Microsoft

The ultimate, in-depth reference

Hundreds of timesaving solutions

Supremely organized, packed with expert advice

Companion eBook

Microsoft Office 365 Administration

Julian Soh, Anthony Puca, Marshall Copeland

Microsoft Office 365 Administration

Inside OUT

Conquer Microsoft Office 365 administration—from the inside out!

Dive into Office 365 administration—and really put your systems expertise to work! This supremely organized reference packs hundreds of timesaving solutions, troubleshooting tips, and workarounds. Discover how the experts tackle deployment, configuration, and management—and challenge yourself to new levels of mastery.

- Simplify enterprise deployment with planning tools and tasks
- Automate Office 365 processes with Windows PowerShell
- Manage user identity with Active Directory and Single Sign-On
- Monitor and maintain the health of Office 365 with Microsoft System Center
- Implement Microsoft Exchange Online, SharePoint Online, and Lync Online
- Control variables in an Exchange Server hybrid implementation
- Customize and deploy Office 365 Professional Plus
- Explore real-world scenarios and apply insider management tips

For Intermediate and Advanced Users

About the Authors

Julian Soh, an enterprise architect at Microsoft, works with customers to evaluate, understand, plan, and design Office 365 adoptions.

Anthony Puca, a datacenter specialist at Microsoft, focuses on Windows Server, Windows Azure, Microsoft System Center, and Microsoft Forefront.

Marshall Copeland, a datacenter specialist at Microsoft, specializes in Windows Azure, Windows Server, and Microsoft System Center.

Companion eBook

Download using the instruction page in the back of the book.

microsoft.com/mspress

ISBN: 978-0-7356-7823-1

9 780735 678231 90000

U.S.A. $49.99
Canada $52.99
[*Recommended*]

Microsoft Office/Microsoft Office 365

Microsoft

Microsoft

Microsoft Office 365 Administration Inside Out

Julian Soh
Anthony Puca
Marshall Copeland

ISBN: 978-0-7356-7823-1

Fifth Printing: March 2015

Printed and bound in the United States of America.

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at *mspinput@microsoft.com*. Please tell us what you think of this book at *http://www.microsoft.com/learning/booksurvey*.

Acquisitions and Developmental Editor: Kenyon Brown

Production Editor: Kara Ebrahim

Technical Reviewers: Darryl Kegg, Scott Wold, Stephen Jones, and Mark Ghazai

Copyeditor: Barbara McGuire

Indexer: BIM Publishing Services

Cover Design: Twist Creative • Seattle

Cover Composition: Ellie Volckhausen

Illustrator: Rebecca Demarest

Contents at a glance

Table of contents

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

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

http://aka.ms/tellpress

PART 4: Integrating and using Office 365 Services

PART 6: Appendix

Foreword

WHEN I think back at why I got into IT, it came down to a constant thirst for innovation and helping solve problems with technology. Innovation can take on two forms: refinement or outright change. Technology really exists to solve problems and can take any form.

As a kid I watched my computers and game consoles change manufacturer and platform at an almost annual clip. That was exciting and still is. It's part of why I'm excited to be in the tech industry. You can see how fluid the technology space is by watching the mobile device and gaming markets right now. In the same way, you can see an evolution of communication styles. Written correspondence, email, instant messaging, social, video calls and online meetings are part of most of our daily repertoire. These things all have hooks into different services, both on-premises and online. The fluidity and constant evolution attracted me and many of us to technology.

Now we are seeing the pendulum swing to where many of the technology services are turning into commodities and things that used to take thousands of dollars of infrastructure to accomplish have been simplified into a few clicks. The automation we spent building in the last decade has turned into service and account hydration. The virtual machines, clustered services, and live migrations have been woven into the fabric of cloud services. It means the building and sizing of infrastructure is real-time and logic-based. As infrastructure people, we've watched this evolve and the elasticity of everything is really cool and getting better with more advances in security, rapid failover, and most other aspects each day.

Office 365 is a leader in the charge to take advantage of the infrastructure and automation improvements to provide highly available services. As the workloads in Office 365 (Exchange, SharePoint, Lync, Yammer, and Office) continue to develop, Office 365 removes the complexity of building out infrastructure and keeping software up to date. The rapid innovation of these services and the evolution of technology they build upon is a reflection of that spark that led many of us into technology careers.

Like any platform, it is extensible, configurable, and manageable. For the seasoned IT pro, many of the aspects around directory service management, user provisioning, PowerShell automation, email, and site administration are consistent with what you've probably been doing. As an IT pro, your stake and role is more valuable than ever. With a background in Exchange or SharePoint, you have a unique view into the inner workings of the services, without the painstaking work of provisioning and de-provisioning servers, patch management, and major upgrades.

Microsoft Office 365 Administration Inside Out is your guide to navigate the landscape to Office 365 from the IT pro lens. It goes much deeper and thoughtfully into the specifics of managing Office 365 workloads. The great thing with this book is that once you start a trial, you can hit the ground running and start getting hands-on. The other great side effect of cloud services is that you generally don't need to worry about test virtual machines or hosted hands-on labs. It's all there, so roll up your sleeves and get started.

—Jeremy Chapman
Director Office 365 Product Management

Introduction

WELCOME to *Office 365 Administration Inside Out*. This book was written specifically for enterprise-level customers who want to adopt Office 365. There are other books that cover the use of Office 365, but this book focuses on the actual integration of Office 365 with on-premises technologies. This integration is often necessary for organizations that already have, and might need to continue to have, some level of on-premises infrastructure for administration or other purposes.

For example, most organizations have Microsoft Active Directory (AD) as an identity management solution and have built groups, policies, and processes based on AD identities. AD is the premium identity management solution and is not intended to be replaced by Office 365. Office 365 leverages on-premises technologies such as AD for security and authentication purposes. There are also organizations that currently have on-premises email systems. They have the option to migrate all or some of those systems or simply adopt portions of email functions in Office 365. These are all examples of enterprise-level decisions that organizations face, and this book addresses these types of real-world implementations and administration.

Who this book is for

This book is intended for Information Technology (IT) system architects who need to integrate Office 365 with existing on-premises technologies. It is also intended for subject matter experts in Exchange, SharePoint, and Lync who design migration and hybrid implementations of these specific Office 365 services. Although this book contains a lot of technical information, it can also serve IT leaders and decision makers such as Chief Information Officers (CIOs) by providing insight to the level of planning and effort required to integrate Office 365 with existing technologies. With that insight, IT leaders and CIOs can plan and budget their Office 365 projects accordingly. There are also security and compliance topics that security professionals will find useful because there are new and specific security considerations for adopting cloud services. This book is not intended for the typical end user or business user, nor is it intended to cover all the functionalities of Exchange, SharePoint, Lync, and Office.

Regardless of your role, we hope this book helps you methodically plan, integrate, and deploy Office 365 services in your organization. We also hope you will get a better understanding about deploying technologies that can make the Office 365 experience a great one for end users and administrators.

Assumptions about you

This book is designed for readers who have a fundamental understanding of Office 365 services, but possess technical expertise in the administration and configuration of the on-premises technologies equivalent to those services. Because Office 365 covers a breadth of technologies including SharePoint, Lync, Exchange, and Office, this book assumes that the audience for each of these technologies has the relevant expertise in configuring and administering these technologies prior to Office 365. In addition, this book includes information that can serve multiple audiences; because of this, it can serve as a great resource for an Office 365 implementation team of experts. During implementation, there is foundational work to complete in the areas of identity management, network assessments, security analysis, and migration planning. As such, this book assumes the readers in these areas have the operational expertise for managing AD, running network assessments, and making configuration changes to networking services such as Domain Name System (DNS), proxies, and firewalls. While not required, readers will benefit most from this book if they have a lab environment to implement the concepts covered in the book.

Conventions

This book uses special text and design conventions to make it easier for you to find the information you need.

Text conventions

Convention	Meaning
Bold	Bold type indicates keywords and reserved words that you must enter exactly as shown. Microsoft Visual Basic understands keywords entered in uppercase, lowercase, and mixed case type. Access stores SQL keywords in queries in all uppercase, but you can enter the keywords in any case.
Italic	Italicized words represent variables that you supply.
Angle brackets < >	Angle brackets enclose syntactic elements that you must supply. The words inside the angle brackets describe the element but do not show the actual syntax of the element. Do not enter the angle brackets.

Convention	Meaning
Brackets [ ]	Brackets enclose optional items. If more than one item is listed, the items are separated by a pipe character (|). Choose one or none of the elements. Do not enter the brackets or the pipe; they're not part of the element. Note that Visual Basic and SQL in many cases require that you enclose names in brackets. When brackets are required as part of the syntax of variables that you must supply in these examples, the brackets are italicized, as in *[MyTable].[MyField]*.
Braces { }	Braces enclose one or more options. If more than one option is listed, the items are separated by a pipe character (|). Choose one item from the list. Do not enter the braces or the pipe.
Ellipsis …	Ellipses indicate that you can repeat an item one or more times. When a comma is shown with an ellipsis (,…), enter a comma between items.
Underscore _	You can use a blank space followed by an underscore to continue a line of Visual Basic code to the next line for readability. You cannot place an underscore in the middle of a string literal. You do not need an underscore for continued lines in SQL, but you cannot break a literal across lines.

Design conventions

INSIDE OUT

This statement illustrates an example of an "Inside Out" heading

These are the book's signature tips. In these tips, you get the straight scoop on what's going on with the software—inside information about why a feature works the way it does. You'll also find handy workarounds to deal with software problems.

Sidebar

Sidebars provide helpful hints, timesaving tricks, or alternative procedures related to the task being discussed.

TROUBLESHOOTING

This statement illustrates an example of a "Troubleshooting" problem statement

Look for these sidebars to find solutions to common problems you might encounter. Troubleshooting sidebars appear next to related information in the chapters. You can also use "Index to Troubleshooting Topics" at the back of the book to look up problems by topic.

Cross-references point you to locations in the book that offer additional information about the topic being discussed.

CAUTION!

Cautions identify potential problems that you should look out for when you're completing a task or that you must address before you can complete a task.

Note

Notes offer additional information related to the task being discussed.

Acknowledgments

Writing a technical book is a challenging yet rewarding experience. Writing a technical book that covers a new technology offering that is rapidly changing and covers the core Microsoft enterprise software takes the experience to an entirely different level. After reading this book, we hope you can appreciate how innovative Office 365 really is. It is a well-planned service with technologies and options to address almost every business scenario. When we meet with organizations that want to adopt Office 365, they often are overwhelmed by its complexity. Our answer to the complexity question is both "yes" and "no." Office 365 can be very easy to adopt. Just turn it on and it is ready. On the other hand, it can be complex if you have a complex environment with complex business needs. To address complex business scenarios, the service needs to be sophisticated. In this book, we provide simple, step-by-step procedures to ease your way through even the most complex scenarios.

We wrote this book during the preview period of the latest release of Office 365. We have made every attempt to continually update the information as we developed the book. However, due to the rapid update cadence of Office 365, the screen shots and information presented here might vary from your environment. Even so, the significant core concepts should remain consistent with the current Office 365 offering.

There are a number of people who have made this project possible. First, the authors would like to thank the great teams at and Microsoft Press for the opportunity to write this book. We also would like to thank Kenyon Brown, our senior editor, for his patience and valuable guidance throughout the project; Kara Ebrahim, our production editor, and her team for making the book look so aesthetically pleasing; and Barbara McGuire, our copy editor, for her excellent edits and valuable comments. We want to thank all our technical reviewers and subject matter experts, who behind the scenes validated all the material and provided very important feedback and corrections. They are Scott Wold, Darryl Kegg, Mark Ghazai, Stephen Jones, Jeremy Chapman, Yann Kristofic, Andreas Kjellman, and Darren Carlsen. We want to thank King County's CIO Bill Kehoe and many other IT leaders and technical experts in other organizations who have been willing to share their experience with us and give us the opportunity to work on their Office 365 projects. Without the vision and courage of these early adopters, it would not have been possible to provide all the real world experience we tried to capture in this book. We also thank the executive management at Microsoft for their support of this project, especially Jeff Tozzi, Dave Rogers, Javier Vasquez, Tori Locke, Dean Iacovelli, and Keith Olinger. Last but not least, we would like to thank the wonderful account teams at Microsoft we worked with, especially Steve Finney, Abel Cruz, Mark Wernet, Chris Wilch, Benjamin Callahan, Steve Kirchoff, Steven Fiore, Tara Larson, Bjorn Salvesen, Arshad Mea, Rick Joyer, Dan Crum, and Adam Loughran.

Julian Soh

This book has been one of the most challenging projects I have ever undertaken. There is so much material that we struggled to keep the scope of the book in check. This book truly has given me the opportunity to gain a deeper appreciation for the innovation, intricacies, and the possibilities that Office 365 offers.

This experience has helped me grow professionally, and I appreciate all the authors who have come before me because it is a huge personal investment in time and commitment for any author. Most importantly, I have been humbled by so many experts who have helped make this book possible. I sincerely would like to thank the efforts of my co-authors Marshall Copeland and Anthony Puca. Not only are they experts in their field, they have been great friends. I am humbled by their expertise and professionalism. I will always treasure this journey we have shared together, and I feel very blessed to have friends like you. I want to personally thank my Office 365 field team for making it such a great place to work and for your unselfish sharing of information. So thank you Bob Ballard, Carl Solazzo, Chuck Ladd, Dennis Guzy, Erika Cheley, Jed Zercher, Joel Martin, Michael Icore, Mike Hacker, Monica Hopelian, Scott Derby, Tim Gade, Stephen Jones, Brian Burns, and Scott Wold.

Finally, I would be remiss if I did not thank my family. I spent many days away from them. They also put up with my multi-tasking between writing chapters and trying to participate in family events. My wife Priscilla has been ever supportive and selfless in taking on all the extra work around the house. Thank you to my daughters Jasmine and Makayla for their understanding and for sacrificing some of our time together for this project. Jasmine, thank you for all the green tea you made me while I was busy typing away late into the night and for taking over the mowing of the yard.

To all these very important people in my life, I dedicate this book to you.

Marshall Copeland

Writing a book is a tremendous undertaking, and I would like to thank my beautiful wife Angela for her patience during the many evenings and weekends I spent hovered over a keyboard. She supports my hectic work with travel for public and customer speaking while keeping me grounded with incredible insight on what's important. For Cecil, Frances, and Barbara. We miss you.

Words are not enough to thank Julian Soh for offering me a seat on this voyage. It became very clear that to be a subject matter expert is quite different from trying to teach others by writing about a subject. Julian, merely saying "thank you" can't express my gratitude enough. Also, I want to thank Anthony Puca for his daily expertise with System Center and the insight he offered during our many conversations. A big thank you to Keith Olinger and Jeff Tozzi for their support during the writing of this book and for being two great people

with amazing guidance to help me grow. You both pour so much effort into everyday work that our entire team is lifted, and we thank you.

Thank you to the many customers who continue to ask "what if" questions and allow me to provide insight to help each of you move forward. Thank you to Bill Gates and Steve Ballmer for building a fantastic company called Microsoft, the best place to work. A special thank you to Charles Fox for helping me see the right direction when I could not. Thank you to Mark Ghazai for all the Windows PowerShell guidance and Hyper-V understanding.

Anthony Puca

I would like to say thank you to my wife Laura for being so understanding during all the nights I was working on this book, taking phone calls when we were on vacation or weekends, and going through this all over again with me. Our rendezvous at the dinner table, when we were trying to keep to the schedule and you were in the middle of your busy season, will not be forgotten.

When two friends, Julian Soh and Marshall Copeland, asked me to accompany them on this effort, I was honestly flattered. Special thanks go to Julian for coming up with the idea and driving it through; we could not have done this without you. Thank you, Marshall and Julian, for being my sounding board, for providing sanity checks and peer reviews, and for all the insightful conversations during those late night and weekend calls.

Working at Microsoft has given me access to some of the most talented, brightest, and passionate people in information technology. Thank you to all of you who contributed in some fashion. Thank you to Keith Olinger, Dave Rodgers, Bob Ballard, and their teams for their support. Thank you to Mark Ghazai and Marek Tyszkiewicz for all the Windows PowerShell scripting. Thank you to Anna Timasheva for your System Center Operations Manager (SCOM) expertise. Thank you to Jeff Tozzi for growing an amazing group that supports state and local government in the U.S. Thank you to my account teams who remind me of the value these things provide to the customers and public: Mark Starr, Nathan Beckham, Todd Strong, Adam Loughran, Elisa Yaros, Bobby Bliven, Don Born, and Kris Gedman.

Support & feedback

The following sections provide information on errata, book support, feedback, and contact information.

Errata

We've made every effort to ensure the accuracy of this book and its companion content. Any errors that have been reported since this book was published are listed on our Microsoft Press site at:

http://aka.ms/Office365_Admin_IO_errata

If you find an error that is not already listed, you can report it to us through the same page.

If you need additional support, email Microsoft Press Book Support at *mspinput@microsoft.com*.

Please note that product support for Microsoft software is not offered through the addresses above.

We want to hear from you

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

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

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

Stay in touch

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

CHAPTER 3

Active Directory Federation Services

MICROSOFT Active Directory Federation Services (AD FS) provides single sign-on (SSO) by using token-based authentication. With SSO, a service will trust the authentication token of a user who has successfully logged on to a disparate but trusted network. As such, the service will grant access without requiring the user to authenticate again. For example, if a user has already been authenticated by Active Directory (AD) and if SSO is configured, Office 365 will provide access to the user without a challenged logon.

SSO through AD FS is not mandatory for Office 365, but enterprise customers usually implement it because of the need or desire to leverage existing identity management solutions such as AD. Remember, too, that we said the user is the most important part of the equation. SSO optimizes the users' experience because they don't need to provide credentials multiple times.

AD FS is commonly considered and discussed together with directory synchronization, which is covered in Chapter 4, "Directory Synchronization."

Note

Office 365 SSO is not available for Office 365 for professionals and small businesses or for Office 365 Small Business Premium Preview. For more information, see KB article 2662960 at *http://support.microsoft.com/kb.2662960*. SSO is available only for Office 365 Enterprise Suites.

Different types of user accounts

Before we dive into AD FS, we need to introduce the different types of user accounts and authentication methods available in Office 365.

As with any computer system, a user needs an account to access Office 365. This chapter covers the different ways in which user accounts can be created and maintained. We also describe the user experience when accessing Office 365 based on the different account types.

There are essentially two classes of user accounts:

- Cloud identity
- Federated identity

Cloud identity

Cloud identities are user accounts that are created directly in Office 365 through the admin center. The passwords associated with cloud identities are also stored in Office 365. Cloud identities can be managed through the admin center as well as through Windows PowerShell. Windows PowerShell provides you with account management capabilities that might not be available through the admin center. For example, you can assign user passwords or remove password expiration dates by using Windows PowerShell, but these options are not available in the admin center. Windows PowerShell also opens the door for automation and bulk processing of accounts. We will dive deeper into Windows PowerShell in later chapters because Windows PowerShell is definitely the tool of choice for administering Office 365 at the enterprise level.

When a user tries to access an Office 365 service, she will be prompted for a logon name and a password, as shown in Figure 3-1. The user name and password will be validated by Office 365 before access to services is granted. For cloud identities, Office 365 is the authoritative authentication source known as standard authentication.

Federated identity

Federated identities refer to user accounts that are maintained outside of Office 365, such as in AD. Federated identities are the most commonly used accounts in an enterprise because most enterprises already have an identity management solution such as AD. Because Office 365 is built to be enterprise-ready, it will leverage your AD environment. We discuss other non-AD identity management solutions in later chapters, but for now we will assume AD as the authoritative identity source.

There are many benefits to leveraging your AD environment. For one, AD is most likely mature and you have already configured features such as Group Policy Objects (GPOs) that define password complexity requirements. Furthermore, from a day-to-day management standpoint, you and your administrators are probably using tools such as the Active Directory User and Computer (ADUC) management console. In this scenario, if you introduce cloud identities with Office 365, you would have to maintain a second set of user accounts in Office 365, thereby doubling your workload.

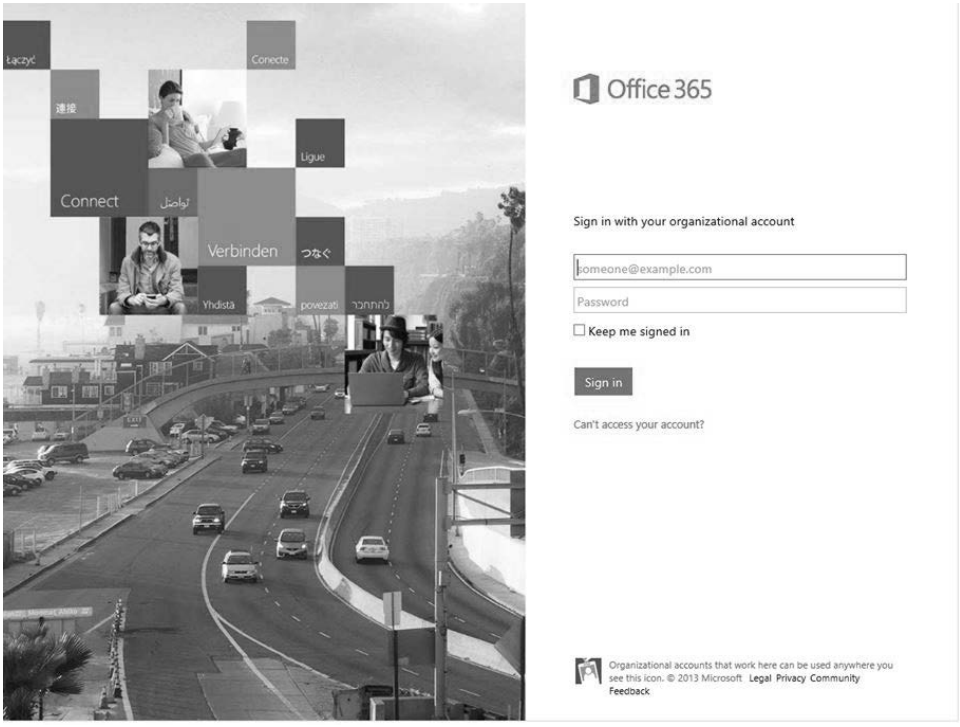

Figure 3-1 Office 365 logon window.

For example, let's say you create a new user account for a new employee in AD and that user requires access to Office 365. Without federated identities, you will have to manually create and maintain a corresponding user account in Office 365 for the new employee. Whenever an employee leaves your organization, you will have to ensure you delete, or disable, the user account in Office 365 in addition to deleting or disabling the employee's account in AD. Therefore, while cloud identities can be used in an enterprise and are easy to implement, they are definitely not the best approach from a long-term, administration standpoint.

Integrating Active Directory with Office 365

To fully leverage AD in Office 365, follow these general steps:

- Add your domain name to your Office 365 tenant.
- Set up and configure SSO through AD FS (optional; we cover this process later in this chapter starting with the "Active Directory Federation Services" section).
- Install and configure the Directory Sync tool (covered in Chapter 4).

> **Note**
>
> **If you know you will be implementing SSO, we recommend you implement it prior to installing the Directory Sync tool. However, it is not uncommon for organizations to first implement directory synchronization before AD FS. In fact, in our experience, this has been quite a common approach.**

The first step to integrating AD with Office 365 is to add your domain name to your Office 365 tenant. To do so, you first need to own a fully qualified domain name (FQDN). A fully qualified domain name is defined as a routable Internet domain name, such as .com, .net, or .org. A non-routable domain name, such as .lcl or .local, cannot be added.

Adding your domain name to Office 365

You can add your domain name to Office 365 through Windows PowerShell scripting. For now, we will use the graphical interface to accomplish this task:

1. Log on to your Office 365 admin center at *https://portal.microsoftonline.com* and click the domains link, as shown in Figure 3-2.

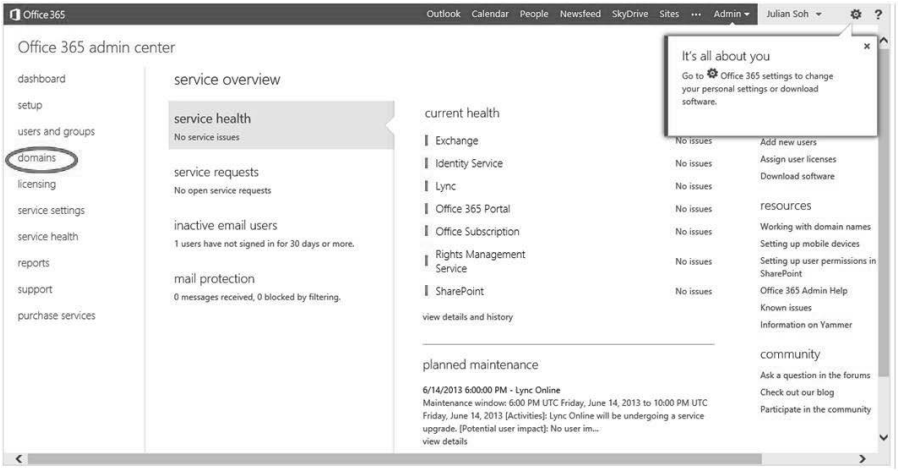

Figure 3-2 Office 365 admin center.

The domains page shows all the domains your Office 365 tenant is associated with and their respective status. As you can see, you can associate multiple domains to a tenant. However, once a domain has been associated to an Office 365 tenant, you will not be able to associate that same domain to another Office 365 tenant. By default, you should at least see the domain name that you used to first sign up for Office 365. It should be in the form of <*Name*>.onmicrosoft.com.

2. To associate a domain to this tenant, click the Add a domain link, as shown in Figure 3-3.

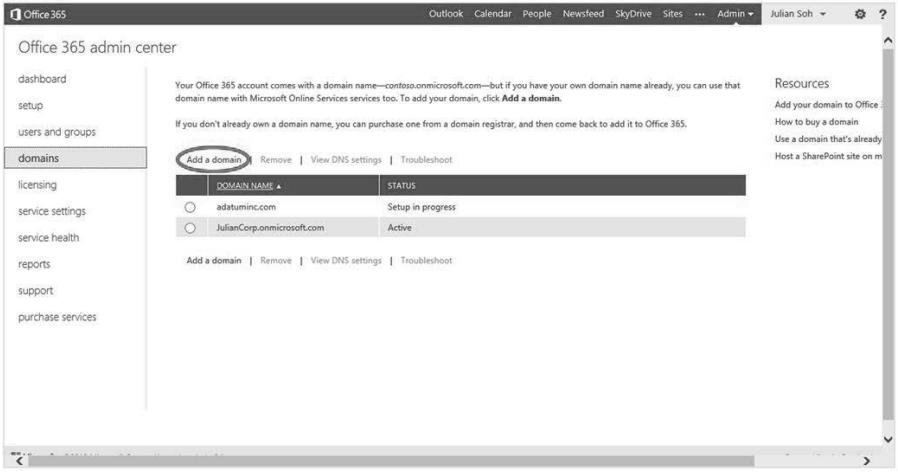

Figure 3-3 Add a domain.

3. Click Specify a domain name and confirm ownership.

4. Enter your domain name in the text box and click next, as shown in Figure 3-4.

Remember that you can add only an Internet routable domain, and the domain you specify must not have been previously associated with another Office 365 tenant. Do not worry if you do not remember whether a domain has been associated with another tenant. You will be notified if that is the case.

5. After you click next, Office 365 informs you if the domain has been previously associated. If not, you can proceed to the next task, which is to verify the domain.

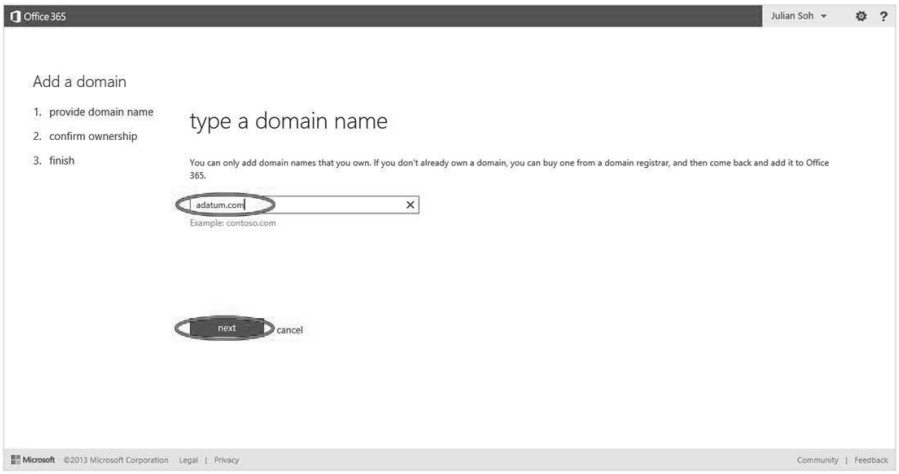

Figure 3-4 Enter your domain name.

You now need to confirm you own the domain and have the authority to add this domain name to Office 365. Office 365 asks you to create a TXT record in your Domain Name Service (DNS) server that is authoritative for the domain you just added. Office 365 also lists instructions on how to do this if your DNS is hosted by an Internet Service Provider (ISP) or registrar such as Go Daddy.

1. Select your ISP to view the specific instructions or select General Instructions if you are hosting your own DNS, which is often the case for an enterprise. In this example, we will select General Instructions. Figure 3-5 shows the list of available instructions.

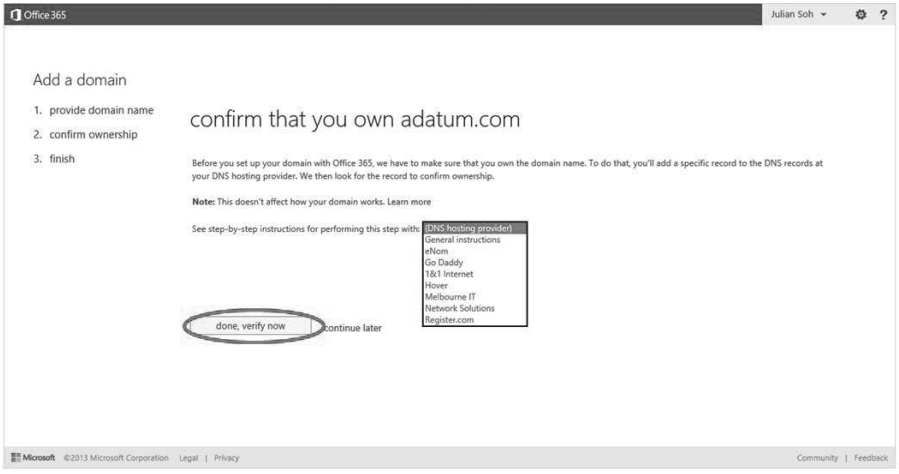

Figure 3-5 Confirm domain and instructions to modify DNS.

2. When you have selected the instruction that applies to you, the instruction will appear on the same page. In this example, when we selected General Instructions, we were given the option to create either a TXT record or an MX record in DNS that contains a unique number. During verification, Office 365 will resolve the domain through DNS and will attempt to locate these records. Personally, we have always used a TXT record instead of an MX record, but both options are available to you. Figure 3-6 shows information for General Instructions.

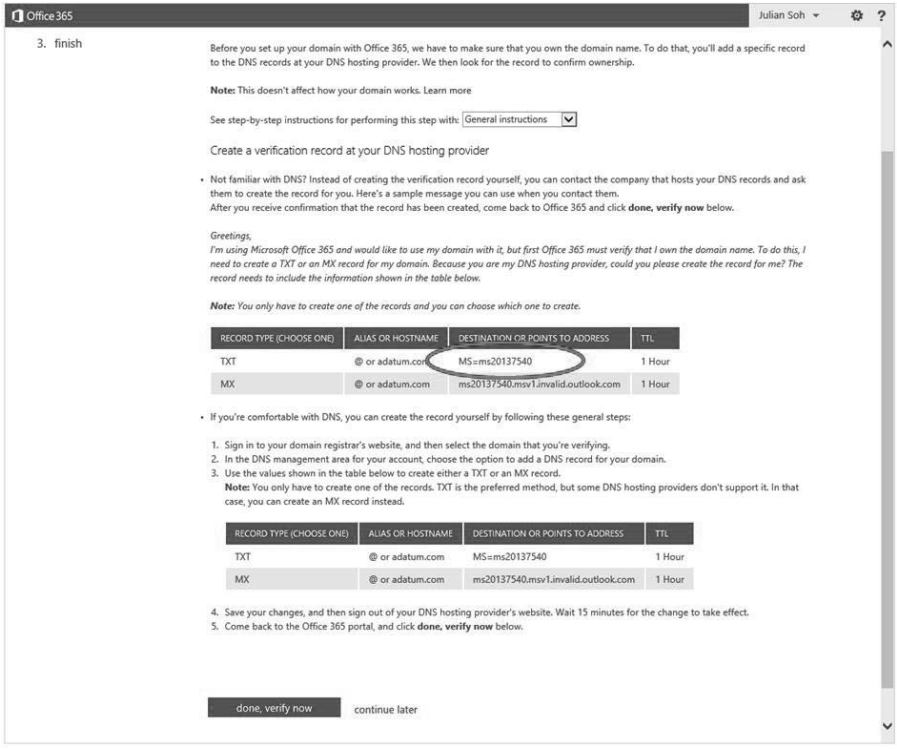

Figure 3-6 General Instructions to modify DNS.

3. Next, make the changes to your DNS. When you are done, click the done, verify now button. If you need more time or need to rely on someone else to make the DNS changes for you, just close the window. You can come back and verify the domain later.

Entering a DNS TXT record

In this section, we show you how to add the required TXT record to a Windows DNS server.

1. Log on to your DNS server. Using the Microsoft Management Console (MMC) for DNS, right-click the domain you are adding to Office 365 and select the Other New Records option, as shown in Figure 3-7.

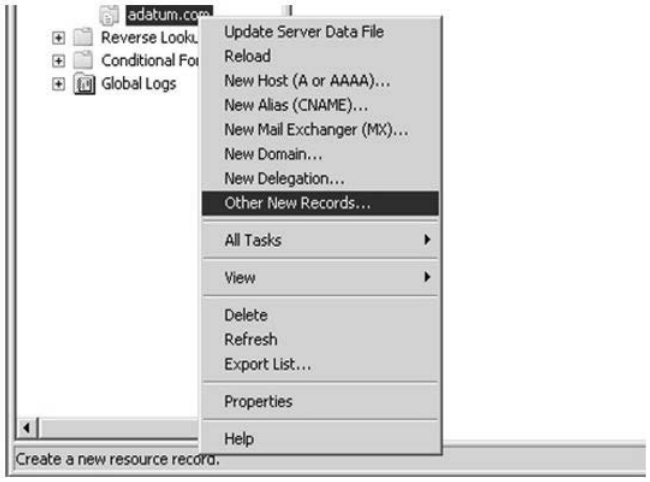

Figure 3-7 Microsoft Management Console for DNS server.

2. In the Resource Record Type dialog box, scroll down until you locate the Text (TXT) record type. Select it and click Create Record, as shown in Figure 3-8.

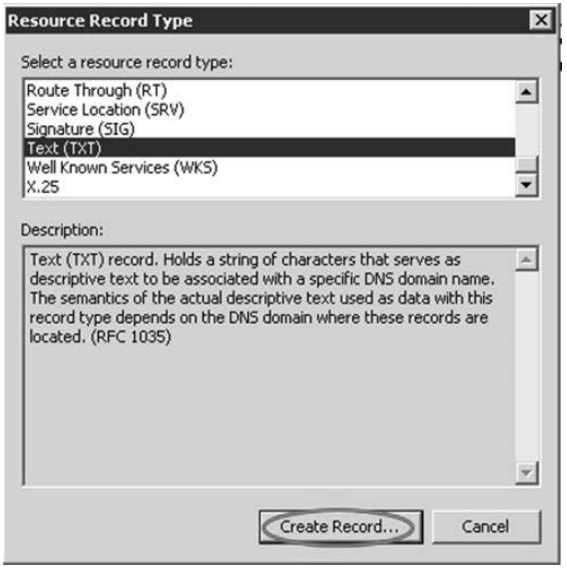

Figure 3-8 Create a Text (TXT) record type.

3. Lastly, as shown in Figure 3-9, leave the Record name field blank. In the Text field, enter the TXT record as instructed by Office 365 (see Figure 3-6, General Instructions to modify DNS). This usually takes the form of MS=ms1234567. When you are done, click OK.

