

OFFICIAL MICROSOFT LEARNING PRODUCT

20346C

Managing Office 365™ Identities and Services

MCT USE ONLY. STUDENT USE PROHIBITED

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

© 2015 Microsoft Corporation. All rights reserved.

Microsoft and the trademarks listed at <http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx> are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners

Product Number: 20346C

Part Number (if applicable): X19-82804

Released: 03/2015

MICROSOFT LICENSE TERMS MICROSOFT INSTRUCTOR-LED COURSEWARE

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to your use of the content accompanying this agreement which includes the media on which you received it, if any. These license terms also apply to Trainer Content and any updates and supplements for the Licensed Content unless other terms accompany those items. If so, those terms apply.

**BY ACCESSING, DOWNLOADING OR USING THE LICENSED CONTENT, YOU ACCEPT THESE TERMS.
IF YOU DO NOT ACCEPT THEM, DO NOT ACCESS, DOWNLOAD OR USE THE LICENSED CONTENT.**

If you comply with these license terms, you have the rights below for each license you acquire.

1. DEFINITIONS.

- a. "Authorized Learning Center" means a Microsoft IT Academy Program Member, Microsoft Learning Competency Member, or such other entity as Microsoft may designate from time to time.
- b. "Authorized Training Session" means the instructor-led training class using Microsoft Instructor-Led Courseware conducted by a Trainer at or through an Authorized Learning Center.
- c. "Classroom Device" means one (1) dedicated, secure computer that an Authorized Learning Center owns or controls that is located at an Authorized Learning Center's training facilities that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.
- d. "End User" means an individual who is (i) duly enrolled in and attending an Authorized Training Session or Private Training Session, (ii) an employee of a MPN Member, or (iii) a Microsoft full-time employee.
- e. "Licensed Content" means the content accompanying this agreement which may include the Microsoft Instructor-Led Courseware or Trainer Content.
- f. "Microsoft Certified Trainer" or "MCT" means an individual who is (i) engaged to teach a training session to End Users on behalf of an Authorized Learning Center or MPN Member, and (ii) currently certified as a Microsoft Certified Trainer under the Microsoft Certification Program.
- g. "Microsoft Instructor-Led Courseware" means the Microsoft-branded instructor-led training course that educates IT professionals and developers on Microsoft technologies. A Microsoft Instructor-Led Courseware title may be branded as MOC, Microsoft Dynamics or Microsoft Business Group courseware.
- h. "Microsoft IT Academy Program Member" means an active member of the Microsoft IT Academy Program.
- i. "Microsoft Learning Competency Member" means an active member of the Microsoft Partner Network program in good standing that currently holds the Learning Competency status.
- j. "MOC" means the "Official Microsoft Learning Product" instructor-led courseware known as Microsoft Official Course that educates IT professionals and developers on Microsoft technologies.
- k. "MPN Member" means an active Microsoft Partner Network program member in good standing.

- l. "Personal Device" means one (1) personal computer, device, workstation or other digital electronic device that you personally own or control that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.
- m. "Private Training Session" means the instructor-led training classes provided by MPN Members for corporate customers to teach a predefined learning objective using Microsoft Instructor-Led Courseware. These classes are not advertised or promoted to the general public and class attendance is restricted to individuals employed by or contracted by the corporate customer.
- n. "Trainer" means (i) an academically accredited educator engaged by a Microsoft IT Academy Program Member to teach an Authorized Training Session, and/or (ii) a MCT.
- o. "Trainer Content" means the trainer version of the Microsoft Instructor-Led Courseware and additional supplemental content designated solely for Trainers' use to teach a training session using the Microsoft Instructor-Led Courseware. Trainer Content may include Microsoft PowerPoint presentations, trainer preparation guide, train the trainer materials, Microsoft One Note packs, classroom setup guide and Pre-release course feedback form. To clarify, Trainer Content does not include any software, virtual hard disks or virtual machines.

2. **USE RIGHTS.** The Licensed Content is licensed not sold. The Licensed Content is licensed on a **one copy per user basis**, such that you must acquire a license for each individual that accesses or uses the Licensed Content.

2.1 Below are five separate sets of use rights. Only one set of rights apply to you.

a. **If you are a Microsoft IT Academy Program Member:**

- i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
- ii. For each license you acquire on behalf of an End User or Trainer, you may either:
 - 1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User who is enrolled in the Authorized Training Session, and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
 - 2. provide one (1) End User with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
 - 3. provide one (1) Trainer with the unique redemption code and instructions on how they can access one (1) Trainer Content,**provided you comply with the following:**
- iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
- iv. you will ensure each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
- v. you will ensure that each End User provided with the hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
- vi. you will ensure that each Trainer teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,

- vii. you will only use qualified Trainers who have in-depth knowledge of and experience with the Microsoft technology that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Authorized Training Sessions,
- viii. you will only deliver a maximum of 15 hours of training per week for each Authorized Training Session that uses a MOC title, and
- ix. you acknowledge that Trainers that are not MCTs will not have access to all of the trainer resources for the Microsoft Instructor-Led Courseware.

b. If you are a Microsoft Learning Competency Member:

- i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
- ii. For each license you acquire on behalf of an End User or Trainer, you may either:
 - 1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Authorized Training Session and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware provided, **or**
 - 2. provide one (1) End User attending the Authorized Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
 - 3. you will provide one (1) Trainer with the unique redemption code and instructions on how they can access one (1) Trainer Content,
provided you comply with the following:
- iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
- iv. you will ensure that each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
- v. you will ensure that each End User provided with a hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
- vi. you will ensure that each Trainer teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,
- vii. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for your Authorized Training Sessions,
- viii. you will only use qualified MCTs who also hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Authorized Training Sessions using MOC,
- ix. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
- x. you will only provide access to the Trainer Content to Trainers.

c. **If you are a MPN Member:**

- i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
- ii. For each license you acquire on behalf of an End User or Trainer, you may either:
 1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Private Training Session, and only immediately prior to the commencement of the Private Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
 2. provide one (1) End User who is attending the Private Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
 3. you will provide one (1) Trainer who is teaching the Private Training Session with the unique redemption code and instructions on how they can access one (1) Trainer Content, **provided you comply with the following:**
- iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
- iv. you will ensure that each End User attending an Private Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Private Training Session,
- v. you will ensure that each End User provided with a hard copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
- vi. you will ensure that each Trainer teaching an Private Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Private Training Session,
- vii. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Private Training Sessions,
- viii. you will only use qualified MCTs who hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Private Training Sessions using MOC,
- ix. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
- x. you will only provide access to the Trainer Content to Trainers.

d. **If you are an End User:**

For each license you acquire, you may use the Microsoft Instructor-Led Courseware solely for your personal training use. If the Microsoft Instructor-Led Courseware is in digital format, you may access the Microsoft Instructor-Led Courseware online using the unique redemption code provided to you by the training provider and install and use one (1) copy of the Microsoft Instructor-Led Courseware on up to three (3) Personal Devices. You may also print one (1) copy of the Microsoft Instructor-Led Courseware. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.

e. **If you are a Trainer.**

- i. For each license you acquire, you may install and use one (1) copy of the Trainer Content in the form provided to you on one (1) Personal Device solely to prepare and deliver an Authorized Training Session or Private Training Session, and install one (1) additional copy on another Personal Device as a backup copy, which may be used only to reinstall the Trainer Content. You may not install or use a copy of the Trainer Content on a device you do not own or control. You may also print one (1) copy of the Trainer Content solely to prepare for and deliver an Authorized Training Session or Private Training Session.

- ii. You may customize the written portions of the Trainer Content that are logically associated with instruction of a training session in accordance with the most recent version of the MCT agreement. If you elect to exercise the foregoing rights, you agree to comply with the following: (i) customizations may only be used for teaching Authorized Training Sessions and Private Training Sessions, and (ii) all customizations will comply with this agreement. For clarity, any use of “*customize*” refers only to changing the order of slides and content, and/or not using all the slides or content, it does not mean changing or modifying any slide or content.

2.2 **Separation of Components.** The Licensed Content is licensed as a single unit and you may not separate their components and install them on different devices.

2.3 **Redistribution of Licensed Content.** Except as expressly provided in the use rights above, you may not distribute any Licensed Content or any portion thereof (including any permitted modifications) to any third parties without the express written permission of Microsoft.

2.4 **Third Party Notices.** The Licensed Content may include third party code that Microsoft, not the third party, licenses to you under this agreement. Notices, if any, for the third party code are included for your information only.

2.5 **Additional Terms.** Some Licensed Content may contain components with additional terms, conditions, and licenses regarding its use. Any non-conflicting terms in those conditions and licenses also apply to your use of that respective component and supplements the terms described in this agreement.

3. **LICENSED CONTENT BASED ON PRE-RELEASE TECHNOLOGY.** If the Licensed Content’s subject matter is based on a pre-release version of Microsoft technology (“**Pre-release**”), then in addition to the other provisions in this agreement, these terms also apply:

- a. **Pre-Release Licensed Content.** This Licensed Content subject matter is on the Pre-release version of the Microsoft technology. The technology may not work the way a final version of the technology will and we may change the technology for the final version. We also may not release a final version. Licensed Content based on the final version of the technology may not contain the same information as the Licensed Content based on the Pre-release version. Microsoft is under no obligation to provide you with any further content, including any Licensed Content based on the final version of the technology.
- b. **Feedback.** If you agree to give feedback about the Licensed Content to Microsoft, either directly or through its third party designee, you give to Microsoft without charge, the right to use, share and commercialize your feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft technology, Microsoft product, or service that includes the feedback. You will not give feedback that is subject to a license that requires Microsoft to license its technology, technologies, or products to third parties because we include your feedback in them. These rights survive this agreement.
- c. **Pre-release Term.** If you are an Microsoft IT Academy Program Member, Microsoft Learning Competency Member, MPN Member or Trainer, you will cease using all copies of the Licensed Content on the Pre-release technology upon (i) the date which Microsoft informs you is the end date for using the Licensed Content on the Pre-release technology, or (ii) sixty (60) days after the commercial release of the technology that is the subject of the Licensed Content, whichever is earliest (“**Pre-release term**”). Upon expiration or termination of the Pre-release term, you will irretrievably delete and destroy all copies of the Licensed Content in your possession or under your control.

- 4. SCOPE OF LICENSE.** The Licensed Content is licensed, not sold. This agreement only gives you some rights to use the Licensed Content. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the Licensed Content only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the Licensed Content that only allows you to use it in certain ways. Except as expressly permitted in this agreement, you may not:

 - access or allow any individual to access the Licensed Content if they have not acquired a valid license for the Licensed Content,
 - alter, remove or obscure any copyright or other protective notices (including watermarks), branding or identifications contained in the Licensed Content,
 - modify or create a derivative work of any Licensed Content,
 - publicly display, or make the Licensed Content available for others to access or use,
 - copy, print, install, sell, publish, transmit, lend, adapt, reuse, link to or post, make available or distribute the Licensed Content to any third party,
 - work around any technical limitations in the Licensed Content, or
 - reverse engineer, decompile, remove or otherwise thwart any protections or disassemble the Licensed Content except and only to the extent that applicable law expressly permits, despite this limitation.
- 5. RESERVATION OF RIGHTS AND OWNERSHIP.** Microsoft reserves all rights not expressly granted to you in this agreement. The Licensed Content is protected by copyright and other intellectual property laws and treaties. Microsoft or its suppliers own the title, copyright, and other intellectual property rights in the Licensed Content.
- 6. EXPORT RESTRICTIONS.** The Licensed Content is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the Licensed Content. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.
- 7. SUPPORT SERVICES.** Because the Licensed Content is “as is”, we may not provide support services for it.
- 8. TERMINATION.** Without prejudice to any other rights, Microsoft may terminate this agreement if you fail to comply with the terms and conditions of this agreement. Upon termination of this agreement for any reason, you will immediately stop all use of and delete and destroy all copies of the Licensed Content in your possession or under your control.
- 9. LINKS TO THIRD PARTY SITES.** You may link to third party sites through the use of the Licensed Content. The third party sites are not under the control of Microsoft, and Microsoft is not responsible for the contents of any third party sites, any links contained in third party sites, or any changes or updates to third party sites. Microsoft is not responsible for webcasting or any other form of transmission received from any third party sites. Microsoft is providing these links to third party sites to you only as a convenience, and the inclusion of any link does not imply an endorsement by Microsoft of the third party site.
- 10. ENTIRE AGREEMENT.** This agreement, and any additional terms for the Trainer Content, updates and supplements are the entire agreement for the Licensed Content, updates and supplements.
- 11. APPLICABLE LAW.**

 - a. United States. If you acquired the Licensed Content in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

b. Outside the United States. If you acquired the Licensed Content in any other country, the laws of that country apply.

- 12. LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the Licensed Content. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.
- 13. DISCLAIMER OF WARRANTY. THE LICENSED CONTENT IS LICENSED "AS-IS" AND "AS AVAILABLE." YOU BEAR THE RISK OF USING IT. MICROSOFT AND ITS RESPECTIVE AFFILIATES GIVES NO EXPRESS WARRANTIES, GUARANTEES, OR CONDITIONS. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS WHICH THIS AGREEMENT CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS, MICROSOFT AND ITS RESPECTIVE AFFILIATES EXCLUDES ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.**
- 14. LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT, ITS RESPECTIVE AFFILIATES AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO US\$5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.**

This limitation applies to

- anything related to the Licensed Content, services, content (including code) on third party Internet sites or third-party programs; and
- claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

Please note: As this Licensed Content is distributed in Quebec, Canada, some of the clauses in this agreement are provided below in French.

