.com or John.Smith@onmicrosoft.com. You can keep using this domain for your user ID or you can add your organization domain names.

Many businesses would rather use their own domains for email addresses and public websites. However, this requires a Small Business, Midsize Business, or Enterprise version of Office 365. Therefore, if you own the contoso.com domain, you can then assign contoso.com for the email addresses and the public website (such as contoso.com and www.contoso.com).

X REF
Administrator roles are covered in greater detail in Lesson 3.

The first account created is assigned the global administrator role. A global administrator is the administrator of the Office 365 portal. He can manage service licenses, users and groups, domains, and subscribed services. He is also a SharePoint Online administrator.

The user ID that you create when you sign up includes the domain, as in alan@contoso.onmicrosoft.com. You can continue using this domain for your user ID and for other users that you add to your subscription. Some users do this while they're using a trial version.

Microsoft has multiple data centers throughout the world. When you sign up for an Office 365 account, you have to select a country or region, which determines the primary storage location for the customer's data. For example, if you sign up for an account in North America, at this time, the primary data centers are located in the United States. If you are accessing the online services portal from a region other than North America, the web pages you are viewing will be hosted in that region's data center. For the Asia-Pacific region, data centers are kept in Hong Kong and Singapore. To determine where the data is stored, search the Microsoft website for "Office 365" and "Where is my data?"

SIGN UP FOR OFFICE 365

GET READY. To sign up for Office 365, perform the following steps on a computer running Windows 10 with a connection to the Internet.

1. On Win10A, log on using the **contoso\administrator** account and the **Pa$$word** password.
2. On the Taskbar, click the **Microsoft Edge** icon to open Microsoft Edge.
3. Go to **http://office.microsoft.com/en-us/business/**.
4. Click **See plans & pricing**, and click **See more plans & pricing**. Review the plans; evaluate the differences between the Business plans and the Enterprise plans.
5. At the top of the window, click the **Office 365 Enterprise E4** option and review the options offered by Office 365 Enterprise E4.
6. Near the top of the window, click the **Free trial with Office 365 Enterprise E3** option.

7. Click **Free trial**.
8. On the Let's get to know you page, enter the following information:

   First Name: <Your first name>

   Last Name: <Your last name>

   Email: <Your email address>

   Phone: <Your phone number>

   <FirstName><LastName>Office365<Month><Year>

   Therefore, if your name is John Smith and you are performing this lab in June 2015, you would type the following:

   JohnSmithOffice365062015, which produces a login domain of

   JohnSmithOffice365062015.onmicrosoft.com

   Click **Next**.
9. On the Create your user ID page, for the User ID, type the following:

   <FirstInitial><LastName>

   Therefore, if your name is John Smith, you would type the following:

   JSmith
10. Ensure the domain name uses the following format:

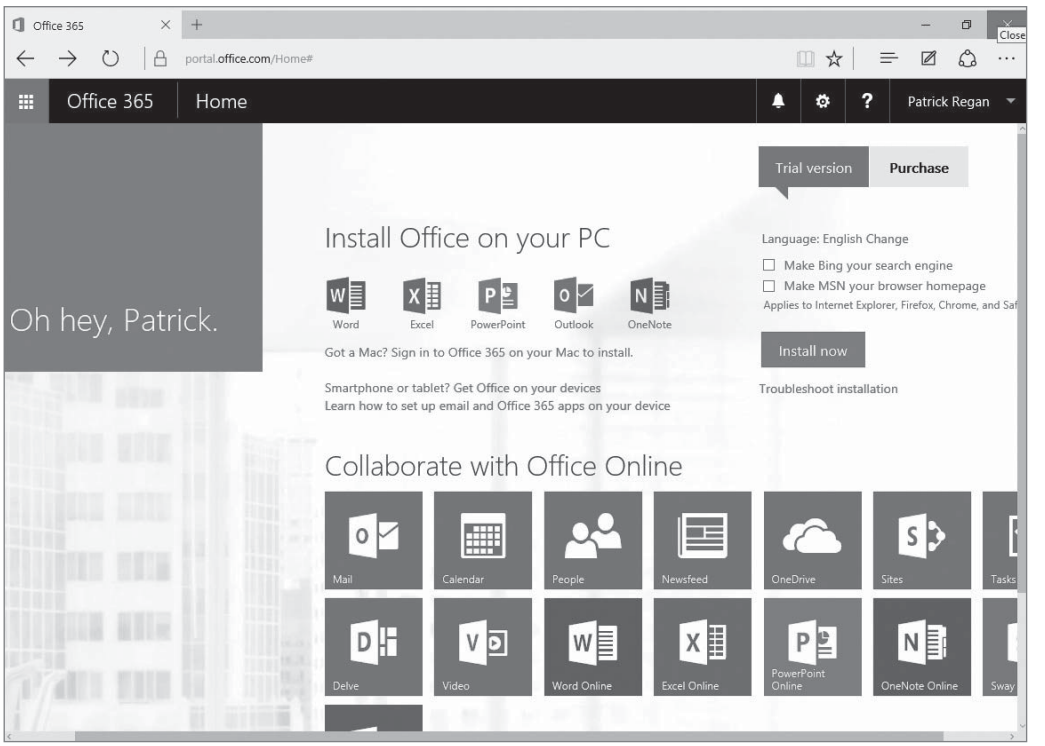
    <FirstName><LastName>Office365<Month><Year>

    Therefore, if your name is John Smith and you are performing this lab in June 2015, you would type the following:

    JohnSmithOffice365062015.
11. For the Password text box and the Confirm password text box, type **Pa$$w0rd**.
12. On the Prove. You're. Not. A. Robot page, select **Send text message**. Then type your phone number in the appropriate text box.
13. Click **Create my account**.
14. If a Don't lose access to your account dialog box displays, type a phone number (preferably a mobile number) and then click **Save and continue**.
15. In the Enter your verification code text box, type the code that you receive from your phone and click **Create my account**.
16. On the Save this info page, the Office 365 sign-in page is https://portal.office.com. Be sure to record your Office 365 user ID. Click the right arrow.
17. On the Don't lose access to your account page, specify a mobile phone number and alternate email address, which can be used to reset your password. Click **Save and continue**.
18. On the Install Office on your PC page (as shown in Figure 2-2), click **Install now**.
19. When you are prompted to run or save the executable file, click **Run**.
20. In the Welcome to your new Office window, click **Next**.
21. On the First things first page, click **No thanks** and then click the **Accept** button.
22. On the Meet OneDrive page, click **Next**.
23. On the Welcome! page, click **Next**.
24. On the Take a look at what's new page, click **No, thanks**.
25. When the installation completes, click **All done**.
26. Click the Office 365 settings button (the gear button at the top-right corner of the webpage) and then click **Office 365 settings**.
27. Scroll to the bottom of the window to view the assigned licenses. Then click **Save**.

Figure 2-2

Installing Office 2016 from Office 365



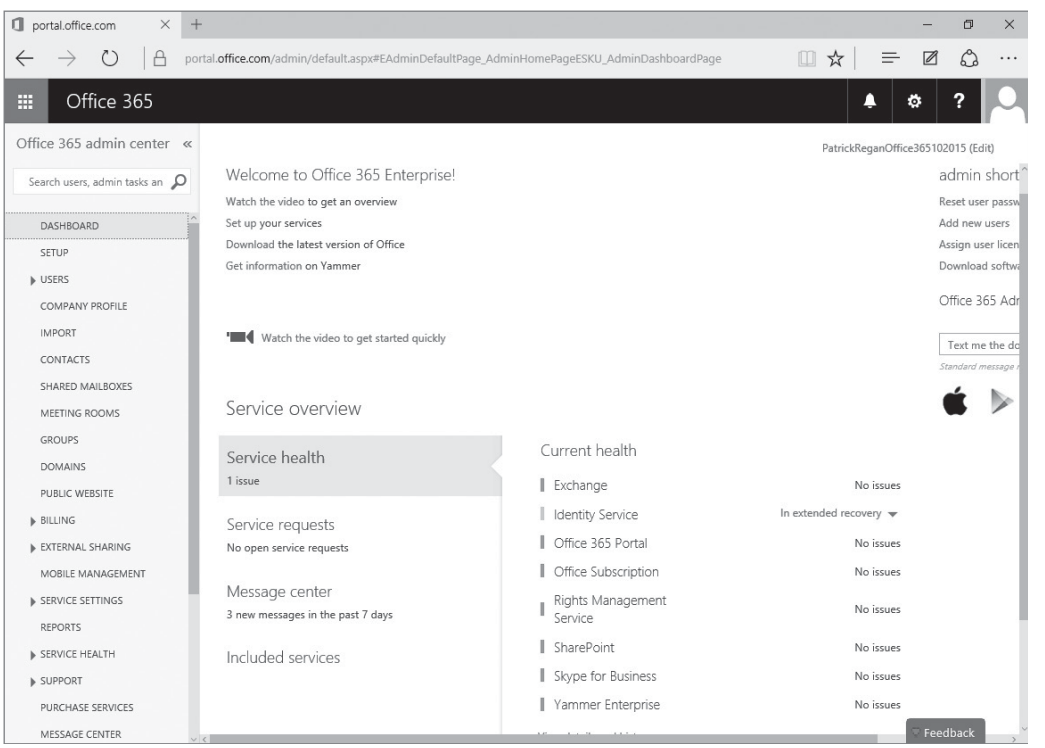
Setting up the Initial Configuration of Cloud Services for Office 365

CERTIFICATION READY
Set up the initial configuration of cloud services (for Office 365)
2.4

To manage the Office 365 services, you will open the Office 365 portal (https://portal.office.com) and click the Admin button to launch the Office 365 Admin Center, as shown in Figure 2-3.

Figure 2-3

Managing Office 365 with the Office 365 Admin Center



Domain Name System (DNS) is a naming service that is used by a Transmission Control Protocol / Internet Protocol (TCP/IP) network and is an essential service used by the Internet. Every time a user accesses a web page, she must type a URL. Before the client communicates with the web server, the client computer needs to use DNS to retrieve the IP address of the web server, similarly to someone using a phone book to find a phone number. When an enterprise client needs to communicate with a corporate server, the enterprise client also uses DNS to find the IP address of the corporate service. The DNS servers are often referred to as name servers.

TCP/IP is the most popular networking protocol suite used in the world and is the same protocol used with the Internet. Of course, the Internet is a worldwide network that links billions of computers. For a client computer or host to communicate on a TCP/IP network, a client must have an IP address.

Traditional IP addresses based on IPv4 featured a four-byte address written in a four-octet format. Each octet ranges from 0 to 255. An example of an IP address is 24.64.251.189 or 192.168.1.53. Most users would have difficulty remembering hundreds of telephone numbers and hundreds of IP addresses. The Naming resolution infrastructure enables an administrator to assign logical names to a server or network resource by IP address and translates a logical name to an IP address.

DNS was developed as a system and a protocol to provide up-to-date name resolution. The benefits of DNS include the following:

- **Ease of use and simplicity:** Allows users to access computers and network resources with easy-to-remember names.
- **Scalability:** Allows the workload of name resolution to be distributed across multiple servers and databases.
- **Consistency:** Allows IP addresses to be changed while keeping the host names consistent, making network resources easier to locate.

A DNS resolver is a service that uses the DNS protocol to query for information about DNS servers using UDP and TCP port 53.

To register a top-level domain, which can be used for your email and website, you go to a domain registrar company and search for and purchase a domain. When you click DOMAINS from the Office 365 Admin Center, you can click Buy domain to check availability and eventually purchase a domain from GoDaddy. Figure 2-4 shows the Manage domains page. To keep the domain, you will have renew the domain from time to time, such as once a year or once every couple of years.

DNS is a hierarchical system consisting of a tree of domain names. At the top of the tree is the root zone (see Figure 2-5). The tree can then be organized into zones, each served by a name (DNS) server. Each zone can contain one domain or many domains. The administrative responsibility over any zone can be delegated or divided by creating a subdomain, which can be assigned to a different name server and administrative entity.

Each node or leaf in the tree is a ***resource record (RR)***, which holds information associated with the domain name. The most common resource record is the host address (A or AAAA), which lists a host name and the associated IP address.

A domain name consists of one or more labels. Each label can be up to 63 characters. The fully qualified domain name cannot exceed a total length of 253 characters.

The right-most label designates the top-level domain. For example, *microsoft.com* consists of two labels. The top-level domain is com. The hierarchy of domains descends from right to left. Each label to the left specifies a subdomain of the domain or label on the right. Therefore, in our example, *microsoft* is a subdomain of the *com* domain.

Figure 2-4

Managing domains

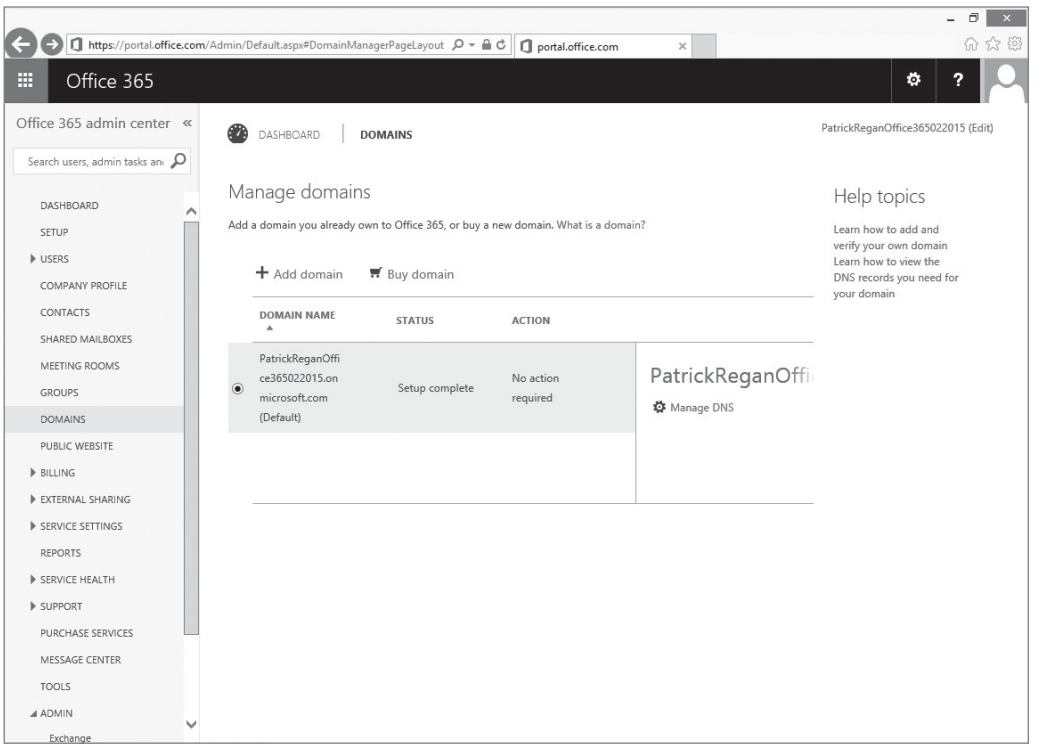
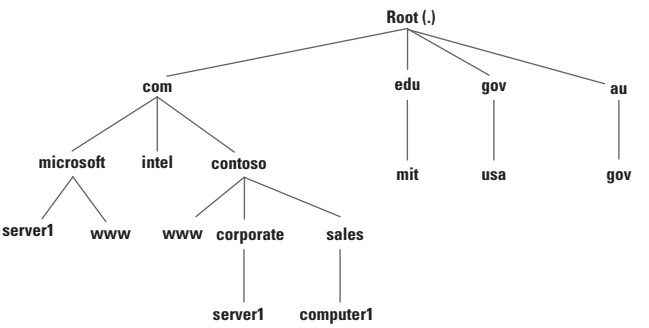


Figure 2-5

Distributing domain names through the DNS hierarchy system



Traditionally, ***top-level domains*** consist of generic top-level domains and international country codes (such as *us* for United States, *uk* for United Kingdom, *de* for Germany, and *jp* for Japan). Traditional generic top-level domains include the following:

.com	Commercial
.org	Organization (originally intended for nonprofit organizations)
.edu	Educational
.gov	U.S. governmental entities
.net	Network (originally intended for the portal to a set of smaller websites)

Over the years, many other generic domains have been added, such as aero, biz, coop, info, int, jobs, name, and pro. More recently, organizations can purchase their own top-level domains.

Second-level domains are registered to individuals or organizations. Examples include:

microsoft.com	Microsoft Corporation
mit.edu	Massachusetts Institute of Technology
gov.au	Australian government

Second-level DNS domains can have many subdomains, and any domain can have hosts.

A ***host*** is a specific computer or other network device in a domain. For example, *computer1.sales.contoso.com* is the host called *computer1* in the sales subdomain of the *contoso.com* domain. A host has at least one IP address associated with it. For example, www.microsoft.com represents a particular address.

If you have *server1.corporate.contoso.com*, *com* is the top domain. *contoso* is a subdomain of com, and corporate is a subdomain of *contoso*. In the *corporate* domain, you find one or more addresses assigned to *server1*, which as 192.168.1.53. So as a result, when you type *server1.corporate.contoso.com* into your browser, the client sends a query to a DNS server asking what the IP address is for *server1.corporate.contoso.com*. The DNS server responds back with the 192.168.1.53 address. The client then communicates with the server with the address of 192.168.1.53.

A DNS zone database is made up of a collection of resource records, which are used to answer DNS queries. Each resource record (RR) specifies information about a particular object. Each record has a type, an expiration time limit, and some type-specific data.

When you create a user account, certain properties define the user account, such as first name, last name, and login name. When you define a printer in Active Directory, you define a name of the printer and a location. A printer does not have a first name or a last name. Just as you have different types of objects in Active Directory, you also have different types of resource records in DNS, with different fields.

When you create a new zone, two types of records are automatically created:

- **Start of Authority (SOA) record:** Specifies authoritative information about a DNS zone, including the primary name server, the e-mail of the domain administrator, the domain serial number, and the expiration and reload timers of the zone.
- **Name Server (NS) record:** Specifies an authoritative name server for the host.

You have to add additional resource records as needed. The most common resource records are:

- **Host (A and AAAA) record:** Maps a domain/host name to an IP address.
- **Canonical Name (CNAME) record:** Sometimes referred to as an Alias, maps an alias DNS domain name to another primary or canonical name.
- **Pointer (PTR) record:** Maps an IP address to a domain/host name.
- **Mail Exchanger (MX) record:** Maps a DNS domain name to the name of a computer that exchanges or forwards e-mail for the domain.
- **Service Location (SRV) record:** Maps a DNS domain name to a specified list of host computers that offer a specific type of service, such as Active Directory domain controllers.

The PTR records in the reverse lookup zone and all of the other record types are in the forward lookup zone.

ADD A DOMAIN TO OFFICE 365

GET READY. To add a domain to Office 365, perform the following steps on a computer running Windows 10 with a connection to the Internet.

1. On Win10A, log on using the **contoso\administrator** account and the **Pa$$word** password.
2. On the Taskbar, click the **Internet Explorer** icon to open Internet Explorer and then open and sign into Office 365 (https://portal.office.com).
3. Click the **Admin** button and then click **DOMAINS**.
4. On the Manage domains page, choose **Add domain**.
5. Verify that you own the domain by creating a record at your DNS hosting provider or domain registrar.
6. On the Add users page, create the users with email addresses on this domain.
7. On the Set domain purpose page, select **Exchange Online**.
8. On the Set up domain page, the necessary DNS records that need to be added to your DNS zone will be displayed: For Exchange Online, you will need:
   - An MX record to route mail to Office 365.
   - A CNAME Autodiscover record so that email clients like Outlook can automatically discover the Office 365 server.
   - A TXT record to help prevent spam.
9. If necessary, on the Manage domains page, you change the default domain by naming by choosing the domain and then choose **Set as default**.

■ Enabling Microsoft Intune

THE BOTTOM LINE

Microsoft Intune is a cloud-based management solution that allows you to manage your computers when they are connected to or not connected to the corporate network. In fact, you don't even have to be part of your domain. Microsoft Intune helps you manage your computers and mobile devices through a web console. It provides the tools, reports, and licenses to ensure your computers are always current and protected. For mobile devices, it also allows you to manage your remote workforce by working through Exchange ActiveSync or directly through Microsoft Intune.

Microsoft Intune can be operated in cloud-only mode or in a new unified configuration option that integrates the cloud-based environment with Microsoft System Center 2012 Configuration Manager Service Pack 1 or System Center 2012 R2/2016 Configuration Manager. Microsoft Intune utilizes a subscription model in which you are charged on a per-user basis.

Here are some of the things you can do with Microsoft Intune:

- Manage your mobile devices and computers through a web-based console anywhere at any time through Exchange ActiveSync and System Center 2012 R2/2016 Configuration Manager.
- Manage your Microsoft Intune subscription, add new users and security groups, set up and manage service settings, and access service status via a Microsoft Intune Account portal.
- Assess the overall health of devices across your organization using the Microsoft Intune Administration console.

- Organize users and devices into groups (geographically, by department, and by hardware characteristics).
- Manage updates for computers in your organization.
- Enhance security of your managed devices by providing real-time protection, by keeping virus definitions current, and by automatically running scheduled scans.
- Access the overall health of your managed devices through the use of alerts.
- Deploy policies to secure data on mobile devices to determine which mobile devices can connect, enroll, rename, and un-enroll devices.
- Wipe mobile devices in case they are stolen.
- Deploy software and detect and manage software installed on computers.
- Manage licenses purchased through Microsoft Volume Licensing agreements.
- Run reports on software, hardware, and software licenses to help confirm current needs and to plan for the future.
- Provide a cloud-based, self-service portal where users can enroll and manage their devices, search for and install software applications, and request help.

Microsoft Intune deploys a client agent on each device that you want to manage. The Microsoft Intune agent communicates back to the Microsoft Intune administration console, allowing you to inventory software and hardware assets in your organization.

Microsoft Intune can be deployed with the following configurations:

- **Microsoft Intune Stand-Alone Cloud Configuration:** With this configuration, you have to administer your computers and devices (Windows 10, Windows 8/8.1, Windows RT, Windows Phone 8, Android, and Apple iOS) through the Administrator console. Although this configuration allows you to create and manage policies, inventory your devices, and upload and publish software, it does not support the discovery of mobile devices.
- **Microsoft Intune Cloud + On-Premise Configuration:** This configuration integrates Microsoft Intune with your existing Active Directory and Exchange environment. With this configuration, you can discover mobile devices using Exchange ActiveSync, synchronize your user accounts with your Active Directory, and manage your mobile devices through Microsoft Intune.
- **Microsoft Intune + System Center Configuration Manager:** This configuration allows you to manage your computers and mobile devices from the System Center Configuration Manager 2012 R2/2016 console.

Identifying the Requirements and Dependencies for Using Microsoft Intune

CERTIFICATION READY
Identify the requirements and dependencies for using Office 365 and Microsoft Intune
2.1

While Office 365 was a browser-based service, Microsoft Intune is used to manage devices. Therefore, Microsoft Intune requires that your firewalls will pass communications between the managed devices and your Microsoft Intune services.

To manage computers that are behind firewalls and proxy servers, you must set up firewalls and proxy servers to allow communications to access Microsoft Intune and related services. Although you should be aware of the fact that there are several websites necessary for Microsoft Intune, you don't have to memorize all of these for the exam:

- ***.manage.microsoft.com:** Port 80 and 443
- ***manage.microsoft.com:** Port 80 and 443

- **manage.microsoft.com:** Port 80 and 443
- ***.microsoftonline-p.com:** Port 80 and 443
- ***.microsoftonline-p.net:** Port 80 and 443
- ***.spynet2.microsoft.com:** Port 443
- **blob.core.windows.net:** Port 80
- **c.microsoft.com:** Port 80 and 443
- **c1.microsoft.com:** Port 80 and 443
- ***.googleapis.com1:** Port 80 and 443
- **wustat.microsoft.com:** Port 80 and 443

To access Microsoft Update Services, you will need to access the following:

- ***.update.microsoft.com:** Port 80 and 443
- **download.microsoft.com:** Port 80 and 443
- **update.microsoft.com:** Port 80 and 443
- ***.download.windowsupdate.com:** Port 80 and 443
- **download.windowsupdate.com:** Port 80 and 443
- ***.windowsupdate.com:** Port 80 and 443
- **windowsupdate.microsoft.com:** Port 80 and 443
- **ntservicepack.microsoft.com:** Port 80 and 443

To perform DNS lookup requests, you will need to access the following:

- **manage.microsoft.com.nsatc.net:** Port 80

To access documentation, Help, and support, users will need to access the following:

- ***.livemeeting.com:** Port 80 and 443
- ***.microsoftonline.com:** Port 80 and 443
- ***.social.technet.microsoft.com:** Port 80
- **blogs.technet.com:** Port 80
- **go.microsoft.com:** Port 80
- **onlinehelp.microsoft.com:** Port 80
- **www.microsoft.com:** Port 80

For the users to install Microsoft Intune client, they must have Internet connectivity and 200 MB available disk space. You can install the Microsoft Intune client on the following operating systems:

- Windows Vista Business, Enterprise and Ultimate
- Windows 7 Professional, Enterprise or Ultimate
- Windows 8/8.1 Pro or Enterprise
- Windows 10 Pro or Enterprise

To install the Microsoft Intune client, you will need administrative permissions on the client computer. In addition, you will need to have a minimum of Windows Installer 3.1. If you have any of the following incompatible client software, you will have to remove the incompatible client software:

- Any version of System Center 2016 Configuration Manager
- Any version of System Center 2012 Configuration Manager
- Any version of Configuration Manager 2007
- Any version of Systems Management Server

Lastly, the Microsoft Intune company portal website is supported by the default web browser for each supported platform including

- Internet Explorer 9 or later
- Google Chrome
- Mozilla Firefox

The more clients you have, the more total bandwidth you need. To install the client, you will consume the following:

- Intune client installation: 125 MB, One time
- Client enrollment package: 15 MB, One time

In addition, additional downloads include:

- Endpoint Protection agent: 65 MB, One time
- Operations Manager agent: 11 MB, One time
- Policy agent: 3 MB, One time
- Remote Assistance via Microsoft Easy Assist agent: 6 MB, One time

Additional downloads are possible when there are updates for this content type.

- Daily client operations: 6 MB, Daily
- Endpoint Protection malware definition updates: Varies, but typically 40 KB to 2 MB, Daily, up to three times a day.
- Endpoint Protection engine update: 5 MB, Monthly

In addition, you will need to plan for Windows and software updates and software distribution.

Selecting a Cloud Service Plan for Microsoft Intune

CERTIFICATION READY
Select a cloud service plan
2.2

Compared to Office 365, a Microsoft Intune subscription is licensed on a per-user basis. Therefore, if you need to add more users, you just buy additional licenses. If you need to reduce the number of subscriptions, you just reduce the number of licenses.

According to the official Microsoft Intune site, the subscription for Microsoft Intune include the following:

- System Center 2012 R2 (or higher) Configuration Manager
- 20 GB of storage for application distribution
- Software distribution
- PC Endpoint Protection
- Software licensing inventory reports
- Hardware inventory reports
- Mobile device app publishing
- Alerts and monitoring
- Security policy management
- 99.9% scheduled uptime service level agreement
- Best-in-class support

Signing up for Cloud Services for Microsoft Intune

CERTIFICATION READY
Sign up for cloud services (for Microsoft Intune)
2.3

When you sign up for Microsoft Intune, you are assigning a domain name, to which onmicrosoft.com will be added as a suffix. Therefore, if you define contoso, your domain name would be contoso.onmicrosoft.com. Similar to Office 365, after you complete the sign-up process, you cannot change the domain name. However, also like Office 365, you can add your own custom domain names to Microsoft Intune.

Before you create new user accounts or synchronize accounts from your Active Directory, you should decide whether you are going to use the .onmicrosoft.com domain or add your custom domain name. If you do not configure a custom domain name and suffix, each user account receives the onmicrosoft.com suffix for her user principal name (UPN).

The first user created will be a tenant administrator and service administrator for Microsoft Intune. The tenant administrator manages the subscription, including billing, cloud storage, and managing the users who can use Intune. The service administrator performs the day-to-day tasks, including managing mobile devices or computers, deploying policy or software, and running reports.

SIGN UP FOR MICROSOFT INTUNE

GET READY. To sign up for Microsoft Intune, perform the following steps on a computer running Windows 10 with a connection to the Internet.

1. On Win10A, log on using the **contoso\administrator** account and the **Pa$$word** password.
2. On the Taskbar, click the **Microsoft Edge** icon to open Microsoft Edge.
3. Open the **http://www.microsoft.com/en-us/server-cloud/products/microsoft-intune/** website. Click **Try Now**.
4. On the signup page, type the following information:

   Country or Region: <Your country or region>

   Organization language: <Your language>

   First Name: <Your first name>

   Last Name: <Your last name>

   Organization: <Your last name> Corporation

   Address: <Your street address>

   City: <Your city>

   State: <Your state>

   Zip code: <Your zip code>

   Phone number: <Your phone number>

   Email address: <Your email address>
5. In the New domain name text box, type the following:

   <FirstName><LastName>Training<Month><Year>

   Therefore, if your name is John Smith and you are performing this lab in June 2015, you would type the following:

   JohnSmithTraining062015 (in front of *.onmicrosoft.com*)
6. Click **Check availability**.

7. In the New user ID text box, type your first initial and last name. Therefore, if your name is John Smith, type JSmith.
8. For the Create new password text box and the Confirm new password text box, type **Pa$$w0rd**.
9. In the Verification text box, type the code displayed.
10. Click **I accept and continue**.
11. Click **Continue**.
12. If a Microsoft Intune login screen appears, in the Password text box, type **Pa$$w0rd** and then click **Sign in**.
13. If a Don't lose access to your account message displays, click **Remind me later**.
14. On the Microsoft Intune Admin Overview screen, in the menu bar just below the web-page address, click **Admin Console**.
15. If a message appears, indicating the application requires Microsoft Silverlight, click **Get Microsoft Silverlight**. When you are prompted to run or save Silverlight_x64.exe, click **Run**. If the User Account Control dialog box displays, click **Yes**.
16. In the Install Silverlight dialog box, click **Install now**. When you are prompted to enable Microsoft Update, click **Next**. Click **Close**.
17. If you are prompted to log in, type **Pa$$w0rd** in the Password text box.

Setting up the Initial Configuration of Cloud Services for Microsoft Intune

CERTIFICATION READY
Set up the initial configuration of cloud services (for Microsoft Intune)
2.4

For Microsoft Intune, there are two administrative websites: the Microsoft Intune Account Portal and the Microsoft Intune Admin Console.

The tenant administrator can log on to the Microsoft Intune Account Portal (https://account.manage.microsoft.com/) to perform the following tasks (see Figure 2-6):

- Manage user accounts and subscription
- Configure directory synchronization from your on-premises Active Directory
- Manage the security groups
- Assign Microsoft Intune licenses to users
- Configure the domain name that you use with your subscription
- Manage billing and purchase details for your subscription, including the number of licenses you have, or the amount of cloud storage space you can use
- Find links to view the health of the Intune service

Users who have a sign-in status of Allowed can also use the account portal to reset their account password and edit their profile. By default, all user accounts are Allowed.

The service administrator or the tenant administrator with the global administrator role can log on to the Microsoft Intune Admin Console (https://admin.manage.microsoft.com/) and manage day-to-day operations (see Figure 2-7), including:

- Set policies for computers and mobile devices
- Upload and deploy software like software updates and apps
- Manage Intune Endpoint Protection on computers
- View device status and run reports

Figure 2-6

Viewing the Microsoft Intune Account Portal

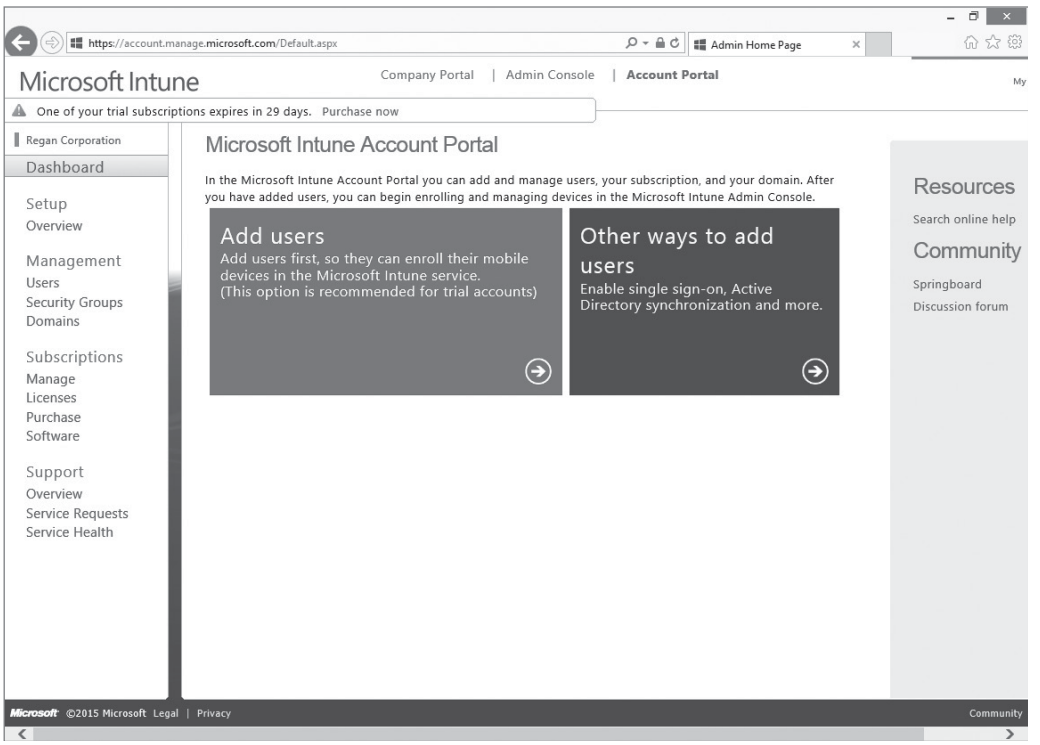
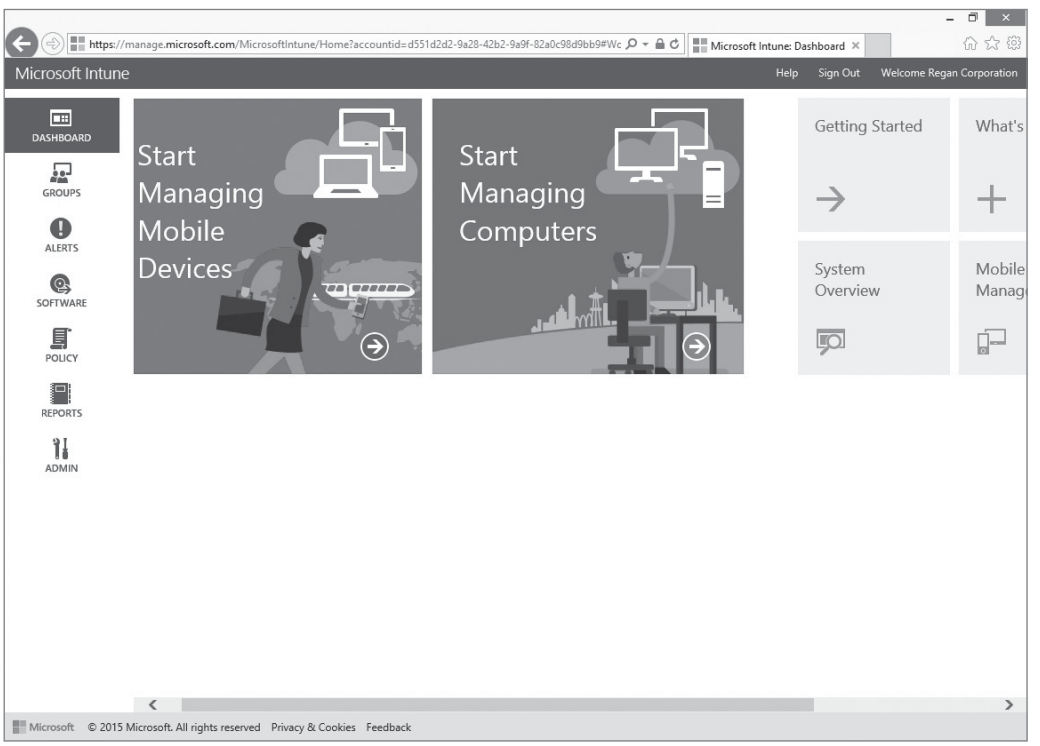


Figure 2-7

Viewing the Microsoft Intune Admin Console



After you subscribe to Microsoft Intune, you need to perform the following tasks:

1. Configure a domain name.
2. Add users and assign licenses for your subscription.
3. Manage Microsoft Intune licenses for users.

4. Assign administrative users.
5. Configure Security Groups.
6. Customize the Company Portal.
7. Add devices to your subscription.

The domain name defines the account that users sign in with. To add a domain to the Microsoft Intune subscription, the domain is configured using the Microsoft Intune Account Portal.

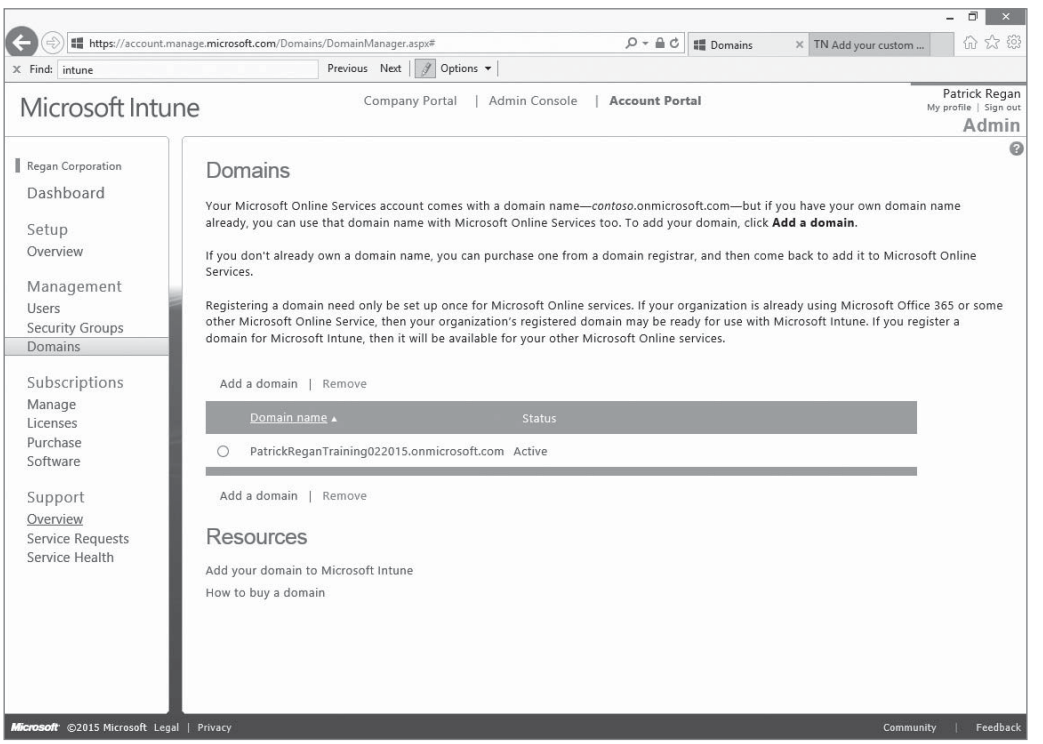
ADD AND VERIFY A DOMAIN

GET READY. To add and verify a domain, perform the following steps on a computer running Windows 10 with a connection to the Internet.

1. On Win10A, log on using the **contoso\administrator** account and the **Pa$$word** password.
2. On the Taskbar, click the **Microsoft Edge** icon to open Microsoft Edge.
3. Open and logon to the Microsoft Intune Account Portal (https://account.manage.microsoft.com).
4. Under Management click **Domains**.
5. On the Domains page (as shown in Figure 2-8), click **Add a domain**.

Figure 2-8

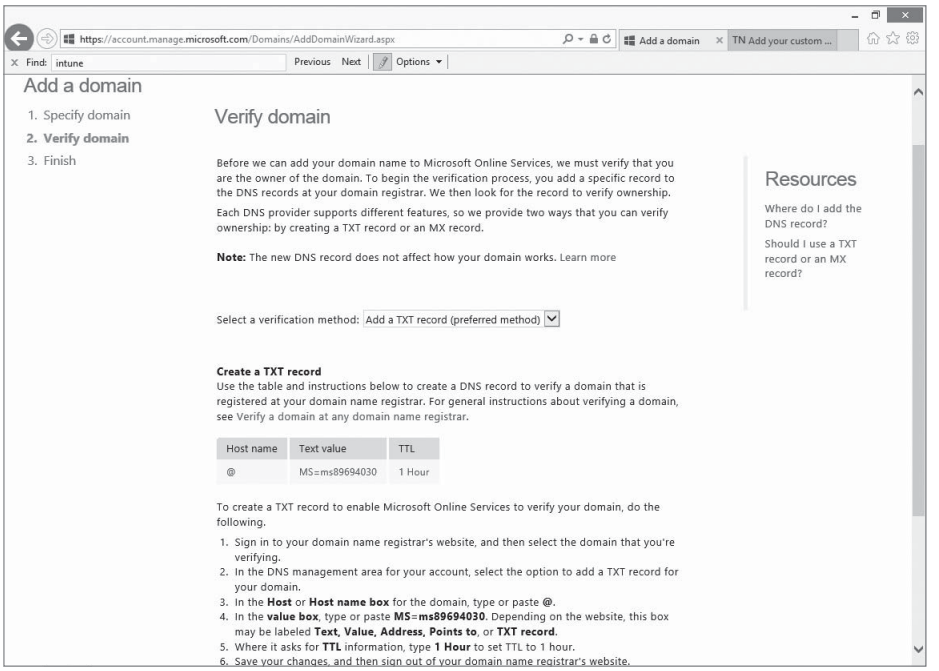
Managing domains



6. On the Specify domain page, in the text box, type the domain that you want to add and then click **Next**.
7. A common method to verify that you own a domain is to add a TXT record to the DNS zone for the domain. Therefore, after you add a TXT record to the zone, go back to the Verify domain page (as shown in Figure 2-9) and click the **Verify** button at the bottom of the page.

Figure 2-9

Verifying the domain



■ Understanding Microsoft Azure

THE BOTTOM LINE

Microsoft Azure (formerly known as Windows Azure) is a cloud-computing platform used for building, deploying, and managing applications and services through a global network of Microsoft-managed datacenters. Although Microsoft Azure has its own web-based tools, you can also use System Center Virtual Machine Manager (VMM) and App Controller.

Microsoft Azure includes the following features:

- Websites with support for ASP.NET, PHP, Node.js, or Python that can be deployed using FTP, Git, Mercurial, or Team Foundation Server
- Virtual machines that run both Windows Server and Linux virtual machines
- Cloud services including Microsoft's platform as a service (PaaS) environment that are used to create scalable applications and services
- Data management using SQL Database (formerly known as SQL Azure Database) that can integrate with Active Directory, Microsoft System Center, and Hadoop
- Media services that use PaaS to provide encoding, content protection, streaming, and/or analytics

When you use Microsoft Azure, you are leasing cloud resources provided by Microsoft. Microsoft Azure resources can be self-contained in the cloud (such as when you want to have websites with databases) or you can extend your organization's data center to the cloud by using IaaS. By using IaaS, you can run applications in the cloud while maintaining full control over the virtual machines themselves.

XREF

IaaS is discussed in more detail in Lesson 1.

In a virtual environment, you can create multiple virtual machines by deploying the Windows Server 2012 R2/2016 operating system on the Hyper-V host or cloud service that it runs under. You can also upload a Windows Server 2012 R2/2016 image template VHD file or a Windows Server 2012 R2/2016 preconfigured image VHD file. You can then use the cloud tools to manage the hosted virtual machines.

Microsoft provides several tools to deploy and manage servers running Windows Server 2012 R2/2016 on public and private clouds:

- System Center 2012 R2/2016 Virtual Machine Manager (VMM)
- Microsoft Azure virtual machine (VM) tools
- System Center 2012 R2/2016 App Controller

Virtual Machine Manager (VMM) provides a single administrative tool for deploying virtual servers and managing a virtualization infrastructure, including hosts, virtual machines, storage, networks, and libraries. You can also use VMM to update virtual servers.

The Microsoft Azure Web Portal (see Figure 2-10) includes multiple tools for creating and managing virtual machines that are hosted on the Microsoft Azure cloud platform. With these tools, you can create VMs, attach disks, upload a Windows Server VHD file, load balance virtual machines, and manage availability of virtual machines.

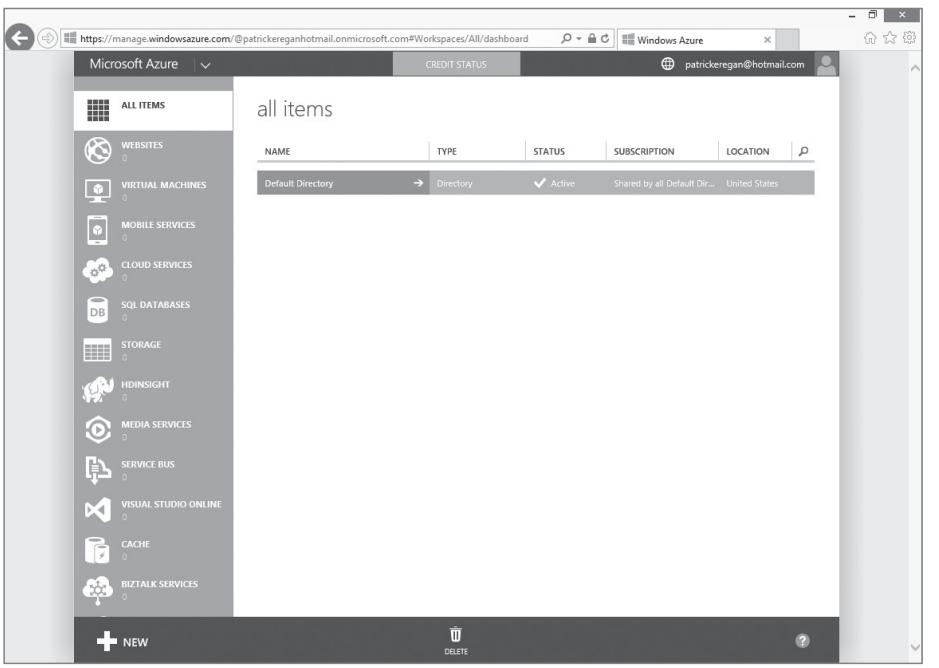


Figure 2-10

Using the Microsoft Azure Web Portal

The App Controller application allows administrators to deploy and manage services across the Microsoft private cloud services and the Microsoft public cloud services, such as Microsoft Azure. App Controller has a web-based interface that enables administrators to manage services rather than servers.

Understanding Virtual Machines

Virtualization has become quite popular during the last few years. By using ***virtual machine*** technology, you can run multiple operating systems concurrently on a single machine, which allows separation of services while keeping cost to a minimum. It can also be used to create Windows test systems in a safe, self-contained environment. Microsoft Hyper-V is a hypervisor-based virtualization system for x64 computers starting with Windows Server 2008. The ***hypervisor*** is installed between the hardware and the operating system and is the main component that manages the virtual computers.

Server virtualization in Windows Server 2012 R2/2016 is based on a module called a hypervisor. Sometimes called a ***Virtual Machine Monitor (VMM)***, the hypervisor is responsible for abstracting the computer's physical hardware and creating multiple virtualized hardware environments, called virtual machines (VMs). Each VM has its own (virtual) hardware configuration and can run

a separate copy of an operating system. Therefore, with sufficient physical hardware and the correct licensing, a single computer running Windows Server 2012/2012 R2/2016 with the Hyper-V role installed can support multiple VMs, which you can manage as though they were standalone computers.

TAKE NOTE*

VMM is usually associated with older virtual machine technology. Don't confuse VMM with System Center Virtual Machine Manager (VMM), which is a software package that is used to manage a virtual machine environment based on Microsoft Hyper-V, VMWare ESX/ESXi, and Citrix XenServer.

To run several virtual machines on a single computer, you need to have sufficient processing power and memory to handle the load. However, since most servers often sit idle, virtualization utilizes the server's hardware more efficiently.

To keep each virtual server secure and reliable, each server is placed in its own logical partition that isolates processing and memory. A ***partition*** is a logical unit of storage in which operating systems are hosted. The partition is not to be confused with a disk partition or a volume that divides a storage area. Each virtual machine accesses the hypervisor, which handles interrupts to the processor and redirects them to the respective partition.

By using Hyper-V Manager, you can create new virtual machines and define the hardware resources that the system should allocate to them. In the settings for a particular virtual machine, depending on the physical hardware available in the computer and the limitations of the guest operating system, you can specify the number of processors and the amount of memory a virtual machine should use, install virtual network adapters, and create virtual disks using various technologies, including storage area networks (SANs).

By default, Hyper-V stores the files that make up virtual machines in the folders you specified on the Default Stores page during installation. Each virtual machine uses the following files:

- A virtual machine configuration (.xml) file in XML format that contains the virtual machine configuration information, including all settings for the virtual machine
- One or more virtual hard disk (.vhd or .vhdx) files to store the guest operating system, applications, and data for the virtual machine

A virtual machine may also use a saved-state (.vsv) file, if the machine has been placed into a saved state.

Understanding Azure Services

Microsoft Azure has a wide range of services that you can tap into. The popular services include Cloud Services, SQL Database, Storage, Virtual Machines, and Websites.

By providing the following services, Azure can be customized to fulfill the needs of virtually any organization:

- **API Management:** Allows you to publish APIs to developers, partners and employees securely.
- **Application Insights:** Can be used to detect issues, solve problems, and continuously improve your web applications by providing real time information, including availability, performance, and usage.
- **Automation:** Allows you to automate the creation, deployment, monitoring, and maintenance of resources in your Azure environment using a highly scalable and reliable workflow execution engine.
- **Azure Active Directory (Azure AD or AAD):** Provides identity management and access control capabilities for your cloud applications. It can be synchronized with the on-premises domain controllers. You can also enable Single Sign-On (SSO) to simplify user access to cloud applications and to support conditional access.

- **Azure Rights Management:** Protects confidential or sensitive information by using encryption, identity, and authorization policies.
- **Backup:** Allows you to back up to and restore from the cloud using familiar tools in Windows 2016, Windows Server 2012/Windows Server 2012 R2, or System Center 2012 R2/2016 Data Protection Manager.
- **Batch:** Allows you to run large-scale parallel and High Performance Computing (HPC) workloads in Azure.
- **BizTalk Services:** Provides Business-to-Business (B2B) and Enterprise Application Integration (EAI) capabilities for delivering cloud and hybrid integration solutions.
- **CDN:** Short for Content Delivery Network, allows you to deliver high-bandwidth content to end-users around the world with low latency and high availability via a robust network of global data centers.
- **Cloud Services:** Allows you to move or extend your corporate infrastructure to the cloud.
- **Data Factory:** Produces trusted information from raw data in cloud or on-premises sources. It can create, orchestrate and schedule high-available, fault-tolerant workflows of data movement and transformation activities. It can also monitor all your data pipelines and service health.
- **DocumentDB:** A fully-managed NoSQL document database service that offers query and transactions over schema-free data, predictable and reliable performance, and rapid development.
- **Event Hubs:** Enables elastic scale telemetry and event ingestion with durable buffering and sub-second end-to-end latency for millions of devices and events.
- **ExpressRoute:** Enables you to create private connections between Azure datacenters and infrastructure at your premises or in a colocation environment.
- **HDInsight:** A Hadoop-based service that brings an Apache Hadoop solution to the cloud. It is typically used to manage Big Data on a cloud-based data platform that manages data of any type and any size.
- **Key Vault:** Offers an easy, cost-effective way to safeguard keys and other secrets in the cloud using Hardware Security Modules (HSMs).
- **Machine Learning:** Allows you to easily design, test, operationalize and manage predictive analytics solutions in the cloud.
- **Managed Cache:** Creates a cache that will increase access to applications and data.
- **Media Services:** Offers cloud-based media solutions from several existing technologies, including ingest, encoding, format conversion, content protection, and both on-demand and live streaming capabilities.
- **Mobile Services:** Provides a scalable cloud back-end for building Windows Store, Windows Phone, Apple iOS, Android, and HTML/JavaScript applications. It can be used to store data in the cloud, authenticate users, or send push notifications to your application within minutes.
- ***Multi-Factor Authentication (MFA)*:** By having more than one method of authentication, you can help prevent unauthorized access to on-premises and cloud applications.
- **Notification Hubs:** Allows a scalable, cross-platform push notification infrastructure that can be used for broadcasting push notifications to millions of users at once or tailoring notifications to individual users.
- **Operational Insights:** Enables you to collect, correlate, and visualize all your machine data (such as event logs, network logs, and performance data) from on premise and cloud assets.
- **Redis Cache:** A popular open source cache for your Azure applications.
- **RemoteApp:** RemoteApp helps employees stay productive anywhere on a variety of devices (such as Windows, Mac OS X, iOS, or Android).
- **Scheduler:** Allows you to invoke actions that call HTTP/S endpoints or post messages to a storage queue on any schedule.
- **Azure Search:** Provides a fully managed service for adding sophisticated search capabilities to web and mobile applications.