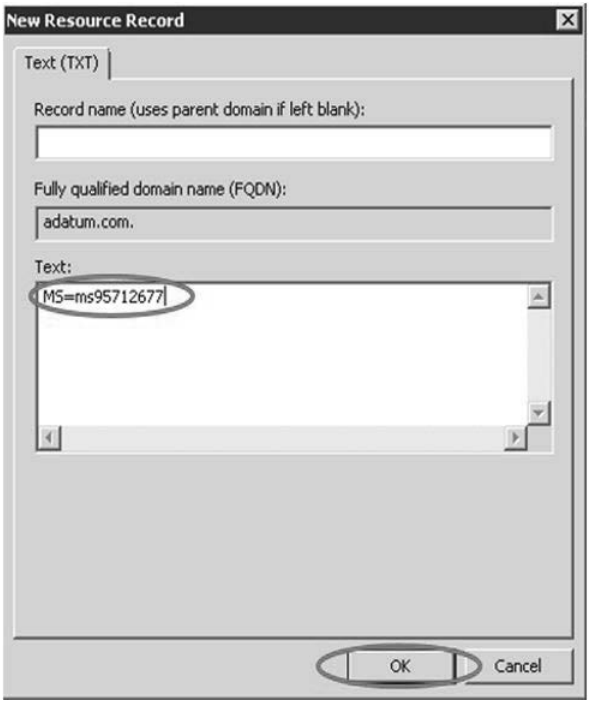

Figure 3-9 Creating the Text (TXT) record.

Verifying the domain

Now that we have created the TXT record, Office 365 will be able to verify that you have the authority to add the domain to your tenant. There is no need to wait for DNS convergence because Office 365 does not cache its DNS lookup of TXT records for domain verification purposes, so you can immediately start the verification process.

If you are still on the Office 365 page waiting for domain verification (see Figure 3-6) and if it has not yet timed out, you can click the done, verify now button. If you have to log on to the admin center again, follow these steps to confirm ownership:

1. From the admin center, click domains in the left pane, and then click the Setup in progress link in the Status column, as shown in Figure 3-10.

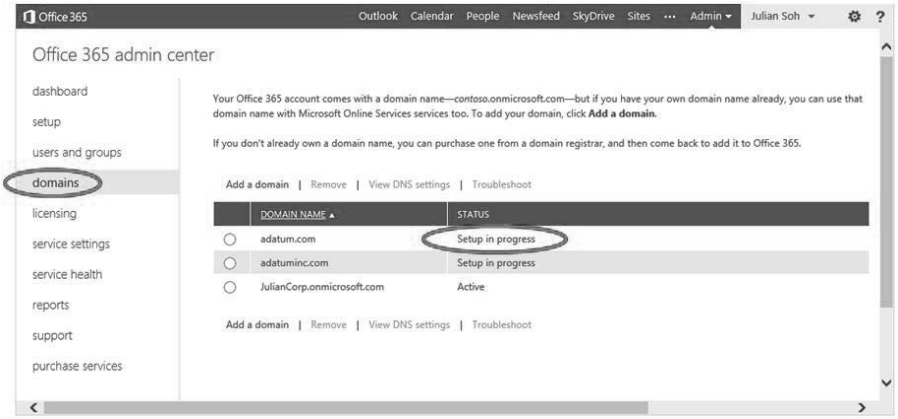

Figure 3-10 Domains page in the admin center.

2. Click Specify a domain name and confirm ownership.

3. Click the done, verify now button.

After your domain has been successfully verified, the next task is to specify how users will be added to Office 365.

Adding users and assigning licenses

We will explain how to add users through directory synchronization in Chapter 4. Therefore, we need to specify that users will be added at a later time. Follow these steps to specify that you will add users later:

1. If you are on the Add a domain page of Office 365, skip to the next step. Otherwise, from the admin center, click domains, and then click the Setup in progress link in the Status column, as shown in Figure 3-10.

2. On the Add a domain to Office 365 page, notice that the link in Step 2, which is Add users and assign licenses, is now active. Furthermore, the link in Step 1, which is Specify a domain name and confirm ownership, is no longer active and a check is shown for that step. This indicates you have completed the task. Click the Add users and assign licenses link.

3. Select the I don't want to add users right now option and click next.

You are now ready to finish the third task, which is to define the domain purpose and configure DNS.

Setting the domain purpose and configuring DNS

Setting the purpose of the domain means defining whether the domain will be used for Exchange Online, Lync Online, or SharePoint Online. Follow these steps to set the domain purpose:

1. If you are on the Add a domain to Office 365 page, skip to the next step. Otherwise, from the admin center click domains, and then click the Setup in progress link in the Status column, as shown in Figure 3-10.

2. At the Add a domain to Office 365 page, notice that the link in Step 3, which is Set the domain purpose and configure DNS, is now active. Furthermore, there are checks next to Steps 1 and 2 to indicate you have completed the tasks. Click the Set the domain purpose and configure DNS link.

3. On the Set up domain page, you have the option to choose Exchange Online, Lync Online, SharePoint Online, or any combination of the three. The screen to set the domain purpose will look similar to the one shown in Figure 3-11. Select the services you want to associate with the domain and click next.

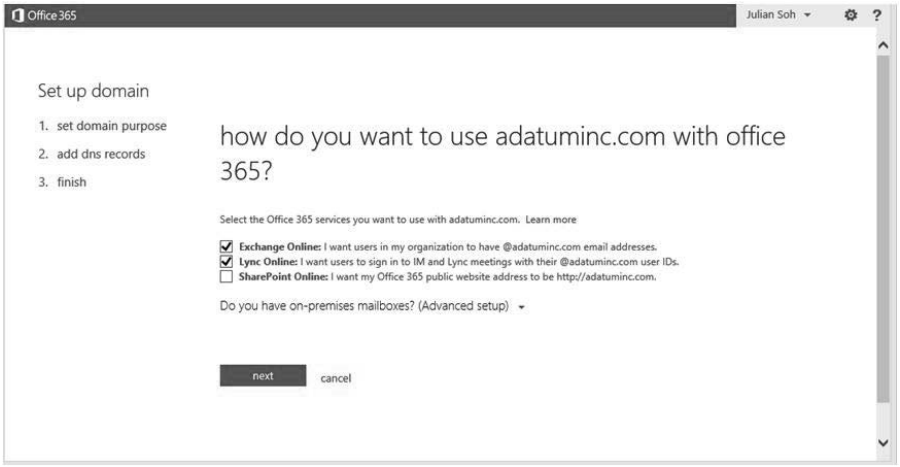

Figure 3-11 Set domain purpose.

4. Setting the domain purpose in the preceding step allows Office 365 to determine the necessary records you need to add to your DNS server, as shown in Figure 3-12. Office 365 does not manage DNS records but still provides services that require specific DNS entries for them to work. Add the records to your DNS server, then click done, go check. Office 365 will check that the DNS records are correctly created and will inform you if any errors are found. If there are no errors, you will receive a

message that the domain is ready to work with the Office 365 services you selected. The domain status will then be changed to Active instead of Setup in progress.

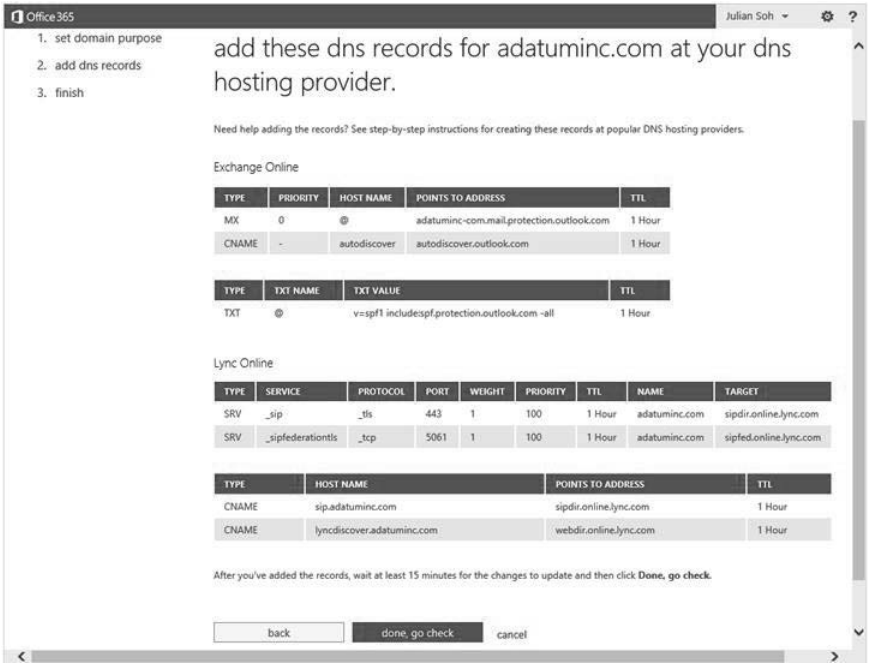

Figure 3-12 DNS settings for services that are associated to a verified domain.

> **Note**
>
> **Choosing to specify SharePoint Online as a service associated to your domain name provides you the capability to host a public-facing website. However, a public-facing SharePoint Online website is currently not intended to be a full-featured web content management solution. If you do choose to use a public-facing site, and also want to use Exchange Online and Lync Online, you will need to first associate Exchange and Lync. Save the changes and configure your DNS for Exchange Online and Lync Online, then come back to specify SharePoint Online as a service to associate with the domain name.**

Active Directory Federation Services

AD FS is a role in Windows Server. The most prominent and primary reason to use AD FS with Office 365 is that it allows an AD user to seamlessly access Office 365 without having to re-supply her credentials again. As mentioned earlier, this ability is often referred to as

single sign-on (SSO). AD FS is an optional implementation and is not required for Office 365. However, if your organization decides to implement AD FS, the minimum AD FS version required by Office 365 is version 2.0; thus, it is often referred to as AD FS 2.0.

However, aside from SSO, there are other benefits of AD FS. Because AD FS facilitates the authentication of users through AD, you can take advantage of group policies. AD FS can also control location-based access to Office 365. For example, if you want to allow employees to be able to access Office 365 only from the corporate environment and not from external networks, you can do so through AD FS and AD. If you require two-factor authentication, you must accomplish it with AD FS and SSO.

You can use AD FS for other purposes as well. A common use of AD FS is to federate with B2B partner networks. If you already have AD FS set up in your environment for other purposes, you might be able to use the existing AD FS infrastructure for Office 365. Likewise, after you set up AD FS for Office 365, you might be able to use it for other non-Office 365 business needs.

Single sign-on experience

Before we begin to install and configure AD FS 2.0, let us first take a look at the end-user experience when SSO with Office 365 is and is not in place.

Scenario 1: No single sign-on experience

In this scenario, a user is not authenticated through SSO. Each time the user attempts to access Office 365, he is prompted to supply a valid user name and password, whether he is attempting to access Office 365 from within the corporate network or from a public network logon.

Scenario 2: User is logged on at work

In this scenario, a user is at work and logs on to the corporate network. The enterprise AD authenticates the user so she has a valid claim token. When the user accesses Office 365 services, by opening Outlook to access email or by opening a browser to access the corporate intranet that is hosted in SharePoint Online, the Office 365 federation gateway will acknowledge the claim token and will not produce a logon prompt. This provides an SSO experience because the user does not need to present her logon credentials again.

Scenario 3: Remote worker on a virtual private network connection

A remote worker or teleworker is one who is not on the corporate network. Traditionally, these workers will use a technology such as a virtual private network (VPN) client to securely create an encrypted communication channel between their personal computers

and the corporate network. This is known as a tunnel within the public network. Because it is encrypted, the communication is deemed secure.

In this scenario, a user presents his logon credentials during the VPN session initialization. The credentials are passed to the corporate network. After authenticated, the user possesses a claims token, as in Scenario 2. At this point, if the user opens his email or accesses the corporate intranet that is hosted in Office 365, the situation will be the same as it is for the worker in Scenario 2. That is, the user will not be prompted for his logon credentials again.

Scenario 4: Remote worker is not logged on to the corporate network

In this scenario, a remote worker has access to the Internet through a non-corporate network, such as her home office or the public Internet provided by a hotel. She can choose to log on through VPN, but for the sake of discussion let us assume this user does not do so because she does not need to access any corporate resources on the corporate network. Instead, she only wants to read email or access the corporate intranet that is hosted in Office 365. So she opens a browser and enters the uniform resource locator (URL) of the corporate intranet. Because she is not authenticated by AD, either locally or through VPN, she does not possess a valid token.

Office 365 presents the user with the Office 365 logon window, as shown in Figure 3-1. The user attempts to log on using her User Principal Name (UPN) user name. Office 365 recognizes that the user is trying to log on with a UPN suffix belonging to a domain that is federated and thus redirects the user to the AD FS server, as shown in Figure 3-13. The federation server presents a logon window to obtain the user's credentials. The user successfully enters her credentials and is issued a valid claim token. She then is redirected back to Office 365, where she is now granted access to Office 365 services.

In light of the different scenarios, it is a good idea to have a communication plan so you can communicate to your users what they will see when AD FS and SSO are in place.

Single sign-on requirements

The minimum requirements for setting up SSO with AD FS for Office 365 are divided into AD requirements and AD FS server requirements.

The server requirements to install the AD FS role are straightforward:

- AD FS must be installed on a server that is joined to a domain and running either Windows Server 2008 or Windows Server 2008 R2.
- AD FS 2.0 or above must be installed on a domain controller (DC).

Figure 3-13 Office 365 logon portal redirecting you to sign in through the AD FS server.

- Internet Information Server (IIS) must be installed.
- Deployment of an AD FS 2.0 or above proxy server if you plan to allow users to connect from outside the company network. While an AD FS proxy is recommended, it is not required. Furthermore, the AD FS proxy and AD FS server cannot be set up on the same machine.

AD requirements to implement AD FS 2.0 for Office 365 can be more complex and impactful. The following are the AD requirements:

- AD with a minimum functional level of Windows Server 2003 in mixed or native mode.
- AD default UPN must be identical to the domain name you added in the preceding section.

For more information about AD FS requirements, see *http://technet.microsoft.com/en-us/library/dn151311.aspx*.

> **Note**
>
> **User Principal Name (UPN) is the most common problem we see in AD. Most companies implemented AD many years ago when the Internet was still young and cloud computing was virtually unheard of. The Internet was considered the wild west with all its promises and dangers. Back then, a common security best practice was to give AD a non-routable UPN. The common UPN suffix used is typically .lcl or .local. The reason why Office 365 requires a valid UPN suffix is twofold. One, we will be creating a federation between Office 365 and the local AD during the AD FS installation. This requires the domain to be added to Office 365 as we saw earlier in the chapter. Adding the domain to Office 365 requires the validation of a TXT or MX record through DNS, so the domain needs to be valid and routable. Second, when we install directory synchronization, the user name for an Office 365 account is in UPN format (example <*User Alias*>@adatum.com). The Directory Sync tool uses the UPN of the local AD to create the user account in Office 365. If the UPN of the local AD is not added and verified in Office 365, as will be the case with a non-routable UPN, then the user will be created with the default onmicrosoft.com UPN suffix that was created when the Office 365 tenant was created (example: <*User*>@adatum.onmicrosoft.com).**

Follow these general steps to implement SSO using AD FS:

- Remediate your AD UPN suffix.
- Install IIS on the server that will host AD FS.
- Protect IIS with an Secure Sockets Layer (SSL) certificate.
- Install and configure AD FS 2.0.

Remediating the UPN suffix

The good news about remediating the UPN suffix in AD is that you do not need to replace your old UPN suffix if it is not federated with Office 365. In fact, you are not able to replace the original UPN that was used when you first created a forest.

A common reason why you need to add a UPN might be because the current one is not routable or you might not want to federate it for some reason. The solution is to add an alternate UPN suffix to your AD forest. To do so, you can use Windows PowerShell or the Active Directory Domains and Trusts MMC. The following steps show how to add a UPN with the Active Directory Domains and Trusts MMC:

1. Start the Active Directory Domains and Trusts MMC, as shown in Figure 3-14.

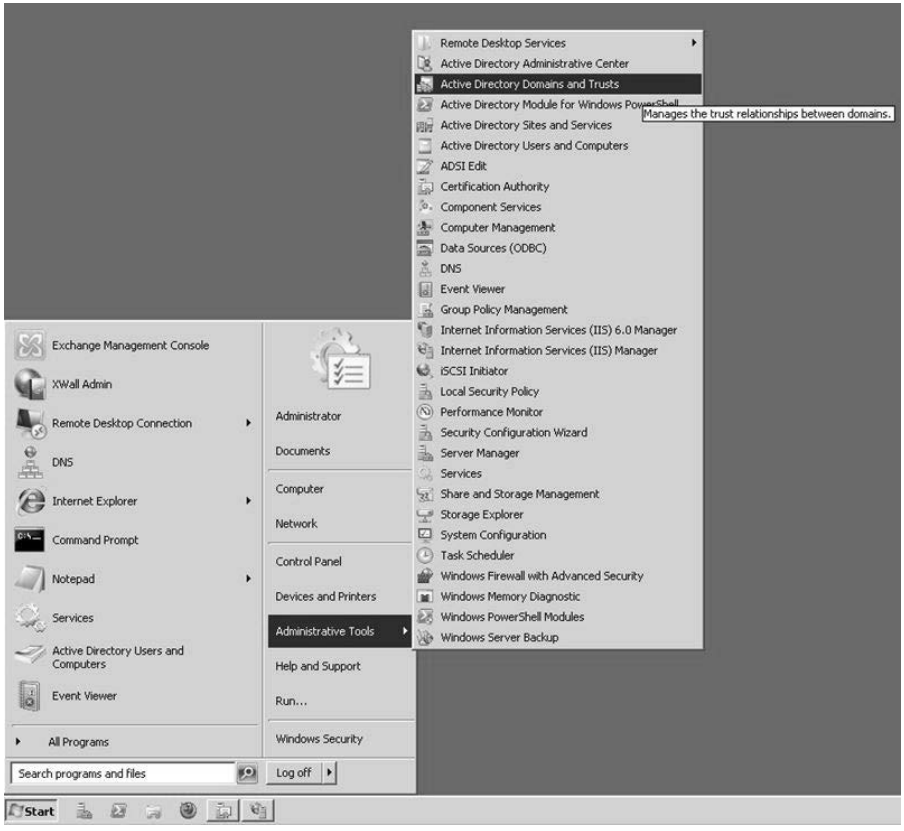

Figure 3-14 Active Directory Domains and Trusts MMC.

2. Right-click Active Directory Domain and Trusts and select Properties, as shown in Figure 3-15.

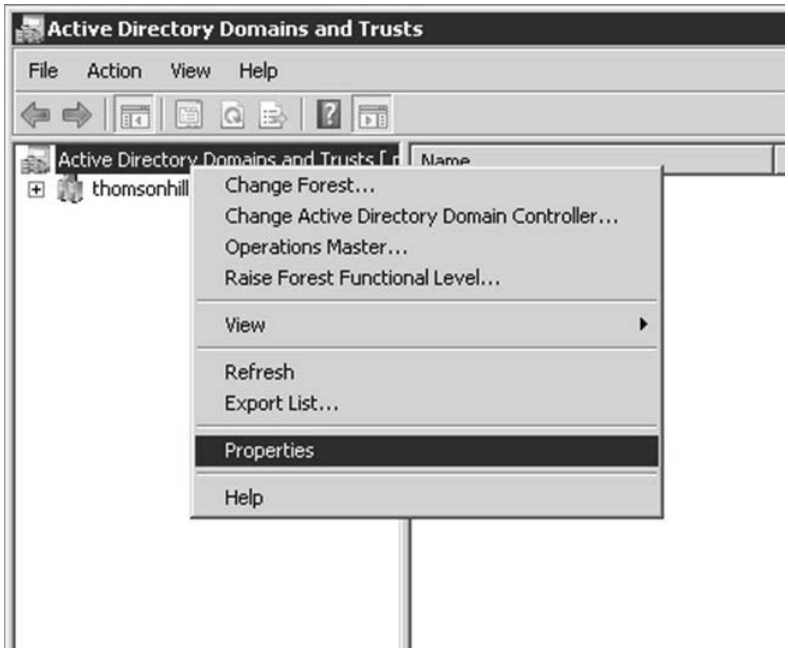

Figure 3-15 Accessing the properties of the AD UPN.

3. On the UPN Suffixes tab, enter the domain name you associated with Office 365 and click Add. Do not type @ before the UPN suffix because it will be added automatically. For example, to add adatum.com as an alternate UPN suffix, type adatum.com and not @adatum.com, as shown in Figure 3-16.

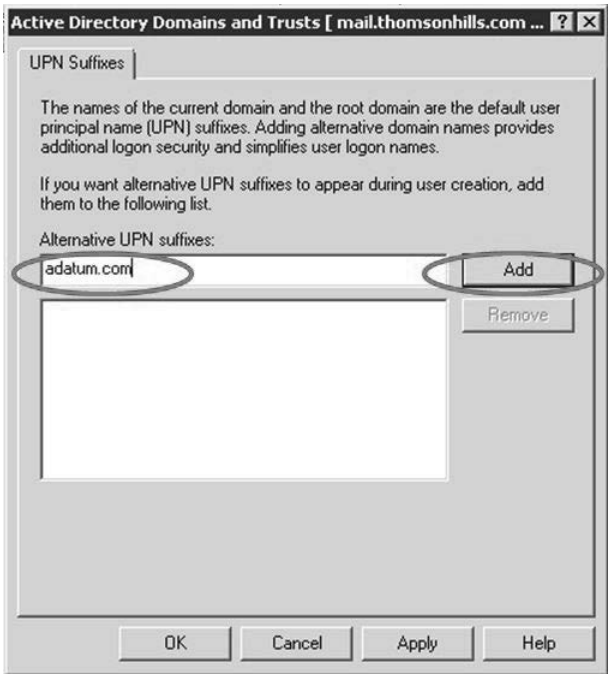

Figure 3-16 Adding an alternative UPN to the forest.

4. Click OK.

Now that you have added an alternative UPN to the forest, it will appear as an option in the user logon name settings in the Active Directory User and Computers (ADUC) MMC when you create a new user, as shown in Figure 3-17. All the UPN suffixes listed here will be associated with the user logon, but the one that is selected is known as the default UPN suffix. The default UPN suffix is the one that will be used by the Directory Sync tool to create the user in Office 365, so it is important to select the correct default UPN suffix when creating the user.

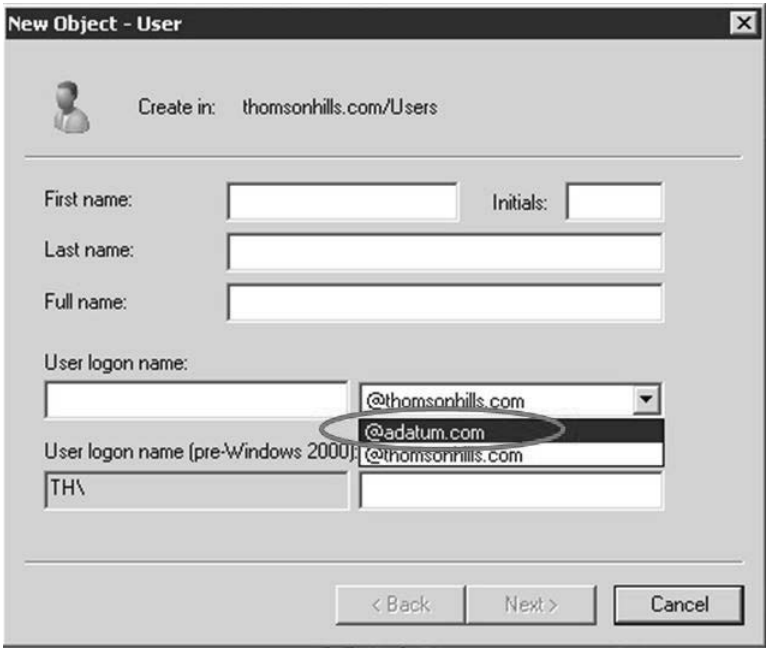

Figure 3-17 Setting the default UPN suffix when creating a user in ADUC.

It is not possible to change the default UPN suffix because it is associated with the AD forest when the forest was first created. Therefore, you will need a way to properly set the UPN suffix of all previous users to the correct default UPN suffix so that Directory Sync can correctly create the Office 365 account. You will also need to select the correct UPN suffix for new users at the time they are created. This can be done manually, as shown in Figure 3-16. This can also be automated using several methods such as Windows PowerShell or through Forefront Identity Manager (FIM). Automation is the preferred approach because it is easy to forget to set the correct default UPN suffix for new users.

Windows PowerShell is also the method you will use to bulk set users' default UPN, either organization-wide or by OU.

The following Windows PowerShell script updates the UPN suffix of all users in a particular OU:

```
#Script to update the UPN suffix
#Replace the fields indicated with <> with actual field names

import-module ActiveDirectory

Get-ADUser -SearchBase "ou=<OU Name>,dc=<domain name>,dc=<com or org or net>"
-SearchScope OneLevel -filter * |
ForEach-Object {
```

```
        $newUPN = $_.UserPrincipalName.Replace('<currentUPNsuffix>', '<newUPNsuf-
fix>')
        $_ | Set-ADUser -server <servername> -UserPrincipalName $newUPN
       }
```

The next sample script updates an entire domain, instead of just a single OU, to replace the default UPN suffix of thomsonhills.com to adatum.com. The *-whatif* parameter is used so that when the script is run, it shows the effects of the script without actually making any changes. If the output is what you expect, then remove the *-whatif* parameter to have the script make the changes when you run it. Figure 3-18 shows a script being executed in the Windows PowerShell 3.0 Integrated Scripting Environment (ISE).

```
import-module ActiveDirectory

Get-ADUser -SearchBase "dc=thomsonhills,dc=com" -SearchScope subtree -filter * |
ForEach-Object {
        $newUPN = $_.UserPrincipalName.Replace('thomsonhills.com', 'adatum.com')
        $_ |
        Set-ADUser -server mail -UserPrincipalName $newUPN -whatif
       }
```

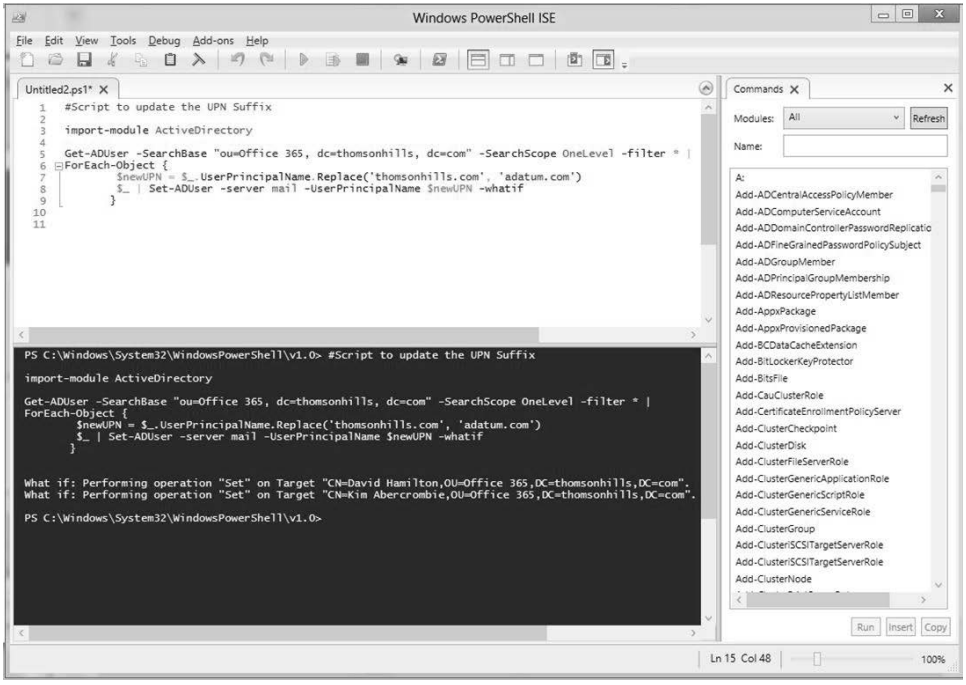

Figure 3-18 Windows PowerShell Integrated Scripting Environment (ISE) modifying the UPN suffix.

> **Note**
>
> **A user can authenticate to AD through the UPN or by the legacy NetBIOS method (*Domain**Username*). Adding an alternate UPN suffix and changing the default UPN suffix for users will not affect the NetBIOS logon method. When you add multiple alternate UPN suffixes, a user can log on with any of the UPNs, but Directory Sync will use only the default UPN suffix from the Office 365 account creation process. That is why it is important to make sure the default UPN is set to the domain associated with Office 365 or it will not be able to create the user with that UPN. Instead, Directory Sync will create the account with the default initial Office 365 UPN suffix, which is in the form of @<*CompanyName*>.onmicrosoft.com.**

Aside from the UPN suffix in AD, it is important to remember that Office 365 relies on AD attributes for information. For example, the Global Address List (GAL) information for users as well as distribution lists (DLs) rely on AD information. Therefore, you will need to ensure these attributes are populated in AD so the information will be available in Office 365.

Installing IIS on the AD FS server

AD FS requires the IIS role on the server. Install the IIS role by following these steps:

1. In Control Panel, select the Turn Windows features on or off option.
2. Select Roles in the Server Manager MMC.
3. In the Roles Summary pane, see if Web Server (IIS) is listed as an installed role. If you see it, then you are done and can skip the rest of the steps and go straight to the "Requesting and Installing Certificates" section.
4. If you do not see it, click the Add Roles link in the Roles Summary pane on the right.
5. Let the Add Roles Wizard guide you. When you are prompted to select roles to install, select the check box for Web Server (IIS).
6. Let the wizard guide you through the rest of the installation. Once complete, the IIS role will be installed.

You are now ready to protect the IIS Server with an SSL certificate for the default website.

Requesting and installing certificates

Now that we have IIS installed on the AD FS server, we need to address the issue of security certificates before we can install AD FS 2.0.

You need a security certificate to protect your AD FS server. AD FS relies on the IIS default website, which needs to be protected by an SSL certificate, to secure the communications between the client computer and the AD FS server.

Credentials are transmitted over this SSL connection, so it is important that the connection is encrypted. The SSL certificate also identifies the federation server, giving users confidence that they are authenticating to the organization and not a server impersonating as the organization.

Setting up the certificate is fairly straightforward. When you install the AD FS server later in the "Installing and configuring AD FS 2.0" section, you will see that the AD FS installation will use the default website in IIS, which is why we installed IIS first.

You have the option to purchase an SSL certificate from a known certificate authority (CA), or you can use your enterprise CA if you have one.

Creating the certificate request

Follow these steps to create a certificate request:

1. Click Start, click Administrative Tools, and then click Internet Information Services (IIS) Manager.

2. In the IIS MMC, select the IIS server. In the middle pane, scroll down until you see Server Certificates, then double-click the icon, as shown in Figure 3-19.

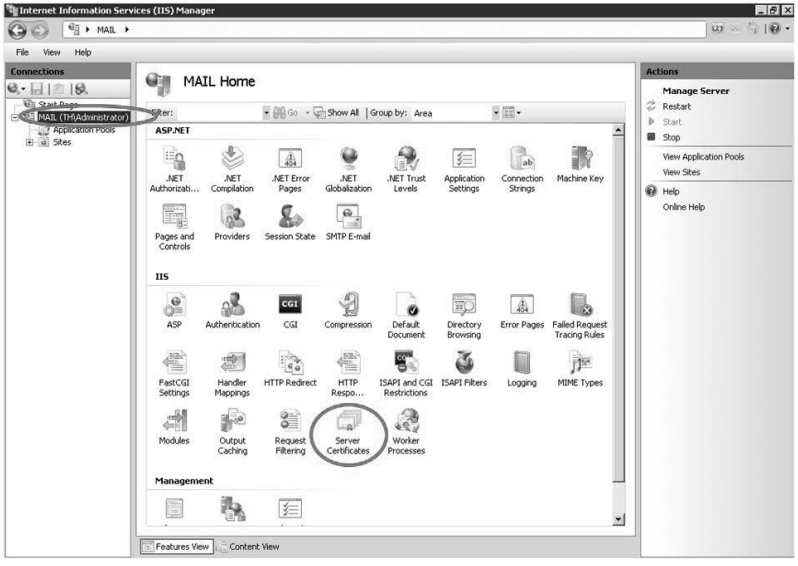

Figure 3-19 Select the Server Certificates option in IIS Manager MMC.

3. In the Actions pane, select Create Certificate Request, as shown in Figure 3-20.

Figure 3-20 Create Certificate Request.

4. Complete all fields in the Distinguished Name Properties page of the Request Certificate Wizard, as shown in Figure 3-21. Note that in the Common name text box, you should enter the fully qualified domain name (FQDN) of the federation service. For example, if you plan to refer to your federation service as *fs1.adatum.com*, then enter that FQDN in the text box. All fields are required. Click Next when you are done.

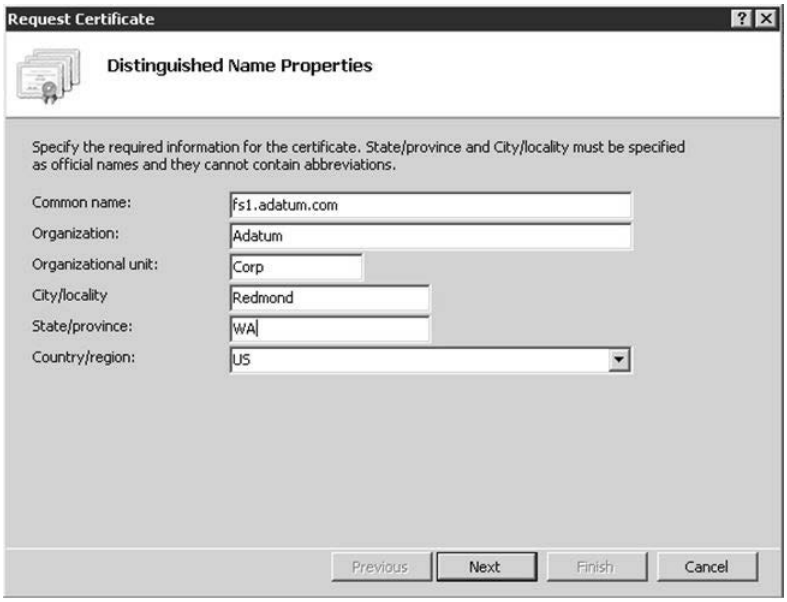

Figure 3-21 Information required for the certificate.

INSIDE OUT The controversy about wildcard certificates

Consider using wildcard certificates because they provide you the flexibility and convenience to change the host or service name without having to reissue the certificate. However, there is a long, ongoing debate about avoiding wildcard certificates as a security best practice. Whether you are a proponent of wildcard certificates or not will depend on your security posture and professional stance on this topic; however, this is beyond the scope of discussion for this book. We are simply pointing out that there are benefits to using wildcard certificates whenever there are name changes to servers and services involved, including the AD FS service.

TROUBLESHOOTING

Be careful of name duplication

It is important to make sure the FQDN federation service is NOT the same as the server name in AD. In fact, it should not be the same as any other server in AD. For example, let us say you want to refer to your federation service as fs1.adatum.com, but when you set up this server and joined it to AD you also named it fs1. In this case, you will need to change the server name to something else or the AD FS installation wizard will not be able to set the SPN during installation. For more information, see "AD FS 2.0: Guidance for Selecting and Utilizing a Federation Service Name" at *http://social.technet.microsoft.com/wiki/contents/articles/4177.aspx*.

5. On the Cryptographic Service Provider Properties page, we recommend that you select the Microsoft RSA SChannel Cryptographic Provider with a bit length of 2,048, as shown in Figure 3-22. Although a 1,024 bit length is acceptable, it is more susceptible to cryptanalytic attacks. For more information about certificates for AD FS, see *http://technet.microsoft.com/en-us/library/adfs2-help-certificates(v=WS.10).aspx*.