Remarque : Ce le contenu sous licence étant distribué au Québec, Canada, certaines des clauses dans ce contrat sont fournies ci-dessous en français.

EXONÉRATION DE GARANTIE. Le contenu sous licence visé par une licence est offert « tel quel ». Toute utilisation de ce contenu sous licence est à votre seule risque et péril. Microsoft n'accorde aucune autre garantie expresse. Vous pouvez bénéficier de droits additionnels en vertu du droit local sur la protection des consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit local, les garanties implicites de qualité marchande, d'adéquation à un usage particulier et d'absence de contrefaçon sont exclues.

LIMITATION DES DOMMAGES-INTÉRÊTS ET EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES. Vous pouvez obtenir de Microsoft et de ses fournisseurs une indemnisation en cas de dommages directs uniquement à hauteur de 5,00 \$ US. Vous ne pouvez prétendre à aucune indemnisation pour les autres dommages, y compris les dommages spéciaux, indirects ou accessoires et pertes de bénéfices.

Cette limitation concerne:

- tout ce qui est relié au le contenu sous licence, aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers; et.
- les réclamations au titre de violation de contrat ou de garantie, ou au titre de responsabilité stricte, de négligence ou d'une autre faute dans la limite autorisée par la loi en vigueur.

Elle s'applique également, même si Microsoft connaissait ou devrait connaître l'éventualité d'un tel dommage. Si votre pays n'autorise pas l'exclusion ou la limitation de responsabilité pour les dommages indirects, accessoires ou de quelque nature que ce soit, il se peut que la limitation ou l'exclusion ci-dessus ne s'appliquera pas à votre égard.

EFFET JURIDIQUE. Le présent contrat décrit certains droits juridiques. Vous pourriez avoir d'autres droits prévus par les lois de votre pays. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre pays si celles-ci ne le permettent pas.

Revised July 2013

Welcome!

Thank you for taking our training! We've worked together with our Microsoft Certified Partners for Learning Solutions and our Microsoft IT Academies to bring you a world-class learning experience—whether you're a professional looking to advance your skills or a student preparing for a career in IT.

- **Microsoft Certified Trainers and Instructors**—Your instructor is a technical and instructional expert who meets ongoing certification requirements. And, if instructors are delivering training at one of our Certified Partners for Learning Solutions, they are also evaluated throughout the year by students and by Microsoft.
- **Certification Exam Benefits**—After training, consider taking a Microsoft Certification exam. Microsoft Certifications validate your skills on Microsoft technologies and can help differentiate you when finding a job or boosting your career. In fact, independent research by IDC concluded that 75% of managers believe certifications are important to team performance¹. Ask your instructor about Microsoft Certification exam promotions and discounts that may be available to you.
- **Customer Satisfaction Guarantee**—Our Certified Partners for Learning Solutions offer a satisfaction guarantee and we hold them accountable for it. At the end of class, please complete an evaluation of today's experience. We value your feedback!

We wish you a great learning experience and ongoing success in your career!

Sincerely,

Microsoft Learning
www.microsoft.com/learning

Microsoft | Learning

¹ IDC, Value of Certification: Team Certification and Organizational Performance, November 2006

Acknowledgements

Microsoft Learning would like to acknowledge and thank the following for their contribution towards developing this title. Their effort at various stages in the development has ensured that you have a good classroom experience.

Anthony Steven – Course Designer and Content Developer

Anthony Steven is a subject matter expert on Office 365 and a Microsoft Certified Systems Engineer. He designed this course and proposed that the on-premises environment be hosted in Windows Azure, a first for Microsoft Learning Experience (LeX). Previously, he designed and developed Course 10968: Designing an Office 365 Infrastructure, the first LeX design course with paper-based labs that received five-star feedback from students.

He has written books on Exchange Server, Windows Server, .NET Framework and J2EE, UNIX migration and Windows NT. He is also a Lieutenant Colonel in the Army Cadet Force, a writer and composer of musicals and a motivational speaker. In his Army career, he was an Armored Reconnaissance officer in the 13th/18th Royal Hussars and a Special Forces operative.

David Coombes – Content Developer

David is a Principal Technologist at Content Master, and has many years' experience in the writing and designing of training courses, technical guides, and whitepapers. David's key technical areas are Windows operating systems, networking, security, and infrastructure technologies. David has been involved in Microsoft online technologies from the early days of MOS/BPOS, through to Office 365.

Recent projects have included technical reviews for 10968A: Designing for an Office 365 Infrastructure; and implementing and managing private and hybrid cloud solutions with Hyper-V, Windows Server, and System Center technologies, including hybrid cloud device management, and on-premises and cloud user synchronization.

Other recent projects have included a lead developer role covering on-premises and cloud-based Active Directory configuration and management, and identity management and role-based access control.

David is an experienced lab developer, and was responsible for developing the Windows Azure scripts for this ground-breaking course. In his spare time David attempts to keep a 25-year old VW camper van on the road, and is also trying (and failing), along with his wife and two children, to tire out a 1 year old dog.

Steve Ryan – Subject Matter Expert

Steve is a Senior Technologist in the Content Master IT Professional (UK) team with over 13 years' experience in training and technical authoring. He was one of the first Microsoft Certified Trainers to achieve Windows Server 2003 MCSE status in the UK and has authored numerous MOC ILT courses for Microsoft Learning. He has also written technical documentation, including security guides, whitepapers and e-Learning courseware.

He is an MCITP in Windows Server and an MCTS in Windows Server 2008, Windows Vista, and Office SharePoint Server 2007.

Recent projects include Office 365 Technical Assessments for Small Business, Pre-Sales Technical Assessments for The New Office for the Worldwide Partner Group (WPG), Office 15/Office 365 OLT Launch courses for WPG, CIE for Office 365 for MS Involve, 2-day Office 15 Ignite course for TechReady, and two 5-day ILT courses for SharePoint 2013.

Martin Coetzer – Subject Matter Expert

Martin Coetzer is a Portfolio Architect with the Microsoft Learning eXperiences team. He is responsible for managing the Office 365, Exchange, Lync, SharePoint, Office and Dynamics certification portfolios. Prior to

this Martin was a consultant responsible for architecting and deploying Microsoft technologies at medium to large customers around the world.

Daniel Soto – Technical Reviewer

Daniel Soto is a Consultant for CloudStrategies, LLC, which operates out of Cedar Knolls, NJ. Daniel has been working in the Network and Communications Management field for over eight years. During this time, he has held a number of leadership positions working as an architect/designer, information systems manager, consultant, and network/system engineer. Daniel brings great depth of experience, technical skills, and management capabilities to his current position where he supports Enterprise Cloud Services Integration with Microsoft Office 365, Hyper V, and Windows Azure Active Directory. He has held senior positions with Calypso Cay Resorts and AOK Networking. He worked for five years as the Director of Technology for Calypso Cay Resorts and has since pursued a career in Virtualization and Cloud Services.

Allan Jacobs – Technical Reviewer

Allan Jacobs is a trainer, consultant, and writer based in New York City. While technically an independent, Allan works almost exclusively for Global Knowledge and spends a good deal of his time travelling to client sites and training centers throughout the United States. Allan has taught many Train the Trainer sessions for instructional skills, as well as Lync and System Center. Allan was also co-author of the revision of the Microsoft Official Courseware for OCS 2007 R2 and the Lync 2013 Depth Support Engineer Course. In his younger days Allan practiced law, something that he has successfully avoided for the last fifteen years.

Randy Muller – Technical Reviewer

Randy Muller, MCT, MCT: Regional Lead, MCSE, CEH, CHFI, is an independent trainer and consultant specializing in Amazon Web Services, Azure, Microsoft Private Cloud, Office 365, System Center and Unified Communications. Randy was an Army Officer stationed twice in Germany where he began his IT career in the mid-80s. Since then he has been an IT consultant in Australia and the United States, an author and a technical trainer.

Contents

Module 1: Preparing for Office 365

Module Overview	1-1
Lab A: Setting up the Lucerne Publishing Datacenter Environment	1-2
Lesson 1: Introduction to Office 365	1-14
Lesson 2: Provisioning Tenant Accounts	1-25
Lesson 3: Planning a Pilot	1-31
Lesson 4: Enabling Client Connectivity	1-38
Lab B: Preparing for Office 365	1-45
Module Review and Takeaways	1-55

Module 2: Managing Users, Groups, and Licenses

Module Overview	2-1
Lesson 1: Manage Users and Licenses by Using the Administration Center	2-2
Lesson 2: Manage Security and Distribution Groups	2-8
Lesson 3: Manage Cloud Identities with Windows PowerShell	2-12
Lab A: Managing Users, Groups, and Licenses	2-21
Lab B: Continue Lucerne Publishing Datacenter Setup	2-32
Module Review and Takeaways	2-36

Module 3: Administering Office 365

Module Overview	3-1
Lesson 1: Manage Administrator Roles in Office 365	3-2
Lesson 2: Configure Password Management	3-8
Lesson 3: Administer Rights Management	3-13
Lab: Administering Office 365	3-25
Module Review and Takeaways	3-37

Module 4: Planning and Managing Clients

Module Overview	4-1
Lesson 1: Plan for Office Clients	4-2
Lesson 2: Manage User-driven Client Deployments	4-12
Lesson 3: Manage IT Deployments of Office 365 ProPlus	4-16

Lesson 4: Office Telemetry and Reporting	4-22
Lab: Managing Clients	4-28
Module Review and Takeaways	4-41
Module 5: Planning DNS and Exchange Migration	
Module Overview	5-1
Lesson 1: Add and Configure Custom Domains	5-2
Lesson 2: Recommend a Mailbox Migration Strategy	5-12
Lab: Preparing for Exchange Migration	5-30
Module Review and Takeaways	5-39
Module 6: Planning Exchange Online and Configuring DNS Records	
Module Overview	6-1
Lesson 1: Plan for Exchange Online	6-2
Lesson 2: Configure DNS Records for Services	6-22
Lab: Configuring DNS Records and Migrating to Exchange Online	6-31
Module Review and Takeaways	6-44
Module 7: Administering Exchange Online	
Module Overview	7-1
Lesson 1: Configure Personal Archive Policies	7-2
Lesson 2: Manage Anti-malware and Anti-spam Policies	7-17
Lesson 3: Configure Additional Email Addresses for Users	7-29
Lesson 4: Create and Manage External Contacts, Resources, and Groups	7-35
Lab: Administering Exchange Online	7-50
Module Review and Takeaways	7-68
Module 8: Configuring SharePoint Online	
Module Overview	8-1
Lesson 1: Manage SharePoint Site Collections	8-2
Lesson 2: Configure External User Sharing	8-12
Lesson 3: Plan a Collaboration Solution	8-21
Lab: Configuring SharePoint Online	8-28

Module Review and Takeaways	8-37
Module 9: Configuring Lync Online	
Module Overview	9-1
Lesson 1: Plan for Lync Online	9-2
Lesson 2: Configure Lync Online Settings	9-9
Lab: Configuring Lync Online	9-14
Module Review and Takeaways	9-21
Module 10: Implementing Directory Synchronization	
Module Overview	10-1
Lesson 1: Prepare On-premises Active Directory for DirSync	10-2
Lesson 2: Set up DirSync	10-14
Lesson 3: Manage Active Directory Users and Groups with DirSync In Place	10-23
Lab: Implementing Directory Synchronization	10-28
Module Review and Takeaways	10-46
Module 11: Implementing Active Directory Federation Services	
Module Overview	11-1
Lesson 1: Planning for AD FS	11-2
Lesson 2: Install and Manage AD FS Servers	11-14
Lesson 3: Install and Manage AD FS Proxy Servers	11-22
Lab: Implementing Active Directory Federation Services	11-26
Module Review and Takeaways	11-44
Module 12: Monitoring Office 365	
Module Overview	12-1
Lesson 1: Isolate Service Interruption	12-2
Lesson 2: Monitor Service Health	12-12
Lesson 3: Analyze Reports	12-14
Lab: Monitoring Office 365 (Optional)	12-23
Module Review and Takeaways	12-28

About This Course

This section provides a brief description of the course, audience, suggested prerequisites, and course objectives.

Course Description

This course is an intensive and in-depth look at how to manage services Office 365, and in particular, how to manage identities, both in the cloud, and in situations where Office 365 is synchronized with on-premises Active Directory or where additional single-sign on (SSO) has been deployed.

Each module focuses on a specific area of Office 365, except for Modules 5 and 6, which together cover the highly interrelated areas of Domain Name System (DNS) and Exchange Online. The course starts with simpler configuration topics before moving on to more complex areas, such as Exchange Online migration, directory synchronization, and single-sign on (SSO) with Active Directory Federation Services (AD FS).

Course Scenario

The scenario in this course provides the framework for the practical labs that reinforce the knowledge covered in the modules. Hence, the scenario forms a linking narrative that explains what you are being asked to carry out in the labs.

Lucerne Publishing is a global media and printing corporation that owns a number of subsidiary companies, including Litware Inc, Proseware Inc, and the Graphic Design Institute. The group has just under 2,000 employees around the world and provides stories for newspapers, prints novels, licenses and creates and distributes digitally signed artwork for publication purposes.