- **Service Bus:** Provides a messaging infrastructure that sits between applications.
- **Site Recovery:** Provides a simple, cost-effective disaster recovery that can replicate and, if needed, recover resources in the private cloud.
- **SQL Database:** Provides a relational database service that enables you to rapidly create, extend, and scale relational applications into the cloud.
- **Storage:** Offers non-relational data storage, including Blob, Table, Queue, and Drive storage.
- **StorSimple:** Offers a unique hybrid cloud storage solution that provides primary storage, archive, and disaster recovery.
- **Stream Analytics:** Provides an event-processing engine that helps uncover insights from devices, sensors, cloud infrastructure, and existing data properties in real time.
- **Traffic Manager:** Allows you to load-balance incoming traffic across multiple hosted Azure services whether they're running in the same datacenter or across different datacenters around the world.
- **Virtual Machines:** Enables you to deploy a Windows Server or Linux image in the cloud.
- **Virtual Network:** Enables you to create Virtual Private Networks (VPN) within Azure and securely link these with on-premises network.
- **Visual Studio Online:** A cloud-based Application Lifecycle Management (ALM) solution that provides hosted code repositories and issue tracking, load testing, and automated builds. Visual Studio Online is licensed separately from Azure Services.
- **Websites:** Enables you to deploy web applications on a scalable and reliable cloud infrastructure.

Understanding Azure Disaster Recovery, High Availability, Redundancy, and Fault Tolerance

Microsoft Azure has a wide range of tools that provide high availability, redundancy, and fault tolerance to keep your cloud components running 24/7 and to provide a wide range of tools you can use to recover from a disaster.

When deploying any application or service, you need to look at availability, which is the percentage of time applications and services can be accessed. The effective availability of your cloud service is also affected by the various Service Level Agreements (SLAs) of other dependent services.

For example, Azure provides the following SLA:

- **Compute:** 99.95%, which allows 21.6 minutes of downtime per month.
- **SQL Database:** 99.90%, which allows for 43.2 minutes of downtime per month.
- **Storage:** 99.90%, which allows for 43.2 minutes of downtime per month.

If any of these go down, an application will go down. When you combine all of the SLAs (99.95%x99.90%x99.90%), the overall SLA/general service available for the entire application is 99.65%, which gives you 151 minutes of downtime per month.

To print high availability, Azure provides the Azure Business Continuity Technical Guidance, which can be found by searching the Microsoft website.

The ***Microsoft Azure Fabric Controller (FC)*** is responsible for provisioning and monitoring the condition of the Azure compute instances. When it checks the status of the hardware and software of the host and guest machine instances and detects a failure, it will automatically relocate the VM instances.

To provide redundancy to your application, it is recommended that you group two or more virtual machines in an Availability Set. By using an Availability Set, two VMs that provide the same service will be hosted on two different physical hosts so that if one physical host goes down, the other VM is not affected. As a result, Availability Sets provide redundancy, including when you are performing maintenance or when one of the hosts go down.

Microsoft Azure Site Recovery is a software component used to orchestrate protection for virtual machines that are located on on-premises Hyper-V host servers located in the VMM cloud. With Microsoft Azure Site Recovery, you can configure:

- **On-premises to on-premises protection:** Replicates on-premise virtual machines to another on-premise site.
- **On-premises to Azure protection:** Replicates on-premise virtual machines to Azure by configuring and enabling protection settings in Azure Site Recovery vaults. Virtual machine data replicates from an on-premises Hyper-V server to Azure storage.

Microsoft Azure Site Recovery can be used to replicate a large number of virtual machines between the primary site and a disaster recovery site. By using the Microsoft Azure cloud and the Recovery Manager service, you can access all of the components necessary to orchestrate the failover of virtual machines in one data center to another, even when one of the data center sites is unresponsive.

Recovery Manager has the following requirements:

- System Center 2012 R2/2016 VMM or VMM 2012 SP1 with cumulative update 3
- Windows Server 2012 with latest updates, Windows 2012 R2, or Windows Server 2016

To configure Azure Site Recovery, perform the following steps:

1. Create an Azure Site Recovery vault, including specifying a vault key.
2. Install the Site Recovery agent on the VMM servers that you want to register in the vault.
3. Specify protection settings for the cloud, including source and target settings, recovery points and snapshots, and initial replication settings.
4. Create mappings between VM networks on source and destination VMM servers.
5. Create mappings between storage classifications on source and target VMM servers.
6. Enable protection for virtual machines.
7. Create and customize recovery plans that specify how virtual

SUMMARY SKILL MATRIX

In this lesson you learned:

- Microsoft Office 365 is a Microsoft subscription–based software service that enables users to access their documents and collaborate with others from anywhere using their computers, the Internet, or their smart devices. Office 365 moves the traditional Office suite to the cloud.
- Office 365 is designed to work with the current or immediately previous versions of Internet Explorer, Microsoft Edge, or Firefox or the latest versions of Chrome or Safari. It also designed to work with any version of Microsoft Office in mainstream support.
- Office 365 offers several plans designed for small, midsize, and enterprise-level businesses. The Office 365 Business (300 users) plan and the Office 365 Enterprise E3 and E4 (unlimited users) plan includes a subscription for Office 2016 for up to five PCs/Macs.
- A domain name represents the online identity of companies or individuals. You can use your domain name in Office 365 with your emails and SharePoint sites.

- Microsoft Intune is a cloud-based management solution that allows you to manage your computers when they are connected to or not connected to the corporate network. In fact, you don't even have to be part of your domain. Microsoft Intune helps you manage your computers and mobile devices through a web console. It provides the tools, reports, and licenses to ensure your computers are always current and protected.
- Compared to Office 365, a Microsoft Intune subscription is licensed on a per-user basis. Therefore, if you need to add more users, you just buy additional licenses. If you need to reduce the number of subscriptions, you just reduce the number of licenses.
- Microsoft Azure (formerly known as Windows Azure) is a cloud-computing platform used for building, deploying, and managing applications and services through a global network of Microsoft-managed datacenters. Although Microsoft Azure has its own web-based tools, you can also use System Center 2012 R2/2016 Virtual Machine Manager (VMM) and App Controller.

■ Knowledge Assessment

Fill in the Blank

Complete the following sentences by writing the correct word or words in the blanks provided.

1. _____ provides Microsoft Office, Exchange, Skype for Business Online, and SharePoint based on a subscription service.
2. If you want Microsoft Office, SharePoint, Exchange, voicemails, and Skype for Business Online, for your large corporation, you will need to use the _____ licensing plan.
3. _____ is a cloud-based management solution that allows you to manage computers and other devices.
4. _____ is a cloud-computing platform that provides a virtual machine infrastructure.
5. In Office 365, _____ provides instant messaging.
6. If you have a domain called litware.com, _____ is the default name for the SharePoint public website.
7. When configuring DNS for Office 365, the _____ record is used to help prevent spam.
8. To access the Microsoft Intune company portal, you should use Internet Explorer _____ or higher.
9. You can run _____ virtual machines on Microsoft Azure.
10. When using Azure, _____ provides identity management and access control capabilities for your cloud applications.

Multiple Choice

Circle the letter that corresponds to the best answer.

1. Which Office 365 licensing plan is targeted for user who can have up to five devices?
   a. Personal
   b. Home
   c. ProPlus
   d. Business Essentials

2. In Office 365, which role is assigned to the first user?
   a. Site administrator
   b. System administrator
   c. Account administrator
   d. Global administrator

3. Which of the following is used to determine which Microsoft data center will be used to store data for an Office 365 account?
   a. The data center that has the most resources available
   b. The location of where you signed up for the account
   c. The selected data center
   d. The specified user location

4. Which port must be open to perform a query for DNS?
   a. UDP and TCP port 53
   b. UDP and TCP port 80
   c. UDP and TCP port 389
   d. UDP and TCP port 25

5. Which DNS resource record maps a host name to an IP address?
   a. A
   b. CNAME
   c. PTR
   d. SRV

6. Which Microsoft Intune deployment integrates with your existing Active Directory and Exchange environment?
   a. Microsoft Intune Stand-Alone Cloud Configuration
   b. Microsoft Intune Cloud + On-Premise Configuration
   c. Microsoft Intune + System Center Configuration Manager
   d. Microsoft Intune + System Center Operations Manager

7. Which of the following is the least expensive Office 365 plan that offers Exchange and SharePoint with enterprise-specific legal compliance features?
   a. Business Premium
   b. E3
   c. E4
   d. ProPlus

8. Which clients can be used with the Microsoft Intune client? (Choose all that apply)
   a. Windows XP
   b. Windows Vista
   c. Windows 7
   d. Windows 10

9. When you sign up for Office 365, which two domains are you assigned? (Choose all that apply)
   a. <domainname>-private.sharepoint.com
   b. <domainname>-public.sharepoint.com
   c. <domainname>.com
   d. <domainname>.onmicrosoft

10. Which of the following is responsible for provisioning and monitoring the condition of the Azure compute instances?
    a. Azure Virtual Machine Manager
    b. Azure Site Manager
    c. Azure Fabric Controller
    d. Azure Virtual Machine Converter

True / False

Circle T if the statement is true or F if the statement is false.

T F 1. The CNAME DNS resource record is used to redirect a host name to a server with another name.

T F 2. To share documents inside and outside of your organization and to collaborate on projects, you should use Microsoft Exchange.

T F 3. For devices managed by Microsoft Intune, the device must be able to communicate with manage.microsoft.com and windowsupdate.microsoft.com.

T F 4. You do not need additional network bandwidth when using Office 365.

T F 5. You should not use the cloud if you need to maintain the security of your applications.

■ Case Projects

Scenario 2-1: Upgrading Microsoft Office

As an administrator for the Contoso Corporation, you manage nearly 800 computers running a mix of Windows 7, Windows 8, and Windows 10 machines with a mix of Office 2007 and 2010. You need to upgrade Office and your Exchange environment with the least amount of effort. You also want the ability to use the newest version of Microsoft Office. Describe the best solution.

Scenario 2-2: Using Your Domain Name

You are an administrator for the Adatum Corporation and you are ready to deploy Office 365. You want to use SharePoint for your external website and Exchange for your corporate email. However, you want to keep the adatum.com name for the website and the email addresses. Describe the solution you need to use in order to ensure Office 365 can use this domain name.

Scenario 2-3: Selecting an Office 365 Licensing Plan

You are an administrator for the Contoso Corporation and you are ready to purchase Office 365 for your 800 users. First, however, you need to determine which licensing plan that you want to purchase. Right now, you want your users to have the newest version of Office that can be used online or on their local computers. You want also want to use Microsoft Exchange and Microsoft SharePoint. Describe the licensing plan you should use and explain your reasoning.

Scenario 2-4: Selecting a Cloud Service Plan for Microsoft Intune

As the administrator the Contoso Corporation, you manage a system of about 500 users working from their home offices. You want to be sure that their mobile or office computers are protected with the newest updates, install software, and perform inventory. Describe the solution you need to use and the licensing plan you should purchase.

3

LESSON

Administering Office 365 and Microsoft Intune

OBJECTIVE DOMAIN MATRIX

Technology Skill	Objective Domain Description	Objective Domain Number
Administering Office 365 • Creating Users and Groups and Assigning Services and Licenses in Office 365 • Assigning Permissions in Office 365 • Monitoring Service Health in Office 365	Create users and groups and assign services and licenses Assign permissions in Office 365 Monitor service health in Office 365	3.1 3.2 3.3
Administering Microsoft Intune • Creating Users and Groups and Assigning Services and Licenses in Microsoft Intune • Assigning Permissions in Microsoft Intune • Monitoring Service Health in Microsoft Intune	Create users and groups and assign services and licenses Assign permissions in Microsoft Intune Monitor service health in Microsoft Intune	3.1 3.2 3.3

KEY TERMS

account identity
Active Directory Directory Services (AD DS)
Active Directory Federation Services (AD FS)
Billing Administrator
cloud identity
criteria membership
direct membership
distribution group
distribution list
federated identity
Global Administrator
group
mail-enabled security group
Microsoft Azure Active Directory (AD)
Microsoft Azure Active Directory Sync (DirSync) Tool
Microsoft Intune groups
Microsoft Intune Service Administrator
Microsoft Intune Tenant Administrator
Microsoft partner
Multi-Factor Authentication (MFA)
online identity
Password Administrator
recipients
RSS
security group
Service Administrator
Service Support Administrator
Single Sign-On (SSO)
synchronized identity
user location
User Management Administrator

You work as an administrator for the Contoso Corporation. Now that you have purchased the E4 licenses for Office 365 for your corporate office users and Microsoft Intune to manage your users that work from their home offices, you need to figure out the best way to manage these cloud services while providing users with full functionality of these cloud services.

■ Administering Office 365

THE BOTTOM LINE

Office 365 is administered through the Office 365 Admin Center through the https://portal.office.com/Admin website. From there, you can establish users and licenses, create groups, run reports, and manage services such as Exchange and SharePoint.

From the Office Admin Center, you can access the Exchange Admin Center, the SharePoint Admin Center, the Lync Admin Center, and Microsoft Azure Active Directory (AD). You can also view the service health and service requests.

Creating Users and Groups and Assigning Services and Licenses in Office 365

Office 365 is managed by using the Office 365 Admin Center. From here, you can create users and groups, manage software licenses, generate reports, and purchase services. The person who signs up your company for Office 365 is the Global Administrator by default. This person can then grant administrator permissions to other users in the organization as needed to distribute the workload.

CERTIFICATION READY
Create users and groups, and assign services and licenses
3.1

When performing authentication, authorization, and auditing on a system or infrastructure, you have to first establish identities, such as a user or computer account. The most common form of authentication is to use a password.

DIFFERENTIATING BETWEEN CLOUD IDENTITIES

Office 365 supports the following three sign-in models/identity models for Office 365. The model that you choose will determine how you manage your user accounts for Office 365 and how user passwords are verified:

- ***Online identity*** **(**Also known as ***account identity***)**:** Accounts are created manually with the Office 365 Admin Center.
- ***Synchronized identity*****:** Accounts are based on an on-premises directory, such as Active Directory, and are synchronized with directory sync/password sync.
- ***Federated identity*****:** Accounts are based on an on-premises directory, such as Active Directory, but user passwords are verified by the on-premises identity provider.

The simplest identity model is the cloud identity model, which allows you to use Office 365 right away. In this mode, a user is created and managed in Office 365. The user account is stored in Azure Active Directory and the password is verified by ***Microsoft Azure Active Directory (AD)***. ***Azure AD*** is a cloud-based Infrastructure as a Service (IaaS) that you can use for identity management and access control. It allows you to manage your applications and identity services without having to manage a computer.

XREF
To learn more about IaaS, see Lesson 1.

Azure AD provides the following features:

- Active Directory authentication services in public or private clouds
- Cloud-based storage for directory service data
- Federation services
- A service for extending an on-premises Active Directory environment to cloud services

For larger organizations, synchronized identity is the most common—whereby you install the ***Microsoft Azure Active Directory Sync Tool (DirSync) Tool*** (explained later in this section) to synchronize the organization's Active Directory accounts with the Azure Active Directory.

Active Directory Directory Services (AD DS) is a Microsoft directory service that works with a ***Windows domain*** (a grouping of computers that are registered with a central database stored on domain controllers that runs on a Windows server). Active Directory authenticates and authorizes all users and computers on the Windows domain by using Lightweight Directory Access Protocol (LDAP), Kerberos, and DNS.

Azure AD provides high availability and scalability. It can integrate with on-premises AD DS, including directory synchronization and ***Single Sign-On (SSO)***. SSO provides the ability for a user to log on once yet gain access to all systems without being prompted to log on again. You also can limit the data that synchronizes to Azure AD. Lastly, Azure AD provides an application-programming interface to perform management tasks and to query the directory data.

To authenticate through Azure AD, you can use one of the following web-based authentication protocols:

- OAuth 2.0 is an open standard for authorization that provides granular access control to destination services as specified in RFC 6749. Access can be provided temporarily.
- Security Assertion Markup Language 2.0 (SAML 2.0) is an open standard XML protocol made up of security tokens and claims. The security token used with SAML contains claims, which are typically Active Directory attributes that the workflow application uses to make decisions for authorization and access.
- Web Services Federation (WS-Federation) is a security mechanism that allows identity federation so that users in one realm (or directory) can access resources in another realm.

To integrate with an on-premises Active Directory environment, you can use one of the following:

- The Microsoft Azure Active Directory Sync (DirSync) Tool runs on an on-premises, domain-joined computer to provide directory synchronization to Azure AD. Used primarily to synchronize user objects and user attributes, DirSync is a requirement for SSO.
- ***Active Directory Federation Services (AD FS)*** is deployed onsite and provides SSO for applications and services that reside onsite or in Azure. AD FS enables all authentications to take place in the on-premises Active Directory and offers Multi-Factor Authentication (MFA).
- On-premises AD DS is the authentication provider and the source of directory data. AD DS is a requirement for DirSync, AD FS, and SSO.

If you have configured synchronization between Active Directory and Azure, you can manage your user accounts with the standard Active Directory tools, such as Active Directory Users and Computers. If you are not using directory synchronization, you can manage your accounts in Azure using the Microsoft Azure AD management portal or the Microsoft Azure Directory Module for Windows PowerShell.

Because DirSync sends confidential information outside the domain, you must carefully plan how to synchronize information between Active Directory and Azure. Without out proper planning, the synchronization could reduce performance and create administrative overhead.

You can filter the Active Directory user objects that use DirSync from the on-premises Active Directory domain to Azure AD in three ways:

- Filtering by organizational unit (OU)
- Filtering by domain
- Filtering by user object attributes

You can install the DirSync tool on a domain computer but not on a domain controller. To maintain security, you should install the DirSync tool on a highly secure server that is accessible only by domain administrators or other trusted administrators.

Before you perform the initial synchronization, you should synchronize in a pre-production environment. For larger organizations, you should perform the initial synchronization after hours. Azure AD synchronizes every three hours by default.

When you configure the directory synchronization, a service account named MSOL_AD_SYNC is created. If you are synchronizing more than 50,000 objects, a full installation of Microsoft SQL Server is required.

The federated identity model requires a synchronized identity, but user passwords are verified by the on-premises identity provider. As a result, the password hash does not need to be synchronized to Azure Active Directory. This model uses AD FS or a third-party identity provider.

CREATING AND MANAGING USERS AND IDENTITIES

You can create accounts with the Office 365 Admin Portal or by using Windows PowerShell. You can also add users to Office 365 using an Excel spreadsheet comma separated value (CSV) format text file.

ADD A NEW USER TO YOUR OFFICE 365 ADMIN PORTAL

GET READY. To add a new user in Office 365, log into your Office 365 Admin Portal as the Administrator and then perform the following steps.

1. On Win10A, log on using the **contoso\administrator** account and the **Pa$$word** password.
2. On the Taskbar, click the **Microsoft Edge** icon to open Microsoft Edge and then open and sign in to Office 365 (https://portal.office.com).
3. Click the **Admin** button, click **USERS,** and then click **Active Users**, as shown in Figure 3-1.
4. In the middle pane, click **+** to create a new office 365 user.
5. When the Create new user account window opens, type the first name, last name, display name, and user name in the First name, Last name, Display name and User name text box.
6. Click the **Type password** option. In the Enter password and Re-enter password text boxes, type a password (such as **Pa$$word**), as shown in Figure 3-2. Click **Create**.
7. When the user account has been created, click **Close**.

Figure 3-1

Adding new users

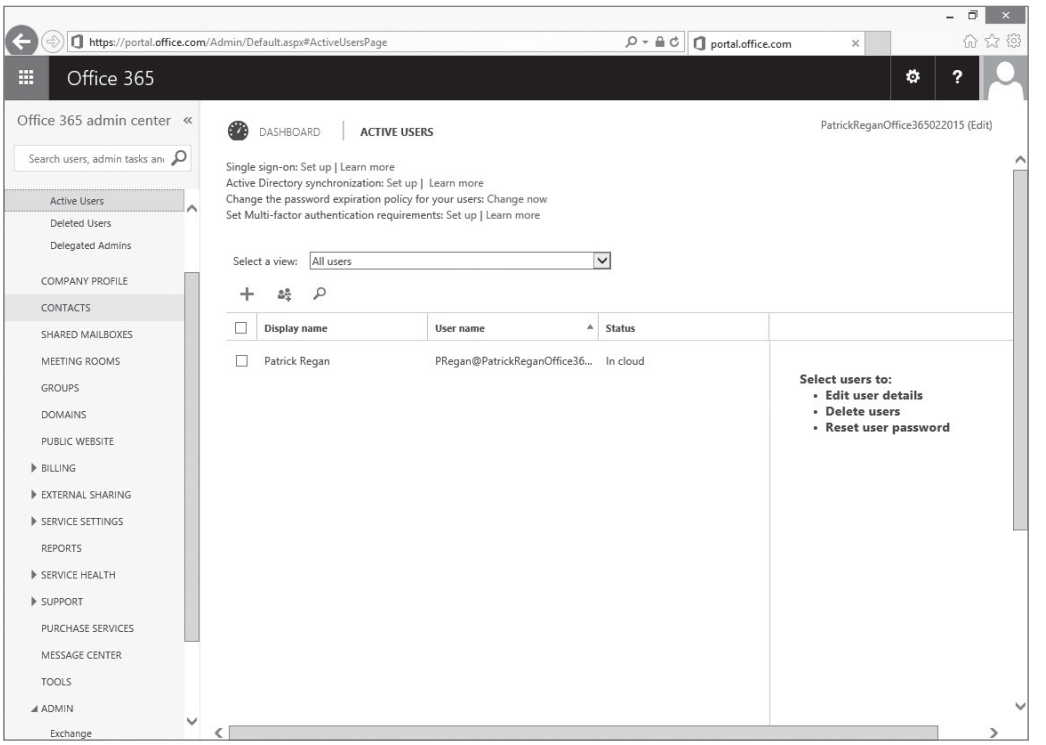
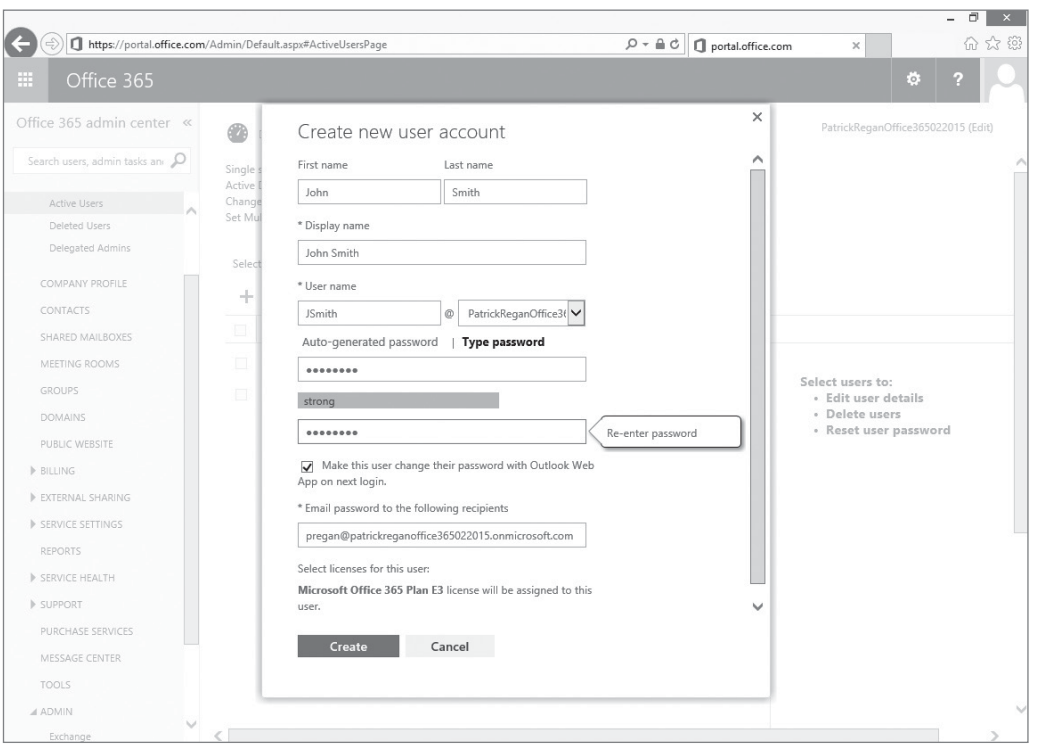


Figure 3-2

Specifying user information



Some of the general administrative tasks you will perform in Office 365 include the following:

- Resetting a user's password
- Configuring a password expiration policy
- Viewing the overall health of Office 365
- Personalizing the default SharePoint team site

RESET A USER'S PASSWORD IN OFFICE 365

GET READY. To reset a user's password in Office 365, log into your Office 365 Admin Portal as the Global Administrator and then perform the following steps.

1. On Win10A, log on using the **contoso\administrator** account and the **Pa$$word** password.
2. On the Taskbar, click the **Microsoft Edge** icon to open Microsoft Edge and then open and sign into Office 365 (https://portal.office.com).
3. Click the **Admin** button, click **USERS**, and then click **Active Users**.
4. Select the checkbox for the user that you want to change the password for. Then click **RESET PASSWORD**.
5. On the send results in email page, the Send email option is already selected with an email address the password will be sent to. In addition, the Make this user change their password with Outlook Web App on next logon option is selected. Click **Reset password**.
6. When the password is changed, the user name and new password will be displayed, click **Finish**.

Office 365 also offers ***Multi-Factor Authentication (MFA)***, in which users are required to acknowledge a phone call, a text message, or an app notification on their smartphones after correctly entering their passwords. Office 365 administrators can enroll users for MFA in the Office 365 Admin Center.

X REF

For more information about MFA, see Lesson 2.

DELETING AND RESTORE USERS

The steps used to delete an account vary according to whether you are using an online account or using directory synchronization. If you are using online accounts, accounts can be deleted using the Office 365 Admin Center or by using Windows PowerShell. If you are using directory synchronization, you can delete users from the local Active Directory.

DELETE A USER IN OFFICE 365

GET READY. To delete a user in the Office 365 Admin Portal as the Global Administrator, perform the following steps.

1. On Win10A, log on using the **contoso\administrator** account and the **Pa$$word** password.
2. On the Taskbar, click the **Microsoft Edge** icon to open Microsoft Edge and then open and sign into Office 365 (https://portal.office.com).
3. Click the **Admin** button, click **USERS**, and then click **Active Users**.
4. Select the checkbox for the user that you want to delete and then click **DELETE**.
5. When you are prompted to confirm this action, click **Yes**.

When an account is deleted, it becomes inactive. For approximately 30 days after deleting the account, you can still restore it.

RESTORE A DELETED USER IN OFFICE 365

GET READY. To restore a deleted user in the Office 365 Admin Portal as the Global Administrator, perform the following steps.

1. On Win10A, log on using the **contoso\administrator** account and the **Pa$$word** password.
2. On the Taskbar, click the **Microsoft Edge** icon to open Microsoft Edge and then open and sign into Office 365 (https://portal.office.com).
3. Click the **Admin** button, click **USERS,** and then click **Deleted Users**.
4. Select the checkbox for the user that you want to restore and then click **Restore users**.
5. When the restore is completed, click **Close**.

CREATING AND MANAGING GROUPS

Office 365 offers four types of groups:

- Groups
- Security groups
- Mail-enabled security groups
- Distribution lists

A ***group*** is used to communicate, collaborate, and schedule events with other users. Users can create, find, and join Groups from their inboxes or calendars and then share files on a dedicated OneDrive for Business page (which is accessed by clicking the OneDrive button after logging into Office 365). A group is usually created by users and is displayed in the Groups section of the Office 365 Admin Center. To participate in a group, a user needs a One Drive for Business license and an Exchange Online license.

XREF

Office 365 licensing is covered in Lesson 2.

Similar to an Active Directory security group, an Office 365 ***security group*** is used to grant access permissions to a group of users. For example, you can create a security group and then assign the read/write permission to the SharePoint Online site. Any user that is part of the security group will be granted the read/write permission to the SharePoint Online site.

The ***mail-enabled security group*** is used to grant access permission to resources in Active Directory. While it is a security group that can be used to grant access permissions to a group of users, it can also be used to send emails to all users at once.

The ***distribution list***, also referred to as a ***distribution group***, is used to send emails to multiple users at once. Distribution lists are used to group users together who require frequent communication.

CREATE A SECURITY GROUP IN OFFICE 365

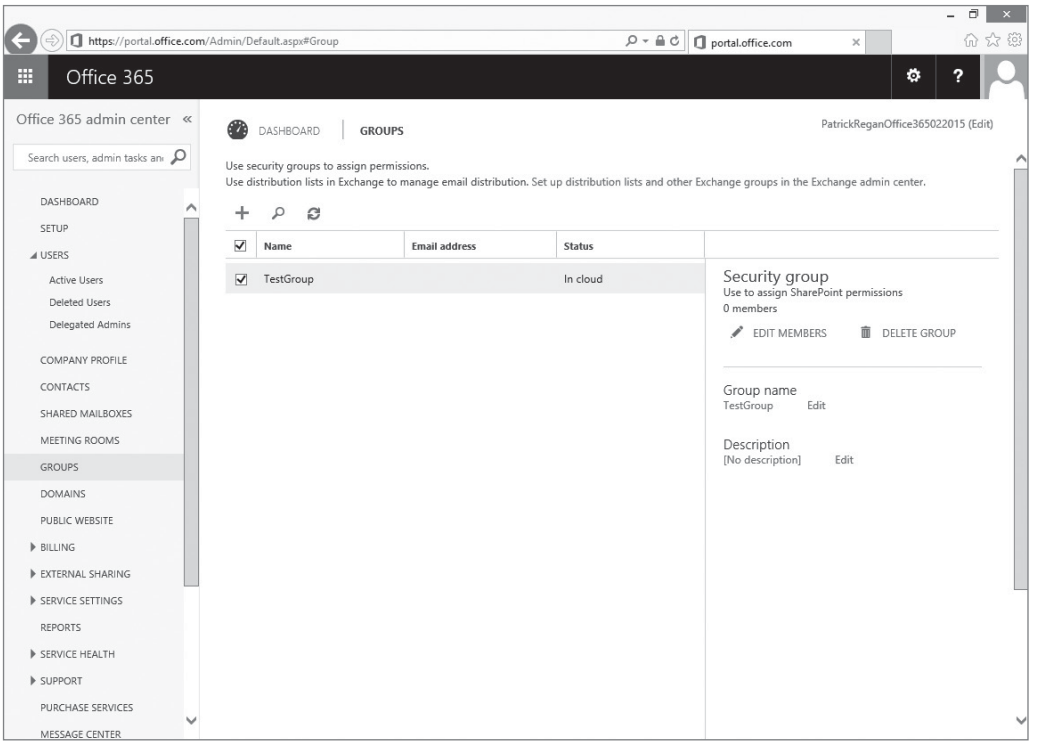
GET READY. To create a security group in the Office 365 Admin Portal as the Global Administrator, perform the following steps.

1. On Win10A, log on using the **contoso\administrator** account and the **Pa$$word** password.
2. On the Taskbar, click the **Microsoft Edge** icon to open Microsoft Edge and then open and sign into Office 365 (https://portal.office.com).
3. Click the **Admin** button and then click **GROUPS** (see Figure 3-3).
4. Click the **+** sign.
5. In the Create security group window, in the Group name text box, type a name of the group and then click **Create**.
6. Type a name and description for the group and then click **Create**.
7. When the group is created successfully, click **Edit members**.

8. Click **Add Member**. In the Add members to the group window, in the search box, type a full or partial user name. Then click the name that you want to add.

Figure 3-3

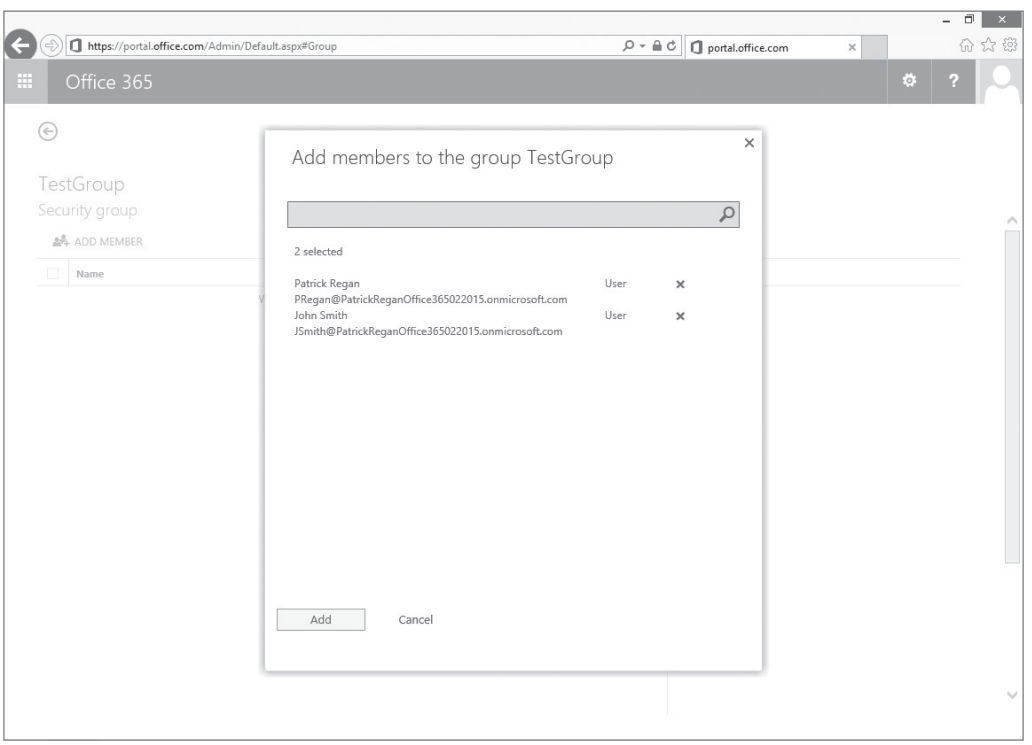
Managing groups



9. When the accounts are specified, click **Add** (see Figure 3-4).

Figure 3-4

Adding members to a group



10. Click **Close**.
11. Click the left arrow button to go back to the Groups list.

If you need to add or remove members from a group, simply select the group that you want to edit and then click EDIT MEMBERS. To delete a group, select the group that you want to delete and then click DELETE GROUP.

ASSIGNING AND REVOKING LICENSES

When you assign a license to a user, the user will receive the following licenses:

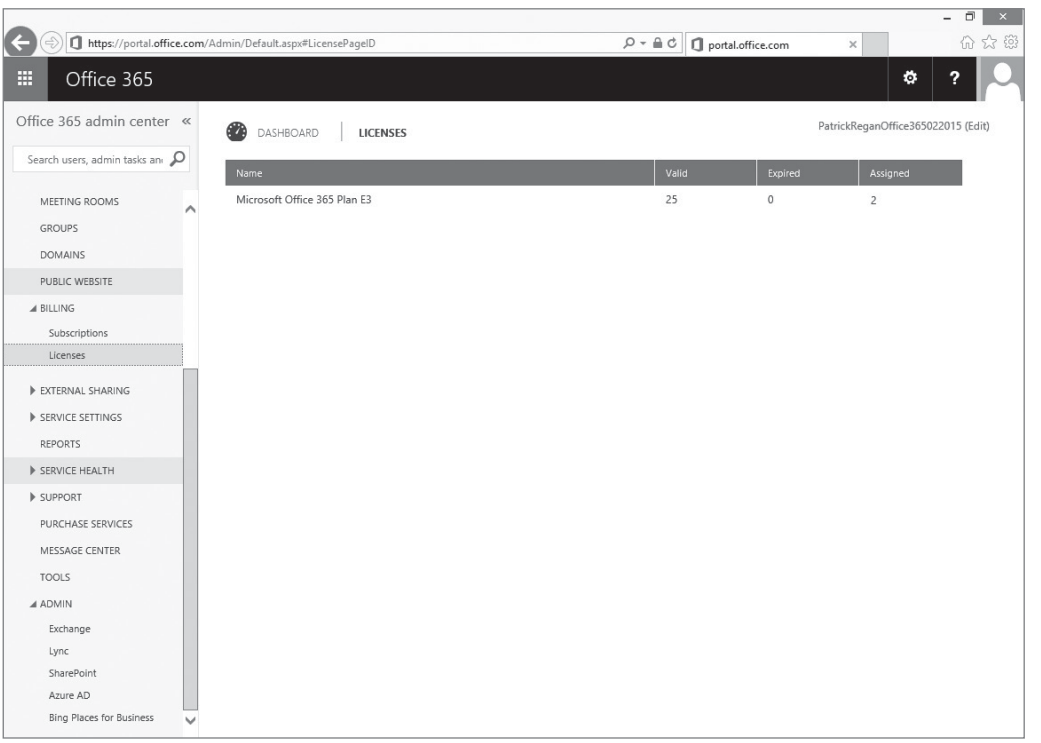
- For Exchange Online, a mailbox is created for the user.
- For SharePoint Online, edit permissions to the default SharePoint Online team site are assigned to the user.
- For Lync Online, the user will have access to the features associated with the license.
- For Office 365 ProPlus, the user will be able to download Microsoft Office on as many as 5 Macs or PCs.

VIEW THE LICENSES USED IN OFFICE 365

GET READY. To view the licenses used in the Office 365 Admin Portal as the Global Administrator, perform the following steps.

1. On Win10A, log on using the **contoso\administrator** account and the **Pa$$word** password.
2. On the Taskbar, click the **Microsoft Edge** icon to open Microsoft Edge and then open and sign into Office 365 (https://portal.office.com).
3. Click the **Admin** button, click **BILLING**, and then click Licenses (see Figure 3-5).

Figure 3-5
Viewing licenses



The Global Administrator or User Management Administrator can assign and unassign licenses. When a user's license is removed, the data is held for 30 days before it is permanently deleted—with the exception of documents that are saved on SharePoint Online.

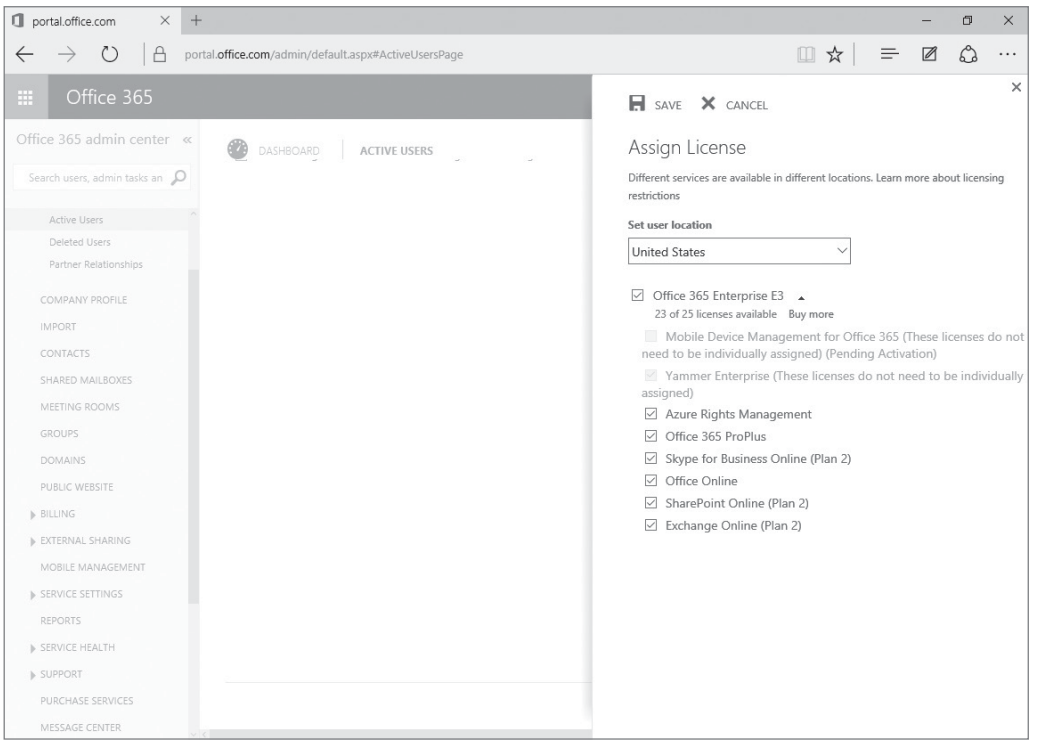
ASSIGN OR UNASSIGN A LICENSE FOR A USER IN OFFICE 365

GET READY. To assign or unassign a license for a user in the Office 365 Admin Portal as the Global Administrator, perform the following steps.

1. On Win10A, log on using the **contoso\administrator** account and the **Pa$$word** password.
2. On the Taskbar, click the **Microsoft Edge** icon to open Microsoft Edge and then open and sign into Office 365 (https://portal.office.com).
3. Click the **Admin** button, click **USERS,** and then click **Active Users**.
4. Select the checkbox for the user and next to Assigned license and then click **Edit.** You can expand the license list, as shown in Figure 3-6.

Figure 3-6

Assigning a license to a user



5. Select and deselect the license as needed.
6. Click **SAVE**.

DETERMINING USER LOCATIONS

When you edit the assigned license, you can also define the ***user location*** for the user. The location will specify the datacenter location for hosting the content. The availability of services and features for a Microsoft cloud service (including Office 365 and Microsoft Intune) varies by country or region. For example, Voice over Internet Protocol (VoIP) might be available to users in certain countries or regions.

Assigning Permissions in Office 365

Office 365 provides several administrator roles that can be assigned to help distribute the workload of managing Office 365. The Global Administrator is assigned to the person who sets up Office 365 initially. This is the most powerful account in the organization. The other administrator roles can be assigned to users according to your organization's specific needs.

CERTIFICATION READY
Assign permissions in Office 365
3.2

Five administrator roles are available for Office 365 enterprises:

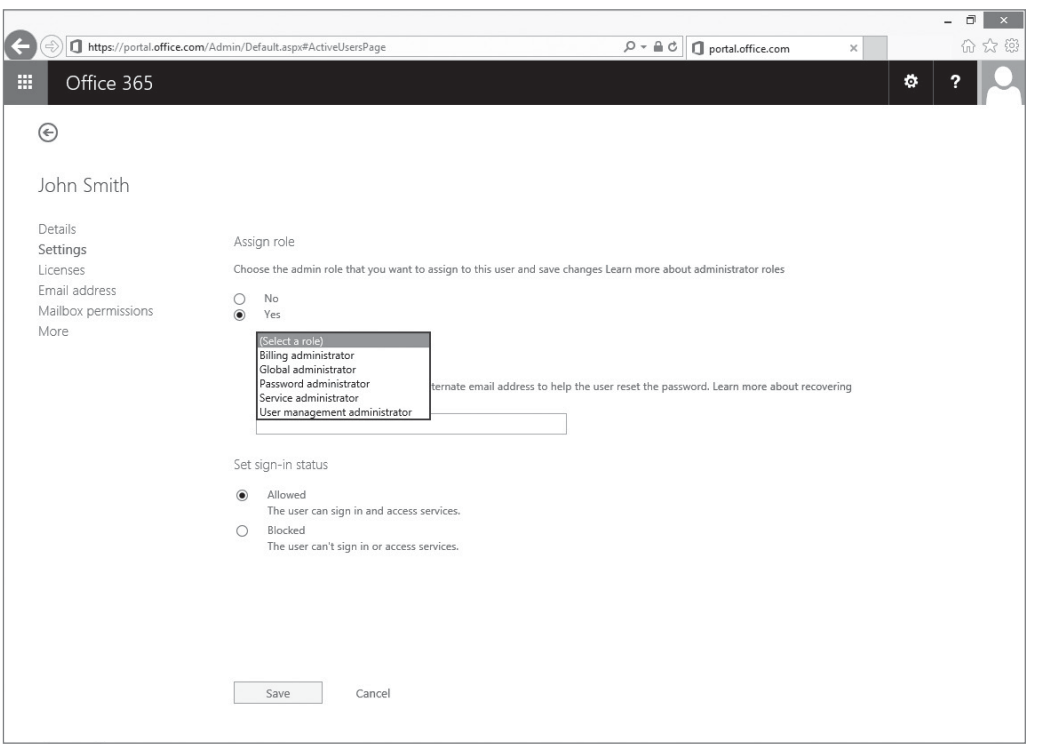
- ***Global Administrator*:** Has access to all administrative features. This is the person who signs up for Office 365. Only a Global Administrator can assign other administrative roles. Only one person in the company can serve in this role.
- ***Billing Administrator*:** Manages purchases, support tickets, and subscriptions; monitors the overall health of the services.
- ***Password Administrator*:** Manages requests for services, resets passwords, and monitors the overall health of the services. Users in this role can reset passwords only for users and other Password Administrators.
- ***Service Administrator*:** Manages service requests and monitors overall health of services.
- ***User Management Administrator*:** Manages user accounts and user groups, resets passwords, and manages service requests. User Management Administrators can also monitor the overall health of services. They cannot reset passwords for Billing, Global, or Service Administrators and they cannot delete a Global Administrator or create other administrators.

ASSIGN AN ADMINISTRATOR ROLE TO A USER IN OFFICE 365

GET READY. To assign an administrator role to a user in the Office 365 Admin Portal as the Global Administrator, perform the following steps.

1. On Win10A, log on using the **contoso\administrator** account and the **Pa$$word** password.
2. On the Taskbar, click the **Microsoft Edge** icon to open Microsoft Edge and then open and sign into Office 365 (https://portal.office.com).
3. Click the **Admin** button, click **USERS,** and then click **Active Users**.
4. Select the user whose administrator role you want to change and then click **Edit**.
5. Click **Settings**. Under Assign role, click **Yes**.
6. Choose a role from the list, as shown in Figure 3-7.

Figure 3-7
Assigning a role to a user



7. In the Alternate email address box, type an email address that is not connected to Office 365. This email address is used for important notifications, including resetting your administrator password, so the user must be able to access the email account whether the user can access Office 365 or not.
8. Click **Details**. Click the arrow next to Additional details, and in the Mobile phone text box, type the number of a mobile phone—including the country code if the user has one—that can receive a text (SMS) message. This phone number is also used in the process of resetting your administrator password.
9. When you have finished, click **Save**.

Some organizations might choose to have an individual manage the organization's Office 365 subscriptions and licenses by assigning a user as a delegated administrator. The roles a ***Microsoft partner*** (a Microsoft-designated independent company that provides Microsoft-related products or services) can set is:

- Full administration, which has privileges equivalent to a Global Administrator
- Limited administration, which has privileges equivalent to a Password Administrator

To add a Delegated Administrator in Office 365, the partner sends an email asking for permission to act as a Delegated Administrator. After you read the partner's terms in the email, you can authorize the agreement by clicking the link. When the authorization page in Office 365 opens, under delegated administration, click yes to authorize the partner to be your delegated administrator. You can then review the delegated administrators by clicking the Delegated admins under Users in the Office 365 Admin Portal.

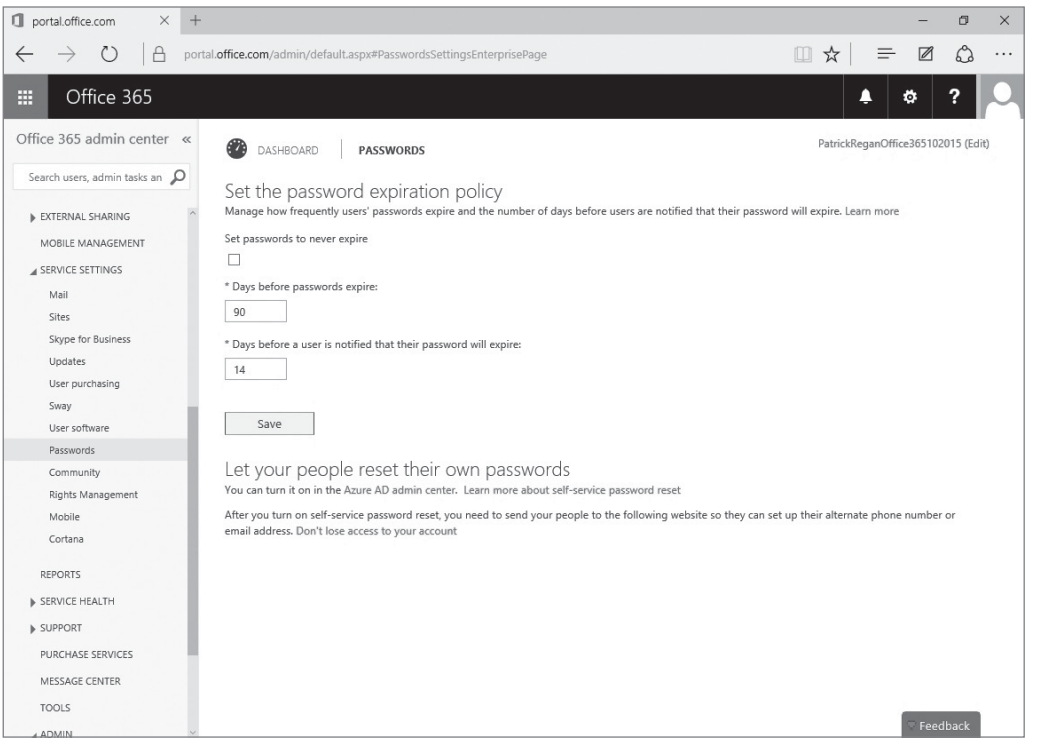
To ensure users change their passwords on a regular basis, you need to configure a password policy in Office 365. The password policy will make user passwords expire after a certain number of days. You can also change the number of days before users are notified of password expirations and you can configure a policy whereby the password never expires.

CONFIGURE A PASSWORD EXPIRATION POLICY IN OFFICE 365

GET READY. To configure a password expiration policy in Office 365, log into the Office 365 Admin Portal as the Global Administrator and then perform the following steps.

1. On Win10A, log on using the **contoso\administrator** account and the **Pa$$word** password.
2. On the Taskbar, click the **Microsoft Edge** icon to open Microsoft Edge and then open and sign into Office 365 (https://portal.office.com).
3. Click **Admin**. Then from the menu on the left, click **SERVICE SETTINGS**.
4. In the menu at the top, click **Passwords**.
5. In the Days before passwords expire field (see Figure 3-8), type **100.** The default is set to 90 days.
6. In the Days before a user is notified that their password will expire field, type **20.** The default is set to 14 days.

Figure 3-8
Changing the password expiration policy



7. Click **Save**.

Monitoring Service Health in Office 365

As users depend upon Office 365 more and more, you will want to make sure you monitor the health of the services you provide. Office 365 provides an excellent dashboard to monitor the current status of all services and to learn about any upcoming planned maintenance.

CERTIFICATION READY
Monitor service health in Office 365
3.3

The Service Health option shows seven days of health history, including today, in the Office 365 Admin Portal. You can also click to view the past 30 days of health history if desired and if any planned maintenance is coming.

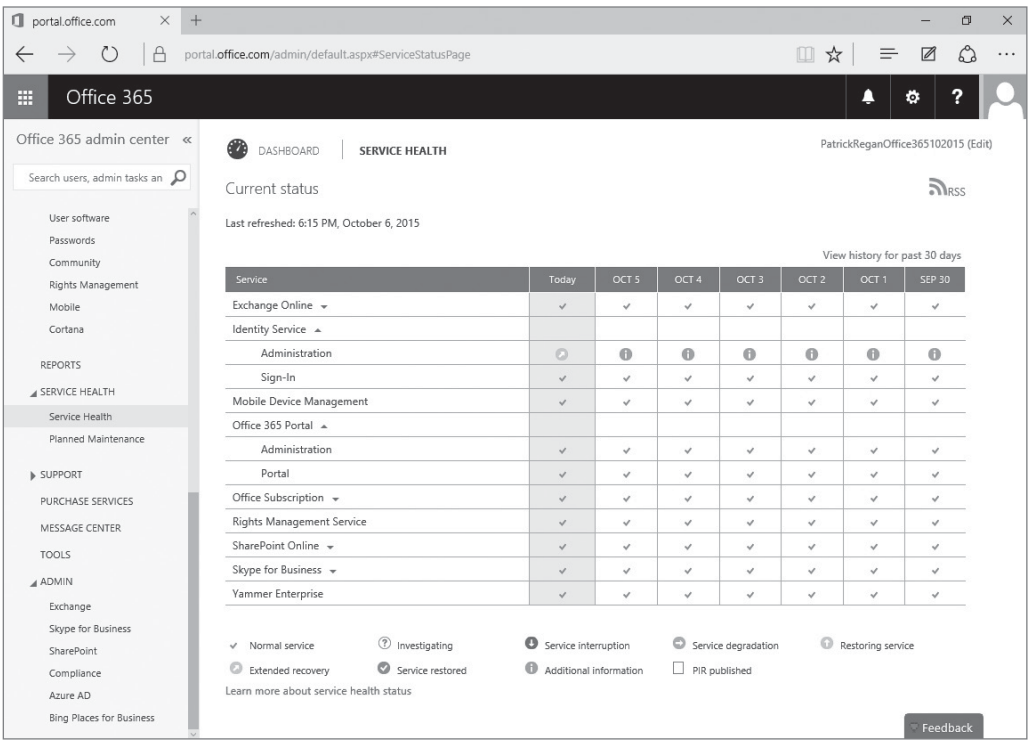
VIEW THE OVERALL HEALTH OF OFFICE 365

GET READY. To view the overall health of Office 365, log into your Office 365 Admin Portal as the Global Administrator and then perform the following steps.

1. On Win10A, log on using the **contoso\administrator** account and the **Pa$$word** password.
2. On the Taskbar, click the **Microsoft Edge** icon to open Microsoft Edge and then open and sign into Office 365 (https://portal.office.com).
3. Click **Admin**. In the menu on the left, expand SERVICE HEALTH by clicking **SERVICE HEALTH**. Then to view the current status of the services provided by Office 365 (see Figure 3-9), click **Service Health**.