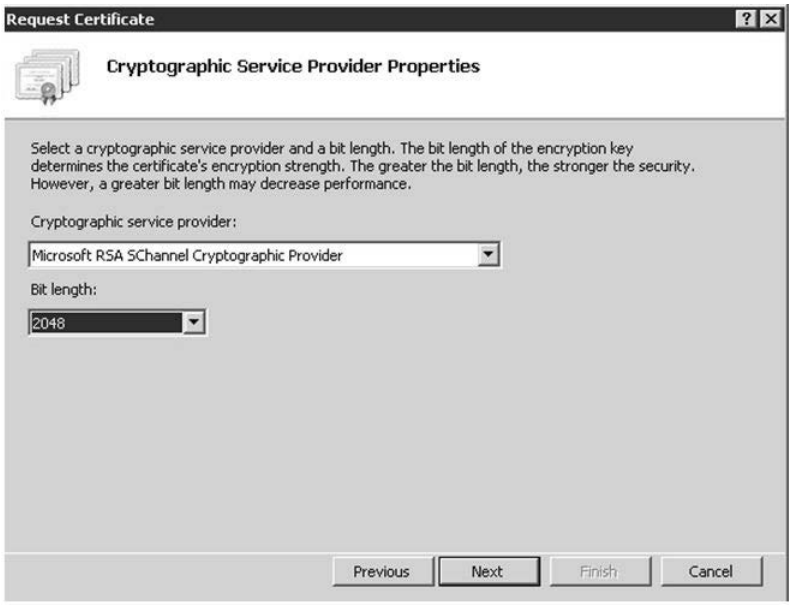

Figure 3-22 Cryptographic Service Provider Properties page with 2,048 bit length.

6. Lastly, specify a file name for the certificate request, which you will use with a third-party certificate provider or with your enterprise certificate authority.

7. Purchase an SSL certificate from a third-party certificate provider or use your enterprise PKI infrastructure if you have one. If you plan to purchase a certificate, skip the following "Using your enterprise certificate authority to issue a certificate" section and go to a domain registrar such as Go Daddy to purchase the certificate.

8. Enter the federation service FQDN in your external DNS because Office 365 will need to resolve the federation service to your AD FS server farm or proxy farm.

Using your enterprise certificate authority to issue a certificate

If you purchased your certificate from a third-party provider, you can skip this section. Otherwise, follow these steps to have your certificate server issue you a certificate:

1. From your enterprise CA server, click Start, All Programs, and Accessories. Right-click Command Prompt and select Run as administrator.

2. In the Command Prompt window, enter the following command:

```
certreq -submit -attrib "CertificateTemplate:WebServer" <path and file name of
Certificate Request file>
```

As shown in Figure 3-23, we issued the command and used Request.txt because that is the file name we used when we generated the certificate request earlier.

Figure 3-23 Using the *certreq* command on the CA server to issue a certificate.

Installing the certificate on IIS

Regardless of whether you purchased a certificate from a domain registrar or had your CA issue it, you should now have in your possession a certificate file, which usually has a .cer extension as part of the file name. Follow these steps to install the certificate on your IIS server:

1. On the AD FS server, start IIS Manager.

2. In the Connections pane, select the AD FS server, double-click Server Certificates in the middle pane, and click Complete Certificate Request in the Actions pane, as shown in Figure 3-24.

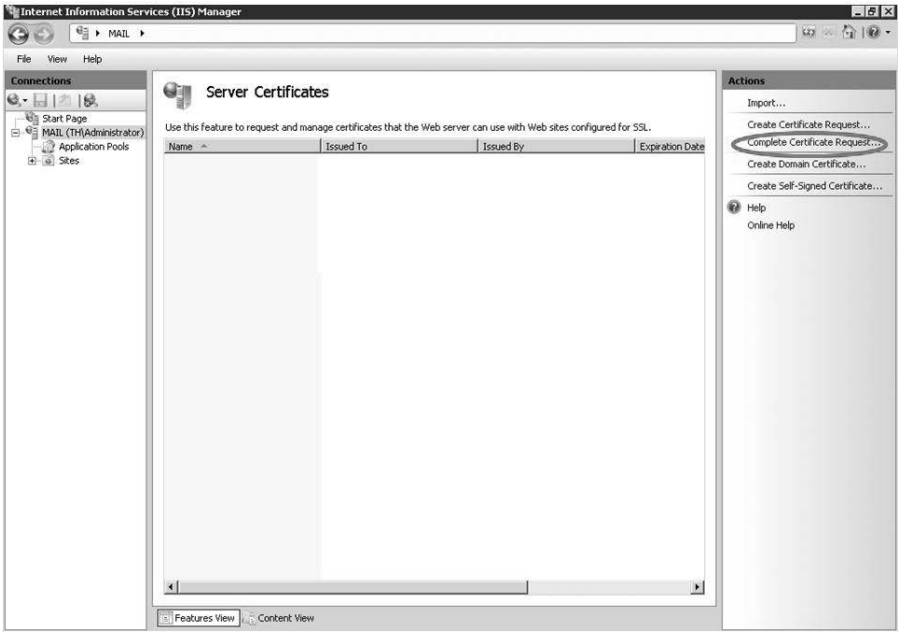

Figure 3-24 Complete Certificate Request in IIS Manager.

3. When prompted for the file name, browse to where you stored your .cer certificate file and select it. Give it a friendly name that will allow you to easily recognize it later, and complete the installation of the certificate.

Protecting the default website with the certificate

Now that we have installed the certificate, we need to use it for the default website. Follow these steps to apply the certificate to the default website:

1. From the AD FS server, start IIS Manager.

2. In the Connections pane, expand the ADFS server node, and then expand the Sites node. Right-click Default Web Site and select Edit Bindings, as shown in Figure 3-25.

Figure 3-25 Edit the bindings of the Default Web Site.

3. Select the HTTPS protocol in the Site Bindings window, and then click Edit.

4. In the drop-down box for SSL certificate, select the certificate you installed in Step 3. You should be able to recognize it by the friendly name you gave the certificate when you installed it.

5. Click OK when you are done, and then click Close.

Now the IIS server is ready to host the AD FS service. Next, we will plan for our AD FS infrastructure and carry out the installation.

Planning the AD FS architecture

When planning for AD FS, there are several considerations from a design standpoint:

- The number of AD FS servers in the farm
- Whether or not to deploy an AD FS proxy
- Whether to use the Windows Internal Database (WID) that comes with AD FS or use a dedicated SQL server for the AD FS database

AD FS server farm

The number of AD FS servers in the farm, which in turn determines the availability of the farm, is by far the most important design consideration because AD FS is the enabler for authentication through AD. There are other factors that might affect AD FS availability, such as network availability, that you also will need to take into consideration when designing your AD FS deployment. After you deploy AD FS for Office 365, if your AD FS servers are inaccessible, then access to Office 365 will not be possible. Therefore, it is important to build redundancy at the network and server layers.

At the very minimum, two AD FS servers in a single farm that is front ended with a load balancer will provide the needed redundancy. If one server is down for maintenance or for any other reason, authentication through the AD FS farm will still be possible and access to Office 365 will not be interrupted.

AD FS proxy

An AD FS proxy role is recommended if you plan to allow users to connect to Office 365 with SSO from outside the corporate network. Implementing an AD FS proxy is not required in this scenario, but it is a security best practice. Figure 3-26 shows a typical AD FS architecture.

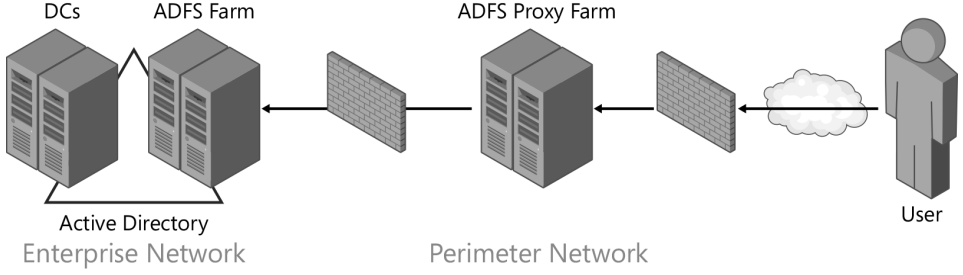

Figure 3-26 Typical AD FS and AD FS proxy implementation in an enterprise.

Implementing an AD FS proxy is beyond the scope of this book because it is more an of on-premises network and server infrastructure discussion rather than an Office 365 discussion. Therefore, we do not cover the process of implementing an AD FS proxy or how to implement redundancy through the deployment of server farms and failover clusters. However, in the following sections we show you how to install AD FS 2.0 on a server and how to establish the relationship with Office 365 to reap the benefits of SSO and extend enterprise controls into Office 365.

INSIDE OUT **Leveraging Windows Azure**

Many decision makers in organizations realize the benefits of AD FS and regard it as a requirement rather than an optional component. At the same time, they are concerned that introducing AD FS adds a single point of weakness in the implementation of Office 365 because the 99.9 percent service level agreement (SLA) for Office 365 is meaningless if AD FS is unavailable. This is where an Infrastructure as a Service (IaaS) solution such as Windows Azure can make a difference. By implementing AD FS in Windows Azure, organizations without the ability to create geo-redundant networks can take advantage of a different type of cloud service to minimize the risk of an on-premises AD FS environment becoming unavailable and thereby affecting the availability of Office 365.

AD FS database

When deploying AD FS 2.0, you have the opportunity to use either the Windows Internal Database (WID) that comes with AD FS, which is the default, or a dedicated SQL server. The first AD FS server in the farm is known as the *primary federation server*, and subsequent AD FS servers are known as *secondary federation servers*.

The AD FS database, regardless of whether you choose to deploy WID or SQL, is used to store configuration information. The information in the database is replicated across the AD FS servers in the farm. The database on the primary federation server is a read-write database, while the ones on the secondary federation servers are read-only. In the event that the primary federation server becomes permanently unavailable, you will need to promote a secondary federation server to a primary federation server. There can be only one primary federation server in the farm.

Deciding whether to use WID or a dedicated SQL server requires you to be aware of the limitations of using WID. Using WID limits your AD FS farm to five servers. For most organizations, except the largest of enterprises, this is usually not a problem. There are other limitations when using WID that are not applicable to Office 365, such as being limited to only 100 trust relationships. This limitation might become an issue if you are planning to leverage your AD FS farm for other purposes besides Office 365.

Installing and configuring AD FS 2.0

Before starting the installation for AD FS 2.0, make sure you have completed all the preceding tasks. At this point, you already should have completed the following:

- Be familiar with the SSO experience your users will see and have a communication plan prepared.
- Understand the requirements for AD FS.
- Remediate your AD by ensuring you have the right UPN suffix added.
- Ensure existing users have the correct primary UPN suffix.
- Install IIS on the AD FS server.
- Create and install the security certificate for the default website in IIS on the AD FS server.

TROUBLESHOOTING

Download AD FS from Office 365

Do not directly add the AD FS role to the server through the Turn Windows features on or off link in Control Panel. Download and use AdfsSetup.exe instead.

When you have completed the preceding tasks, you are ready to install AD FS 2.0:

1. Create a service account for AD FS. In AD, create a service account that the AD FS service will use. Make sure this service account is part of the Administrators group of the local AD FS server. No special AD group memberships are required for this account; Domain Users is sufficient. We assume you know how to create AD service accounts and assign group membership in AD, so we do not provide details about how that is done.
2. Download the AD FS 2.0 software. The AD FS software package is a single executable file called AdfsSetup.exe. You can download it from the Microsoft Download Center at *http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=10909*, as shown in Figure 3-27. Follow the instructions at the Download Center, which eventually will lead you to a list of the AdfsSetup.exe options. Select the package that applies to your server operating system.

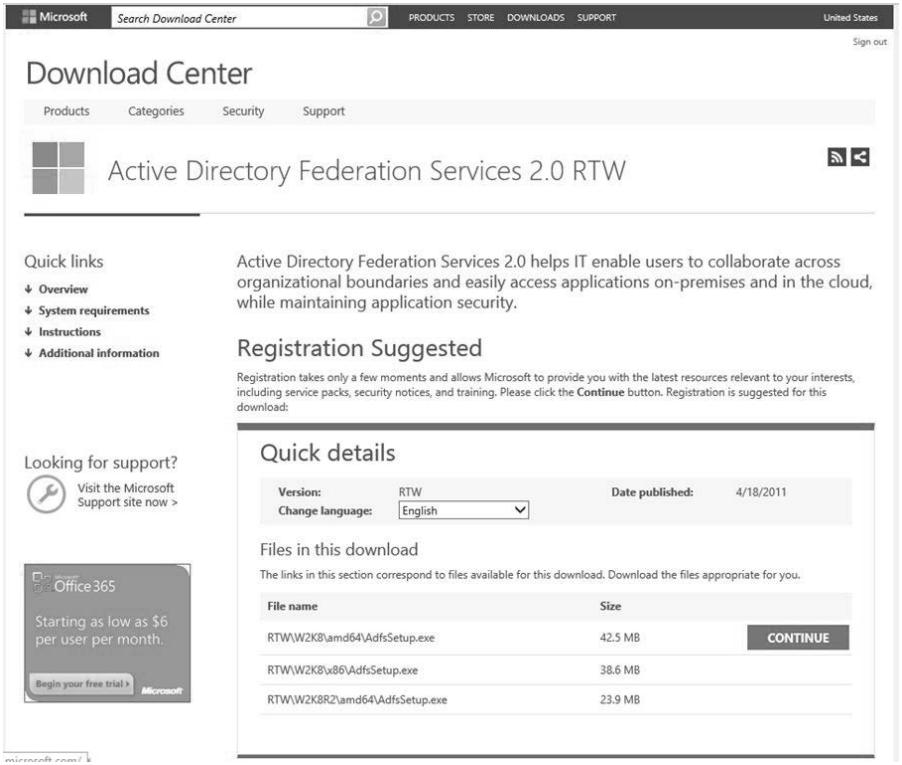

Figure 3-27 Microsoft Download Center with the AD FS 2.0 software.

3. Run AdfsSetup.exe.

4. Click Next at the Welcome to AD FS 2.0 Setup Wizard page.

5. Read and accept the Microsoft Software License Terms and click Next, as shown in Figure 3-28.

Figure 3-28 Accept the Microsoft Software License Terms for AD FS.

6. In the Active Directory Federation Services 2.0 Setup Wizard, select the Federation server option, as shown in Figure 3-29, and then click Next.

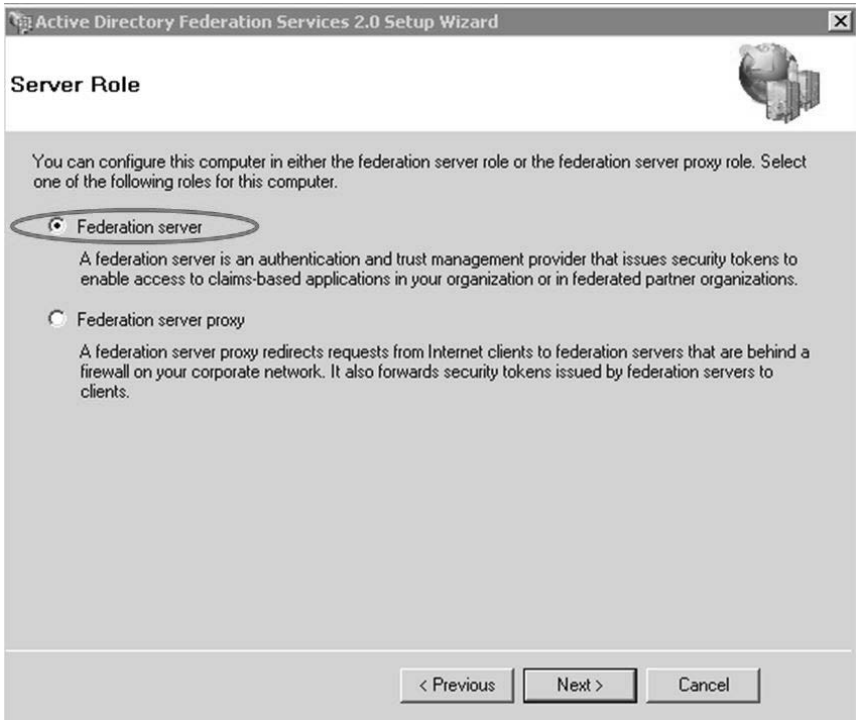

Figure 3-29 Install the AD FS server role.

7. As shown in Figure 3-30, the wizard will check for AD FS prerequisites and will install the required components if needed. Take note of the components the wizard will install, and then click Next.

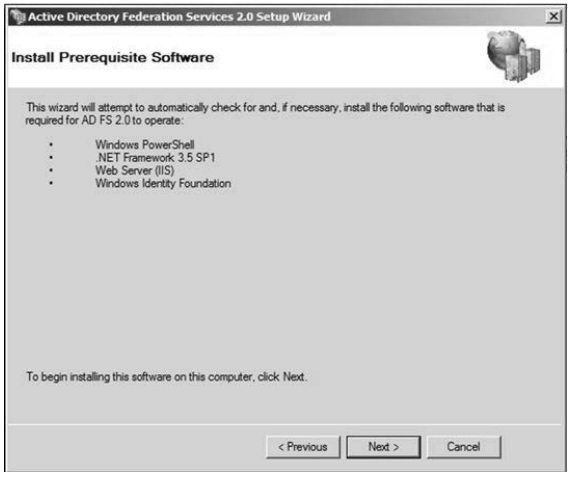

Figure 3-30 Installing AD FS prerequisites.

8. After the installation is complete, select Start the AD FS 2.0 Management snap-in when this wizard closes, as shown in Figure 3-31, and then click Finish.

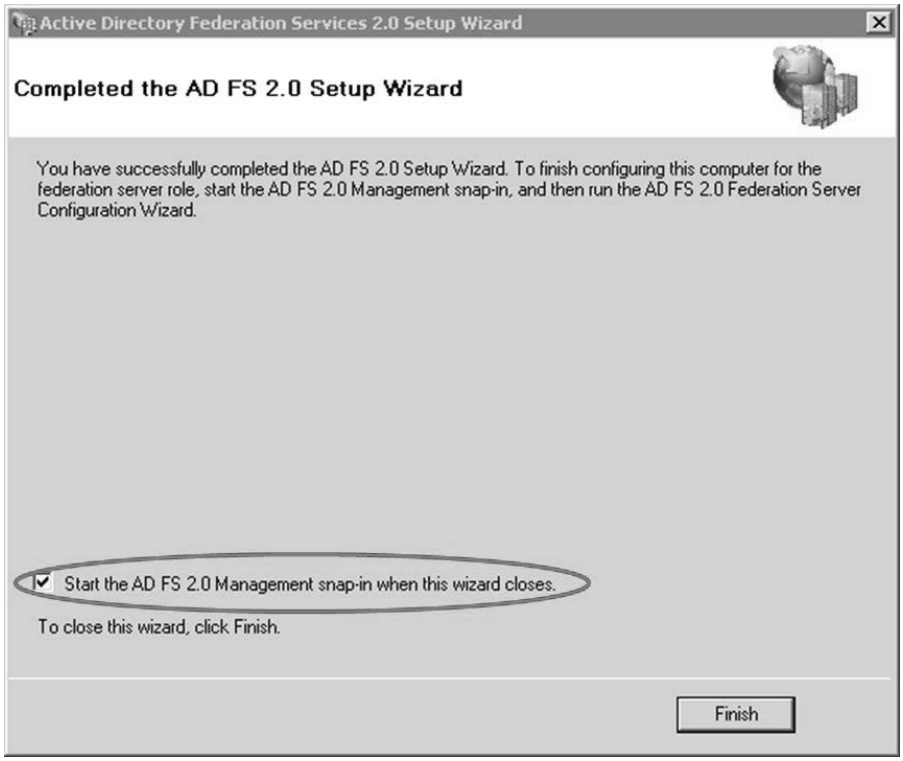

Figure 3-31 Start the AD FS 2.0 Management snap-in.

9. Because we selected the check box to start the AD FS Management snap-in in the preceding step, it will start at this time. Click the AD FS 2.0 Federation Server Configuration Wizard link in the middle pane, as shown in Figure 3-32.

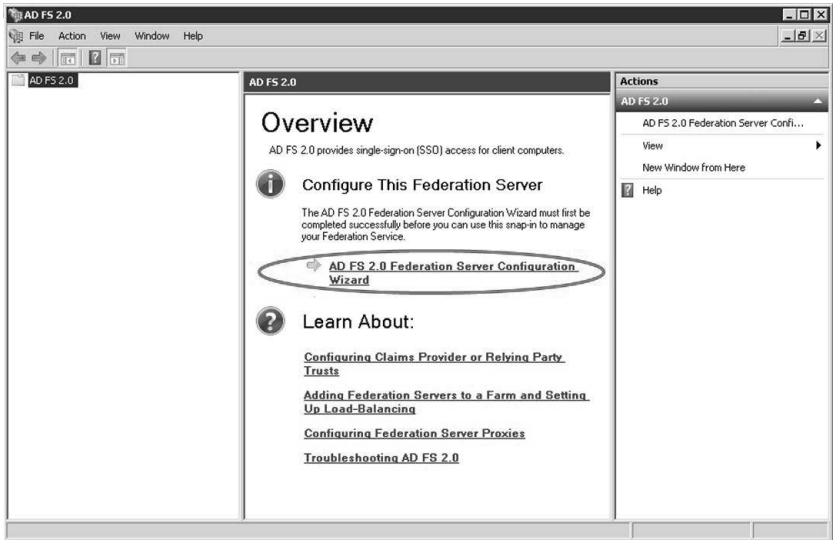

Figure 3-32 AD FS 2.0 Federation Server Configuration Wizard.

10. Because this is the first and primary federation server, select the Create a new Federation Service option, as shown in Figure 3-33, and then click Next.

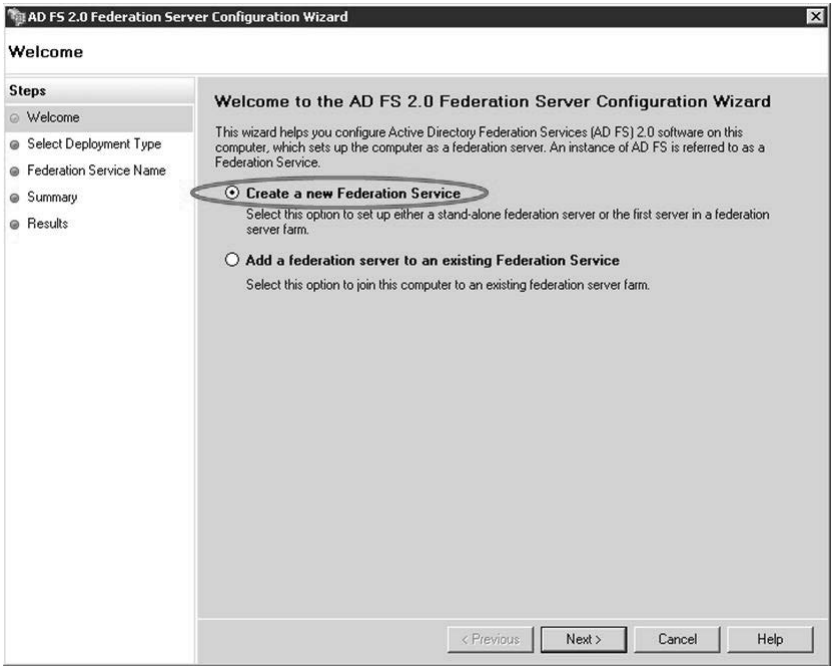

Figure 3-33 Create a new Federation Service.

11. In the Select Stand-Alone or Farm Deployment page, select New federation server farm, as shown in Figure 3-34, so you have the option to add more servers to the farm later.

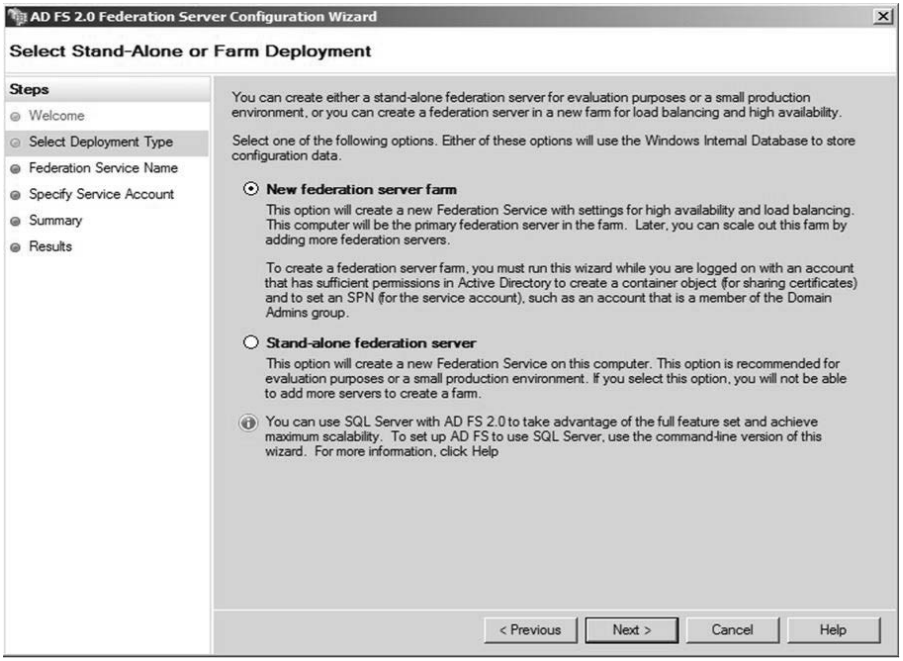

Figure 3-34 Create a new AD FS farm.

TROUBLESHOOTING

Problem with a stand-alone AD FS server

Remember our discussion earlier about AD FS potentially being a weak link for Office 365? For that reason, you should build an AD FS farm for a production environment. A stand-alone AD FS server will not allow you to add additional servers later.

12. The wizard will query the default website in IIS and should select the certificate you installed on the default website, as shown in Figure 3-35. Click Next.

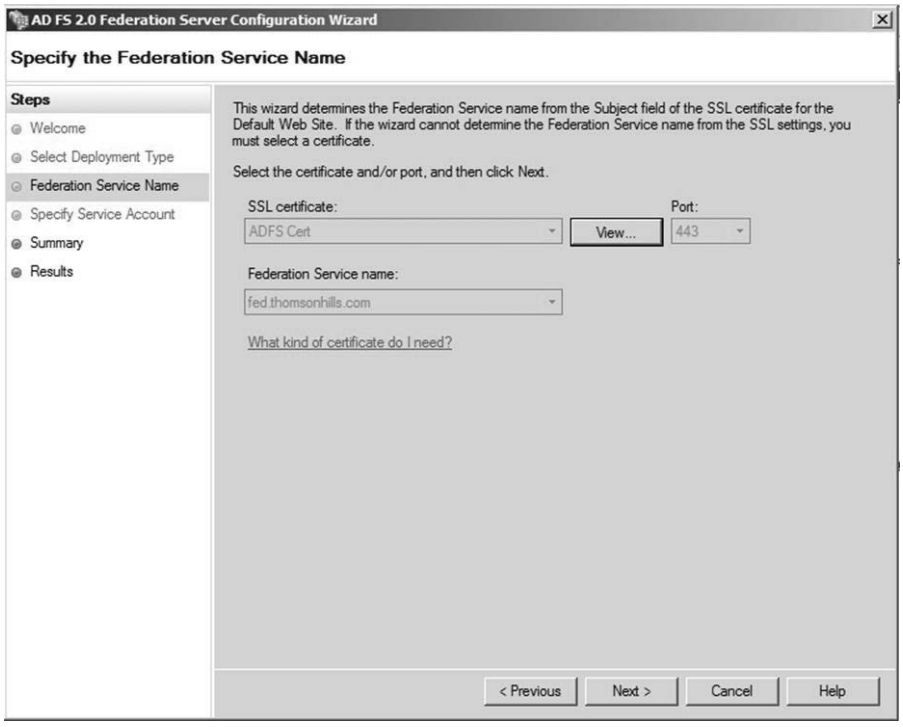

Figure 3-35 AD FS 2.0 Federation Server Configuration Wizard detects the certificate for the Default Web Site.

13. On the Specify a Service Account page, select the AD FS service account you created earlier, as shown in Figure 3-36. If you did not create the service account, you can use Active Directory Domain Services (AD DS) or Windows PowerShell to create the account. As a reminder, the service account must be a member of the Local Administrators group of the AD FS server. Click Next.

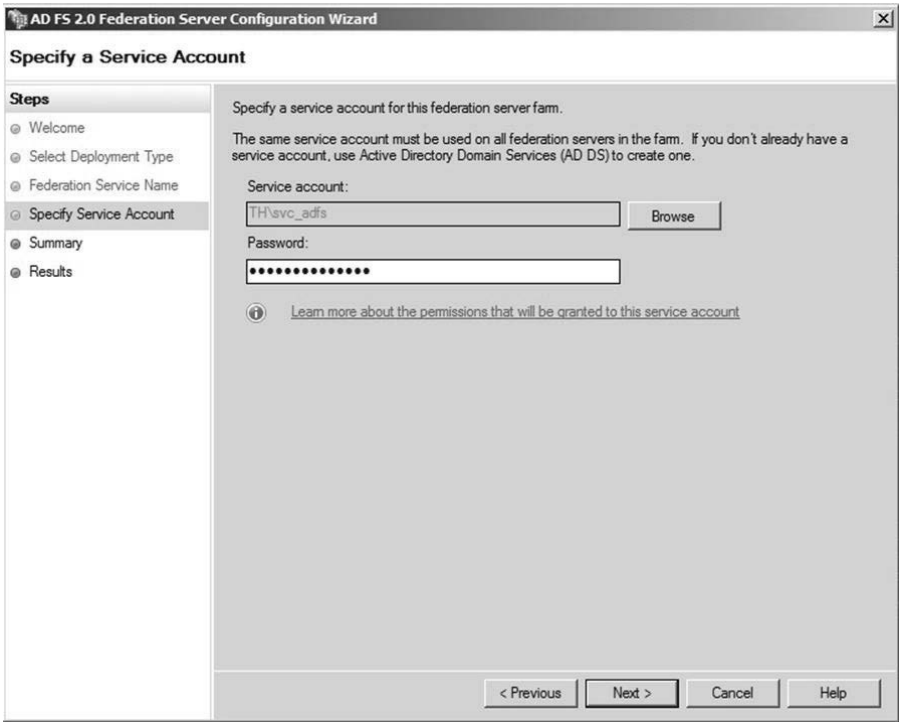

Figure 3-36 Select the AD FS service account.

14. On the Summary page, click Next to begin the AD FS configuration. When the configuration is complete, a Configuration Results page will appear that reports any issues, similar to the one shown in Figure 3-37.

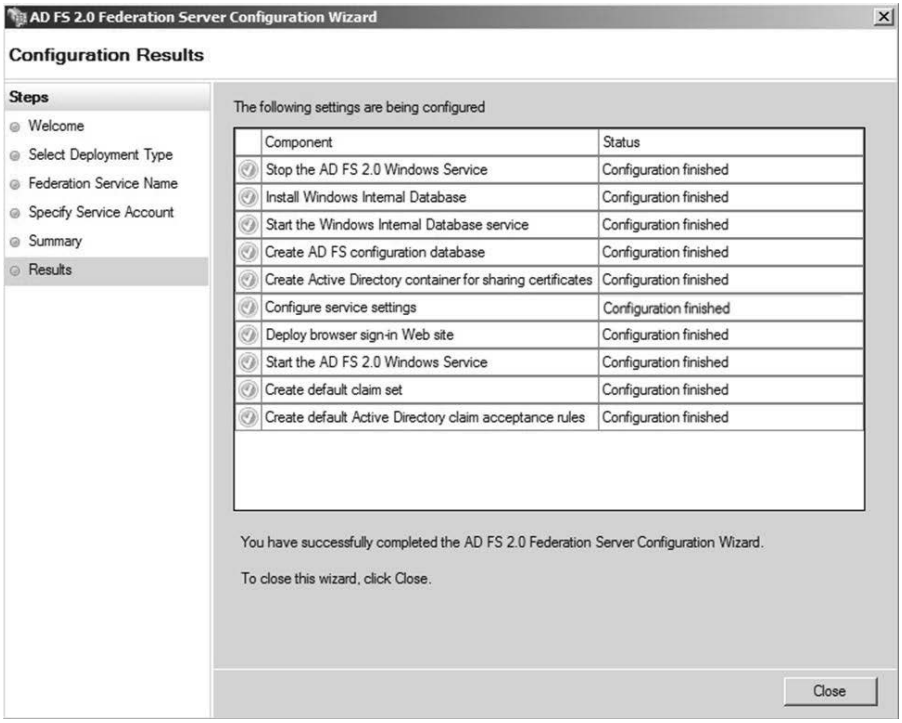

Figure 3-37 Configuration Results page showing AD FS 2.0 was successfully installed.

TROUBLESHOOTING

SPN was not set

You might be required to set the SPN for the service account manually. A common problem that occurs is when your host name is the same as the certificate issued to the default website. You can either change the server host name or revoke and reissue the certificate. The first option is usually simpler. Once you have done so, run the following command in a command line window as an administrator:

```
setspn -a host\<fully qualified servername> <domain>\<service account>
```

For example, if the fully qualified host name is fed.adatum.com and the service account is adatum\svc_adfs, the command will be the following:

```
setspn -a host\fed.adatum.com adatum\svc_adfs
```

15. Download and install the current AD FS 2.0 update rollup. For more information about the update rollup, see Knowledge Base (KB) article 2681584 at *http://support.microsoft.com/kb/2681584*.

Testing the federation server

Now that we have installed AD FS 2.0, we need to test that it is responding. Use a client computer located in the same forest as the AD FS server. From the client's browser, enter the URL of the AD FS server and append /FederationMetadata/2007-06/FederationMetadata.xml to the end of the URL. For example, if your federation server's URL is https://fed.adatum.com, enter the URL in the client's browser, as shown in the following example:

```
https://fed.adatum.com/FederationMetadata/2007-06/FederationMetadata.xml
```

If the federation server is responding correctly, you will see an XML document similar to the one shown in Figure 3-38.

Figure 3-38 XML document and service description when accessing the AD FS server's URL.

Converting the domain from standard authentication to identity federation

Now that we have installed IIS, bound the AD FS service to the IIS server, applied the necessary certificates applied to the IIS server, tested AD FS, and can see the XML schema, it is safe to say that AD FS is now operational and can service authentication requests.

The last step is to convert your domain that is in Office 365 from standard authentication to identity federation. This action will cause Office 365 to redirect access requests by users with the UPN suffix of the domain to your AD FS for authentication, unless a user already has a valid token from a previously successful authentication. Converting the tenant to identity federation for a domain will not affect or alter the logon experience of cloud identity accounts.

To convert the domain from standard authentication to identity federation, we will need to switch back to Windows PowerShell. Follow the steps in one of the two following sections that best describes your environment.

AD FS server is installed on Windows Server 2008 R2

1. Download and install the Windows Azure Active Directory Module for Windows PowerShell cmdlets, formerly known as the Microsoft Online Services Module for Windows PowerShell cmdlets. The 32-bit version of the Windows Azure Active Directory Module for Windows PowerShell is located at *http://go.microsoft.com/FWLink/p/?Linkid=236298* and the 64-bit version is located at *http://go.microsoft.com/FWLink/p/?Linkid=236297*.

2. Start the Windows Azure Active Directory Module for Windows PowerShell cmdlets.

3. Enter the following command, which will produce a logon prompt for a user name and password:

```
$cred = Get-Credential
```

4. The credentials you provide will be stored in the *$cred* variable. At the logon prompt, use your Office 365 Global Administrator account name.

> **Note** **Why save a credential in a variable?**
>
> **Technically, when managing identity with Windows PowerShell you can simply use the command *Connect-MsolService*. You do not need to save the credential in a variable first. However, we saved the credential in a variable in our example because we will need it when we use Windows PowerShell for Exchange Online, so we are just keeping it consistent throughout the book.**

5. Enter the following command, which will attempt to connect and authenticate to an Office 365 tenant using the logon credentials you stored in *$cred*:

```
Connect-MsolService -Credential $cred
```

6. Lastly, enter the following command to convert the domain from standard authentication to identity federation in Office 365. Note that the *-SupportMultipleDomain* parameter is optional. Use it only if you will be federating other top-level domains (TLDs) with this Office 365 tenant.

```
Convert-MsolDomainToFederated -DomainName <domain name> -SupportMultipleDomain
```

   If you do not receive any Windows PowerShell error messages, which are usually red in color, then your domain now supports identity federation. We will verify this in the "Verifying a successful conversion of a domain" section.

The AD FS server is installed on Windows Server 2008 SP2 or on a remote Windows 7 workstation

1. Download and install the Windows Azure Active Directory Module for Windows PowerShell cmdlets, formerly known as the Microsoft Online Services Module for Windows PowerShell cmdlets. The 32-bit version of the Windows Azure Active Directory Module for Windows PowerShell cmdlets is located at *http://go.microsoft.com/FWLink/p/?Linkid=236298* and the 64-bit version is located at *http://go.microsoft.com/FWLink/p/?Linkid=236297*.