The organization is moving to Office 365 to provide a more scalable business model that enables employees, authors, and illustrators to collaborate together and be more effective at selling their work globally.

For tax reasons, the organization's headquarters is in Berne in Switzerland, where the majority of its permanent staff work. However, it also has regional headquarters in the major continents and a number of content creators who work from home.

Hence, the customer will begin by managing user accounts in the cloud. However, when they discover that there are too many account changes happening, they make the decision to move to DirSync. Soon thereafter, they find that they need to implement enterprise search in hybrid SharePoint, so they have to implement single sign-on (SSO) through Active Directory Federation Services (AD FS).

The scenario implements the Office 365 FastTrack deployment approach, as covered in Course 10968B: *Designing for Office 365 Architecture*.

Audience

This course is intended for the following two audiences:

Primary Audience

- Specialty: IT Professional
- Typical Job Description: Consultant
- Role: Implementer
- Responsibilities: Evaluating, planning, deploying, and operating Office 365 services, including its identities, dependencies, and supporting technologies
- Skill Level: 300

Secondary Audience

- Specialty: IT Professional
- Typical Job Description: Network Administrator, IT Manager
- Role: Administrator
- Responsibilities: Managing and maintaining Office 365, including identities, document protection, integration with on-premises directory services, and compliance with service level agreements
- Skill Level: 200-300

Student Prerequisites

This course requires that you meet the following prerequisites:

Knowledge

- Completion of Clinic 40041 or equivalent technical knowledge.
- Cloud-based service concepts
- Overview of Office 365 and its component services
- Active Directory Directory Service
- TCP/IP network routing
- Domain Name Services (DNS)
- X.509 Certificates
- Firewall ports

Experience

- Using Windows PowerShell
- Administering Office 365 with Office 365 Admin Center
- Working with virtual machines
- Using Remote Desktop

Course Objectives

After completing this course, students will be able to:

- Prepare for the Office 365 Pilot and check the customer environment
- Configure DNS settings to support migration of customer domains to Office 365 and service provision.
- Manage users, groups and licenses in Office 365
- Administer administrator accounts in Office 365, manage passwords and apply Rights Management Services
- Plan for and manage the deployment of Office 365 clients
- Plan to migrate to or co-exist with Exchange Online
- Administer Exchange Online by configuring anti-spam and anti-malware settings
- Plan, set up and configure SharePoint Online to meet business requirements
- Plan and configure Lync Online to meet business requirements

- Plan and implement Directory synchronization with password synchronization for on-premises account administration
- Plan, implement and configure Active Directory Federation Services for single sign-on
- Monitor Office 365 and generate reports to ensure compliance with service level agreements

Course Outline

The course outline is as follows:

- **Module 1:** Preparing for Office 365
- **Module 2:** Managing Users, Groups, and Licenses
- **Module 3:** Administering Office 365
- **Module 4:** Planning and Managing Clients
- **Module 5:** Planning DNS and Exchange Migration
- **Module 6:** Planning Exchange Online and Configuring DNS Records
- **Module 7:** Administering Exchange Online
- **Module 8:** Configuring SharePoint Online
- **Module 9:** Configuring Lync Online
- **Module 10:** Implementing Directory Synchronization
- **Module 11:** Implementing Active Directory Federation Services
- **Module 12:** Monitoring Office 365

Course Materials

The following materials are included with your kit:

- **Course Handbook:** a succinct classroom learning guide that provides the critical technical information in a crisp, tightly-focused format, which is essential for an effective in-class learning experience.
 - **Lessons:** guide you through the learning objectives and provide the key points that are critical to the success of the in-class learning experience.
 - **Labs:** provide a real-world, hands-on platform for you to apply the knowledge and skills learned in the module. Each lab provides step-by-step lab solution guidance. Because of the complexity of the labs, the Lab Answer Key is displayed within the lab rather than at the end of the course.
 - **Module Reviews and Takeaways:** provide on-the-job reference material to boost knowledge and skills retention.
 - **Lab Answer Keys:** provide step-by-step lab solution guidance. The Lab Answer Keys are displayed within the labs themselves rather than at the end of the manual.



Additional Reading: Course Companion Content on the <http://www.microsoft.com/learning/en/us/companion-moc.aspx> **Site:** searchable, easy-to-browse digital content with integrated premium online resources that supplement the Course Handbook.

- **Modules:** include companion content, such as questions and answers, detailed demo steps and additional reading links, for each lesson. Additionally, they include Lab Review questions and answers and Module Reviews and Takeaways sections, which contain the review questions and answers, best practices, common issues and troubleshooting tips with answers, and real-world issues and scenarios with answers.
- **Resources:** include well-categorized additional resources that give you immediate access to the most current premium content on TechNet, MSDN®, or Microsoft® Press®.



Additional Reading: Student Course files on the <http://www.microsoft.com/learning/en/us/companion-moc.aspx> **Site:** includes the Allfiles.exe, a self-extracting executable file that contains all required files for the labs and demonstrations.

- **Course evaluation:** at the end of the course, you will have the opportunity to complete an online evaluation to provide feedback on the course, training facility, and instructor.
 - To provide additional comments or feedback on the course, send an email to support@microsoft.com. To inquire about the Microsoft Certification Program, send an email to mcp@microsoft.com.

Virtual Machine Environment

This section provides the information for setting up the classroom environment to support the business scenario of the course.

Virtual Machine Configuration

In a first for Microsoft Learning eXperiences (LeX) IT Professional courses, the virtual machines that make up the lab environment are hosted on Microsoft Azure, rather than running locally. This arrangement enables each student to have a fixed public IP address, thus enabling the advanced connectivity scenarios later in the labs. In the scenario, the VMs are all running in the Lucerne Publishing datacenter, which is at a remote location from the Headquarters of the business.



Note: There are NO snapshots for the labs – each lab runs on from the previous one. This requirement is due to the nature of the Microsoft Azure hosting environment and the

The Microsoft Azure images are all running Windows Server 2012. These servers host the following functionality:

- Active Directory domain controller, DNS, Certificate Authority
- Exchange Server 2013/SQL Server 2012 (for AD FS configuration database)
- 2 x AD FS server in fault-tolerant farm
- AD FS Proxy

In addition, there are two domain-joined client VMs in Microsoft Azure, which are Windows Server 2012 with the Desktop Experience enabled.

In the classroom, each student has a workgroup-based Windows 8 client VM that accesses the Internet through a Threat Management Gateway (TMG) server.

The following table shows the role of each virtual machine that is used in this course:

Virtual machine	Operating System	Role	Hosted in	Domain or workgroup
TMG1	Windows Server 2008 R2	Threat Management Gateway. Provides secure access to the Internet and protects the LUC-CL1 image.	Hyper-V on student's local computer	Workgroup
LUC-CL1	Windows 8	Used to simulate a typical client computer and to connect to Office 365 and the Lucerne Publishing datacenter environment	Hyper-V on student's local computer	Workgroup
LUC-DC1	Windows 2012	Provides Active Directory Directory Services and Domain Name Service (DNS).	Windows Azure	Domain (Domain controller)
LUC-EX1	Windows 2012	Runs Exchange Server for on-premises email	Windows Azure	Domain
LUC-SV1	Windows 2012	AD FS server	Windows Azure	Domain
LUC-SV2	Windows 2012	AD FS server	Windows Azure	Domain

Virtual machine	Operating System	Role	Hosted in	Domain or workgroup
LUC-SV3	Windows 2012	AD FS Proxy	Windows Azure	Workgroup
LUC-CL2	Windows 2012	Emulates domain-joined Windows 8 client	Windows Azure	Domain
LUC-CL3	Windows 2012	Emulates domain-joined Windows 8 client	Windows Azure	Domain

Software Configuration

The following software is installed on each student LUC-CL1 VM:

- Windows Azure PowerShell
- Microsoft Web Platform Installer 4.6
- IIS 8.0 Express
- IIS Express Application Compatibility Database for x64
- IIS Express Application Compatibility Database for x86
- Microsoft SQL Server 2012 Express LocalDB
- Windows Azure Authoring Tools - v2.2
- Windows Azure Emulator - v2.2
- Windows Azure Libraries for .NET - v2.2
- Windows Azure Storage Tools - v2.2

The remaining software is installed by the student themselves as part of the setup process.

Course Files

The files associated with the labs in this course are located in the <install_folder>\Labfiles\LabXX folder on the student computers.

Classroom Setup

Each classroom computer will have the same virtual machine configured in the same way.

Course Hardware Level

To ensure a satisfactory student experience, Microsoft Learning requires a minimum equipment configuration for trainer and student computers in all Microsoft Certified Partner for Learning Solutions (CPLS) classrooms in which Official Microsoft Learning Product courseware is taught.

- Hardware level 6 with dual monitors

Module 1

Preparing for Office 365

Contents:

Module Overview	1-1
Lab A: Setting up the Lucerne Publishing Datacenter Environment	1-2
Lesson 1: Introduction to Office 365	1-14
Lesson 2: Provisioning Tenant Accounts	1-25
Lesson 3: Planning a Pilot	1-31
Lesson 4: Enabling Client Connectivity	1-38
Lab B: Preparing for Office 365	1-45
Module Review and Takeaways	1-55

Module Overview

Office 365 is now a major part of the Microsoft range of software and services, enabling the delivery of the power of Microsoft Exchange, Microsoft SharePoint®, Microsoft Lync®, and Microsoft Office over the Internet to users located anywhere in the world. This service can be delivered on multiple platforms to provide enterprise-grade email, conferencing, and other IT services.

To implement Office 365 effectively, organizations need to ensure they can manage identities effectively. With user accounts both in the cloud and potentially on-premises, consultants, implementers, and administrators must be able to plan for, cope with, and manage a wide range of factors that affect how Office 365 works and identify the best way to manage user accounts and services.

This module reviews the features of Office 365 and identifies recent improvements to the service. It then identifies the challenges in deploying Office 365 and the benefits of the FastTrack approach compared to the traditional plan/prepare/migrate deployment process. After this, you will examine how to plan the pilot, provision tenant accounts and, finally, verify that clients can connect to the Office 365 service.



Note: This course does not cover the entire FastTrack process; this content is covered in course *10968B: Designing for Office 365 Infrastructure*.

Objectives

After completing this module, you should be able to:

- Describe the features and benefits of Office 365.
- Plan a pilot deployment of Office 365.
- Provision new tenant accounts.
- Check that clients can connect to the Office 365 service.

Lab A: Setting up the Lucerne Publishing Datacenter Environment

Scenario

In this preliminary lab, you set up Lucerne Publishing's datacenter for their "on-premises" infrastructure. This process requires students to set up a Windows® Live ID and sign up for a Microsoft Azure Learning Pass (both of which should have been done prior to class).

If students have not yet completed either of these tasks, they should do so now by performing the first two tasks in Exercise 1. Students can skip these tasks if they have already completed these steps.

Each student will then run a PowerShell® script in Microsoft Azure Active Directory that provisions this on-premises environment within Microsoft Azure. In this course, Microsoft Azure is used to represent both the Lucerne Publishing datacenter and the Lucerne Publishing corporate network. Microsoft Azure enables everyone in the classroom to have their own environment and public IP address, which means that Exchange can be migrated to Office 365, and Single Sign-On (SSO) can be enabled from any computer.

Objectives

By the end of this lab, you will have:

- Signed up for a new Windows Live ID.
- Signed up for Microsoft Azure.
- Created the Lucerne Publishing datacenter environment.

Lab Setup

Estimated Time: The bulk of this lab is centered on the provisioning script that you run in Exercise 1, Task 4. Run times for this script during Microsoft's testing have varied widely, ranging from 30 minutes to 4 hours, depending upon location, environment, and Azure system load. The average run time is usually around 2 to 3 hours, but a 4 hour run time should not be surprising. The lab should finish in time before your provisioned environment is needed by Module 2, Lab A. You should monitor the provisioning script periodically to ensure that it is running. If at any point you receive an error, perform Exercise 2, which recovers your environment so that you can re-run the provisioning script.

Virtual machine: 20346C-LUC-CL1

Username: **Student1**

Password: **Pa\$\$w0rd**

The classroom environment consists of the following virtual machines and domain names:

Hyper-V virtual machines:

- **LUC-CL1** is a Windows 8 computer, representing a remote, non-domain-joined workstation. Runs on the classroom Hyper-V host.


Azure virtual machines:

- **LUC-DC1** is the domain controller and DNS for Lucerne Publishing, and is hosted in Azure as part of the "Lucerne Publishing datacenter".
- **LUC-EX1** is the on-premises Exchange server for Lucerne Publishing, and is hosted in Azure as part of the "Lucerne Publishing datacenter".

- **LUC-SV1** and **LUC-SV2** are the AD FS server farm for Lucerne Publishing, and are hosted in Azure as part of the "Lucerne Publishing datacenter".
- **LUC-SV3** is the AD FS Proxy server for Lucerne Publishing, and is hosted in Azure as part of the "Lucerne Publishing datacenter".
- **LUC-CL2** and **LUC-CL3** simulate domain-joined workstations, but for this course are actually Windows Server 2012 computers with the Desktop Experience feature enabled, and are also hosted in Azure as part of the "Lucerne Publishing corporate network".