Figure 3-9

Reviewing the status of Office 365 services

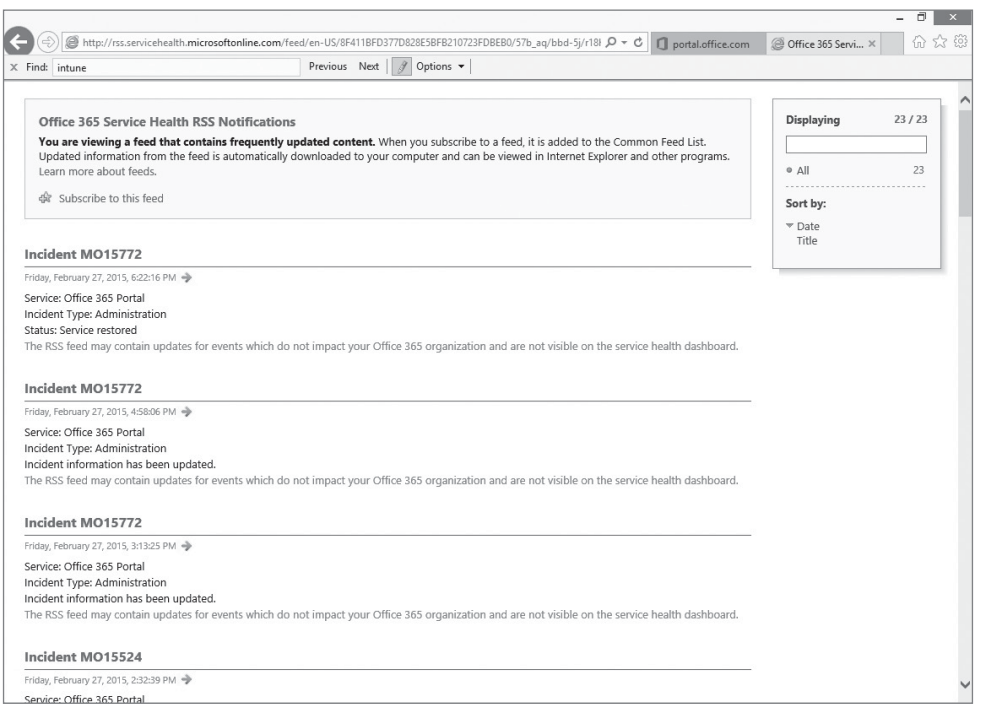


4. To determine whether there is an upcoming maintenance planned, click **Planned Maintenance**.

At the top-right of the Current status window, you will see an RSS link. ***RSS*** (Rich Site Summary or Really Simple Syndicate) is a family of standard web feed formats that are published frequently with updated information. An RSS feed is used to receive timely updates of a website or aggregate data from a site. It can be used with blog entries and news headlines. Since your organization can depend on Office 365, you can click the RSS link to subscribe to the RSS feed so that you can quickly check the status of your Office 365 subscription. To subscribe to the feed, click the Subscribe to this feed link (as shown in Figure 3-10). RSS feeds can be read from Microsoft Outlook.

Figure 3-10

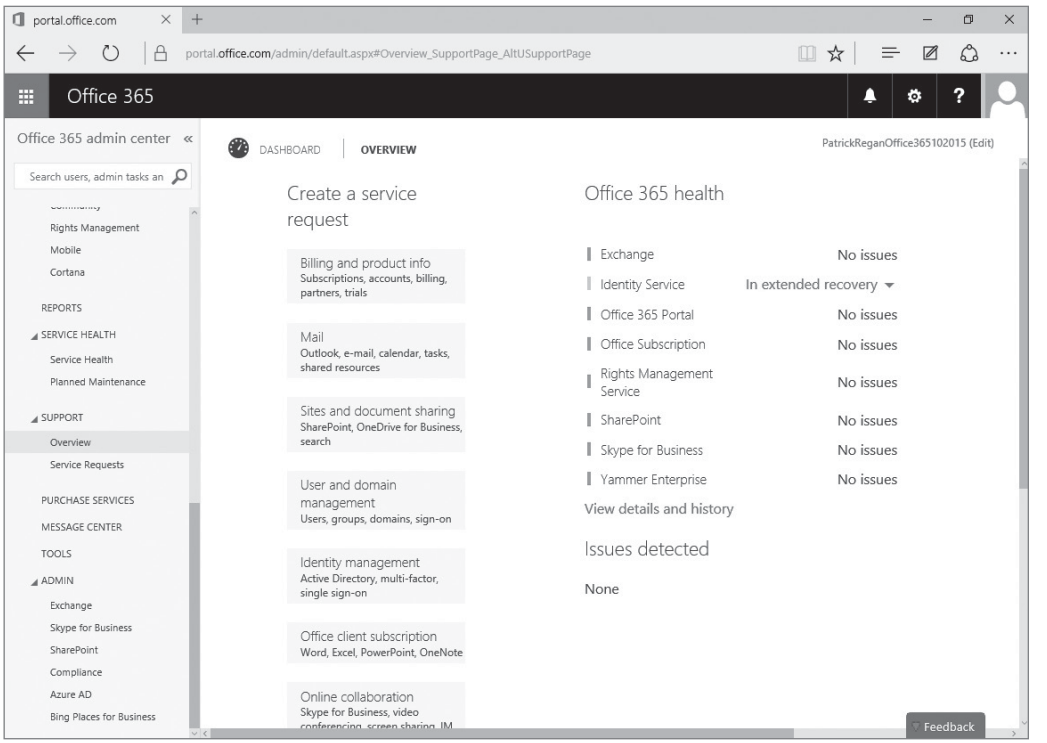
Subscribing to an Office 365 health feed



To quickly view health of Office 365, you can expand the SUPPORT option and then click Overview, as shown in Figure 3-11. Any issues will be displayed under the Issues detected section.

Figure 3-11

An overview of Office 365 health



If you have any problems with Office 365, you can open a service request by selecting the appropriate category under the Create a service request section, such as Billing, Mail, Online collaboration, Sites and document sharing, and so on. To view the status of your service request, expand SUPPORT and click Service Requests.

■ Administering Microsoft Intune

THE BOTTOM LINE

Because Microsoft Intune is a cloud-based tool, it is managed using the Microsoft Intune account portal (https://manage.microsoft.com), where you can add users, create groups, create policies, and configure alerts. You can also configure updates and software to be installed.

When you set up Microsoft Intune and then sign up for Microsoft Intune, you will need to perform the following steps.

1. Add Intune Users.
2. Create groups to organize users and devices.
3. Create policies and prepare to deploy an application Install Intune software on computers.
4. Set up mobile devices to work with Intune.
5. Configure alerts, notifications, and reports.

Creating Users and Groups and Assigning Services and Licenses in Microsoft Intune

To make the process of deploying Microsoft Intune policies, software packages, and software updates more efficient, consider using Microsoft Intune groups. ***Microsoft Intune groups***, which are used to quickly organize and manage your computers and users, are created and managed in the Groups workspace.

CERTIFICATION READY
Create users and groups, and assign services and licenses
3.1

Microsoft Intune groups are separate from Active Directory groups, although you can use AD security groups as part of a query to select members when creating a Microsoft Intune group. After your groups are set up, you can deploy Microsoft Intune policies, software packages, and software updates to them.

ADDING USERS TO MICROSOFT INTUNE

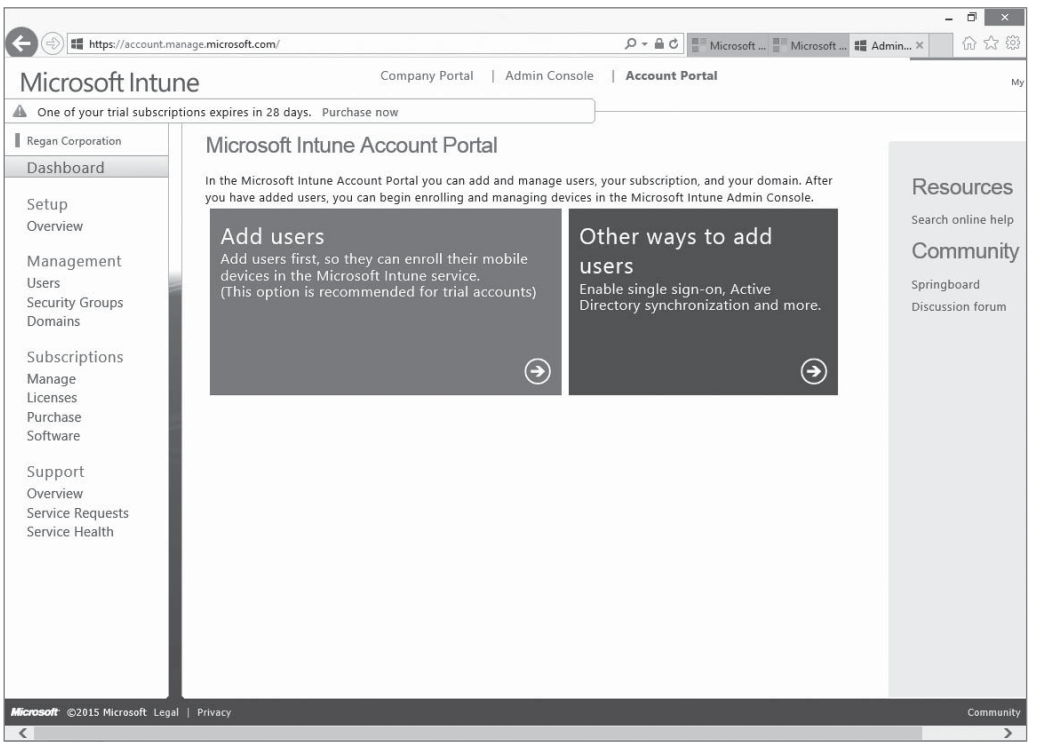
Before users can enroll their devices, they must be members of a Microsoft Intune user group. When you provision users, you define device owners as managed users in Microsoft Intune.

ADD A USER FROM THE MICROSOFT INTUNE ACCOUNT PORTAL

GET READY. To add a user from the Microsoft Intune Account Portal, perform the following steps.

1. Log in to the **Microsoft Intune Account Portal** at https://account.manage.microsoft.com.
2. Click **Add users**, as shown in Figure 3-12.

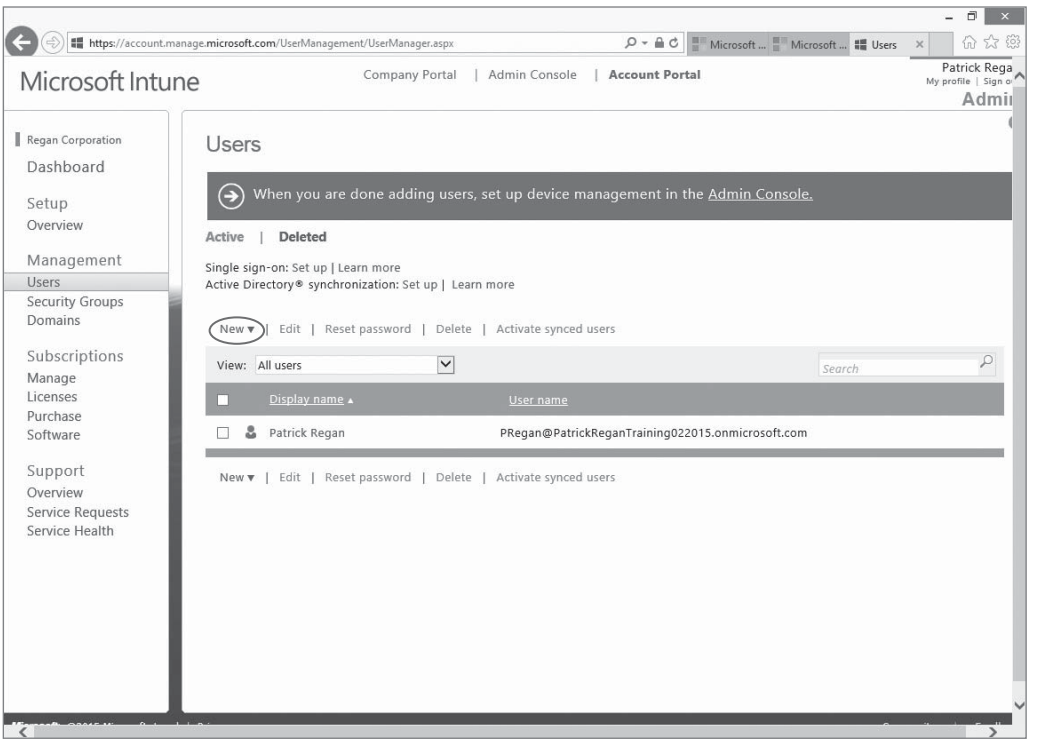
Figure 3-12
Adding users



3. On the Users page (see Figure 3-13), click **New > User**.
4. On the Details page, in the appropriate text boxes, type the first name, last name, display name, and user name. Click **Next**.

Figure 3-13

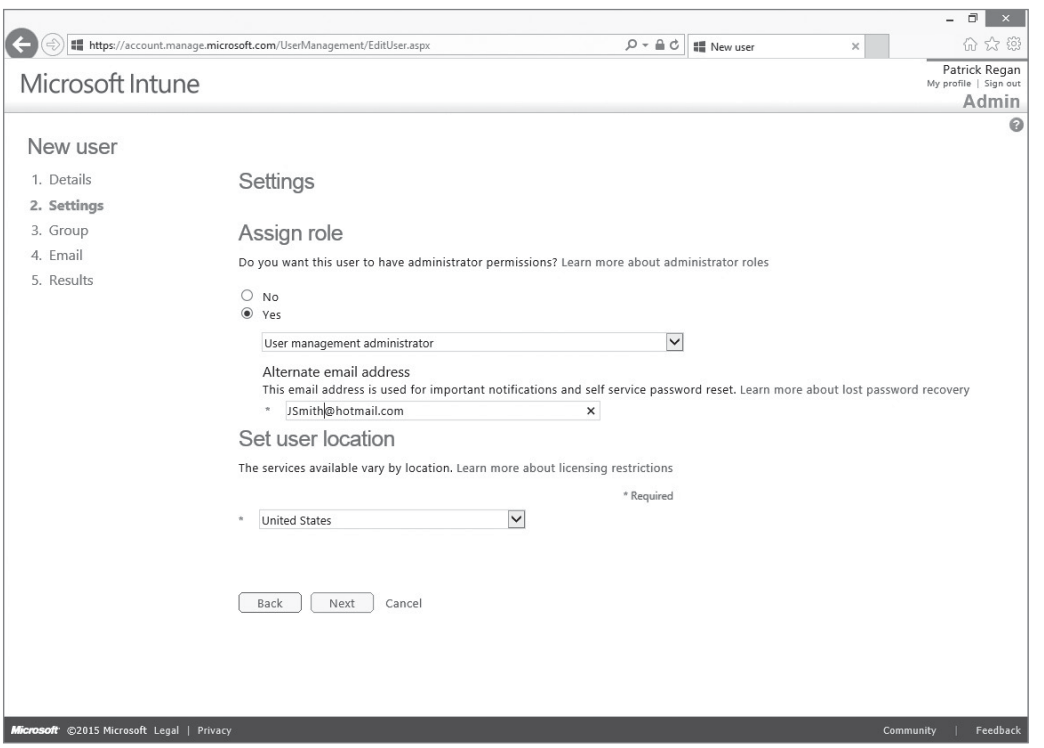
Managing Users



5. On the Settings page, specify **Yes** or **No** if you want the user to have administrator permissions. If you select Yes (as shown in Figure 3-14), you can choose one of the following:
   - Billing administrator
   - Global administrator
   - Password administrator
   - Service Support Administrator
   - User management administrator

Figure 3-14

Assigning roles



6. In the Set user location area, specify the user location. Click **Next**.
7. On the Group page, click **Next** to accept the default and assign a license for Intune to the user's account.
8. On the Email page, in the text box, specify up to five email addresses that will receive notifications of the user name and temporary password for the account. If you have more than one email address, separate the addresses with a semicolon (;). Click **Create**.
9. On the Results page, you can view the new account name and its temporary password. Intune automatically creates the temporary password. Click **Finish**.

When you add user accounts to your subscription, Intune assigns an available license to the user account. If you need to revoke a license, simply select the user in the Intune console and then click Edit.

ADDING COMPUTERS TO MICROSOFT INTUNE

You can install the Microsoft Intune client on computers running Windows XP Professional (SP3), Windows Vista (Enterprise, Ultimate, or Business Edition), Windows 7 (Enterprise, Ultimate, or Professional), and Windows 8/8.1 (Professional and Enterprise), or Windows 10 (Professional and Enterprise). You can deploy the Microsoft Intune client on both physical computers and virtual machines.

Before installing the Microsoft Intune client, you need to consider how you want to handle malware. If you have existing software that protects against these types of threats, Microsoft Intune Endpoint Protection detects the software and does not install the Endpoint component.

The following options are available for deploying the client:

- **Administrator deployment:** Using this option, you basically download the client software and manually install it on the target computers. When you need to install it on a large number of computers, you can automate the process by using Group Policy.
- **User-initiated enrollment for computers:** Using this option, users can self-enroll their computers through the Microsoft Intune company portal.
- **Install the client software as part of an image:** Using this option, you can deploy the Microsoft Intune client as part of a system image deployment. The computer is automatically enrolled when the image is installed.

PERFORM AN ADMINISTRATOR DEPLOYMENT OF THE MICROSOFT INTUNE CLIENT

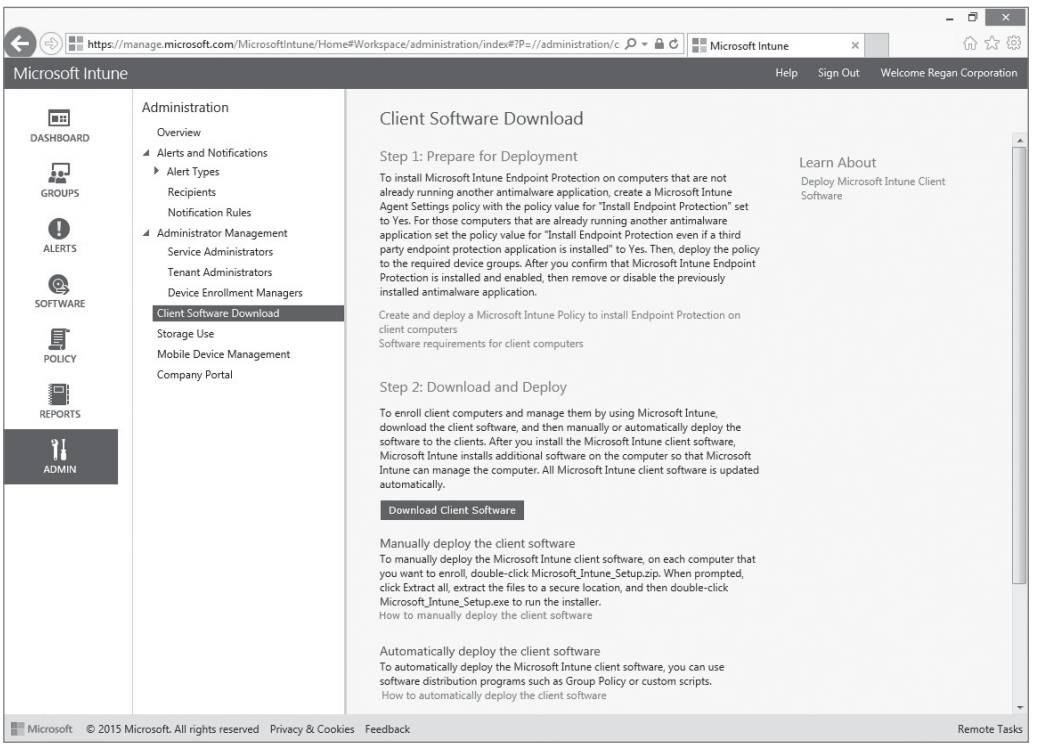
GET READY. You need to agree to and set up a Microsoft Intune account to complete this exercise. To complete an administrative deployment of the Microsoft Intune client on a Windows 10 computer, perform the following steps.

1. Log in to the Windows 10 computer on which you want to install the Microsoft Intune Client software.
2. Open Microsoft Edge, type **https://manage.microsoft.com** into the address field, and then press **Enter**.
3. If the message This application requires Microsoft Silverlight appears, click **Get Microsoft Silverlight** and then select **Run**.
4. To accept the licensing agreement, click **Install now**.

5. On the Enable Microsoft Update page, click **Next**.
6. On the Dashboard, click Start Managing Computers.
7. On the Client Software Download page, as shown in Figure 3-15, click **Download Client Software**.

Figure 3-15

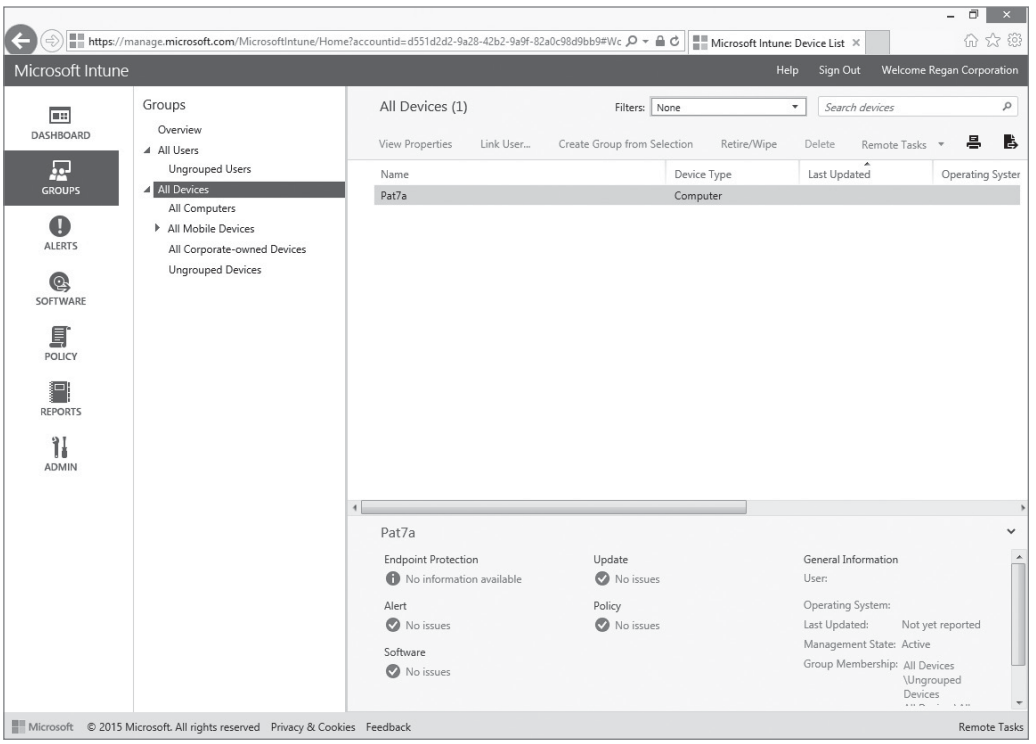
Downloading Microsoft Intune client software



8. From the Windows Edge box, click **Save as**.
9. In the Save As box, click **Desktop** and then click **Save**. This places a file named Windows_Intune_Setup.zip on your desktop.
10. Minimize the Microsoft Intune console, right-click the **Windows_Intune_Setup.zip** file and choose **Extract All**.
11. In the Select a Destination and Extract Files box, click **Extract**. After the extraction has completed, you should see two files: Windows_Intune_Setup.exe and WindowsIntune.accountcert. These files must be kept together at all times. The WindowsIntune.accountcert is used by the setup program.
12. Double-click **Windows_Intune_Setup.exe.**
13. In the Microsoft Intune Setup Wizard, click **Next**.
14. Click **Finish**. Microsoft Intune continues to update and install software on the computer. You can use the computer while the process continues in the background.
15. Maximize the Microsoft Intune console and then click in the left pane. When the pane slides out, click **Groups > All Devices**. When the installation is done, you should see the computer name listed (see Figure 3-16).

Figure 3-16

Viewing the computer as it appears in the Microsoft Intune Admin Console



TAKE NOTE* After the installation has completed, the protection and update agents continue to perform additional setup and configuration steps. This includes downloading the required malware definitions and any other agent updates. The computer should appear in the Microsoft Intune Admin Console in a few minutes, but it can take up to 30 minutes to complete the inventory and for the status updates to process.

In the previous exercise, you performed an Administrator deployment and the Windows 8/8.1 computer was enrolled as part of the installation. If you wanted to allow your users to self-enroll their computers, they would need to be an administrator on the local computer, connect to the Microsoft Intune portal using an Internet Explorer or Microsoft Edge browser, and use a Microsoft Online ID. To learn more about how self-enroll works, visit Microsoft and search "Microsoft Intune User-Initiated Enrollment for Computers." When performing this process, these are the general steps:

1. Click All My Devices.
2. Click Enroll your computer.
3. Click Download Software.
4. Click Run.
5. Click Next to. To start the Microsoft Intune Setup Wizard, click Next.
6. Click Finish when. When the installation is completed, click Finish.

TAKE NOTE* To install the Microsoft Intune Client as part of an image, search Microsoft's website for "Microsoft Intune Installing the Client Software as Part of an Image." When working with images, you will most likely deploy them to multiple computers, which might not be connected to the Internet. For an installation of the client to complete, you need an Internet connection; therefore, you need to make sure the computer with the image is not enrolled before it has been fully deployed to the client. To accomplish this, you can perform a delayed installation of the Microsoft Intune client by using the following command-line argument to launch the install: Windows_Intune_Setup.exe /PrepareEnroll.

ADDING DEVICES TO MICROSOFT INTUNE

Microsoft Intune can also be used to protect and manage devices such as tablets and smartphones running Android, iOS, Windows Phone, or Windows RT operating systems while allowing users access to company email, data, and applications.

TAKE NOTE* Using the Microsoft Intune client software, computers running Windows 8.1 or 10 can be managed as mobile devices or as computers.

Before you can enroll mobile devices, you must prepare the Intune service by selecting the appropriate Mobile Device Management (MDM) authority. The MDM authority setting determines whether you manage mobile devices by using Microsoft Intune or by using System Center Configuration Manager with Intune integration.

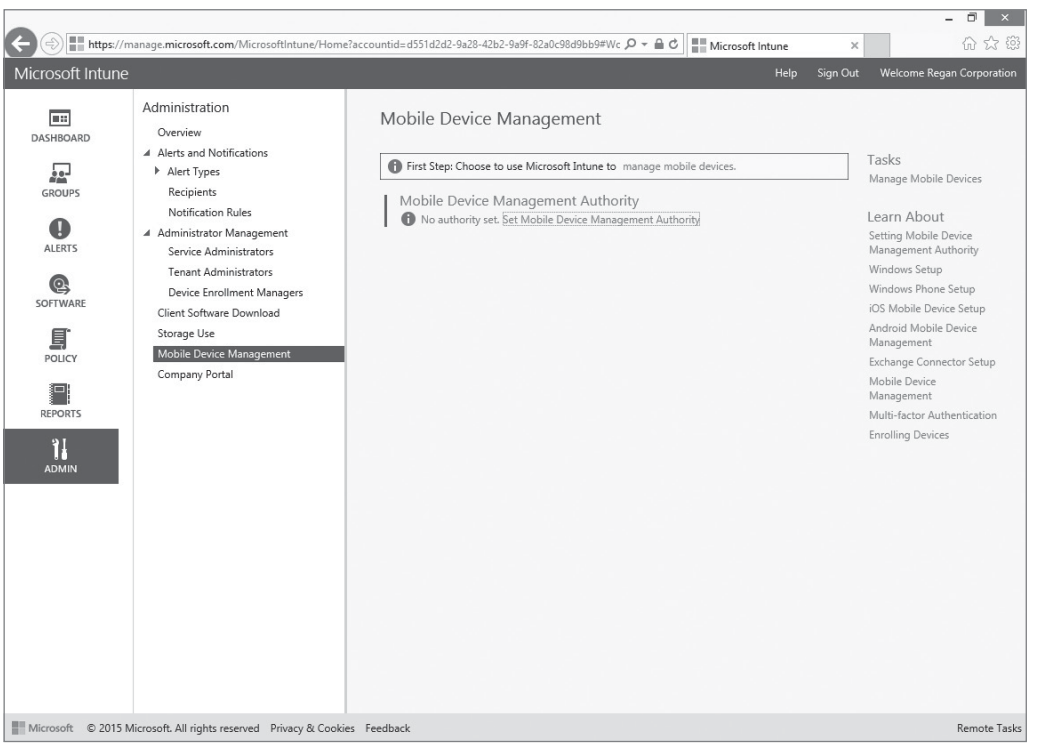
SET THE MOBILE DEVICE MANAGEMENT (MDM) AUTHORITY

GET READY. To set the MDM authority for Microsoft Intune, from the Microsoft Intune Admin Console, perform the following steps.

1. Log in to the **Microsoft Intune Admin Console** at https://admin.manage.microsoft.com.
2. Click **Admin** and then click **Mobile Device Management**, as shown in Figure 3-17.

Figure 3-17

Viewing Mobile Device Management



3. Click **Set Mobile Device Management Authority**.
4. In the Mvanage Mobile Devices dialog box, select the **Use Microsoft Intune to manage my mobile devices** option. Be sure to read the warning. Click **OK**.
5. Click **OK**.

You can enroll devices by enabling mobile device enrollment with the Microsoft Intune Company Portal or you can enroll corporate-owned devices with the Device Enrollment Manager in Microsoft Intune.

With Microsoft Intune, you can manage mobile devices directly or through Exchange ActiveSync. Exchange devices can be managed using on-premises servers and hosted Microsoft Office 365 Exchange in the cloud. If System Center 2012 R2/2016 Configuration Manager is deployed in your environment, you can use the Microsoft Intune service to manage mobile devices while performing all management tasks in the System Center Configuration Manager console.

Microsoft Intune can manage Windows Phone 8/8.1 and Windows 10 devices, iOS devices, and Android devices. To enroll Windows devices, you must deploy the Microsoft Intune Company Portal app to the devices. The Company Portal app, which can be downloaded from Microsoft's Download Center, must be code-signed with a certificate that is trusted by Windows Phone 8/8.1 or Windows 10 devices.

To enroll iOS devices, you need to obtain an Apple Push notification service certificate that enables Microsoft Intune to securely communicate with the Apple Push Notification service. To obtain an Apple Push Notification, you must download the Certificate Signing Request from Microsoft Intune and then request an Apple Push Notification service certificate from the Apple website.

To enroll Android devices, you must download the Android Company Portal app from Google Play. This application allows you to enroll Android devices for direct management.

To enroll devices, you will need to perform the following steps:

1. Set the Mobile Device Management Authority for Microsoft Intune.
2. Set up direct management for mobile devices.
3. Provision users for device enrollment.
4. Enroll devices.

SET UP DIRECT MANAGEMENT FOR MOBILE DEVICES

GET READY. To set up direct management of Windows Phone 8/8.1 devices, perform the following steps.

1. Log in to the **Microsoft Intune Admin Console** at https://admin.manage.microsoft.com.
2. In the workspace shortcuts pane, click the **Admin** icon.
3. In the navigation pane, under Mobile Device Management, click **Windows Phone**. Figure 3-18 shows the Windows Phone Mobile Device Management Setup page.

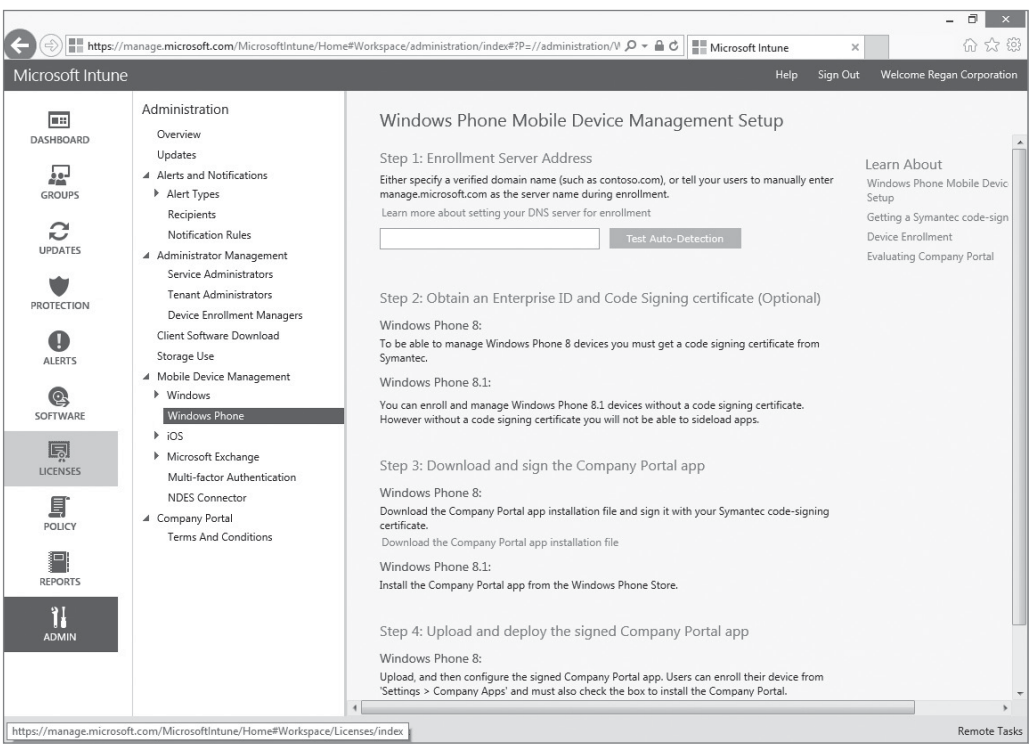


Figure 3-18

Setting up Windows Phone Mobile Device Management

4. Under Step 1: Enrollment Server Address, type the name of the verified domain and then click **Test Auto-Detection**.
5. Scroll down to the Step 5: Upload and Deploy the Company Portal section and click **Upload Signed App File**.
6. In the Microsoft Intune Software Publisher Wizard, click **Next**.
7. On the Software setup page for the Specify the location of the software setup files option, click the **Browse** button to browse to the signed Windows Phone 8 Company Portal app that you generated when you completed the prerequisites.
8. Under the Code-signing certification option, click the **Browse** button to browse to the code-signing certificate (.pfx) file. In the Certificate password text box, type a password for the certificate. Click **Next**.
9. On the Software description page, complete the fields (Publisher, Name, and Description). These fields will be seen by the users on their devices. You will also specify an URL for software information and specify a category. Click **Next**.
10. On the Summary page, click **Upload**.
11. When the software is uploaded, click **Close**. The company portal can now be automatically deployed to all users who enroll.

To enroll Windows 8.1 or Windows 10 devices, log in to the Intune portal and click Add Device. During this process, users will provide their credentials. After a certificate is installed on the device, the user must select Install company app or Hub so that the device can be managed by Intune.

When a user accesses the Company Portal, she will be prompted for credentials. If you didn't create a public domain CNAME, Windows and Windows Phone users are prompted for the server address and must type **manage.microsoft.com**. Windows Phone 8.1, Windows Phone 10, and iOS phone users can then view their Enrolled Devices to enroll their phones.

If it is the first time the user is visiting the portal, she will be prompted to access the terms and conditions. If the user accepts the terms and conditions, she will continue to the portal. If the user declines, she will receive a link to unenroll.

CREATING AND MANAGING GROUPS

You can create groups that include users and you can create groups that include devices. What you cannot do is include users and devices in the same group. Most administrators create groups that are organized in one or more of the following ways:

- **Geographical organization:** Portland, Seattle, Los Angeles
- **Departmental organization:** Executives, Human Resources, Marketing
- **Physical organization:** Desktops, Laptops

In the Groups workspace, you see the default groups created for devices and for users when Microsoft Intune is initially setup. For example, under the All Computers group, you will find the Windows 8.1/10 computer you installed the Microsoft Intune Client software on earlier.

After a closer look, you should see there is a hierarchy for the groups. For example, the All Direct Managed Devices and the All Exchange ActiveSync Managed Devices are child groups under the parent All Mobile Devices. You can deploy software updates, policies, and software applications to multiple groups or to a parent group while excluding one or more child groups. You can also add and exclude specific group members.

TAKE NOTE*

To protect your production environment, consider creating a test computer group that can be used to roll out and trial new updates. Once in place, you can select the members from within the Microsoft Intune Admin Console. This should be reflective of the different operating systems you want to test on. Even though computers are added to the new group, they still retain their membership in any other groups. This allows you to still assign updates to them without impacting other computers in those groups.

When setting up a group in Microsoft Intune, you have the option to manually or dynamically add users or devices to a group. You can also take a mixed approach and use both methods when creating a group.

- ***Direct membership*:** The process of manually adding users or devices from within the Microsoft Intune Admin Console. You can manually include and exclude specific members from the group.
- ***Criteria membership*:** This involves defining certain types of criteria that Microsoft Intune runs a query against to find users or devices. When it finds users or computers that match the criteria, it dynamically adds them as members to the group. The group automatically updates with members as changes occur.
- **Mixed:** A group that consists of members added manually and dynamically.

When adding devices to a group using membership criteria, you have the following options to include or exclude members from the parent group:

- Computers from organizational units you specify
- Computers from domains you specify

When defining direct membership, you have the option to include or exclude specific members form groups you specify.

Group membership is recursive. This means that if you use a dynamic membership query and set the criteria that a user is a member of an AD DS security group named Marketing to be included in the group, you can pick up additional indirect users in the query. For example, if Mary is a member of the Marketing Interns security group and the Marketing Interns security group is a member of the Marketing security group, then she is included in your query and added to the Marketing group.

CREATE A DEVICE GROUP USING DIRECT MEMBERSHIP

GET READY. To create a device group using Direct membership, from the Microsoft Intune Admin Console, perform the following steps.

1. Log in to the **Microsoft Intune Admin Console** at https://admin.manage.microsoft.com.
2. In the left pane, select **Groups**.
3. In the Tasks section, click the **Create Group**.
4. In the Group name field, type **My Test Group**.
5. In the Description field, type **Computers used to test deployments of new updates**.
6. Under Select a parent group, click **All Devices**.
7. Click **Next**.
8. On the Define Membership Criteria page (as shown in Figure 3-19), click **Next**.
9. On the Define Direct Membership page (as shown in Figure 3-20), click **Browse**. Be careful to select the Browse button that is just to the right of the Include specific members field. If you select the one on the far right, you will exclude specific members.
10. Choose the Windows 10 computer you installed the Microsoft Intune client software on in the earlier exercise and then click **Add**. Your Windows 10 computer should appear in the Include specific members column. Click **OK** to continue.
11. On the Define Direct Membership page, click **Next**.
12. Review the General Criteria Membership and Direct Membership summary page and then click **Finish**.
13. Under Groups, click **My Test Group**, and then click **Devices**. The computer should appear as a member of the group.

Figure 3-19

Defining membership criteria

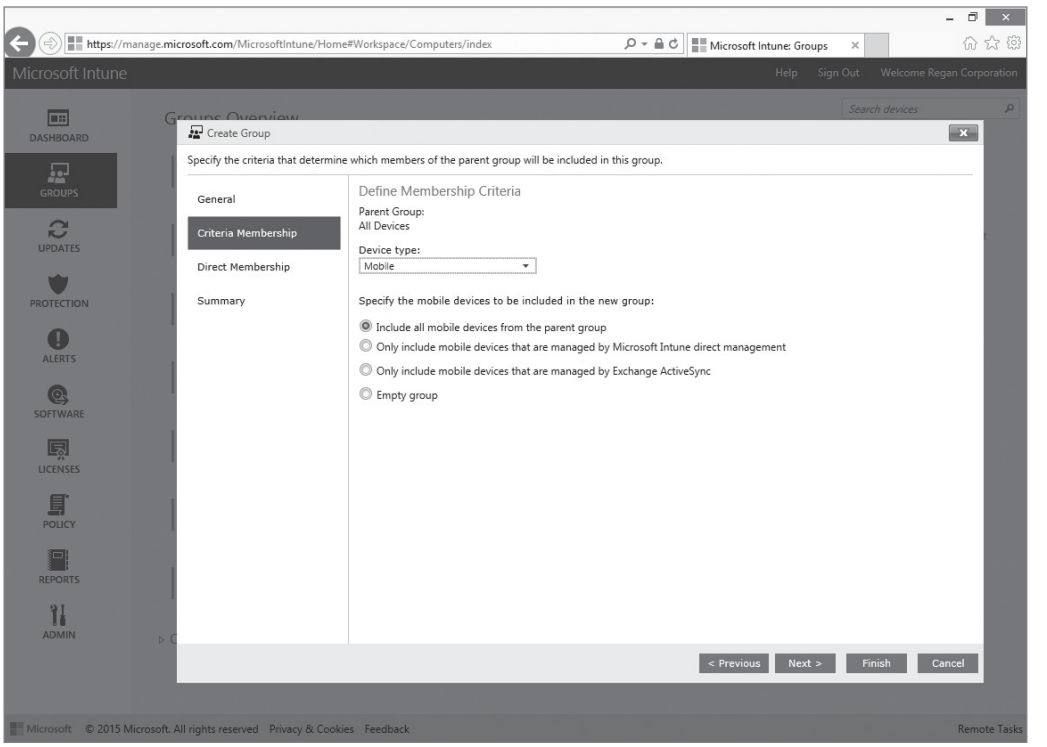
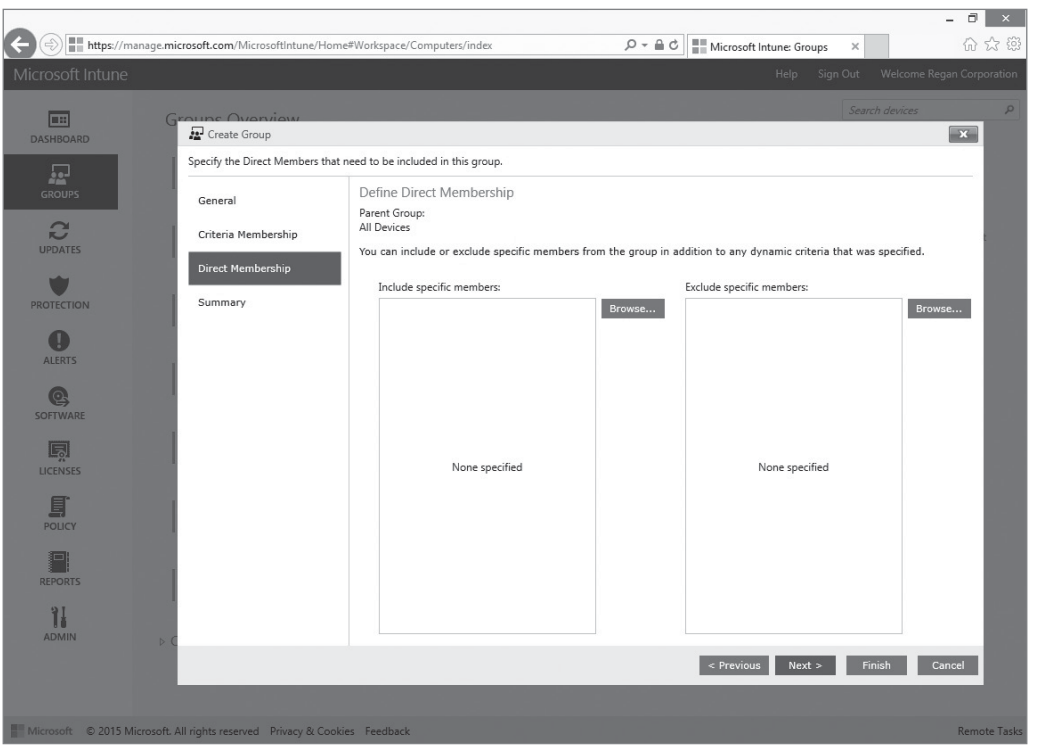


Figure 3-20

Specifying Direct membership



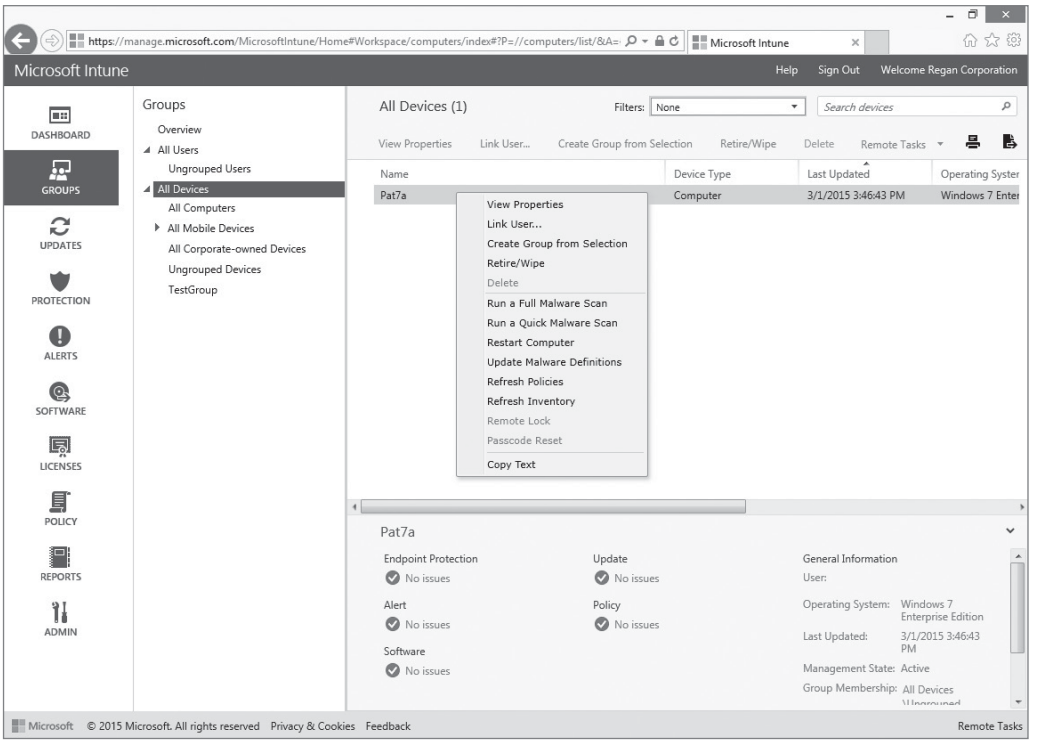
PROTECTING YOUR DATA USING MICROSOFT INTUNE

Because mobile devices can store sensitive corporate or private information, when the device is lost or stolen, the data on the device can pose a significant security risk. Once a device has been added to Microsoft Intune, you can perform a selective wipe that removes only company data, perform a full wipe that restores the device to its factory setting, perform a remote lock,

or perform a passcode reset, as shown in Figure 3-21. Based on whether the device is a smartphone or whether it is a computer, some of these options will not be available and thus will be grayed out.

Figure 3-21

Managing a device in Microsoft Intune



Assigning Permissions in Microsoft Intune

Microsoft Intune can be a very powerful tool. As with any cloud solution, you must determine the best way to assign roles and permissions to Microsoft Intune.

CERTIFICATION READY
Assign permissions in Microsoft Intune
3.2

For most administrator functions, it is best to use the built-in roles that are included with Microsoft Intune. However, if you do not have a technical staff available within your company, you can use a Microsoft Partner to help assist in managing your devices.

ASSIGNING OR REVOKING ADMINISTRATIVE ROLES

Microsoft Intune supports two types of Administrator roles. Although each can gain access to the Microsoft Intune Admin Console, the roles do differ in the tasks they can execute:

- ***Microsoft Intune Tenant Administrator*:** Has full control and rights regarding the Admin Console. They can add or delete service administrator accounts and assign other tenant administrators. The person who sets up Microsoft Intune and accepts the Microsoft Online Subscription Agreement when it is purchased is assigned this role. You should create at least one more person with this role so you have a backup. Microsoft Tenant Administrators are assigned via the Microsoft Intune Admin Console at https://admin.manage.microsoft.com.
- ***Microsoft Intune Service Administrator*:** Has full access to the Microsoft Intune Admin Console and can perform all operations, including adding or deleting another Service Administrator account. They cannot modify data in the console; they can only view the data it contains and run reports. Microsoft Intune Service Administrators are assigned via the Microsoft Intune Admin Console at https://admin.manage.microsoft.com.

Each tenant administrator is assigned one of the following roles:

- ***Billing Administrator*:** Makes purchases, manages subscriptions, manages support tickets, and monitors service health.
- ***Global Administrator*:** Has access to all administrative features. The person who signs up for Microsoft Intune automatically becomes the first global administrator in your tenant. Only global administrators can assign other administrator roles.
- ***Password Administrator*:** Resets passwords, manages service requests, and monitors service health. Password administrators can reset passwords only for users and other password administrators.
- ***Service support administrator*:** Manages service requests and monitors service health.
- ***User management administrator*:** Resets passwords, monitors service health, and manages user accounts, user groups, and service requests.

If an organization has a large number of singe-user mobile devices, an organization can assign the Device Enrollment Manager role to an account so that the user can:

- Enroll more than five devices in Microsoft Intune
- Log on to the Company Portal to get company apps
- Install and uninstall software
- Configure access to company data

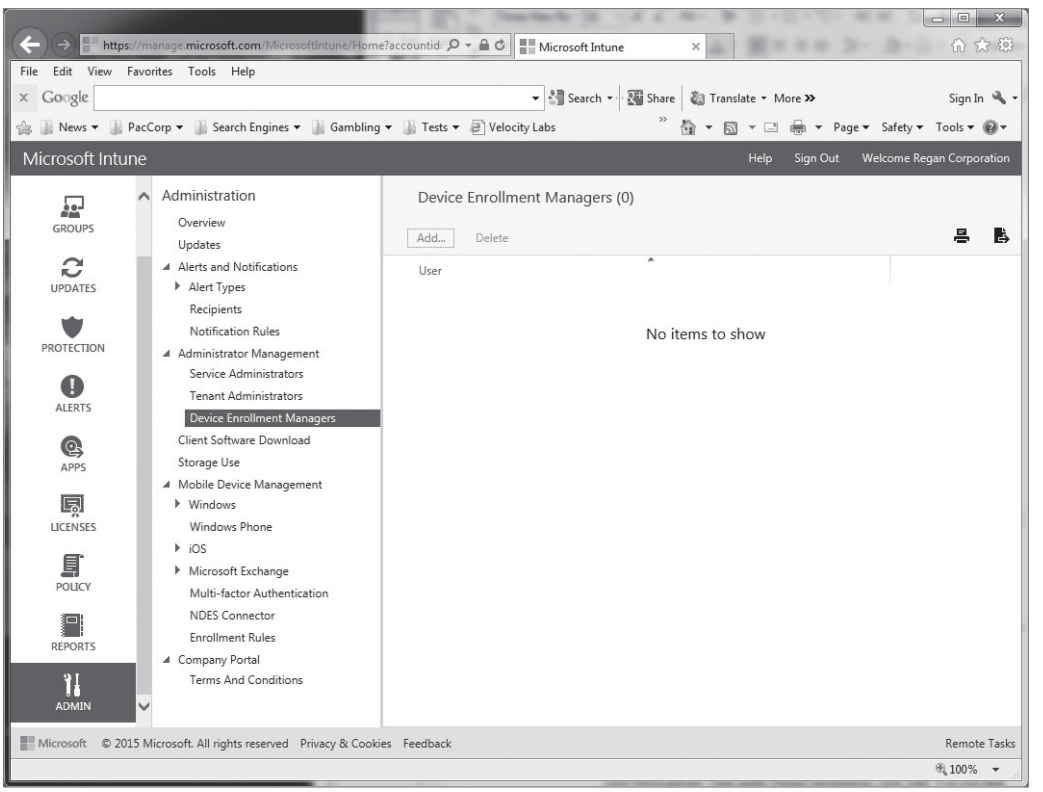
ADD A USER TO THE DEVICE ENROLLMENT MANAGER ROLE

GET READY. To add a user to the Device Enrollment Manager role, perform the following steps.

1. Log in to the **Microsoft Intune Account Portal** (https://admin.manage.microsoft.com).
2. In the navigation pane, click **Admin**
3. Click **Administrator Management > Device Enrollment Managers** (see Figure 3-22).

Figure 3-22

Adding a Device Enrollment Manager role



4. On the Device Enrollment Managers page, click **Add**.
5. In the Add Device Enrollment Manager dialog box, in the User ID text box, type the user ID of a Microsoft Intune account that is not an Intune administrator. Click **OK**.

TAKE NOTE*

Remember that Office 365 and Microsoft Intune have different administrators. While the two services are cloud services offered by Microsoft, management of these two services are separate from each other. In addition, Microsoft Intune has multiple portals/console for managing Microsoft Intune. The Microsoft Intune Admin Console is at https://manage.microsoft.com), which allows you to configure groups, updates, protection, alerts, apps, policies, and administrator roles. The Microsoft Intune Account Portal is at https://account.manage.microsoft.com; it is used to manage users, subscriptions, and service requests.

If you want to add or move a user to an administrative role, open the Microsoft Intune Account Portal (https://account.manage.microsoft.com), click Users, select the user you want to modify, and then click Edit. You then click the Settings tab and specify the tenant role.

MANAGING DELEGATED ADMINS

If you would like your systems to be managed by a Microsoft partner, open the Microsoft Intune Account Portal (https://account.manage.microsoft.com) and click Subscriptions. Then under Partner information, click Add. You will then be prompted to enter a Microsoft partner ID.

MANAGING POLICIES

Microsoft Intune has policies that help configure the security settings on mobile devices, computer updates, Endpoint Protection, firewall settings, and the end-user experience. These policies apply to domain-joined computers in any domain and to non-domain joined computers.

Since Group Policy can be used to set many of the same settings, when you deploy Microsoft Intune client software and establish Microsoft Intune policies, you need to ensure that the clients do not receive GPOs with similar and/or conflicting settings.

SET THE DEFAULT MICROSOFT INTUNE POLICIES

GET READY. To set up the default Microsoft Intune policies, perform the following steps.

1. Open the Microsoft Intune Admin Console (https://manage.microsoft.com) and click **Admin**.
2. Click **Policy**, as shown in Figure 3-23.
3. Under Tasks, click **Add Policy**.
4. In the Create a New Policy dialog box (as shown in Figure 3-24), the following policy templates are displayed in the list of templates in the left pane:
   - Mobile Device Security Policy
   - Windows Firewall Settings
   - Microsoft Intune Agent Settings
   - Microsoft Intune Center Settings
5. Select the policy template you wish to set up and then click **Create and Deploy a Policy with the Recommended Settings**. To view the settings before you create the policy, click **View the recommended settings for this policy template** that will be used as the default for this policy.
6. After you configure the settings that you want to apply in your default policy, type a name and an optional description for the policy and then click **Save Policy**.
7. When prompted to specify if you want to deploy the policy now, click **Yes**.