2. Install the Windows Azure Active Directory Module on a remote server running Windows 2008 R2 or on a Windows 7 workstation.

3. On your AD FS server, right-click the shortcut to Windows PowerShell and run it as an administrator. Next, enter the following command:

```
Enable-PSRemoting -force
```

> **Note**
>
> **The *Enable–PSRemoting* command creates a Windows Remote Management (WinRM) listener service on all IP addresses on the server using the HTTP protocol through port 5985. It also creates the required Windows Firewall rules to allow the Windows Remote Management application to go through port 5985. This allows a remote workstation or server to execute remote Windows PowerShell commands against this server.**

4. To confirm that the Windows Remote Management service has been configured, execute the following command to see the configuration details:

```
winrm enumerate winrm/config/listener
```

5. Return to the remote server or workstation on which you installed the Windows Azure Active Directory Module and start the module.

6. Enter the following command, which will produce a logon prompt for a user name and a password:

   ```
   $cred = Get-Credential
   ```

   The credentials you provide will be stored in a variable called *$cred*. When you see the logon prompt, enter your Office 365 Global Administrator account name.

> **Note** **Why save a credential in a variable?**
> **Technically, when managing identity with Windows PowerShell you can simply use the command *Connect-MsolService*. You do not need to save the credential in a variable first. However, we saved the credential in a variable in our example because we will need it when we use Windows PowerShell for Exchange Online, so we are just keeping it consistent throughout the book.**

7. Enter the following command, which will attempt to connect and authenticate to an Office 365 tenant using the logon credentials that you stored in *$cred*:

   ```
   Connect-MsolService -Credential $cred
   ```

8. Enter the following command to set the context to that of the AD FS server:

   ```
   Set-MsolAdfscontext -Computer <FQDN of federation server>
   ```

9. Lastly, enter the following command to convert the domain from standard authentication to identity federation in Office 365:

   ```
   Convert-MsolDomainToFederated -DomainName <domain name> -SupportMultipleDomain
   ```

   Note that the *-SupportMultipleDomain* parameter is optional. Use it only if you will be federating other top-level domains (TLDs) with this Office 365 tenant.

   If you do not receive any Windows PowerShell error messages, which are usually red in color, then your domain is now a federated domain. We will verify this in the "Verifying a successful conversion of a domain" section.

Verifying a successful conversion of a domain

There are two main ways you can verify that federation has been successfully accomplished:

- Using Windows PowerShell
- Using the AD FS 2.0 Management snap-in

Windows PowerShell

You can verify your federation settings for the domain by issuing the following Windows PowerShell command after you have connected to Office 365 by using the *Connect-MsolService* command, as shown in Figure 3-39.

```
Get-MsolDomainFederationSettings –DomainName <your domain name FQDN>
```

For example:

```
Get-MsolDomainFederationSettings –DomainName thomsonhills.com
```

If you execute *Get-MsolDomainFederationSettings* without passing the *–DomainName* parameter, you will be verbosely prompted for a domain name.

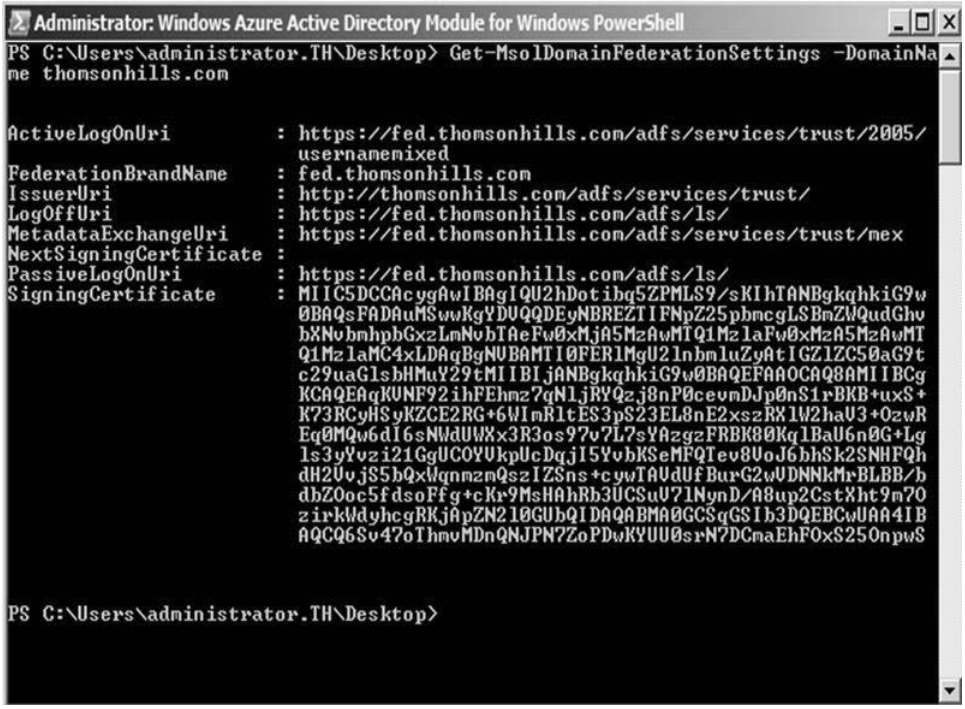

Figure 3-39 Results after entering a command with the *Get-MsolDomainFederationSettings* cmdlet.

AD FS 2.0 Administration snap-in

You can also verify that a federation trust has been established between AD and Office 365 by looking at the trust relationships in the AD FS 2.0 Administration console. Follow the steps below:

1. Start the AD FS 2.0 Administration console.
2. In the left pane, expand the Trust Relationships node and select Relying Party Trust, as shown in Figure 3-40. You should see an entry in the middle pane for a trust relationship with the Microsoft Office 365 Identity Platform.

Figure 3-40 Verifying that federation trust has been established with Office 365.

Updating the federation URL endpoint

The federation URL endpoint is the FQDN of the federation server or service that Office 365 will redirect a user to once it detects the user is trying to log on with a UPN suffix that is associated to an identity federated domain.

If for any reason you need to change the federation URL endpoint, you can do so by following these steps:

1. Start the AD FS 2.0 Management console.

2. Right-click the AD FS 2.0 root node and select Edit Federation Service Properties from the drop-down box, as shown in Figure 3-41.

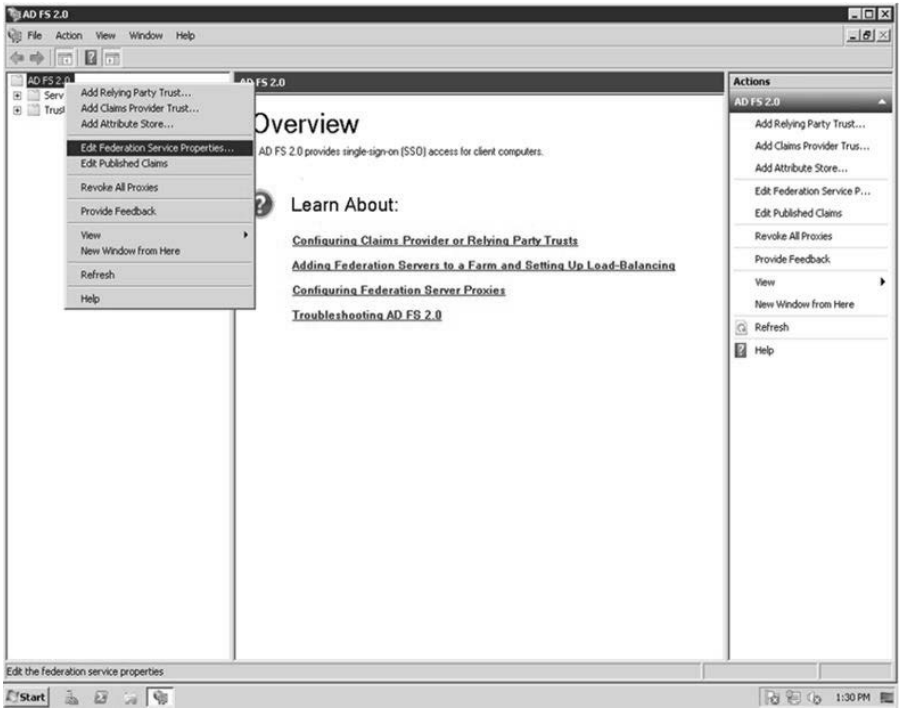

Figure 3-41 Edit Federation Service Properties using AD FS 2.0 MMC.

3. Edit the three properties of the federation service, as shown in Figure 3-42.

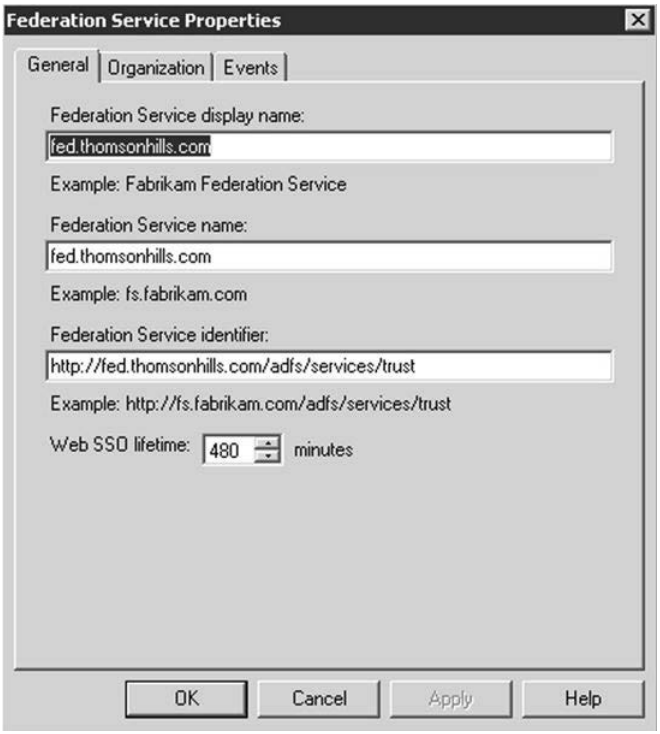

Figure 3-42 Properties of the federation service.

> **Note** **SSO lifetime**
>
> **AD FS 2.0 issues Security Assertion Markup Language (SAML) tokens that Office 365 consumes through the use of authentication cookies. Authentication cookies facilitate SSO in Office 365. The period of time that each authentication cookie can be used is represented by the SAML token's lifetime, which can be modified through the Web SSO lifetime setting, as shown in Figure 3-42. In the preceding example, once a user has been authenticated by AD FS the user will not be prompted for credentials for 480 minutes. If the user logs off and logs on again before 480 minutes, the SSO lifetime is reset.**

4. Click OK to save the settings and restart the AD FS 2.0 service, as shown in Figure 3-43.

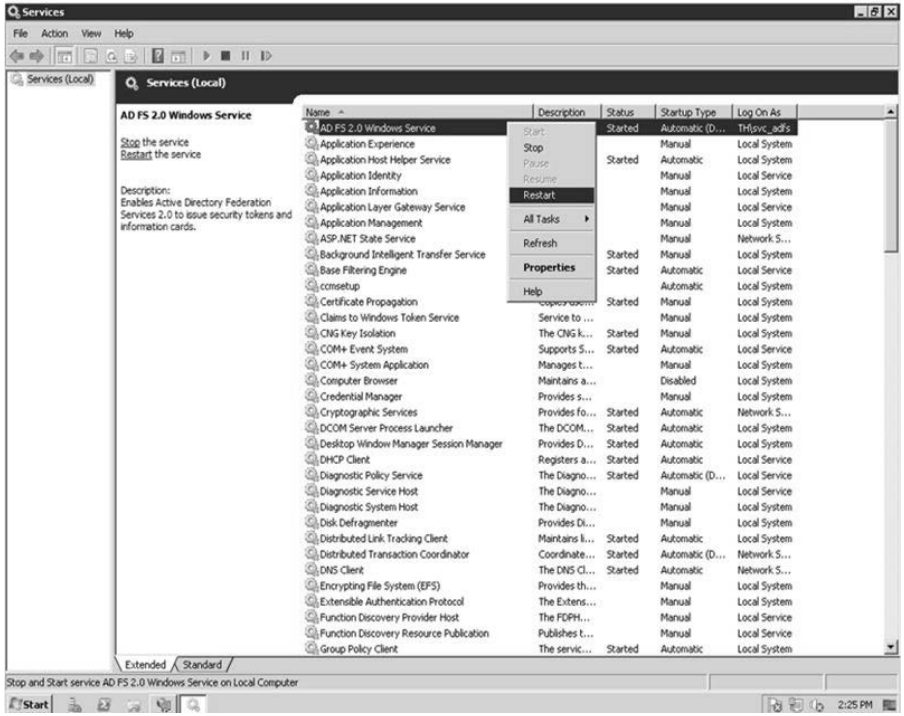

Figure 3-43 Restart the AD FS 2.0 service from the Services MMC.

5. If you have a wildcard certificate, you do not need to do anything with the certificate, assuming you did not change the domain name of your AD FS service. However, if you do not have a wildcard certificate and need to add a new certificate, you will first need to issue the following Windows PowerShell command from your AD FS server to turn off the AD FS automatic certificate rollover feature:

```
Set-ADFSProperties –AutoCertificateRollover $False
```

6. Skip this step if you do not need to update your certificate. Acquire or generate your new certificate.

7. Skip this step if you do not need to update your certificate. From the AD FS 2.0 Management console, expand the Service node under the root node, and then click Certificates. In the Actions pane, click Add Token-Signing certificate and add your new certificate. Click Add Token-Decrypting certificate, and then click Set Service Communications. See Figure 3-44.

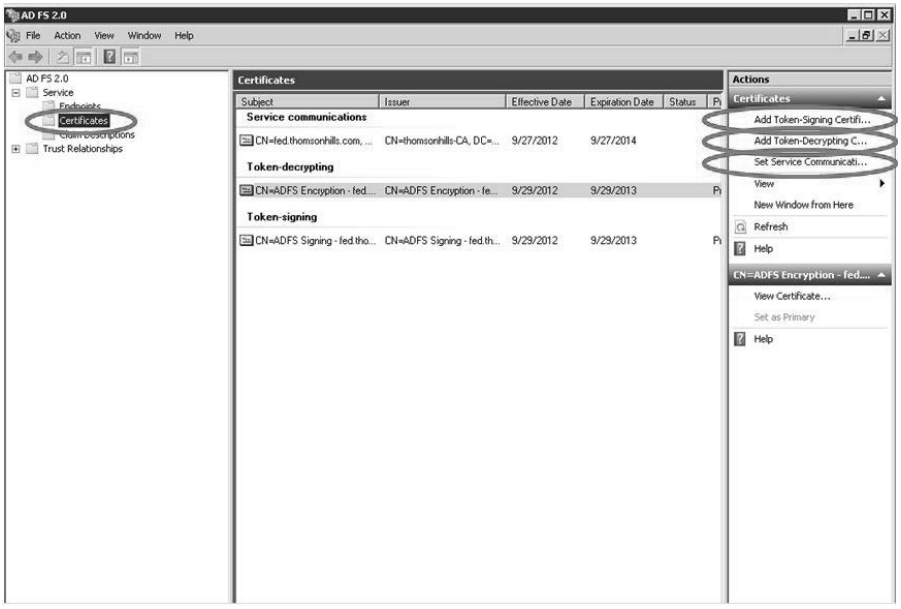

Figure 3-44 Add Token-Signing Certificate, Add Token-Decrypting Certificate, and Set Service Communications.

8. Lastly, enter the following Windows PowerShell command from the Windows Azure Active Directory Module:

```
Update-MSOLFederatedDomain –DomainName <YourFederatedDomain FQDN>
```

> **Note**
>
> **By this time, you should be somewhat familiar with Windows PowerShell. Thus, for Step 8 we omitted the Windows PowerShell commands you would normally use to connect to Office 365 first, namely the *Get-Credential* and *Connect-MsolService* commands. Furthermore, if you are executing these commands from a remote server running Windows 2008 R2 or a Windows 7 workstation and not from your AD FS server, remember you need to also execute the *Set-MsolAdfsContext* command. Refer to previous sections if you need to refresh your memory.**

9. Issue the following Windows PowerShell command from the Windows Azure Active Directory Module to determine if the federation URL endpoint is successfully updated:

```
Get-MsolDomainFederationSettings –DomainName <your domain FQDN>
```

Removing Active Directory Federation Services

In the event you need to remove AD FS and disable SSO for a domain in your tenant, there are a few important things you need to know:

- As with most actions, you will use the Windows Azure Active Directory Module and Windows PowerShell to convert the federated domain in Office 365 back to a standard domain.
- Previously federated user accounts, if they existed prior to federation, will not revert to using the original Office 365 passwords they had prior to federation.
- Temporary passwords will be generated for all federated users.
- The temporary passwords are stored in a file. You will specify the path and the name of the file as one of the parameters.
- Users will have to log on with their new temporary password and will be prompted to provide a new permanent password.
- If you choose to uninstall the AD FS role from your server, the virtual directories in the default website will not be removed. This must be done manually.
- If you choose to uninstall the AD FS role from your server, the AD FS database will not be removed. This can be done manually.
- Disabling SSO is also known as converting a domain from identity federation to standard authentication.

TROUBLESHOOTING

Accounts affected by reverting from identity federation to standard authentication

After you convert a domain in Office 365 from identity federation to standard authentication, all the user accounts associated with that domain will become unusable until you either convert the domain back to identity federation or until the users are also converted. Another word of caution is that the users will need to be assigned new passwords.

Converting a domain from identity federation to standard authentication

The first step you need to take to break federation is to convert the domain from federated to standard using Windows PowerShell. The second step, which is optional, is to uninstall AD FS 2.0 from the server.

The following scenarios show how to convert a domain from federated to standard. Choose the scenario that is right for you and follow the steps.

AD FS server that has the Windows Azure Active Directory Module installed

1. From the AD FS Server, start the Windows Azure Active Directory Module.

2. Enter the following Windows PowerShell command to initiate a logon prompt, which you will use to supply your Office 365 credentials, and store the credentials in a variable named *$cred*:

   ```
   $cred=Get-Credential
   ```

3. Enter the following command, which will attempt to connect and authenticate to an Office 365 tenant using the logon credentials you stored in *$cred*:

   ```
   Connect-MsolService -Credential $cred
   ```

4. Enter the following command to remove the Rely Party Trust information from the Office 365 authentication system federation service and the on-premises AD FS 2.0 server:

   ```
   Convert-MsolDomainToStandard -DomainName <domain name> -SkipUserCoonversion
   [$true|$false] –PasswordFile:<path and filename>
   ```

5. If the *–SkipUserConversion* parameter is set to *$true*, a password file will not be generated and the user accounts that are associated with the domain will become unusable until either the domain is converted back to identity federation or each account is converted using the *Convert-MSOLFederatedUser* cmdlet, which we will discuss shortly. An actual command might look something like this:

   ```
   Convert-MsolDomainToStandard –DomainName adatum.com –SkipUserConversion $false
   –PasswordFile c:\TempPwd.txt
   ```

> **Note** **Why not convert users?**
>
> **Why would you use *Convert-MsolDomainToStandard* with the *–SkipUserConversion $true* parameter so as not to convert users? One such scenario might be when you need to re-establish the Relying Party Trust. There have been a few occasions where we had to remove the Relying Party Trust because of an AD FS issue, and then turn around and use the *Convert-MsodDomainToFederated* to re-establish the Relying Party Trust. In such a scenario, we really do not want to convert the users.**

6. Now that we have removed the Relying Party Trust, we need to reset the authentication setting for the domain. Enter the following command to accomplish this:

```
Set-MsolDomainAuthentication –Authentication Managed –DomainName <domain name>
```

7. If you need to manually convert user accounts to standard authentication because you used the *–SkipUserConversion $true* parameter, then enter this command:

```
Convert-MsolFederatedUser –UserPrincipalName <user@domain-name> -NewPassword
"<password>"
```

   An actual command will look something like this:

```
Convert-MsolFederatedUser –UserPrincipalName julian@adatum.com –NewPassword
"Office365Rocks"
```


INSIDE OUT **Bulk conversion of user accounts**

It might not be feasible for you to manually convert each user by repeatedly issuing the Windows PowerShell command, as shown in Step 6. To bulk convert users, you will have to write a script to iterate through a list of users and manually convert them. We use the following example script:

```
#Script to bulk convert users
#after Domain has been converted from
#Identity Federated to Standard Authentication

Cred$=Get-Credential
Connect-MsolService –Credential Cred$

Get-MsolUser –All | ForEach-Object {
   Convert-MsolFederatedUser –UserPrincipalName $_.UserPrincipalName –NewPass-
word “Temp-pwd”
}
```

Completely uninstall AD FS 2.0

The following process completely removes AD FS:

- Determine the location of the Certificate Sharing Container in Active Directory.
- Uninstall AD FS from the server(s) in the farm.
- Restore IIS by manually removing virtual directories and ADFSAppPool.
- Manually remove the Certificate Sharing Container in Active Directory.

As you can see, uninstalling AD FS completely will require a few manual steps because not everything is removed as part of the uninstallation process. One of the manual steps you need to do is remove the Certificate Sharing Container in Active Directory. To do so, you might need to determine where this container is located before the last AD FS server in the farm is removed.

Determining the location of the Certificate Sharing Container in Active Directory

When we run the AD FS Configuration Wizard during installation to create a new AD FS server and farm, it creates a Certificate Sharing Container in Active Directory. When you uninstall, the Certificate Sharing Container is not automatically deleted, so we will need to do this manually.

The actual removal of the Certificate Sharing Container will be carried out later. For now, we just need to determine the container's location. We do this now because the Windows PowerShell commands to reveal the location of the container have to be run prior to uninstalling the last AD FS server in the farm.

To determine the location of the Certificate Sharing Container, follow these steps:

1. From an AD FS server, start Windows PowerShell.
2. Execute the following Windows PowerShell commands:

```
Add-PsSnapin Microsoft.Adfs.Powershell
Get-AdfsProperties
```

3. Take note of the *CertificateSharingContainer* property, as shown in Figure 3-45. We will use this information at a later step. In the example below, the pertinent information revealed by the Windows PowerShell script is CN=ADFS,CN=Microsoft,CN=Program Data,DC=thomsonhills,DC=com.

The GUID for the AD FS farm in this example is CN=2e9a65b9-3a14-43e1-b9ec-d965fb6272c5. Take note of the GUID of your farm.

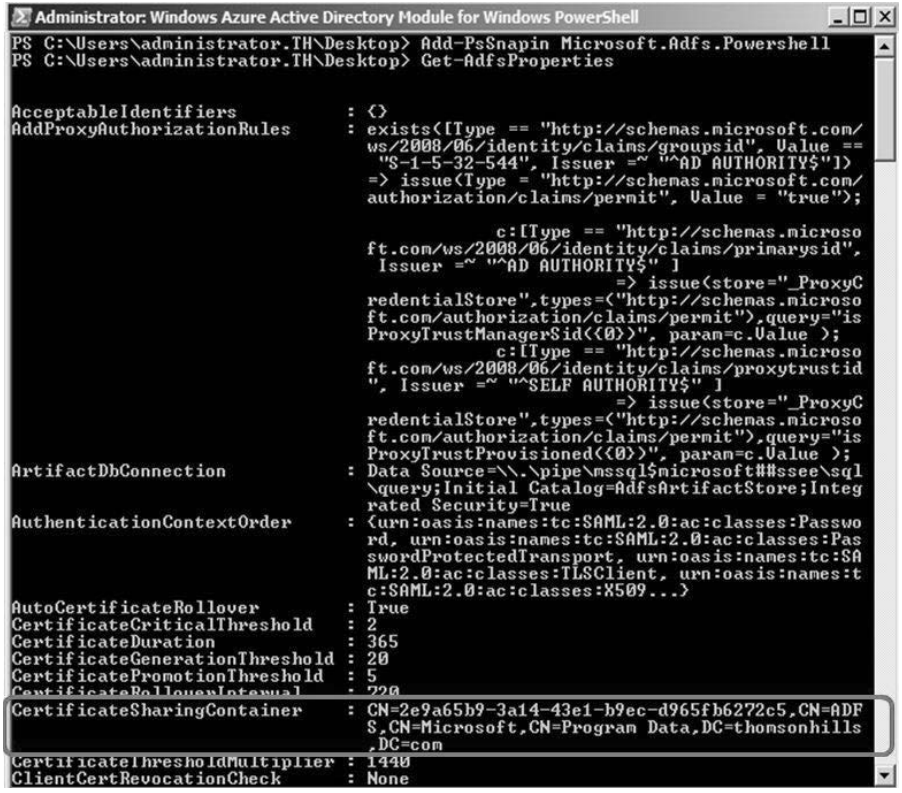

Figure 3-45 Take note of the value for the CertificateSharingContainer.

Now that we know the location of the Certificate Sharing Container, we can start uninstalling AD FS 2.0 from the servers in the farm.

Uninstalling AD FS 2.0

As mentioned earlier in the chapter, if you need to remove the AD FS 2.0 role from your server, you will need to follow these steps:

1. Open Control Panel and in the Category view, click Programs.

2. Select the View Installed Updates link and search for the Active Directory Federation Services 2.0 component.

3. Select the Active Directory Federation Services 2.0 component and click Uninstall, as shown in Figure 3-46.

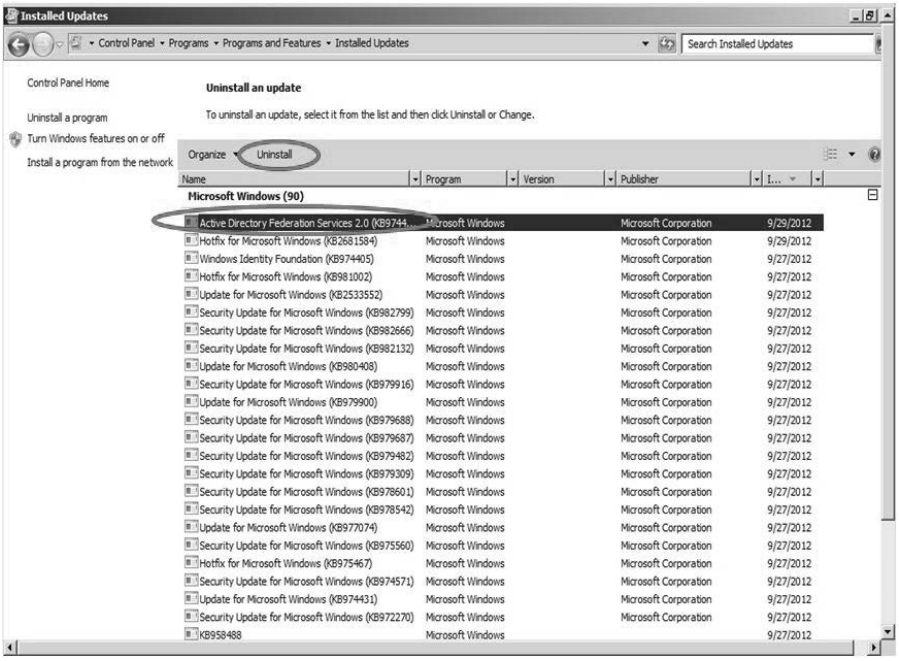

Figure 3-46 Uninstall Active Directory Federation Services 2.0.

Restoring IIS

Uninstalling AD FS 2.0 does not restore IIS to its original state. When you installed AD FS 2.0, the setup created virtual directories in IIS and an application pool for AD FS. These are not removed as part of the uninstall process, so you will have to do this manually. The virtual directories that were created in IIS are /adfs and /adfs/ls, and the application pool that was created is named ADFSAppPool, as shown in Figure 3-47.

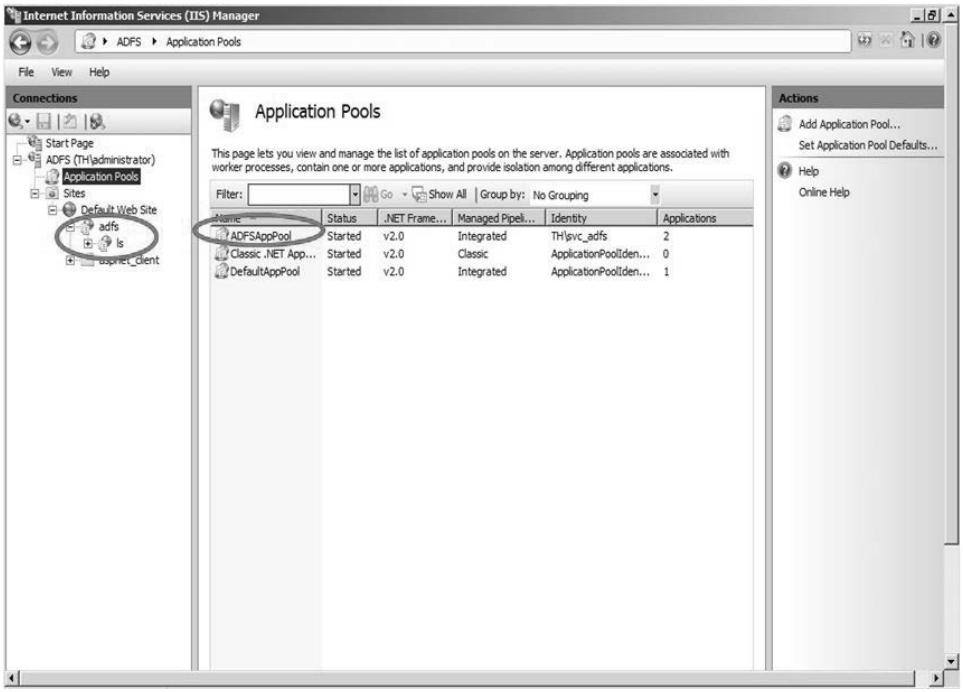

Figure 3-47 Virtual adfs directories and application pool.

To remove the application, application pools, and directories, follow these steps:

1. In IIS, navigate to the /adfs/ls directory.
2. Right-click the directory and select Remove, as shown in Figure 3-48.

Figure 3-48 Remove the application in /adfs/ls.

3. Repeat the same steps for the /adfs directory.

4. Select the Application Pools node and locate the ADFSAppPool application pool. Right click it and select Remove, as shown in Figure 3-49, or simply select Remove on the Actions pane.

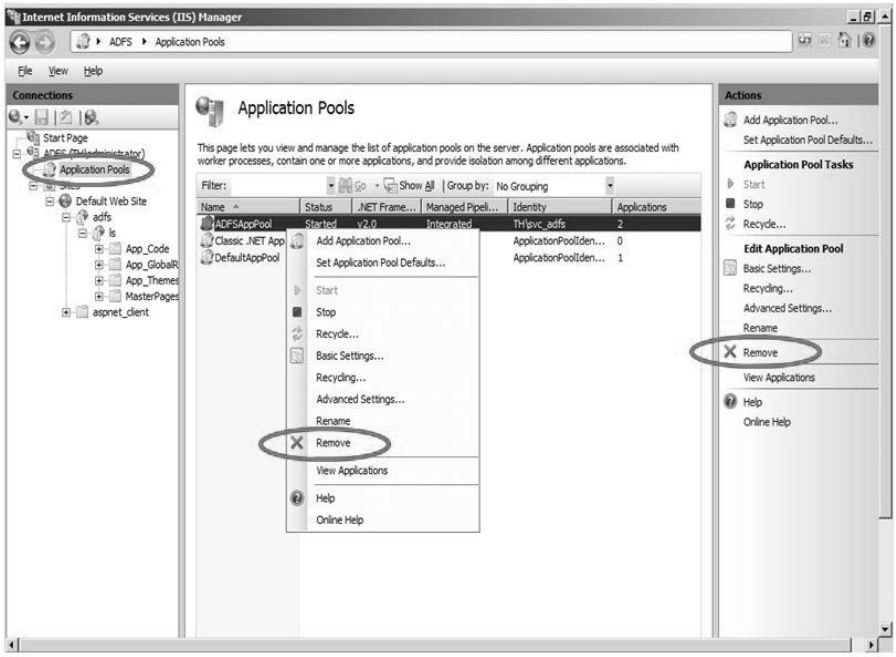

Figure 3-49 Remove the ADFSAppPool application pool.

5. Lastly, we need to remove the actual directories. Open Windows Explorer and navigate to %systemdrive%\inetpub.

6. Right-click the \adfs directory and select Delete, as shown in Figure 3-50.

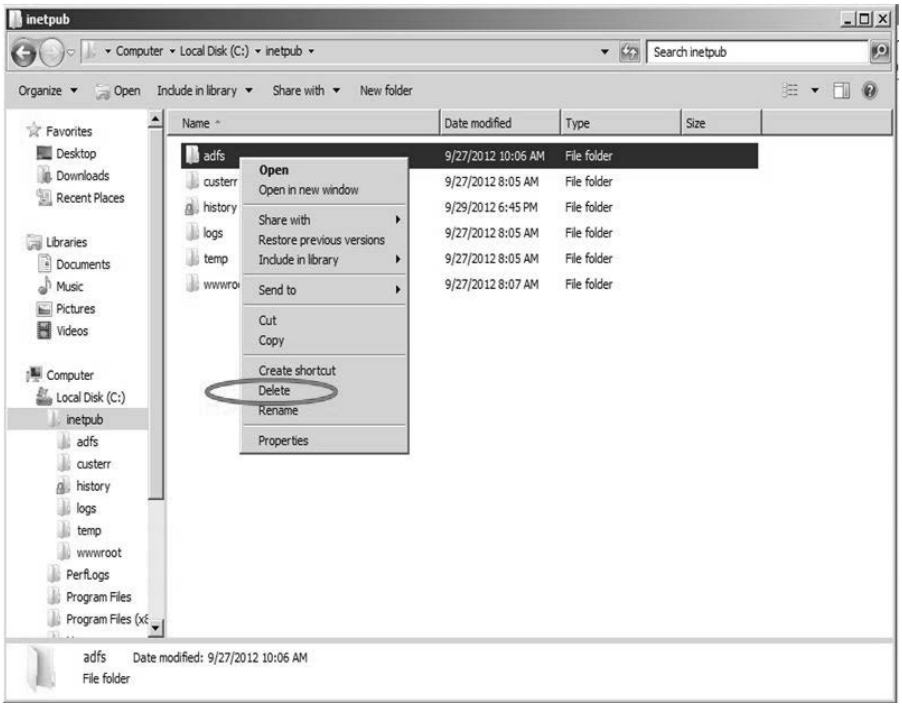

Figure 3-50 Delete the \adfs subdirectory.

Removing the Certificate Sharing Container

From an earlier step, you should have gathered the location information for the Certificate Sharing Container. We will now use that information to manually remove the container from AD by following these steps:

1. From a Windows 2008 or later Server that has the Active Directory Domain Services role installed, click Start. Click Run, and then type ADSIEdit.msc, as shown in Figure 3-51.

   If you need to install ADSIEdit on a server that is not running Windows 2008 or on a workstation, see "ADSI Edit (adsiedit.msc)" at *http://technet.microsoft.com/en-us/library/cc773354.aspx*.

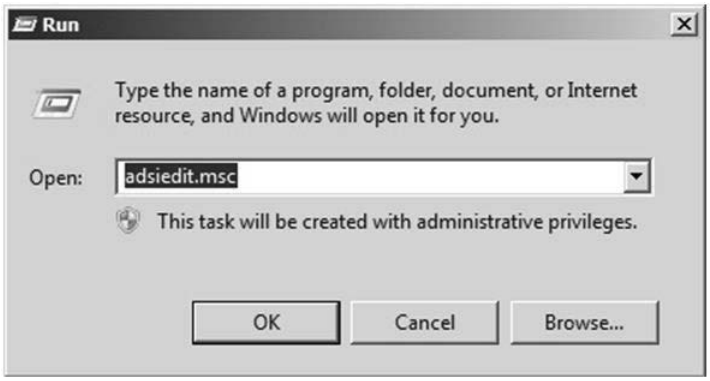

Figure 3-51 Run ADSIEdit.msc.