Domain names:

- **LucernePublishing.local** is Lucerne Publishing's internal private domain name.
- **LucernepublishingXXXX.onmicrosoft.com** is the temporary Office 365 domain assigned to Lucerne Publishing at the start of the pilot project, where XXXX is a unique Lucerne Publishing number that you will enter during Lab 1B in this module.
- **LabXXXXX.o365ready.com** represents Lucerne Publishing's public domain name (such as LucernePublishing.com), where XXXXX is a unique O365ready.com number that you will enter in Lab 2B in the next module.

 **Note:** Lab usage is billed at the going commercial rate for the West US datacenter. All Azure-hosted virtual machines must be shut down each night to avoid excessive charges. Failure to shut them down may result in not having enough credits to complete the class. **Do NOT shut down VMs in the Azure portal; this can result in IP address issues.**

Exercise 1: Set Up and Configure the Lucerne Publishing Data Center Environment

Scenario

Lucerne Publishing currently has a datacenter in Geneva that hosts the company's on-premises environment, which consists of Active Directory Domain Services, Exchange Server 2013, their document management system, customer relationship management (CRM) servers, and an enterprise resource planning (ERP) system. In effect, the IT department acts like an independent supplier and client computers connect to this datacenter environment over the Internet through its fixed IP address. Connectivity to the Internet is provided through a local Microsoft Threat Management Gateway server, which proxies out the requests to the data center.

In this lab, you set up and configure a simplified form of this data center environment, which includes a domain controller, an Exchange Server 2013 computer, two other domain-joined servers, a non-domain joined server and two client machines. You will use Windows Azure PowerShell scripts to carry out this automated process.

The primary setup script is **Provision.ps1**, which provisions your on-premises environment within Microsoft Azure. This script is designed so that if any errors occur while it was running, you can simply re-run the script and it will pick up from where it left off. If any errors occur when running the script originally, then re-running the script is the first step in the recovery process (see Exercise 2).

The Provision.ps1 script performs the following tasks:

1. Creates the Affinity Group if it does not exist.
2. Creates a storage account if it does not exist.
3. Copies the VHDs (storage blobs) that have not yet been copied.

4. Creates the VMs that do not yet exist.

WARNING: IT IS ESSENTIAL THAT YOU DO NOT CLOSE THE WINDOWS AZURE POWERSHELL SESSION DURING THE BUILD PROCESS OR AT THE END OF THE LAB.

If you accidentally close this session or restart the LUC-CL1 VM, you must perform the following steps before proceeding to their next exercise or task:

1. On LUC-CL1, press the Windows key.
2. On the Start screen, right-click **Windows Azure PowerShell**, and then click **Run as administrator**.
3. At the User Account Control dialog box, click **Yes**.
4. At the Windows Azure PowerShell prompt, type the following command, and press Enter:
CD E:\Setupfiles.
5. At the Windows Azure PowerShell prompt, type the following command, and press Enter:
Set-ExecutionPolicy -Scope Process Unrestricted -Force.

The main tasks for this exercise are as follows:

1. Sign up for a Windows Live Account (if needed)
2. Obtain Microsoft Azure Subscription (if needed)
3. Start LUC-CL1 and TMG Computers
4. Provision Lucerne Publishing "On-premises" Environment
5. Verify Domain Controller Setup (Optional)
6. Check Azure Account Balance

► **Task 1: Sign up for a Windows Live Account (if needed)**

NOTE: Students should have already completed Tasks 1 and 2 prior to arriving for this course. If you have not yet completed either of these tasks, then you should do so now. If you have completed both of these tasks, then proceed to Task 3.

1. Log on to **LUC-CL1** with a user name of **Student1** and a password of **Pa\$\$w0rd**.
2. In the Start screen, click **Desktop**.
3. On the desktop task bar, click **Internet Explorer**.
4. In the address bar, enter **http://live.com** and press Enter.
5. Click **Sign up now**.
6. Under **Name**, enter your first and last name.
7. In **User name**, select a user name that is not currently in use.
8. Leave the domain name as **outlook.com**.
9. In **Create password** and **Reenter password**, enter a suitable eight-character or longer password. Make a note of this password.
10. Under **Country/Region**, select your local region.
11. Enter any additional information, such as ZIP code or post code.

12. Enter a **Birthdate**.
13. Select your **Gender**.
14. Under **Country code**, select the country code for your mobile device.
15. In **Phone number**, enter the number of your mobile phone.
16. In **Alternate email address**, enter your existing email address.
17. Under **Enter the characters you see**, type in the letters and numbers displayed. Click **New** for a different combination if required.
18. Click to clear the **Send me promotional offers from Microsoft, you can unsubscribe at any time** option.
19. Click **Create account**.

► **Task 2: Obtain Microsoft Azure Subscription (if needed)**

NOTE: Students should have already completed Tasks 1 and 2 prior to arriving for this course. If you have not yet completed either of these tasks, then you should do so now. If you have already completed both of these tasks, then proceed to Task 3.

1. This course uses resources in Microsoft Azure and requires that students have a Microsoft Azure account. Learning Centers are authorized by Microsoft to assign Azure Learning Passes to students for this course.

Each student's Azure Learning Pass will provide them with an active Azure subscription that:

- a. Supports 8 or more VM cores to complete the labs.
 - b. Provides a \$100 US credit. Costs of services used during the labs will be charged against this credit balance.
2. Ask your instructor for details if you have not yet been assigned your Azure Learning Pass.

► **Task 3: Start LUC-CL1 and TMG Computers**

1. On the student host computer, click **Start**, point to **Administrative Tools**, and click **Hyper-V Manager**. Alternatively, on Windows 8, press the Windows key, type **Hyper-V**, and then click **Hyper-V Manager** on the Start screen.
2. In **Hyper-V Manager**, right-click **MSL-TMG1** and click **Start**.
3. Right-click **20346C-LUC-CL1** and click **Start**.
4. Right-click **20346C-LUC-CL1** and click **Connect**.
5. Log on to LUC-CL1 as **Student1** with a password of **Pa\$\$w0rd**.
6. If scroll bars are visible on the desktop when you start up LUC-CL1, perform the remaining steps in this task to adjust the resolution of the screen to fit with your host computer's monitor. If scroll bars are not visible, then proceed to the next task.
7. On LUC-CL1, right-click on the desktop and click **Screen resolution**.
8. In the **Screen Resolution** dialog box, next to **Resolution**, select **1024 x 768**, and click **Apply**.
9. Next to **Resolution**, select **1280 x 1024** and click **Apply**.
10. Check to see that there are no scroll bars on the desktop.
11. Click **OK** to close the Screen Resolution window.

► Task 4: Provision Lucerne Publishing “On-premises” Environment

Note: If at any point the scripts look stuck, make sure you did not accidentally “mark” the text by clicking on the Windows Azure PowerShell console window text area. You can unfreeze by hitting **Enter**. If the Azure window says “Select Administrator: Windows Azure PowerShell” then it will not update; this happens if you click anywhere in the PowerShell window. If this occurs, press **Esc** to enable updating again.

While running each PowerShell script, you should be observant for messages that may be displayed in different colors:

- Verbose messages in yellow or white
- Success messages in green
- Status messages in blue
- Error messages are usually red; these need to be addressed before proceeding.

1. On LUC-CL1, press the Windows key.
2. On the **Start** screen, right-click **Windows Azure PowerShell**, and then click **Run as administrator**.
3. At the **User Account Control** dialog box, click **Yes**.
4. If the **Do you want to run software from this untrusted publisher?** prompt appears in Windows Azure PowerShell, type **A** and then press Enter.
5. At the **Windows Azure PowerShell** prompt, type the following command and press Enter:
CD E:\Setupfiles
6. At the **Windows Azure PowerShell** prompt, type the following command and press Enter:
Set-ExecutionPolicy -Scope Process Unrestricted -Force
7. At the **Windows Azure PowerShell** prompt, type the following command and press Enter:
Get-AzurePublishSettingsFile
8. In Internet Explorer, sign in with the Live ID associated with your Azure account; this should be **username@outlook.com**, (where username@outlook.com is the Windows Live address you registered in Lab 1A, Exercise 1, Task 1).
9. At the **Internet Explorer Save File** dialog box, click the **Save** drop-down, and then click **Save as**.
10. Note the name of your publish settings file: _____

Note: File names can be quite long; therefore, if you are not familiar with using Autocomplete when typing file names, you can optionally change the name to a shorter, more user-friendly name when you save the file in the next step (for example, **XXX.publishsettings**, where XXX are your initials).

11. In the **Save As** dialog box, navigate to **E:\Setupfiles**, and click **Save**.
12. Switch to the **Windows Azure PowerShell** prompt, type the following command and press Enter:
Import-AzurePublishSettingsFile -PublishSettingsFile "E:\Setupfiles*name of your downloaded publish settings file*"
Important: Wait until the import has completed before proceeding to the next step.
13. To run the first provisioning script, at the **Windows Azure PowerShell** prompt, type the following command and press Enter:
.\Provision.ps1

Important: The command starts with dot space dot backslash.

Note: If you get red script errors, you should stop the script execution by pressing Ctrl + C, and then proceed to **Exercise 2 (Recover from Provisioning Errors)**.

14. When prompted, enter the eight-digit number for your Learning Center and press Enter. Your instructor will provide you with this number.
15. When prompted, enter your three-digit student number and press Enter. Your instructor will provide you with this number.
16. Make a note of your "unique suffix" from the Window Azure prompt; you will need this later in this lab:

17. Microsoft's testing has shown that Provision.ps1 run times have varied widely, ranging from 30 minutes to 4 hours, depending upon location, environment, and Azure system load. The average run time is usually around 2 to 3 hours, but a 4 hour run time should not be surprising. The lab should finish in time before your provisioned environment is needed by Module 2, Lab A.

Important: While the script is running, the instructor should continue with the rest of the course, starting with the lecture content in **Lesson 1, Introduction to Office 365**. You can proceed up to **Module 2, Lab A** while the script is running.

Note: If you get red script errors, you should stop the script execution by pressing Ctrl + C, and then proceed to **Exercise 2 (Recover from Provisioning Errors)**.

18. When the script has completed, type the following command at the **Windows Azure PowerShell** prompt and press Enter:

.. \AzureStatus.ps1

Important: The command starts with dot space dot backslash.

This script should display the following information for each Azure virtual machine:

Name	InstanceStatus	PowerState	IPAddress
LUC-CL3	ReadyRole	Started	10.0.0.10
LUC-CL2	ReadyRole	Started	10.0.0.9
LUC-SV1	ReadyRole	Started	10.0.0.6
LUC-DC1	ReadyRole	Started	10.0.0.4
LUC-EX1	ReadyRole	Started	10.0.0.5

Name	InstanceStatus	PowerState	IPAddress
LUC-SV2	ReadyRole	Started	10.0.0.7
LUC-SV3	ReadyRole	Started	10.0.0.8

19. **IMPORTANT:** If any of the Azure virtual machines in the prior table was not created, then you must re-run the Provision.ps1 script by repeating steps 13-18.

You should only proceed to the next task if the provisioning script completed with no errors and all of the expected Azure virtual machines were created.

► Task 5: Verify Domain Controller Setup (Optional)

Note: This task is optional. While Microsoft testing has shown that domain controller setup has always been successful following provisioning, you can manually verify the setup by performing the following steps.

1. On **LUC-CL1**, on the Taskbar, click **File Explorer**.
2. Navigate to **E:\RDP_files**, and verify the following files exist:
 - a. LUC-DC1.rdp
 - b. LUC-EX1.rdp
 - c. LUC-SV1.rdp
 - d. LUC-SV2.rdp
 - e. LUC-SV3.rdp
 - f. LUC-CL2.rdp
 - g. LUC-CL3.rdp
- Note:** You have the option to download and install Remote Desktop Connection Manager (RDCMan) on LUC-CL1 or onto the local host computer to manage the Microsoft Azure RDP sessions. RDCMan is available from <http://go.microsoft.com/fwlink/?LinkId=401125>.
3. Double-click **LUC-DC1.rdp**.
4. If a Remote Desktop Connection warning message appears, click **Don't ask me again for connections to this computer** and click **Connect**.
5. Connect as **LUCERNE\LucAdmin**, password: **Pa\$\$w0rd**.
6. If another Remote Desktop Message appears, click **Don't ask me again for connections to this computer** and click **Yes**.

Note: When connecting to LUC-DC1, Microsoft's testing has, on rare occasions, received a message asking if you want to install updates. Do NOT install updates if such a message appears.

7. On **LUC-DC1**, in **Server Manager**, click **Tools** and then click **Active Directory Users and Computers**.

Note: You can use Active Directory Administrative Center to carry out the tasks in Active Directory Users and Computers.

8. In the **Lucerne Publishing** domain, verify that the following organizational units (OU) are empty: **Accounts, Engineering,** and **Sales**.
9. In the **Lucerne Publishing** domain, verify that the **Computers** OU contains the following computers:
 - a. LUC-EX1
 - b. LUC-SV1
 - c. LUC-SV2
 - d. LUC-CL2
 - e. LUC-CL3
10. Verify server to server communications by pinging the following IP addresses. To ping a server open a command prompt and type **ping <IP address>** (e.g. ping 10.0.0.5).
 - a. 10.0.0.5
 - b. 10.0.0.6
 - c. 10.0.0.7
 - d. 10.0.0.8
11. Minimize the RDP session.