Figure 3-23

Managing policies

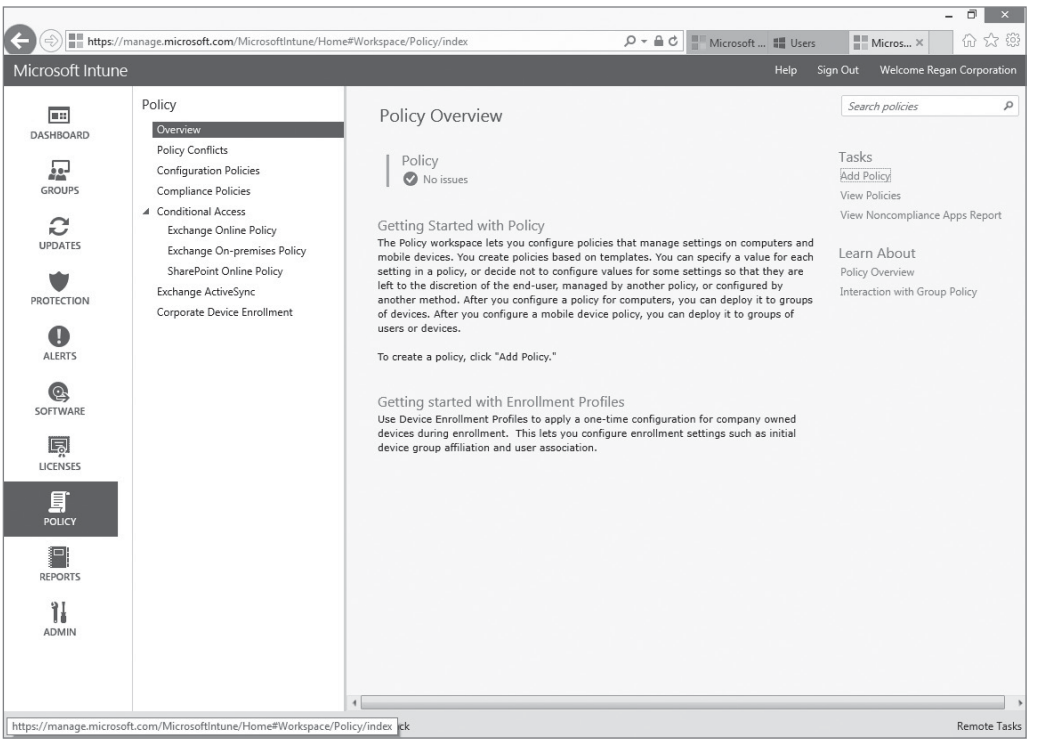
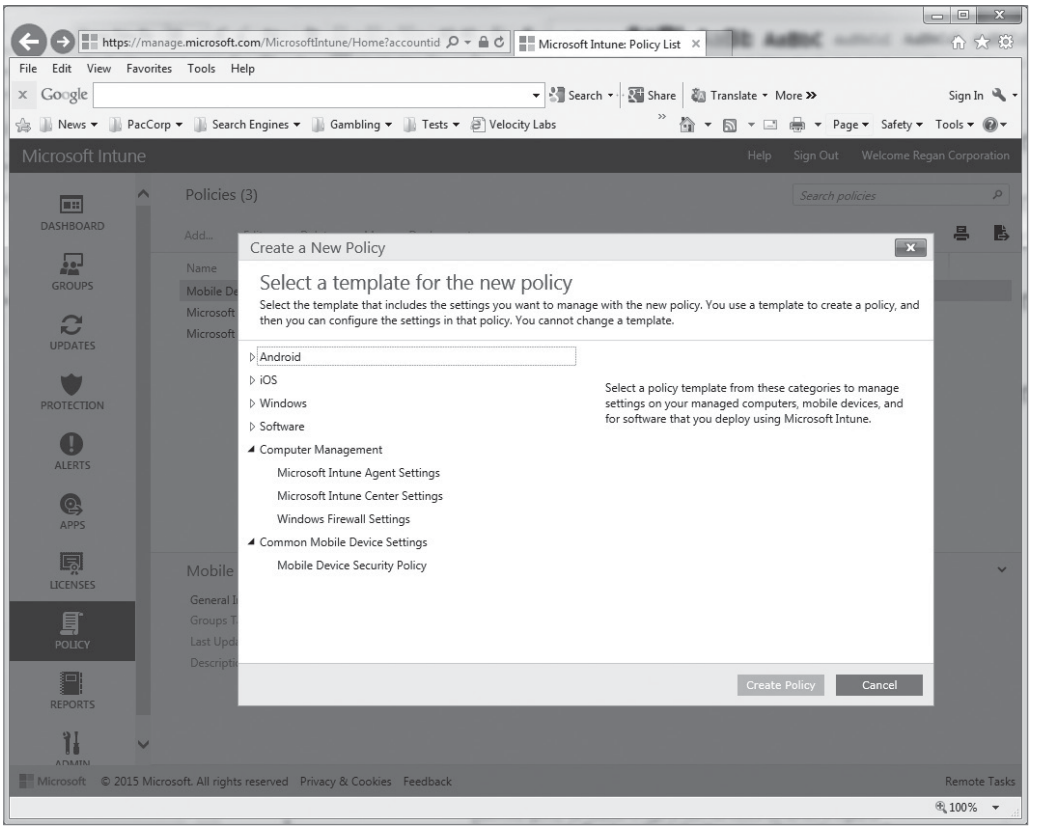


Figure 3-24

Adding a Microsoft Intune policy



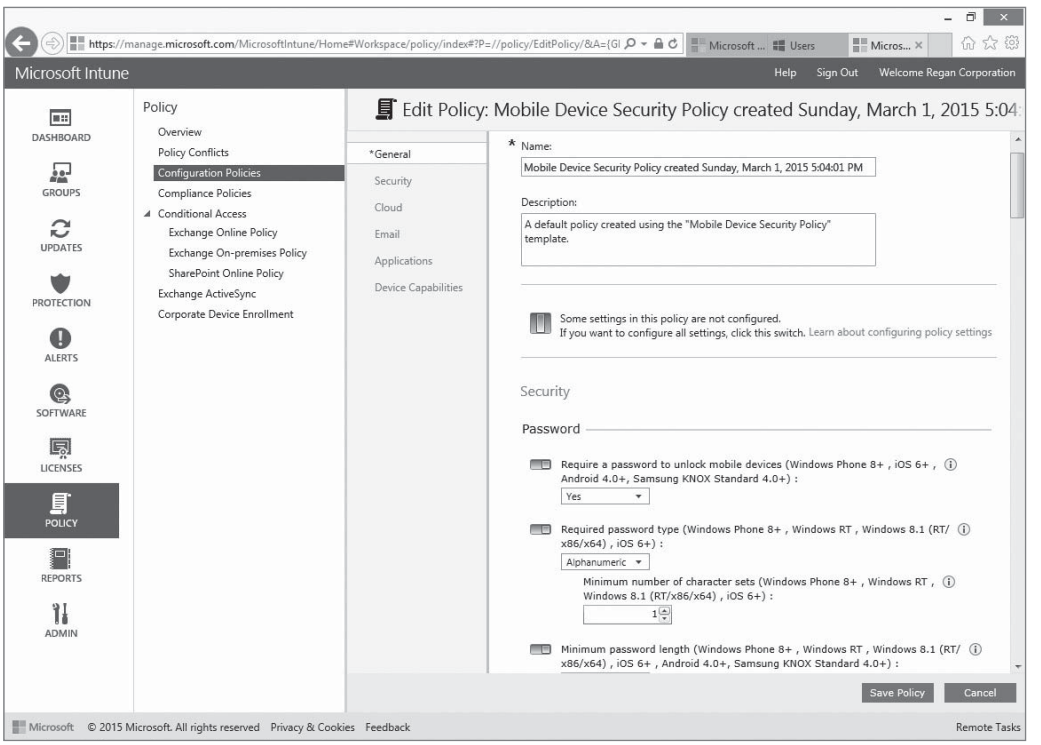
8. In the Select the groups to which you want to deploy this policy dialog box, select the **All Devices** group or **All Users** group (depending on the policy you have selected) and then click **OK**.
9. Repeat these steps as needed for your other default policy settings.

MANAGING PASSWORD POLICIES

To configure a password policy, you will configure a Mobile Device Security Policy, as shown in Figure 3-25. Within this option, you can require a password to unlock mobile devices, specify the type of password (alphanumeric or numeric), specify the minimum password length, specify a simple or strong password, specify the number of sign-in failovers before the device is wiped or the screen is turned off, and specify whether the system will remember password history so that the same password is not reused over and over.

Figure 3-25

Defining a password policy



MANAGING SUBSCRIPTIONS AND LICENSES

Managing your subscription and licenses is done with the Microsoft Intune Account Portal (https://account.manage.microsoft.com). By clicking the Manage link in the Subscription section, you can manage your billing and subscription.

Monitoring Service Health in Microsoft Intune

Computers configured with the Microsoft Intune agent can be tracked both on and off the corporate network. As computers are configured with the Microsoft Intune agent, they start to report back to Microsoft Intune. Because Microsoft Intune is cloud-based, users do not have to be attached to your corporate network to receive updates, patches, or receive help removing malware.

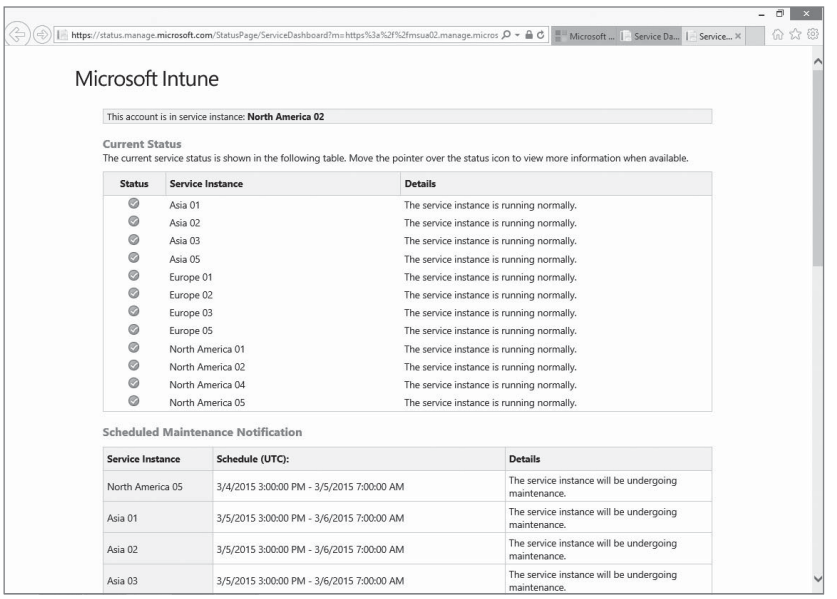
CERTIFICATION READY
Monitor service health in Microsoft Intune
3.3

MONITORING THE SERVICE HEALTH DASHBOARD AND MAINTENANCE SCHEDULE IN MICROSOFT INTUNE

To view the service status of Microsoft Intune, simply open the Microsoft Intune Admin Console, click Admin > Overview, and then click View Service Status. The Service Dashboard will show the current status and any upcoming scheduled maintenance, as shown in Figure 3-26.

Figure 3-26

Viewing the Microsoft Intune Service Dashboard



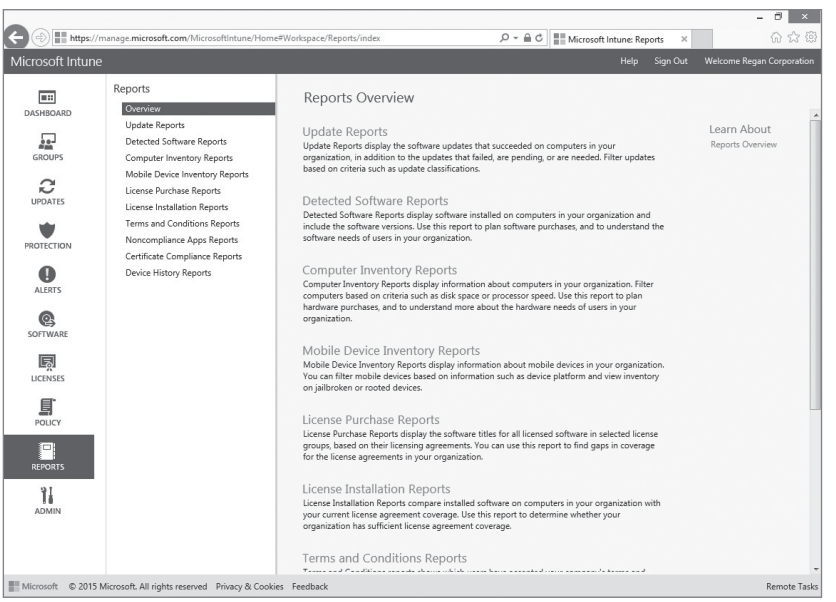
REVIEWING STANDARD REPORTS IN MICROSOFT INTUNE

Using Microsoft Intune, you can monitor your on-network and off-network machines through standard reports and you do so in real-time.

Microsoft Intune offers several types of reports. Although Microsoft Intune provides a snapshot of your machines through its reporting feature (see Figure 3-27), you should also monitor them in real time.

Figure 3-27

Reviewing Microsoft Intune standard reports



The various Microsoft Intune report types are described as follows:

- **Update Reports:** Provides information about software updates that succeeded, failed, or are currently pending or those that are needed on computers in your organization.
- **Detected Software Reports:** Provides information about software installed on computers in your organization.
- **Computer Inventory Reports:** Provides information about hardware used in your organization.

- **Mobile Device Inventory Reports:** Displays information about mobile devices in your organization.
- **License Purchase Reports:** Displays licensed software titles across your organization.
- **License Installation Reports:** Compares installed software with your current licensing agreement.
- **Terms and Conditions Reports:** Shows which users have accepted your company's terms and conditions and which versions they accepted.
- **Noncompliant Apps Reports:** Displays information about the users who have apps installed that are on the noncompliant; also displays a compliant apps list that you define.
- **Certificate Compliance Reports:** Displays which certificates have been issued to users and devices via the Network Device Enrollment Service.
- **Device History Reports:** Displays a historical log of retire, wipe, and delete actions.

Reports can be used to:

- Identify computers that are not running Endpoint Protection Software.
- Identify computers running another malware protection product.
- Investigate and troubleshoot malware activity.
- Identify computers that need updates or computers where updates have failed to install

CONFIGURING ALERT TYPES

The Alerts workspace is designed to help you quickly assess the overall health of the computers in your organization. By using alerts, you can gain a better understanding of how your computers are running and take the necessary steps to fix any problems before those problems impact user productivity. The Alerts workspace enables you to perform the following functions:

- Configure alert types.
- Select recipients for email notifications.
- Associate recipients with notification rules.

There are over 180 alert types available in Microsoft Intune. Based on your organization's needs, you can enable the alert types you think are important and disable those that are not appropriate for your network environment. You can also configure alert thresholds that are used to determine how often an alert is triggered before it is displayed.

Selecting an alert (as shown in Figure 3-28) provides you with additional information in the bottom pane.

SELECTING RECIPIENTS

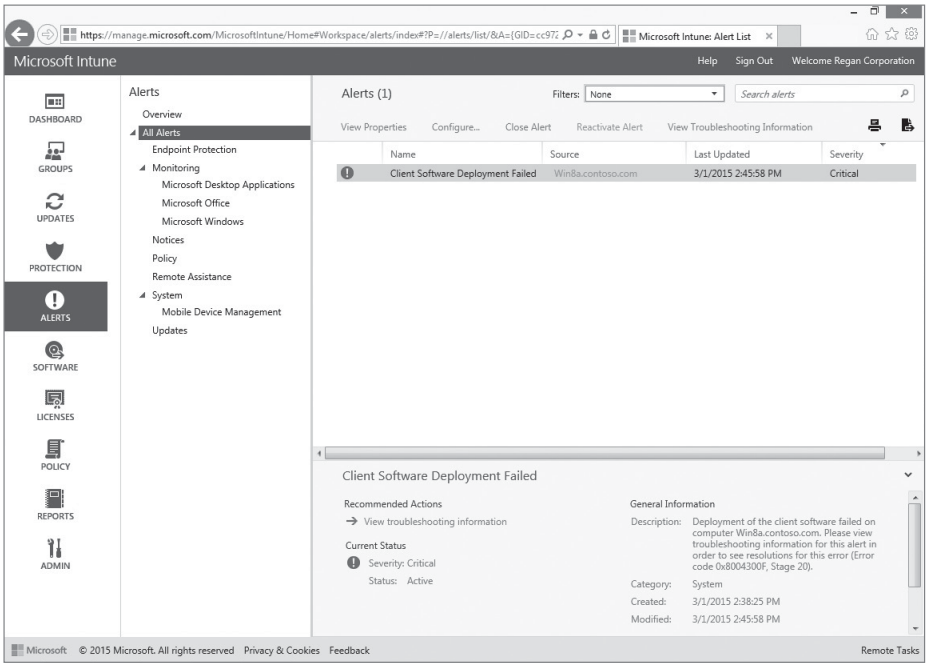
Recipients are individuals who you assign to receive email notifications when alerts occur. Recipients are assigned in the Admin > Alerts and Notifications > Recipients location of the Microsoft Intune Administrator console. To add a new recipient, just click Add and then type the recipient's email address and specify the language to use for email notification. After you have a list of recipients in place, you need to select Notification Rules.

Microsoft Intune includes five notification rules that you can target to a recipient:

- **All Alerts:** Shows all alerts, including critical, informational, and warning alerts.
- **Critical Alerts:** Shows only the most important alerts that affect the use of Microsoft Intune.
- **Informational Alerts:** Shows the lowest level of alerts.
- **Remote Assistance Requests:** Shows a list of remote assistance requests.
- **Warning Alerts:** Shows the second level of alerts that might indicate potential problems.

Figure 3-28

Viewing alert types



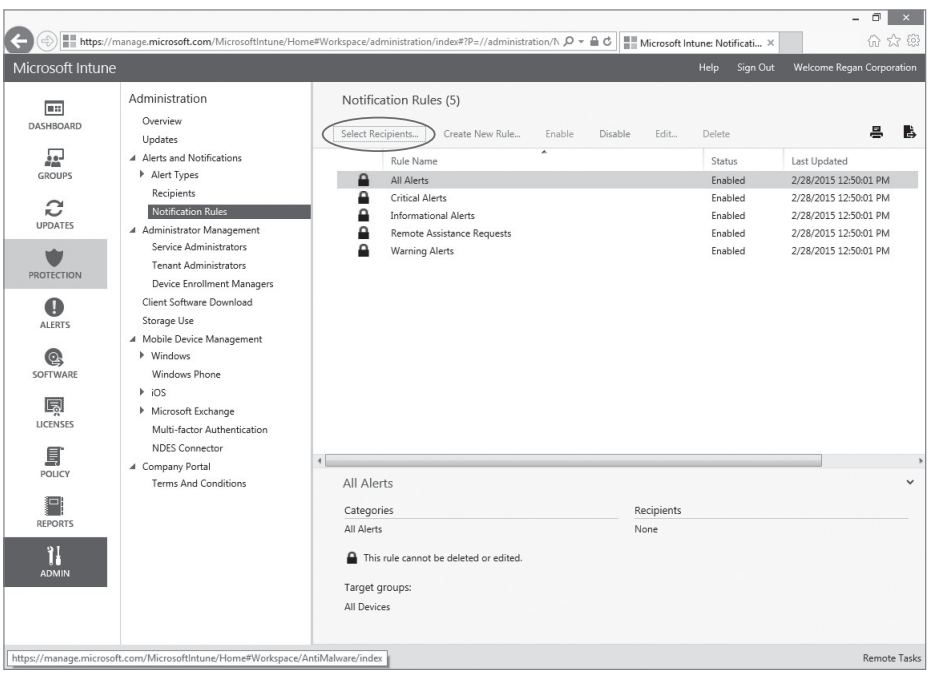
To add a recipient to one of these alert types, from the menu, choose ADMIN > Alerts and Notifications > Notifications Rules. Under Notification Rules, click the alert type, and then click Select Recipients (see Figure 3-29). Select the box next to each recipient that you want to receive email notifications specified by the rule and then click OK.

MANAGING SUPPORT REQUESTS

Technical support for Microsoft Intune is available online, by phone, or by using self-help. To find the telephone numbers and email addresses for technical support, you can logon to the Microsoft Intune Account Portal (https://account.manage.microsoft.com) and click Service Requests under the Support section. Self-help is available by clicking the Help link located at the top right-right corner of the Microsoft Intune Admin Console (https://manage.microsoft.com).

Figure 3-29

Selecting recipients for alert types



SUMMARY SKILL MATRIX

In this lesson you learned:

- Office 365 is administered through the Office 365 Admin Center through the https://portal.office.com/Admin website. From there, you can establish users and licenses, create groups, run reports, and manage services such as Exchange and SharePoint.
- Office 365 supports three sign-in models/identity models for Office 365. The model that you choose will determine how you manage your user accounts for Office 365 and how user passwords are verified.
- When you edit the assigned license, you can also define the user location for the user. The location specifies the datacenter location for hosting the content.
- As users depend upon Office 365 more and more, you will want to make sure you monitor the health of the services you provide. Office 365 provides an excellent dashboard to monitor the current status of all services and to learn about any upcoming planned maintenance.
- Microsoft Intune has multiple portals/consoles that can be used when managing Microsoft Intune. The Microsoft Intune Admin Console is at https://manage.microsoft.com; it allows you to configure groups, updates, protection, alerts, apps, policies, and administrator roles. The Microsoft Intune Account Portal is at https://account.manage.microsoft.com; it is used to manage users, subscriptions, and service requests.
- Because mobile devices can store sensitive corporate or private information, when the device is lost or stolen, the data on the device can pose a significant security risk. Once a device has been added to Microsoft Intune, you can perform a selective wipe that removes only company data, perform a full wipe that restores the device to its factory setting, perform a remote lock, or perform a passcode reset.
- As computers are configured with the Microsoft Intune agent, they start to report back to Microsoft Intune. Because Microsoft Intune is cloud-based, users do not have to be attached to your corporate network to receive updates, patches, or receive help removing malware.

■ Knowledge Assessment

Fill in the Blank

Complete the following sentences by writing the correct word or words in the blanks provided.

1. When using Office 365, _____ is used for identity management and access control.
2. The _____ has full access to all administrative features in Office 365.
3. When you would like a Microsoft partner to manage Office 365, the partner becomes a _____.
4. The easiest way to manage Office 365 issues is to subscribe to the _____.
5. In Microsoft Intune, when you manually add users or devices to a group, you are using _____.
6. _____ rights allow the administrator to reset passwords and manage user accounts and groups.
7. _____ provides information about software installed on computers in your organization.
8. In Office 365, the _____ includes accounts created manually with the Office 365 Admin Portal.
9. In Microsoft Intune, to enroll Windows devices, you must deploy the Windows Phone 8 _____.
10. When you install Windows_Intune_Setup.exe, you must also include _____.

Multiple Choice

Circle the letter that corresponds to the best answer.

1. Which of the following should be used to ensure that your Active Directory users are available in Office 365?
   a. Federated Identity Sync Tool
   b. Microsoft Intune Groups
   c. Azure Active Directory Sync (DirSync) Tool
   d. OAuth 2.0

2. Which of the following solutions should be used to quickly add multiple users to Office 365?
   a. You should use the Azure Active Directory Sync (DirSync) Tool.
   b. You should use OAuth 2.0.
   c. You should send an Invite email to users.
   d. You should use a CSV file.

3. Which type of group is used to send emails to multiple users at once without giving security access to other objects?
   a. A distribution list.
   b. An email-enabled security group.
   c. A send list.
   d. An organizational unit.

4. In Microsoft Intune, you want the helpdesk personnel to manage service requests and to reset passwords. Which role should be assigned to the helpdesk personnel?
   a. Global Administrator
   b. Password Administrator
   c. User Management Administrator
   d. Billing Administrator

5. Which two object types can be added to Microsoft Intune groups? (Choose all that apply)
   a. users
   b. location-based objects
   c. organizational units
   d. devices

6. Which options are available to deploy the Microsoft Intune client? (Choose all that apply)
   a. Install the client software as part of an image
   b. Administrator deployment
   c. Email install
   d. User-Initiated Enrollment for computers

7. In Microsoft Intune, which administrator manages subscriptions and purchases?
   a. Global Administrator
   b. Password Administrator
   c. User Management Administrator
   d. Billing Administrator

8. Which policy allows you to make a PIN mandatory for smartphones managed by Microsoft Intune?
   a. Mobile Device Security Policy
   b. Windows Firewall Settings
   c. Microsoft Intune Agent Settings
   d. Microsoft Intune Center Settings

9. In Office 365, which identity model has accounts in Active Directory but user passwords are verified by the local domain controllers?
   a. Domain identity
   b. Synchronized identity

c. Cloud identity
d. Federated identity

10. Several users are unable to connect to Office 365, but you are able to log on to Office 365. Which of the following actions should be taken to resolve this issue?
a. You should run the Microsoft Office Dviagnostic Tool.
b. You should review the health history in the Office 365 dashboard
c. You should sign up for the Office 365 RSS feed.
d. You should review the Internet Explorer logs in the Event Viewer.

True / False

Circle T if the statement is true or F if the statement is false.

T F 1. In Office 365, the easiest identity model to set up is federated identity.

T F 2. When a user is removed from Office 365, the data is retained for 30 days before it is permanently deleted.

T F 3. You can install the Microsoft Intune client on Android devices, iOS devices, and Windows phones.

T F 4. The Microsoft Intune Tenant Administrator has full control of Microsoft Intune.

T F 5. To open a support request for Microsoft Intune, you should always use the Microsoft Intune Admin Console.

■ Case Projects

Scenario 3-1: Selecting an Identity Model for Office 365

You are an administrator for the Contoso Corporation and you want to integrate your Active Directory structure with Office 365 so that you can manage your user accounts with Active Directory Users and Computers. Describe the best solution.

Scenario 3-2: Implementing Groups in Microsoft Intune

You are an administrator for the Contoso Corporation and you need to establish groups so that you can best manage clients who are running Windows, iOS, and Android devices. Besides making sure that a device is up-to-date, you will need to deploy several applications from time to time. Describe how you should manage the groups for Microsoft Intune.

Scenario 3-3: Assigning Roles in Office 365

You an administrator for the Contoso Corporation, which has approximately 800 users. You have a helpdesk of five employees and a server management team of four employees. You also have a manager who is responsible for paying the bills. Which roles should you assign to these employees?

Scenario 3-4: Monitoring Service Health in Office 365

You are administrator for the Contoso Corporation and you just converted your users to Office 365. Because Office 365 is the primary application for your users and it handles your emails and SharePoint sites, you need to make sure that you know when there are problems with Office 365 as soon as possible so that you can take immediate steps to fix them. Describe the best solution.

4

LESSON

Using and Configuring Microsoft Cloud Services

OBJECTIVE DOMAIN MATRIX

Technology Skill	Objective Domain Description	Objective Domain Number
Configuring Exchange Online • Managing Recipients • Managing Mobile Devices with Exchange Online • Managing Anti-Spam and Antivirus Settings • Protecting Against Spam and Viruses	Configure Exchange Online	4.1
Configuring SharePoint Online • Creating SharePoint Team Sites • Setting Up Social Features • Applying Themes • Setting Storage and Resource Limits Configuring OneDrive • Accessing OneDrive from a Browser • Creating a File Within OneDrive • Uploading Files to OneDrive • Sharing a Document in OneDrive • Accessing OneDrive from the OneDrive Desktop App for Windows	Configure SharePoint Online, including OneDrive	4.2
Configuring Skype for Business Online	Configure Skype for Business Online	4.3
Configuring Microsoft Intune • Automating Installs • Sideloading and Deeplinking Software • Identifying Software and Hardware Requirements • Reviewing Hardware Assets • Managing Updates by Using Microsoft Intune	Configure Microsoft Intune	4.4

KEY TERMS

adware
Automatic Update Approval rules
backdoor
Bayesian filters
buffer overflow
connection filter
contact
content filter
deeplinking
distribution group
equipment mailbox
Exchange ActiveSync
fetching
Group Policy
mailbox
malicious software
malware
Microsoft Intune
Microsoft SharePoint
Microsoft Silverlight
newsfeed
Office 365 group
OneDrive
OneDrive desktop app for Windows
OneDrive for Business
recipient
remote wipe commands
resource mailbox
room mailbox
rootkit
security group
Sender Policy Framework (SPF)
shared mailbox
sideloading
site collection
Skype
Skype for Business
Skype for Business Online
spam
spyware
System Center Configuration Manager
themes
Trojan horse
virus
worm
Yammer

As an administrator for the Contoso Corporation, you are ready to transfer users to Microsoft Exchange Online, Microsoft SharePoint Online, Skype for Business Online, and Microsoft Intune. Therefore, you need to determine the best way to configure these components so that users can perform their job, while keeping the data and corporation secure.

■ Configuring Exchange Online

THE BOTTOM LINE

For most organizations, email is the most popular form of communications when conducting business. The advantage of using Exchange Online and Outlook Online is that there is very little configuration necessary. You do not have to install and configure one or more servers.

CERTIFICATION READY
Configure Exchange Online
4.1

Using Outlook Online is very similar to using Outlook Web App (OWA) or running a local copy of Outlook. Of course, Outlook Online is already configured to send emails from your account after logging on.

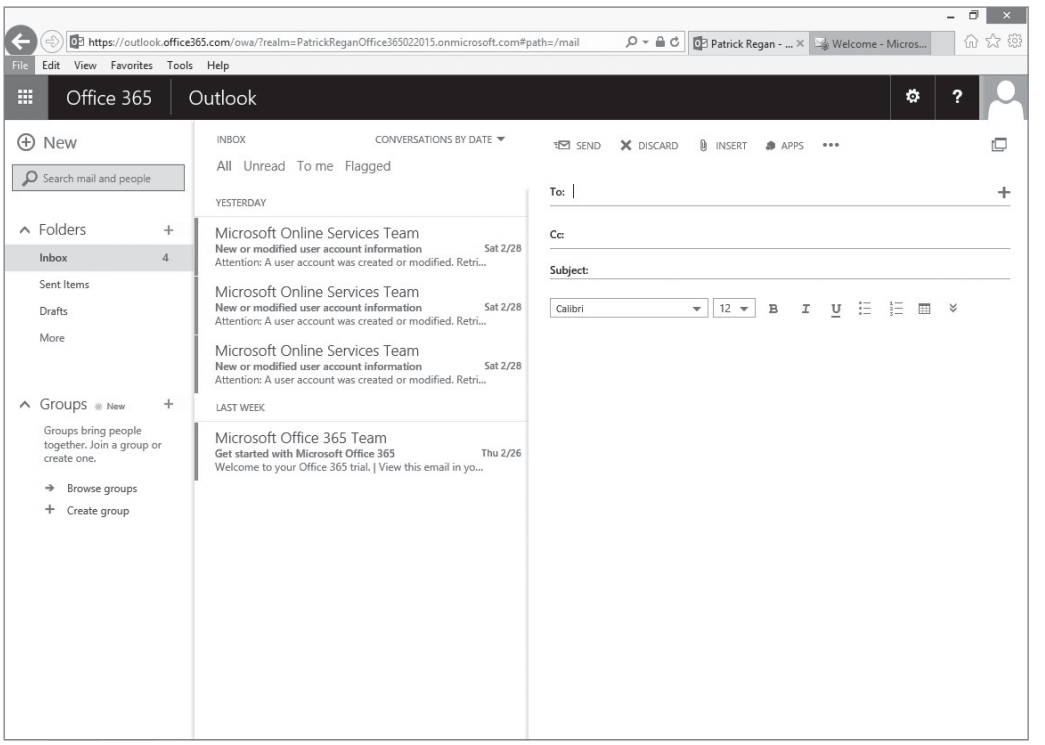
CREATE AN EMAIL IN OUTLOOK ONLINE

GET READY. To create an email in Outlook Online, perform the following steps.

1. Log on to Office 365 (https://portal.office.com).
2. If it is the first time you have accessed the Outlook Web App, you will be prompted to select your language and time zone. Click **save**.
3. At the top of the web page, click **People**.
4. To generate a new email, at the top-left corner of the window, click **New**. A new email opens in the right pane (see Figure 4-1).

Figure 4-1

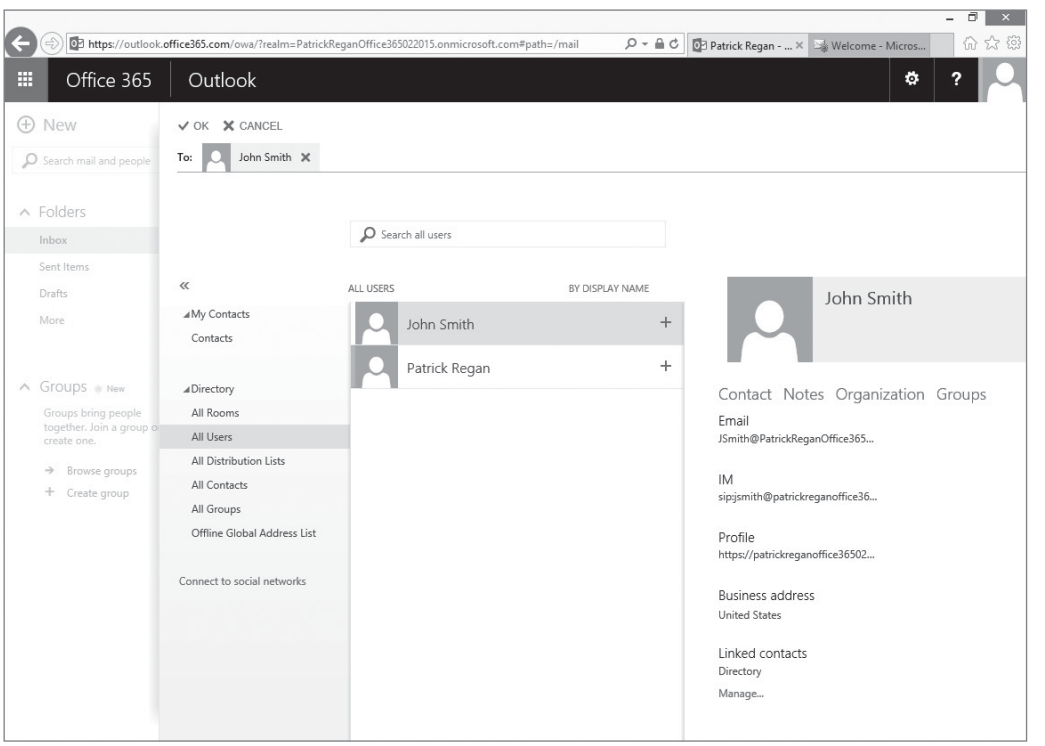
Composing a new email



5. In the To line, type an email address that you want to send the email to. Alternatively, you can click the **+** sign to open your contact list. After doing so, you can click **>>** to access the organization's address lists, such as All Users (see Figure 4-2), All Contacts, or All Groups. Then double-click the user or group.

Figure 4-2

Accessing the organization's address lists



6. In the Subject line, type a subject (such as Test Email). In the body of the email, type a message (such as Hello). When you are ready to send the email, click **SEND**.

Managing Recipients

A ***recipient*** is the identity used in Exchange Online that is used to identify users and resources that can send and receive messages. It is a mail-enabled object in Active Directory to which Exchange can deliver or route messages.

Exchange Online has the following recipients:

- Mailboxes
- Shared mailboxes
- Resources
- Contacts
- Groups

MANAGING MAILBOXES

A ***mailbox*** is a mail-enabled Active Directory user that represents a user that has an email address that can receive emails internally and externally. When you add a user to Office 365 using the Office 365 Admin Center, you can assign an email address to the user.

ADD A MAILBOX IN OFFICE 365

GET READY. To add a mailbox in Office 365, perform the following steps.

1. Sign in to Office 365 (https://portal.office.com) and then click the **Admin** icon.
2. On the left pane, click **Users > Active Users**, as shown in Figure 4-3.

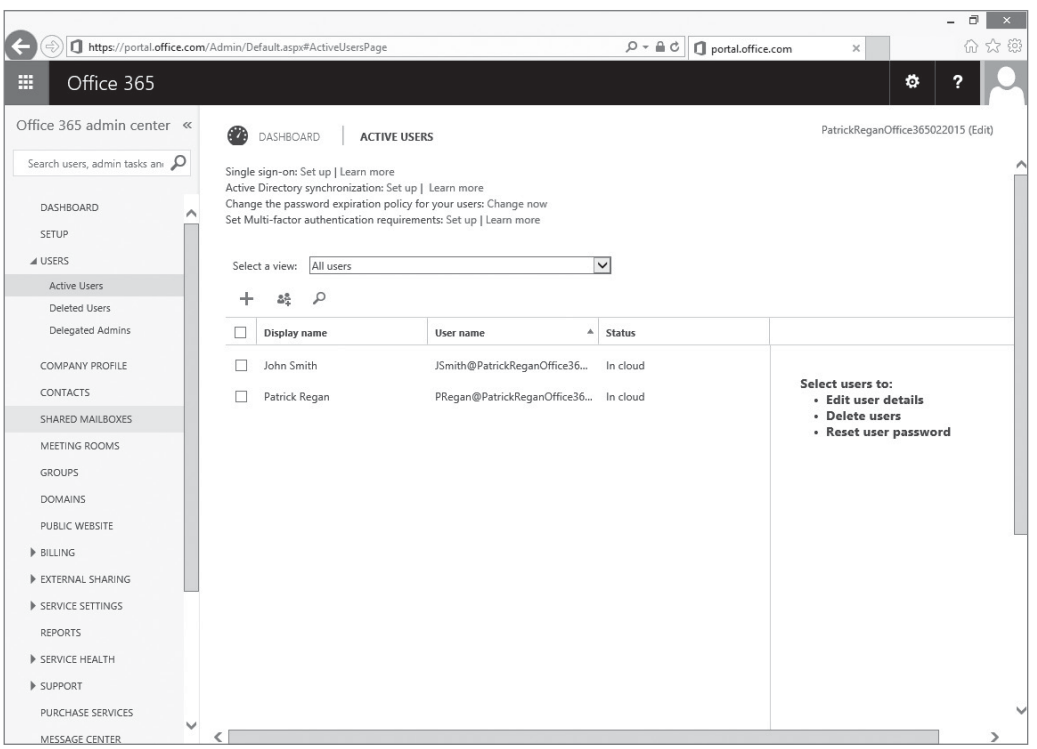
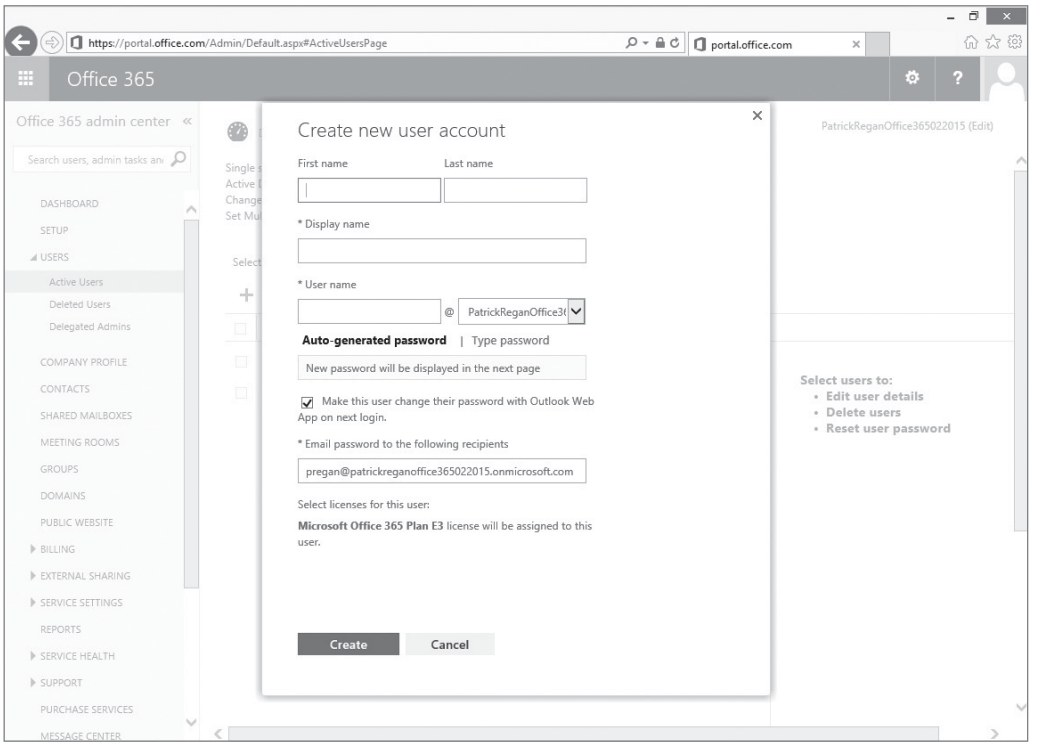


Figure 4-3
Viewing active users

3. Choose the + button. The Create new user account dialog box opens, as shown in Figure 4-4.

Figure 4-4

Creating a new user



4. Type a First name, Last name, Display name, and User name in the appropriate boxes.
5. If you have more than one domain, be sure to select the right domain for the user in the drop-down box.
6. Click **Type password**.
7. In the Enter password text box and the Re-enter password text box, type a password (such as **Pa$$w0rd**).
8. In the Email password to the following recipients text box, type the email addresses of the people who you want to receive a copy of this user's account information. Don't send the email to their new Office 365 email address because they won't be able to get it.
9. Click **Create**.
10. When the account is created, click **Close**.

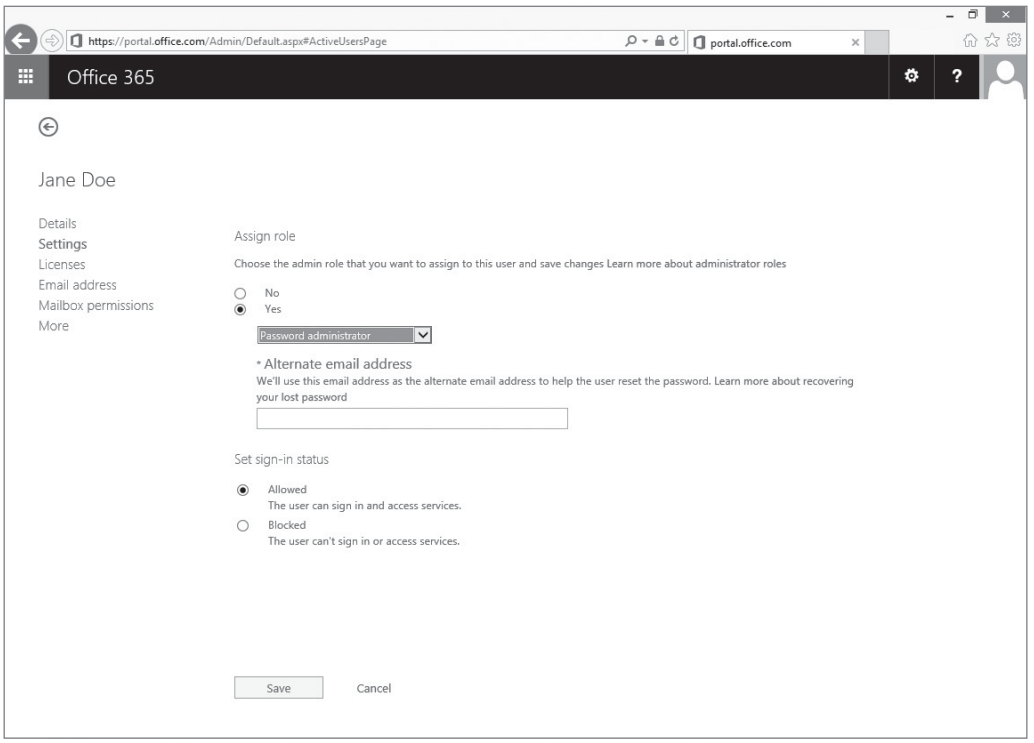
The password is temporary. Therefore, users will need to change the password within 90 days. When the user signs into https://portal.office.com for the first time, he will be prompted to change his password. To reset a password, select the check box for the user and then click RESET PASSWORD.

To manage the details, settings, and licenses, select the check box for the user and then click EDIT. On the Details page, you will modify the First name, Last name, Display name, User name and the Domain. You can also click Additional details to configure the Job title, Department, Phone numbers, and Address.

On the Settings page, you can assign an Office 365 administrator role, such as Global Administrator or Password Administrator. You can also disable the account by selecting the Blocked option, as shown in Figure 4-5.

Figure 4-5

Modifying settings

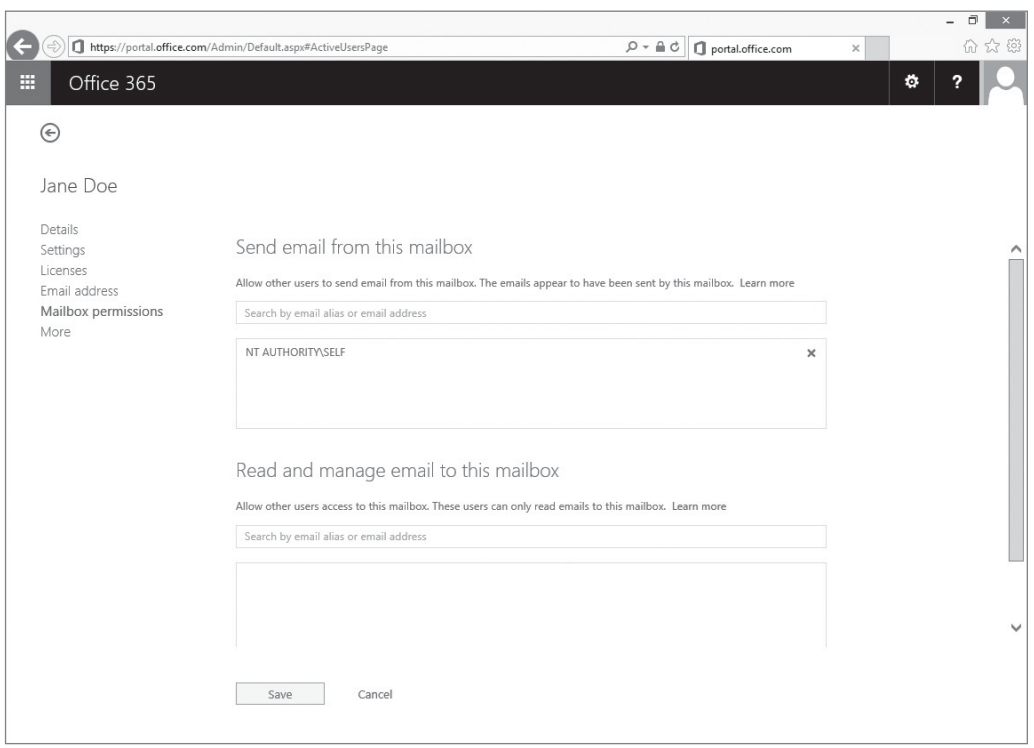


The Licenses page allows you to set the user location and assign licenses, such as Azure Rights Management, Office 365 ProPlus, Skype for Business Online, Office Online, SharePoint Online, or Exchange Online. The Email address page allows you to assign multiple addresses to a user. However, a user must have a primary address that is used to send emails from.

To allow another user access to a mailbox, access the Mailbox permissions page, as shown in Figure 4-6. The Send email from this mailbox section provides an assistant with the ability to

Figure 4-6

Assigning mailbox permissions

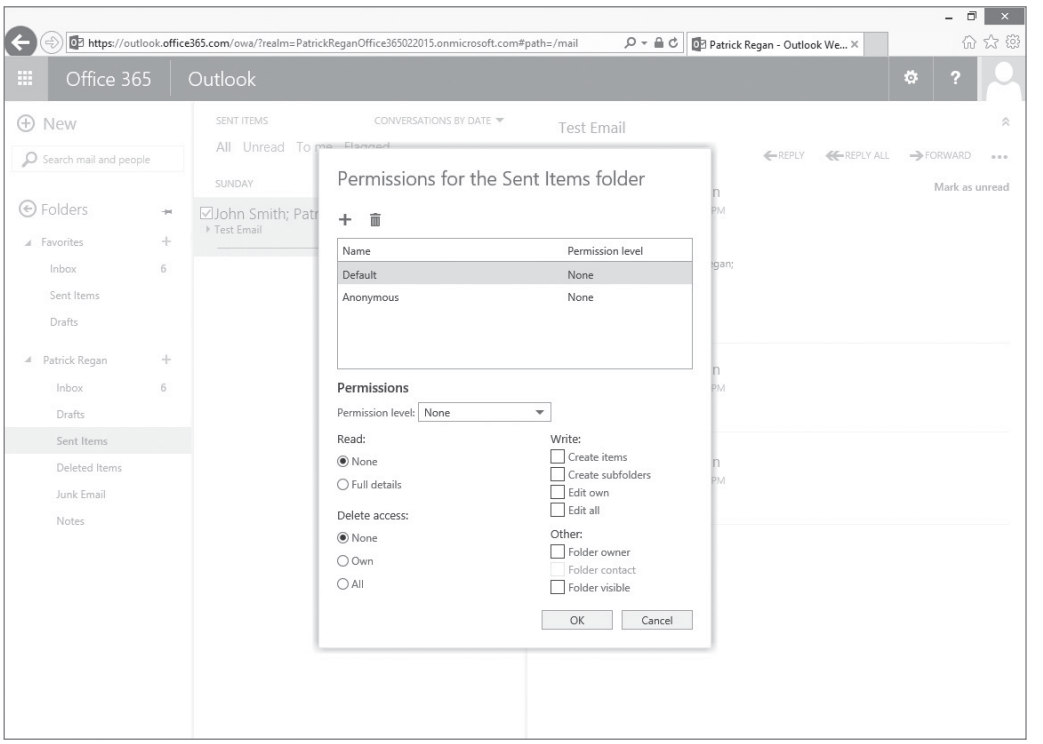


send email from this mailbox. The Read and manage email to this mailbox section allows an assistant with full access to the user's mail and calendar.

A user can also delegate their mailbox permissions to another user. For example, a user can open Outlook Online and right-click a folder (such as the Sent Items folder) and choose Permissions. In the Permissions window (as shown in Figure 4-7), you can click the + button to add a user and then assign permissions for the folder only without providing full access to the entire mailbox.

Figure 4-7

Configuring permissions for an Outlook folder



MANAGING SHARED MAILBOXES

A ***shared mailbox*** is a mailbox that is associated with one or more users and is assigned an external email address that can receive emails internally and externally. When a person in the group replies to a message sent to the shared mailbox, the email appears to be from the shared mailbox, not from the individual user. It allows a mailbox to be monitored by several people.

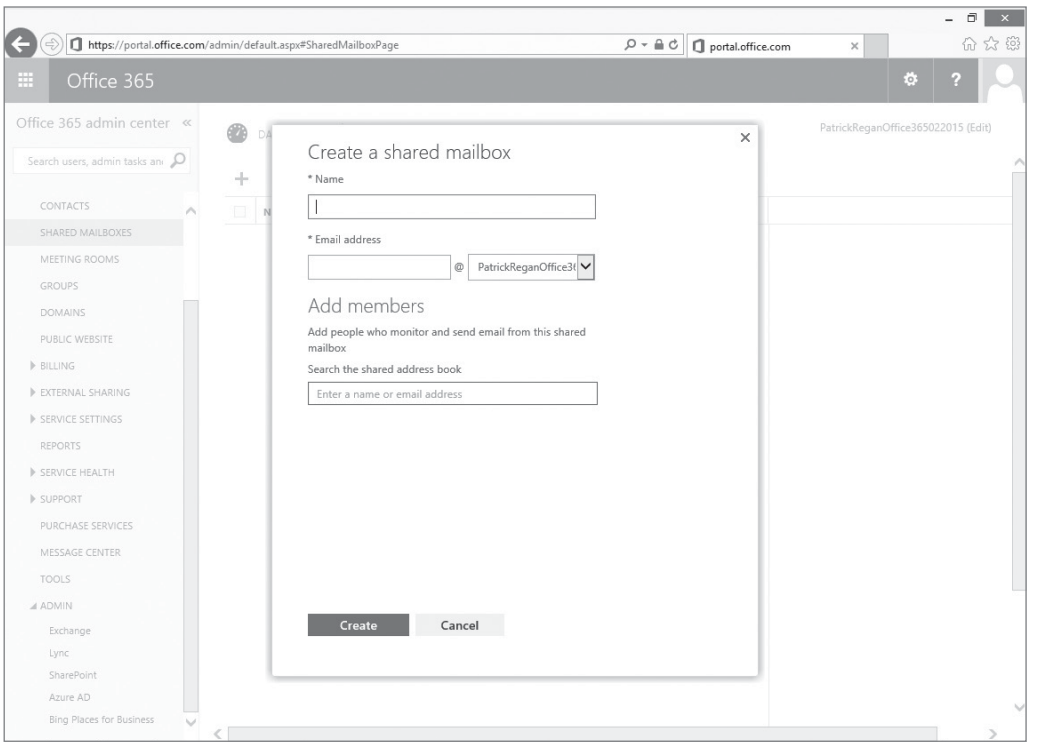
A shared mailbox doesn't have its own user name and password and you cannot log into a shared mailbox directly using Outlook or Outlook Web App. Instead, you must be granted permissions to the shared mailbox and then access it using Outlook or Outlook Web App. You don't need to assign licenses to shared mailboxes unless they have exceeded their storage quota of 10 gigabytes (GB).