2. Right-click ADSI Edit and select Connect to, as shown in Figure 3-52.

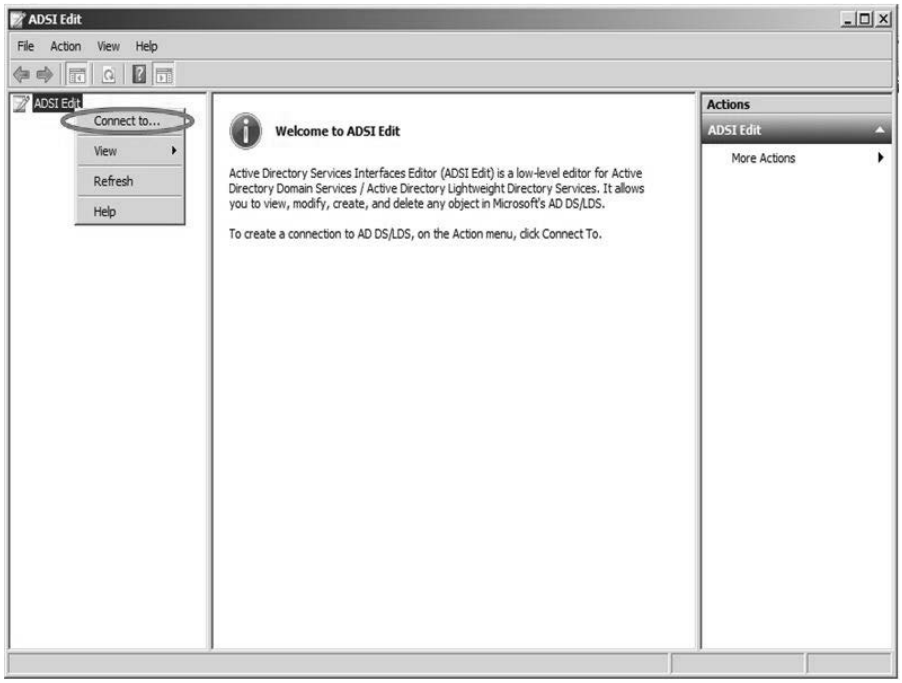

Figure 3-52 Right-click ADSI Edit and select Connect to.

3. Under Connection Point, click Select a well-known Naming Context, as shown in Figure 3-53. Then click OK.

Figure 3-53 Select the default naming context.

4. Refer to the location information of the Certificate Sharing Container you collected at the very beginning. In our example, we noted that the container is at CN=ADFS,CN=Microsoft,CN=Program Data,DC=thomsonhills,DC=com.

Applying this information to our example, and reading backward starting from DC=thomsonhills,DC=com, expand CN=Program Data, followed by CN=Microsoft, and finally CN=ADFS. Navigate in that order, as shown in Figure 3-54.

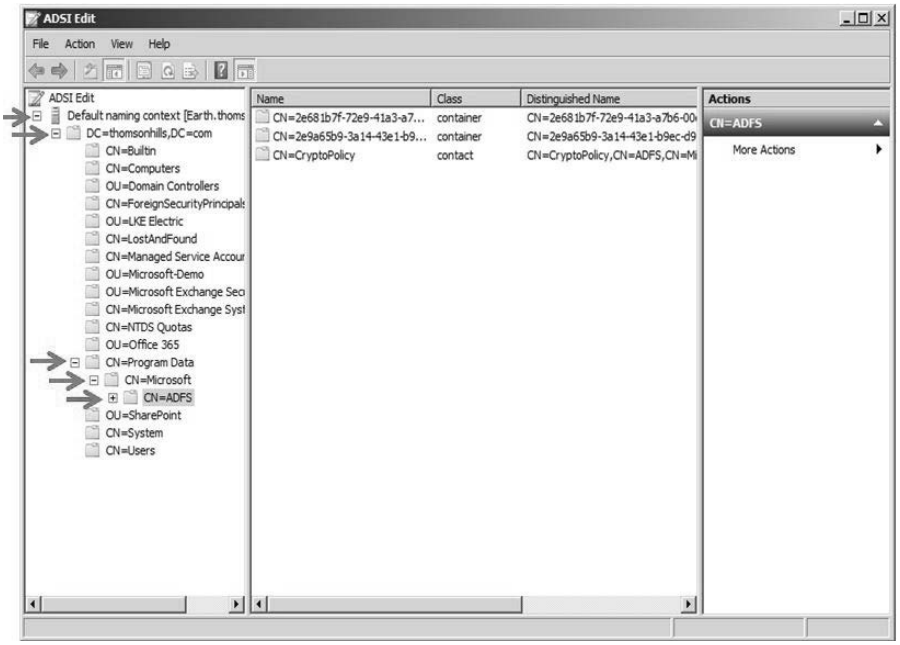

Figure 3-54 Locating the Certificate Sharing Container in ADSIEdit.msc.

5. Look for the GUID of the farm. You should already have that information from an earlier step. In our example, the GUID we are looking for is 2e9a65b9-3a14-43e1-b9ec-d965fb6272c5, as shown in Figure 3-55. Right-click the appropriate GUID and select Delete.

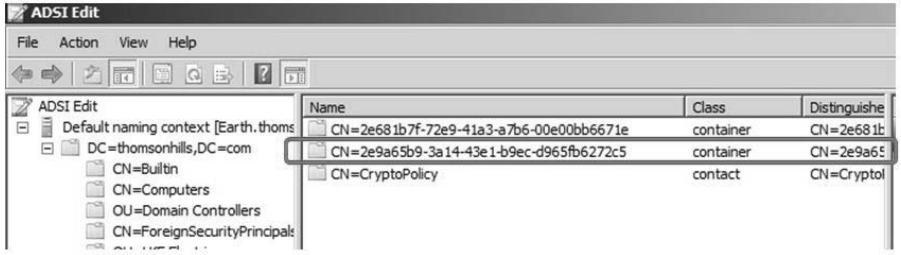

Figure 3-55 Locate, right-click, and delete the GUID that matches the AD FS farm.

You have now completely uninstalled AD FS and manually cleaned up all the objects and settings that were not removed by the uninstallation process.

Summary

In this chapter, we undertook and implemented SSO, a key component that is unique to enterprises and available only in the Office 365 Enterprise (A1/G1/E1, A3/G3/E3, or A4/G4/E4) suite offerings. There are many technologies that made this possible, the most important of which is a healthy Active Directory.

With most enterprise Office 365 deployments, we advocate an Active Directory health assessment. As a reminder, the Microsoft Office 365 Deployment Readiness Toolkit will analyze your AD for Office 365 readiness. The most important thing is to ensure that your forest has a routable UPN suffix that you will assign to the users in the forest. This is also a requirement for directory synchronization (Directory Sync), which we will cover Chapter 4, "Directory Synchronization." The planning work you did in Chapter 2, "Planning and preparing to deploy Office 365," should have prepared your environment and made the tasks in this chapter less daunting.

It is also important to stress that when you turn on SSO, you are in fact deferring authentication to your on-premises AD FS farm. Therefore, if the AD FS farm is unreachable for whatever reason, Office 365 services will be unavailable for users who are not yet authenticated. Invest in the time and architecture to build a robust AD FS farm and consider alternative and redundant options such as Windows Azure IaaS to supplement your AD FS farm.

CHAPTER 12

Mailbox migration and administering Exchange Online

In Chapter 10, "Introducing Exchange Online," we covered the different models of deploying Exchange Online, and in Chapter 11, "Planning and deploying hybrid Exchange," we implemented an Exchange Online hybrid environment. We also performed tests to confirm key mailbox operations.

Now that you have incorporated Exchange Online in your environment, it is time to discuss mailbox migration options and administering the different messaging workloads. As we mentioned before, this book is about Office 365, so we will focus only on Exchange Online and hybrid administration topics in this chapter.

Mailbox migration options

There are three primary types of migration options:

- Cutover migration
- Staged migration
- Hybrid deployment migration

A cutover migration is a process where all on-premises mailboxes and contents are migrated as a single batch and is applicable to Exchange 2003, 2007, 2010, and 2013 with fewer than 1,000 mailboxes. You must disable directory synchronization if you would like to do a cutover migration.

A staged migration is a process where a subset of mailboxes and content is migrated in several batches over time and is applicable only to Exchange 2003 and 2007. A staged migration is typically the approach if you have more than 1,000 mailboxes. A special consideration for staged migration is that you need to identify mailboxes that must be in the same migration batch. The mailboxes of individuals participating in delegate permissions must be kept together. Therefore, they need to belong to the same batch when you plan a staged migration.

If your organization has Exchange 2010 or 2013 with more than 1,000 mailboxes, you will need to implement an Exchange hybrid deployment, which is what you implemented in Chapter 11.

Figure 12-1 shows a flowchart depicting migration options available to your organization based on your on-premises configuration.

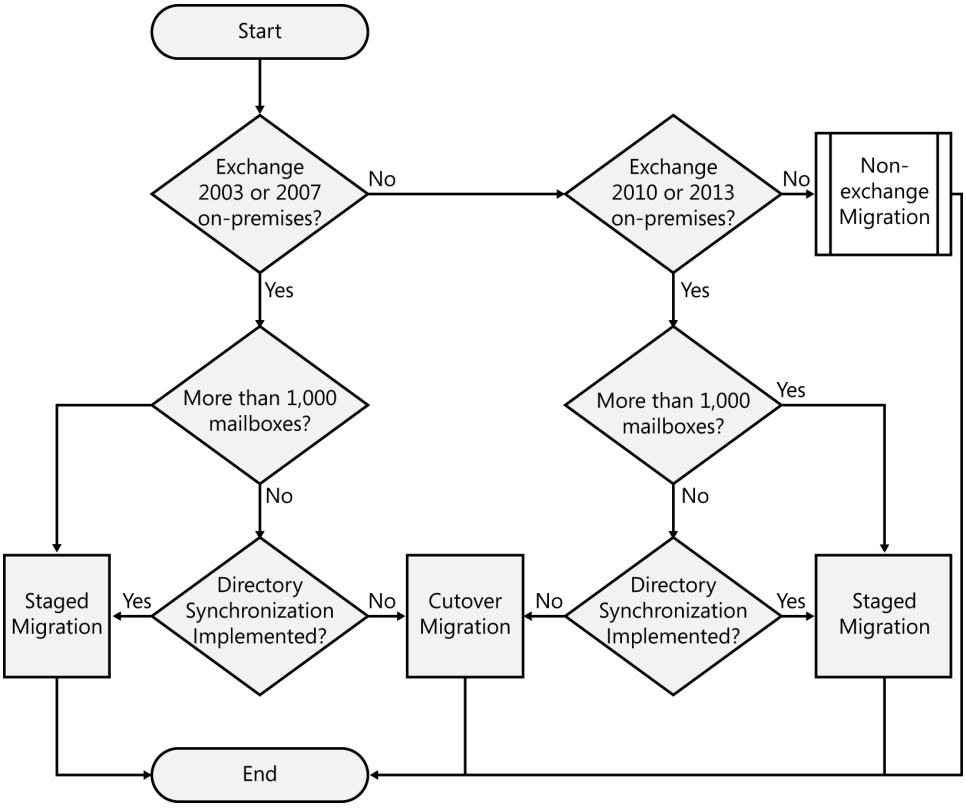

Figure 12-1 Migration options.

Cutover migration

A cutover migration is ideal for organizations with 1,000 mailboxes or less. The other important requirement for a cutover migration is that directory synchronization has not been established. The reason for this is because the cutover migration will create users in Office 365 as part of the process. Therefore, if directory synchronization is already synchronizing Active Directory (AD) objects to Office 365, you need to use a staged migration or migrate using a hybrid deployment.

A cutover migration is initiated through the Exchange admin center (EAC) for the latest release of Office 365. For organizations that are currently on Office 365 but have not been upgraded to the latest release, this is done through the Exchange Control Panel (ECP). You can also use Windows PowerShell to provision new Exchange Online mailboxes, and then migrate mailbox data from your on-premises Exchange to Exchange Online.

Before we look at how a cutover migration is set up, it is useful for you to know what happens when you execute a cutover migration. When a cutover migration is initiated, the following processes occur:

- The migration service provisions new mailboxes in Exchange Online by reading the on-premises Exchange 2003 or 2007 address book.
- On-premises distribution groups and contacts are migrated to Exchange Online.
- The migration service then migrates the contents, contacts, and calendar items from on-premises mailboxes to their corresponding online mailboxes. This part of the process is called initial synchronization.
- On-premises mailbox contents are synchronized with their corresponding online mailboxes every 24 hours. This part of the process is called incremental synchronization.
- When you are ready to complete the migration, change the MX record to start routing emails to the online mailboxes and end the migration. Exchange will conduct a final synchronization and notify the administrator through email that the migration is complete. The email notification will contain two reports:
    - **MigrationErrors.csv** This report contains a list of mailboxes that failed to migrate and information about the error.
    - **MigrationStatistics.csv** This report contains a list of mailboxes and the corresponding number of items migrated. The report also includes a unique password assigned to each mailbox that the user will need to change after initial log on. Remember that this is because the cutover migration creates new accounts as part of the migration process.

You have the option to use Autodiscover or manually configure connection settings prior to initiating the cutover migration. Configuring Autodiscover was covered in Chapter 11.

Cutover migration with the ECP

Follow these steps to execute a cutover migration using the ECP:

1. Log on to Outlook Web App (OWA).
2. On the Options menu located at the upper-right corner of the OWA window, select See All Options, as shown in Figure 12-2.

Figure 12-2 Options menu in OWA.

3. Select the Manage Myself option, and then select My Organization, as shown in Figure 12-3. This will take you to the ECP.

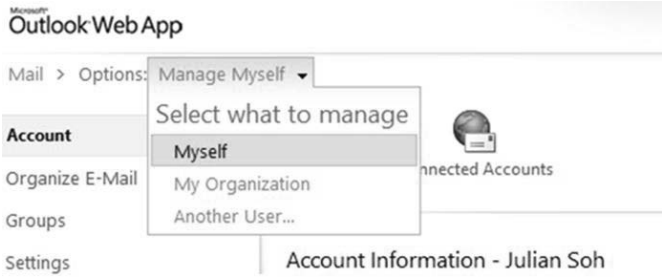

Figure 12-3 Access the ECP through the Manage My Organization menu item.

4. When the ECP appears, select the E-Mail Migration tab on the Users & Groups page, as shown in Figure 12-4.

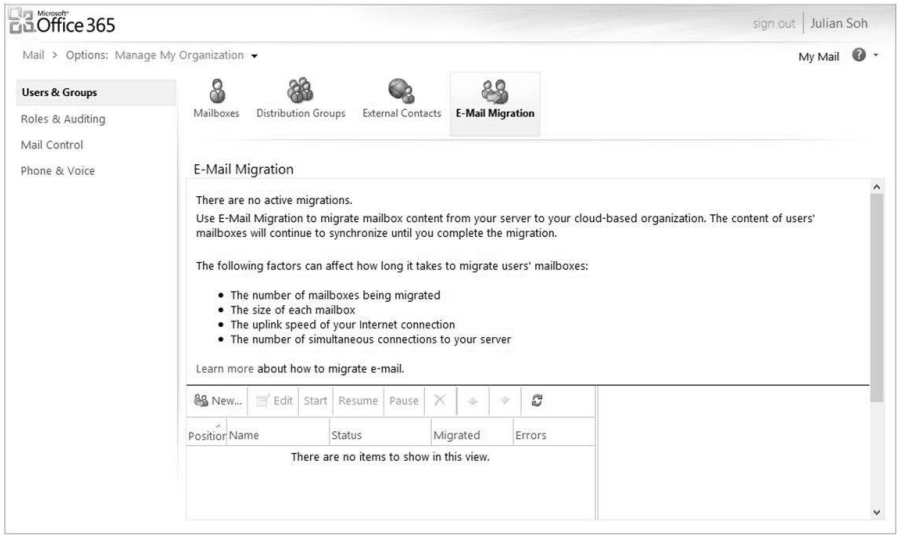

Figure 12-4 Exchange Control Panel (ECP).

5. The main pane shows migration processes and their corresponding statuses and errors. If there are any existing migration processes, you will see them listed here and you can edit, start, resume, pause, or delete the processes by using the controls on this page. To create a new cutover migration, click New.

6. Select whether to use Autodiscover, manually configure connection settings, or use IMAP for mailbox content migration, and then click Next.

7. Provide an administrator's email address, log on with a credential and password, and enter the number of mailboxes to migrate simultaneously. The default is to migrate three mailboxes simultaneously, and the maximum is 50. Click Next.

8. ECP will test the connection to your on-premises Exchange server with the Autodiscover or manual connection settings. When the connection is successful, you will be prompted to provide a name for the batch migration.

9. Provide email addresses that the migration report should be sent to by typing in the addresses or by using the Browse button to select from the global address list.

> **Note**
>
> **For more information about migrating all mailboxes to Office 365 through a cutover migration, see *http://help.outlook.com/en-us/140/ms.exch.ecp.emailmigrationwizardexchangelearnmore.aspx*.**

Cutover migration with EAC

If your organization is using the latest release of Office 365, the ECP will not be an available graphical user interface (GUI) option. Instead, you will use the EAC. To initiate a cutover migration using the EAC, follow these steps:

1. Access the Office 365 admin center at *https://portal.onmicrosoft.com*.
2. After authentication, select Exchange from the Admin menu, as shown in Figure 12-5.

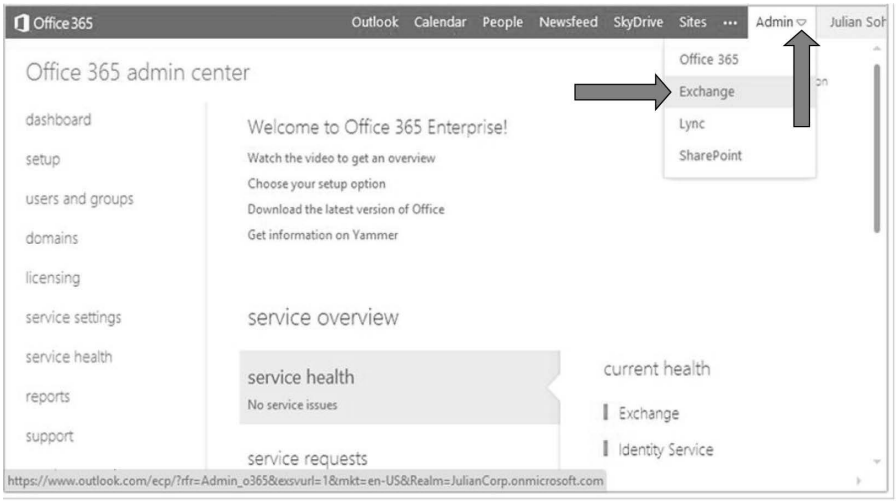

Figure 12-5 The Office 365 admin center.

3. In the EAC, select recipients on the pane on the left, and then click the migration tab, as shown in Figure 12-6.

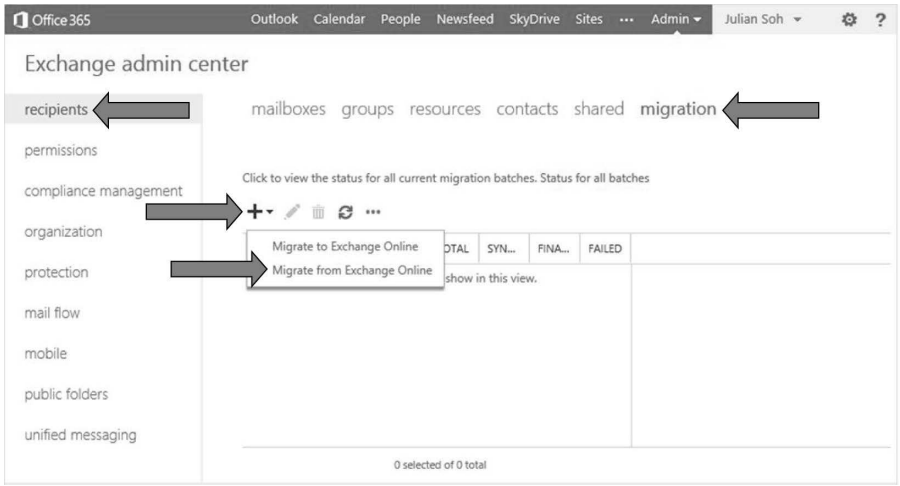

Figure 12-6 The EAC with the migration options.

4. Select Migrate to Exchange Online. You will be provided with migration options, as shown in Figure 12-7. Select the Cutover migration option, and then click next.

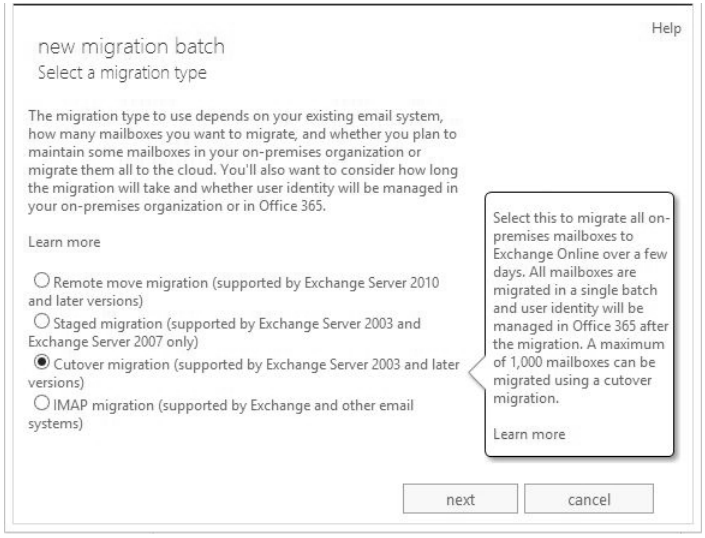

Figure 12-7 Migration options in the EAC.

5. Provide the email address of any one of the mailboxes that will be migrated, and then provide an on-premises administrator credential, as shown in Figure 12-8. Click Next.

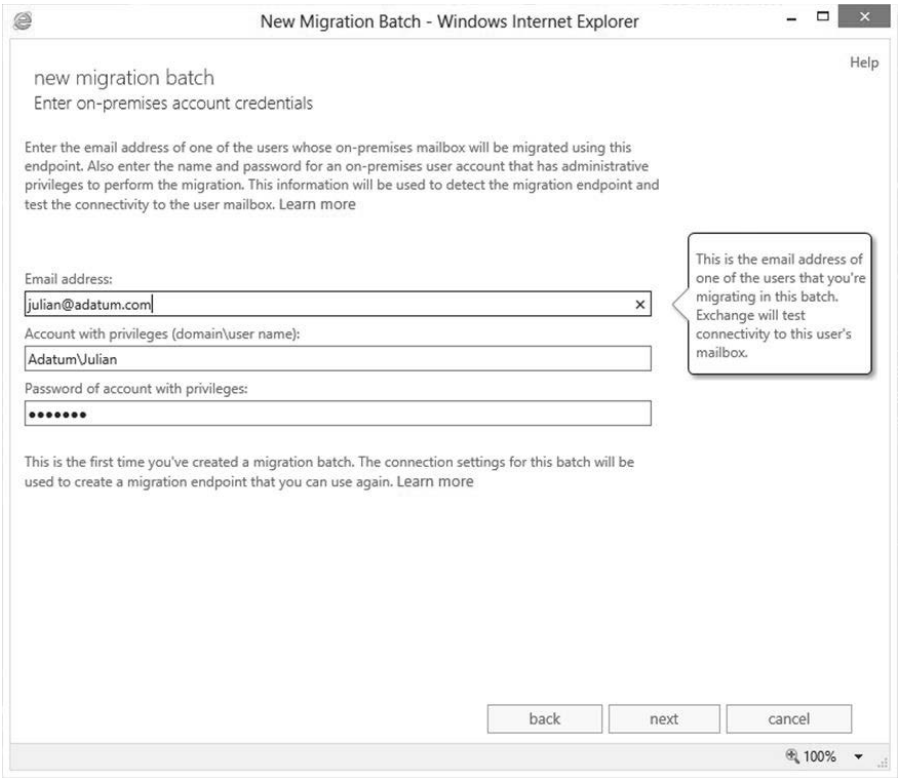

Figure 12-8 Credentials and email information for a new cutover migration batch.

6. Enter a name for the cutover migration, as shown in Figure 12-9, and then click Next.

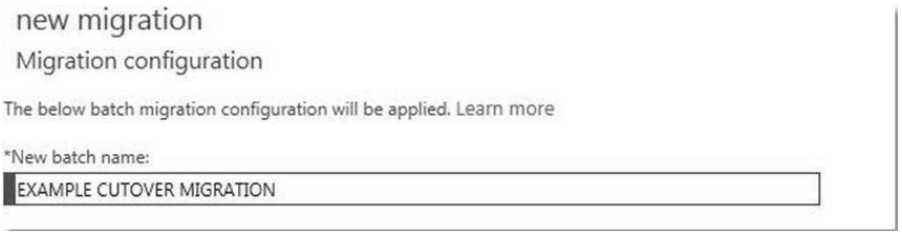

Figure 12-9 Name the cutover migration.

7. Choose to either manually or automatically start the migration and provide email addresses that a report should be sent to after the migration is complete, as shown in Figure 12-10, and then click new.

Figure 12-10 Start migration and email address of administrators.

Staged migration

A staged migration is initiated through the EAC, the ECP, or through Windows PowerShell. It is similar to a cutover migration except that you have the ability to identify a subset of mailboxes to migrate through a .csv file. Staged migration is the appropriate migration method if directory synchronization is already implemented.

Before we examine how to set up a staged migration, it is useful for you to know what happens during a staged migration. When you initiate a staged migration, the following processes occur:

- The migration service checks that directory synchronization is configured, prompts for the .csv file, and checks that each entry in the .csv file is a mail-enabled user (MEU) in Office 365.
- The service then converts the MEUs into mailboxes and populates the *TargetAddress* property of the on-premises mailbox with the email address of the cloud mailbox.
- After the *TargetAddress* property has been updated for all mailboxes, you will receive an email with a list of mailboxes that have been successfully created and converted. Mailbox contents are not migrated yet, but the users can start using the mailbox without any MX record changes. This is because if emails arrive at the on-premises mailbox, they will be redirected to Exchange Online because of the *TargetAddress* property.

- The migration service then starts to migrate the contents, contacts, and calendar items from the on-premises mailboxes to their corresponding online mailboxes. When content migration is done, another report is emailed to administrators.
- At this point, you can create and start additional migration batches.
- When you are done with migration, change the MX records so that email will be directly delivered to the online mailboxes. You can then complete the migration. The migration service will carry out any necessary cleanup and checks to make sure every MEU that has a corresponding on-premises mailbox has been migrated. A final status report will then be sent to the administrator.

Creating a .csv file

The first order of business to carry out a staged migration is to create a .csv file containing the attributes of mailboxes you want to migrate. The first row of the .csv file is the header row and should contain only the following attribute names:

- *EmailAddress* This is the SMTP address of the mailbox and is the only required attribute.
- *Password* The password that will be set for the cloud-based mailbox after it is migrated. This is an optional attribute and is not required if single sign-on (SSO) is enabled. If you set the password in the .csv file and SSO is enabled, it will be ignored. Simply leave this box blank if it does not apply to your configuration.
- *ForceChangePassword* This Boolean attribute specifies whether the user must change the password when first logging on to the cloud mailbox. The value is either *True* or *False*. This is also an optional attribute and is not required if SSO is enabled. If you set this attribute in the .csv file and SSO is enabled, it will be ignored. Simply leave this box blank if it does not apply to your configuration.

Figure 12-11 shows an example of a .csv file for a staged migration. This .csv file will cause the staged migration process to migrate five mailboxes, set the password for the new cloud mailboxes to NewPa$$word, and require only Anna and Scott to change their password upon initial logon to their respective cloud mailboxes.

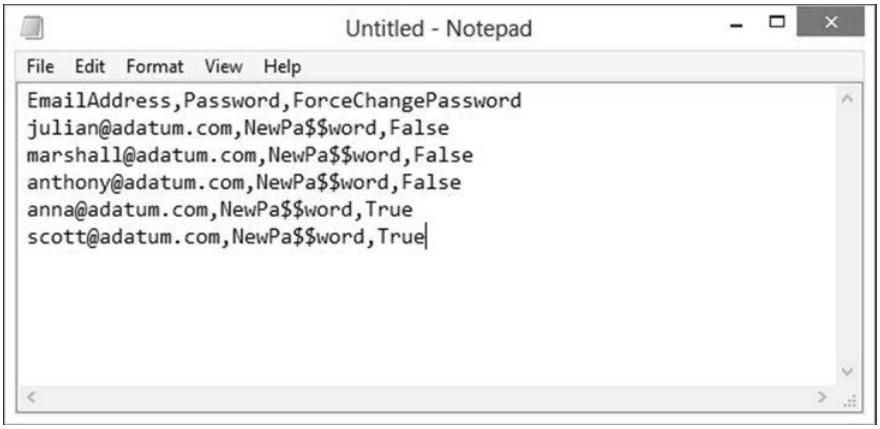

Figure 12-11 Contents of a .csv file for staged migration.

A .csv file is required regardless whether the staged migration is initiated through the ECP, the EAC, or Windows PowerShell. Furthermore, the .csv file can contain only these attributes.

INSIDE OUT **Support for non-ASCII characters**

If you need to support non-ASCII or special characters in your .csv file, then save it with UTF-8 encoding.

Staged migration with ECP

Follow these steps to initiate a staged migration using the ECP:

1. Log on to OWA.
2. From the Options menu located at the upper-right corner of the OWA window, select See All Options, as shown in Figure 12-2.

3. Select the Manage Myself option, and then select My Organization, as shown in Figure 12-3.

4. When the ECP appears, select the E-Mail Migration tab on the Users & Groups page, as shown in Figure 12-4.

5. Click New to create a new migration batch and decide whether to use Autodiscover to detect settings or to manually specify the settings by selecting the option that applies to your scenario:

   - **Exchange 2007 and later versions** Automatically detect connections settings with Autodiscover
   - **Exchange 2003 and later versions** Manually specify connection settings
   - **IMAP**

6. Provide an administrator's email address, log-on credential, password, and the number of mailboxes to migrate simultaneously. The default is to migrate three mailboxes simultaneously, and the maximum is 50.

7. When prompted for the .csv file, click the Browse button to navigate to the location and file, and then provide a name for this staged migration batch, as shown in Figure 12-12. Note that by default, a report will be sent to the administrator's email address identified in Step 7. You can provide additional email addresses if you want to have the report directed to other administrators in addition to the administrator identified in Step 7. The batch name cannot contain spaces or special characters. Click Next.

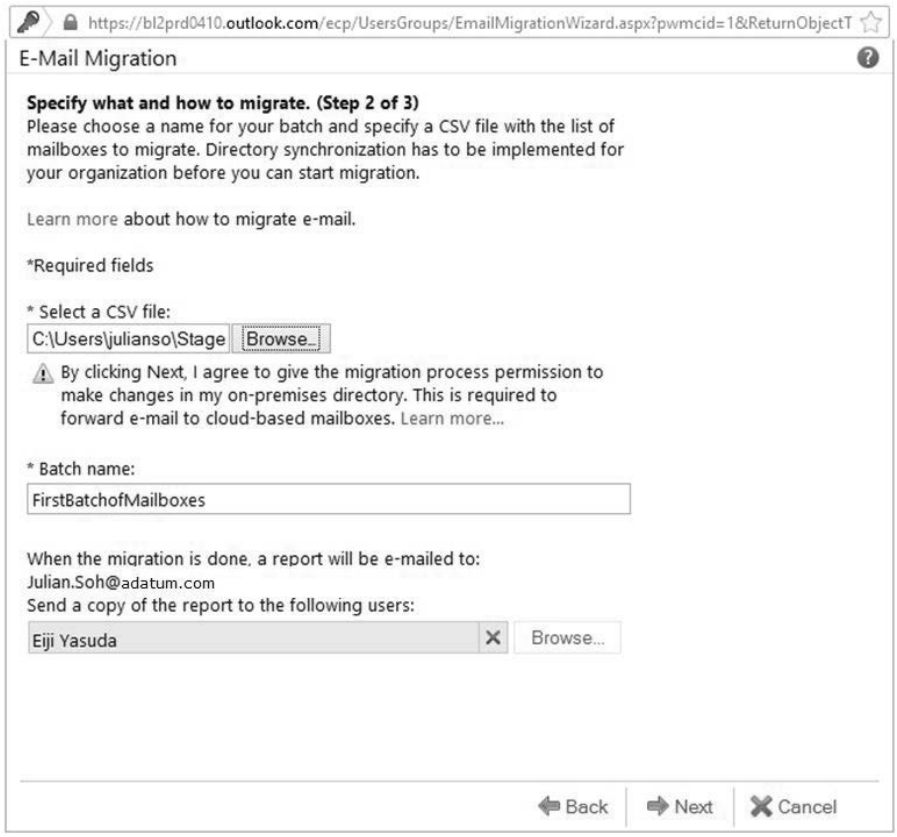

Figure 12-12 Upload a .csv file, a batch name, and a report.

8. The migration wizard will verify the .csv file and contents to make sure there are no errors before creating the migration batch. If there are validation errors, you will see a warning such as the one shown in Figure 12-13. Click the Show error details link to get detailed information about the errors. The errors could be invalid email addresses or formatting errors in the .csv file. In this particular case, we had an email address in the .csv file that was not properly formatted.

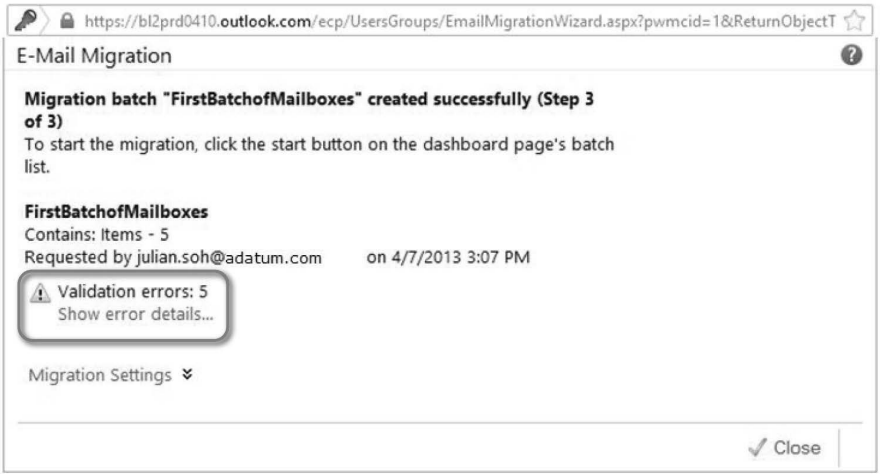

Figure 12-13 Validation errors with a .csv file.

9. Click Close.

10. On the E-Mail Migration page in the ECP, the staged batch migration you just created should be listed, as shown in Figure 12-14. Select it and click Start to begin the batch migration.

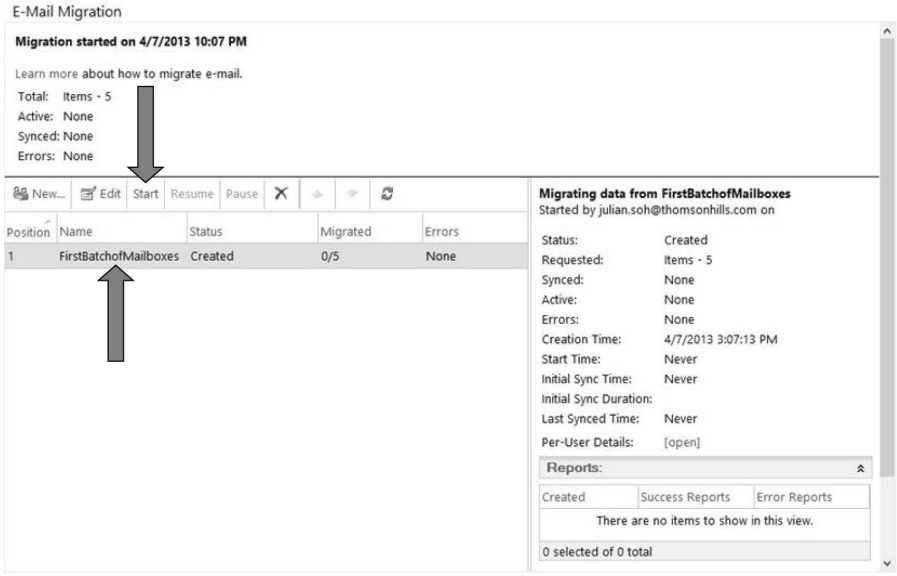

Figure 12-14 Starting a migration batch.