► Task 6: Check Azure Account Balance



Note: Lab usage is billed at the going commercial rate for the West US datacenter. All Azure-hosted virtual machines must be shut down each night to avoid excessive charges. Failure to shut them down may result in not having enough credits to complete the class.

WARNING: Do NOT shut down VMs in the Azure portal; this can result in IP address issues.

1. To check your Azure account balance, in a browser, go to: **<http://azure.microsoft.com/en-us/>**
2. Click **Portal**.
3. Sign in using the Microsoft Account associated with your Azure subscription.
4. At the top of the page click on the box at the top center of the page that says **Credit Status or Account Status** to see your current balance.
5. You do not need the Azure Portal for any additional lab steps in this course. However, it can be left logged in so that you can monitor progress against your account balance.

Results: At the end of the lab, you will have a working “on-premises” environment in the Lucerne Publishing data center. In reality, this environment is hosted in Microsoft Azure.

Exercise 2: Recover from Provisioning Errors (If Required)

Scenario

There is no scenario for this exercise.

IMPORTANT: You should only perform the tasks in this exercise if you have experienced problems when setting up and configuring the Lucerne Publishing Datacenter environment in Lab A, Exercise 1, Task 4.

There are three parts to the recovery process. The first two parts (Recovery Steps 1 and 2) have been designed to automatically recover from the errors received. If errors still occur after running both of these automated processes, then you must manually perform a series of steps (in Recovery Step 3) to remove the Azure artifacts before attempting to provision the Lucerne Datacenter one last time. The recovery process has been designed so that hopefully one of the automated processes in Recovery Steps 1 or 2 fixes the problem, thereby saving you from having to manually perform the steps in Recovery Step 3. However, if both of the automated fixes do not resolve the issue, then you must perform the manual process to complete the provisioning.

A summary of the recovery process is as follows:

1. **Recovery Step 1 – Re-run Provision.ps1.** In most cases, re-running the Provision.ps1 script will fix the problem.
 - a. If this fixes the problem, then skip Recovery Steps 2 and 3 and continue with Lab A, Exercise 1, Task 4, starting with step 14.
 - b. However, if re-running Provision.ps1 again fails, then proceed to Recovery Step 2.
2. **Recovery Step 2 – Run RemoveAll.ps1 and then Re-run Provision.ps1.** If re-running Provision.ps1 in the prior step still results in an error, then run the RemoveAll.ps1 script before re-running Provision.ps1 again.
 - a. If this fixes the problem, then skip Recovery Step 3 and continue with Lab A, Exercise 1, Task 4, starting with step 14.
 - b. However, if re-running Provision.ps1 fails again after having run the RemoveAll.ps1 script, then proceed to Recovery Step 3.
3. **Recovery Step 3 – Perform Manual Recovery Steps and then Re-run Provision.ps1.** If the provisioning script still encounters an error after you ran RemoveAll.ps1, then you must manually remove the Azure artifacts before re-running the provisioning script.
 - a. If this fixes the problem, then continue with Lab A, Exercise 1, Task 4, starting with step 14.
 - b. However, if re-running Provision.ps1 fails after you manually performed the recovery steps in this task, then contact your instructor.

The main tasks for this exercise are as follows:

1. Recovery Step 1 – Re-run Provision.ps1
2. Recovery Step 2 – Run RemoveAll.ps1 and then Re-run Provision.ps1 (If Required)
3. Recovery Step 3 – Perform Manual Recovery Steps and then Re-run Provision.ps1 (If Required)

► **Task 1: Recovery Step 1 – Re-run Provision.ps1**

The first step in the recovery process is to re-run the provisioning script. In most cases rerunning Provision.ps1 will fix the problem.

1. At the **Windows Azure PowerShell** prompt, type the following command and press Enter:

```
. .\Provision.ps1
```

Note: Your next step depends on whether you receive any errors when running the provisioning script.

2. **No errors; Successful recovery:** If the provisioning script prompts you for your 8 digit Learning Center number without encountering an error, then return to **Exercise 1, Task 4** (Provision Lucerne Publishing "On-premises" Environment) starting with step 14, where you will enter the 8 digit Learning Center number and continue with the provisioning process.
3. **Errors occurred; Failed recovery:** If you get red script errors, you should stop the script execution by pressing Ctrl + C, and then proceed to **Task 2: Recovery Step 2**.

► **Task 2: Recovery Step 2 – Run RemoveAll.ps1 and then Re-run Provision.ps1 (If Required)**

You should only perform this task if you encountered an error when re-running the Provision.ps1 script in Recovery Step 1. In this task, you will run the RemoveAll.ps1 script and then re-run the Provision.ps1 script.

1. On LUC-CL1, press the Windows key.
2. On the **Start** screen, right-click **Windows Azure PowerShell**, and then click **Run as administrator**.
3. At the **User Account Control** dialog box, click **Yes**.
4. If the **Do you want to run software from this untrusted publisher?** prompt appears in **Windows Azure PowerShell**, type **A** and then press Enter.
5. At the **Windows Azure PowerShell** prompt, type the following command and press Enter:
CD E:\Setupfiles
6. At the **Windows Azure PowerShell** prompt, type the following command and press Enter:
Set-ExecutionPolicy -Scope Process Unrestricted -Force
7. At the **Windows Azure PowerShell** prompt, type the following command and press Enter:
..\RemoveAll.ps1
8. At the **Windows Azure PowerShell** prompt, type the following command, and press Enter:
..\Provision.ps1

Note: Your next step depends on whether you receive any errors when running the provisioning script.

9. **No errors; Successful recovery:** If the provisioning script prompts you for your 8 digit Learning Center number without encountering an error, then return to **Exercise 1, Task 4** (Provision Lucerne Publishing "On-premises" Environment) starting with step 14, where you will enter the 8 digit Learning Center number and continue with the provisioning process.
10. **Errors occurred; Failed recovery:** If you get red script errors, you should stop the script execution by pressing Ctrl + C, and then proceed to **Task 3: Recovery Step 3**.

► **Task 3: Recovery Step 3 – Perform Manual Recovery Steps and then Re-run Provision.ps1 (If Required)**

You should only perform this task if you encountered an error when re-running the Provision.ps1 script in Recovery Step 2. In this task, you will manually remove the Azure artifacts before re-running the Provision.ps1 script.

1. In **LUC-CL1**, run **Windows PowerShell**.
2. On the Taskbar, click **Internet Explorer**.

3. In the address bar, type **http://manage.windowsazure.com** and press Enter.
4. Sign in with the Live ID associated with your Azure account; this should be **username@outlook.com**, (where username@outlook.com is the Windows Live address you registered in Lab 1A, Ex 1 Task 1).
5. In the Microsoft Azure portal, click **VIRTUAL MACHINES**.
6. In the virtual machines list, click **LUC-DC1**, and on the bottom bar, click **DELETE**, and then click **Delete the attached disks**. If virtual machine **LUC-DC1** is not listed, go to step 9.
7. At the confirmation prompt, click **YES**.
8. Wait until the deletion has completed.
9. In the virtual machines list, click **LUC-EX1**, and on the bottom bar, click **DELETE**, and then click **Delete the attached disks**. If virtual machine **LUC-EX1** is not listed, go to step 12.
10. At the confirmation prompt, click **YES**.
11. Wait until the deletion has completed.
12. In the virtual machines list, click **LUC-SV1**, and on the bottom bar, click **DELETE**, and then click **Delete the attached disks**. If virtual machine **LUC-SV1** is not listed, go to step 15.
13. At the confirmation prompt, click **YES**.
14. Wait until the deletion has completed.
15. In the virtual machines list, click **LUC-SV2**, and on the bottom bar, click **DELETE**, and then click **Delete the attached disks**. If virtual machine **LUC-SV2** is not listed, go to step 18.
16. At the confirmation prompt, click **YES**.
17. Wait until the deletion has completed.
18. In the virtual machines list, click **LUC-SV3**, and on the bottom bar, click **DELETE**, and then click **Delete the attached disks**. If virtual machine **LUC-SV3** is not listed, go to step 21.
19. At the confirmation prompt, click **YES**.
20. Wait until the deletion has completed.
21. In the virtual machines list, click **LUC-CL2**, and on the bottom bar, click **DELETE**, and then click **Delete the attached disks**. If virtual machine **LUC-CL2** is not listed, go to step 24.
22. At the confirmation prompt, click **YES**.
23. Wait until the deletion has completed.
24. In the virtual machines list, click **LUC-CL3**, and on the bottom bar, click **DELETE**, and then click **Delete the attached disks**. If virtual machine **LUC-CL3** is not listed, go to step 27.
25. At the confirmation prompt, click **YES**.
26. Wait until the deletion has completed.
27. In the Microsoft Azure portal, click **CLOUD SERVICES**, and on the bottom bar, click **DELETE**. If no **Cloud Services** object is listed, go to step 30.
28. At the confirmation prompt, click **YES**.
29. Wait until the deletion has completed.
30. In the Microsoft Azure portal, click **NETWORKS** and on the bottom bar, click **DELETE**; if no virtual network is listed, go to step 33.

31. At the confirmation prompt, click **YES**.
32. Wait until the deletion has completed.
33. In the Microsoft Azure portal, on the networks page, click **DNS SERVERS** and on the bottom bar, click **DELETE**; if no DNS is listed, go to step 36.
34. At the confirmation prompt, click **YES**.
35. Wait until the deletion has completed.
36. In the Microsoft Azure portal, click **STORAGE** and on the bottom bar, click **DELETE**; if no storage is listed, go to step 39.
37. At the confirmation prompt, click **YES**.
38. Wait until the deletion has completed.
39. In the Microsoft Azure portal, click **SETTINGS**, then click **AFFINITY GROUPS**, and then, on the bottom bar, click **DELETE**. If no Affinity Group object is listed, go to step 42.
40. At the confirmation prompt, click **YES**.
41. Wait until the deletion has completed.
42. At the **Windows Azure PowerShell** prompt, type the following command and press Enter:

```
.. \Provision.ps1
```

Note: Your next step depends on whether you receive any errors when running the provisioning script.

43. **No errors; Successful recovery:** If the provisioning script prompts you for your 8 digit Learning Center number without encountering an error, then return to **Exercise 1, Task 4** (Provision Lucerne Publishing "On-premises" Environment) starting with step 14, where you will enter the 8 digit Learning Center number and continue with the provisioning process.
44. **Errors occurred; Failed recovery:** If you get red script errors, you should stop the script execution by pressing Ctrl + C, and then contact your instructor.

Lesson 1

Introduction to Office 365

This first lesson provides you with a refresh on the components and benefits of Office 365. Although you are probably familiar with this information, you need to have a consistent view of the capabilities of this platform. It is also important that you can identify the improvements in the latest service pack and that you know where to find information about service updates.

It is also important to remember that Office 365 is very much regarded as a key component in the development of Microsoft product and services offerings, so you should be fully conversant with each offering. However, it is understood that students will have differing depths of knowledge about each online service.

Lesson Objectives

After completing this lesson, you should be able to:

- Explain the purpose and function of Office 365.
- Describe the core components of the Office 365 service.
- Identify optional components of Office 365.
- Explain the benefits of Office 365.
- List the improvements in the latest service pack of Office 365.
- Explain the traditional deployment methodology.
- Highlight the issues with this older process.
- List the phases in the new FastTrack approach.
- Highlight the advantages of the FastTrack approach.
- Provide an overview of the activities within each phase of the FastTrack approach.
- Correlate the Office 365 FastTrack process with Microsoft Operations Framework V4.0.





Overview of Office 365

Office 365 is Microsoft's premier cloud-based productivity suite that delivers software as a service (SaaS) to users around the world. This latest release has been updated to meet customers' greater expectations and to deliver innovation and value within the workplace.

There are four main areas in which Office 365 provides significant improvements: devices, cloud, social, and control.

Devices

The entire Office user interface has been updated and made more engaging, with a clean, fast, and fluid experience. You can interact with it using touch, pen, mouse, or keyboard. The new Office works great across all your devices, especially on Windows 8.1, where you get a more immersive, touch-optimized experience. Office Mobile gives you a consistent, yet

	Devices <ul style="list-style-type: none"> • Fast and fluid experience with touch, pen, mouse, and keyboard • Immersive touch-optimized Windows 8 apps • Support for Windows phone, iOS phones, and Android phones
	Cloud <ul style="list-style-type: none"> • Office – on-demand, roaming, and up-to-date • New cloud app development model • Enterprise-grade reliability and standards
	Social <ul style="list-style-type: none"> • Newsfeeds and microblogging, extend with Yammer • Pervasive social capabilities across Office • Multiparty HD video and Skype federation
	Control <ul style="list-style-type: none"> • DLP, data retention, and unified eDiscovery • Reimagined deployment model for Office apps • Common management experience across Office 365

platform-optimized Office experience. The Office Mobile apps are available on Windows Phone and iPhone, and OneNote® and Lync Mobile are also available for iOS and Android phones.

Cloud

Office 365 was designed for the cloud as an on-demand service that is always up-to-date. It includes the latest release of the Office desktop suite that installs on demand through a new cloud application deployment model. By combining cloud services and web technologies, this new class of apps extends and personalizes the way we create and consume information from within Office and SharePoint. Office 365 is also an enterprise-grade cloud productivity solution with robust security, guaranteed reliability, and industry standards compliance, including ISO-27001, EU Model clauses, HIPAA, and FISMA.