ADDING A SHARED MAILBOX IN OFFICE 365

GET READY. To add a shared mailbox in Office 365, perform the following steps.

1. Sign in to Office 365 (https://portal.office.com) and then click the **Admin** icon.
2. Click **SHARED MAILBOXES**.
3. Click the **+** button.
4. In the Create a shared mailbox dialog box (as shown in Figure 4-8), in the Name text box, type a name of the shared mailbox.

Figure 4-8
Creating a shared mailbox



5. In the Email address box, type the email address that you want to assign to the mailbox.
6. To give access to the shared mailbox, type a name or email address in the Search the shared address book text box.
7. Click **Create**.

To edit the members assigned to the shared mailbox, select the check box next to the shared mailbox and then click EDIT MEMBERS. To delete the mailbox, select the check box next to the shared mailbox and then click DELETE. To change the name of the mailbox, click Edit. For advanced features such as delegating access to the mailbox, modifying contact information, adding email addresses, or adding the mailbox to a group, click Edit more properties.

MANAGING RESOURCES

A ***resource mailbox*** is a mailbox that represents a shareable resource, such as a conference room, a training room, a projector, a company car, or a mobile computer. It is primarily used to schedule the resource among users within the organization. A resource mailbox can be organized according to an equipment mailbox or a room mailbox.

An ***equipment mailbox*** is a resource mailbox assigned to a resource that is not location-specific. When a user needs a projector for a meeting, he can include the projector (equipment mailbox) in a meeting request just as you would any other user. If other users try to reserve the projector for the same time, they will see that the projector is not available. Just like a user cannot be in two meetings at once, the project cannot be in two meetings at once.

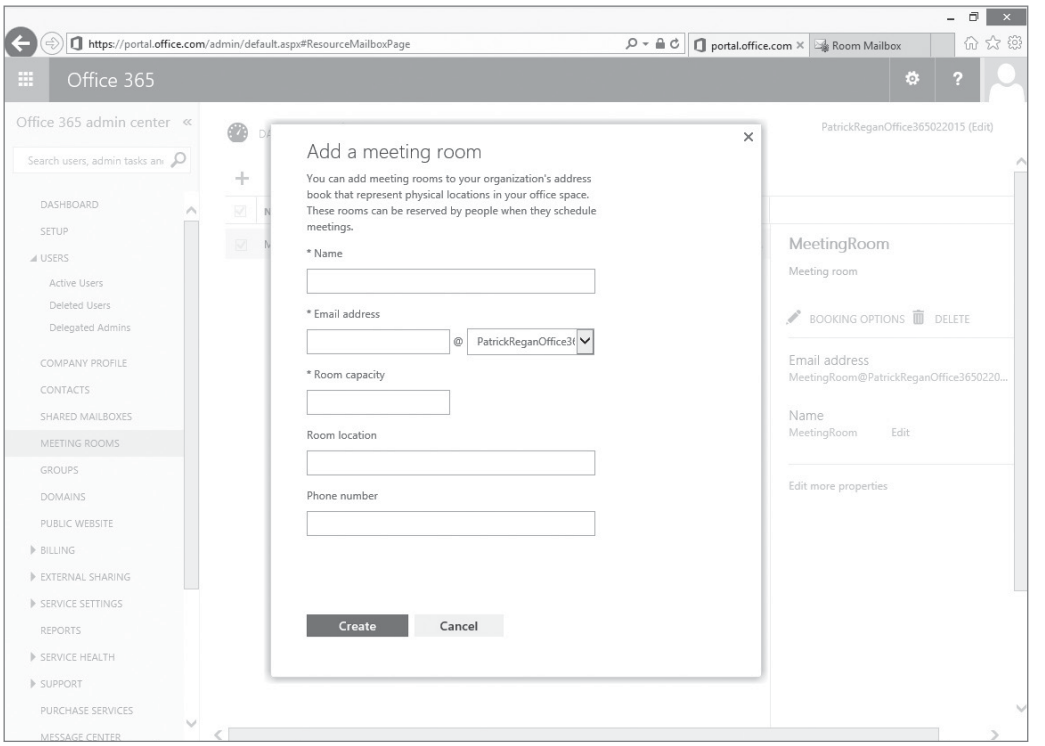
ADD A ROOM MAILBOX IN OFFICE 365

GET READY. To add a room mailbox in Office 365, perform the following steps.

1. Sign in to Office 365 (https://portal.office.com) and then click the **Admin** icon.
2. Click **MEETING ROOMS**.

3. Click the **+** button to create a new meeting room.
4. In the Add a meeting room dialog box (see Figure 4-9), in the Name text box, specify the name of the room.

Figure 4-9
Creating a shared mailbox



5. In the Email address text box, type an email address.
6. In the Room capacity text box, specify the number of people that the room can handle.
7. In the Room Location text box and the Phone number text box, type a room location and a phone number. Click **Create**.
8. To specify the booking options, click **BOOKING OPTIONS**.
9. By default, on the booking delegates page, the booking delegates is configured to accept or decline booking requests automatically. If you want someone to approve the question, click **Select delegates who can accept or decline booking requests** and then click the **+** button to add delegates.
10. On the booking options page, you can configure repeating meetings, the maximum booking lead time, and the maximum duration hours.
11. Click **save**.

MANAGING CONTACTS

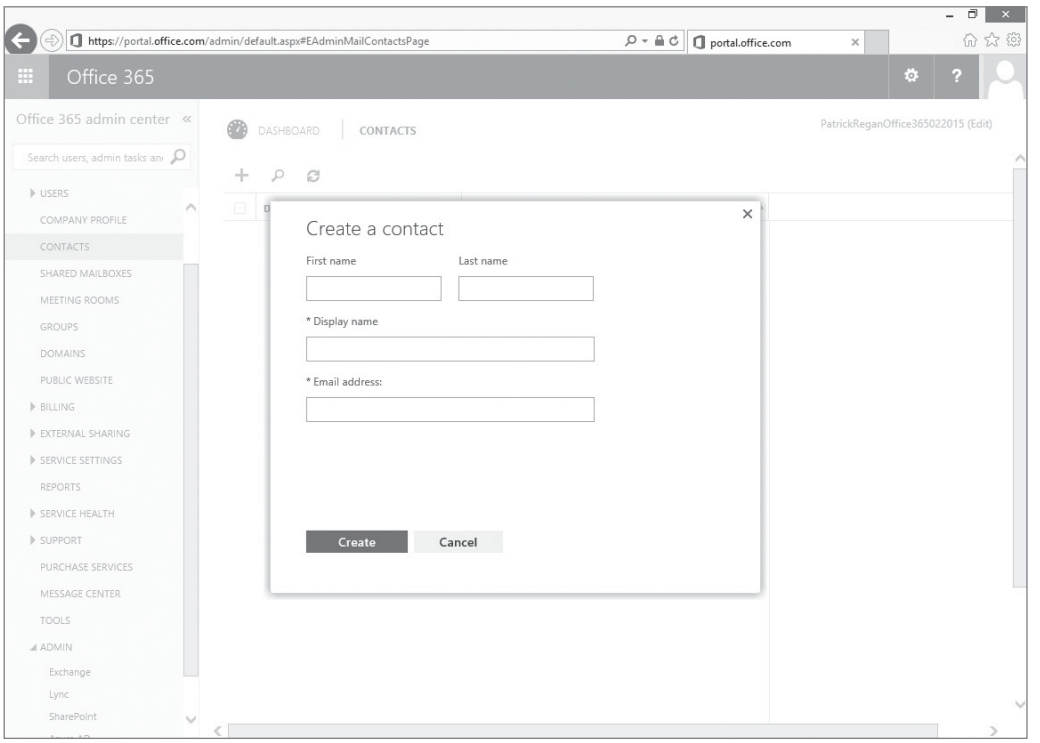
A ***contact*** is a mail-enabled Active Directory object that contains contact information about a person or organization that exists outside of the Exchange organization. Each mail contact has an external email address. Because a contact is available in Active Directory and the Exchange organization, users can easily find the contact. When they send email to the contact, the email will be rerouted to the external address.

ADD A CONTACT IN OFFICE 365

GET READY. To add a contact in Office 365, perform the following steps.

1. Sign in to Office 365 (https://portal.office.com) and then click the **Admin** icon.
2. Click **CONTACTS**.
3. To create a new contact, click the **+** button.
4. In the Create a contact dialog box (see Figure 4-10), in the First name text box and the Last name text box, type the contact's first and last name.

Figure 4-10
Adding a contact



5. In the Email address text box, type the contact's external email address.
6. Click the **Create** button.

MANAGING GROUPS

A ***distribution group*** is an Active Directory object that includes a list of users who can receive emails sent to an email address that is automatically distributed to those users. There are two types of groups that can be used to distribute messages:

- Mail-enabled universal distribution groups (also called distribution groups) can be used only to distribute messages.
- Mail-enabled universal security groups (also called ***security groups***) can be used to distribute messages as well as to grant access permissions to resources in Active Directory.

ADD A SECURITY GROUP IN OFFICE 365

GET READY. To add a security group in Office 365, perform the following steps.

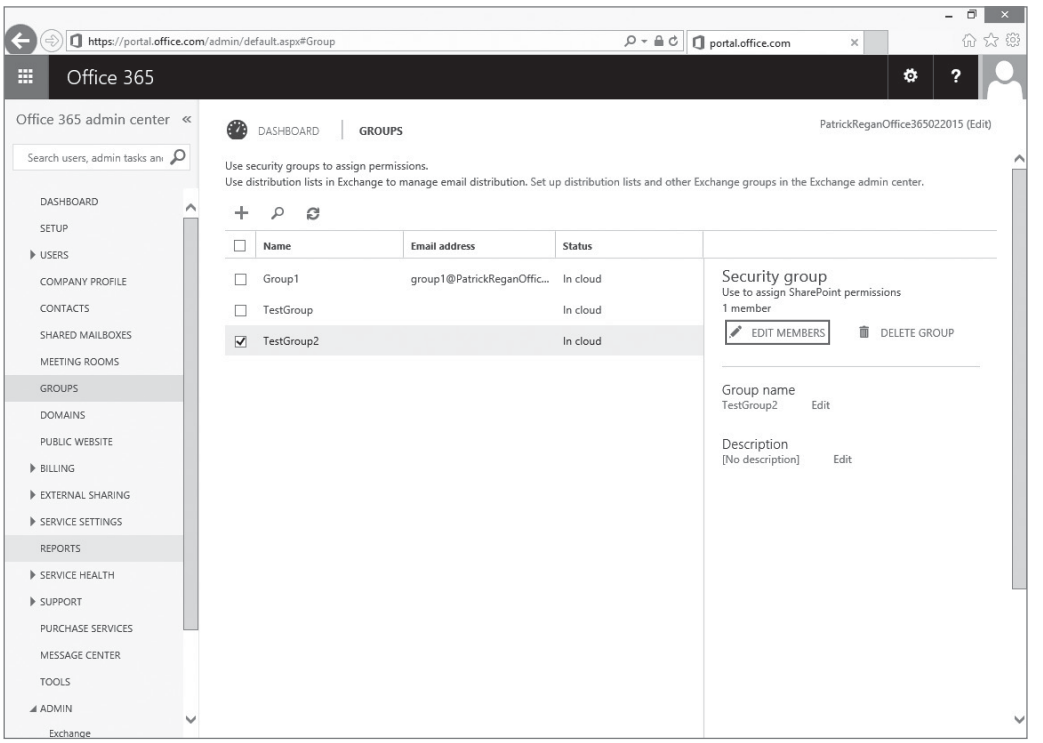
1. Sign in to Office 365 (https://portal.office.com) and then click the **Admin** icon.
2. Click **GROUPS**.

3. Click the **+** button.
4. In the Create security group dialog box, in the Group name, type a group name and then click **Create**.
5. When the group is successfully created, click **Edit members**.
6. Click **ADD MEMBER**.
7. In the Add members to the group dialog box, in the search box, type a name or partial name. Then right-click the search box and choose the desired name. Repeat the process until the users are added.
8. Click **Add** to add the members.
9. When the users are created, click **Close**.

To modify group members, select the check box for the desired group and then click EDIT MEMBERS, as shown in Figure 4-11. To delete the group, select the check box for the desired group and then click DELETE GROUP.

Figure 4-11

Modifying group members



ADD A DISTRIBUTION GROUP IN OFFICE 365

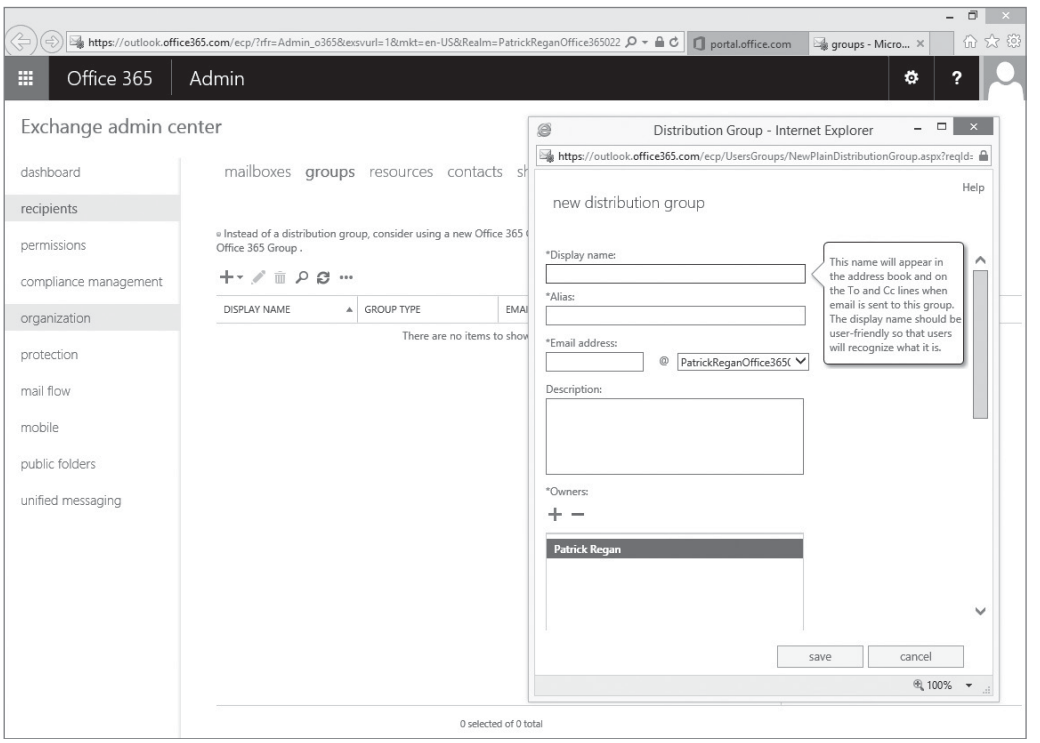
GET READY. To add a distribution group in Office 365, perform the following steps.

1. Sign in to Office 365 (https://portal.office.com) and then click the **Admin** icon.
2. Click **GROUPS**.
3. In the left pane, expand **ADMIN** and then click **Exchange**.
4. On the Exchange Admin Center page, under recipients, click **groups**.
5. To create a group, click the **+** button. You can then select Distribution group, Security group, or Dynamic distribution group. In this particular case, select **Distribution group**.

6. In the Distribution Group dialog box (as shown in Figure 4-12), in the Display name text box, type a name for the group. The display name is the name that will appear in the address book and on the To and Cc lines when email is sent to the group.

Figure 4-12

Creating a distribution group



7. In the Alias text box, type a name that will be used as part of the email address.
8. If you have more than one domain, select the appropriate domain.
9. To add an owner to the group, in the Owners group section, click the **+** button. In the Select Owner dialog box, select the user you want to add, and then click the **Add** button. Click **ok**.
10. To add a member to the group, in the Members group section, click the **+** button. In the Select Members dialog box, select the user you want to add, and then click the **Add** button. Click **ok**.
11. At the bottom of the window, select **Open**, **Closed**, or **Owner approval**.
12. Click **save**.

If you have an Office 365 business, enterprise, or government plan, an ***Office 365 group*** is a shared workspace for email, conversations, files, and calendar events where group members can collaborate. One advantage of a group is that new members can go back and look at previous emails, conversations, and files so that they can be brought up to speed on group activities.

An Office 365 group can be public or private. Anyone can join a public group and view the content and conversations. A private group is more secure because it is available only to its members. Joining a private group requires approval from a Group Administrator. Although you might not be able to participate in a private group that you are not a member of, you can send email to a private group and receive replies from that private group.

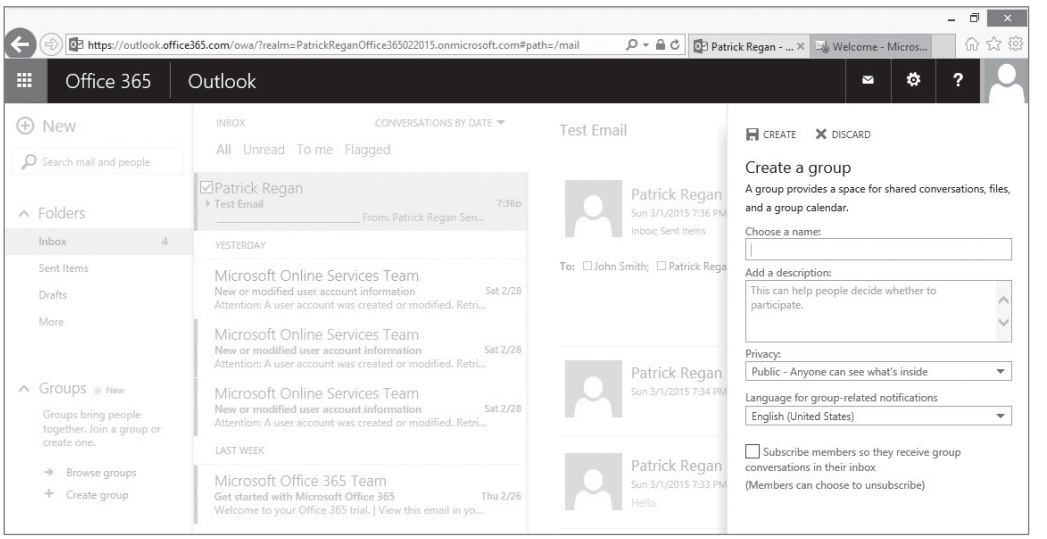
CREATE AN OFFICE 365 GROUP IN OUTLOOK ONLINE

GET READY. To create an Office 365 group in Outlook Online, perform the following steps.

1. Sign in to Office 365 (https://portal.office.com) and then click the **Outlook** icon.
2. To create an Outlook Online group, click the **Create group** option in the left pane.
3. On the Create a group page (as shown in Figure 4-13), in the Choose a name text box, type **Group1**.

Figure 4-13

Creating an Outlook Online group



4. Set the Privacy to one of the following:
   - **Public:** Anyone can see what's inside
   - **Private:** Only approved members can see what's inside
5. Specify a **Language for group-related notifications**.
6. If necessary, select the **Subscribe members so they receive group conversations in their inbox**. Members can choose to unsubscribe.
7. Click **Create**.
8. On the Add members page, type a name of a user that you want to add and then press **Enter**.
9. When done, click **Add**.

To manage these groups, open the Office 365 Admin Portal, click Group, and then select the check box for the desired group. To edit members or edit admins, click the EDIT MEMBERS AND ADMINS link. You can also double-click the group to open the Members and Admins view.

Managing Mobile Devices with Exchange Online

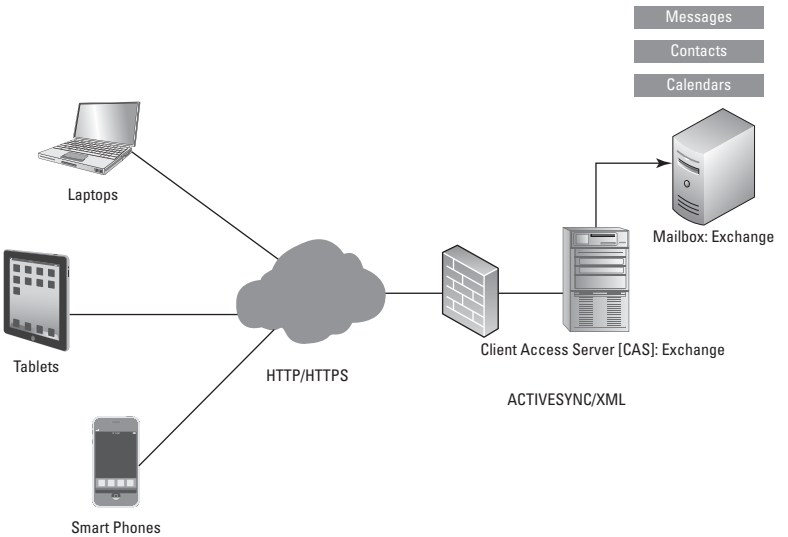
Exchange ActiveSync enables you to create mobile device policies that can increase security for your corporate network.

Exchange ActiveSync is a client synchronization protocol based on XML that enables you to connect your mobile device to your Exchange mailbox.

ActiveSync enables communications from ActiveSync-compliant mobile devices, such as a Windows Phone, an Apple iPhone, an iPad, an iPod, or a Google Android phone. The features available with ActiveSync vary on each device because the manufacturers determine which features they want to support with the protocol. ActiveSync works over HTTP and HTTPS (see Figure 4-14) and supports offline access to messages, contacts, and calendar information.

Figure 4-14

Using ActiveSync over HTTP/HTTPS



ActiveSync provides you with tools to control policies and to manage and secure your mobile devices. Here are just a few of the tasks you can perform with ActiveSync:

- You can issue ***remote wipe commands***—which clear all corporate and user information stored on the device—in case the mobile device is lost or stolen. You can also remotely lock the device.
- You can specify the length and complexity of the password for the mobile device (requiring a password that is 4 to 18 alphanumeric characters), and you can configure the number of password attempts.
- You can specify the lock behavior, such as automatically locking a phone after a specified time of non-use.
- You can require encryption on the mobile device and/or the device's removable storage card.
- You can control which types of mobile devices/users are allowed to connect to your Exchange Server.
- You can run, view, and export reports.

Some of the built-in security features in mobile devices can be controlled from Exchange Server, so you can create security policies that are automatically sent to each device the next time the mobile device starts synchronizing. These settings can harden security on the devices by requiring stronger passwords, enabling encryption, and controlling which older devices are allowed to connect to your network.

You create ActiveSync mailbox policies to simplify management of mobile devices. These policies, which can be applied to each of your Exchange ActiveSync users, enable you to apply settings to a user's mobile device.

A new mobile device mailbox policy includes the following settings:

- **Name**: Displays the name of the mobile policy.

- **This is the default policy:** Sets the policy as the default.
- **Allow mobile devices that do not fully support these policies to synchronize:** Enables you to decide whether to allow mobile devices that do not support some or all of the selected policies.

Policies for Exchange ActiveSync:

- **Require a password:** This option enables you to configure additional password requirements, as follows:
  - **Allow simple passwords:** Enables mobile devices to use simple passwords (for example, 1234).
  - **Require an alphanumeric password:** Requires lower- and uppercase letters, numbers, and symbols.
  - **Password must include this many character sets:** Options include 1,2,3,4. Selecting 2 means you need to use at least 2 of the character sets (for example, letters and numbers).
- **Require encryption on device:** Enables encryption on the mobile device.
- **Minimum password length:** Sets minimum length for password; specify the number in the space provided.
- **Number of sign-in failures before device is wiped:** When a user fails to sign in after the specified number of attempts, the device is wiped.
- **Require sign-in after the device has been inactive for (minutes):** Locks devices after they are idle for the number of minutes you specify, requiring users to sign in again.
- **Enforce password lifetime (days):** Specifies the number of days before the password must be changed. If you enable this feature, users are prompted to reset their password after the number of days you specify.
- **Password recycle count:** Enables you to determine the number of different passwords a user must use before they can reuse a password. You can specify a number from 0 through 50.

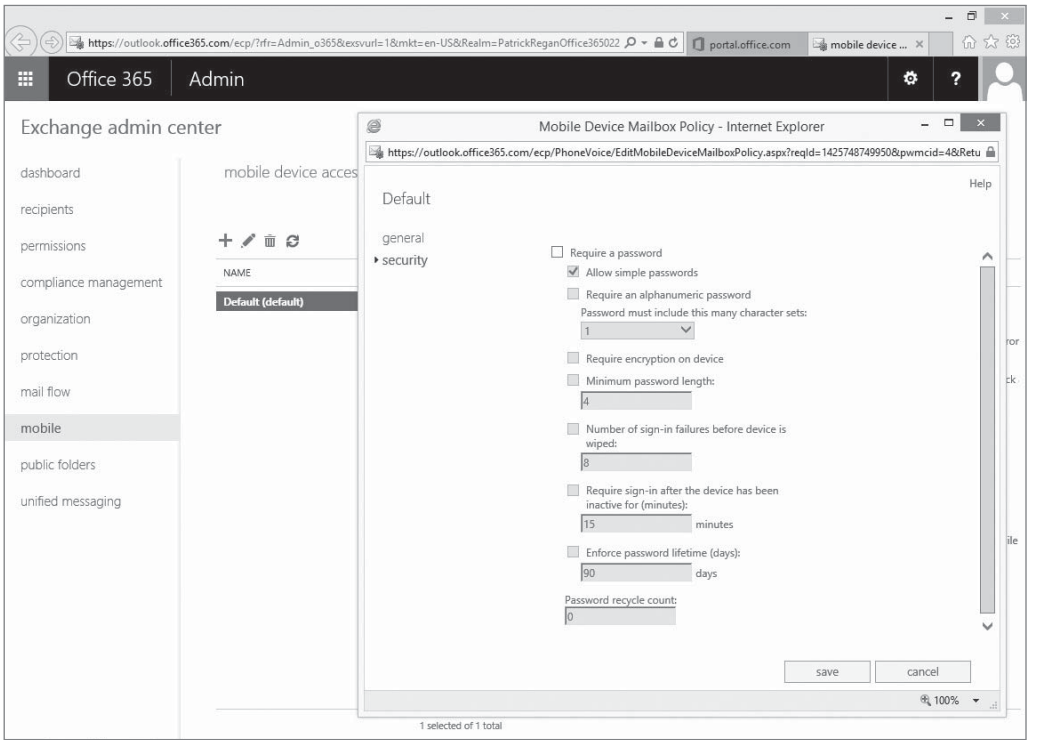
MODIFY A MOBILE DEVICE MAILBOX POLICY

GET READY. To modify a mobile device mailbox policy, perform the following steps.

1. Sign in to Office 365 (https://portal.office.com) and then click the **Admin** icon.
2. Click **GROUPS**.
3. In the left pane, expand **ADMIN** and then click **Exchange**.
4. On the Exchange Admin Center page, click **Mobile** and then click **mobile device mailbox policies**.
5. Double-click the Default (default) mobile device mailbox policy.
6. In the Mobile Device Mailbox Policy dialog box, click Security (see Figure 4-15).
7. Select **Require a password**.
8. Select **Require an alphanumeric password**.
9. Under the Password must include this many character sets section, click the drop-down box and then select **3**. Character sets include upper case, lower case, numbers and symbols.
10. Select **Minimum password length** and, in the field that appears, type **6.**
11. Select **Enforce password lifetime (days)** and, in the field that appears, type **60.**
12. Under Password recycle count, type **5**.
13. Click **save**.

Figure 4-15

Configuring a mobile device policy



SET UP EXCHANGE ACTIVESYNC ON A WINDOWS PHONE

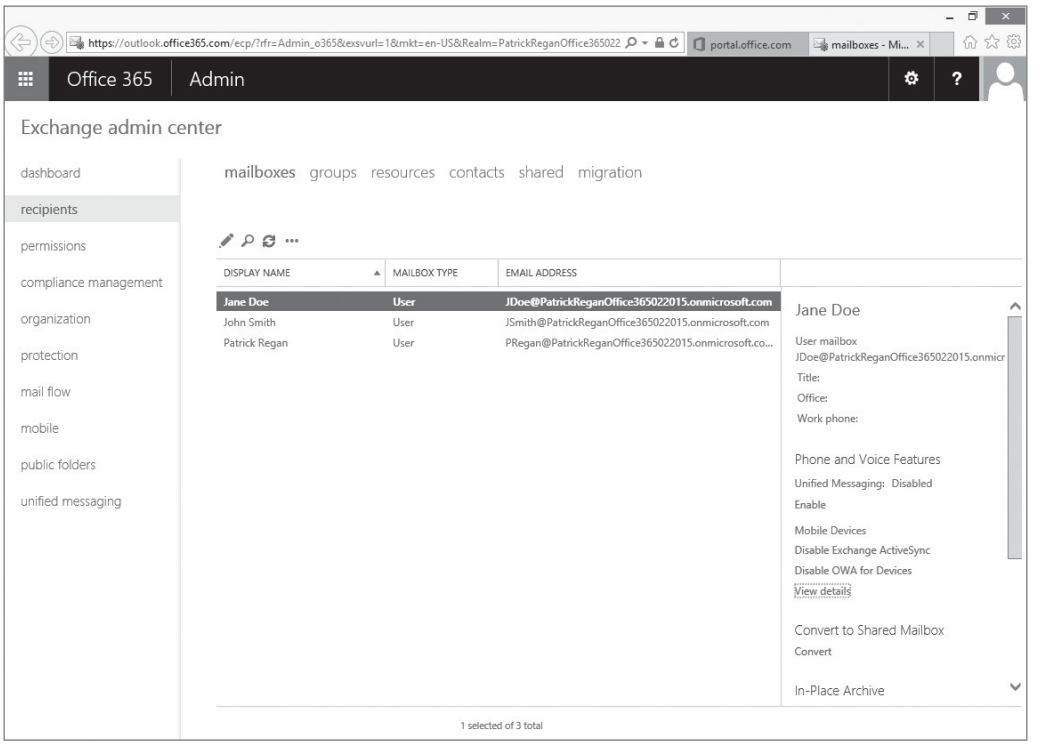
GET READY. To set up Exchange ActiveSync on a Windows Phone, perform the following steps.

1. On Start, swipe left to the App list, select **Settings**, and then select **email + accounts**.
2. Select **add an account > Outlook**.
3. Type your email address and password and then select **Sign in**. Windows Phone will try to set up your email account automatically. If setup completes successfully, proceed to Step 8.
4. If you see the message Check your information and try again, you might have mistyped your password. Verify that you typed the correct email address and password. At this stage, you don't need to specify any values for User name and Domain. Select **Sign in**. If setup completes successfully, proceed to Step 8.
5. If your email account can't be set up automatically, you'll see the message We couldn't find your settings. Select **Advanced**. You'll need to type the following information:
   - **Email address**: This is your full email address (for example John.Smith@contoso.com).
   - **Password**: This is the password for your email account.
   - **User name**: This is your full email address (for example, John.Smith@contoso.com).
   - **Domain**: This is the part of your email address after the @ sign (for example, contoso.com).
   - **Server**: This is the name of your Exchange server. If you're connecting to your Office 365 email, use outlook.office365.com for your server name.
6. Select the **Server requires encrypted (SSL) connection** box.
7. Select **Sign in**.
8. If ActiveSync asks you to enforce policies or set a password, select **OK**.

Having a strong mobile policy in place goes a long way toward protecting your user's mobile device, but when one of your users loses a phone or it is stolen, you need to rely on something more than just your mobile policy. In those situations, the best approach is to remotely wipe the device. To disable Exchange Active Sync or to disable OWA for devices, open the Exchange Admin Center, click recipients > mailboxes, and select a user (see Figure 4-16). Then on the right side of the page, under Phone and Voice Features, click the appropriate option. To wipe a phone, click View details, select the mobile device that you want to wipe, and then click the wipe data icon (fourth icon).

Figure 4-16

Managing mailboxes in the Exchange Admin Center



Managing Anti-Spam and Antivirus Settings

If you have been working with supporting computers even for only a short while, you should know that viruses and spam are a threat to any computer or corporation. In fact, the number of viruses and spam has been growing significantly each year.

Malicious software, sometimes called ***malware***, is software that is designed to infiltrate or affect a computer system without the owner's informed consent. The term "malware" is usually associated with viruses, worms, Trojan horses, spyware, rootkits, and dishonest adware. As a network administrator or computer technician, you need to know how to identify malware, how to remove it, and how to protect a computer from it.

Because it is now quite common for computers to be connected to the Internet, there are more opportunities than ever for your organization's computers to be infected by malware. Indeed, over the past few years, a staggering amount of malware has been produced. As a security professional, you are responsible for protecting your organization's computers against infection. Furthermore, if a computer on your network does somehow happen to get infected by malware, you must make sure this infection does not spread to other computers.

Many early forms of malware were written as experiments or pranks. Most of the time, they were intended to be harmless or merely annoying. However, as time passed, malware increasingly became a tool for vandalism or compromising private information. Today, malware can even be used to launch denial of service (DoS) attacks against other systems, networks, or websites, causing those systems to have performance problems or become inaccessible.

As mentioned before, malware can be divided into several categories, including the following:

- Viruses
- Worms
- Trojan horses
- Spyware and dishonest adware
- Rootkits
- Backdoors

A computer ***virus*** is a program that can copy itself and infect a computer without the user's consent or knowledge. Early viruses were usually some form of executable code that was hidden in the boot sector of a disk or as an executable file (for example, a filename with an .exe or .com extension). Later, as macro languages began to be used in software applications (such as word processors and spreadsheet programs), virus creators seized upon this technology, embedding malicious macros in documents of various types. Unfortunately, because macro code is automatically executed when a document is opened, these documents can infect other files and cause a wide range of problems on affected computer systems. Today, websites also pose a virus threat, as they can be written in various programming and scripting languages and may include executable programs. Therefore, whenever you access the Internet, your system is under constant threat of infection.

A ***worm*** is a self-replicating program that copies itself to other computers on a network without any user intervention. Unlike a virus, a worm does not corrupt or modify files on the target computer. Instead, it consumes bandwidth and processor and memory resources, slowing the system down or causing it to be unusable. Worms usually spread via security holes in operating systems or TCP/IP software implementations.

A ***Trojan horse*** is an executable program that appears as a desirable or useful program. Because it appears to be desirable or useful, users are tricked into loading and executing the program on their systems. After the program is loaded, it might cause a user's computer to become unusable, or it might bypass the user's system security, allowing his personal information (including passwords, credit card numbers, and a Social Security number) to be accessible by an outside party. In some cases, a Trojan horse may even execute adware.

Spyware is a type of malware that is installed on a computer to collect a user's personal information or details about her browsing habits, often without the user's knowledge. Spyware can also install additional software, redirect your web browser to other sites, or change your home page. One example of spyware is a keylogger, which records every key a user presses. When a keylogger is installed on your system, whenever you type in credit card numbers, Social Security numbers, or passwords, the information is recorded and eventually sent to or read by someone without your knowledge. (It should be noted that not all keyloggers are bad, however, as some corporations use them to monitor their corporate users.)

Adware is any software package that automatically plays, displays, or downloads advertisements to a computer after the software is installed or while the application is being used. Although adware might not necessarily be bad, it is often used with ill intent.

A ***rootkit*** is a software or hardware device designed to gain administrator-level control over a computer system without being detected. Rootkits can target the BIOS, hypervisor, boot loader, kernel, or less commonly, libraries or applications.

A ***backdoor*** is a program that provides someone with remote, unauthorized control of a system or initiates an unauthorized task. Some backdoors are installed by viruses or other forms of malware. Other backdoors might be created by programs on commercial applications or with a customized application made for an organization.

Viruses and worms often exploit what is known as a ***buffer overflow***. In all application programs including Windows itself, there are buffers that hold data. These buffers have a fixed size. If too much data is sent to these buffers, a buffer overflow occurs. Depending on the data sent to the overflow, a hacker might be able to use the overflow to send passwords to himself, alter system files, install backdoors, or cause errors on a computer. When patches are released to fix a potential buffer overflow, the patch adds code to check the length of data sent to the buffer to make sure that it does not overflow.

Sometimes it is easy to see that you are infected with malware. Other times, you may never know that you have it. Some common symptoms of malware include the following:

- Poor system performance
- Unusually low levels of available memory
- Poor performance while connected to the Internet
- Decreased response rates
- Longer start-up times
- Instances in which your browser closes unexpectedly or stops responding
- Changes in your browser's default home or default search pages
- Unexpected pop-up advertising windows
- Addition of unexpected toolbars to your browser
- Instances in which unexpected programs automatically start
- Inability to start a program
- Malfunctions in Windows components or other programs
- Missing programs or files
- Unusual messages or displays on your monitor
- Unusual sounds or music played at random times
- Creation and/or installation of unknown programs or files
- Appearance of unknown browser add-ins
- Corrupted files
- Unexpected changes in file sizes

Of course, to see these symptoms, you might need to actively look for them. For example, when your Windows machine becomes slow, you might start Task Manager to view processor and memory utilization. You could then look at the ongoing processes to see which process is using the greatest amount of processor and memory resources. You might also review the processes and services in memory (again, you can use Task Manager). In addition, you could use the System Configuration. Of course, to be able to determine which processes and services are rogue, you need to have a baseline of what processes and services are currently running on your healthy system for comparison purposes. Finally, to detect malware, you should use an up-to-date antivirus program and an up-to-date antispyware package, which together can scan your entire system and look for malware in real time as you open files and access websites.

With the many tools attackers can now use to deliver malware, it is easy to see the importance of protecting your computer from all types of malware threats. Of course, when protecting yourself, a little common sense can go a long way.

Email has become an essential service for virtually every corporation. Unfortunately, much of the email received by a company's employees consists of unsolicited messages called ***spam*** or junk email, some of which can carry malware and may lead to fraud or scams.

The idea behind spam is to send a lot of unsolicited bulk messages indiscriminately, hoping that a few people will open the email, navigate to a website, purchase a product, or fall for a scam. For the people who create it, spam has minimal operating costs. Over the last few years, spam amounts have increased exponentially, and today, spam accounts for at least 90 percent of all the email in the world.

Besides the risk of malware and fraud associated with spam, there is also a loss of productivity for email recipients as they sort through unsolicited emails. In addition, the IT department will need to install additional storage and provide sufficient bandwidth to accommodate the extra email. Therefore, you should always install a spam blocking device or software that includes antivirus protection. The program will provide a second layer to protect your network from viruses.

The best place to establish a spam filtering system is on a dedicated server or appliance or as part of a firewall device or service. You can direct all email to the spam filter by changing your DNS Mail Exchanger (MX) record to point to the antispam server or device. Any email that is not considered spam will be forwarded to your internal email servers.

When establishing a spam filtering system, keep two things in mind. First, spam filtering systems will not catch every single spam message. Like an antivirus package, a spam filtering solution needs to be kept up to date and constantly tweaked. You might also need to add email addresses, email domains, IP address ranges, or keywords into a black list. Any email with traits on the black list will automatically be blocked. Of course, you need to take care when using a black list to make sure you don't make the criteria so broad as to start blocking legitimate email.

Many antispam solutions also use a real-time blackhole list (RBL) or DNS-based blackhole list (DNSBL) that can be accessed freely. RBLs and DNSBLs are lists of known spammers that are updated frequently. Most mail server software can be configured to reject or flag messages that have been sent from a site listed on one or more such lists. Because spammers look for ways to get around this, it is just one tool that can help reduce the amount of spam that gets through.

As email is identified as spam, it is usually quarantined or stored temporarily in case a legitimate email has been mistakenly placed in this category. While the number of miscategorized messages should be relatively low, you will need to train your helpdesk personnel and possibly your users to access quarantined email so they can release misplaced messages to their destined email boxes. In addition, you need to add the sender's email address or domain to a white list so that it will not be identified as spam in the future.

Detecting spam can be a daunting task if you've ever had to do it manually. Besides the obvious advertising phrases and other keywords, spam systems will also look at an email's header to analyze information about the email and its origin.

Sometimes, spammers will try to spoof an email address or IP address, whereby a message has a fake send-from email address or IP address so that it will not get blocked by spam filters. For example, if email is sent from a yahoo.com domain, an antispam system could do a reverse lookup using the DNS PTR record to see the IP address of the yahoo.com domain. If that IP address does not match where the email said it came from, the message is considered spam and will be blocked.

Sender Policy Framework (SPF) is an email validation system designed to prevent email spam that uses source address spoofing. SPF allows administrators to specify in DNS SPF records in the public DNS which hosts are allowed to send email from a given domain. If email for a domain is not sent from a host listed in the DNS SPF, it will be considered spam and blocked.

Today, antispam packages use special algorithms, such as ***Bayesian filters***, to determine whether email is considered spam. These algorithms usually analyze previously received emails and create a database using a number of attributes. Then, when a computer receives an email, it compares that email to the attributes it has collected to determine whether the message is spam.

Protecting Against Spam and Viruses

Office 365 has several tools that minimize the amount of unwanted messages that reach a user's mailbox while providing a strong defense against malicious software.

Office 365 runs a multi-engine online virus scanning service in Exchange Online Protection (EOP) with multiple anti-spam technologies. Office 365 provides the following defenses against malware and spam:

- Malware filtering
- Outbound spam control
- Spam quarantine
- Connection filtering
- Content filtering

CONFIGURING OFFICE 365 MALWARE FILTERS

EOP users multiple malware detection engines to scan incoming and outgoing mail. As with any antivirus server, the engines are frequently updated as new virus definitions appear. In Office 365, you can configure a malware policy that defines what happens when malware is detected and you can configure a malware rule that defines who the policy applies to.

Malware filters are configured through the protection settings in Exchange Online. You can also configure rules and policies separately by using Windows PowerShell. Exchange Online comes with a preconfigured malware filter that simply deletes the message without providing any notifications. This policy, which applies to everyone, can be edited but not deleted. You also cannot change to whom the policy applies. If during your planning you identify that your company needs differing protection arrangements for different internal groups, you can add malware filters and fine-tune the settings to meet the identified requirements.

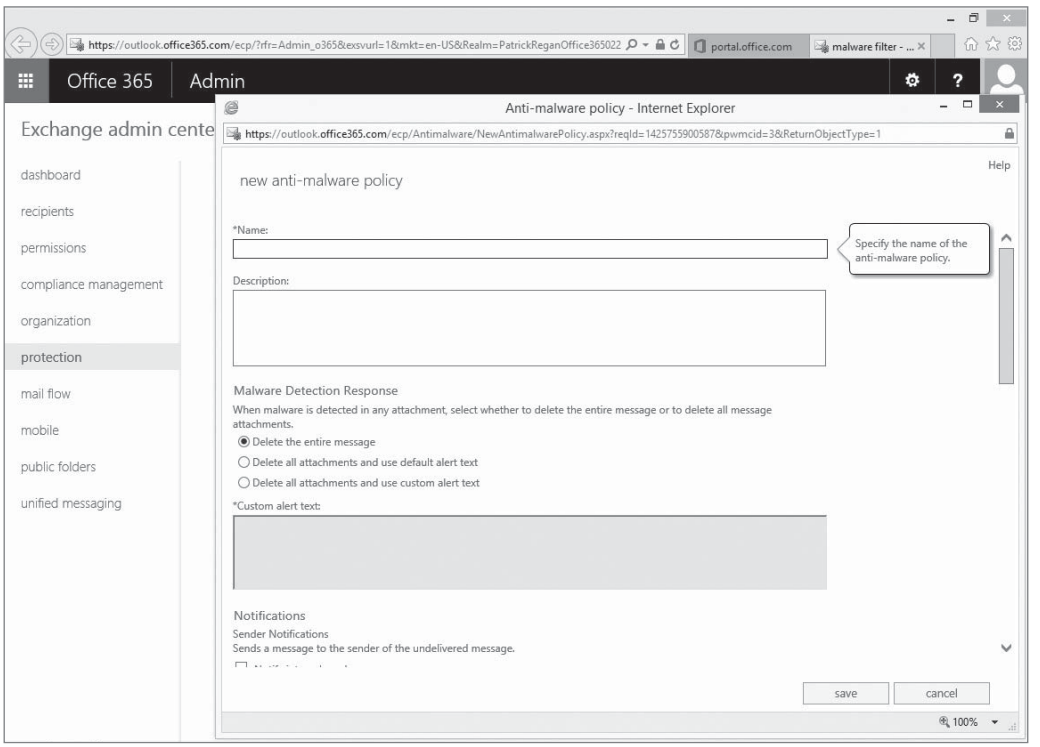
CONFIGURE A NEW MALWARE DETECTION RULE AND POLICY

GET READY. To configure a new malware detection rule and policy, perform the following steps.

1. Sign in to Office 365 (https://portal.office.com) and then click the **Admin** icon.
2. Expand **ADMIN**, click **Exchange**, and then click **protection**.
3. Click **malware filter**.
4. On the malware filter page, click the **+** (new) button. The new anti-malware policy page opens, as shown in Figure 4-17.
5. In the Name text box, type a distinctive name for the new policy.
6. Under Malware Detection Response, select one of the following options:
   - Delete the entire message (which does not send any notification)
   - Delete all attachments and use default alert text
   - Delete all attachments and use custom alert text (If you select this option, you can specify the alert text to be sent in response to a malware detection in the Custom alert text box)
7. Under Notifications, you can select the following options:
   - Notify internal senders (notifies users within the organization that their message had a virus)
   - Notify external senders (notifies users outside the organization that their message had a virus)

Figure 4-17

Creating a new anti-malware policy



8. Under Administrator Notifications, check the options to have the administrator notified of infected messages:
   - Select Notify administrator about undelivered messages from internal senders and enter the email address of the administrator (this email could be that of a managing partner).
   - Select Notify administrator about undelivered messages from external senders and enter the email address of the administrator (this can be different to the previous email address).
9. Under Customize Notifications, select the option for Use customized notification text, enter a From name, Address, message Subject and content of the Message in the relevant fields.
10. Under Applied To, you can now specify to whom this policy applies. Options that you can select are:
    - The recipient is <select name or names>
    - The recipient domain is <enter a registered Office 365 domain>
    - The recipient is a member of <select group>
11. Click **save** to store the new policy.

Policies are applied in order from the highest priority to the lowest. The default policy is always the lowest priority, which is used to simply delete the offending messages.

MANAGING OFFICE 365 OUTBOUND SPAM CONTROL AND SPAM QUARANTINE

In Office 365, Exchange Online uses anti-spam message headers and spam confidence levels to reduce the number of incoming spam messages. When EOP scans an incoming message, it inserts an X-Forefront-Antispam-Report header (X-header) into the message. Fields to show how the message was processed.

The message fields are as follows:

- **CTRY:** The country from which the message connected to the service, based on the connecting IP address. The connecting IP address may not be the same as the originating sending IP address.

- **LANG:** The language in which the message was written, as specified by the country code.
- **SCL:** The Spam Confidence Level (SCL) value of the message.
- **SRV:BULK:** The message was identified as a bulk email message. If the Block all bulk email messages advanced spam filtering option is enabled, it will be marked as spam. If it is not enabled, it will only be marked as spam if the rest of the filtering rules determine that the message is spam.
- **SFE:** Filtering was skipped and the message was let through because it originated from a safe sender.
- **BLK:** Filtering was skipped and the message was blocked because it originated from a blocked sender.
- **SPM:** The message was marked as spam by the content filter.
- **SKS:** The message was marked as spam prior to being processed by the content filter. This includes messages where the message matched a Transport rule to automatically mark it as spam and bypass all additional filtering.
- **NSPM:** The message was marked as non-spam and was sent to the intended recipients.

As an incoming message goes through a spam filter, the emails are assigned a spam score/SCL value:

- **-1:** Message comes from safe sender, safe recipient, or safe IP address, which is delivered to inbox.
- **0 to 1:** Message scanned and found to be cleaned, which is delivered to inbox.
- **5-6:** Message is identified as spam, which is sent to the junk email folder.
- **9:** Message is identified as high confidence spam, which is sent to junk email folder.

EOP does not use SCL levels, 2, 3, 4, 7, and 8. You can use content filtering policies to delete the high confidence spam. You can also set SCL conditions in transport rules.

MANAGING OFFICE 365 CONNECTION FILTERS

Exchange Online provides a ***connection filter*** that enables you to configure filtering based on IP addresses, with separate allow and block lists. The allow lists are typically addresses or ranges that you trust. Block lists are addresses or subnets of known spammers from which you do not want to receive emails. You can also configure safe lists that are automatically allowed in. When configuring these lists, remember that allow settings typically override block settings.

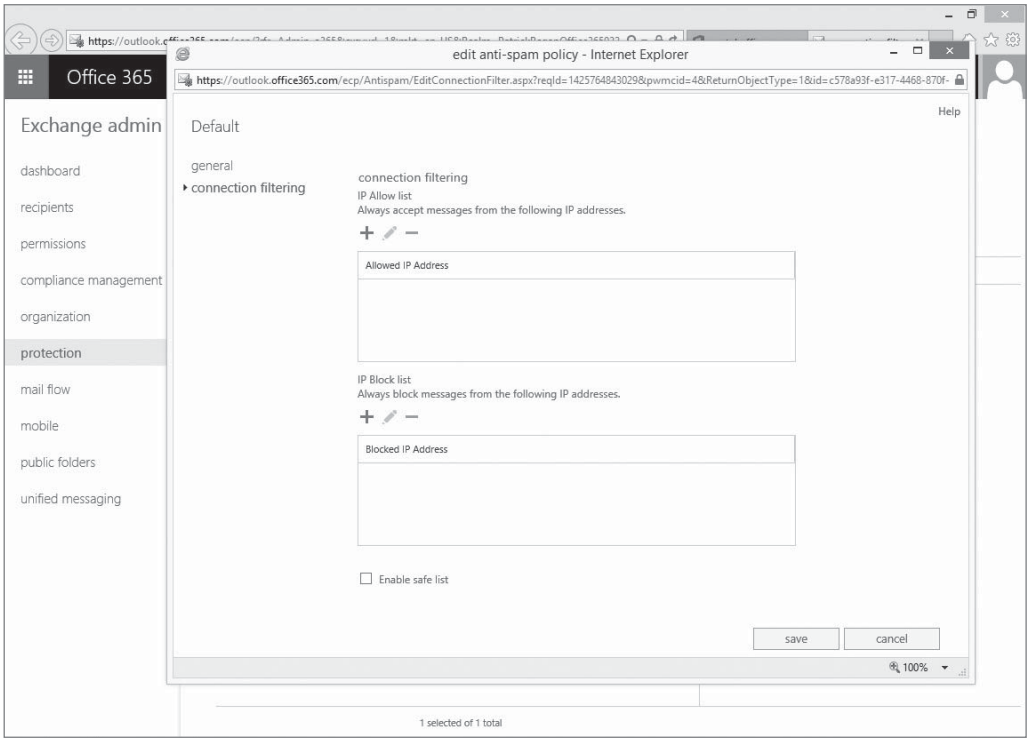
CONFIGURE A CONNECTION FILTER

GET READY. To configure a connection filter, perform the following steps.

1. Sign in to Office 365 (https://portal.office.com) and then click the **Admin** icon.
2. Expand **ADMIN**, click **Exchange**, and then click **protection**.
3. Click **connection filter**.
4. Double-click the **Default filter** and then click the **connection filtering** tab as shown in Figure 4-18.
5. Under IP Allow list, click the **+** (add) button.
6. On the add allowed IP address page, type the IP address or range that you want to allow and then click **ok**.
7. Under IP Block list, click the **+** (add) button.
8. On the add blocked IP address page, type the IP address or range that you want to deny and then click **ok**.
9. If required, check **the Enable safe list** option and then click **save**.

Figure 4-18

Defining connection filtering



MANAGING OFFICE 365 CONTENT FILTERS

Content filter is provide a range of basic and advanced filtering options and automatically add spam processing headers and assign a spam confidence level to the messages before delivery to user mailboxes. These settings include:

- General (name, description)
- Actions
- International spam
- Advanced options
- Applied to

Exchange Online provides a default content filter with the following settings:

- **Spam:** Move message to Junk Email folder.
- **High confidence spam:** Move message to Junk Email folder.
- **International spam:** No settings configured.
- **Advanced options:** All off, except for Block all bulk email messages.

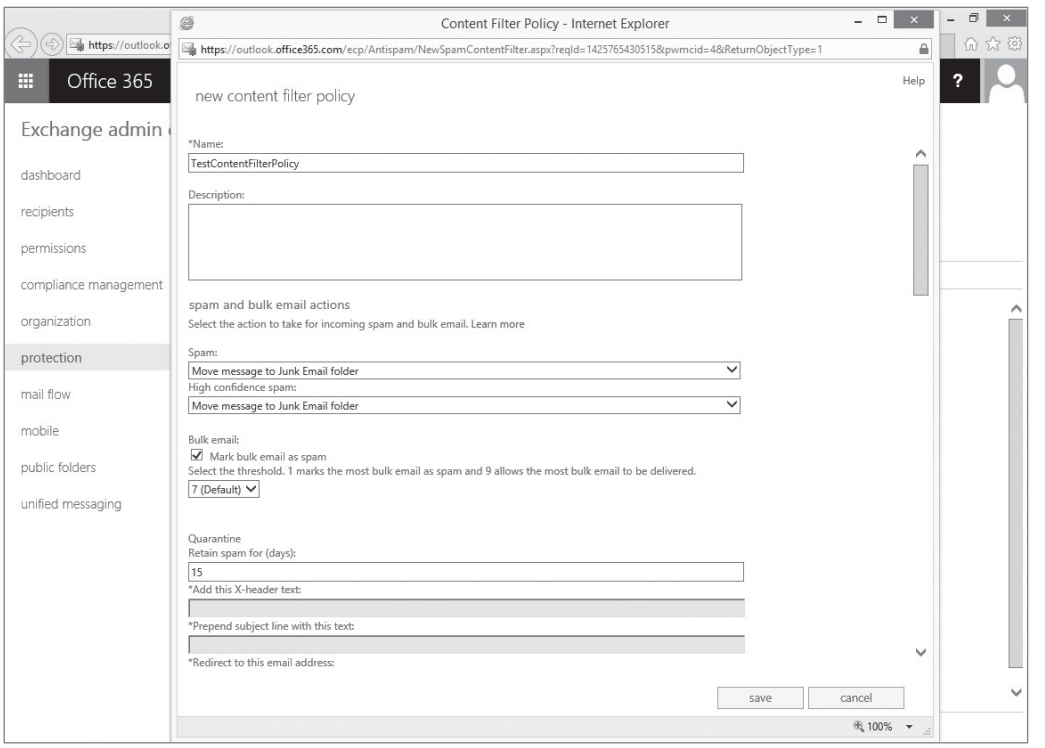
CONFIGURE CONTENT FILTERS

GET READY. To configure content filters, perform the following steps.