11. After you have started the migration, you can monitor the process by selecting the batch migration and looking at the statistics located in the right pane, as shown in Figure 12-14. The status of the migration, number of mailboxes migrated, and errors are also listed along with the migration batch.

Staged migration with EAC

Starting a staged migration from the EAC is similar to a cutover migration from the EAC. Follow these steps to initiate a staged migration from the EAC:

1. Access the Office 365 admin center at *https://portal.onmicrosoft.com*.

2. After authentication, click the Admin menu on the upper-right corner of the page and select Exchange, as shown in Figure 12-5.

3. In the EAC, select recipients on the pane on the left and then select the migration tab, as shown in Figure 12-6.

4. Select Migrate to Exchange Online. You will be provided with migration options, one of which is a staged migration. Select it, as shown in Figure 12-15, and then click next.

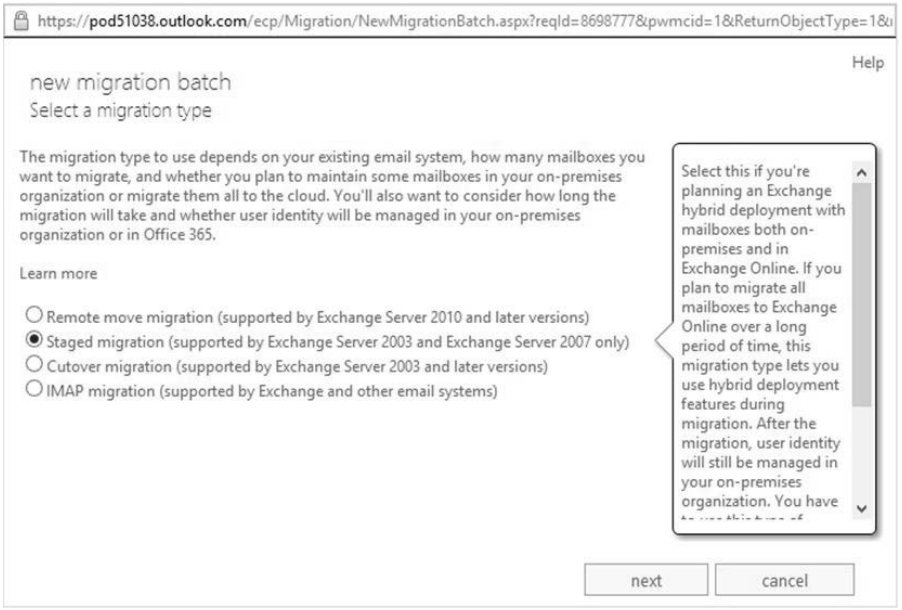

Figure 12-15 Select Staged migration from the list of migration options.

5. Click the Browse button, navigate to the location of the .csv file, and select it. The wizard will read the .csv file, determine the number of mailboxes to be migrated, and display that information, as shown in Figure 12-16. Click next.

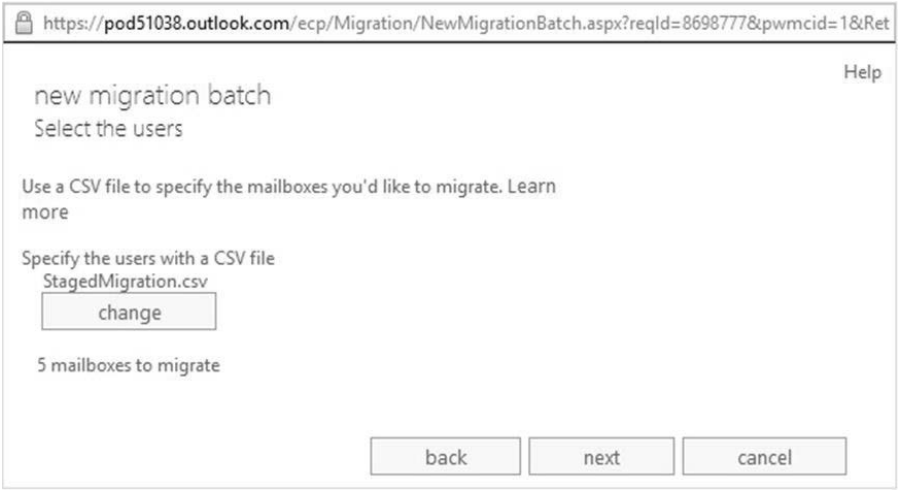

Figure 12-16 Selecting the .csv file in the EAC migration wizard.

6. Provide account credentials of an account that has access to the on-premises mailboxes that need to be migrated. The account is in the down-level format (*domain**user name*), as shown in Figure 12-17. Do not use the user principal name (UPN) as the account name. Click next.

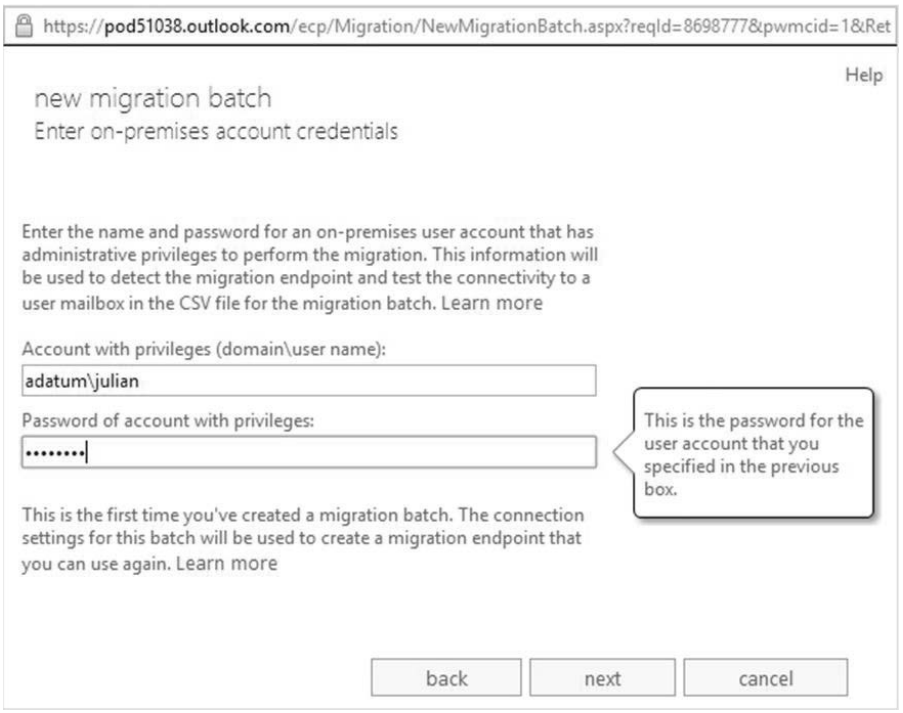

Figure 12-17 Provide credentials of an account with permissions to on-premises mailboxes.

7. The migration wizard will try to automatically detect settings. If it is not able to do so, you will need to manually provide your on-premises server settings, as shown in Figure 12-18. Enter the information, if requested, and click next.

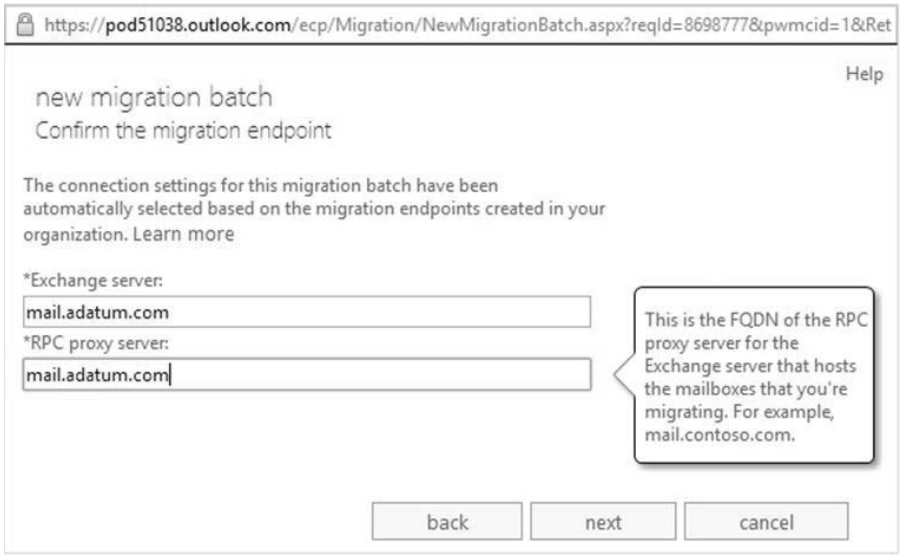

Figure 12-18 Connection settings in the event that automatic detection fails.

8. Give the migration batch a name, as shown in Figure 12-19, and then click next.

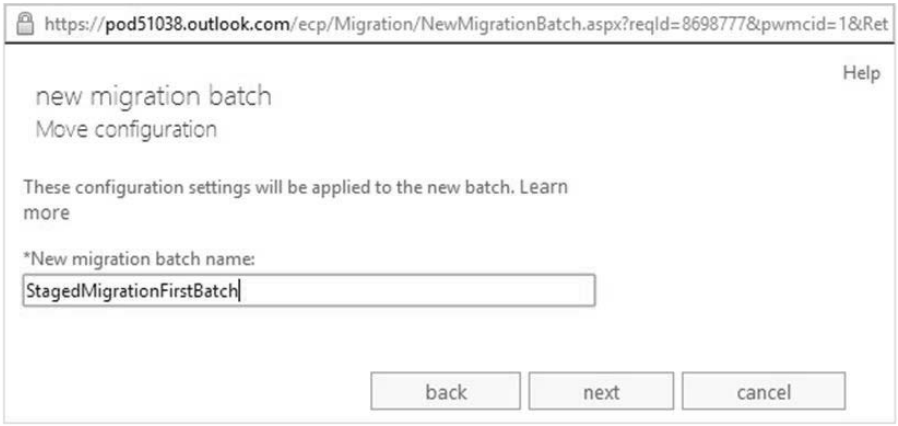

Figure 12-19 Provide a name for this phased migration batch.

9. Click browse to select administrators who should receive a report when the migration is completed, as shown in Figure 12-20. Click new to create the migration batch.

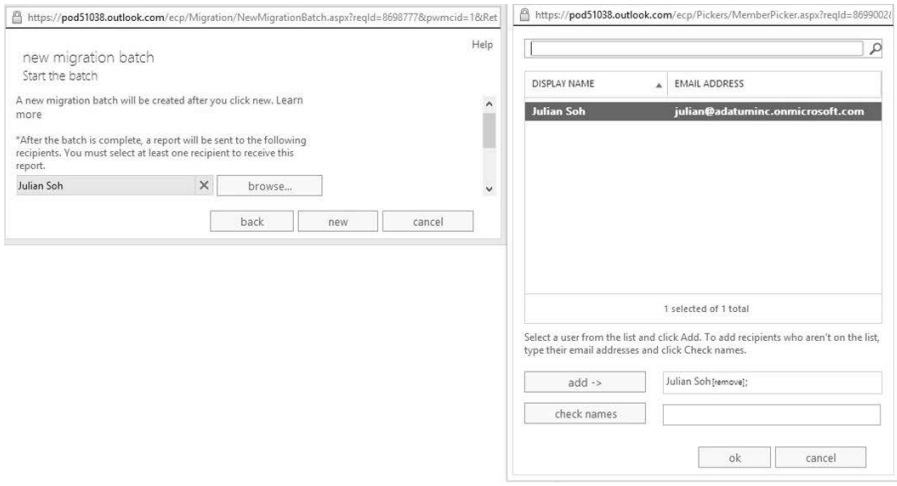

Figure 12-20 Select report recipients.

10. After the migration batch is created, you can view its status and start it from the EAC, as shown in Figure 12-21.

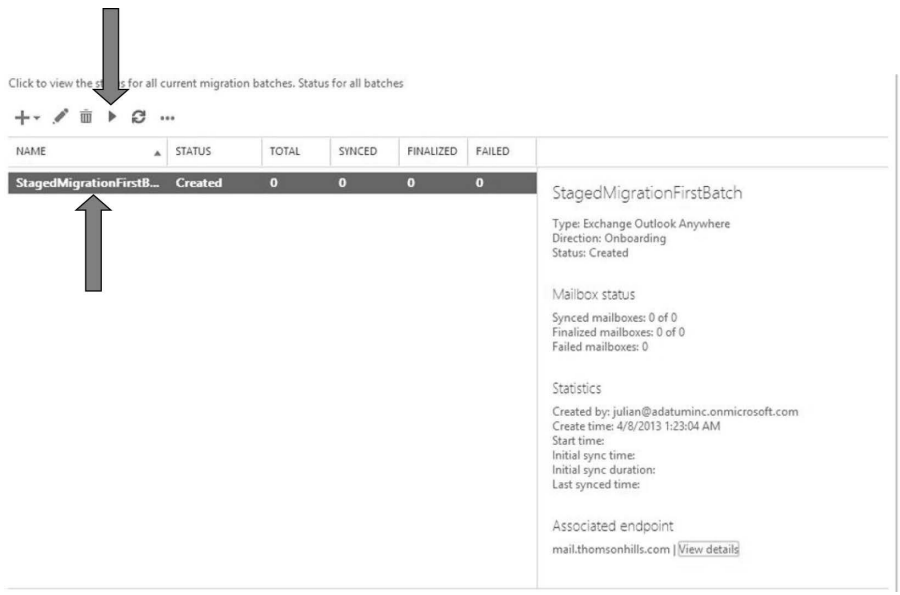

Figure 12-21 Starting the phased batch migration.

IMAP migration

An IMAP migration is commonly used in migrations from non-Exchange email systems to Exchange Online. As the name implies, the on-premises email system will need to have the IMAP protocol enabled to use an IMAP migration method. Prior to initiating an IMAP migration, there are two manual tasks you must perform:

- Create the Exchange Online mailboxes for users whose mailbox contents you want to migrate.
- Create a .csv file with the email address, user name, and password for each mailbox you will be migrating.

Like cutover and staged migrations, you will use either the ECP or EAC GUI to initiate an IMAP batch migration. You can also use Windows PowerShell to initiate an IMAP batch migration.

Creating a .csv file

Create a .csv file to target the on-premises users' mailboxes whose content you want to migrate to Exchange Online. The first row of the .csv file is the header row and should contain only the following attribute names:

- *EmailAddress* This is the user ID for the user's cloud-based mailbox in UPN format. Note that this is not the SMTP address; this is the user ID in Office 365.
- *UserName* This is the user logon name for the on-premises mailbox on the IMAP server.
- *Password* This is the password for the user's account on the on-premises IMAP mailbox server.

The .csv file for an IMAP migration batch must not be larger than 10 MB and cannot contain more than 50,000 rows. Furthermore, all three attributes are required. Contacts, calendar items, and tasks cannot be migrated with the IMAP method.

IMAP migration with the ECP

Follow these steps if your organization has not been upgraded to the latest release of Office 365 and would like to use the ECP to initiate an IMAP migration. This section assumes you have created mailboxes in Exchange Online for the on-premises users for whom you want to migrate content.

1. Log on to OWA.

2. From the Options menu located at the upper-right corner of the OWA window, select See All Options, as shown in Figure 12-2.

3. Select the Manage Myself option at the upper left, and select My Organization, as shown in Figure 12-03. This will take you to the ECP.

4. In the ECP, as shown in Figure 12-04, select E-Mail Migration under Users & Groups.

5. To create a new IMAP migration, click New, then select IMAP.

6. As shown in Figure 12-22, provide the fully qualified domain name (FQDN) of the on-premises email server in the IMAP server box. Select the authentication type, encryption level, and the IMAP port if it is not the standard port 993 for IMAP. Finally, specify the number of mailboxes to simultaneously migrate. Click Next.

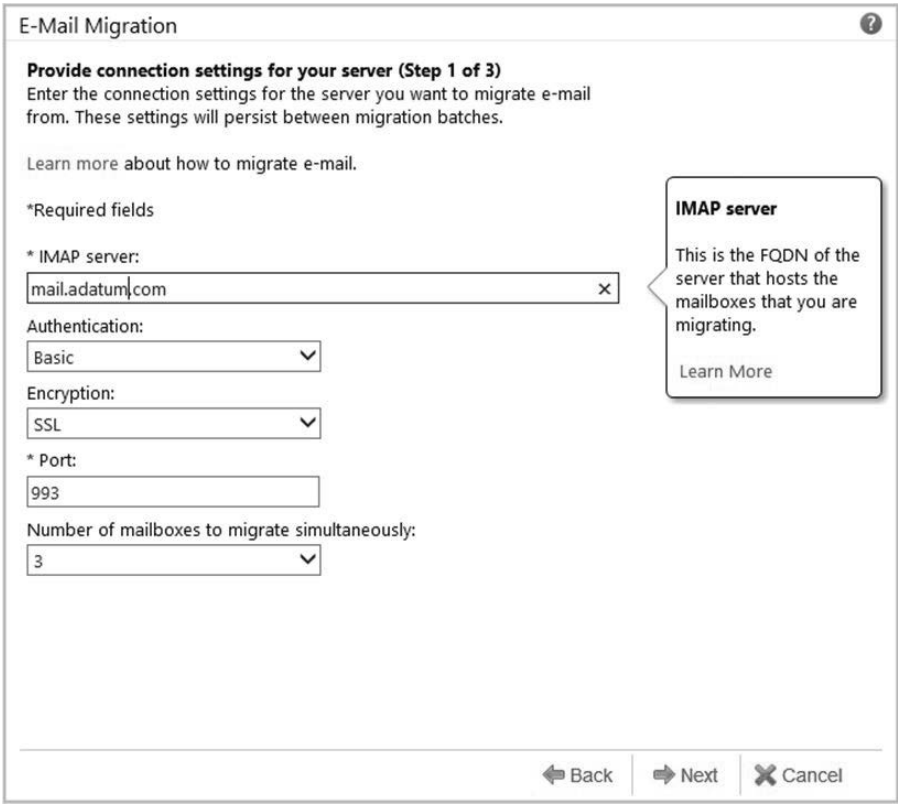

Figure 12-22 IMAP server settings.

7. The migration wizard will test the connection settings by attempting to connect to the on-premises mail server with the IMAP protocol. If successful, it will prompt you for the .csv file.

8. Click the Browse button to navigate to the location and .csv file. Provide a name for the IMAP migration in the Batch name box. Batch names cannot have spaces or special characters.

9. Click Add folders to exclude if you do not want to migrate the contents of certain folders, such as contents in the Deleted Items folder.

10. Type the name of the folder and click the Add button to add the folder to the exclusion list. Make sure you type the name of the folder exactly as it appears. Repeat this step until all the folders you want to exclude are added to the list. Click OK.

11. To send copies of the migration report to other administrators, click Browse at the bottom of the page and add other administrators. Click Next.

12. Exchange Online will check the .csv file to ensure that no errors are detected. If there are no errors, you will be notified that the .csv file successfully passed the checks.

13. Review the information about the migration batch, and then click Close.

14. The IMAP migration batch should now appear in the list in the ECP E-Mail Migration window. Select it, and then click Start to initiate the migration.

15. After the migration is completed, change your MX records so that new mail will be delivered to the cloud mailboxes.

IMAP migration with the EAC

If your organization is using the latest release of Office 365 and would like to use the EAC, follow these steps to initiate an IMAP migration:

1. Access the Office 365 admin center at *https://portal.onmicrosoft.com*.

2. After authentication, click the Admin menu on the upper-right corner of the page and select Exchange, as shown in Figure 12-05.

3. In the EAC, under recipients, select the migration tab from the main pane, as shown in Figure 12-6.

4. Select Migrate to Exchange Online. You will be provided with migration options, one of which is IMAP migration. Select it, and then click next.

5. Click the Browse button and navigate to the location and the .csv file. Click Open, and then click next.

6. Exchange Online will check the .csv file to ensure that no errors are detected. If there are no errors, you will see the number of mailboxes detected in the .csv file. Click next to continue.

7. As shown in Figure 12-23, provide the FQDN of the on-premises email server in the IMAP server box. Select the authentication type, encryption level, and the IMAP port if it is not the standard port 993 for IMAP. Finally, specify the number of mailboxes to simultaneously migrate. Click next to continue.

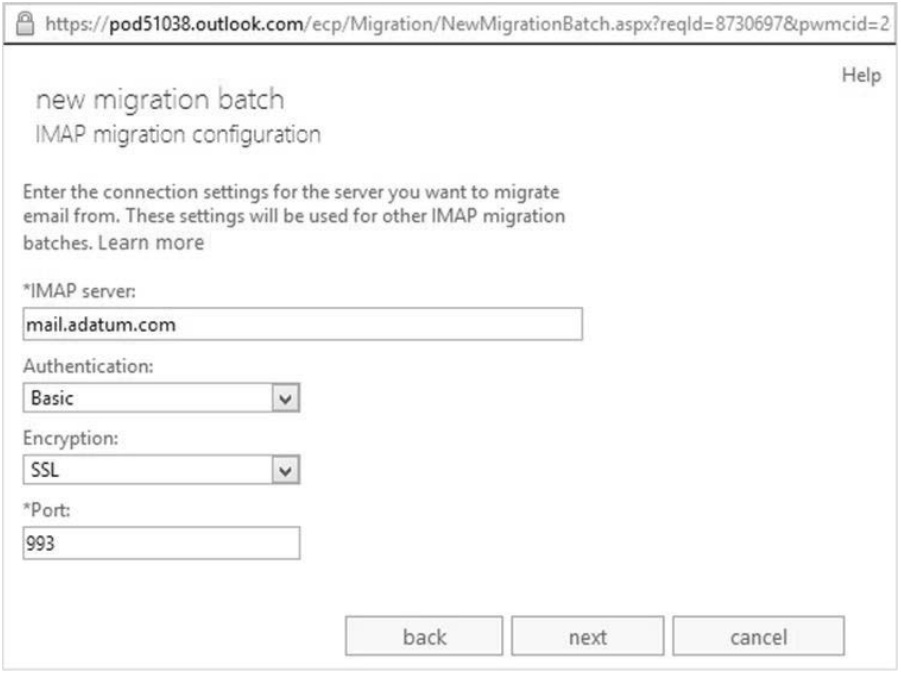

Figure 12-23 Provide IMAP connection settings.

8. If the IMAP settings in Step 7 are correct and Exchange Online can connect to the on-premises server through IMAP, the wizard will use the information to create a migration endpoint. On the Confirm the migration endpoint page, click next.

9. After the migration endpoint has been successfully created, the information about the endpoint will be displayed on the IMAP migration configuration page. Click next.

10. On the Move configuration page, provide a name for the migration batch, and then click next.

11. On the Start the batch page, click browse to select additional administrators to whom you would like to send a copy of the migration report once the migration is complete.

12. Select whether to automatically start the batch or to manually start it later. Click new to create the batch.

13. After migration is complete, modify your MX record to point to Office 365 Exchange Online.

Migration using remote Windows PowerShell

Windows PowerShell can be used to initiate cutover or staged migrations. The commands are slightly different depending on whether you are using the latest release of Office 365 or not.

Using remote Windows PowerShell with Office 365 with Exchange Online 2010

A cutover migration to Exchange Online 2010 can be done through remote Windows PowerShell by following these steps:

1. Connect to Exchange Online by creating a *PSSession* using the following commands:

```
Import-Module MSonline

$cred = Get-Credential

Connect-MsolService -Credential $cred

$Session = New-PSSession -ConfigurationName Microsoft.Exchange-ConnectionUri
https://ps.outlook.com/powershell/ -Credential $cred -Authentication Basic
-AllowRedirection

Import-PSSession $Session -AllowClobber
```

2. Create a connection string containing the migration settings:

```
$MigrationSettings = Test-MigrationServerAvailability –Exchange –Credentials
(Get-Credential) –ExchangeServer <on-premises Exchange fqdn> -RPCProxyServer
<external Outlook Anywhere fqdn>
```

3. When prompted, enter the on-premises credentials of a user who has full access privileges to the on-premises mailboxes.

4. Create the migration batch by entering the following command:

```
New-MigrationBatch –Exchange –Name <Batch Name> -ExchangeConnectionSettings
$MigrationSettings.ConnectionSettings –MaxConcurrentMigrations <number of
concurrent migrations> -TimeZone <TimeZone in double quotes, example "Pacific
Standard Time">
```

5. Start the migration by entering the following command:

```
Start-MigrationBatch
```

6. During the migration, you can monitor the progress by entering the following command:

```
Get-MigrationBatch | fl Status
```

INSIDE OUT **Cutover migration best practices**

Plan to do a cutover migration over a weekend and change the MX record as soon as the cutover migration is successfully completed. Remember that cutover migrations are for organizations with 1,000 or fewer mailboxes, and even though there is a final synchronization, it is common for mailboxes to be missing items between synchronizations if a cutover migration is left in synchronized mode for an extended period of time. Therefore, plan to complete a cutover migration in a single pass and switch the MX records as soon as possible. It also helps if prior to the migration you set the Time to Live (TTL) for your MX records to be fairly short, thereby reducing the time required for Domain Name System (DNS) convergence. The *Complete-Migration* cmdlet is deprecated as of April, 2012. For more information, *see http://community.office365.com/en-us/blogs/office_365_technical_blog/archive/2012/04/04/why-administrators-don-t-see-the-complete-migration-button-in-the-e-mail-migration-tool.aspx*.

Using remote Windows PowerShell with the latest release of Office 365 with Exchange Online 2013

Follow these steps to initiate a migration to Exchange Online 2013 using remote Windows PowerShell:

1. Open a new *PSSession* by entering the following commands:

```
Import-Module MSonline

$cred = Get-Credential

Connect-MsolService -Credential $cred

$Session = New-PSSession -ConfigurationName Microsoft.Exchange-ConnectionUri
https://ps.outlook.com/powershell/ -Credential $cred -Authentication Basic
-AllowRedirection

Import-PSSession $Session -AllowClobber
```

2. Enter the following command to create a new migration endpoint:

```
$SourceEndPoint = New-MigrationEndpoint -ExchangeOutlookAnywhere -Name
SourceEndPoint -Credentials (Get-Credential) -ExchangeServer <on-premises
Exchange FQDN> -RpcProxyServer <on-premises Outlook Anywhere FQDN>
-EmailAddress <SMTP address of an on-premises mailbox to be migrated>
```

3. To create a cutover migration batch, go to Step 4. To create an IMAP migration batch, go to Step 5. To create a *staged migration* batch, enter the following command:

```
$StagedBatch = New-MigrationBatch -Name StageBatch1 -SourceEndpoint
$SourceEndPoint.Identity -CSVData ([System.IO.File]::ReadAllBytes("<path and
filename of CSV file"))
```

4. To create a cutover migration batch, enter the following command:

```
$CutoverBatch = New-MigrationBatch -Name CutoverBatch1 -SourceEndpoint
$SourceEndPoint.Identity -TimeZone "<Time Zone. For example:
Pacific Standard Time>"
```

5. To create an IMAP migration batch, enter the following command:

```
$IMAPBatch = New-MigrationBatch –Name
```

6. Start the migration batch automatically by adding the *–AutoStart* parameter to the commands in Step 3 or 4. Otherwise, you can manually start the migration batch by entering the following command:

```
Start-MigrationBatch –Identity $StagedBatch.Identity
```

or

```
Start-MigrationBatch –Identity $CutoverBatch.Identity
```

Migration with an Exchange hybrid environment

Migration after establishing an Exchange hybrid environment is one of the most popular approaches because, unlike the other methods we have covered so far, after you establish an Exchange hybrid environment, you can move mailboxes to the cloud and back to on-premises. Part of setting up an Exchange hybrid environment is to implement an Exchange 2010 Service Pack 3 (SP3) Client Access Server (CAS). This introduces the Mailbox Replication Service (MRS) that comes with the 2010 SP3 CAS. MRS is the service responsible for carrying out mailbox moves.

In Chapter 11, we discussed in depth how an Exchange hybrid model is implemented. As such, we will not be covering the steps again here.

Microsoft Exchange PST Capture

With Exchange Online, your users have large mailboxes with access to a personal archive. As mentioned before, this makes personal folders (.pst) files obsolete. If your organization has .pst files, in addition to migrating mailboxes you might have to search for .pst files on computers in your organization so you can incorporate the contents into personal archives. This can be accomplished with Microsoft PST Capture.

PST Capture works with Exchange on-premises and Exchange Online. Therefore, you have two import options:

- Discover .pst files and import contents to an on-premises Exchange server first, then migrate mailboxes to Exchange Online. In this scenario, the on-premises Exchange server must be Exchange 2010 or Exchange 2013.
- Discover .pst files and import contents directly to Exchange Online.

PST Capture comprises the following components:

- **PST Capture Central Service** The Central Service maintains the list of .pst files found in your organization and manages the migration of the data into Exchange Online.
- **PST Capture Agent** This is the component that needs to be installed on computers in your organization and is responsible for locating .pst files associated to the computer it is installed on. The agent is also responsible for transmitting the .pst file to the Central Service during import operations.
- **PST Capture Console** The PST Console is the administrator interface to configure .pst discovery, configure the import process, and also import .pst files from network storage devices that do not have capture agents installed.

> **Note**
>
> **For more information about Microsoft PST Capture, see *http://technet.microsoft.com/en-us/library/hh781036(EXCH.141).aspx*. Pay special attention to the permissions required for PST Capture. The PST Capture Console and Agent also require the .NET Framework 4.5.**

Installing and using PST Capture

Implementing a PST Capture strategy involves installing the PST Capture Console first. Follow these steps to install the PST Capture Console:

1. Download Microsoft PST Capture and PST Capture Agent from the Microsoft Download Center at *http://www.microsoft.com/en-us/download/details.aspx?id=36789*.

2. Use a user account that is part of the local Administrators Group of a host computer to install the PST Capture Console. The host computer must have a 64-bit operating system that is Windows 7 or Windows 8, Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012. It also must have the .NET Framework 4.5.

3. Next, you need to deploy the agents. Even though you can manually install the PST Capture agent, to distribute it to multiple computers you need to use a software distribution solution such as System Center Configuration Manager. You can start Windows installer with the following parameters to initiate an unattended installation:

   ```
   Msiexec /I PSTCaptureAgent.msi /q CENTRALSERVICEHOST=<IP Address or FQDN of
   Capture Console> SERVICEPORT=6674
   ```

4. After all the agents have been distributed to the computers on your network, start the PST Capture Console. As shown in Figure 12-24, there are two major actions: New PST Search and New Import List.

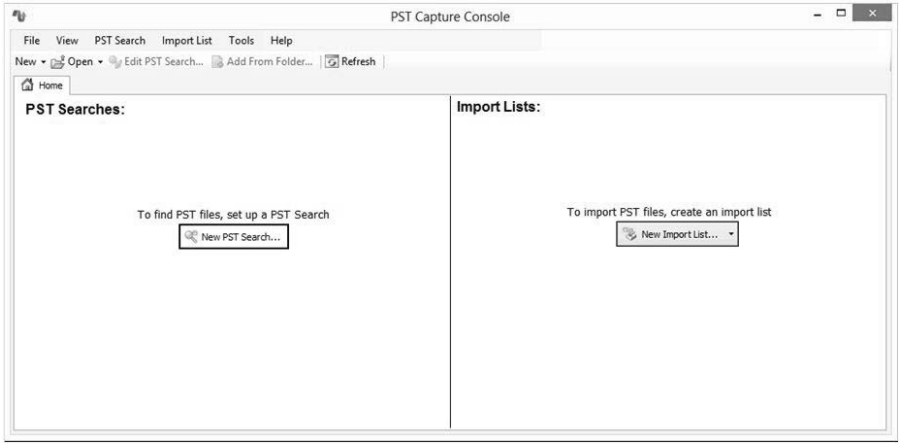

Figure 12-24 PST Capture Console.

5. Before searching for .pst files, you need to specify your online connection settings. From the Tools menu, select Settings.

6. On the Settings page, under Online Connection, provide the credentials of an Office 365 administrator account.

7. If you are migrating .pst content directly to Office 365 Exchange Online, select the The above is an Office 365 Server check box and provide the server name. To determine your Exchange Online server name, use the ECP by going to OWA, selecting Options, selecting See All Options, and clicking the Settings for Post Office Protocol (POP), IMAP, and SMTP access link, as shown in Figure 12-25.

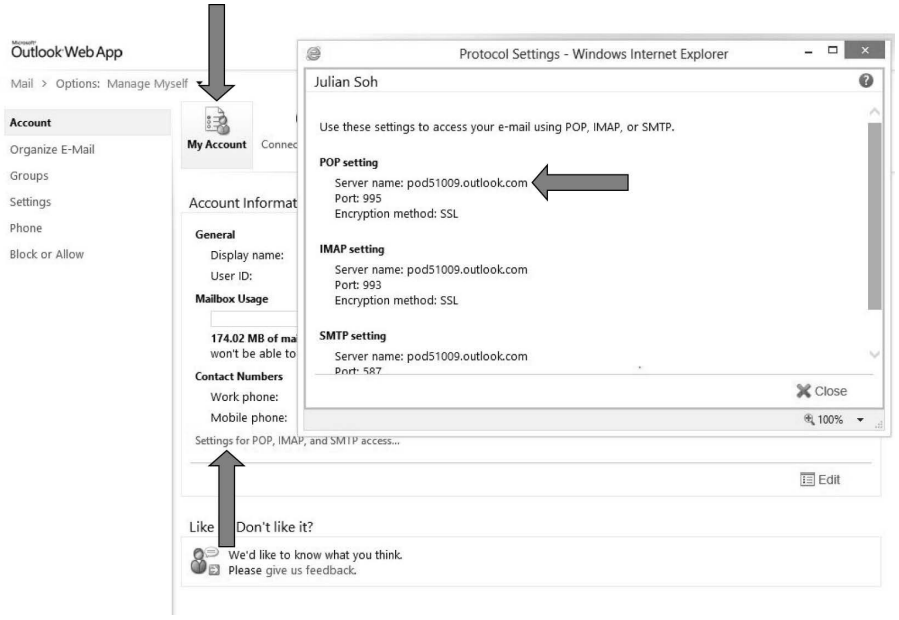

Figure 12-25 ECP showing your Exchange Online information.

8. After you have entered the information in the Online Connection Settings page, click Check. If the PST Capture Console can connect to Exchange Online with the credentials, you will see the "Successfully connected to Exchange Online" message, as shown in Figure 12-26. Click OK to save the settings and close the window.

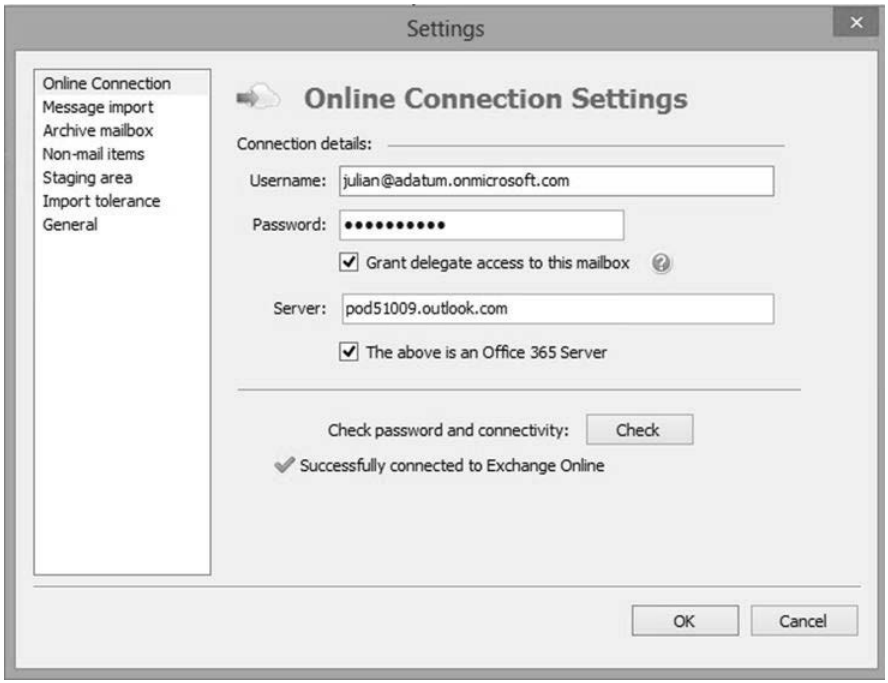

Figure 12-26 Successfully connected to Exchange Online.

9. Click New PST Search to invoke the New PST Search Wizard, as shown in Figure 12-27. Note that there are four steps. At the first step, select the Computers node, and then click Next.