Social

Social networking is changing the way people work and interact, both inside and outside the office. Office 365 integrates social networking into the organization by providing newsfeeds and microblogging services that can be extended with Yammer. Access to information about people is easier than ever to find and ties in with presence status through Microsoft Lync. Lync now also supports multiparty high-definition video and federation with Skype.

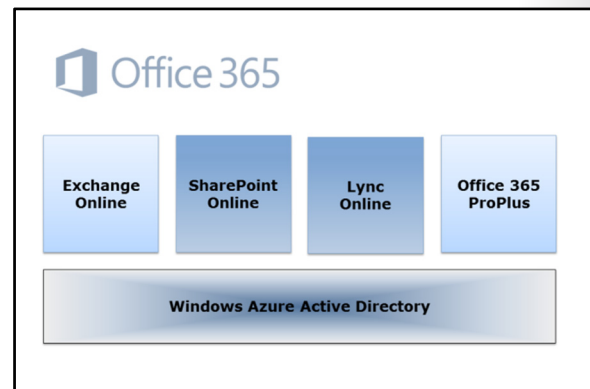
Control

Office 365 provides a secure and safe way for organizations to keep control of their business data. Data Loss Prevention (DLP) controls the passage of sensitive information within the organization, and unified eDiscovery enables searching across multiple data sources. Archiving and data hold capabilities ensure that critical information cannot be deleted, and Office 365 provides a unified management experience across all its services.

Core Components of Office 365

Since knowledge of the basic Office 365 features is a prerequisite for this course, this topic does not delve into the details of the feature set; rather, this topic simply recaps on the main components of the service.

The core services in Office 365 consist of cloud-based equivalents of three of Microsoft's premier server products, along with an integrated directory service and an install-on-demand version of Office 2013. These popular productivity applications enable organizations of all sizes to move their entire IT infrastructure to the cloud or to implement a range of hybrid options, depending on need.



 **The service descriptions for the latest version of Office 365 can be found here:**

<http://go.microsoft.com/fwlink/?LinkId=285516>

Microsoft Azure Active Directory

Underpinning all the Office 365 services is Microsoft Azure Active Directory (Microsoft Azure AD), an online instance of Active Directory that also provides authentication and authorization services for other Microsoft cloud offerings, including Microsoft Azure and Windows Intune™. Authentication through Microsoft Azure AD can be on a cloud-only basis, through directory synchronization (with optional

password synchronization), or include full integration with on-premises directory services through support for Active Directory Federation Services or other SSO providers.

Exchange Online

Microsoft Exchange Online in Office 365 is the latest release of this world-leading messaging and collaboration platform, providing one location for composing, reading, and storing email, calendar, contact, and task information in Microsoft Outlook®, Outlook Web Access, or Outlook Mobile. Exchange Online includes a massive 50 GB mailbox (up from 25 GB) combined with unlimited storage within the archive mailbox in the Office 365 E3 or E4 plans or Exchange Online Plan 2. Exchange Online supports access from most mobile devices, including BlackBerry, iPhone, Nokia, and Windows Phone.



Note: The unlimited storage available within the archive mailbox can store up to 100 GB of Outlook data without restriction. Additional storage increments are available by contacting Microsoft Office 365 Support.

SharePoint Online

Using Microsoft SharePoint Online, you can share important documents, insights, and status updates with colleagues. You can keep teams in sync and manage important projects, find vital documents, and locate people easily. Using SharePoint can also help you to stay up-to-date with company information and news, regardless of whether you are in or out of the office. Storage space is initially set at 10 GB per tenant and 500 MB per user, but storage upgrades are available. In addition, each user receives another 25 GB in OneDrive™ for Business (up from 7 GB) for additional document storage or transfer.

Lync Online

Lync Online provides presence and instant messaging information, so users can identify whether people are available and then chat, call, and video conference with each other. By using Lync Online, you can also create online meetings with audio, video, and web conferencing for up to 250 people, including anonymous users from outside the organization. You can implement multiparty high-definition (HD) video with hardware that supports this capability. To improve productivity, Lync Online provides integration with users' calendars in Microsoft Exchange and also enables the "click to communicate" feature in Outlook, SharePoint, and other Office applications.





Office 365 ProPlus

Some Office 365 plans include Office 365 ProPlus, which is a downloadable version of Microsoft's world-leading productivity suite of applications, including Word® 2013, Excel® 2013, PowerPoint® 2013, Outlook 2013, Access® 2013, Publisher 2013, OneNote 2013, InfoPath®, and the Lync 2013 client. There are also Web App versions of Word, Excel, PowerPoint, and OneNote.

Office 365 ProPlus supports streaming deployment, which enables users to click the application installation icon and start using the application itself while the program installs in the background. This deployment method also enables users to run Office 365 ProPlus alongside earlier versions of Microsoft Office.

Optional Components of Office 365

Organizations can also subscribe to optional components within Office 365 that can enhance their use of this cloud-based service and provide users with additional facilities to increase productivity. These optional components include Yammer, Project Online, Project Pro for Office 365, and Microsoft Office Visio® Pro for Office 365.

Product	Plan	Includes
	SharePoint Online	Replacement of SharePoint as the primary enterprise social experience
	Project Pro for Office 365	Subscription version of Project Professional client software with roaming access and click to run
	Project Online	Online-only version of Project server, delivering enterprise project, program, and portfolio management
	Project Online with Project Pro for Office 365	Subscription version of Project Professional client with online capabilities of Project Online
	Microsoft Office Visio Pro for Office 365	Subscription version of the advanced diagramming software, including roaming access and click to run
	Microsoft Dynamics CRM	Subscription version of Microsoft Dynamics CRM provides customer management information in the cloud

Yammer

Microsoft’s enterprise social networking tool is now becoming more integrated with Office 365, with the option for SharePoint Online users to replace their activity stream in SharePoint Online with Yammer. To make this change, users click a Yammer link and sign in to this service through a separate browser window. Future integration will include SSO between the Yammer service and Office 365 and using the Yammer Newsfeed instead of the one in SharePoint Online.

Project Online

Project Online is the cloud version of Microsoft Project Server, and enables organizations to get started, prioritize project portfolio investments, and deliver with the intended business value. A key value proposition with Project Online is that it enables global organizations to plan portfolios of projects in multiple time zones.

Project Pro for Office 365

Project Pro for Office 365 provides desktop project management capabilities for small teams and organizations. This service can be combined with Project Online for organizations that need full project-management capabilities on the desktop, combined with the ability to participate online from virtually anywhere on almost any device.

Microsoft Office Visio Pro for Office 365

Office Visio Pro for Office 365 is a subscription version of the versatile diagramming and flow charting application that is Visio Professional 2013. Users can install it on up to five devices and it includes Visio on Demand, which a user can use to install the application temporarily on any PC running Windows 7 or Windows 8.

Microsoft Dynamics CRM Online

Microsoft Dynamics CRM Online is the cloud-based version of Microsoft Dynamics® CRM (Customer Relationship Management). It enables sales teams to engage more effectively with customers and use familiar Office tools to achieve targets for sales, marketing, customer care, and social media interaction.

Benefits of Office 365

Office 365 provides a range of benefits for organizations of all sizes. A key part of the exceptional value provided by Office 365 is that it includes a full copy of the latest version of the familiar Office applications. Unlike the full packaged product version of Office Professional 2013, Office 365 ProPlus comes with generous usage rights on up to five devices. This familiarity, combined with new productivity enhancements in the most recent update and the simplified licensing and deployment model, makes Office 365 a compelling service.

- Familiar and full Office applications are available online
- Advanced IT controls and configuration
- Optimized experiences for common devices
- Reliable services run at scale with a 99.9 percent SLA
- Continuous innovation
- Trusted service

Office 365 provides a simple yet powerful unified web-based administrative interface that enables organizations or their managing partners to configure settings from anywhere in the world. It also supports Windows PowerShell scripts and interactive commands through the Microsoft Azure Active Directory PowerShell Module (formerly the Microsoft Online Services Module for Windows PowerShell).



For more information about the Microsoft Azure AD PowerShell module, go to:

<http://go.microsoft.com/fwlink/?LinkId=313233>

Office 365 embraces the concept of “bring your own device,” (BYOD) and in conjunction with Windows Intune, even large and highly-structured organizations with strictly defined IT policies can work with user-supplied devices in a range of platforms and sizes. Windows Surface with Windows RT, Windows Phone, iPhone and iPad, Android, BlackBerry, and Nokia (Symbian) devices are all supported, albeit with different functionality levels.



Windows Intune provides cloud-based system management of PCs and mobile devices. For more information, see the following link:

<http://go.microsoft.com/fwlink/?LinkId=401126>

Office 365 includes a true financially backed Service Level Agreement (SLA). This SLA provides a service credit for up to 100 percent of the month’s fees if the service uptime falls below 99.9 percent.



To view the Service Level Agreement for Microsoft Online Services, see:

<http://go.microsoft.com/fwlink/?LinkId=321165>

Office 365 delivers a program of continuous innovation through service upgrades (major) and service updates (minor). A service upgrade is like a move from Exchange Server 2010 to Exchange Server 2013, whereas service updates are similar to service pack installations. Because of the cloud-based nature of the Office 365 service, Microsoft can deliver these updates continuously without customers having to plan for potentially disruptive upgrades to their internal infrastructure. Customers will also be kept on the latest version of the Microsoft platform, thus helping ensure that their users have the most productive applications and the best experience for communication and collaboration.

Finally, Office 365 provides a trusted service that enables organizations to get on with their core business activity and not have to worry about providing their own IT. Microsoft’s geographically dispersed data centers, with data replication between these locations, provide a service that companies of all sizes can trust to deliver the applications they need to compete effectively.

Improvements in the Latest Office 365 Service Upgrade

Office 365 delivers its promise of continuous innovation through a series of service upgrades and service packs. Service upgrades are completely automated and typically have minimal effect on the organization. For example, an Outlook user might be required to restart Outlook, but all his email messages will still be available directly following the upgrade.

The 2013 service upgrade updates the different online services to the latest releases. All the other features of Office 365 either remain or have been significantly enhanced. In summary, the 2013 service upgrade includes the following changes:

- Exchange Online is now based on Exchange Server 2013.
- SharePoint Online is now based on SharePoint Server 2013.
- Lync Online is based on Lync Server 2013.
- Office 365 ProPlus is now Office 2013 Professional.

Individual changes in the 2013 upgrade include:

- A new look for Outlook Web App that is optimized for easy touch access on tablets and mobile phones.
- Improved anti-malware protection to help prevent malware from ever reaching inboxes.
- Better collaboration in SharePoint Online, making it easier to share documents with external users and manage external sharing.
- Inclusion of OneDrive for Business, a cloud storage option where users can keep documents synchronized with their hard-drive for off-line access.
- A new Lync Web App that delivers a full Lync Meeting experience with high-definition video and VoIP, all from a browser.
- One-click meeting access; whether you're at the office or on the road, you no longer need to remember dial-in numbers and passcodes.
- An improved administrative interface, including greater control over distribution groups, contacts, shared mailboxes, calendar publishing, and social media integration.

The following link describes how Microsoft uses the recently released Office 365 for Business Public Roadmap for communicating updates and providing a forward looking view of its service plans:



<http://go.microsoft.com/fwlink/?LinkId=321167>

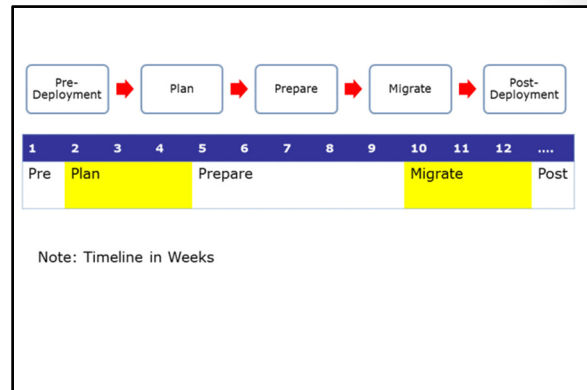


Note: If an advised service upgrade date is inconvenient, customers can postpone this date once.

	Exchange Online	SharePoint Online	Lync Online	Office 365 ProPlus
Upgrade	Updated to Exchange 2013	Updated to SharePoint 2013	Updated to Lync 2013	Updated to Office 2013
Detailed changes	New Outlook Web App for mobiles Improved anti-malware Social media integration (Facebook and LinkedIn)	Better collaboration with external users OneDrive for Business with 25 GB storage for easier file sharing	New Lync Web App delivering HD video and VoIP from a browser One-click meeting access	Use of Office Web Apps in OneDrive for Business and team sites

Traditional Deployment Methodology

In a traditional on-premises deployment, you typically go through a structured process that involves many interminable planning meetings, filling in numerous checklists, and attempting to reduce risks to the minimum acceptable level. The old Office 365 deployment model echoes this process with five phases, consisting of pre-deployment planning and consultation, followed by a planning phase, a preparation phase, the core migration phase, and some consequential post-deployment work to ensure everything is working correctly.