1. Sign in to Office 365 (https://portal.office.com) and then click the **Admin** icon.
2. Expand **ADMIN**, click **Exchange**, and then click **protection**.
3. Click **content filter**.
4. Click the **+** (new) icon.
5. On the new content filter policy page (as shown in Figure 4-19), specify a policy Name and optional Description.

Figure 4-19

Defining a content filter policy



6. Under the spam and bulk email actions section, set what you want to happen to Spam and High confidence spam. Depending on which option you set, you might have to configure additional fields:
   - Move message to Junk Email folder (default)
   - Add X-header (and set the X-header text)
   - Prepend subject line with text (and add the prepended subject line text)
   - Redirect message to email address (and add the redirect email address)
   - Delete message
   - Quarantine message (and set the number of days that you want to keep quarantined messages for up to the maximum of 15)
7. Under international spam, you can filter for messages in specific languages and from individual countries. Check the boxes for Filter email messages written in the following languages or Filter email messages sent from the following countries or regions and then, under each option, click the **+** icon. Click the language or country to filter, click **add**, and then click **ok**.
8. In advanced options, in the Increase Spam Score section, select which of the following message characteristics you want to indicate that a message is more likely to be junk:
   - **Image links to remote sites:** any message with image links to remote websites will receive an increased spam score.
   - **Numeric IP address in URL:** any message that has numeric-based URLs (most often in the form of an IP address) will receive an increased spam score.
   - **URL redirect to other port:** any message that contains a hyperlink that redirects the user to ports other than port 80 (regular HTTP protocol port), 8080 (HTTP alternate port), or 443 (HTTPS port) will receive an increased spam score.
   - **URL to .biz or .info websites:** When this setting is enabled, any message that contains a .biz or .info extension in the body of a message will receive an increased spam score.

9. In the mark as spam section, set the following options to match your spam policy planning:
   - **Empty messages:** any message in which the body and subject line are both empty, and which also has no attachment, will be marked as spam.
   - **JavaScript or VBScript in HTML:** any message that uses JavaScript or Visual Basic Script Edition in HTML will be marked as spam.
   - **Frame or IFrame tags in HTML:** any message that contains the "Frame" or "IFrame" HTML tag will be marked as spam. These tags are used on websites or in HTML messages to format the page for displaying text or graphics.
   - **Object tags in HTML:** any message that contains the "Object" HTML tag will be marked as spam. This HTML tag allows plug-ins or applications to run in an HTML window.
   - **Embed tags in HTML:** any message that contains the "Embed" HTML tag will be marked as spam. This HTML tag allows varying data types to be embedded into an HTML document. Examples include sounds, movies, or pictures.
   - **Form tags in HTML:** any message that contains the "Form" HTML tag will be marked as spam. This HTML tag is used to create website forms. Email advertisements often include this tag to solicit information from the recipient.
   - **Web bugs in HTML:** any message that contains a Web bug will be marked as spam. A web bug is a graphic designed to determine whether a web page or email message has been read.
   - **Apply sensitive word list:** any message that contains a word that's included in the sensitive word list will be marked as spam.
   - **SPF record:** hard fail: messages that hard fail an SPF check will be marked as spam (SPF filtering is always performed). Turning this setting on is recommended for organizations that are concerned about receiving phishing messages. (In order to avoid false positives for messages sent from your company, make sure that the SPF record is correctly configured for your domains.)
   - **Conditional Sender ID filtering: hard fail:** any message that hard fails a conditional Sender ID check is marked as spam. Turning this setting on is recommended for organizations that are concerned about phishing, especially if their own users are being spoofed. This option combines an SPF check with a Sender ID check to help protect against message headers that contain forged senders.
   - **NDR backscatter:** any message that matches the non-delivery report (NDR) bounce characteristics will be marked as spam. It is not necessary to enable this setting if your organization uses EOP to send outbound mail.
   - **Block all bulk email messages:** any message that is identified as bulk mail, such as advertisements and marketing emails, will be marked as spam.
10. In Test Mode Options, you can configure what happens when a match is made to a test-enabled advanced option above. Select one of the following choices:
   - **None:** The message is marked as spam but nothing else happens.
   - **Add the default test X-header text:** Select this check box to insert the following text as part of the incoming message header: X-CustomSpam: This message was filtered by the custom spam filter option.
   - **Send a Bcc message to this address:** Specify an email address or addresses to send copies of the messages that are filtered in test mode. Separate multiple addresses with a semicolon.
11. Under Applied To, select conditions such as the recipient is, the recipient is a member of a group, or the recipient is a member of a domain.
12. Click **save**.

MANAGING MICROSOFT INTUNE ENDPOINT PROTECTION

Microsoft Intune includes Endpoint Protection, which provides real-time protection against malware threats, keeps malware definitions up-to-date, and automatically scans computers. Once the client is installed onto a device, Endpoint Protection automatically protects the device.

Similar to Microsoft Defender, Microsoft Intune Endpoint Protection provides real-time protection and scan capabilities against viruses and other forms of malware. As with any antivirus package, Endpoint Protection virus and spyware definitions are constantly updated as new viruses are discovered. Therefore, to protect against newer viruses, you must keep Endpoint Protection updated. Since Microsoft Intune is managing Endpoint Protection, Microsoft Intune will update the virus and spyware definitions.

The Endpoint Protection Console can be opened by clicking the Microsoft Intune Endpoint Protection icon on the notification section of the taskbar. The console includes four tabs:

- The Home tab allows you to check the status of Endpoint Protection, including whether Endpoint Protection is up to date and whether Endpoint Protection is protecting your system. It also gives you the option to initiate a scan.
- The Update tab provides you with information about your virus and spyware definitions. It is important to keep these current to ensure your computer is protected at all times.
- The History tab provides information about items that have been detected in the past and the actions that were taken with them.
- The Settings tab is where you can fine-tune how Endpoint Protection works.

As explained in Lesson 3, you can use a policy to configure Endpoint Protection settings.

■ Configuring SharePoint Online

THE BOTTOM LINE

SharePoint is a popular web platform developed by Microsoft that offers a powerful, flexible, and scalable centralized web application. Although SharePoint looks like a typical web site, it's actually a web content management system, a document management system, and a collaboration tool.

CERTIFICATION READY
Configure SharePoint Online, including OneDrive
4.2

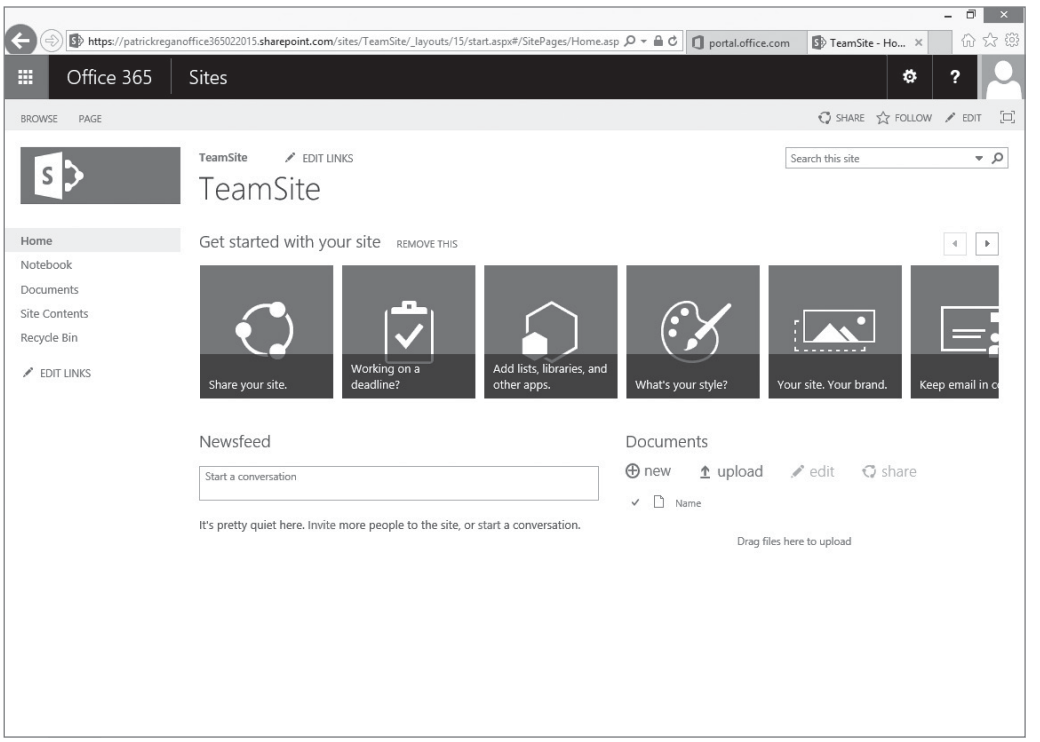
SharePoint is a suite of services that provides a web site/portal that allows users to organize and retrieve information; using SharePoint, users can easily collaborate on projects. SharePoint also allows the tracking and management of projects and business processes. To accomplish all of this, SharePoint provides the following:

- A central repository for information that can be easily organized and retrieved
- An easy-to-use and familiar environment
- A flexible, customizable platform
- Tools to create information easily
- Tools to share and exchange information
- Controls to protect data
- Tools to track tasks and processes
- Tools to manage workflows

SharePoint allows for quick learning, lower support costs, effective management, improved security, and easy growth. Of course, the trick to working with SharePoint is to configure SharePoint in a way that organizes the organization's data and communicates the correct information in a timely manner. It should also be noted that users get just the right amount of information—not too little and not too much. Since SharePoint displays as a Web site/portal, users need only use a web browser to access SharePoint. Figure 4-20 shows the default TeamSite.

Figure 4-20

The default TeamSite



Creating SharePoint TeamSites

A ***site collection*** is a grouping of sites. Every site collection has a single root site, under which the other sites are built. All sites within the site collection have the same site owners and share the same administrative settings.

A SharePoint Online administrator is responsible for creating and deleting site collections. Based on your needs, you can create multiple SharePoint sites.

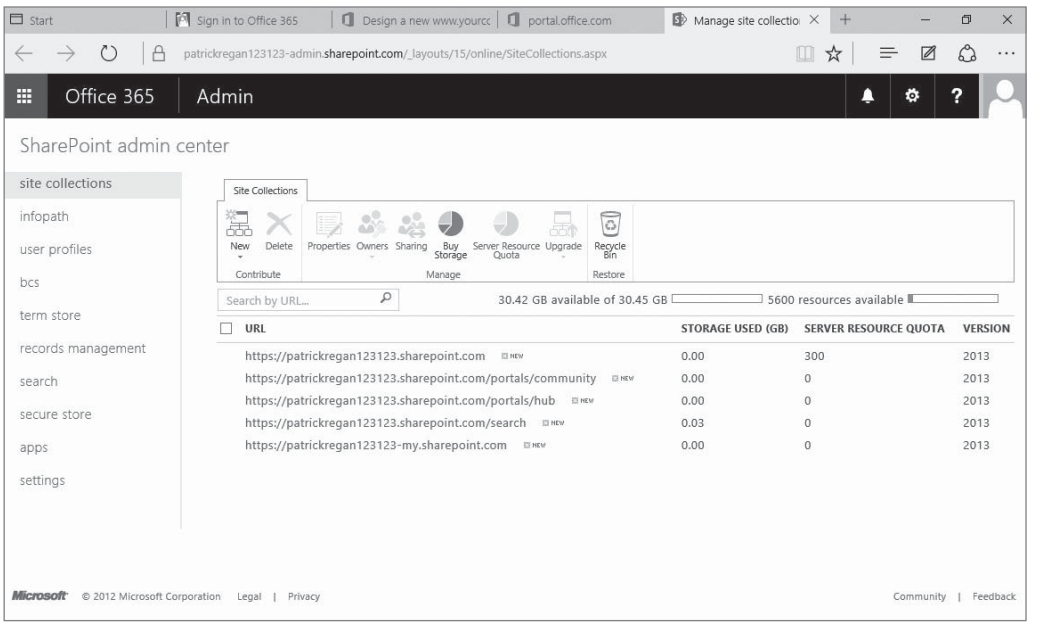
CREATE A SITE COLLECTION

GET READY. To create a SharePoint site collection in Office 365, perform the following steps.

1. Sign in to Office 365 (https://portal.office.com) and then click the **Admin** icon.
2. Expand **ADMIN** and then click **SharePoint**. Site collections are shown in Figure 4-21.
3. In the ribbon, choose **New** > **Private Site Collection**.
4. In the new site collection dialog box (see Figure 4-22), specify the following:
   - A Title for the site collection.
   - A Web Site Address for the site collection. You can choose either /sites or /teams as part of the path and then supply a further path extension to be the path to the site in the empty text box.
   - A language for the site collection. (You must ensure you select the correct language for your site collection here, because it cannot be changed afterwards.)
   - A template that matches the purpose of the site collection. For example, if your site collection is going to be used for a specific project, choose the Project Site template from the list. (There are three categories of templates to choose from: Collaboration, Enterprise, or Publishing. Or you can pick the Custom template, which enables you to select a template at a later time.)

Figure 4-21

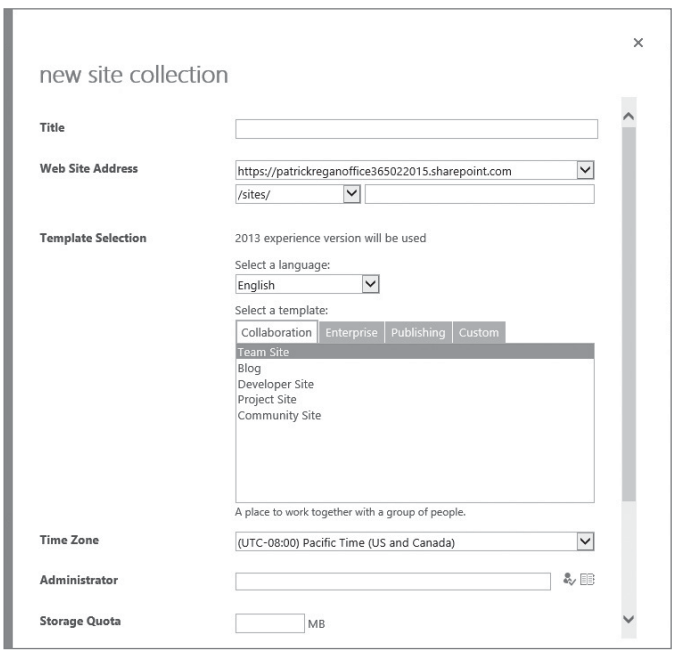
Viewing site collections



- An appropriate Time Zone.
- A site collection Administrator. You can use either the Check Names button or the Browse button to help find a user's name.
- A Storage Quota to allocate to this site collection. This must not exceed the total storage available that is displayed next to the box.
- A Server Resource Quota to allocate to this site collection.

Figure 4-22

Creating a new site collection



5. Click **OK**.

It will take a few minutes for the collection to be created. When the site collection is created, it will be highlighted in blue as a hyperlink. At this point, the assigned site collection administrator can begin creating and managing sites in the site collection.

The properties page of the site collection displays the following information:

- Title
- Website address
- Primary administrator and administrators
- Number of subsites
- Storage usage, quota, and warning level
- Resource usage, quota, and warning level

ADD SITE COLLECTION ADMINISTRATORS

GET READY. To add SharePoint site collection administrators in Office 365, perform the following steps.

1. Sign in to Office 365 (https://portal.office.com) and then click the **Admin** icon.
2. Expand **ADMIN** and then click **SharePoint**.
3. Select the check box next to the appropriate site collection.
4. On the ribbon, in the Manage section, choose **Owners** and then click **Manage Administrators**.
5. In the manage administrators dialog box, under Primary Site Collection Administrator, change the user name for the primary site collection administrator.
6. Use the **Check Names** button to verify that the user names are valid.
7. Choose **OK**.

The Sharing option on the site collection page allows you to share the site collection with users outside your organization. This can be done through invitations or by providing anonymous guest links.

At the top of the page, you will find three tabs

- **Browse:** Enables you to display the page without any obstructions.
- **Page:** Contains tools that enable you to edit your public website pages and modify the layout and elements.

If you have a project that requires sharing or collaborating with clients or vendors, you can create a site collection, which will enable sharing. A site can be shared by a site owner or a user with Full Control permission on a site, There are three methods for sharing site content with external users:

- You can share your entire site with external users by inviting them to sign in with either a Microsoft account or with an Office 365 user ID.
- You can share individual documents with external users by inviting them to sign in to your site with either a Microsoft account or with an Office 365 user ID.
- You can share individual documents with external users by sending them an anonymous guest link to view or edit the document.

Although external users can use Office Web Apps to view and edit documents, they will not be able to create personal sites and they will not have their own OneDrive for Business library. They will not be able to view organizational news feeds, they cannot edit profiles, and they cannot change their pictures or view aggregated tasks. In addition, external users cannot be a site collection administrator and they will have limitations when performing searches with the Search Center.

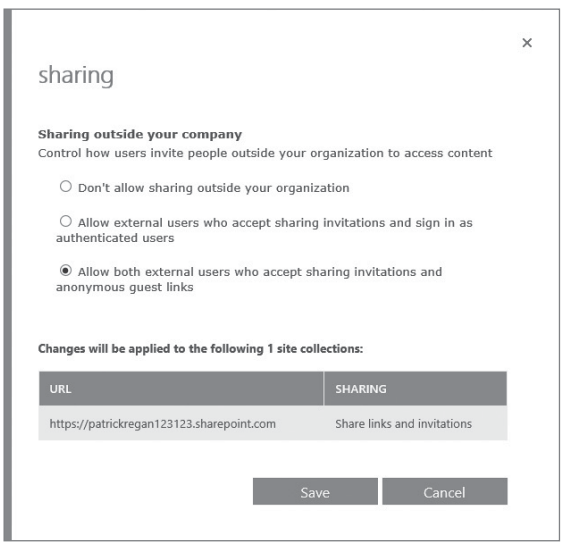
CONFIGURE EXTERNAL SHARING FOR A SITE COLLECTION

GET READY. To configure external sharing for a site collection in Office 365, perform the following steps.

1. Sign in to Office 365 (https://portal.office.com) and then click the **Admin** icon.
2. Expand **ADMIN** and then click **SharePoint**.
3. On the site collections page, select the check box for the site collection for which you want to configure external sharing.
4. In the Manage section of the ribbon, choose **Sharing**.
5. In the Sharing dialog box (as shown in Figure 4-23), choose one of the following:
   - Don't allow sharing outside your organization: Prevent users from sharing sites or content with any external users.
   - Allow external users who accept sharing invitations and sign in as authenticated users: Require that any external user who has received an invitation to access shared content to log in with a Microsoft account before being allowed to access the content.
   - Allow both external users who accept sharing invitations and anonymous guest links: Allow external users who have received an invitation and signed in with a Microsoft account to access shared content; will also allow users to share documents directly with external users through anonymous guest links.

Figure 4-23

Sharing a SharePoint site



6. Click **Save**.

After you enable external sharing, you can share the entire site or individual documents. To share an entire site, you need to send them an invitation to the site. They will then log on to the site with a Microsoft account or an Office 365 ID and access the content. The message sent will include a link to the site and an optional message. The invitation can be redeemed only once. Therefore, it cannot be shared or used by others to gain access.

When you send the invitation, you determine the permissions the external user will have on the site:

- **Full Control:** Chosen by selecting the Sitename Owners [Full Control] option.
- **Edit:** Chosen by selecting the Sitename Members [Edit] option.
- **Read:** Chosen by selecting the Sitename Visitors [Read] option.

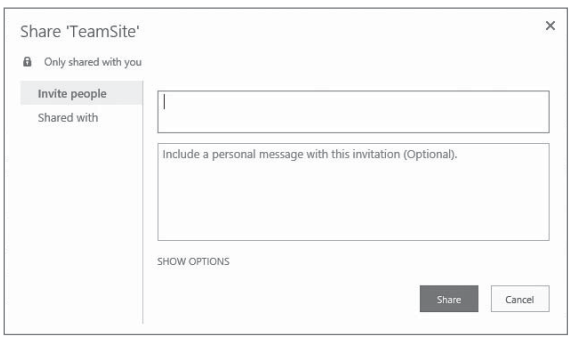
INVITE USERS TO A SITE COLLECTION

GET READY. To invite users to a site collection in Office 365, perform the following steps.

1. Navigate to the site you wish to share with an external user.
2. Choose **SHARE**.
3. In the Share sitename dialog box (as shown in Figure 4-24), type the email address of the external user you want to invite to share your document. (If you want to share with an internal user, just type their name.)

Figure 4-24

Inviting users to a site collection



4. Type a message that will be included as part of your invitation.
5. Click **SHOW OPTIONS**.
6. Under Select a group or permission level, in the drop-down list, select **Sitename Visitors [Read]**.
7. Click the **Share** button.
8. When the external user receives the emailed invitation, he will see your message and will need to click the Go To sitename link and then sign in with either a Microsoft account or an Office 365 ID.

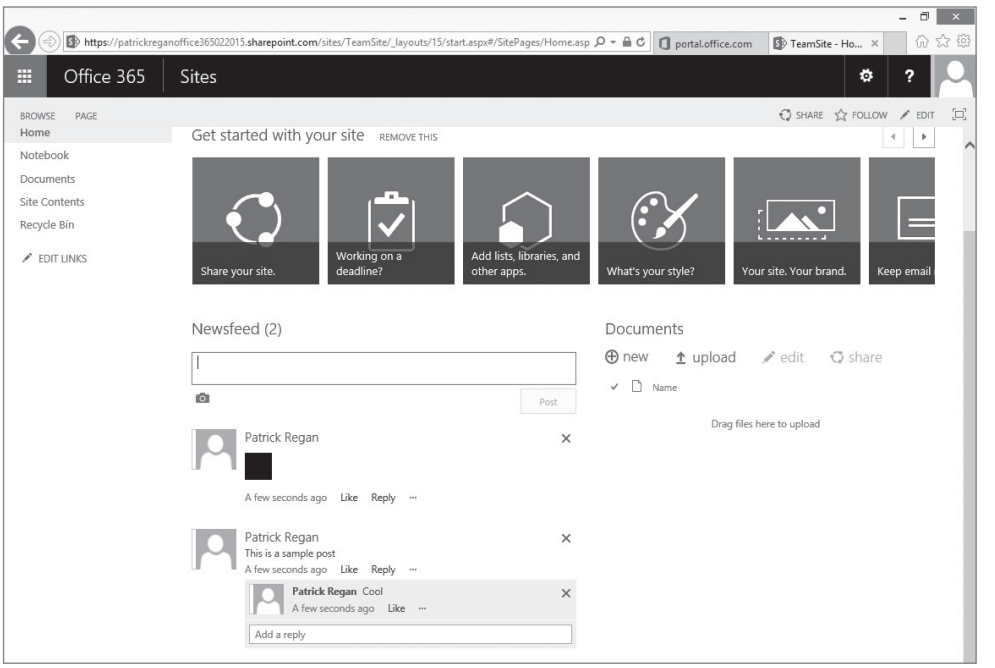
Setting up Social Features

Social networking expands collaboration by providing additional methods for users to work and interact inside and outside the office. A public ***newsfeed*** allows users to stay in tune with conversations between groups of people and to see updates about their activities, as shown in Figure 4-25. Besides text, you can also upload pictures.

Yammer is an enterprise collaboration platform that allows private communication within an organization. Yammer limits access based on the user's Internet domain so that only a user with the appropriate email address can join the respective network.

By default, the SharePoint Newsfeed is used for the organization's Enterprise Social Collaboration network. However, you can replace the SharePoint Newsfeed with Yammer, so that users can use Yammer as an ad-hoc collaboration tool that enables them to easily share documents, notes, ideas and images. While you can use both SharePoint Newsfeed and

Figure 4-25
Using a newsfeed



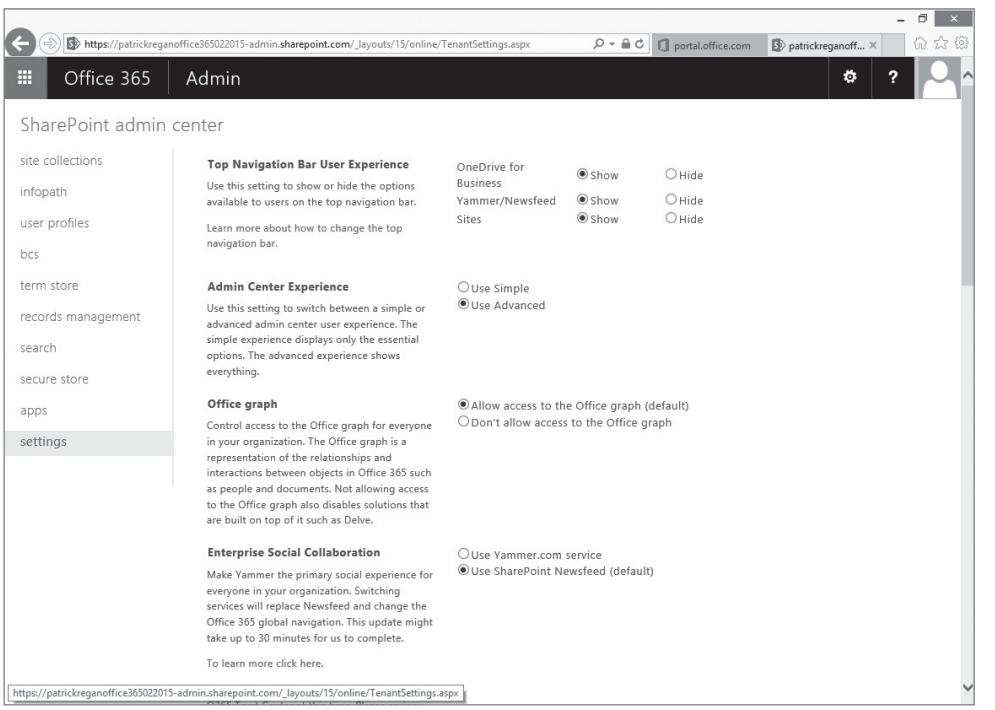
SharePoint Social, you users can follow people, "like" or reply to comments, share updates, post poll questions, and praise other users. With Yammer, you can also filter conversations, set up immediate, daily, or weekly update emails on specific groups, and direct-message other users.

REPLACE THE NEWSFEED LINK WITH A LINK TO YAMMER

GET READY. To replace the newsfeed link with a link to Yammer in Office 365, perform the following steps.

1. Sign in to Office 365 (https://portal.office.com) and then click the **Admin** icon.
2. Expand **ADMIN**, and then click **SharePoint**.
3. Click **Settings** (see Figure 4-26).

Figure 4-26
Managing SharePoint settings



4. Under Enterprise Social Collaboration, choose **Use Yammer.com service**.
5. Click **OK**.

Applying Themes

Themes define SharePoint site color schemes, including those that are applied to menus, system pages, the ribbon, and so forth. You can choose a color scheme that complements the look and feel of your company's web page.

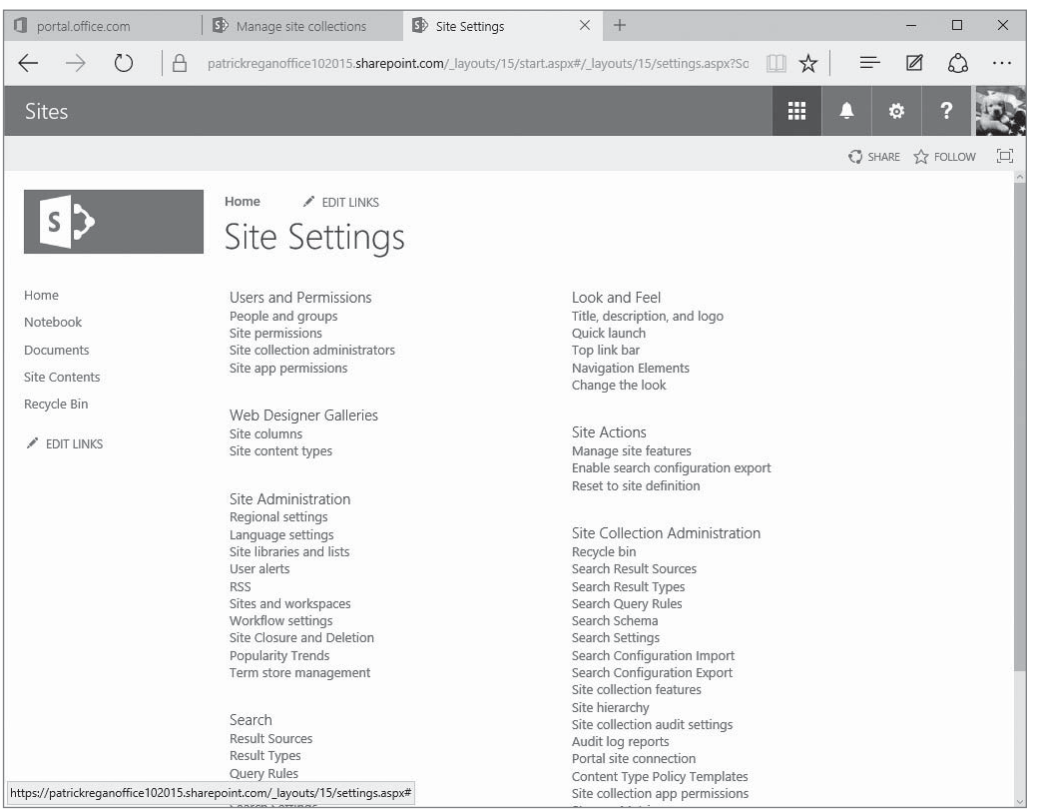
By clicking the Site tab, you can change the look, edit the title, and change the logo. You can also edit the menu navigation, and edit site elements such as footer and address fields.

MODIFY THE THEME FOR A SHAREPOINT SITE

GET READY. To modify the theme for a SharePoint site in Office 365, perform the following steps.

1. Navigate to the site.
2. At the top of the page, click the **Settings** button and then click **Site Settings**.
3. On the Site Settings page (as shown in Figure 4-27), click **Change the Look**.

Figure 4-27
The Site Settings page



4. Click a theme. On the Change the look page, click **Try it out**.
5. On the preview page, click **Yes, keep it.**
6. To change the title, click **Title, description, and logo**.

7. On the Site Settings > Title, description, and logo page, in the Title text box, type a new title.
8. To upload a new logo, click the **FROM COMPUTER** option. On the Add a document page, for the Choose a file option, click the **Browse** button. In the Open dialog box, navigate to a picture and double-click the picture. Click **OK** to close the Add a document page.
9. Click **OK** to close the Site Settings > Title, description, and logo page.

Setting Storage and Resource Limits

When you sign up for SharePoint Online for Office 365, you are allocated storage space based on your number of users (10 GB + 500 MB * number of users). Therefore, if you have 10 users, you will have 10 GB + 500 MB * 10 users = 15 GB. If necessary, you can buy more storage through the SharePoint Online admin center at a cost per gigabyte (GB) per month.

If you choose to use the pooled storage model, you can set the storage management option to auto and then SharePoint will disregard any existing limits you had set previously on your site collections and reset them all to 1 TB. New Office 365 customers will have the pooled storage model enabled by default. If you want to fine-tune the storage space allocated to each site collection, you can set the storage management option to manual and specify individual site collection storage limits.

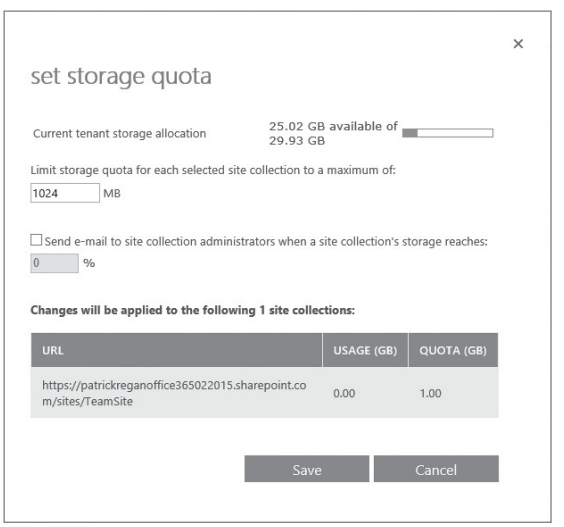
MANAGE STORAGE LIMITS

GET READY. To manage the storage limits for Office 365 SharePoint, perform the following steps.

1. Sign in to Office 365 (https://portal.office.com) and then click the **Admin** icon.
2. Expand **ADMIN** and then click **SharePoint**.
3. Click **settings**.
4. For the Site Collection Storage Management, select **Manual**.
5. Click **OK**.
6. Click **site collections**.
7. Select the check box for the site you want to limit and then click **Storage Quota**.
8. In the Limit storage quota, enter the maximum number of megabytes to be allocated to each site collection, as shown in Figure 4-28.

Figure 4-28

Setting the storage quota for a site



9. Check the check box for the **Send email to site collection administrators when a site collection's storage reaches:** option, which will send a message to site collection admins when the site collections are approaching the storage limit. You can also enter a number between 1 and 100 for the percentage of the limit to reach before an email alert is triggered.
10. Click **Save**.

■ Configuring OneDrive

THE BOTTOM LINE

OneDrive, formerly named SkyDrive, is a file-hosting service that allows you to create and store files and folders and then share them with other users and groups.

CERTIFICATION READY
Configure SharePoint Online, including OneDrive
4.2

OneDrive is a free (up to 1 GB), secure file-hosting service that enables your users to store, synch, and share files across devices using the cloud. Office 365 comes with 1 GB of OneDrive storage for each user. Additional storage can be purchased. You can also use it to synchronize files and folders that you select across multiple devices. If you forget to include a file within your synch folder, you can use OneDrive to connect to your remote computer, locate the file, and then upload it to your OneDrive space. This process is called ***fetching***.

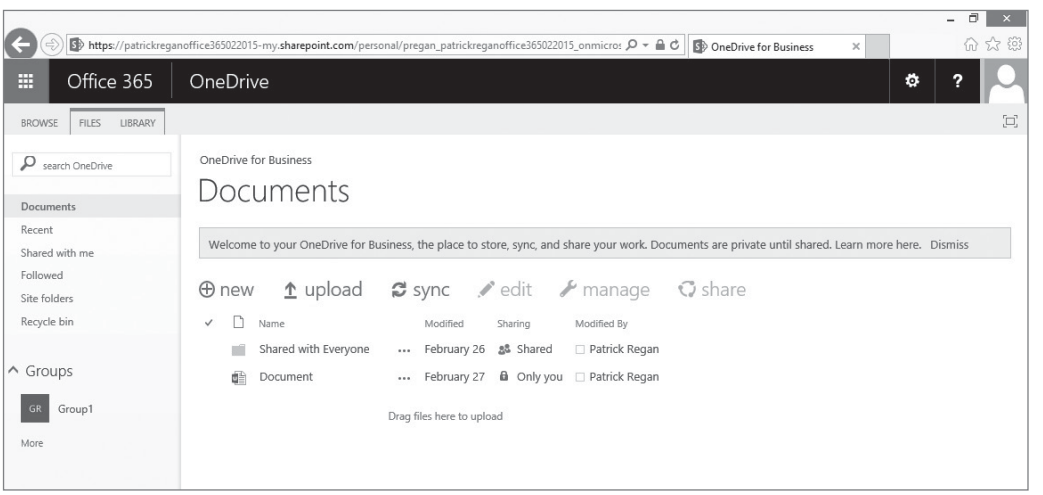
The public offering of OneDrive, is intended for personal use and is easily comparable to Dropbox. You store files in in your OneDrive and access them from anywhere. ***OneDrive for Business*** is different than the public version of OneDrive because it is based on. However, since OneDrive for Business is based on SharePoint, it can be used by team members to store and work on documents with others and it helps ensure that business files for your users are stored in a central location.

Accessing OneDrive from a Browser

You can access OneDrive from a browser using your Microsoft User Account from anywhere you have an Internet connection.

While OneDrive can be accessed from a browser at http://onedrive.live.com, OneDrive for Business is accessed from the Office 365 Admin Portal. After you are logged in to Office 365, you can click the OneDrive button to open the OneDrive Admin Console (see Figure 4-29),

Figure 4-29
The OneDrive for Business Console



on which you can upload, download, create, and share folders and files. If your computer is configured to support fetching, you can also connect to it remotely from the OneDrive for Business Console.

The following options are available:

- **Documents:** Includes folders created on the OneDrive account. You can also see the number of files each folder contains by looking at the number located in the lower-right corner of each folder. Selecting any of these folders opens and displays its content.
- **Recent:** Includes a list of documents that have been recently created on the OneDrive account.
- **Shared with me:** Provides a list of documents or folders that have been shared with you.
- **Followed:** Documents that you are keeping track of so that they can be easy to find later.
- **Site folders:** Shows a list of team sites/document libraries that you are following.
- **Recycle Bin:** A temporary holding area of deleted documents that can be restored.
- **Groups:** Displays a list of groups that include users with whom you frequently communicate and share documents. When you create a group, users receive emails asking them to join. After clicking the link, they are taken to the Groups page, on which they can communicate with other members via email and also view any files that have been shared to the group.

Creating a File Within OneDrive

OneDrive allows you to collaborate with other users on documents (provided those users have Microsoft accounts). Because documents are stored in the cloud, you can access these documents anytime you are connected to the Internet.

When used with Office 365, OneDrive includes versions of Office apps (Word, Excel, PowerPoint, and OneNote). This allows you to create and edit documents directly from your browser.

CREATE A WORD DOCUMENT WITHIN ONEDRIVE USING A WEB BROWSER

TAKE NOTE* To access OneDrive and complete these steps, you need a Microsoft User Account.

GET READY. To create a Word document within OneDrive using a web browser, log on to a Windows 10 computer with access to the Internet and then perform the following steps.

1. Sign in to Office 365 (https://portal.office.com) and then click the **OneDrive** icon.
2. Click the **Documents** folder.
3. From the menu at the top of the page, click **Create > Folder**.
4. Name the folder Project Files and then click the folder to open it.
5. From the menu at the top of the page, click **Create > Word document**.
6. Type a few words in the document.

   As you type text, The Word document will be saved frequently.
7. To specify a file name, click **Document1** at the top of the window and then replace that name by typing **Project Scope**.
8. Click the **OneDrive** link (located at the upper-left corner, next to Word Online) to return to the main screen.

Uploading Files to OneDrive

In the previous activity, you learned how to create a file directly on OneDrive using the Word app. You can also upload files directly to OneDrive.

When you have existing files on your computer that you want to upload to OneDrive, you can use either of the following two options:

- From the OneDrive Dashboard, navigate to the folder in which you want to store the file. On the menu, click Upload, browse to the file you want from your computer, and then click Open.
- From the OneDrive app installed on your local computer, you can drag and drop the files you want to upload into the OneDrive folder. This automatically syncs with OneDrive. You can also configure OneDrive for the desktop to allow you to fetch files on your PC from other devices.

Sharing a Document in OneDrive

You can also share a document with others by sending it via email, posting it to a social network, or sending others a link to it.

When you want to share documents, you can use the following options:

- **Send email:** This option should be used if you want to give individual users or groups permission to a file or folder. You can then remove permissions for a specific group or individual if necessary. When users receive the link via email and visit OneDrive, the file or folder will appear in their list of shared files. You do not have to know their Microsoft user account address. If they do not have one, they can create one after clicking on the link.
- **Post to:** This option allows you to share the link on Facebook, LinkedIn, or Twitter. Anyone who views the post on your network can forward the link. If you selected the option to allow recipients to edit the document, anyone the link is forwarded to can view and edit the file or folder.
- **Get a link:** This option should be used if you want to share the file with a larger number of recipients. For example, you could post the link on your blog or your website. You can also include this link in an email or via an instant message. When using this option, you can choose from the following types of links:
  - **View only:** Anyone who receives this link can see the files you share.
  - **View and edit:** Anyone with this link can see and edit the files you share.
  - **Public:** Anyone can search for and view your public files, even if you don't share a link if you decide to make it public.

SHARE A DOCUMENT VIA EMAIL

GET READY. To share the Word document you created in the previous exercise with others via email, perform the following steps.

1. From the main screen of OneDrive, click **Files > Documents > Project Files**.
2. Right-click the Word document you saved in the previous exercise (**Project Scope. docx**) and choose **Share.**

3. Type the email address of the person you want to share it with and, if necessary, type a message.
4. If you want the recipient to be able to edit the document, click the **Recipients can edit** option.
5. Click **Share** to send the email message.
6. Click **Close**.

Accessing OneDrive from the OneDrive Desktop App for Windows

With the ***OneDrive desktop app for Windows*** installed on your local computer, you can automatically sync files and folders with the OneDrive cloud. You can then access your resources across multiple devices, such as computers and smartphones.

The OneDrive desktop app for Windows 7 or 8/8.1 can be downloaded directly from your OneDrive account. The OneDrive/SkyDrive app is already built into Windows 10. When you install the app, a folder will be created on your desktop automatically. Anything that you place into this folder is synched with OneDrive.com as well as with your other computers. You can access the folder from within File Explorer, drag new files into the folder, and choose the folders you want to sync on your computer.

INSTALL THE ONEDRIVE DESKTOP APP FOR WINDOWS

GET READY. To install the OneDrive desktop app for Windows, log on to a Windows 10 computer with administrative credentials and access OneDrive.

1. Open **Internet Explorer**, go to **http://onedrive.live.com** and then click **Sign In**.
2. Type your Microsoft User Account and Password.
3. In the left pane, scroll down and click the **Download OneDrive for Windows** link.
4. When prompted with the Do you want to run or save OneDriveSetup.exe? message, click **Run**.
5. After the OneDrive installation is completed and the Introducing your OneDrive folder dialog box appears, click **Get started**.
6. In the Microsoft OneDrive window, provide the Microsoft Account and password. Click **Sign In**.
7. By default, the OneDrive folder will be stored in the c:\users\%username%\OneDrive folder. On the Introducing your OneDrive folder page, click **Next**.
8. On the Sync only what you want page, All files and folders on my OneDrive is already selected. To choose a different folder, click **Choose folders to sync**. Click **Next**.
9. On the Fetch your files from anywhere page, Let me use OneDrive to fetch any of my files on this PC is already selected. Click **Done**.
10. This setting will download everything but the files that are shared with you from your OneDrive.
11. Click **Done**.

Configuring Skype for Business Online

THE BOTTOM LINE

Skype is a telecommunications application that provides video calls and voice-only calls from computers, tablets, and mobile devices to other devices or telephones/smartphones using an Internet connection. Skype also allow users to send instant messages, files, images, and videos. Calls from one Skype user to another Skype user are free, but calls from a Skype user to landline telephones or mobile phones are charged via a debit-based user account system called Skype Credit.

CERTIFICATION READY
Configure Skype for Business Online
4.3

The enterprise edition of Skype is ***Skype for Business***, which replaced Microsoft Office Communicator, Microsoft Lync, and Windows Messenger used with Microsoft Exchange Server. Microsoft offers an online version of Skype with Office 365 called ***Skype for Business Online***. Skype for Business includes instant messaging, Voice over IP, and video conferencing and can use contacts available from Microsoft Outlook/Microsoft Exchange Servers).

Skype for Business and the Online Meeting Add-in for Skype for Business requires the following:

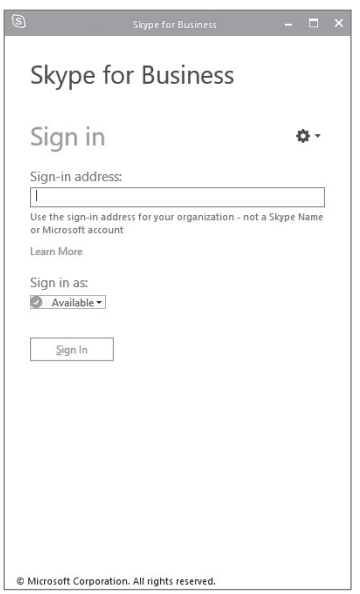
- Windows 7, Windows 8/8.1, Windows 10, Windows Server 2008 R2, or Windows Server 2016.
- Internet Explorer 7 and higher or Mozilla Firefox. If you are using Skype for Business with Microsoft Exchange Online and your organization has deployed an authenticating HTTP proxy, you will need to use Internet Explorer 8 or later.
- To integrate with Office, you need to use Outlook 2010, Outlook 2013, or Outlook 2016.
- To integrate with Microsoft Exchange, you need Microsoft Exchange Server 2010, Microsoft Exchange Server 2013, or Microsoft Exchange Server 2016.

CONFIGURE SKYPE FOR BUSINESS ONLINE

GET READY. To configure Skype for Business Online, log on to a Windows 10 computer with administrative credentials and access OneDrive. Then perform the following steps.

1. Click the **Start** button, click **All Apps**, Expand **Office 2016**, and then click **Skype for Business 2016**.
2. On the Welcome – Skype for Business page, click the **Skip for now** option.
3. In the Skype for Business window (see Figure 4-30), in the Sign-in address text box, type your Office 365 login email address and then click **Sign in**.

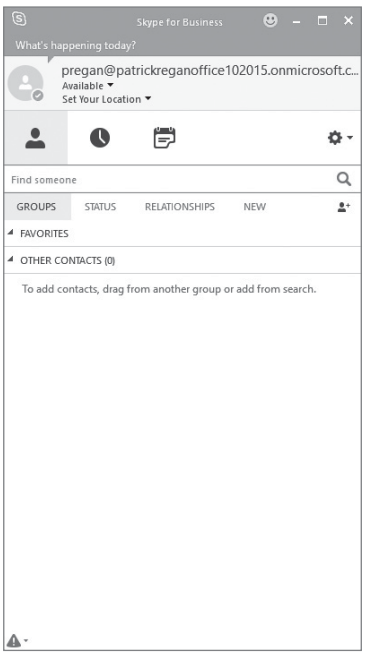
Figure 4-30
Logging into Skype for Business



4. When prompted for a password, type the password in the Password text box and then click **Sign in**. If you want to save your password, click **Yes** when you are prompted to save your Skype for Business sign-in information so that it will sign in automatically.
5. When it you are prompted to confirm whether you want to collect information to improve Skype for Business, click **No**. Skype for Business should look similar to Figure 4-31.

Figure 4-31

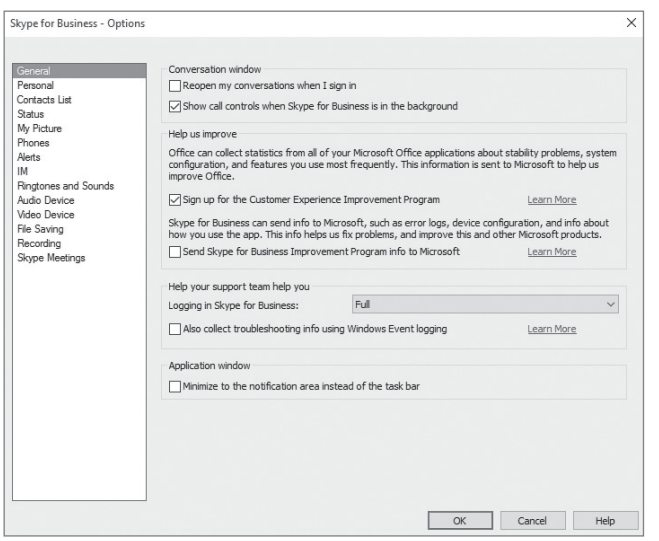
Using Skype for Business



6. Click the **Settings** button (Gear button) and then click **Tools > Options**.
7. On the Skype for Business – Options page (see Figure 4-32), click the **Personal** tab.

Figure 4-32

Configuring Skype for Business



8. To modify the sign-in address, update the address in the Sign-in address text box.
9. Click the **My Picture** tab. If you want to add a picture of yourself for other users to see, click the **Edit or Remove Picture** button. When Office 365 Outlook opens in a

browser, you can then click the folder icon to open a window that can be used to browse to a picture. When done, click the **Save** button and close the browser.

10. To change the ringtones and sounds, click the **Ringtones and Sounds** tab.
11. To change the sound settings, click the **Sound Settings** button, which opens the Control Panel Sound dialog box and displays the Sounds tab.
12. If you need to configure Skype for Business to use a microphone, click the **Audio Device** tab.
13. To configure Skype for Business to use a camera, click the **Video Device** tab.
14. Click **OK** to close the Skype for Business – Options page.

■ Configuring Microsoft Intune

THE BOTTOM LINE

Microsoft Intune is a cloud-based management solution that allows you to manage your computers when they are not inside your corporate network. Microsoft Intune helps you manage your computers and mobile devices through a web console. It provides the tools, reports, and licenses to ensure your computers are always current and protected. For mobile devices, it also allows you to manage your remote workforce by working through ActiveSync or directly through Microsoft Intune.

CERTIFICATION READY
Configure Microsoft Intune
4.4

Microsoft Intune can be operated in cloud-only mode or in a new unified configuration option that integrates the cloud-based environment with Microsoft System Center 2012 Configuration Manager Service Pack 1 or higher. Microsoft Intune utilizes a subscription model in which you are charged on a per-user basis.

Because Microsoft Intune is a cloud service, you do not have to set up and maintain a server infrastructure to use it. You need only a Microsoft Intune subscription.

Microsoft Intune is composed of two components:

- A web-based administrative console.
- Microsoft Intune client software that is downloaded from the Microsoft Intune account administration website using the Windows Live ID and password associated with your Microsoft Intune account.

You can deploy the client software manually and have the target computer navigate to the shared folder and launch the installation, or you can deploy it using software programs such as Group Policy or System Center Configuration Manager (SCCM). ***Group Policy*** is a Windows technology that can be used to configure a computer running Windows, including installing software. Microsoft ***System Center Configuration Manager*** is a software package that offers software installation, software updates, and hardware and software inventory.

After the software is installed on the client, it reports its status to the cloud service from anywhere there is an Internet connection. You can then manage Intune clients using the Microsoft Intune Admin Console (see Figure 4-33), which is accessed via a browser that supports ***Microsoft Silverlight***. Microsoft Silverlight is a free web-browser plug-in that is designed to provide rich Internet applications and media experiences on the web.

From the Microsoft Intune Admin Console, you can perform the following security and management tasks:

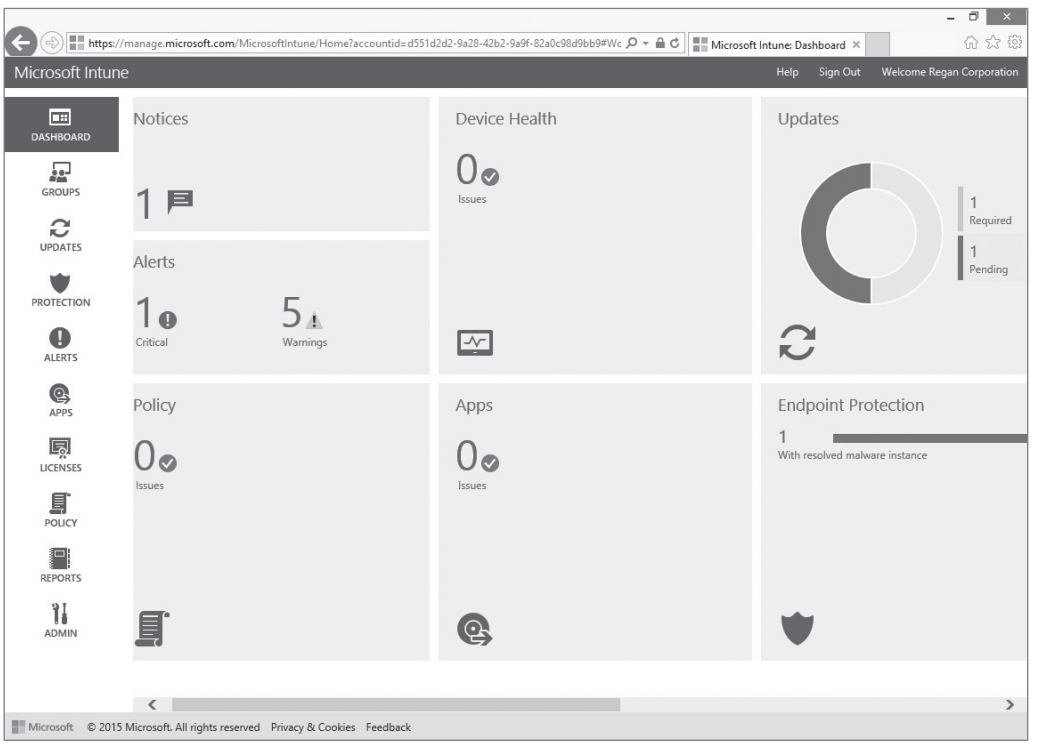
- You can protect your computers from malware.
- You can deploy licensed software (Microsoft Office or third-party applications) to PCs.

- You can manage the deployment of software updates to Microsoft and most third-party software publishers from a central location.
- You can receive updates/alerts from the PCs on your network.
- You can provide remote assistance and perform remote tasks.
- You can track hardware and software inventory.
- You can manage software licenses.
- You can run software update reports, detected software reports, computer inventory reports, and license purchase and installation reports.

TAKE NOTE* To make full use of Microsoft Intune, clients must have the Microsoft Intune client software installed (as you learned in Lesson 3).