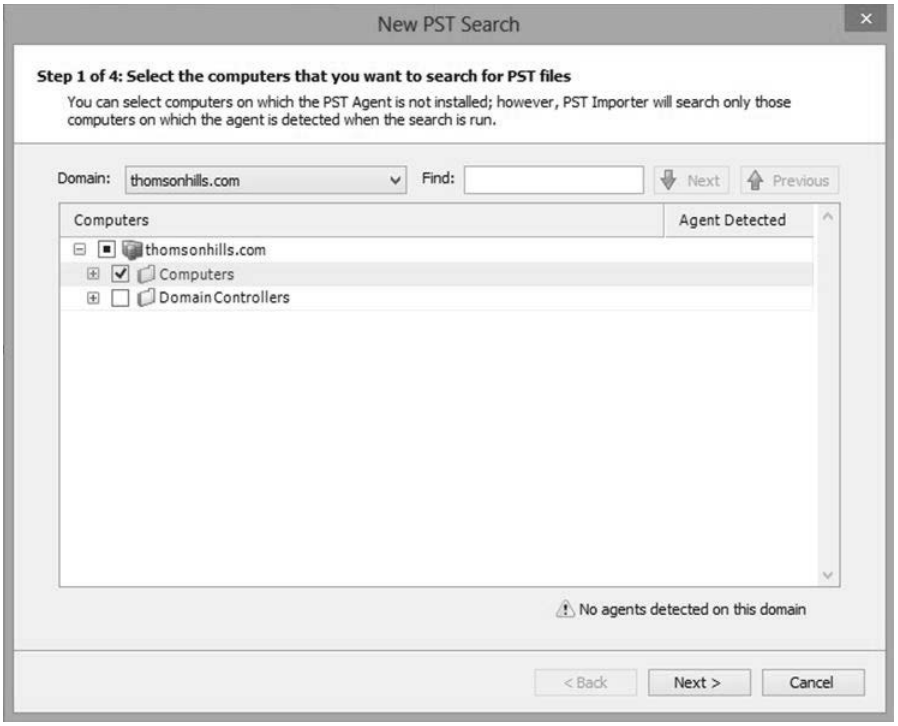

Figure 12-27 New PST Search Step 1 of 4.

10. In Step 2 of the New PST Search Wizard, specify the computers' storage locations to include and exclude when searching for .pst files, as shown in Figure 12-28, and then click Next.

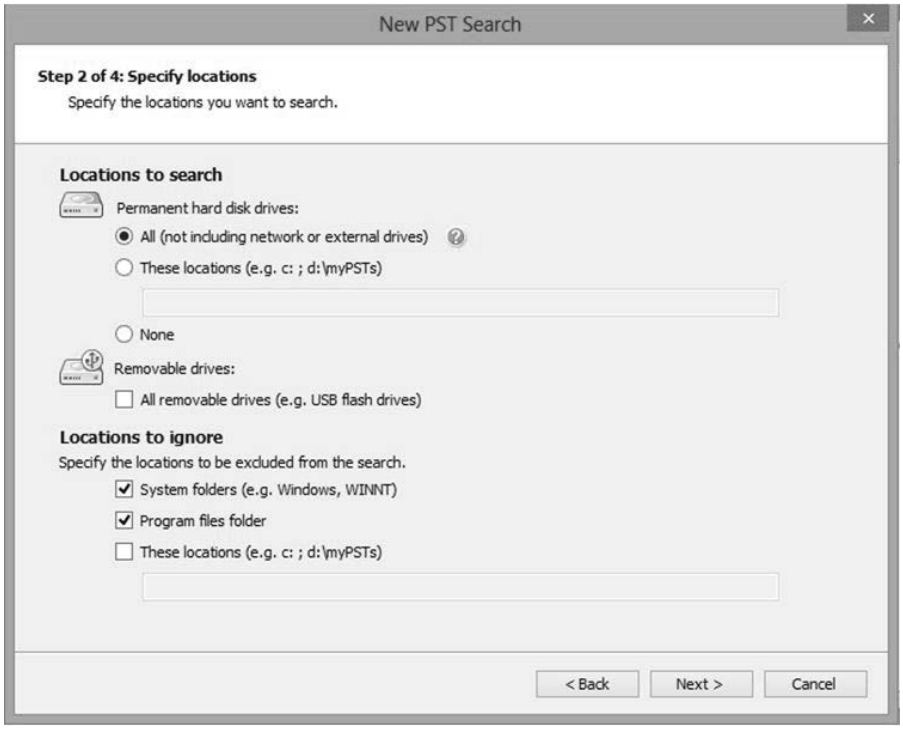

Figure 12-28 New PST Search Wizard Step 2 of 4: Specify locations.

11. In Step 3 of the New PST Search Wizard, you can choose to schedule this search at an off-peak time by specifying the date and time, or you can accept the default of No schedule so you can manually start this search. Click Next.

12. In the last step of the New PST Search Wizard, give the search a name, as shown in Figure 12-29, and then click Finish.

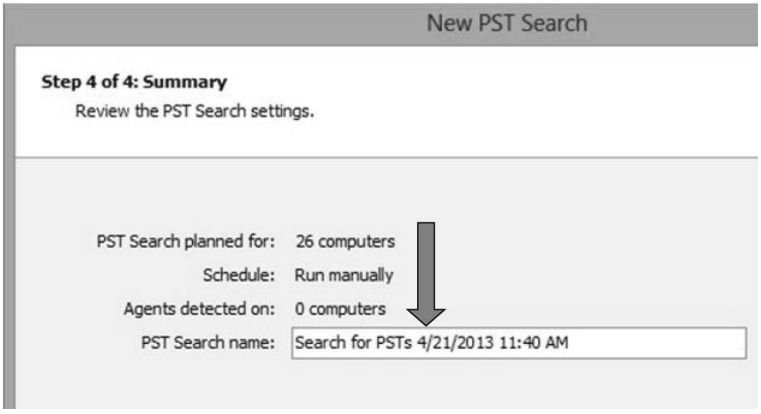

Figure 12-29 New PST Search Wizard Step 4 of 4: Provide a PST search name.

13. A new PST Search is created, and the details are displayed in a separate tab in the PST Search Console, as shown in Figure 12-30. Note the following key information: Number of computers included in the search scope, the status of each task, and whether the search is scheduled or not. Also, make sure the agent is detected for the computers that are in this PST Search. There is a Search All Now button you can use to invoke this search. Click this button to manually start the search now.

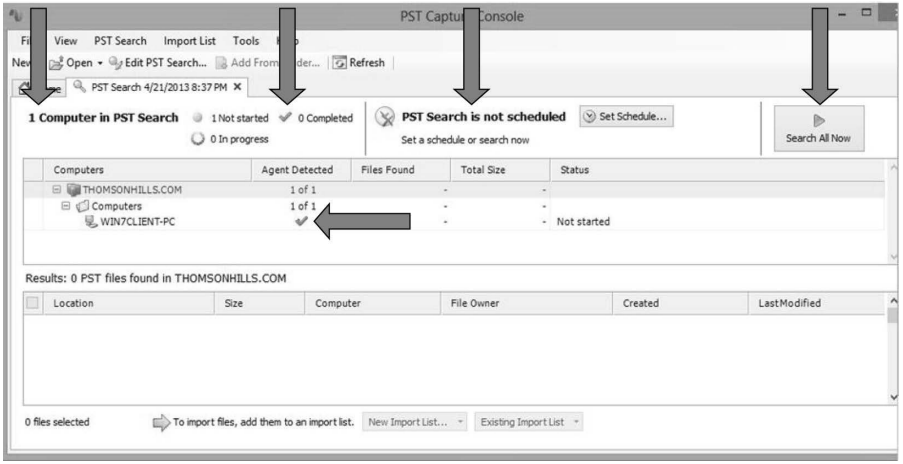

Figure 12-30 PST Capture Console: search information.

14. When the search is complete, the status beside each computer selected will be Completed and the number of PST files found, if any, will be listed in the Files Found column together with the total size of all the PST files found on the computer. Figure 12-31 shows the results of a computed PST search.

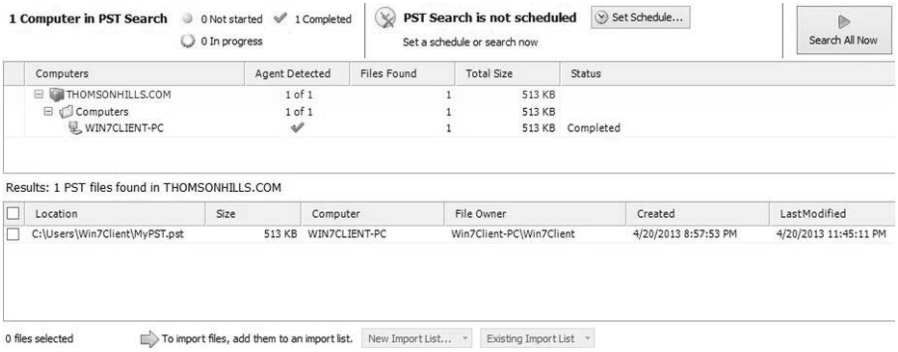

Figure 12-31 PST search results.

15. Select the .pst files you want to import by selecting the check boxes. Then click the New Import List button at the bottom of the page.

16. You will see a drop-down list with two options: Cloud Import List and OnPrem Import List. As mentioned before, you can use PST Capture to import content from .pst files to an on-premises Exchange server or directly into Exchange Online. For this exercise, select Cloud Import List.

17. Set the .pst files to a destination mailbox by clicking the Set mailbox link, as shown in Figure 12-32. A list of mailboxes will be listed in a separate window. Select the destination mailbox from the list, and then click OK.

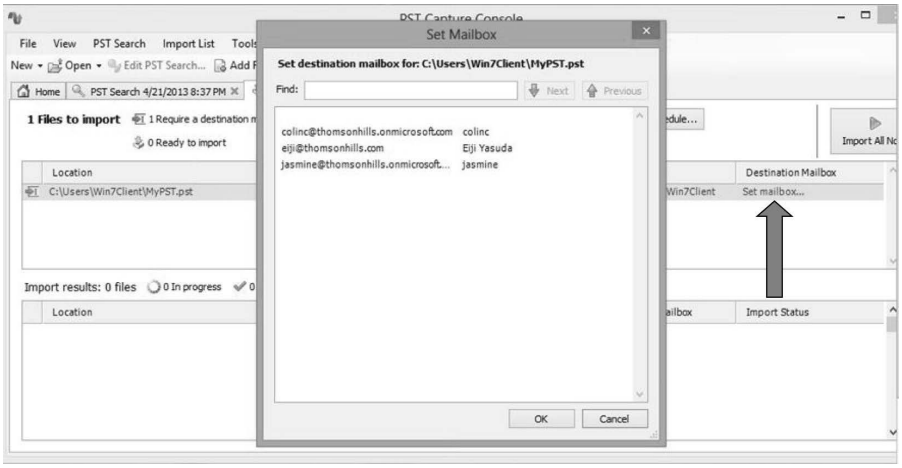

Figure 12-32 Setting destination mailbox.

> **Note**
>
> **If you recently set the online connection settings (Step 8), the Set Mailbox window might be empty. This is because the PST Console has not retrieved a list of all the mailboxes on Exchange Online. Wait for a while, and then try again. Depending on the number of mailboxes in Office 365, it might take some time.**

18. Click the Import All Now button to start importing .pst contents to the respective destination mailboxes.

Although we did not cover all the settings for the PST Capture Console, you can explore the different options available, such as setting the staging area, import tolerance, and whether to import non-mail items such as calendars. Click Tools from the PST Capture Console menu and select Settings. Next, review the available settings options and configure them to meet your organization's needs.

Third-party migration tools

If for some reason the existing tools and options provided by Microsoft do not meet your migration needs, there are always third-party tools you can turn to. Examples of third-party Exchange migration tools are Quest Software, Binary Tree, BitTitan, Cemaphore, and Metalogix. Exchange is a mature platform and has been around for some time. Therefore, third-party tools are readily available and are just as mature.

Migration best practices

There are several best practices when migrating mailboxes. We will list some of the common ones you should consider adopting when migrating mailboxes from on-premises mail servers to Exchange Online.

Reduce the TTL for MX records

In most scenarios, you will want to route incoming email to Exchange Online. Therefore, before starting any of the migration tasks, regardless of whether it is a cutover, staged, or IMAP migration, change the Time To Live (TTL) of your MX records so as to improve the DNS convergence time when you do switch your MX records. The recommendation is that you change the TTL to 3,600 seconds, which is one hour.

Migration performance

There are many factors that affect migration performance, such as the size and number of items in the mailboxes, network bandwidth, network latency, and the on-premises mail servers. Migration performance can also be affected by the time of day and the number of users on the network. That is why you should carry out migrations after the work day is done or over weekends. As an example, after initial tests with a small staged migration batch, Microsoft Consulting Services generally aims to ramp up to a migration rate of 1,000 mailboxes a week, mostly conducted after business hours when network utilization is at the lowest level.

As we mentioned in Chapter 2, "Planning and preparing to deploy Office 365", bandwidth is not necessarily the only factor. Latency and sustained throughput are factors that are just as important when it comes to migration performance. For an idea on how much throughput is required for the different types of migration options we covered in this chapter, refer to the Migration Performance white paper referenced in the following Inside Out sidebar. In the Migration Performance white paper, an important metric to note is that past experience has shown that a 5 GB to 10 GB per hour rate of data migration can be reliably achieved, but depends on the Internet connection.

INSIDE OUT **"Migration Performance" white paper**

Microsoft has provided an excellent TechNet article about migration performance based on experience and observations from actual customer migrations to Office 365. The "Migration Performance" white paper is located at *http://technet.microsoft.com/en-us/library/jj204570*.

If you are going to use Microsoft PST Capture, you can import the .pst files to your on-premises mailbox first and then do a migration, or you can import the .pst files directly to cloud mailboxes. PST imports are bandwidth-intensive operations, so you need to take that into consideration when scheduling and designing your PST import strategy.

Migration service throttling

In the migration exercises that you looked at earlier in this chapter, recall that you have the ability to specify the number of mailboxes that are migrated simultaneously, which by default is three. Specifying the number of mailboxes that should be simultaneously migrated is referred to as migration-service throttling.

Refer again to the "Migration Performance" white paper or test a single mailbox migration to determine the migration throughput. This will help you determine the optimum number of simultaneous migrations your network can support.

User throttling

User throttling mostly affects third-party migration tools. User throttling limits the number of mailboxes a user can access simultaneously and is designed to minimize risks and preserve resources. Therefore, if a migration tool uses a single service account with access to all mailboxes, Office 365 might throttle the service account if it starts to access too many mailboxes simultaneously during the migration process, thereby impacting migration performance. When you evaluate migration tools, make sure that performance will not be impacted by user throttling. Good migration tools generally use Exchange Web Services to impersonate user accounts so Exchange Online is not seeing a single user simultaneously accessing multiple mailboxes, but rather the users accessing their respective mailboxes. Thus, user throttling will not be triggered.

Moving mailboxes back to on-premises Exchange

Moving mailboxes back to on-premises can be facilitated only through an Exchange hybrid environment. Otherwise, you will need to rely on third-party tools. Unlike having the cutover and staged migration options from the EAC and ECP, when moving mailboxes to Office 365, there are no built-in options to carry out the reverse.

As you saw in Chapter 11, after you have implemented an Exchange hybrid environment, the move of a mailbox to Office 365 is done by carrying out a remote move request. To move mailboxes back on-premises, you need to take into consideration whether the mailboxes you want to move were created in Office 365 from the very beginning or whether they were first created on-premises and then moved to Office 365.

Mailbox originally created on-premises

If the mailbox you want to migrate from Office 365 was initially created on-premises and then migrated to the cloud, all you have to do is submit a new remote move request from the Exchange Online organization to the Exchange on-premises organization through the Exchange Management Console (EMC). Follow these steps to see how this is accomplished:

1. Start the EMC. Expand the Microsoft Exchange On-Premises node and navigate to the Recipient Configuration node. As shown in Figure 12-33, right-click the Recipient Configuration node, right-click a mailbox in the middle pane, and select New Remote Move Request from the drop-down menu.

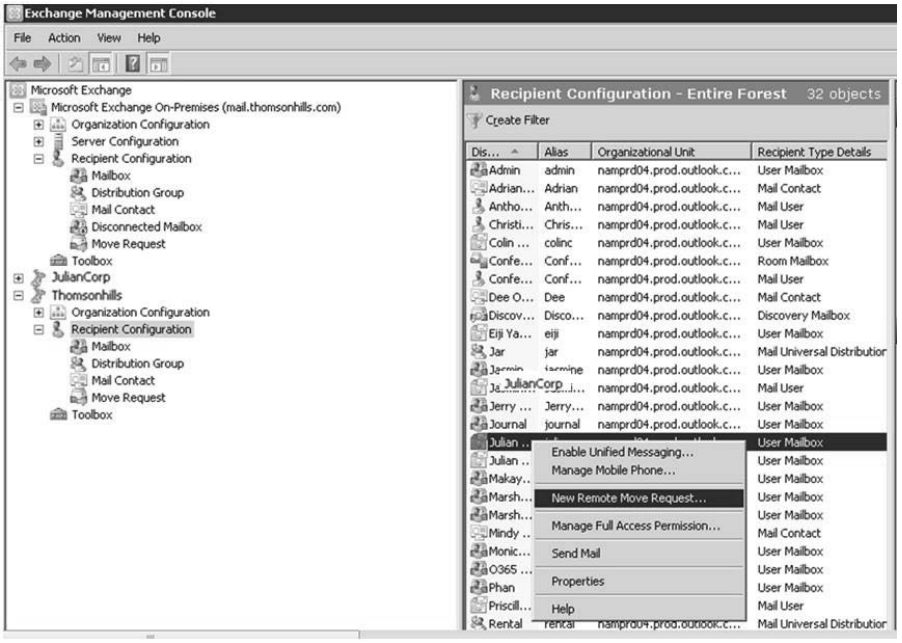

Figure 12-33 Remote Move Request from Office 365.

2. Follow the steps in the Remote Move Request Wizard, as in Chapter 11. When you get to the Move Settings page, select your on-premises domain in the Target Delivery Domain box. In the Remote Target Database box, if you are migrating to an Exchange 2010 server, use the format <*Server*>\<*Database Name*>, as shown in Figure 12-34. If you are migrating to an Exchange 2003 or 2007 server, use the format <*Server*>\<*Storage Group*>\<*Database Name*>; for example, MAIL\First Storage Group\Mailbox Database.

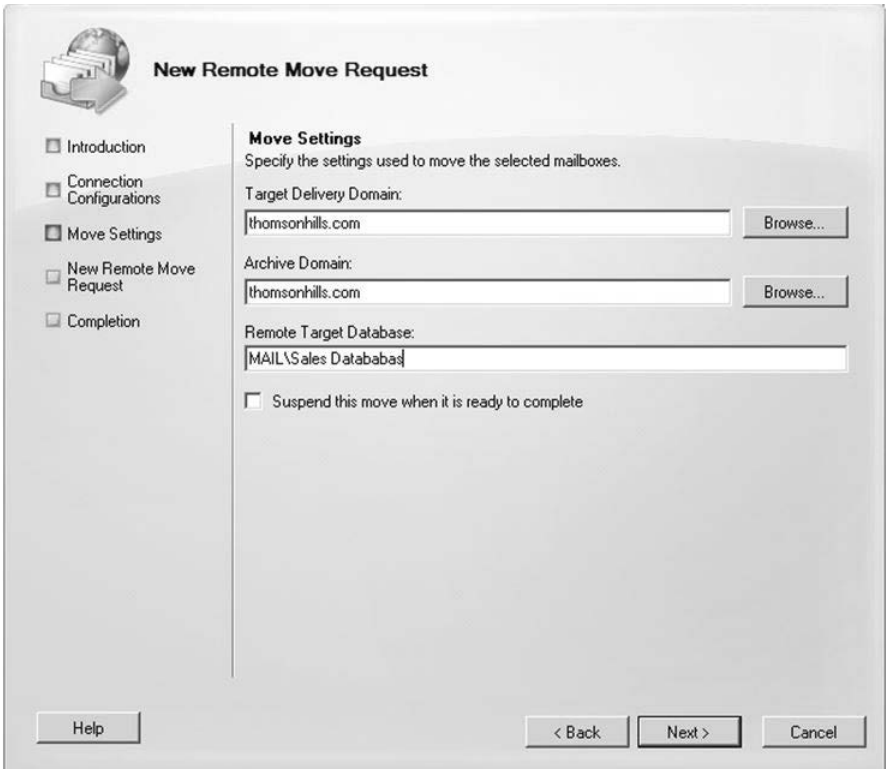

Figure 12-34 Move Settings page.

3. Complete the rest of steps in the New Remote Move Request Wizard, and then click New to initiate the move request.

Mailbox originally created in Exchange Online

If the Exchange Online mailbox you want to move back to on-premises Exchange was originally created in Office 365, you will need to first set the *ExchangeGUID* property on the associated on-premises mailbox. You need to do this because the *ExchangeGUID* property is not synchronized back to the associated on-premises mailbox if the mailbox was initially created in Office 365. For a remote move request to succeed, the value stored in the *ExchangeGUID* property must be the same for the mailbox in Office 365 and the associated on-premises remote mailbox.

Follow these steps to check and set the *ExchangeGUID* property for the on-premises remote mailbox:

1. Start the EMC on your on-premises Exchange hybrid server or management computer.

2. Check if the *ExchangeGUID* property on the on-premises remote mailbox is set by entering the following command. Figure 12-35 shows an example of the output as a result of issuing the command:

```
Get-RemoteMailbox <alias of cloud mailbox to migrate back on-premises> | For-
mat-List ExchangeGUID
```

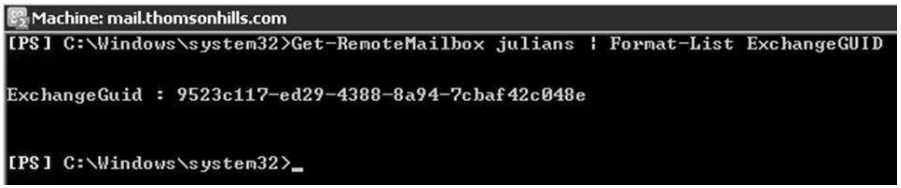

Figure 12-35 Checking the value of *ExchangeGUID*.

3. If the return value for *ExchangeGUID* is ***not*** all zeros, as shown in Figure 12-35, then *ExchangeGUID* is set. You can immediately initiate a remote mailbox move back to on-premises Exchange by following the steps outlined in the "Mailbox originally created on-premises" section.

4. If the return value for *ExchangeGUID* is all zeros, then *ExchangeGUID* is not set. On a separate computer, start the Windows Azure Active Directory Module for Windows PowerShell and connect to Exchange Online. Do not use the Exchange Management Shell. As a reminder, you can use the following syntax to connect to Exchange Online through remote Windows PowerShell:

```
Import-Module MSonline

$cred = Get-Credential

Connect-MsolService -Credential $cred

$Session = New-PSSession -ConfigurationName Microsoft.Exchange-ConnectionUri
https://ps.outlook.com/powershell/ -Credential $cred -Authentication Basic
-AllowRedirection

Import-PSSession $Session -AllowClobber
```

5. Enter the following command to retrieve *ExchangeGUID* for the Exchange Online mailbox, and write down the returned value:

```
Get-Mailbox <alias of the cloud mailbox to migrate back to on-premises> \ For-
mat-List ExchangeGUID
```

6. Go back to the Exchange Management Shell window, and enter the following command to set the value of the *ExchangeGUID* property on the on-premises remote mailbox:

   ```
   Set-RemoteMailbox <alias of cloud mailbox to move> -ExchangeGUID <GUID>
   ```

7. Start an unscheduled directory synchronization process using the *Start-OnlineCoexistenceSync* command. Refer to Chapter 4, "Directory synchronization", if you need a refresher on how to do this.

8. After directory synchronization is complete, you can follow the steps outlined in the preceding section to move the mailbox from the cloud back to on-premises.

Decommissioning on-premises Exchange

The subject of decommissioning on-premises Exchange is most applicable to organizations that have created an Exchange hybrid environment. It might seem logical to consider decommissioning all on-premises Exchange after all mailboxes and email workloads have been migrated. However, it is important to note that if your organization wants to manage Exchange Online with the EMC, a minimum of one Exchange on-premises CAS must still exist in the forest.

If directory synchronization is implemented, Active Directory is then the source of authority, and Microsoft recommends not removing the last Exchange 2010 on-premises server. By removing the last on-premises Exchange server, you will be unable to make changes to the mailbox objects in Exchange Online because the source of authority is defined as on-premises.

The bottom line is that you should keep one Exchange 2010 CAS on-premises, for now. A more detailed discussion about this topic is covered by the Microsoft Exchange team on their team blog referenced in the following Inside Out sidebar.

INSIDE OUT

Microsoft recommendation on decommissioning Exchange on-premises

You can read about the Exchange team's recommendation to maintain on-premises Exchange 2010 CAS and the reasons on the Exchange Team Blog located at *http://blogs.technet.com/b/exchange/archive/2012/12/05/decommissioning-your-exchange-2010-servers-in-a-hybrid-deployment.aspx*.

Administering Exchange Online

Because Exchange on-premises, Exchange Online, and the Exchange hybrid environment are based on a common set of technologies, the management tools and experience are similar across the different deployment models. The administration tools for Exchange are the following:

- 2010 SP3 Exchange Management Console (EMC)
- Windows PowerShell
- Office 365 admin center and the browser-based EAC, including managing Exchange Online Protection (EOP) in the latest release of Office 365 with Exchange Online 2013
- Forefront Online Protection for Exchange (FOPE) Administrator Console for Office 365 with Exchange Online 2010

This book does not cover all the intricacies of administering Exchange and messaging; there are dedicated Exchange books for that. What we will do is provide a summary of the different administration tools and focus on the specifics of administering Exchange Online and the Exchange hybrid environment and introduce you to the new capabilities in Exchange Online 2013.

Exchange Management Console

The EMC serves as a familiar interface for Exchange administrators. To manage Exchange Online through the EMC, you need to maintain an on-premises Exchange Client Access Server (CAS). To use EMC as the administration tool, simply add Exchange Online as a new organization into EMC, as shown in Chapter 11. However, note that there are differences between what you can administer in Exchange on-premises versus Exchange Online, and this is reflected in the EMC. For example, because there is no need for you to manage the server configuration in Exchange Online, the Server Configuration node is not present for the Exchange Online organization in EMC, as shown in Figure 12-36.

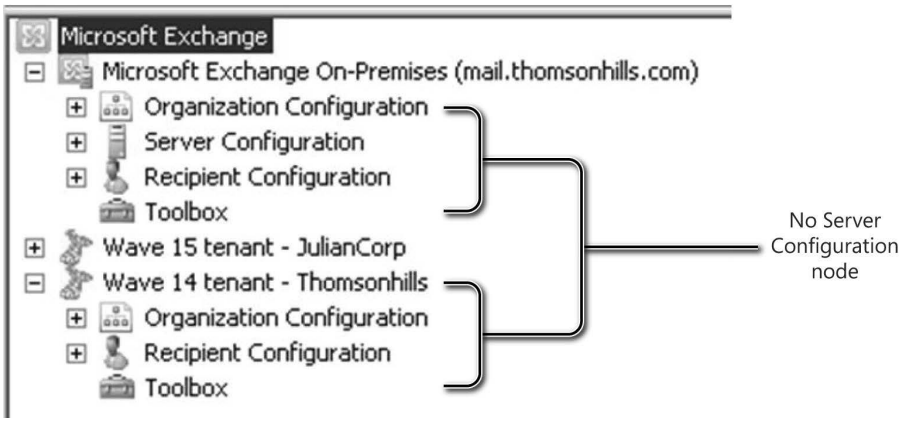

Figure 12-36 Difference between Exchange on-premises and Exchange Online in the EMC.

Implementation of an Exchange hybrid environment through Exchange 2010 SP3 CAS also provides the capabilities to create and manage the hybrid components as workloads, such as remote mailbox moves and managing the hybrid configuration, as shown in Figure 12-37 and through the tasks covered in Chapters 11 and 12, "Mailbox migration and administering Exchange Online".

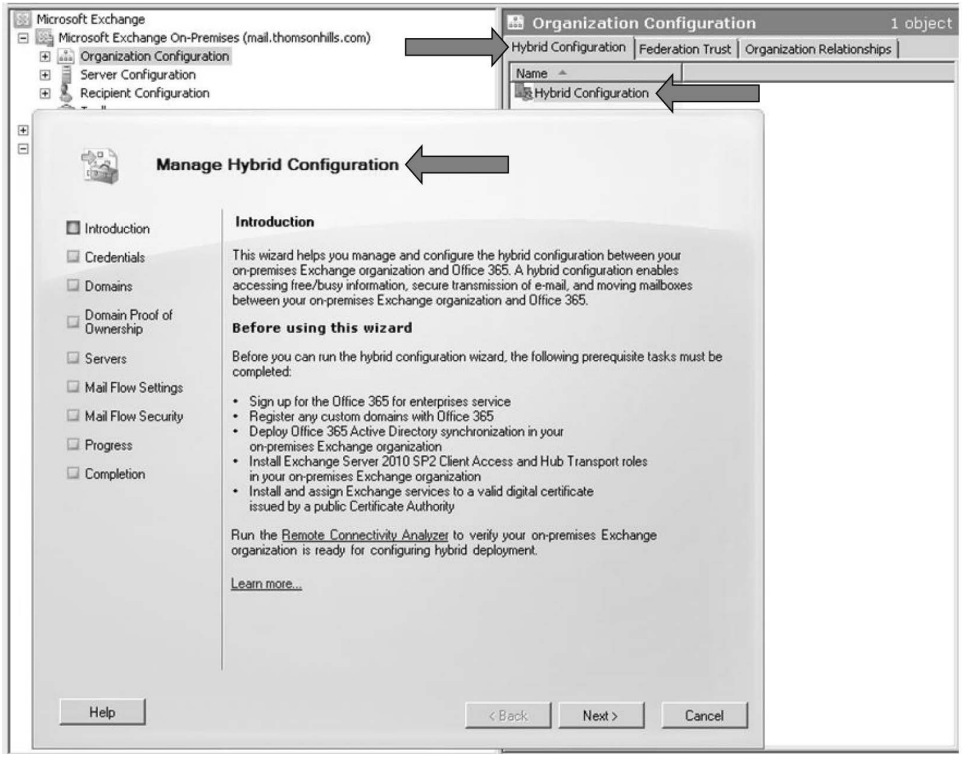

Figure 12-37 Using EMC to manage hybrid configuration.

Exchange Online remote Windows PowerShell

A majority of Office 365 Windows PowerShell cmdlets are for Exchange Online, and Windows PowerShell is the recommended approach to managing Exchange. To manage Exchange Online through remote Windows PowerShell, you first need to establish a new session. We use the following base script as a template in the Windows PowerShell ISE:

```
#Base script for managing Exchange Online

Import-Module MSonline

$cred = Get-Credential

Connect-MsolService -Credential $cred

$Session = New-PSSession -ConfigurationName Microsoft.Exchange-ConnectionUri https://
ps.outlook.com/powershell/ -Credential $cred -Authentication Basic -AllowRedirection

Import-PSSession $Session -AllowClobber

#

# <Exchange Online Management cmdlets> #

#

Remove-PSSession $Session
```

Between the *Import-PSSession* and *Remove-PSSession* commands, you can insert the vast array of remote Windows PowerShell cmdlets for Exchange Online.

> **Note**
>
> **A reference to all the available Windows PowerShell cmdlets for Exchange Online is located at *http://help.outlook.com/en-us/exchangelabshelp/dd575549.aspx*.**

INSIDE OUT

Clear your *PSSession*

It is important to always clear your session with the *Remove-PSSession* cmdlet because there is a maximum of three sessions per logon. Therefore, if you do not clear a session, you run the risk of running out of sessions and will need to wait for a session to timeout before you can open a new session.

Exchange Online administration user interface

Another management tool is a browser-based user interface (UI), which takes the form of the Exchange Control Panel (ECP) or the Exchange admin center (EAC), depending on which release of Office 365 your organization is using. One of the key new capabilities in Exchange is Role Based Access Control (RBAC). RBAC provides the ability to delegate administrative tasks, some of which may be handled by non-technical personnel. For example, the responsibility for conducting electronic discovery (eDiscovery) should belong to compliance or legal personnel. Therefore, there is a need for an easy interface to manage such functions without having to distribute special administrative software or grant excessive administrative privileges.

Exchange Control Panel

The ECP is hosted and accessed through the OWA. Accessing the ECP through OWA was covered earlier in this chapter. Figure 12-38 shows the ECP UI.

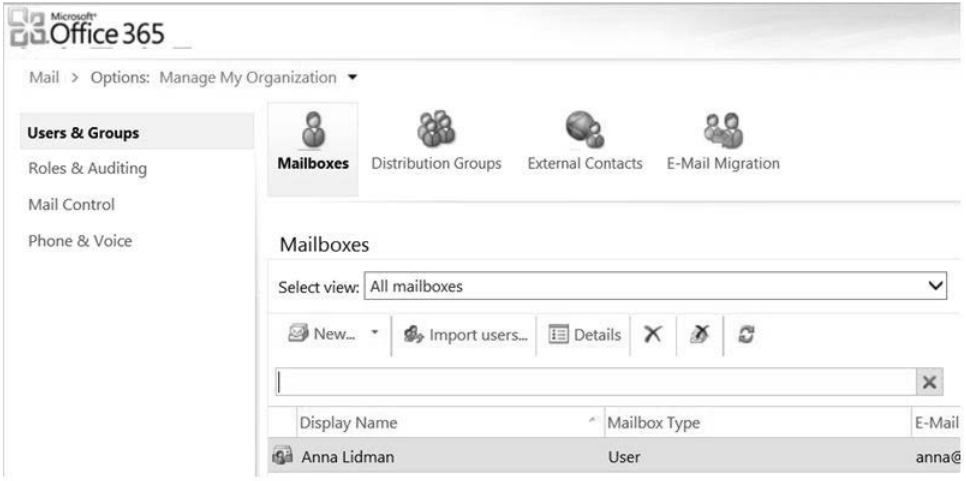

Figure 12-38 The ECP user interface.

Along the left side of the ECP is the navigation pane that groups the administrative functions. Figure 12-38 shows the administrative capability to manage mailboxes, distribution groups, and external contacts. Additionally, you can access the E-Mail Migration wizard on the Users & Groups page.

RBAC and compliance management capabilities are located on the Roles & Auditing page. A number of RBAC roles are available out of the box, as shown in Figure 12-39. However, you can modify the scope of each role's capabilities and create new RBAC roles.

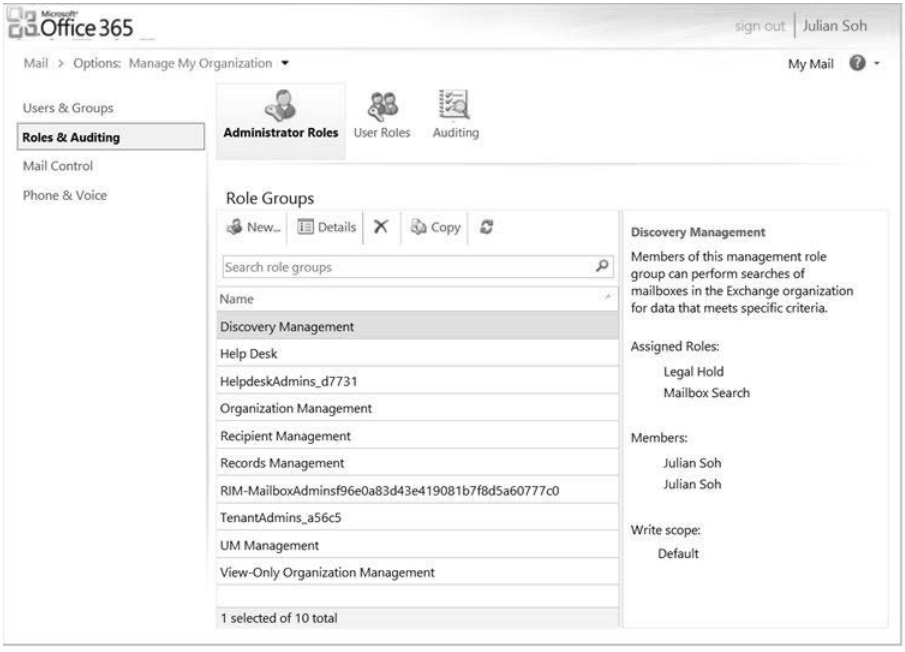

Figure 12-39 Roles & Auditing page in the EMC.