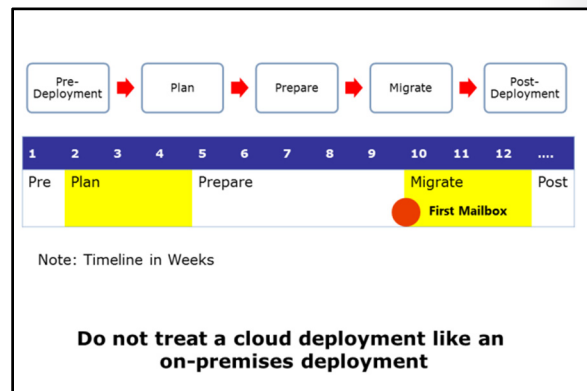
With an on-premises deployment, this complex, risk-adverse approach is understandable, particularly as you are migrating to an environment that is not working. But this approach does result in considerable disadvantages, which are at odds with the responsive nature of the Office 365 platform itself.

Disadvantages of the Traditional Deployment Approach

With the traditional deployment approach, it might take the organization several weeks or even months to reach the migration phase. This is time in which the organization is not able to experience the benefits of Office 365 first-hand. Even when they test out the pilot deployment, that environment would often be lightly used and then discarded, in effect invalidating the pilot and minimizing any useful operational experience that the pilot might provide.

The result of this approach is that it may be two or more months until the first users are migrated across to their Office 365 mailboxes, and three to four months before the organization finally benefits from moving to the new service. This situation is not ideal, both from the sales perspective and from the organization viewpoint.

A key message is that cloud deployments are not like traditional on-premises deployments, and they need a new methodology to suit.



The FastTrack Deployment Process

While the traditional deployment methodology includes five phases, the FastTrack deployment process has only three main parts: Pilot, Deploy, and Enhance.

Pilot

The Pilot phase is implemented in hours and has minimal prerequisites. The aim is to get a representative group of users onto the service and redirecting their mail from their current messaging system to their Office 365 mailboxes. The overall aim is to:

- Use the service early.
- Allow the organization to use the service and see how it fits their needs.
- Show the options for a simple and quick deployment.

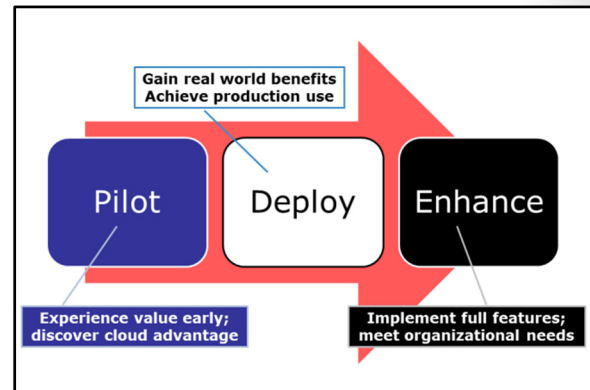
Deploy

The Deploy phase follows directly after the Pilot phase, so none of the pilot effort is wasted. The organization transitions rapidly into the live environment, which enables the organization to:

- Achieve broad production use quickly.
- Meet time to service use with deployment options.

Enhance

Finally, in the Enhance phase, the organization can include optional enhancements to meet its business needs. If these additions are not required, they are simply never implemented.



Advantages of the FastTrack Approach

With the Office 365 FastTrack deployment approach, customers can:

- Experience the value of Office 365 much earlier than with traditional deployment methodologies.
- Evolve into features as and when required.
- Determine how far down the Office 365 migration path to go.

With the FastTrack approach, a rich user experience and productivity solution can be delivered with minimal on-premises requirements, particularly in the Pilot phase. The organization has a choice of deployment models that reflect the investment required against the time to value.

- No throw-away effort on a production pilot
- Full Office 365 user experience with minimal on-premises requirements
- Reduced time to value against effort invested
- Multiple data migration methods:
 - New mailbox, self-service, and IT managed
- Range of identity options:
 - Cloud IDs, synchronized IDs, password sync, and federated IDs
- Deployment portal with prescriptive guidance
 - See the link in the student manual

Continuing the deployment path builds on the previous steps already performed in the Pilot phase, so there is no requirement to restart the effort from scratch. The organization also has the ability to extend and deliver new capabilities to users as their needs change.

There are multiple data migration methods available, including user self-service and IT-driven approaches.

The organization can be provided with the following user identity models to suit their needs:

- Cloud identities
- Synchronized identities (with optional password synchronization)
- Federated identities

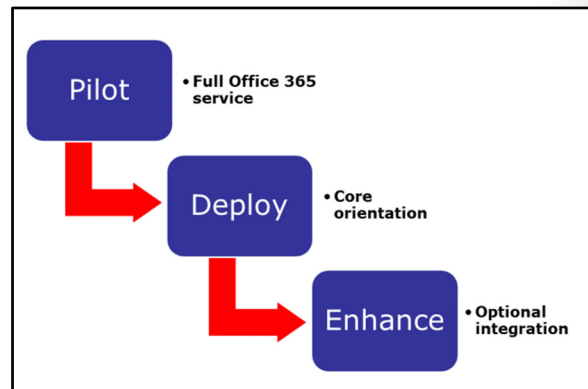
Finally, there is an Office 365 Deployment Portal with prescriptive step-by-step guidance and video instructions for the FastTrack process.

 **See the Office 365 Deployment Portal for prescriptive guidance on deploying Office 365:**

<http://go.microsoft.com/fwlink/?LinkId=306546>

The FastTrack Phases

The three-phase FastTrack process provides a structured approach to implementing Office 365. This table breaks down the phases, identifying the function, timeframe, scale, and activities within each phase.



	Pilot	Deploy	Enhance
Function	Full Office 365 Service	Core enrolment	Optional integration
Timeframe	Hours	Days	Weeks
Scale	Persist to deployment	Company-wide cloud use	Meet additional business needs
Lead by	Users	IT department	Customized
What	Office 365 services: Exchange SharePoint	All Pilot phase features, plus: Shared namespace Simple co-existence	All Deploy phase features, plus: SSO

	Pilot	Deploy	Enhance
	Lync Office Web Apps Office 365 ProPlus Mobile	External sites	Hybrid options Features as required
How	Service domain Cloud identity Web client Office client Self-service	Pilot phase and: IT-led migration Customer domain DirSync Password Sync Admin migrations OnRamp	Deploy phase and: Federated identity Hybrid Exchange Hybrid SharePoint Hybrid Lync Corporate app store Third-party migration tools
Output	Pilot complete	Deploy complete	Extra features deployed

With the Pilot phase, the aim is to implement a full Office 365 service within hours, where the pilot users' data persists into production. The pilot users themselves are expected to get on and use the new environment without extensive support. Because the Pilot phase is very much user-driven, good selection procedures for the pilot users are essential.

Because this is a full pilot, users experience all the services in Office 365. However, there are some features that are not included at this point. In particular, the only directory option is for user identities to be stored in the cloud, and none of the hybrid configurations are possible. During the pilot, the domain name remains as an onmicrosoft.com domain. However, the pilot users have full connectivity to Exchange, SharePoint, and Lync, and they can download and install Office 365 ProPlus.

With the FastTrack approach, moving to the Deploy phase typically takes a few days rather than weeks or months. In this phase, the IT department moves the entire company to the cloud and implements some of the more advanced features, such as Directory Synchronization (DirSync), either with or without password synchronization. The IT department also registers a custom domain with Office 365, such as contoso.com instead of contoso.onmicrosoft.com. Exchange server can be integrated through simple co-existence and external SharePoint sites activated.

In the Enhance phase, the organization has a choice of advanced configuration options. However, they do not have to take on any of them. SSO and hybrid operation with on-premises Exchange, Lync, or SharePoint servers can all be implemented during this phase. However, the overall driving factor at this point is business need—the organization only needs to activate the features that they require. In consequence, it is possible to halt the deployment process before moving to the Enhance phase.

Office 365 and Microsoft Operations Framework

Microsoft Operations Framework (MOF) 4.0 is a metaframework that incorporates the best practices of the service management industry and numerous frameworks into one set of guidance. MOF provides actionable management guidance that enables organizations and service providers to plan, deliver, and operate IT services for organizations of all sizes.

MOF is a particularly appropriate framework to apply when implementing and operating Office 365, as it can also integrate well with the phases of the FastTrack deployment plan. MOF can help solve service delivery issues and enable organizations to meet the challenges of putting new changes into production or complying with quality standards, such as ISO 20000.

MOF provides guidance to IT organizations to help them create, operate, and support IT services while ensuring that the organization's investment in IT delivers the business value they expect at an acceptable level of risk.

MOF helps create an environment where a business and its IT department work together toward operational maturity. MOF is particularly appropriate to Office 365 because it promotes a logical approach to decision-making and communication and to the planning, deployment, and support of IT services.

 **MOF 4.0 is a complex subject and more information about this metaframework is available here:**

<http://go.microsoft.com/fwlink/?LinkId=390861>



Lesson 2

Provisioning Tenant Accounts

An important part of the Office 365 provisioning process is the creation of the tenant account. This activity was not as crucial in the traditional Office 365 deployment methodology because the pilot account typically was not transitioned into deployment. With the FastTrack process, where the pilot account typically persists into the production environment, it is vital that you enter the right information, as certain values that you specify cannot be changed later.

Lesson Objectives

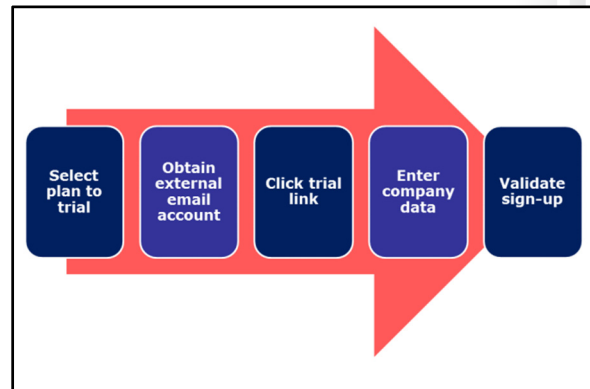
After completing this lesson, you should be able to:

- Describe the process for creating a new tenant account.
- List the information that you need to provide to set up that account.
- List obstacles that can prevent tenant account provisioning from occurring correctly.
- Describe typical tenant account provisioning errors.
- Check that the Office 365 services have been correctly provisioned and are functioning.
- Provide best practices for provisioning tenant accounts.

Process for Creating a Tenant Account

The overall process for creating a tenant account for Office 365 is extremely simple:

1. Decide on which Office 365 plan you want to trial.
2. Ensure you have a valid email account (organizational or Live ID will work fine).
3. Click the trial link on the Office 365 website.
4. Enter the correct information for your organization.
5. Complete the sign-in process by validating the text message or phone call.



Trial accounts are available for the following Office 365 plans:

- Small Business Premium
- Midsize Business
- Enterprise (E3)
- Education
- Government

As mentioned previously, errors in the sign-up process commonly result from organizations selecting the wrong Office 365 subscription for the size of their business. It is currently not possible to change to different product families, such as from the Small Business plan to the Enterprise plan.



Note: The process for provisioning Government and Educational plans is different and is not covered here. This course assumes you are selecting the Enterprise E3 subscription and using the FastTrack process for deployment.

During the trial sign-up, you have to supply a valid email address that already exists. Although the sign-up process creates an email address in the form username@organizationname.onmicrosoft.com, you cannot use that as the email address for the sign-up process.

If you are working for or through a Microsoft partner and you need more than 25 pilot users for an Enterprise E3 trial, then you can apply for an extended trial account. When you request an extended trial tenant to support the FastTrack Pilot, you must submit a form to fasttrackpilot@microsoft.com that provides customer information, partner information, and information about the pilot engagement. After two business days, you should receive a unique provisioning code. This is a single-use code that can only be used to provision the pilot tenant for the organization.


Tenant Account Information

When signing up for a new tenant account, you need to supply information about the person and the company. Note that the fields that you see will be different, depending on the country you select at the beginning. For example, Switzerland includes a Canton field.

Field	Value	Reqd	Change	Type
Country/Region	Name	Yes	No	Drop-down list
First/Last names	Tenant admin	Yes	Yes	Text field, 50 char limit
Email	Tenant admin email	Yes	Yes	Text field
Address 1	Tenant address	Yes	Yes	Text
Address 2	info	No	Yes	
Address 3		No	Yes	
City	Company City	Yes	Yes	Text
State/County	Company state	Yes	Yes	Drop-down or text
Zip/Postal code	Company Zip	Yes	Yes	Text
Phone	Contact phone	Yes	Yes	Text
Organization name	Name of the tenant company	Yes	Yes	Text

Field	Value	Required	Can be changed	Type
Country/Region	Name	Yes	No	Drop-down list
First/Last names	Tenant admin name	Yes	Yes	Text field, 50 char limit
Email	Tenant admin email	Yes	Yes	Text field
Address 1, Address 2, Address 3	Tenant address information	Yes No No	Yes Yes Yes	Text
City	Company City	Yes	Yes	Text
State/County	Company state	Yes	Yes	Drop-down or text

Field	Value	Required	Can be changed	Type
Zip/Postal code	Company Zip	Yes	Yes	Text
Phone	Contact phone	Yes	Yes	Text
Organization name	Name of the tenant company	Yes	Yes	Text

 **Note:** The Tenant administrator's name must be a real name, not "System Administrator". It is also important that the email address used does not become inaccessible when the person registering the account leaves the company.