Figure 4-33

Accessing the Microsoft Intune Admin Console



TAKE NOTE* The Configure Microsoft Intune exam objective also covers creating and deploying policies and setting up notifications. Creating and deploying policies are covered in Lesson 3. Setting up notifications is also covered in Lesson 3.

Automating Installs

When deploying software using Microsoft Intune, there are two types of installations. The first is a required install that automatically installs or pushes the software to the managed computer and requires no user interaction. The second is an available install that publishes the software to the Company Portal or on the mobile Company Portal so your users can install the software themselves.

The software you upload is stored in the Microsoft Intune cloud storage that your organization purchased. To deploy software, access the Software workspace.

The following steps provide an overview of the process for publishing and updating software:

1. **Prepare your software files.** The .msi or .exe file must be placed in a single folder along with any supporting files on the administrator's computer.
2. **Configure and upload the package.** This requires you to type the path to the setup files, the name of the software publisher, the name of the software being deployed, a description, the required architecture (32- or 64-bit), and which operating systems the package will be installed on.

   You also set the detection rule (for example, look for a specific file, registry entry, or MSI product code) to see if the software is already installed when deploying an updated package. After configuration is completed, the file is compressed, encrypted, and uploaded to the Windows Azure storage platform. After it is uploaded, you see the application in the Managed Software workspace.
3. **Deploy the package.** Within the Managed Software workspace, click the package to deploy and select the group to deploy the software package to. The package is now ready for your users.
4. **Client download/installations.** If the client meets all the configuration requirements you set in Step 2, it downloads the package to a temporary folder and begins the silent installation. (The client is configured via a policy to check for new downloads every 8 hours.)
5. **Monitor the deployment status.** To view the progress of installations across your managed computers, you can use the administrative console.

For many applications, the manufacturer includes options to automatically check for updates directly from the client computer. If you want Microsoft Intune to manage this process, you have to disable the manufacturer's feature on each of the managed computers.

Sideloading and Deeplinking Software

There are several ways in which you can install applications using Microsoft Intune. ***Sideloading*** is the process of installing Windows Store applications without using the Windows Store. ***Deeplinking*** identifies an application in the Windows Store by providing a link that will take the user directly to the app in the Windows Store.

If you have access to the app installation files, you can sideload with Microsoft Intune. However, the application can only be deployed after the operating system is deployed. When you sideload an application, you can deploy an app to all Windows accounts on a device or to a specific Windows account on a device.

You can use Microsoft Intune only or integrate Microsoft Intune with Configuration Manager. When using Configuration Manager, you have to install the Microsoft Intune connector. Before you can deploy or sideload your application to Microsoft Intune-managed devices, you need to upload the application into Microsoft Intune.

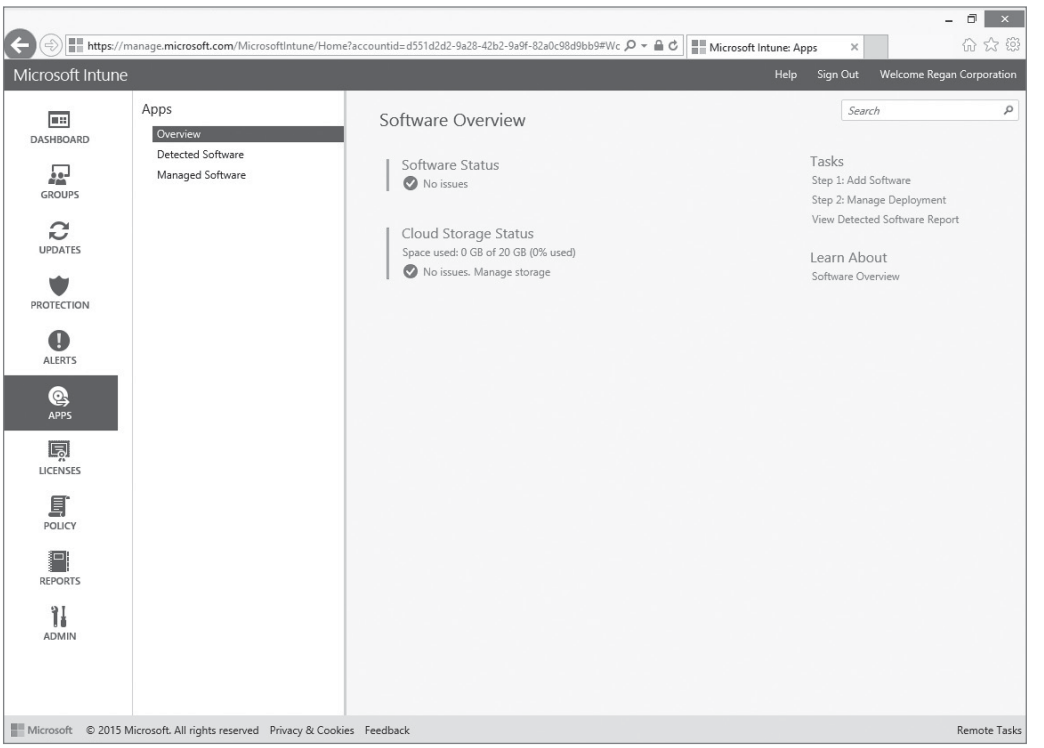
UPLOAD A WINDOWS STORE APP USING MICROSOFT INTUNE

GET READY. To upload a Windows Store app using Microsoft Intune, perform the following steps.

1. Log in to the Microsoft Intune website (https://manage.microsoft.com), click **Admin Console**, and then click the **Apps** workspace.
2. Under Tasks (see Figure 4-34), click **Step 1: Add Software**. If you are prompted to confirm that you want to run Microsoft Intune Software Publisher, click **Run**. If you are asked to sign in, log in with an administrator account for Intune.

Figure 4-34

Managing software with Microsoft Intune



3. In the Add Software Wizard, on the Before you begin page, click **Next**.
4. On the Software setup page, for the Select the software installer file type option, select the Windows app package software installer type. Then in the Specify the location of the software setup files text box, type the local (such as C:\Software\app.exe) or Universal Naming Convention (UNC) path (\\server01\software\app.exe) to the application and then click **Next**.
5. On the Software description page, in the Publisher, Name and Description text boxes, type the publisher, user-friendly name, and description of the application.
6. In the URL for software information text box, you type a URL where more information about the application can be found. Lastly, you can select the category of the software and upload a picture of the software. Click **Next**.
7. On the Requirements page, for the Architecture is option, choose the architecture (32-bit and/or 64-bit). For the Operating System option, select the appropriate operating system. (The default is Any for both options.) Click **Next**.
8. On the Detection Rules page, choose the rules to detect whether the software is already installed by selecting **Detect whether the software is installed by using the following rules (recommended)**. Click the **Add Rule** option and then select one or more of the following options:

   File exists

   MSI product code exists

   Registry key exists
9. Based on the option selected, specify the file, MSI product code, or the registry key in the appropriate text boxes. Click **Next**.
10. On the Command line arguments page, click **Next**.
11. On the Return codes page, click **Next**.
12. On the Summary page, click **Upload**.
13. When the software is uploaded, click **Close**.

After the application is uploaded into Microsoft Intune, you can deploy the application to Microsoft Intune groups, which can contain users or devices that Microsoft Intune manages.

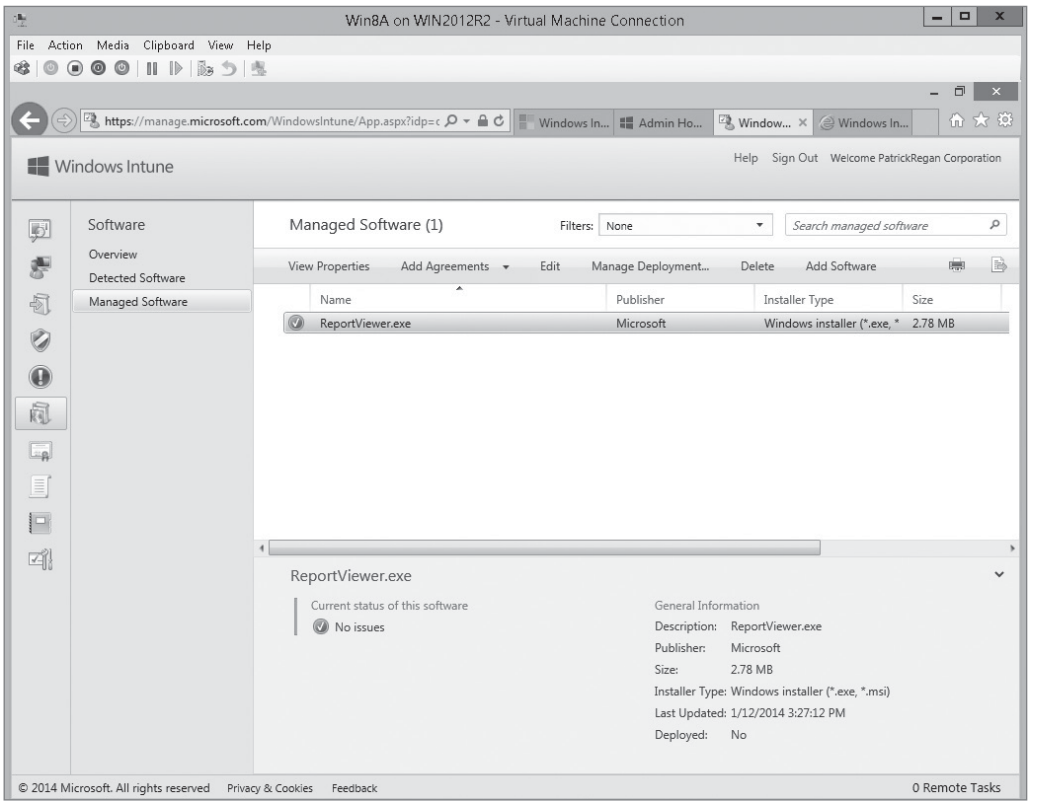
SIDELOAD A WINDOWS STORE APP USING MICROSOFT INTUNE

GET READY. To sideload a Windows Store app using Microsoft Intune, perform the following steps.

1. Log in to the Microsoft Intune website (https://manage.microsoft.com), click **Admin Console**, and then click the **App** workspace.
2. Click **Managed Software** (see Figure 4-35).

Figure 4-35

Managing software with Microsoft Intune



3. Click **Manage Deployment**.
4. In the Deploy Software Wizard, on the Select Groups page, click the group to which you want to deploy and then click **Add**. Click **Next**.
5. On the Deployment Action page, under Approval, select **Required Install** from the pull-down menu.
6. Click **Finish**.

With deeplinking, you can identify an application in the Windows Store that you want to deploy to Windows 10; a link will be provided to the user that will take them directly to the app in the Windows Store. By using deeplinking, the user will not potentially load the wrong app.

To deeplink an application, you must know the URL of the application. You will run the Add Software Wizard to specify the URL from which users can install the application. You will then use the Manage Software task to deploy the application to the users.

DEEPLINK A WINDOWS STORE APP USING MICROSOFT INTUNE

GET READY. To deeplink a Windows Store app using Microsoft Intune, perform the following steps.

1. Log in to the Microsoft Intune website (https://manage.microsoft.com), click **Admin Console**, and then click the **Software** workspace.
2. Under Tasks, click **Step 1: Add Software**. If you are prompted to confirm that you want to run this Microsoft Intune Software Publisher, click **Run**. If you are prompted to sign in, log in with an administrator account for Intune.
3. In the Add Software Wizard, on the Before you begin page, click **Next**.
4. For the Select how this software is made available to devices option, select **External link**. In the Specify the URL text box, type the URL of the application and then click **Next**.
5. On the Software description page, in the Publisher, Name and Description text boxes, type the publisher, user-friendly name, and description of the application.
6. On the Summary page, click **Upload**.
7. When the software is uploaded, click **Close**.

Identifying Software and Hardware Requirements

Understanding software and hardware assets can aid in the planning and deployment process of new software and hardware across your organization. Managing your assets means knowing what software and hardware your organization has.

You can use a software inventory to effectively manage the software and licenses used in your organization. This provides the following information:

- The types of software installed on computers
- The number of copies installed
- The version of software installed
- The publisher
- The category of software

Figure 4-36 shows an example of software information collected from a single Windows 10 virtual machine that runs the Microsoft Intune agent. This was accessed in the Groups workspace for a Windows 10 computer. From here, you can view the information, print it out, or export it to a CSV or HTML file for further analysis.

You can also run a Detected Software Report from the Reports workspace to view software installed on computers across your organization. To further refine the report, you can select only software that meets selected criteria (device group, publisher, and/or category). Categories can include browsers, multimedia and file viewers, and operating system and components.

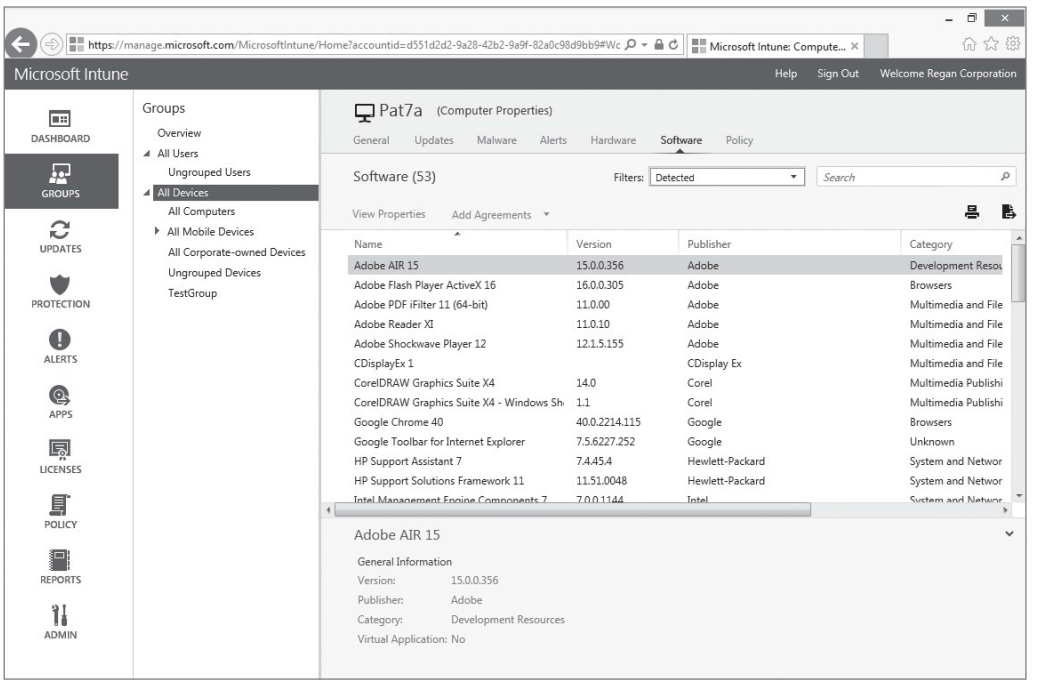
CREATE A DETECTED SOFTWARE REPORT

GET READY. To create a Detected Software Report, perform the following steps.

1. Log in to the Microsoft Intune website (https://manage.microsoft.com) and then open the **Microsoft Intune Admin Console**.
2. In the left pane, click **Reports > Detected Software Reports**.
3. Under Select publishers, click **Edit**.

Figure 4-36

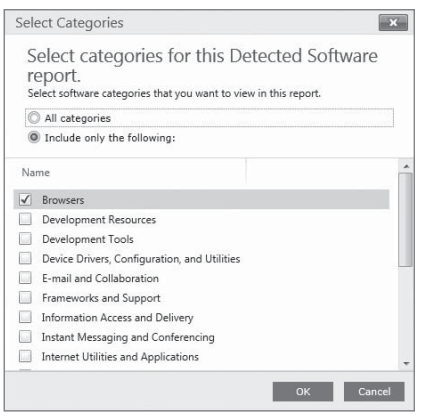
Collecting software information with the Microsoft Intune agent



4. Select **Include only the following**, choose **Microsoft**, and then click **OK**.
5. Under Select categories, click **Edit**.
6. Select **Include only the following**, select **Browsers** (see Figure 4-37) and **Operating System and Components**, and then click **OK**.

Figure 4-37

Creating a Detected Software Report



7. Click **View Report**.
8. Move your mouse over the icon in the upper-right corner and then click **Export**.
9. On the Select the export format for your data page, click the **down arrow** and choose **.html**. Click **Export**.
10. Choose **Desktop** as the location to save your file to and then type **MyWin10Report**.
11. Click **Close**.
12. Open the file and view the report you created. Close it when you are done.

Reviewing Hardware Assets

In addition to tracking the software used on managed computers, Microsoft Intune also collects hardware information from the agent. This happens automatically or on a customizable schedule and the process is entirely invisible to the end user.

There are several benefits to collecting an asset inventory in your organization. They include the ability to:

- Assess whether or not you are maintaining corporate hardware standards (such as processor and memory).
- Track asset depreciation.
- Locate and troubleshoot computers in large organizations.
- Provide information about what computers need an operating system upgrade.
- Provide information about which computers can support a software package.
- Identify computers with common hardware characteristics to aid in deployment of software.

The following information can be collected and reported on both mobile devices and managed computers:

- Operating systems
- Manufacturers
- Models
- Chassis types
- Available disk space
- Physical memory
- CPU speed

TAKE NOTE*

You can run a Computer Inventory Report from the Reports workspace to view hardware installed on computers across your organization. To further refine the report, you can select only computers and devices that meet selected criteria (operating system, model, chassis type, CPU speed, and so on).

Figure 4-38 shows an example of hardware information collected from a single Windows 10 virtual machine running the Microsoft Intune agent. This was accessed via Groups > All Devices > Hardware for a Windows 10 computer.

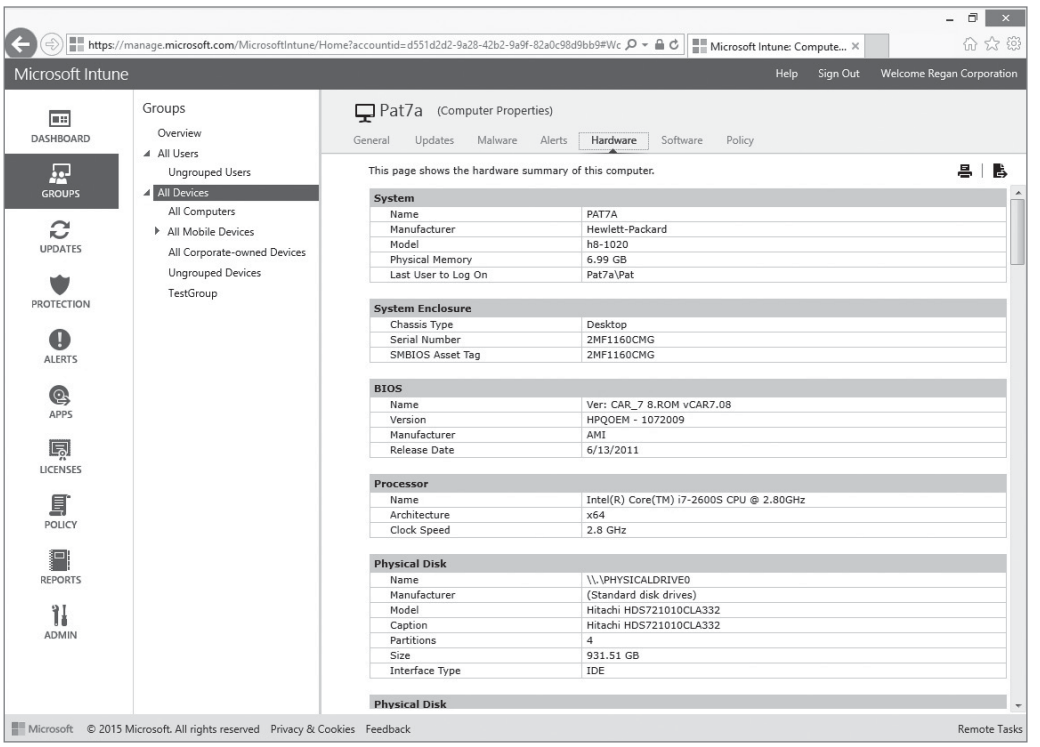
From here, you can view the information, print it, or export it to a CSV or HTML file for further analysis.

The information provided is organized according to the following sections in the report:

- **System:** Name, Manufacturer, Model, Physical memory, Last User to log on
- **System Enclosure:** Chassis type, Serial Number SMBIOS Asset Tag
- **BIOS:** Name, Version, Manufacturer, Release Date
- **Processor:** Name, Architecture, Clock Speed
- **Physical Disk:** Name, Manufacturer Model, Caption, Partitions, Size, interface type
- **Logical Disks:** Name, Drive Type

Figure 4-38

Collecting computer hardware information



- **Network Adapter:** Name, Manufacturer, Product Name, MAC Address, Speed, Connection Status
- **Network Adapter Configuration:** DHCP enabled, DHCP Server address, IP address, leaser information, IP address information, IPSec status
- **Video Controller:** Description, Drive Date, model
- **Monitor:** Name, Manufacturer, Pixels per inch, screen height/width
- **Printers:** Name, Share status, local/network, driver name
- **Physical Memory:** Capacity

CREATE A COMPUTER INVENTORY REPORT

GET READY. To create a Computer Inventory Report, perform the following steps.

1. Log in to the Microsoft Intune website (https://manage.microsoft.com).
2. In the left pane, click **Reports** > **Computer Inventory Reports**.
3. Under Select operating systems, click **Edit**.
4. Select **Include only the following**, choose **Windows 10**, and then click **OK**.
5. Click **View Report**.
6. Move your mouse over the icon in the upper-right corner and then click **Export**.
7. On the Select the export format for your data page, click the **down arrow** and choose **.html**. Click **Export**.
8. Choose **Desktop** as the location to save your file to and then type **MyWin10InvRpt**.
9. Click **Close**.
10. Open the file and view the report you created. Close it when you are done.

Managing Updates by Using Microsoft Intune

In Microsoft Intune, updates are managed via the Updates node in the Admin workspace. When you are in the Updates node, you can view any pending updates, approve or decline updates, configure the automatic approval settings, and set the deadline for update installation in automatic approval rules. From the workspace, you can approve not only Microsoft updates but also non-Microsoft updates.

When working with updates, not all of them are applicable to your situation. To help streamline the process of managing updates, Microsoft Intune distinguishes the updates according to their respective product categories and update classifications. Product categories are used to organize software by product name; update classifications are arranged according the specific type of update (service pack, critical update, or definition update). Microsoft Intune checks for updates only on the products and update classifications you select.

TAKE NOTE* Use the Admin workspace Updates node to configure which updates will be made available and to configure the automatic approval rules. Use the Updates workspace to manage the available updates, including approving and deploying those updates.

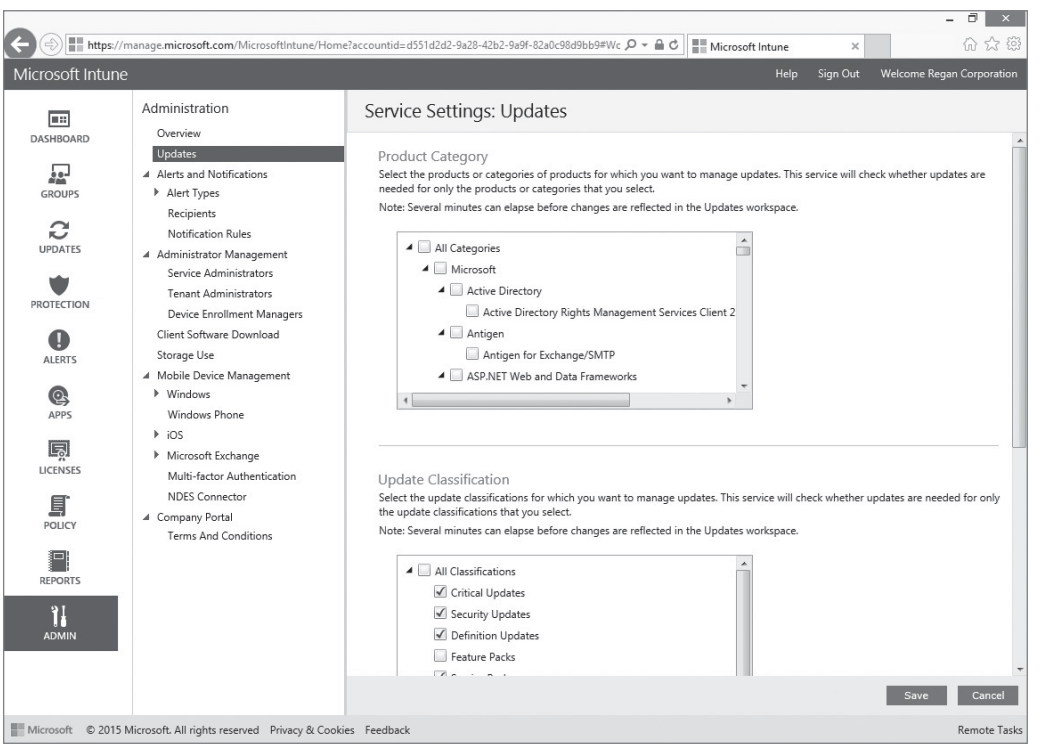
REVIEW PRODUCT CATEGORIES AND CLASSIFICATIONS

GET READY. To review product categories and classifications, perform the following steps.

1. Log in to the **Microsoft Intune Admin Console** at https://manage.microsoft.com.
2. In the left pane, click **Admin**.
3. Click **Updates** (see Figure 4-39).

Figure 4-39

Reviewing product categories and update classifications



4. Review the product categories that you can filter on and then review the update classifications you can filter on.
5. Scroll down to the bottom until you see the Automatic Approval Rules section.

UNDERSTANDING AUTOMATIC UPDATE APPROVAL RULES

Creating ***Automatic Update Approval rules*** can help streamline the management of your computers by specifying which updates will automatically be approved. For example, you can create a rule so that Microsoft Intune automatically approves the installation of all critical and security updates as soon as Microsoft releases them. This ensures your clients are updated as soon as possible.

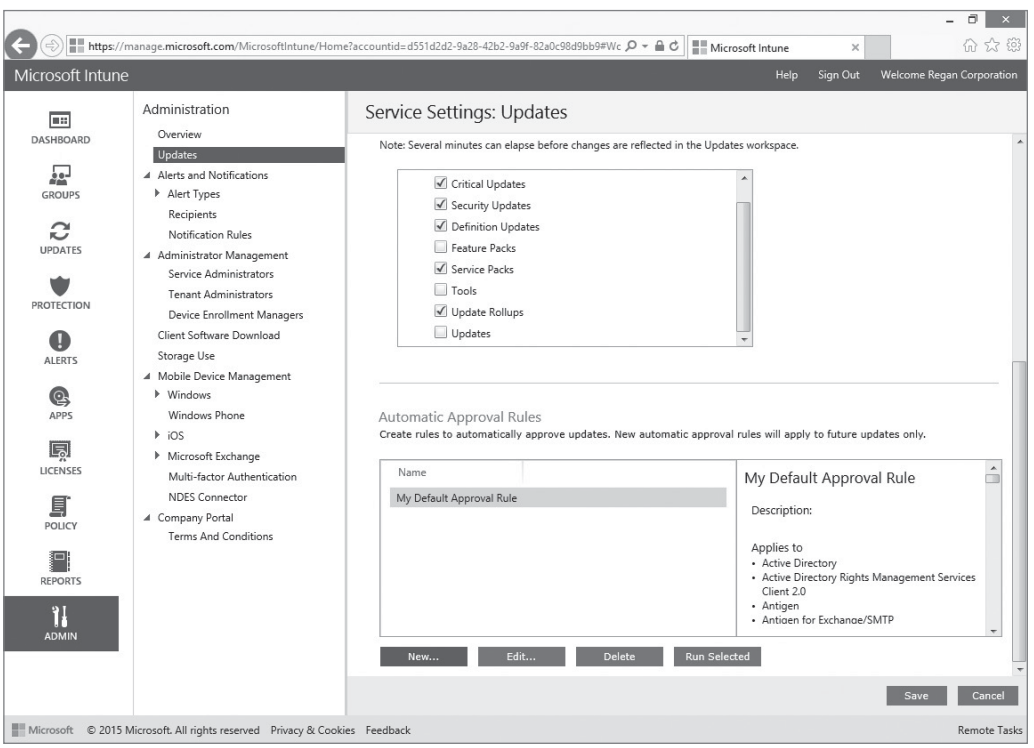
CREATE AN AUTOMATIC UPDATE APPROVAL RULE

GET READY. To create an Automatic Update Approval rule, perform the following steps.

1. Log in to the **Microsoft Intune Admin Console** at https://manage.microsoft.com.
2. In the left pane, click **Admin**.
3. Click **Updates**.
4. Scroll down until you see Select Automatic Approval Rules and then click **New**.
5. In the Name field, type **My Default Approval Rule** and then click **Next**.
6. Select **All Categories** and then click **Next**.
7. Under All Classifications, select **Critical Updates** and select **Security Updates** and then click **Next**.
8. Choose **Test Group** and then click **Add**. Click **Next** to continue.
9. Review the information summary and then click **Finish**.
10. Confirm your new rule appears under the Automatic Approval Rules section (see Figure 4-40).

Figure 4-40

Confirming your Automatic Update approval rule



TAKE NOTE*

The frequency an agent checks for updates is configured via the Policy workspace. The recommended setting is 8 hours, but you can set the frequency to occur between 8 hours and 22 hours.

11. Click **Run Selected** and then click **Save.**

    This step forces the rule to evaluate updates on all computers that run Microsoft Intune agents in the group you specified. After the review, the updates are made available to the computers in the group when they next check in. By default, the Microsoft Intune agent checks in every eight hours for updates. When updates are available, Microsoft Intune installs the updates. If you click Save, the rule applies only to future updates as they are released.
12. In the left pane, click **Updates**.
13. View the status of the updates.

APPROVING UPDATES MANUALLY

TAKE NOTE*

To select multiple groups, you can use the Ctrl or Shift key when selecting the updates to approve.

You might want to review and manage some updates before approving and deploying them. In these situations, you should perform a manual update from the Updates workspace.

In Microsoft Intune, you can manage updates from Microsoft and from third parties. Microsoft updates are included in the Microsoft Intune Admin Console; third-party updates require additional setup. When approving a Microsoft update, you can approve it for a single group or for multiple groups. To approve an update for multiple groups, you can take advantage of the parent and child group hierarchy. For example, you can approve the update for the All Computers group and its child groups will receive the updates via inheritance.

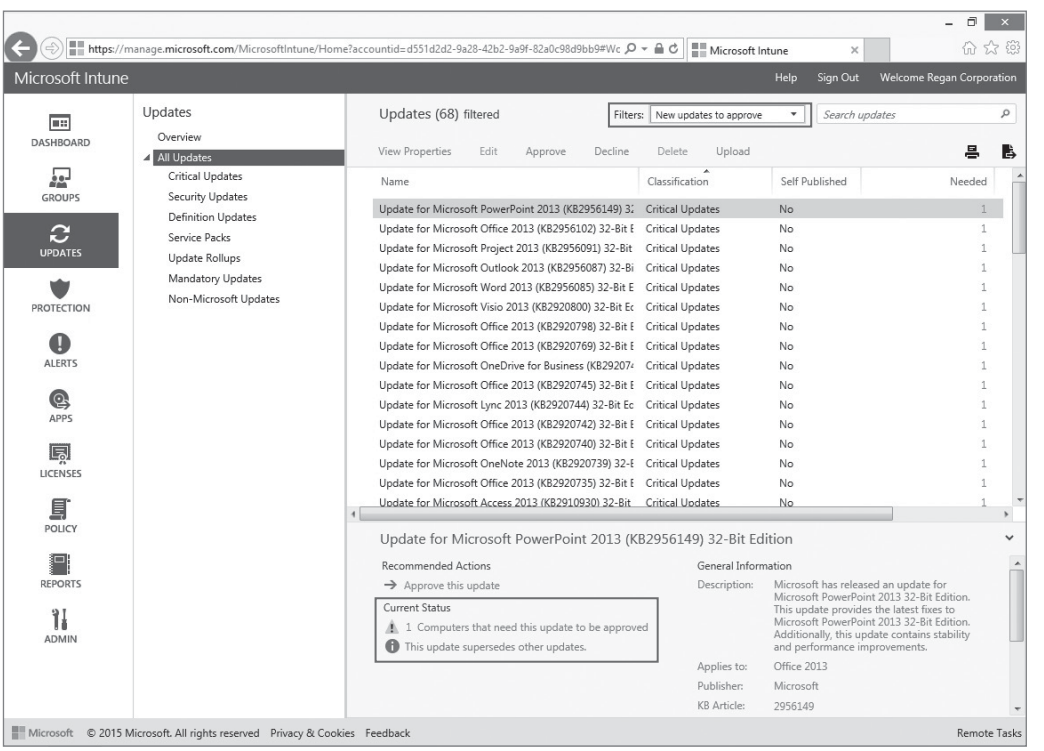
APPROVE AN UPDATE MANUALLY

GET READY. To approve an update manually, perform the following steps.

1. Log in to the **Microsoft Intune Admin Console** at https://manage.microsoft.com.
2. In the left pane, click **Updates**.
3. In the Filters drop down, click **New updates to approve** (see Figure 4-41).

Figure 4-41

Viewing the updates to approve



4. Click one of the updates and review additional information about it.

   By clicking on the name of the update, you can see how many computers need that specific update. By clicking the **Computers that need this update to be approved** link under Current status, you can see the name of the actual computer the update is applied to.
5. Choose one the updates and then click **Approve**.
6. On the Select the groups to which you want to deploy this update page, choose **My Test Group** and then click **Add**.
7. Click **Next**.
8. Under Approval, click **Finish**. Review the message at the bottom of the page for additional information regarding the updates.
9. Click **Finish**.

DECLINING UPDATES

In the previous sections, you learned the process for approving updates either manually or automatically via the Automatic Approval rules. You can also decline updates.

When you decline an update:

- All approvals for the update are removed.
- The update is hidden in default views in the Update console.
- Any associated reported data is lost.

DECLINE AN UPDATE

GET READY. To decline an update, perform the following steps.

1. Log in to the **Microsoft Intune Admin Console** at https://manage.microsoft.com.
2. In the left pane, click **Updates**.
3. Under Update Status, click **New updates to approve**.
4. Choose the update and review its description.
5. Right-click the update and choose **Decline**.
6. After reading the warning prompt, click **Decline**.

SUMMARY SKILL MATRIX

IN THIS LESSON YOU LEARNED:

- For most organization, email is the most popular form of communications when conducting business. The advantage of using Exchange Online and Outlook Online is that there is very little configuration necessary.
- A recipient is the identity used in Exchange Online that is used to identify users and resources that can send and receive messages. It is a mail-enabled object in Active Directory to which Exchange can deliver or route messages.
- If you have been working with supporting computers even for only a short while, you should know that viruses and spam are a threat to any computer or corporation. In fact, the number of viruses and spam have been growing significantly each year.
- Office 365 has several tools that minimize the amount of unwanted messages that reach a user's mailbox while providing a strong defense against malicious software.

- SharePoint is a popular web platform developed by Microsoft that offers a powerful, flexible, and scalable centralized web application. Although SharePoint looks like a typical website, it's actually a web content management system, a document management system, and a collaboration tool.
- A site collection is a grouping of sites. Every site collection has a single root site, under which the other sites are built. All sites within the site collection have the same site owners and share the same administrative settings.
- The Sharing option on the site collection page allows you to share the site collection with users outside your organization. This can be done through invitations or by providing anonymous guest links.
- Themes define SharePoint site color schemes, including those that are applied to menus, system pages, the ribbon, and so forth. Choose a color scheme that complements your company's website.
- OneDrive, formerly named SkyDrive, is a file-hosting service that allows you to create and store files and folders and then share them with other users and groups.
- Skype is a telecommunications application that provides video calls and voice-only calls from computers, tablets, and mobile devices to other devices or telephones/smartphones using an Internet connection. Skype also allow users to send instant messages, files, images, and videos.
- The enterprise edition of Skype is Skype for Business, which replaced Microsoft Office Communicator, Microsoft Lync, and Windows Messenger used with Microsoft Exchange Server. Microsoft offers an online version of Skype with Office 365 called Skype for Business Online.
- Microsoft Intune is a cloud-based management solution that allows you to manage your computers when they are not inside your corporate network. Microsoft Intune helps you manage your computers and mobile devices through a web console.

■ Knowledge Assessment

Fill in the Blank

Complete the following sentences by writing the correct word or words in the blanks provided.

1. Mailboxes, resources, contacts and groups are examples of _____.
2. A _____ is a mailbox that is associated with one or more users and is assigned an external email address.
3. Smartphones and tablets can connect to Exchange Online to get emails using an email application by using _____.
4. When a smartphone that that retrieves email from Exchange Online is stolen, you can perform a _____ command to remove corporate and user information stored on the device.
5. Viruses, spyware, rootkits and Trojan horses are examples of _____.
6. In SharePoint, a _____ is a grouping of sites that have the same site owner and share the same administrative settings.
7. A _____ allows users to stay in tune with conversations between groups of people and to see updates about their activities.
8. A _____ defines the color schemes of a SharePoint site.

9. To simplify access to your OneDrive storage area on your computer running Windows 10, you should use the _____.
10. _____ enables users to use instant messaging with coworkers.

Multiple Choice

Circle the letter that corresponds to the best answer.

1. In Office 365, which of the following is a shared workspace for email, conversations, files, and calendar events?
   a. A security group
   b. A distribution group
   c. An Office 365 group
   d. A dynamic distribution group
2. Which of the following SCL levels have emails that are scanned and found on Exchange Online to be cleaned?
   a. –1
   b. 1
   c. 6
   d. 0
3. You notice that a lot of spam is coming from a specific IP address. Which of the following actions blocks those spam messages on Exchange Online?
   a. Configuring a new malware detection rule and policy
   b. Configuring Intune Endpoint Protection
   c. Configuring a content filter
   d. Configuring a connection filter
4. Which of the following is offered by Office 365 as an upgrade to newsfeeds?
   a. Social interaction
   b. OWA
   c. SharePoint
   d. Yammer
5. When you share a SharePoint site in Office 365, which methods can be used to share the site content? (Choose all that apply)
   a. You can share the whole site by sending invites to sign in with a Microsoft Account or an Office 365 user ID.
   b. You can share individual documents by sending them an anonymous guest link.
   c. You can share individual documents with external users by sending invites to sign in with a Microsoft Account or an Office 365 user ID.
   d. You can configure a VPN tunnel to the SharePoint site.
6. If you have 100 users, which of the following is the default allocated storage space for SharePoint Online?
   a. 20 GB
   b. 50 GB
   c. 60 GB
   d. 100 GB
7. Which browsers can be used when you are using Skype for Business through an authenticating HTTP proxy? (Choose all that apply)
   a. Internet Explorer 7
   b. Internet Explorer 8
   c. Internet Explorer 11
   d. The latest version of Mozilla Firefox

8. With Microsoft Intune, which of the following is used to install a Windows Store application without using the Windows Store?
   a. sideloading
   b. deeplinking
   c. StoreByPass
   d. StoreProxy

9. Multiple users are working from their home offices and thus are often not connected to the corporate network. Which of the following can be used to ensure that their computers have the necessary security updates from Microsoft?
   a. You can install Office 365 Updates.
   b. You can configure Windows to perform a Push Update from an internal Windows Update Server.
   c. You can use VPN Updates.
   d. You can use the Microsoft Intune Update feature.

10. Which of the following is a feature of Microsoft Intune that is considered more effective than automatically installing updates using Windows Updates?
    a. Microsoft Intune is faster than Windows Updates.
    b. Only important updates are available through Windows Updates.
    c. Only Level-2 tested updates are available through Microsoft Intune.
    d. Microsoft Intune provides you with an opportunity to test the updates before pushing them to the clients.

True / False

Circle T if the statement is true or F if the statement is false.

T | **F** **1.** After you create a shared mailbox, you need to change the password to Null.

T | **F** **2.** If you are not a member of an Office 365 private group, you cannot send emails to the private group.

T | **F** **3.** By default, when email is identified as spam based on the SCL value, that email is sent to the junk email folder.

T | **F** **4.** When you want to have a conference with a project team, you can share the SharePoint site and use it as a virtual whiteboard.

T | **F** **5.** When installing applications, deeplinking is the most efficient method to install software automatically.

■ Case Projects

Scenario 4-1: Fighting Spam

You are an administrator for the Contoso Corporation and you are now using the Exchange Online system for your email. Since you have changed to the Exchange Online, you have seen an increase of spam. Describe the steps you can take to reduce spam.

Scenario 4-2: Collaborating on a Project

You are an administrator for the Contoso Corporation and you have just deployed Office 365 to your 800 users using E4 licensing, which will provide Word Online, Excel Online, PowerPoint Online, Outlook Online, OneNote Online, Publisher Online, Access Online, and Skype. You are tasked with creating a collaboration solution for a large project that will consist of two partner

companies and will require the sharing of documents, the sending of emails, and the hosting of virtual meetings. Describe the solution you would recommend.

Scenario 4-3: Protecting Your Systems from Malware

You are an administrator for the Contoso Corporation and some of your users work from their home offices instead of working at a corporate site. You decide to use Microsoft Intune to manage the systems those users access. Describe the steps you should take to ensure that these systems are free from malware.

Scenario 4-4: Securing Smartphones

You are an administrator for the Contoso Corporation and you have just deployed Office 365 to your 800 users. About one-third of your users use smartphones that are configured to get email via ActiveSync. You need to ensure that users keep their phones secured by passwords on their phone. You also need to devise a strategy for protecting sensitive data when a phone is lost or stolen. Describe your proposed solution.

5

LESSON

Supporting Cloud Users

OBJECTIVE DOMAIN MATRIX

Technology Skill	Objective Domain Description	Objective Domain Number
Resolving Issues with Installing Office Applications and Signing In • Troubleshooting Connectivity Issues • Troubleshooting Sign-In Issues and Forgotten Passwords • Troubleshooting Issues with Activating Office Applications • Troubleshooting Difficulty Connecting Mobile Devices to Office 365 and Microsoft Intune • Choosing Between 32-bit and 64-bit Architectures • Identifying System Requirements for Office 365 ProPlus • Using Office Repair	Resolve sign-in and Office application installation issues	5.1
Resolving Issues with Emails and Calendars • Troubleshooting Issues with Sending and Receiving Email • Troubleshooting Issues with Accessing a Delegated Mailbox	Resolve email and calendar issues	5.2
Resolving Issues with SharePoint and OneDrive • Identifying SharePoint Storage Limits • Resolving Issues with Open with Explorer • Resolving Issues with OneDrive Sync • Recovering Deleted Files	Resolve SharePoint and OneDrive issues	5.3
Resolving Issues with Skype for Business Online	Resolve Skype for Business Online issues	5.4

KEY TERMS

add-in
autodiscover
End User Recycle Bin
ipconfig command
Microsoft Office Diagnostic Tools
Microsoft Online Services Sign-In (MOS SIA) Assistant
network address translation (NAT)
nslookup.exe
pathping command
ping command
proxy server
SharePoint recycle bin
Site Collection Recycle Bin
tracert command

Contoso Corporation is ready to implement Office 365 to all users. You need to prepare your helpdesk personnel so that they can support users when they encounter problems. You should also consider setting up training for users because Office 365 will be new to most of them.

■ Resolving Issues with Installing Office Applications and Signing In

THE BOTTOM LINE

The first type of problem that you will encounter will involve users trying to log in to the cloud portal or application. Any time that you transition from local applications to cloud-based applications, there is an initial learning curve for users. So be prepared for a temporary increase in demand for help from users when you implement cloud services. Of course, proper training will help alleviate these issues.

CERTIFICATION READY
Resolve sign-in and Office application installation issues
5.1

When dealing with sign-in problems, you must make sure that users have the correct IP configuration (including IP address, subnet mask, default gateway, and DNS server. In addition, make sure users have Internet access.

Next, make sure users are logging into the correct website. They should be logging into the following sites:

- If a user is using a personal Microsoft Office 365 account, he should use https://outlook.com, https://onedrive.com or https://office.com. The email address used to log in should be a personal email, such as an outlook.com, Hotmail.com, or Gmail account.
- If a user is using a work or school Office 365 account, she should be using https://portal.office.com. The email address used to log in should include the organization's name, such as @contoso.onmicrosoft.com.
- If your organization has deployed Intune, users should be using https://manage.microsoft.com.
- To access the Microsoft Intune Company Portal, users should be using https://portal.manage.microsoft.com.

Troubleshooting Connectivity Issues

Connectivity issues are defined as any problem whereby users cannot access the cloud portal or cloud application. When dealing with connection problems, use basic troubleshooting models and tools to determine the scope of the problem. If only one user is experiencing the problem, the problem is most likely a result of the settings on his computer. Problems will usually be caused by network connectivity, proxy settings, or firewalls.

If you experience network connectivity problems while using Windows 10, use Window Network Diagnostics to begin the troubleshooting process. If there is a problem, Windows Network Diagnostics analyzes the problem and, if possible, presents a solution or a list of possible causes. To run the Windows Network Diagnostics program, right-click the Network and Sharing Center icon in the notification area and choose Troubleshoot problems. You can also right-click the adapter under Network Connections and choose Diagnose.

If the problem still exists, you can also use the following command-line tools:

- ipconfig
- ping
- tracert
- pathping
- netstat
- telnet
- nslookup

By default, all of the tools are available in Windows except telnet. If you want to use telnet, you have to install telnet using Programs and Features.

In addition, you can review the logs shown in Event Viewer. Some error messages might be found in the System and Application logs.

VERIFYING IP CONFIGURATIONS

When you cannot connect to a website or a server, you should first check the client IP configuration. This can be done by using Network Connections or the ipconfig command.

To view your network connections, open the Network Connections under the Network and Sharing Center and then click Status. The General tab reflect whether the adapter has IPv4 and IPv6 connectivity, whether the adapter is enabled, how long the adapter has been running, as well as the speed of the adapter. It will also show you the bytes being sent and received from the adapter. If you click the Details button, you can view the network connection details, including IP addresses, subnet mask, gateway, WINS and DNS servers, and physical/MAC address.

The ***ipconfig command***—one of the most useful commands when troubleshooting network problems—displays all current TCP/IP network configuration values and refreshes the Dynamic Host Configuration Protocol (DHCP) settings. If you execute ipconfig without any parameters (meaning that you type ipconfig at the command prompt and press the Enter key), ipconfig displays the IP address, subnet mask, and default gateway for all adapters. When you execute ipconfig /all, the full TCP/IP configuration for all adapters is displayed, including host name, DNS servers, and the physical/MAC address.

If you are using DHCP servers to assign addresses, ipconfig /renew will renew the DHCP configuration from the DHCP server. This parameter is available only on computers with adapters that are configured to obtain an IP address automatically. You can also use ipconfig /release to release the DHCP address from a network adapter.

If the IP address is invalid, communication might fail. If the subnet mask is incorrect, you might have problems communicating with local or remote hosts. If the default gateway is invalid, you will have problems communicating with remote hosts but you can still communicate with local hosts. If the DNS server is incorrect or missing, the computer might not be able to resolve names and thus communication might fail.

If a computer is configured to receive an IP address from a DHCP server and one does not respond, the computer will use the Automatic Private IP addressing, which generates an IP address in the form of 169.254.xxx.xxx and the subnet mask of 255.255.0.0. When you have an Automatic Private IP address, you can only communicate with computers on the same network/subnet that have an Automatic Private IP address. Therefore, you will most likely not be able to communicate with any host on the network without the proper IP address and subnet mask.

Assuming that you have the correct IP configuration, you need to determine whether you can communicate with the destination host. Windows 10 provides several tools to determine if you have network connectivity; if you don't have connectivity, Windows 10 helps you pinpoint where the failure is occurring.

An extremely valuable tool in troubleshooting is the ***ping command***, which verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) Echo Request messages. The receipt of corresponding Echo Reply messages are displayed along with round-trip times. Ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution. Because the ping command provides you with round-trip times, it can also tell you if the round-trip delay is slow between your host and the destination host.

To ping a host, execute ping followed by a host name or IP address. The ping command also supports the following parameters:

- **–t:** Specifies that ping will continue sending Echo Request messages to the destination until interrupted. To interrupt and display statistics, press Ctrl+Break. To interrupt and quit ping, press Ctrl+C.
- **–a:** Specifies that reverse name resolution is performed on the destination IP address. If this is successful, ping displays the corresponding host name.
- **–n *Count*:** Specifies the number of Echo Request messages sent. The default is 4.
- **–l *Size*:** Specifies the length, in bytes, of the data field in the Echo Request messages sent. The default is 32. The maximum size is 65,527.
- **–4:** Forces the command to ping the IPv4 address.
- **–6:** Forces the command to ping the IPv6 address.

A Request Timed Out response indicates that there is a known route to the destination computer but one or more computers or routers along the path–including the source and destination–are not configured correctly. Destination Host Unreachable indicates that the system cannot find a route to the destination system and therefore does not know where to send the packet on the next hop.

Two other useful commands are the ***tracert command*** and ***pathping command***. The tracert command traces the route that a packet takes to a destination and displays the series of IP routers that are used in delivering packets to the destination. If the packets are unable to be delivered to the destination, the tracert command displays the last router that successfully forwarded the packet. The tracert command also uses the ICMP protocol.

Pathping traces a route through the network in a manner similar to tracert. However, pathping also provides more detailed statistics on the individual hops.

TAKE NOTE* Since ICMP packets can be used in Denial of Service (DoS) attacks, some routers and firewalls block ICMP packets. Therefore, when you try to ping a host with the ping, tracert, or pathping command, it might not respond even though the host is connected.

To isolate network connectivity problems, use the following troubleshooting process:

1. Verify host IP configuration.
2. Use the ping command to gather more information on the extent of the problem:
    - Ping the destination address.
    - Ping the loopback address (127.0.0.1).
    - Ping a local IP address.
    - Ping a remote gateway.
    - Ping a remote computer.
3. Identify each hop (router) between two systems using the tracert or pathping command.

To determine whether you have a network connectivity problem, you should ping the destination by name or by IP address. If the ping command shows you have network connectivity, your problem is most likely with the host requesting the services; or, the services on the destination could be down. It should be noted that if you ping by name, you should verify that the correct address was used.

If you appear not have network connectivity to a server or service, you will need to isolate where the connectivity problem occurs, starting with the host computer. Therefore, you should ping the loopback address and local IP address to determine whether your TCP/IP components are functioning. Next, if you ping a local IP address, your results will demonstrate whether you can communicate on the local subnet that you are connected to. If you still have not found the problem, you can then ping the remote gateway (most likely your default gateway) to determine if you can communicate with the router. Next, pinging a remote computer determines whether you can communicate through your default gateway to a remote subnet. Finally, use the tracert and pathping commands to determine exactly where the problem is.

TROUBLESHOOTING NAME RESOLUTION

Since we often use names instead of addresses, you might need to verify that you have the correct name resolution when specifying a name. In Windows, the most common tool is nslookup.

Nslookup.exe is a command-line administrative tool for testing and troubleshooting DNS name resolution. Entering *hostname* in nslookup will provide a forward lookup of the host name to IP address. Entering *IP_Address* in nslookup will perform a reverse lookup of IP address to host name.

Entering nslookup puts you into an nslookup command environment that allows you to query specific servers using the server command and to query for specific resource records using the set type command.

If you found problems with the DNS, the ipconfig command can be used in certain situations:

- **ipconfig /flushdns:** Flushes and resets the contents of the DNS client resolver cache. During DNS troubleshooting, you can use this procedure to discard negative cache entries from the cache, as well as any other entries that have been added dynamically.
- **ipconfig /displaydns:** Displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local hosts file and any recently obtained resource records for name queries resolved by the computer. The DNS Client service uses this information to resolve frequently queried names quickly, before querying its configured DNS servers.
- **ipconfig /registerdns:** Initiates manual dynamic registration for the DNS names and IP addresses that are configured at a computer. You can use this parameter to troubleshoot a failed DNS name registration or resolve a dynamic update problem between a client and the DNS server without rebooting the client computer. The DNS settings in the advanced properties of the TCP/IP protocol determine which names are registered in DNS.

If you used the nslookup command to test DNS resolution and found a problem with name resolution, you would fix the problem at the DNS server. Unfortunately, previous DNS results that your system processes, such as when you access a web page using a browser, are cached in your memory. Therefore, if you correct the problem, you might need to flush your DNS cache using the ipconfig /flushdns command so that it can query and obtain the corrected values.

TAKE NOTE*

If you use host files or lmhosts files, you should check to see if any entries might be incorrect. NSLookup only tests DNS name resolution and will not check to see if a host file or lmhost file is correct.

TROUBLESHOOTING PROXY SETTINGS

Although CIDR helped use the IPv4 addresses more efficiently, additional steps were necessary to prevent the exhaustion of IPv4 addresses. ***Network address translation (NAT)*** is used with masquerading to hide an entire address space behind a single IP address. In other words, it allows multiple computers on a network to connect to the Internet through a single IP address.

NAT enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. The NAT computer or device is usually a router (including routers made for home and small-office Internet connections) or a proxy server. As a result, you can:

- Provide a type of firewall by hiding internal IP addresses.
- Enable multiple internal computers to share a single external public IP address.