As mentioned earlier, we will leave the detailed administration of Exchange to other resources. However, before we leave this topic it is important to note that you can perform the majority of daily administrative functions through the ECP. As you explore the UI, notice that it is designed to be user friendly so that even non-technical administrators, such as the compliance and legal professionals we identified earlier, can perform administrative tasks.

At this point, we will leave the ECP and move on to discuss Forefront Online Protection for Exchange (FOPE).

Forefront Online Protection for Exchange administration

FOPE is responsible for email protection in Exchange Online 2010 and is a separate interface that is launched through the ECP. From the ECP, select Mail Control and click Configure IP safelisting, perimeter message tracking, and e-mail policies, as shown in Figure 12-40.

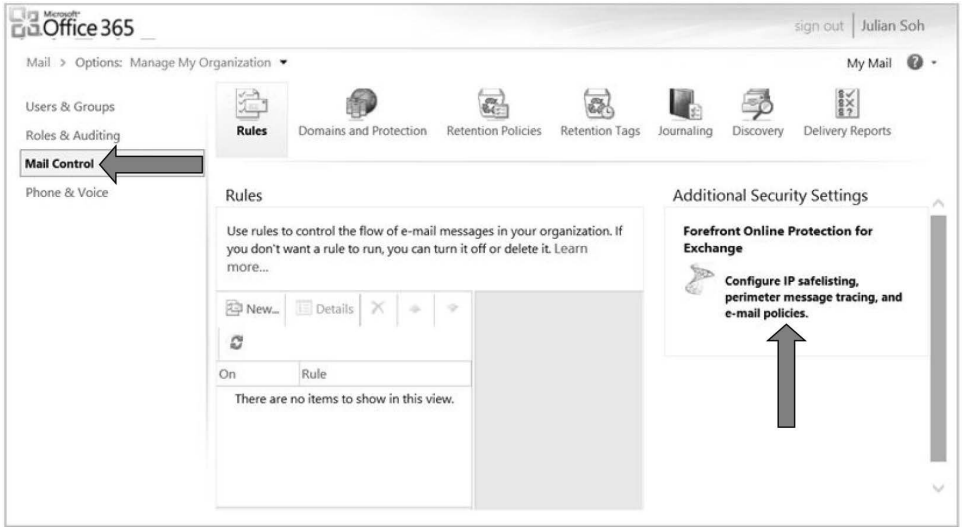

Figure 12-40 Accessing FOPE from the ECP.

This will start the FOPE administration interface, as shown in Figure 12-41. The FOPE administration interface provides statistics on mail hygiene and enables you to create reports, track messages, and create mail-handling policies.

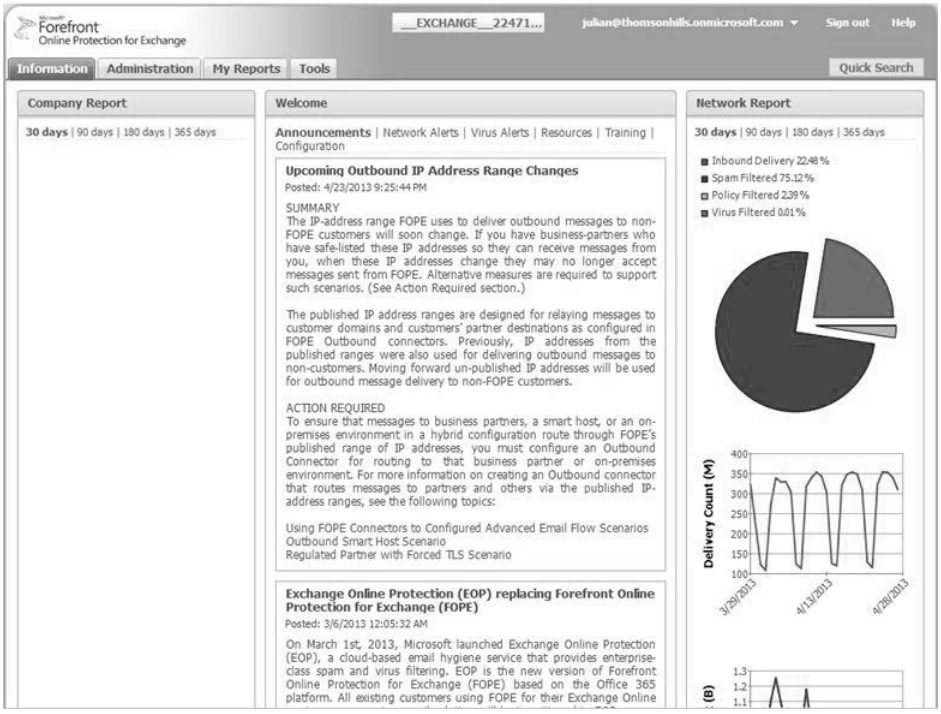

Figure 12-41 FOPE administration interface.

Your core activity in FOPE is the creation of mail policies. Follow these steps to see how mail policies are created and maintained in FOPE:

1. From the FOPE administration console, click the Administration tab, and then select Policy Rules.

2. Click New Policy Rule located under Tasks.

3. Set the domain scope, set the traffic scope, and select the policy's action, as shown in Figure 12-42.

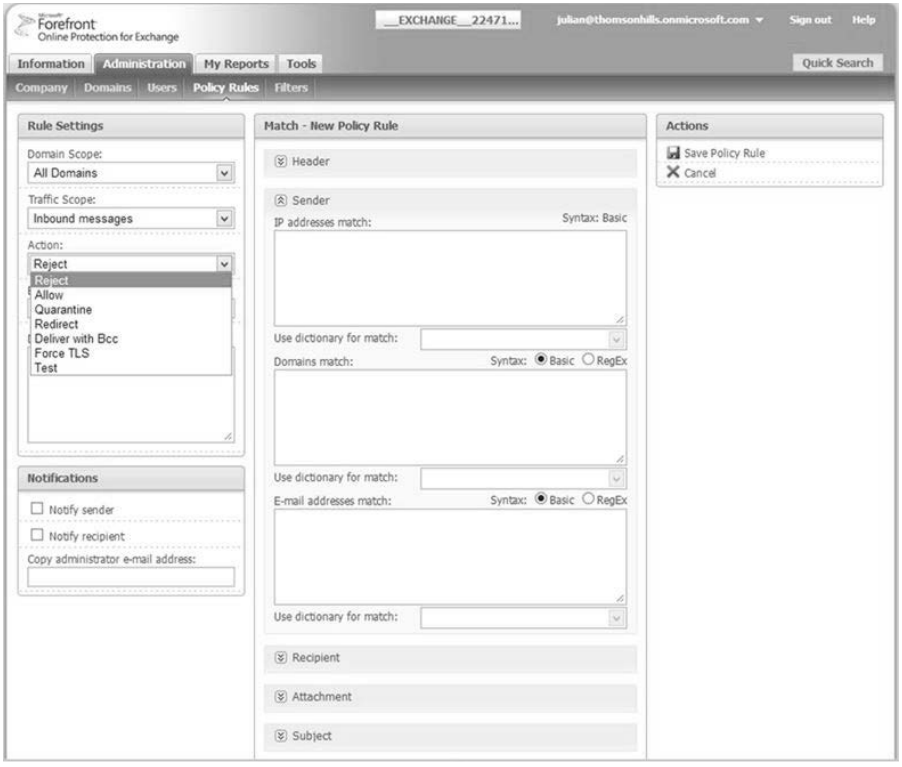

Figure 12-42 New FOPE policy.

4. Provide settings for the Expiration date field, if applicable, and determine if you want to send notifications whenever this rule is triggered.

5. In the Match pane, define the data patterns that would lead to the triggering of this policy. As you can see, you have the option to match by header, sender, and recipient IP addresses, domains, or e-mail address, attachment, subject, body, and message properties.

6. Click Save Policy Rule on the Actions pane to save this policy.

As with the ECP, there are other administrative functions for FOPE that we will let you explore on your own. This section serves only as an introduction to FOPE administration. We will now move on to look at the Exchange admin center (EAC).

Exchange admin center

The EAC is the successor to the ECP in the latest release of Office 365 and, like the ECP, it is a browser-based interface that organizes administrative functions into groups, as shown in Figure 12-43.

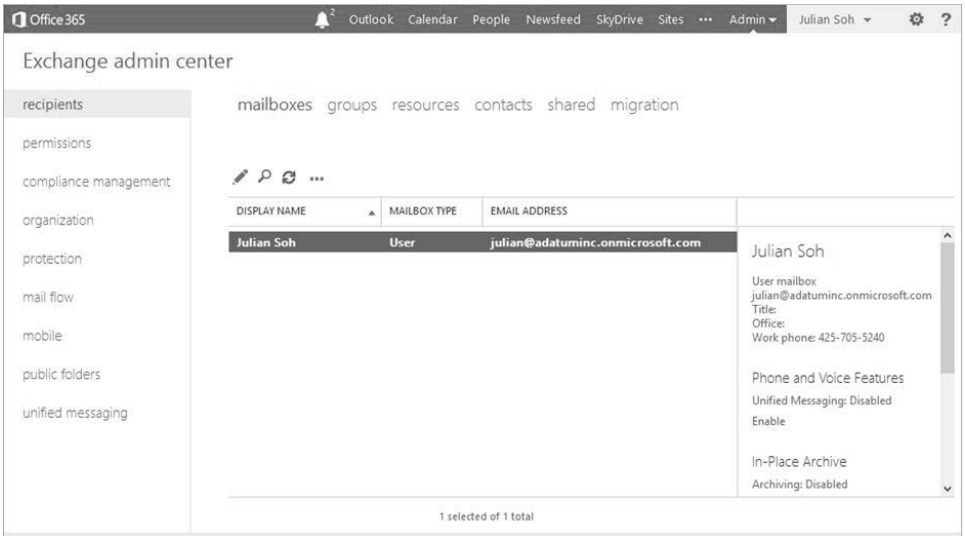

Figure 12-43 The EAC.

The main difference between the ECP and the EAC is the introduction of several new capabilities in Exchange Online 2013 and the respective administration functions that are exposed in the EAC. One of the new capabilities is Data Leakage Prevention (DLP) that is located on the Compliance Management page, as shown in Figure 12-44.

> **Note**
>
> **DLP is a premium feature that requires an Exchange Online Plan 2 subscription. Exchange 2013 implemented on-premises requires an Exchange Enterprise client access license (CAL). In a hybrid Exchange implementation, Exchange Online Plan 2 users are covered for all premium features implemented on-premises, including DLP, and will not require a separate Exchange 2013 Enterprise CAL.**

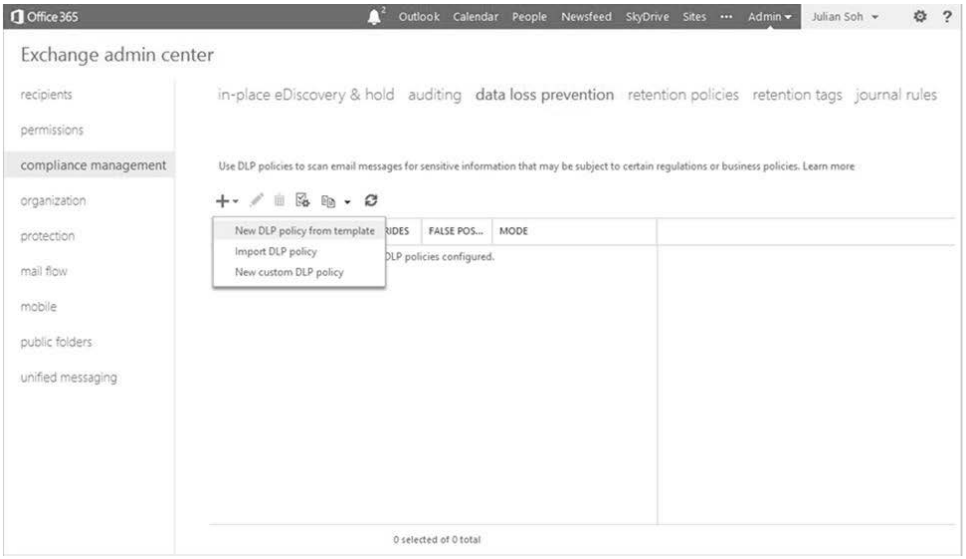

Figure 12-44 Data loss prevention in the EAC.

Prior to the latest release of Office 365, you had to rely on on-premises DLP solutions and have Exchange Online route all email through that solution. With the latest release of Office 365, Exchange Online 2013 provides DLP capability. You can create content triggers that rely on ISO-based templates to recognize data patterns. ISO stands for the International Organization for Standardization and is the internationally recognized entity that develops and publishes international standards. Following are a few examples of the included DLP templates:

- U.S. Health Information Portability Act (HIPAA)
- U.S. Personally Identifiable Information (PII)
- U.S. Social Security Act
- U.S. Financial Information

There are international DLP templates included as well. To see the full list of DLP templates, click the + icon, as shown in Figure 12-44, and then select New DLP policy from template from the drop-down menu. For example, if we create a DLP policy based on the HIPAA template and name the policy HIPAA Rules, this rule will show up in the DLP list of policies. At the same time, the corresponding rules that dictate how to handle emails that trigger this policy will be created in the mail flow section, as shown in Figure 12-45. Notice that you have the granular ability to define actions such as whether to allow overrides, different handling for internal versus external recipients, and how attachments should be handled. You can clear the box next to a rule to disable it or delete it altogether if it does not apply.

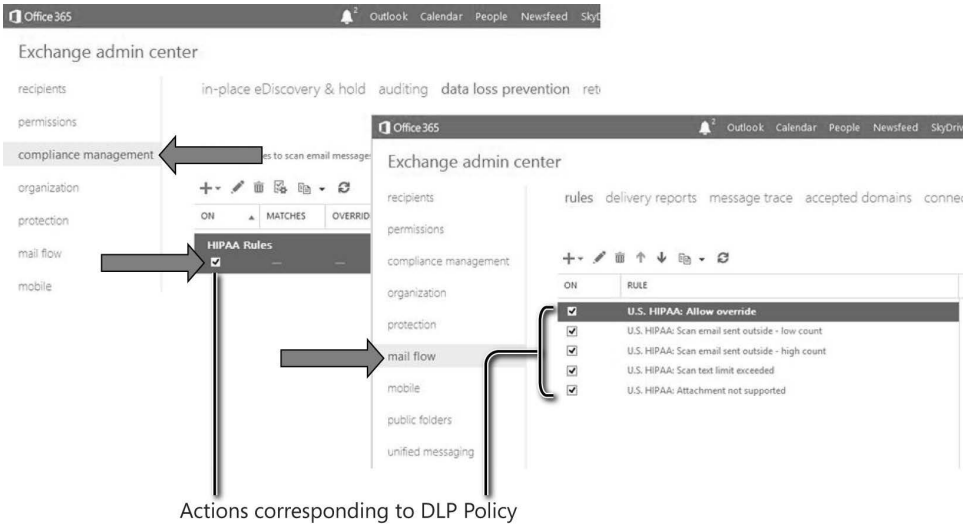

Figure 12-45 DLP policy and the corresponding mail flow rules.

The new DLP feature is an important addition to Exchange Online because it further enhances the service by providing another built-in mechanism to prevent the accidental disclosure of sensitive information through email.

Exchange Online Protection

Exchange Online Protection (EOP), the successor to FOPE, does not have a separate user interface. EOP administration is now fully integrated into the EAC through the protection page, as shown in Figure 12-46.

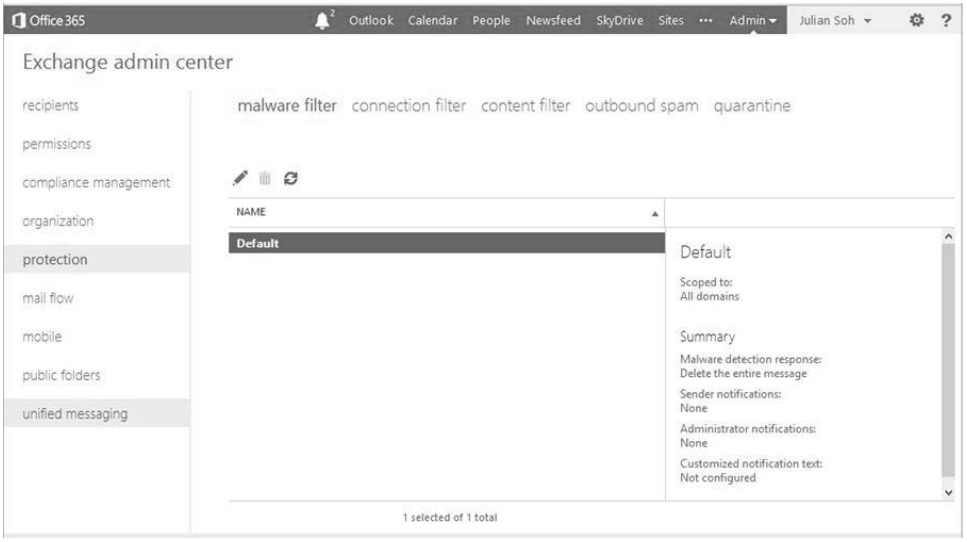

Figure 12-46 EOP management incorporated into the EAC.

As with the other administration tools, we will not go into the details of administration and instead will continue in the following sections to look at other new capabilities of Exchange Online.

Compliance, Legal Hold, and eDiscovery concepts

Compliance, eDiscovery, Legal Hold, and records management are very important topics for many organizations in the public and private sectors because of the legal and financial implications for not properly preserving or disposing of communication content in a timely fashion. Emails usually make up a significant, if not majority, of the content managed by an organization. Almost all legal cases allow or require the introduction of email content and transactions as evidence. As such, Exchange Online 2010 has these compliance capabilities natively built into the service, which is further enhanced in Exchange Online 2013.

The overall compliance strategy for Exchange involves the following key capabilities:

- Preserving content
- Automated deletions
- Enforced retention

Preserving content

Preserving content is the capability to allow for the indefinite storage of content in a centralized location. A centralized storage location can serve as an authoritative data source that will ease management and eDiscovery efforts. Furthermore, if the centralized storage location is big enough, users will feel less compelled to delete content just to free up space, thereby reducing the risk of accidental deletions.

This capability is provided by the introduction of the personal archive, which we will discuss in detail shortly.

Automated deletions

To properly control the deletion of emails and to counter-balance the ability to indefinitely store them, Exchange introduces a concept called messaging records management (MRM). MRM consists of retention tags and policies, which help to automatically archive or delete email based on the age of the email timestamp. We will look at MRM in detail soon.

Enforced retention

Enforced retention is the capability to preserve email content to make it discoverable and yet permit the normal mailbox functions, including deletions and modifications. Enforced retention is accomplished by Exchange Online 2010 Legal Hold. In Exchange Online 2013, this is known as In-Place Hold. We will look at holds in detail shortly.

Putting it all together

As you can see, the three capabilities are designed to work together to form a comprehensive corporate compliance strategy. There is a centralized email storage location that makes search easier and an automated email archiving and deletion mechanism to help manage content without user intervention, thereby reducing human error or oversight. Finally, there is a mechanism to enforce preservation of content that overrides any other action to modify or destroy that content. Let us now look in detail at the actual technologies that provide these three capabilities.

Personal archive

We think of the personal archive as the foundational technology that supports compliance. The personal archive is sometimes referred to as the online archive or Exchange Online Archiving (EOA) if it is implemented as a stand-alone Exchange Online workload.

Before the introduction of the personal archive, users had limited mailbox sizes because of the need to manage the performance of Exchange. That is why Personal Storage Tables (PSTs) became popular. Users either delete emails to free up space in their mailbox or move them to .pst files. Both of these actions are major causes of concern when it comes to compliance.

Exchange Online Plan 1 provides a 25 GB storage that is shared between the primary mailbox and the archive mailbox. Exchange Online Plan 2 provides unlimited archive space that is separate from a 25 GB primary mailbox.

> **Note**
>
> **Remember that Exchange Online Archiving provides each user with an unlimited amount of archive mailbox space that is initially provisioned as 100 GB, and it is accessible through Outlook and Outlook Web App.**

Therefore, the first step to compliance remediation is to assign users a personal archive. You can choose to do this for every user or only for certain users. Provisioning a personal archive can be done through the EAC, ECP, EMC, or Windows PowerShell.

Messaging Records Management

After you have provided users with a generous personal archive, you might still need to implement MRM to automatically archive or dispose of email content. MRM is accomplished through retention tags and retention policies.

Retention tags

Retention tags are discrete actions that can be applied to email messages and folders. Retention tags are designed to be very granular. Here are a few examples of retention tags:

- Move items that are 180 days old from the Inbox to the Personal Archive.
- Permanently delete items in the Personal Archive that are older than 1,825 days (five years).
- Delete, but enable recovery of items that are older than 5 days in the Junk Mail folder.

Retention policies

Retention policies comprise multiple retention tags. It is a way to apply different retention tags to different items under a single policy and to facilitate workflows that carry out sequential actions on items, such as moving items from the primary mailbox to the archive mailbox if they are two years old, and then deleting them after five years. Using the three retention tag examples, you can combine all of them into a single organization retention policy and apply the retention policy to all mailboxes. If you do that, your organization's email compliance statement will look something like this:

Adatum Inc. Email Retention Policy

All emails that are 180 days old are automatically moved from your primary mailbox to your personal archive, where they will reside for 4.5 years, at which time they will be permanently deleted. Emails that are determined by the system to be junk mail are stored in the junk mail folder for 5 days, after which they will be deleted. However, if you believe that an email was accidentally identified as junk and you did not get to it within 5 days, you can recover it from your recycle bin within 14 days after it was automatically deleted.

Holds

Retention policies are sometimes misunderstood because of their name. It is easy to forget that retention tags and policies are responsible only for moving or deleting content to ensure the content does not exceed its retention schedule. Retention tags and policies do not actually preserve content. This means if a user decides to delete an email on the first day it arrives, the retention policy you just put in place does not prevent the user from doing so.

To enforce the preservation of email content, Exchange uses the concept of a Legal Hold (Exchange Online 2010) or an In-Place Hold (Exchange Online 2013). Another interesting concept about enforced preservation is that the user is not prevented from carrying out

actions that modify or delete email content. This is by design because mailbox operations should continue to function normally. This is a very significant Microsoft strategy because it balances your organization's compliance requirements and at the same time does not affect the productivity of your users. When email content is on hold, it is discoverable.

A Legal Hold in Exchange Online 2010 is applied at the mailbox level and implemented through the EMC, ECP, or Windows PowerShell. While the concept of immutability can be accomplished through Legal Hold, the ability to apply it only at the mailbox level might not be granular enough because too much content might be placed on hold. Nonetheless, what is important is that content is immutably preserved and, with a large personal archive, the space consumption as a result of content preservation under Legal Hold is not an issue.

In Exchange Online 2013, Legal Hold is renamed In-Place Hold, and it now addresses the ability for you to be more granular in selecting the content to preserve by introducing two types of In-Place Holds:

- Time-based hold, including indefinite hold
- Criteria-based hold

Time-based hold

Time-based holds, sometimes referred to as rolling holds, work like an MRM retention tag in that the hold is applied based on the timestamp of an email. As long as the timestamp of the email falls within the limits of the time-based hold, the email content will be preserved and is discoverable through a multi-mailbox eDiscovery search. After the timestamp of the email falls outside the time-based holds, the content of the email will no longer be preserved and will be subject to the modification or deletion actions of the user or MRM.

Criteria-based hold

Criteria-based hold relies on keywords and Boolean logic to preserve content. Aside from a keyword criteria match, you can also specify source and recipients, date ranges, and message types (email, calendar items, and so on).

INSIDE OUT **Keyword Query Language**

A new capability that is not very well advertised is the Keyword Query Language (KQL). KQL is a syntax that allows you to conduct proximity searches. The following is an example of KQL syntax:

```
"acquisition" NEAR(n=3) "debt"
```

The preceding KQL syntax allows you to search for content that has the word *acquisition* located a maximum distance of three words from the word *debt*. Search the Internet for other KQL syntax examples.

Creating holds

You can create and apply multiple holds to the entire organization (all mailboxes), to specific individuals, or to distribution groups. If an email is subject to multiple holds, as long as any of the hold remains applicable to the email, then its contents will be preserved and is discoverable.

You can create time-based holds and criteria-based holds on the compliance management page of the EAC, as shown in Figure 12-47.

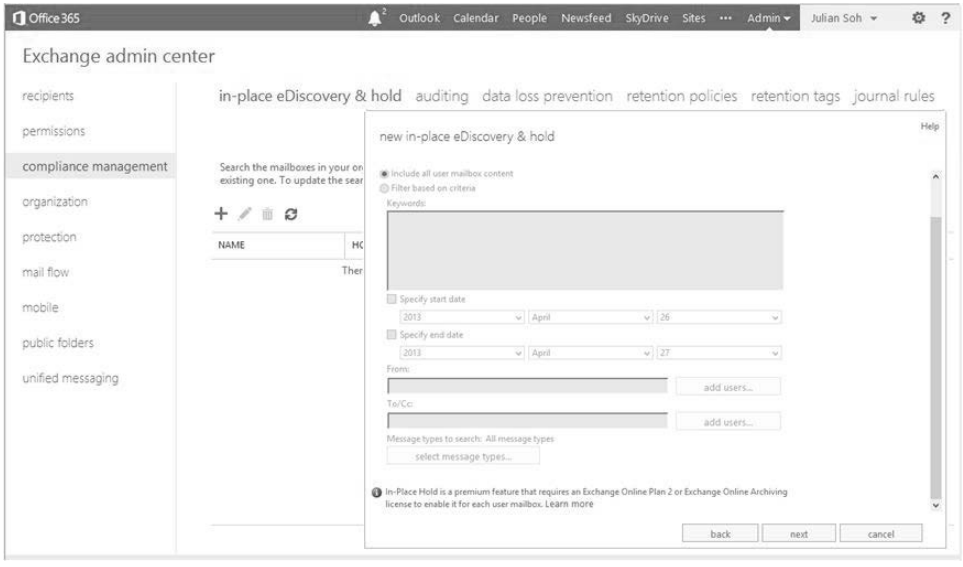

Figure 12-47 Creating In-Place Holds through the EAC.

When prompted for the holding period, you can choose to hold indefinitely or to hold for a certain number of days, as shown in Figure 12-48.

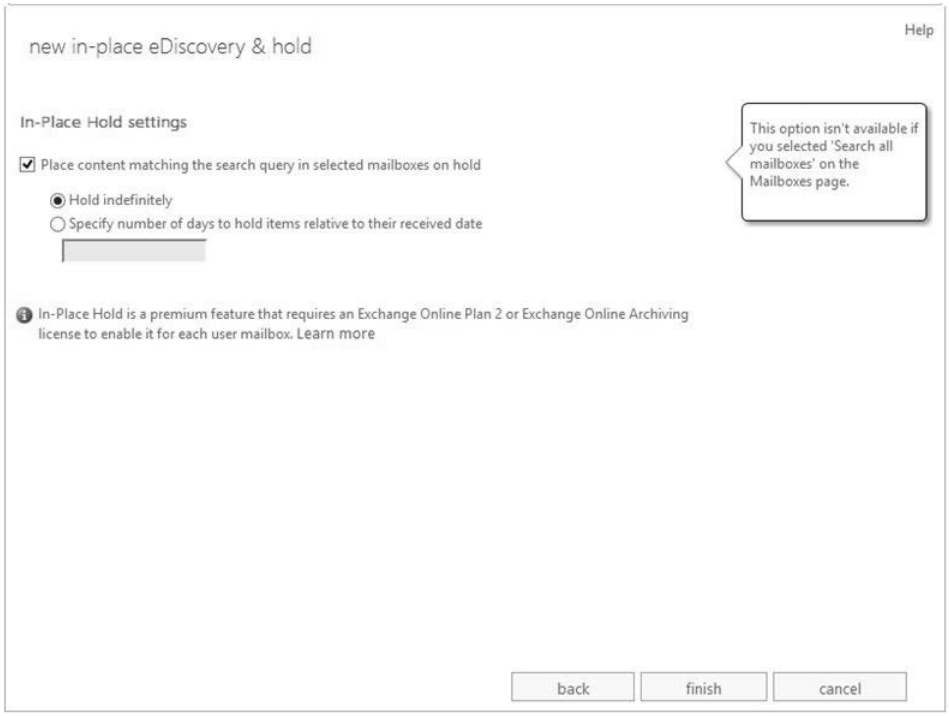

Figure 12-48 Define hold settings.

As an example of a corporate-enforced, In-Place Hold policy, an organization could choose to create an organization-wide, time-based hold by following these steps:

1. In the EAC, select compliance management, and then select in-place eDiscovery & hold.
2. Click the + icon to create a new in-place hold.
3. Provide a name for the hold, and then click next.
4. Select Specify mailboxes to search, and then click the + icon.
5. In the Global Address List (GAL) dialog box, select a distribution group, such as Everyone. Click add, and then click ok to close the GAL. Alternatively, you can simply select the Search all mailboxes option in Step 4. Click next.

6. On the Search query page, select Include all user mailbox content. This enforces the preservation of all email, regardless of content. Click next.

7. On the In-Place Hold settings page, select Place content matching the search query in selected mailboxes on hold. Select the Specify number of days to hold items relative to their received date option. Type 180 in the text box, and then click finish.

You have now implemented an organization-wide, time-based hold. In the event that you need to create a new hold based on criteria rather than time, you will perform the same preceding steps to create a new hold with one difference: instead of selecting Include all user mailbox content in Step 6, select Filter based on criteria and use keywords, Boolean logic, KQL, and the other settings to define your criteria-based search.

Multi-mailbox search (eDiscovery)

Multi-mailbox search enables you to search mailboxes for items that meet your criteria. The results of a multi-mailbox search are stored in a special type of mailbox called the Discovery mailbox. Each tenant is provisioned with a single Discovery mailbox, but you can create additional Discovery mailboxes. Furthermore, each Discovery mailbox is limited to 50 GB.

INSIDE OUT

Concurrent searches

It is not stated explicitly in the Service Description, but you are limited to two concurrent multi-mailbox searches. If you have the need for multiple concurrent searches, you can submit a request to Microsoft Online Support with a business case for the need to temporarily increase this limit.

An alternate option is to create all the required eDiscovery searches, and then write a Windows PowerShell script that checks the status of each search request and attempts to start it if the status of the search is Failed because two other searches are already running. We created a script and had it run every few minutes. The Windows PowerShell script to check the status of the search and attempt to start it is the following:

```
if((Get-MailboxSearch “<search job name>”) status –eq “Failed”
  Start-MailboxSearch –identity “<search job name>” –Force }
```

Results of multi-mailbox searches are located on the same page as In-Place Holds. As you can see in Figure 12-49, by clicking on an existing time-based or criteria-based hold, the information including estimates of the search results are shown in the informational pane to the right.

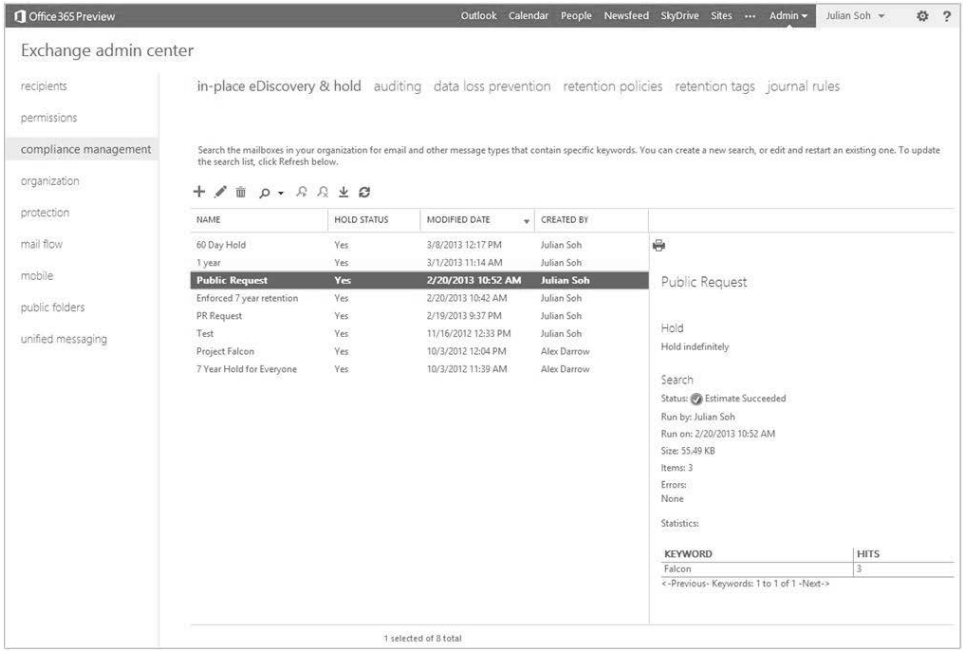

Figure 12-49 Estimate of search results.

By clicking the magnifying glass icon, as shown in Figure 12-50, you can re-run the estimate for search results, preview the search results, or copy the search results.

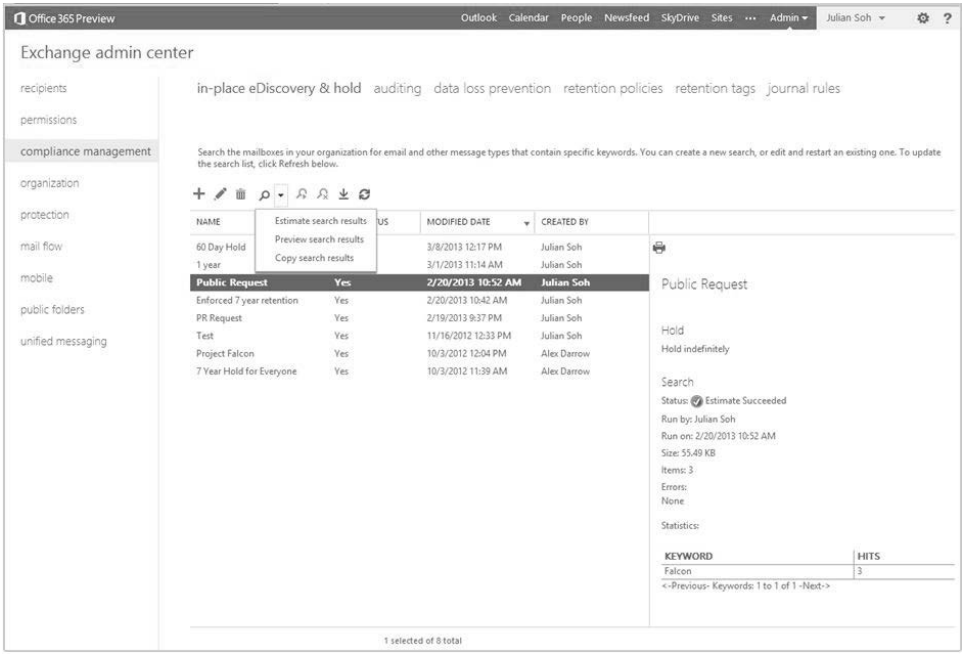

Figure 12-50 Search results options.

Summary

We covered a lot of information in this chapter. We started by looking at the different mailbox migration options, including a strategy to migrate .pst content with PST Capture. We also covered the administration of Exchange and its different workloads, such as Forefront Online Protection for Exchange (FOPE), Exchange Online Protection (EOP), and Data Loss Prevention (DLP). Finally, we covered the compliance capabilities of Exchange Online in the form of In-Place Holds, multi-mailbox search, and Messaging Records Management (MRM).

What we covered in the last three chapters is very specific to Exchange in the cloud. We focused on Exchange hybrid models and mailbox migrations. We hope these chapters have provided you with a strong foundation to understand Exchange Online and how it integrates with your on-premises messaging solution.

Because it is not possible for this book to be exhaustive on all aspects of Exchange administration, bear in mind that Exchange Online 2010 is equivalent to Exchange on-premises 2010, and Exchange Online 2013 is equivalent to Exchange on-premises 2013. Therefore, if you need to dive deeper into the topic of administering Exchange, there are many good books already in the market that focus solely on Exchange administration and all its workloads, and these should meet your needs.

In the next chapter, we will look at SharePoint Online, which is another service provided under Office 365.

Index

D

E

F

G

H

M

N

P

Q

R

S