The private addresses are reserved addresses not allocated to any specific organization. Because these private addresses cannot be assigned to global addresses used on the Internet and are not routable on the Internet, you must use a NAT gateway or proxy server to convert between private and public addresses. The private network addresses is expressed in RFC 1918 as:

- 10.0.0.0–10.255.255.255
- 172.16.0.0–172.31.255.255
- 192.168.0.0–192.168.255.255

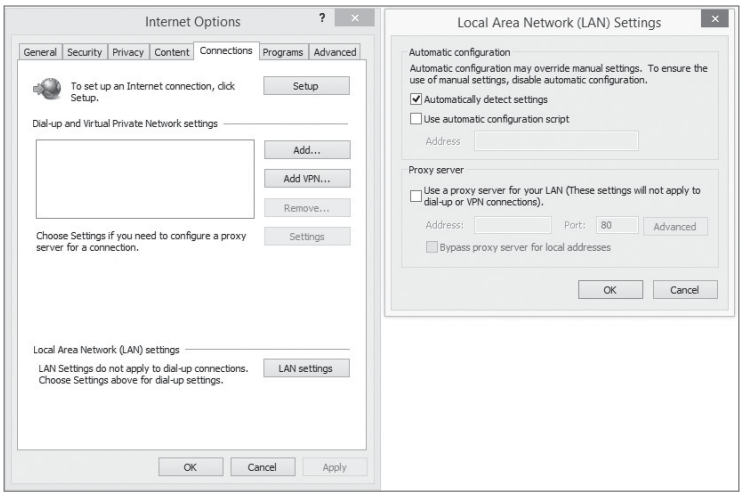
NAT obscures an internal network's structure by making all traffic appear originated from the NAT device or proxy server. A ***proxy server*** is a server that acts as an intermediary for clients seeking resources outside their networks. Medium and large organizations typically use a proxy server. In addition, these organizations require their clients to use the proxy server when accessing the Internet. By using the proxy server, organizations can monitor traffic and provide better security. For organizations that use proxy servers, since client traffic has to go through the proxy server to connect to the Internet, users will need to use the proxy server to access Office 365, Microsoft Intune, and Microsoft Azure.

CONFIGURE A CLIENT TO USE A PROXY SERVER

GET READY. To configure a client to use a proxy server, perform the following steps.

1. Open **Internet Explorer**.
2. Click the **Tools** button and click **Internet options**. Alternatively, you can open the **Control Panel** and double-click **Internet Options**.
3. In the Internet Properties dialog box, click the **Connections** tab.
4. Click the **LAN settings** button.
5. In the Local Area Network (LAN) Settings dialog box (see Figure 5-1), deselect the **Automatically detect settings** option.
6. Select the **Use a proxy server for your LAN** option.
7. In the Address text box, type the host name or IP address of the proxy server. In the Port address, type the port used by the proxy server, such as 80 or 8080.
8. If you do not want to use proxy servers to access local resources, select the **Bypass proxy server for local addresses** option.
9. Alternatively, you can click the **Advanced** button. In the Proxy Settings dialog box, you can specify individual proxy settings for HTTP, Secure, FTP, and Socks. You can also specify exceptions that you do not want to use the proxy server for. Click **OK**.
10. Click **OK** to close the Local Area Network (LAN) Settings dialog box.
11. Click **OK** to close the Internet Options dialog box.

Figure 5-1
Configuring proxy settings



Troubleshooting Sign-In Issues and Forgotten Passwords

If you access the portal for the cloud service, but you have trouble signing in, the problem is typically related to the account or the password.

When you receive a message such as We don't recognize this user ID or password, you should always make sure that you are using the correct user ID or password. The user ID should look like username@domainname.com or username@domainname.onmicrosoft.com. If you try to sign in using the wrong password 10 times, you will receive a You've tried to sign in too many times with the incorrect user ID or password message. In this case, you will have to wait a certain period of time (typically 15 minutes) for your account to be unlocked or to have an administrator unlock your account/reset password. If you cannot remember your password, you will have to have an administrator reset the password.

If you receive a message indicating that the user account is blocked, you can try waiting 15 minutes. If the account is still blocked, have an administrator locate the user in the portal, and under Set sign-in status, make sure the status is set to Allowed. If you can still not get in, try to reset the password.

If multiple users are suddenly having problems connecting the portal or application, be sure to try the portal and application yourself. Also log on to the portal and check the service status to see if there are any current problems. If you find out there is a problem and no problems show in the console, open a ticket for Microsoft.

Troubleshooting Issues with Activating Office Applications

When you install Office applications on a local machine, you need to activate Office or it will operate in a reduced functionality mode after 30 days. To activate your Microsoft product, you are confirming that each copy of the product is not installed on more than the number of computers allowed by the end user license agreement (EULA). The activation process can be performed by using the telephone or the Internet.

If you cannot activate Office over the Internet, you might be trying to access the Internet behind a proxy server or a firewall. If you are behind a firewall, make sure that you can get to all of the following websites:

- http://officecdn.microsoft.com
- https://ols.officeapps.live.com/olsc
- https://activation.sls.microsoft.com
- https://odc.officeapps.live.com
- http://crl.microsoft.com/pki/crl/products/MicrosoftProductSecureServer.crl
- http://crl.microsoft.com/pki/crl/products/MicrosoftRootAuthority.crl
- http://crl.microsoft.com/pki/crl/products/MicrosoftProductSecureCommunicationsPCA.crl
- http://www.microsoft.com/pki/crl/products/MicrosoftProductSecureCommunicationsPCA.crl
- go.microsoft.com
- office15client.microsoft.com
- sls.microsoft.com

If you seem to have no problem connecting to these websites, you should make sure you have the appropriate licenses.

ENSURE YOU HAVE THE APPROPRIATE LICENSE

GET READY. To ensure you have the appropriate license, perform the following steps.

1. Open **Internet Explorer** or **Microsoft Edge** and then sign in to the Office 365 Admin portal.
2. Click **Settings** and then click **Office 365 settings**.
3. Locate the Assigned licenses area. If you see the latest desktop version of Office, then you have an Office subscription assigned correctly. If you don't see the latest desktop version of Office, contact your admin.
4. To see how many installs you have available, or to deactivate another copy of Office, click **Software** (see Figure 5-2). If you deactivate another copy of Office, that copy of office will not be usable.

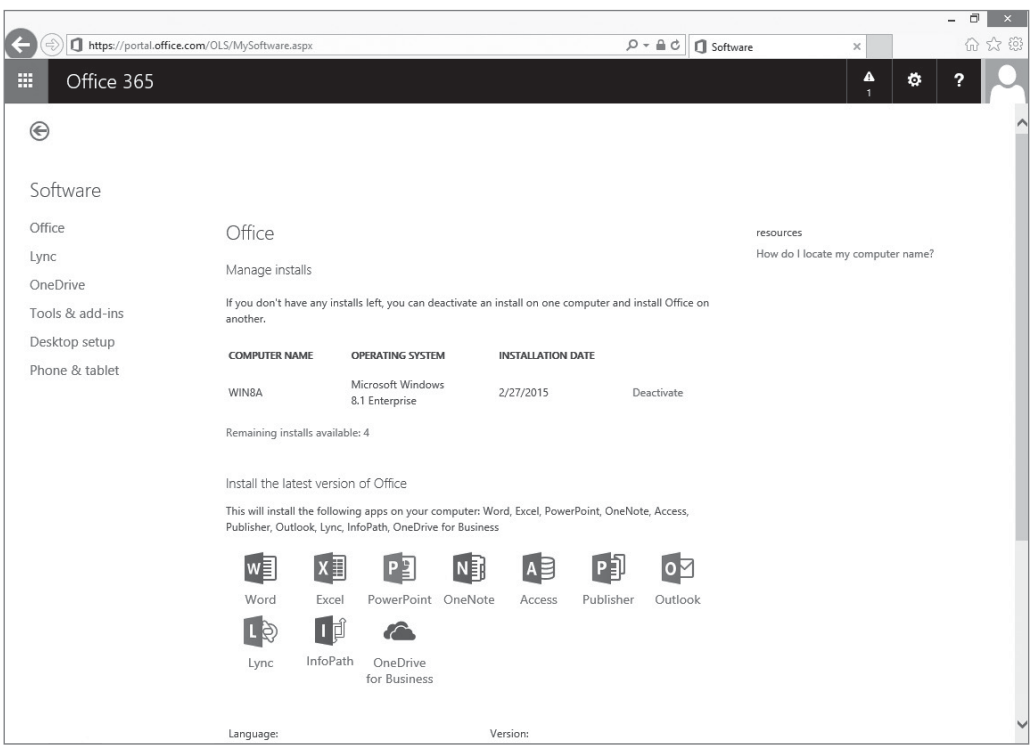


Figure 5-2

Managing your Office installations

Troubleshooting Difficulty Connecting Mobile Devices to Office 365 and Microsoft Intune

You can set up mobile devices to work with Office 365. You can also use Microsoft Intune to manage your mobile devices. The process of adding an Office 365 email account to a Windows Phone also adds OneDrive to the Office app.

To retrieve the instructions to configure Office 365 on mobile devices, go to https://support.office.com and search for "set up a mobile device using Office 365." You can then get instructions on how to set up Office, email, OneDrive, Skype for Business Online, and Yammer. The next exercise shows you how to configure email on a Windows Phone.

SET UP EMAIL ON A WINDOWS PHONE WITH OFFICE 365

GET READY. To set up email on a Windows Phone with Office 365, perform the following steps.

1. On the phone, in the App list, tap **Settings > email+account > add an account**. For the account type, select **Outlook**.
2. Type your work account name (for example, jsmith@contoso.com) and your password. Tap **Sign in**. When the account is set up, tap **Done**.
3. On the email account screen, type the username and password.
4. On the email+account screen, tap your account to open it. From the account settings, you can:
   - Rename the account
   - Set how much content to download
5. Make sure you have selected the check boxes for content you want to sync (such as email, contacts, calendar, and tasks).

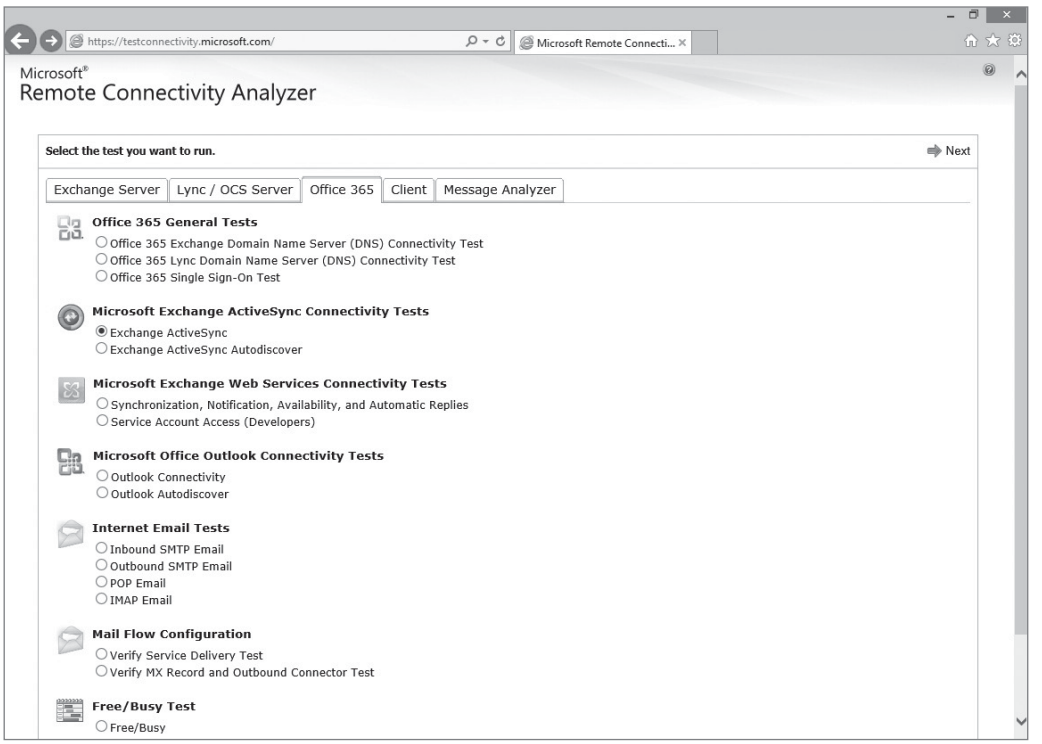
If you have problems connecting to your account or your email:

- Ensure you have Internet connection.
- Ensure the Exchange Online mailbox server that supports the connection is available and that there are is no maintenance or outage issue that would cause it to become unavailable.
- Access the account on the Office 365 Admin Portal and ensure that ActiveSync is enabled.
- Ensure the mobile device isn't blocked by an ActiveSync quarantine rule.
- Ensure Active Sync and ActiveSync Autodiscover are working by going to the Microsoft Remote Connectivity Analyzer, (http://www.testconnectivity.microsoft.com) site, clicking the Office 365 tab (see Figure 5-3), and then selecting the Exchange ActiveSync option and the Exchange ActiveSync Autodiscover option. For each option, you must provide an email address, the Microsoft Online logon ID, and a password.

To deploy Windows Intune to devices, you must ensure that the mobile device can access the Internet. If a user cannot log into the Microsoft Intune company portal, make sure that the account exists in the Microsoft Intune account portal and is not disabled. Also make sure the user is using the correct user name and password and using the correct format (such as jsmith@contoso.com).

Figure 5-3

Testing Microsoft Exchange ActiveSync connectivity



Choosing Between 32-bit and 64-bit Architectures

Besides the various editions of Windows 10, Windows 10 comes in two architectures: IA-32 (32-bit) and x64 (64-bit). While IA-32 supports only 32-bit applications, x64 supports 32-bit and 64-bit applications. The 64-bit version of Windows runs 32-bit applications using Windows on a Windows 64 (WOW64) emulator.

Unfortunately, applications or components that use 16-bit executable, 16-bit installers, or 32-bit kernel drivers will not run on a 64-bit edition of Windows 10. In addition, 64-bit unsigned driver installations stop responding on a 64-bit system. A signed driver includes a digital certificate indicating where the driver comes from and that the driver has not been tampered with.

If you need to run a 16-bit application on 64-bit version of Windows, you could try creating a virtual machine using client Hyper-V that runs a 32-bit version of Windows or you could place the application on a virtual machine that runs a 32-bit version of Windows.

Office is available in 32-bit and 64-bit. Of course, the 64-bit version of Office can only be installed on a 64-bit version of Windows. You should choose to install 64-bit if you need one of the following:

- You work with extremely large data sets, such as large enterprise-level workbooks with complex calculation, many PivotTables, and connections to external databases.
- You work with extremely large pictures, videos, or animations in PowerPoint.
- You work with extremely large Word documents with large tables, graphics, or other objects.
- You're working with files over 2 GB in Project 2013.

Identifying System Requirements for Office 365 ProPlus

Office 365 does not have operating system requirements, except that the operating system you use must be supported by its manufacturer. While Microsoft does not block users from connecting to older operating systems, some features might not be available or might not work as expected.

Office 365 is designed to work with the current or most immediately previous versions of Internet Explorer, Firefox, Chrome, or Safari. If you use older versions of Internet Explorer, users might experience known issues or limitations.

To install Office 2016 or Office 365 ProPlus, you should meet the following minimum system requirements:

- **Operating system:** Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2/2016, Windows 7, Windows 8/8.1, or Windows 10. 32-bit Office can be installed on 32-bit or 64-bit operating systems and 64-bit Office can only be installed on 64-bit operating systems.
- **Processor:** 1 GHZ or faster x86 or 64-bit processor with SSE2 instruction set.
- **Memory:** 1 GB RAM (32-bit) or 2 GB RAM (64-bit) is recommended for graphics features, Outlook Instant Search, and certain advanced functionality.
- **Disk space:** 3 gigabytes (GB)
- **Monitor resolution:** 1280 x 800

Using Office Repair

Microsoft Office is a powerful yet complex suite of programs. If it becomes unstable or does not work as expected, you could try to diagnose and repair Office using ***Microsoft Office Diagnostic Tools***. Microsoft Office Diagnostic Tools is a series of diagnostic tests that are included with Microsoft Office; they help you identify and fix problems with Office.

Before you repair your computer, always restart your computer. If the problem remains, you can then open Programs and Features to perform the repair. If the repair does not work, you can reinstall Office or you can remove and reinstall Office 365 ProPlus.

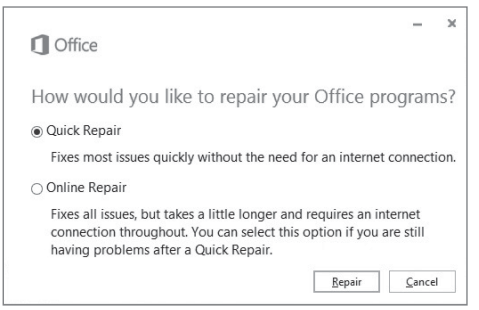
FIX OR REPAIR OFFICE 2016 OR OFFICE 365 PROPLUS

GET READY. To fix or repair Office 2016 or Office 365 ProPlus, perform the following steps.

1. Open the Windows Control Panel. In Windows 8.1, right-click the **Start** button and choose **Control Panel**.
2. Click **Programs > Programs and Features**.
3. Click the Office application you want to repair and then click **Change**.
4. For Microsoft Office 2016 or Office 365 ProPlus, click either **Quick Repair** or **Online Repair**, as shown in Figure 5-4.

Figure 5-4

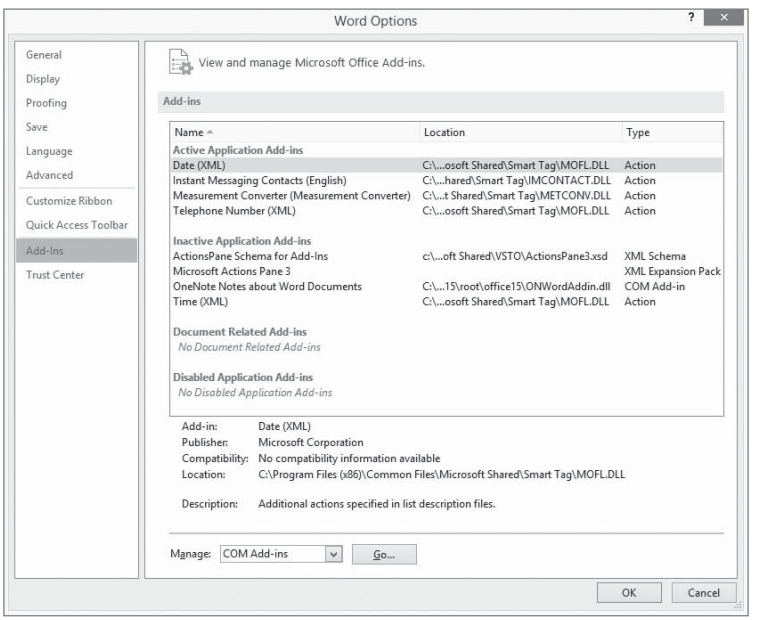
Performing an Office 365 ProPlus repair



An ***add-in*** adds additional functionality to Microsoft Office products. If the problem still exists, the problem could be specific to application add-ins. For example, open a Microsoft application, click the File menu, click Options, and then click Add-Ins (see Figure 5-5). You can then to disable an add-in or you can ensure that an add-in is enabled by clicking Manage, selecting an option (such as COM Add-ins, Actions, Word Add-ins, or Disabled Items) and then click Go. Depending on the option you select, you can add, remove, or disable the option.

Figure 5-5

Viewing Microsoft Word add-ins



■ Resolving Issues with Emails and Calendars

THE BOTTOM LINE

Microsoft's email and calendar programs require a connection to a mail service, such as a local mail server or an Internet mail service (such as Office 365). If the client computer is behind a proxy or firewall, make sure that the client has access to websites.

CERTIFICATION READY
Resolve email and calendar issues
5.2

In Lesson 4, you learned that email and calendar information is delivered to mobile devices using ActiveSync. In Office 365, desktop applications access email by using the Messaging Application Programming Interface (MAPI) over HTTP. Older versions of Office used Remote Procedure Calls (RPC) over HTTP (commonly referred to as

Outlook Anywhere). Each method allows connected users to access email on a corporate Exchange Server or Office 365.

Troubleshooting Issues with Sending and Receiving Email

Issues specific to sending and receiving emails can be frustrating, particularly when emails are time-sensitive. If a user is having problems with email, check the user's Outlook settings and use tools to check connectivity on the machine that is having the problem.

When you are installing Office 2016 or Office 365 ProPlus on a user's computer, you will have to work with the user to run the Add Account Setup wizard and type the user's email address and password. Outlook uses a process called ***autodiscover*** to automatically find the user's settings and to set up an Exchange connection to your account.

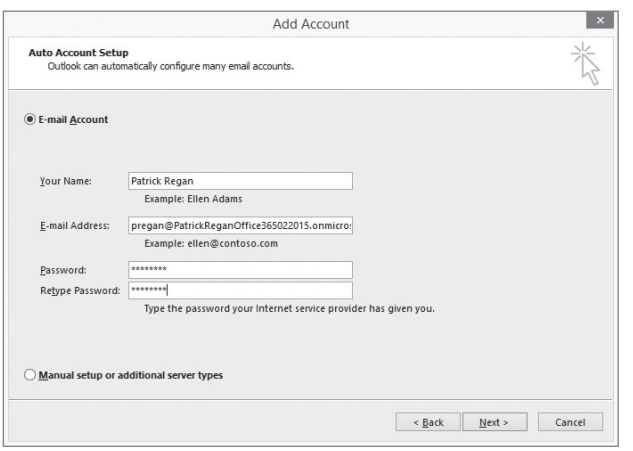
SET UP AN EXCHANGE CONNECTION TO YOUR EMAIL IN OUTLOOK 2016 OR OFFICE 365 PROPLUS

GET READY. To set up an Exchange connection to your email in Outlook 2016 or Office 365 ProPlus, perform the following steps.

1. Open Outlook 2016. If the Microsoft Outlook Startup Wizard opens, on the first page of the wizard, click **Next**. On the E-mail Accounts page, click **Next** to set up an email account. If the Microsoft Outlook Startup Wizard doesn't open, on the Outlook toolbar, click the **File** tab. Then, above the Account Settings button, click **Add Account**.
2. On the Auto Account Setup page (see Figure 5-6), Outlook may automatically fill in the Your Name text box and the E-mail Address text box based on how you're logged on to your computer. If not, you will have to type your name, your email address, and your password in the respective boxes. Once you've done that, and you've typed the correct password, click **Next**. Outlook will finish setting up your account.

Figure 5-6

Configuring an Outlook account



3. If the settings on the Auto Account Setup page aren't filled in or aren't correct, type the correct settings and then click **Next**.
4. When the account is configured, click **Finish**.

The bottom of the Microsoft outlook window should display CONNECTED TO:

MICROSOFT EXCHANGE. If WORKING OFFLINE or DISCONNECTED is displayed, or if a message stays in the Outbox and isn't sent, or if you are not receiving emails, you should log on to the http://mail.office365.com website to make sure email is being received on the cloud application. If the Office 365 web application is working properly, check the following:

1. Make sure that your software and operating system are up-to-date.
2. Repair your Outlook profile (discussed in the following exercise).
3. Create a new Outlook profile.
4. Use the Outlook Connection Status tool and the Remote Connectivity Analyzer.

Make sure that you meet the minimum requirements for Office 365. Then use Windows Update to install the latest patches and feature updates. You can also try to perform a repair Microsoft Office and the Outlook Profile.

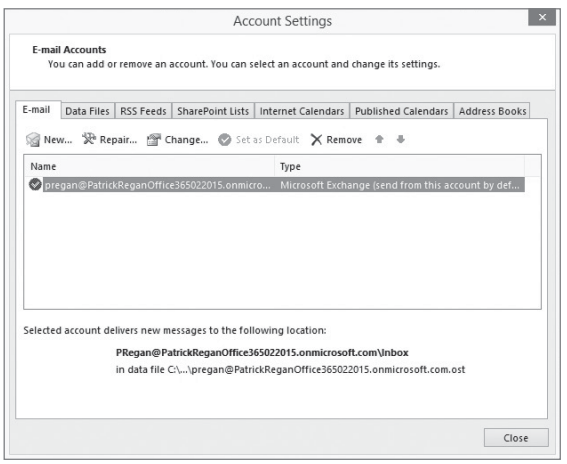
REPAIR AN OUTLOOK PROFILE

GET READY. To repair an Outlook profile, perform the following steps.

1. In Open Outlook 2016, click **File**.
2. Click the down-arrow next to Account Settings and then click **Account Settings**.
3. On the E-mail tab, select your account/profile (as shown in Figure 5-7) and then click **Repair**.

Figure 5-7

Managing Outlook email accounts



4. In the Repair Account Wizard, with the E-mail Account option selected, click **Next**.
5. When you are prompted to restart Outlook for these changes to take effect, click **OK**.
6. Back in the Repair Account Wizard, click **Finish**.
7. Click **Close** to close the Account Settings dialog box.

If the problem still persists, you can run the Outlook Connection Status tool and the Outlook Connectivity tool. To access the Outlook Connection Status tool, launch Outlook, press the Ctrl key, right-click the Outlook icon in the taskbar, and choose Connection Status (see Figure 5-8). Figure 5-9 shows the Outlook Connection Status tool. The Outlook Connection Status can show you if you are having problems communicating with the email server/service.

The Microsoft Remote Connectivity Analyzer tool (https://testconnectivity.microsoft.com) can be used to test outlook connectivity to an Exchange Server and Office 365. It can be used to test ActiveSync, ActiveSync Autodiscover, Outlook Connectivity, Outlook Autodiscover, and SMTP Email via a web page, as shown in Figure 5-10.

Figure 5-8

Opening the Outlook Connection Status tool

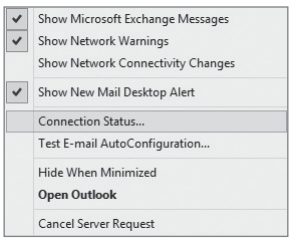


Figure 5-9

Using the Outlook Connection Status tool to view current connections

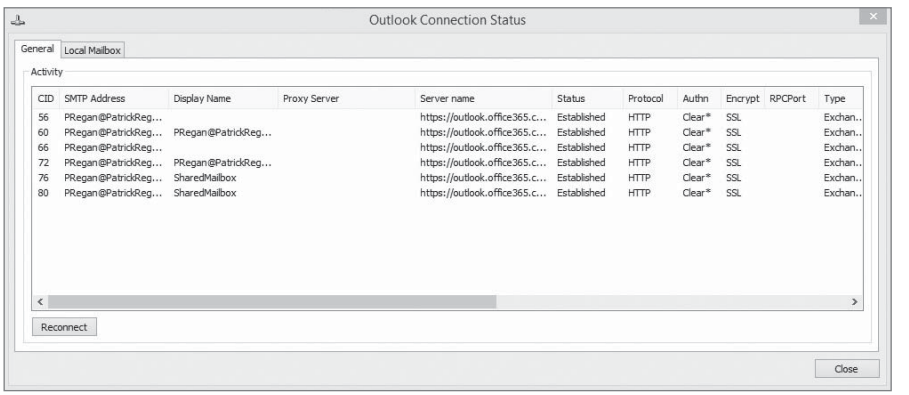
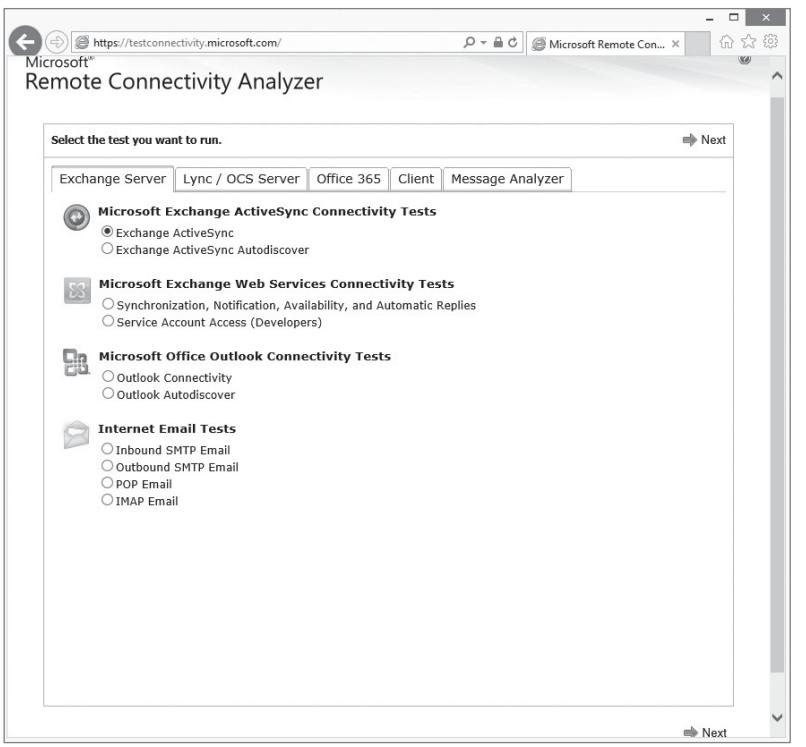


Figure 5-10

Starting the Microsoft Remote Connectivity Analyzer



Troubleshooting Issues with Accessing a Delegated Mailbox

Outlook 2016 and Outlook Online allow you to add multiple Exchange accounts to the same profile. You simply need Full Access permission to the additional Exchange mailbox or you must know the credentials to access the additional Exchange mailbox.

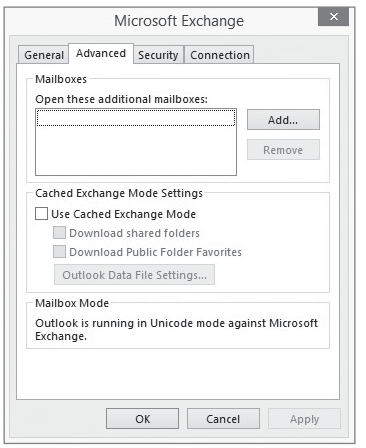
When you open the Account Settings dialog box for Outlook 2016 or Outlook Online, you cannot access your mailbox and the delegated mailbox in the same profile. Instead, you have to add the second mailbox as an additional mailbox.

ADD A SECOND MAILBOX

GET READY. To add a second mailbox as an additional mailbox in Outlook 2016, perform the following steps.

1. Open Outlook 2016, click the **File** tab, and then click **Info**.
2. Click **Account Settings** and then click **Account Settings**.
3. Select the account that you want to manage and then click **Change**.
4. In the Change Account dialog box, click **More Settings**.
5. Click the **Advanced** tab (as shown in Figure 5-11) and then click **Add**.

Figure 5-11
Adding an additional mailbox



6. Type the name of the mailbox and then click **OK**. After you make this change, the additional mailbox is listed on the Advanced tab in the Microsoft Exchange dialog box.
7. In the Microsoft Exchange dialog box, click **OK**.
8. In the Change Account dialog box, click **Next**.
9. Click **Finish** and then click **Close**.

■ Resolving Issues with SharePoint and OneDrive

THE BOTTOM LINE

Office 365 SharePoint is a very reliable system with lots of flexibility. In addition, when using OneDrive for Business, OneDrive services are provided by SharePoint. When using SharePoint or OneDrive for Business, you should use the current or immediately previous versions of Internet Explorer, Firefox, Chrome, or Safari. In addition, if several users are experiencing problems, you should log on to the Office 365 Admin Portal to see if any outages or other problems might be causing a problem.

CERTIFICATION READY
Resolve SharePoint and OneDrive issues
5.3

Whenever you have problems with SharePoint Online or OneDrive, you should remember that the Internet can provide a lot of information about problems that users have encountered. In addition, when troubleshooting these problems, follow basic troubleshooting methodology, which includes identifying the problem, determining the scope of the problem, and gathering information.

Identifying SharePoint Storage Limits

While SharePoint is very scalable, it does have limitations. The limits are partly a result of the SharePoint Online plan you select and partly as result of the number of supported users, storage quotas used, and file-size limits.

When troubleshooting problems with SharePoint Online, you need to make sure that you have not exceeded the following limitations:

- 500 MB per subscribed user unless you purchased additional storage
- Up to 1 TB per site collection; default website public storage is 5 GB
- Up to 1 TB for personal site storage per user
- Up 5,000 items synched in site libraries, including folders and files
- A file upload limit of 2 GB per file
- Up to 2,000 subsites per site collection

In addition, administrators can set storage limits for site collections and sites.

Resolving Issues with Open with Explorer

Because SharePoint can be used to store files in a library, you can upload files and documents to and download files and documents from the SharePoint libraries. To allow for a quick access to these libraries, you can open the library with File Explorer. To open with File Explorer, navigate to a SharePoint library and then click the Open with Explorer button as shown in Figure 5-12. When file explorer opens, you can then drag documents just like you would drag, cut, copy or delete a file from a local drive.

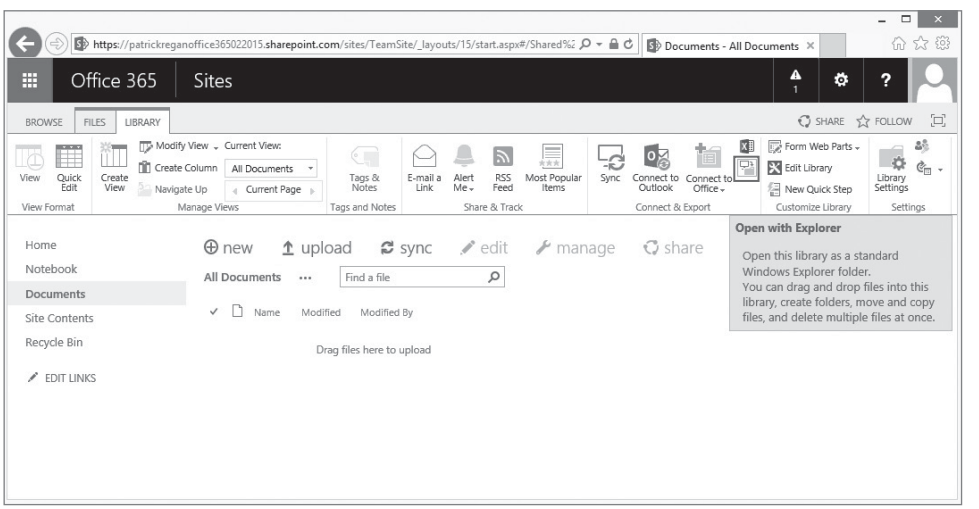


Figure 5-12

Clicking the Opening with Explorer button

If you have issues with SharePoint, including Opening with File Explorer, you should:

- Make sure you are authenticated to Office 365.
- Make sure that SharePoint Online sites are added to your trusted sites.
- Make sure that WebClient services is present and enabled. If it is not, install the Desktop Experience feature.
- Check to see if your system needs any updates or fixes.

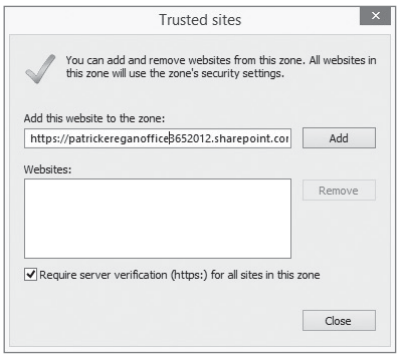
ADD A SHAREPOINT ONLINE SITE TO A TRUSTED SITES ZONE

GET READY. To add a SharePoint Online site to a Trusted Sites zone, perform the following steps.

1. Open Internet Explorer.
2. Click the **Tools** button and then click **Internet options.**
3. Click the **Security** tab, click **Trusted sites**, and then click **Sites.**
4. In the Add this website to the zone text box, type the URL for the SharePoint Online site (such as https://contoso.sharepoint.com) that you want to add to the Trusted Sites zone. See Figure 5-13.

Figure 5-13

Adding sites to the Trusted Sites zone



5. Click **Add.**
6. After you have added each site to the Websites list, click **Close** and then click **OK.**

Resolving Issues with OneDrive Sync

One of the many appealing features of OneDrive is that you can easily store data to the cloud by using the OneDrive app. The primary issue an administrator will encounter when using OneDrive is when OneDrive is not syncing.

OneDrive for Business, which was introduced in Lesson 4, is provided by a SharePoint document library that is located within the SharePoint My Site site.

Files in OneDrive for Business are versioned. Therefore, if you need to recover a file that was deleted in OneDrive or you need to recover a previous version of a file, you can recover the file using the web client. When files are deleted, the deleted files are placed in the Recycle Bin and can be restored for up to 90 days in the web client. Files deleted from the Recycle Bin move into a second-stage recycle bin for an additional 90 days, meaning there is a total of 180 days that a deleted file can be recovered. Users can to go the first-stage Recycle Bin to undelete their own files. Administrators can go to the second-stage Recycle Bin to undelete any files, including files owned by other users that were deleted.

Although Microsoft retains backups of your data and keeps copies in multiple data centers, the Recycle Bin will be the method you'll need to use to recover files. Third-party applications can be used to archive files from SharePoint and OneDrive for Business for an additional cost.

When a user is having sync problems:

- In the OneDrive app, swipe up from the bottom or right-click and then tap or click Sync so that OneDrive will check again for changes.
- Make sure the user has signed in with the correct Microsoft account.

- Make sure that the OneDrive Sync Engine Host is running. Open the Task Manager and click More details. Then in the Processes tab, under Background processes, make sure OneDrive Sync Engine Host appears.
- Make sure that the system that is having a sync problem has the latest Windows updates.
- Verify that the size of the file you are trying to sync doesn't exceed the OneDrive file size limit of 10GB. If a file is too large, you will receive a message indicating *This file is too big to upload or Reduce the size of this file to upload it to . . .*
- Run the OneDrive troubleshooter by going to the Microsoft website and searching for the OneDrive Troubleshooter.
- Check the OneDrive Recycle Bin to make sure that the file or folder has not been accidentally deleted. If you are syncing your OneDrive on a computer, check the Windows Recycle Bin. Also make sure that the file has not been moved.
- Check to see if OneDrive files include a character that's not allowed. The file name should not begin with or end with a space, should not end with a period, and should not begin with two periods. Also, you should not use reserved names, such as AUX, PRN, NUL, CON, COM0, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT0, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, and LPT9.
- Check to see if the file path is too long. The entire path, including the file name, must contain fewer than 255 characters.
- Check to see if OneDrive is blocked by Group Policy or a corporate firewall. You can also open the OneDrive app to see if there is a message indicating *Your system administrator has blocked the use of OneDrive*.
- Reset the re-sync of OneDrive data by executing the OneDrive.exe /reset command.

Recovering Deleted Files

Since SharePoint and OneDrive will be used to store important data, it is important that you know how to recover data when needed. Therefore, you need to understand how the SharePoint Recycle Bin works and how to retrieve files form the Recycle Bin.

The ***SharePoint Recycle Bin***, sometimes known as the ***End User Recycle Bin***, is a holding area for deleted objects. The files in Recycling Bin have a default retention period of 90 days. After that time, or if you manually delete them before that time from the Recycle Bin, they can no longer be restored and cannot be retrieved by any means. Please keep an off-site back up of all important files. Microsoft maintains backups for disaster recovery only.

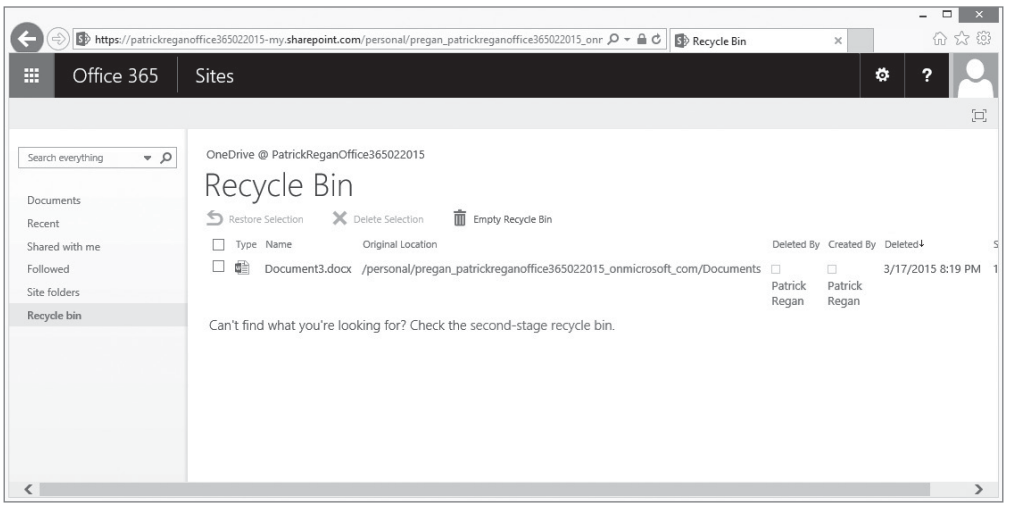
RESTORE FILES USING THE ONEDRIVE RECYCLE BIN

GET READY. To restore files using the OneDrive Recycle Bin, perform the following steps.

1. Open Internet Explorer.
2. Go to the SharePoint website or the OneDrive website.
3. Tap or click **Recycle bin** at the bottom of the left pane, as shown in Figure 5-14.
4. To restore all items, select the checkbox at the top of the list and tap or click **Restore Selection**. To restore or permanently delete individual items, select their check boxes and then click **Restore Selection**. To permanently delete all items, tap or click **Empty Recycle Bin**.

Figure 5-14

Opening the SharePoint Recycle Bin



Site collection administrators can view, restore, or delete any object in the site Recycle Bin; a user can only view, restore, or delete any object that she deleted. If you are the site collection admin, you can click the second-stage Recycle Bin, also known as the ***Site Collection Recycle Bin***, which is a secondary holding area for deleted documents for the entire site collection

When you delete a list, library, file, file version, or other list item, the deleted object will go to the site recycle bin. If you delete the site or workspace, the deleted object will go to the site collection recycle bin.

■ Resolving Issues with Skype for Business Online

THE BOTTOM LINE

As you learned in Lesson 4, Skype for Business Online that can be used for instant messaging (IM), audio and video conversations, and online meetings. Most of the time, Skype just works. However, there might be times when you have to troubleshoot Skype.

CERTIFICATION READY
Resolve Skype for Business Online issues
5.4

To work correctly, Skype requires unrestricted outgoing TCP access to all destination ports above 1024 (recommended) or Ports 80 and 443. If you allow ports above 1024, a port is chosen at random for incoming connections. You will also need the following ports open:

- **Session Initiation Protocol (SIP) Signaling:** TCP Port 443
- **Persistent Shared Object Model (PSOM) Web** Conferencing: TCP port 443.
- **HTTPS downloads:** TCP port 443
- **Audio:** UDP and TCP ports 443, TCP port 3478, UDP and TCP port 50000 – 59999
- **Video:** TCP port 443, UDP port 3478, UDP and TCP ports 50000 – 59999
- **Desktop sharing:** TCP port 443, UDP ports 50000 – 59999
- **Lync Mobile push notifications for Lync Mobile 2010 on iOS and Windows Phone 7.5 devices**: TCP port 5223.

If you want to use a specific port for incoming connections, you must open the alternative port manually.

If you suspect problems with Skype, go to http://heartbeat.skype.com (see Figure 5-15), where you can check the following:

- Call Phones
- Skype Number
- Voice messaging
- Skype SMS
- Video messaging
- Sign in and registration
- Account and paymentst
- Skype Connect

You can also check for any maintenance that might affect Skype.

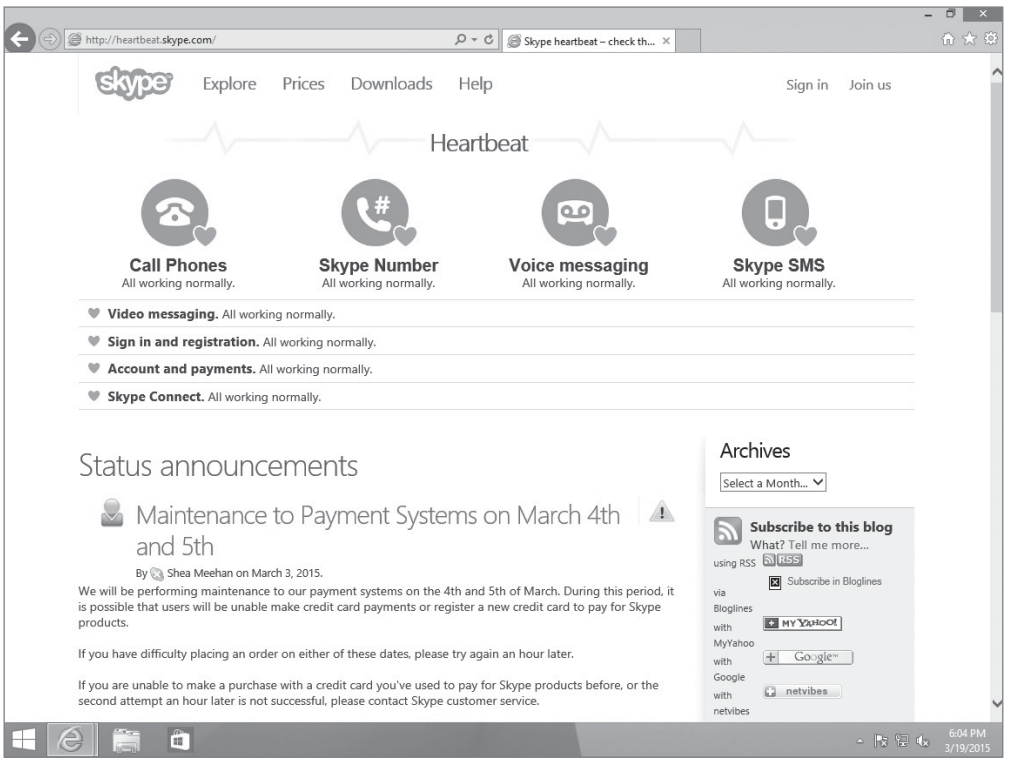


Figure 5-15

Testing Skype with heartbeat .skype.com

You can test your microphone and speakers by opening the Skype for Business options and clicking the Audio Device tab or the Video Device tab. You should first check to see if your microphone and speakers are recognized. If they are not recognized, you need to ensure that proper drivers are loaded and the correct microphone and speaker are selected in the Audio Device tab and the Video Device tab. You should also check to make sure that volume is loud enough and that the devices are connected and turned on. If you click the Audio Device tab, you can test your microphone my speaking into it, which should allow you to see the green volume bar under Microphone move. If you click the Video Device tab when sound is playing, you should see the green volume bar under Speakers move. You should also check the volume levels on the devices and within the Audio Device tab and the Video Device tab.

If you are experiencing poor audio or video quality, you should check for network problems, including looking at the network load. In addition, you should ensure the audio/video device is approved and certified to work with Skype.

SUMMARY SKILL MATRIX

In this lesson you learned:

- The first type of problem that you will encounter will involve users trying to log in to the cloud portal or application. Any time that you transition from local applications to cloud-based applications, there is an initial learning curve for users.
- Connectivity issues are defined as any problem whereby users cannot access the cloud portal or cloud application. When dealing with connection problems, use basic troubleshooting models and tools to determine the scope of the problem. If only one user is experiencing the problem, the problem is most likely a result of the settings on his computer.
- If you access the portal for the cloud service, but you have trouble signing in, the problem is typically related to the account or the password.
- You can set up mobile devices—including Android devices, iPhones, iPads, and Windows Phones—to work with Office 365. You can also use Microsoft Intune to manage your mobile devices. The process of adding an Office 365 email account to a Windows Phone also adds OneDrive to the Office app.
- Office 365 does not have an operating system requirements, except that the operating system you use must be supported by its manufacturer. While Microsoft does not block users from connecting to older operating systems, some features might not be available or might not work as expected.
- Microsoft's email and calendar programs require a connection to a mail service, such as a local mail server or an Internet mail service (such as Office 365). If the client computer is behind a proxy or firewall, make sure that the client has access to websites.
- Office 365 SharePoint is a very reliable system with a lot of flexibility. When using OneDrive for Business, OneDrive services are provided by SharePoint. When using SharePoint or OneDrive for Business, you should use the current or immediately previous versions of Internet Explorer, Firefox, Chrome, or Safari. In addition, if several users are experiencing problems, you should log on to the Office 365 Admin portal to see if any outages or other problems might be causing a problem.
- Since SharePoint and OneDrive will be used to store important data, it is important that you know how to recover data when needed. Therefore, you need to understand how the SharePoint Recycle Bin works and how to retrieve files form the Recycle Bin.
- Skype for Business Online can be used for instant messaging (IM), audio and video conversations, and online meetings.

■ Knowledge Assessment

Fill in the Blank

Complete the following sentences by writing the correct word or words in the blanks provided.

1. To test connectivity to a server, the simplest command to use is the _____ command.
2. To test DNS by performing a DNS query, you should use the _____command.
3. _____ is used with masquerading to hide an entire address space behind a single IP address.
4. When dealing with sign-in problems, you must make sure that users have the correct _____.

5. When a mobile device accesses email from Office 365, it uses _____.
6. Clients using Office 2016 can retrieve email from Office 365 by using _____.
7. If Opening with File Explorer does not work, you should make sure that the SharePoint Online sites are added to your _____.
8. When a site is deleted by mistake, you can restore the site from the _____.
9. When you experience poor video quality, you should look for _____.
10. To check access to Skype, you should use the _____site.

Multiple Choice

Circle the letter that corresponds to the best answer.

1. Which command allows you to see the IP configuration, including the DNS servers and default gateway?
   a. ipconfig /all
   b. tracert
   c. showall
   d. netstat -a
2. Which command is used to show the route that packets take when accessing a specific server?
   a. ping
   b. tracert
   c. netstat
   d. telnet
3. Which server or device can be used to funnel users when users are accessing the Internet and provides better security by hiding internal IP addresses?
   a. Lync server
   b. ActiveSync server
   c. Autodiscover server
   d. Proxy server
4. Which of the following is the easiest way to activate a Microsoft application?
   a. Using a telephone
   b. Retrieving a key from the Microsoft website and entering that key into Office 365.
   c. Using a modem
   d. Using the Internet
5. You are running Skype for Business to connect to an online meeting. While you have no trouble logging on, you are having problems with video as well as desktop sharing. Which of the following is the best course of action for resolving this issue?
   a. Examine the DNS records to see if the zone is not configured correctly.
   b. Examine the firewall the see if it is blocking access to any of the Lync Online websites.
   c. Check to see if any firewalls are blocking the ports used by audio, video, and desktop sharing.
   d. Make sure the user has access to the Internet.
6. Users are having trouble accessing Office 365. Which of the following is most likely the problem?
   a. The trial period for the software has expired
   b. Windows or Office was not activated.
   c. Office 365 is being blocked by a firewall.
   d. Microsoft has denied your company access

7. Word Online is locking up for a user and that user often has to restart Word. There appears to be no other problems with the system. Which of the following is the recommended course of action?
   a. Check your licensing to make sure you have the correct license for Office 365.
   b. You need to repair Office
   c. Make sure the user has Internet access to the Office 365 websites.
   d. You need to reload Windows
8. You have a large file that is 2.4 GB that you want to load into SharePoint. However, it fails every time. What is most likely the problem?
   a. Your file upload limit is 2 GB
   b. Your site collection is full
   c. You are limited to 500 MB of storage
   d. You are having network issues
9. Which of the following tools is used to test connectivity to ActiveSync and to test autodiscovery?
   a. Ipconfig /all command
   b. Outlook Test Tool
   c. Microsoft Remote Connectivity Analyzer
   d. Best Practices Analyzer
10. Which of the following is the default retention period for deleted objects in SharePoint Online?
    a. 30 days
    b. 60 days
    c. 90 days
    d. 180 days

True / False

Circle T if the statement is true or F if the statement is false.

T | **F** **1.** When you change a resource record on a DNS zone and you want the client to see the change immediately, you should run ipconfig /displaydns on the client's computer.

T | **F** **2.** When a user cannot access the Internet while working from the corporate offices, you should check proxy settings.

T | **F** **3.** When using SharePoint Online, the recommended browsers are the newest versions of Internet Explorer, Chrome, or Firefox.

T | **F** **4.** When OneDrive is not syncing properly, the OneDrive.exe /reset command will cause OneDrive data to resync.

T | **F** **5.** SharePoint uses a two-level Recycle Bin.

■ Case Projects

Scenario 5-1: Troubleshooting Office 365 Connectivity

You are an administrator for the Contoso Corporation and a user cannot connect to Office 365. Describe your troubleshooting methodology when dealing with such issues.

Scenario 5-2: Troubleshooting Email Access on a Smartphone

The helpdesk is trying to connect a user's smartphone to the user's email, which is hosted in Office 365. However, the smartphone is displaying a connection failure message. Describe how to troubleshoot this problem.

Scenario 5-3: Resolving SharePoint Online Problems

A user who is working remotely on a company laptop is cannot locate an Excel spreadsheet on a SharePoint Online site. It has been several weeks since the user last accessed the file and he now cannot locate the file. Describe the steps you would take to locate the file.

Scenario 5-4: Resolving Issues with Accessing Skype for Business Online

A user who is working remotely on a company laptop is unable to connect to an online meeting that is accessed with Skype for Business Online. Describe the steps you would take to troubleshoot this problem.

Appendix A
Exam 98-369 Cloud Fundamentals

Exam Objective	Skill Number	Lesson Number
Understand the Cloud		
Describe cloud principles and delivery mechanisms	1.1	1
Describe cloud security requirements and policies	1.2	1
Describe how a cloud service stays up to date and available	1.3	1
Describe the different types of cloud services	1.4	1
Enable Microsoft Cloud Services		
Identify the requirements and dependencies for using Office 365 and Microsoft Intune	2.1	2
Select a cloud service plan	2.2	2
Sign up for cloud services	2.3	2
Set up the initial configuration of cloud services	2.4	2
Administer Office 365 and Microsoft Intune		
Create users and groups, and assign services and licenses	3.1	3
Assign permissions in Office 365 and Microsoft Intune	3.2	3
Monitor service health in Office 365 and Microsoft Intune	3.3	3
Use and Configure Microsoft Cloud Services		
Configure Exchange Online	4.1	4
Configure SharePoint Online, including OneDrive	4.2	4
Configure Skype for Business Online	4.3	4
Configure Microsoft Intune	4.4	4
Support Cloud Users		
Resolve sign-in and Office application installation issues	5.1	5
Resolve email and calendar issues	5.2	5
Resolve SharePoint and OneDrive issues	5.3	5
Resolve Skype for Business Online issues	5.4	5

Index

N

O

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.