When you enter this information, Office 365 will generate a default domain name based on the company name you supply; the default domain name will end with **.onmicrosoft.com**. Again, this value cannot be changed after creation, so it is vital that you check that this name is acceptable. If the name already exists, then a number will be added to make the name unique, such as **lucernepublishing426.onmicrosoft.com**.

You are then asked to enter a password and indicate a mechanism for validating the sign-up. Passwords should be at least 10 characters long and contain a random mixture of upper case and lower case letters, numbers, and special characters.

To validate the sign-up, you can select from either having a text message sent to you or receiving a phone call. You should specify the country and number for your phone. If using the text option, ensure that the phone number is capable of receiving texts.

Once you click **Create My Account** the confirmatory six-digit number will either be sent to your phone or you will be called, depending on your prior selection. Enter that number into the confirmation dialog box and your tenant account is set up.

Obstacles to Tenant Account Provisioning

In addition to avoiding errors when signing up for a new tenant account, you must be aware of the following obstacles to signing up to Office 365 and what you need to do to fix them.

Issue	Remedy
Tenant name unavailable	Check that there is not an existing trial account for the organization or use another name
Offensive or restricted name with Government accounts	Do not use an offensive or restricted name associated with another government department
Domain name unavailable	Another trial account is in existence – close the trial account
Provisioning time	SharePoint can take up to an hour to provision – allow in timescales

Issue	Remedy
The requested tenant name may be unavailable as it has already been taken	Check that there is not an existing trial account for the organization or use another name.
With Government accounts, name may be on the offensive or restricted list	Do not use an offensive or restricted name associated with another government department.
Domain name unavailable	Another trial account is in existence – close the trial account.
Provisioning time	SharePoint can take up to an hour to provision.

Tenant Account Provisioning Errors

When setting up a tenant account, there are some potential errors that you must avoid, as mistakes here have the potential to cause the pilot or the Office 365 deployment to fail. These errors include:

- Selecting the wrong tenant type.* Although there is now a wizard that enables you to change between Office 365 plans, signing up for the wrong tenant type can have unexpected results when you try to configure options such as multiple domains, directory synchronization, and Information Rights Management (IRM).
- Specifying the global administrator name.* The global administrator (that is the person who first signs up) must have a real first and last name. You cannot use a name such as "System Administrator".
- Confirming who signed up for the trial.* It can be problematic if you have an unknown person sign up for the original trial who then leaves, and you subsequently cannot access their email.
- Selecting the tenant name.* If you incorrectly select the tenant name, you cannot change it later.

• Wrong tenant type (most common failure)
• Global Administrator name
• Identity of person signing up
• Correct tenant name
• Global Administrator password
• Global Administrator email address

- *Recovering the global administrator password.* The signup information must be entered correctly to be able to recover the password.
- *Managing the global administrator email address.* It is important not to lose the email address assigned to the tenant for global administrator password recovery.

 **For more information on the difference between the Office 365 versions, go to the Office 365 website for your country and follow the links to the Office 365 plans.**

<http://go.microsoft.com/fwlink/?LinkId=390863>

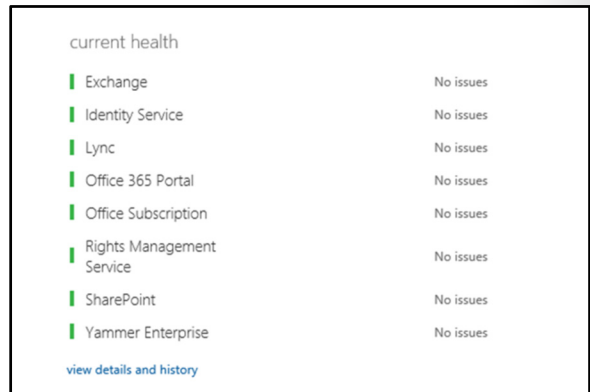
 **For information on changing Office 365 plans, see the following link:**

<http://go.microsoft.com/fwlink/?LinkId=401127>

Services Provisioning Status


After you have signed up for the Office 365 tenant account, you can then log on and view the services provisioning process. Note that this process can take up to an hour for the SharePoint services to come online.

To find out the current status of your Office Services, log on to Office 365 with your administrator credentials, and in the Office 365 Admin Center page, you can see the current status of your services.



current health	
Exchange	No issues
Identity Service	No issues
Lync	No issues
Office 365 Portal	No issues
Office Subscription	No issues
Rights Management Service	No issues
SharePoint	No issues
Yammer Enterprise	No issues
view details and history	

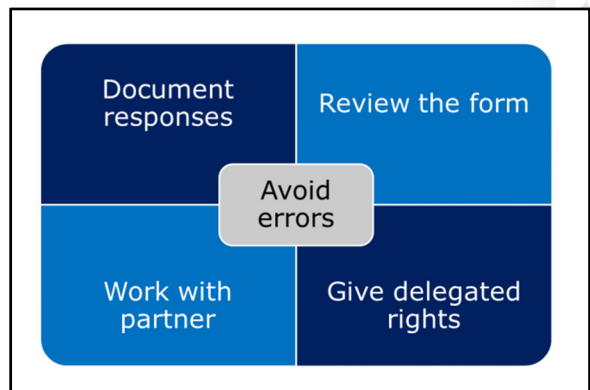
For more information on the services, click the **view details and history** link, which takes you to the page where you can see a breakdown by service type of all the services for the last seven days. There is an additional link to show the past 30 days.

 **Note:** The link to the RSS feed takes you to the Office 365 Service Health RSS Notifications page.

Guidelines for Tenant Account Provisioning

To ensure that you set up your tenant account correctly, it is recommended that you perform the following best practices:

- Document everything as you do it. Print off the sign-up forms when you have filled them in, even if you only print them to file.
- Get additional people to review the form before submitting it. Ideally, find exacting people who are good at spotting errors.
- Work with your Microsoft partner or cloud



service partner to complete the signup forms.

- Select a managing partner and give them delegated administrator rights after setup.
- Avoid the errors in this lesson!

You should now be able to proceed to checking for client connectivity.

Lesson 3

Planning a Pilot

In this lesson, you review the overall factors that can affect an Office 365 deployment. However, it is important to realize that these are not necessarily complete deployment blockers, merely factors about which you need to be aware. This is the strength of the FastTrack process—your customers can take it as far as they want and can reach a deployment position where they realize value from the Office 365 platform without affecting their existing infrastructure or compromising on the benefits of the cloud-based service.


Lesson Objectives

After completing this lesson, you should be able to:

- Analyze the organization and scope the project.
- Identify any scalability limits with Office 365.
- List the activities within the Pilot phase of the FastTrack approach.
- Select pilot users.
- Identify the outcomes from the pilot.
- Describe the activities that need to happen after the pilot completes.
- List resources to help with the FastTrack deployment.

Initial Customer Analysis

The first task before starting the pilot is an initial analysis of the environment as part of the qualification process. The analysis does not need to be in great depth at this point. You may also find that much of this information is already available and documented within the organization.

 **This analysis is part of the Office FastTrack three-day offering. For more information, see the following link:**

<http://go.microsoft.com/fwlink/?LinkId=321169>

- Industry sector
- Number and type of users
- Geographic spread and working patterns
- Device types and operating systems
- IT department size, location, and management style
- Workloads and migration requirements
- Management attitude to cloud services

With any pilot of Office 365, it is important to identify the industry sector the organization is in, because this information will provide insight into the method of working and anticipated behavior. For example, IT companies tend to be more dynamic and prepared to try new technologies, whereas those working in the oil and gas industry are extremely safety conscious.

Following the industry sector, you should then identify the number and types of IT users. User types typically fall into two main categories:

- *Information workers.* Users who work at desks or on the move and primarily create or process data.

- *Kiosk workers.* Users who do not need regular access to a computer or mobile device to carry out their tasks.

You also need to know how those users are distributed. Are they in a few large offices, such as an insurance company, or in many small ones, such as a car dealership? Do they work at home, either occasionally or permanently, and do they need to access data on the move?

What devices do their users have? Does the organization have a BYOD policy in place or are there local impromptu arrangements?

How does the company currently deliver IT? Do they have a centralized department or a distributed arrangement? Is the IT in-house or outsourced? How are IT services viewed, and how is the department managed?

What compliance and data retention requirements does the company need to consider? Some organizations have strict compliance regulations in respect to data management, storage, recording, and transmission.

What are the company's security requirements? Are they likely to be targeted and what level of protection should they adopt?

What workloads does the company have that do not need to be migrated to Office 365? Look at areas such as custom applications, business information systems, and stock control environments and consider whether these applications will remain on premise.

Finally, what is likely to be the attitude within the company to moving to the cloud? Being aware of this attitude and having a strategy and tactics to deal with it is essential for a smooth deployment.

At this point, the information does not have to be particularly accurate. For example, rounding user numbers to the nearest thousand or hundred are fine. If there is already an established relationship with the organization or you already work within the company, much of this information should already be available.

Scalability Limits

Although Office 365 can provide an excellent service for the majority of organizations, there are some scalability limits and potential conflicts of which you need to be aware. Some of these limits may complicate the FastTrack migration process, and some of these limitations are currently not addressed in Office 365. However, there are plenty of mitigating approaches available to address these issues.



Note: This course assumes that organizations will be migrating to the Enterprise E3 plan. Therefore, inherent scalability limits with the mid-sized and small business versions of Office 365 are not discussed.

	Hybrid configuration supports single Exchange Organization only; Limits on bulk email
	File upload limit – 2 GB; Over 500,000 users – contact Microsoft Support; No full-trust code
	DirSync with over 300,000 users – contact Microsoft Support; Caution with third-party directory services

Exchange Online

Exchange Online in a hybrid environment is only supported with single Exchange organizations. There are mitigating approaches to this and other issues that are covered in the Enhance phase of this course.

SharePoint Online

You should contact Microsoft Support if you are migrating an organization with more than 500,000 users. SharePoint Online does not support full-trust code, but it can be configured in a hybrid arrangement with on-premises SharePoint implementations using SSO.

Microsoft Azure Active Directory

If the organization has more than 300,000 objects in Active Directory (previously 50,000) and you are planning to use directory synchronization, contact Microsoft Support. If the organization is not using Active Directory Directory Services, additional configuration may be required.

Pilot Activities

The Pilot phase consists of the following activities that must be performed in consecutive order:

1. *Checking prerequisites.* Make sure you have assessed the organization's environment correctly for the pilot.
2. *Setting up pilot domains.* Determine the domain policy and identify customer domains for the pilot.
3. *Adding users.* Select users to be part of the pilot.
4. *Connecting existing email accounts.* Determine the available options for connecting to the existing email system.
5. *Setting up collaboration sites.* Establish use and requirements for SharePoint sites.
6. *Preparing pilot users.* Plan communications with pilot users.
7. *Testing the pilot.* Identify success factors for testing the pilot.
8. *Running the pilot.* Record the results of planning decisions.
9. *Completing the pilot.* Feed the results into Deploy phase planning.

For each of these activities, there are planning activities that you need to perform.

1. Checking prerequisites
2. Setting up pilot domains
3. Adding users
4. Connecting existing email accounts
5. Setting up collaboration sites
6. Preparing pilot users
7. Testing the pilot
8. Running the pilot
9. Completing the pilot

Pilot User Planning

The process of selecting and involving pilot users into the Office 365 FastTrack Pilot is vitally important and has the potential to make or break the pilot process. Therefore, it is essential to select the right people with a balanced mix of interests, abilities, and attitudes to help ensure the FastTrack Pilot is successful.

- *Determine the number of pilot users.* The first planning decision is to define the number of users to be part of the pilot. As a rule of thumb, you should consider a pilot that employs at least five percent of the Information Worker user base, spread evenly throughout the departments. Any less than this figure indicates poor preparation and buy-in from your organization.
- *Plan for pre-pilot users.* With larger organizations, it may be necessary to deploy some pre-pilot users. With these larger pilot engagements, it can be useful to initially roll out Office 365 to a small subset of users, to help identify issues, before including a wider user community.
- *Select the pilot users.* Pilot users typically meet the following criteria:
 - Full-time employees for more than six months.
 - Trained information workers.
 - Representative of the overall function of the company.
 - A mix of age, experience, and seniority within the department they work for.
 - Prepared to provide feedback on the pilot.
- *Create and implement a Pilot user communication plan.* Effective communications with the pilot users are vital and need to start up to three weeks before the pilot itself.
- *Train and support the pilot users.* Microsoft does not support Office 365 pilot users, so planning user and helpdesk training and support for the Pilot phase is an important part of the experience.

Select pilot users who are:

- Full-time employees
- Trained information workers
- Representative of the overall function of the company
- A mix of age, experience, and seniority within the department they work for
- Prepared to provide feedback on the pilot

Pilot Outcomes

Successful outcomes from the pilot phase are as follows:

- Provision the Office 365 service.
- Create the initial users in the service.
- Enable active use of mail by pilot users.
- Deploy Office 365 ProPlus to pilot users (if required).
- Enable user evaluation of Office 365 services.
- Validate the service integration into the organization landscape.

- Provision the Office 365 service
- Create the initial users in the service
- Enable active use of email by pilot users
- Deploy Office 365 ProPlus to pilot users (if required)
- Enable user evaluation of Office 365 services
- Validate the service integration into the customer landscape
- Establish an Office 365 environment that can move to production

- Establish an Office 365 environment that can move to production.

This information needs to be recorded in real time during the pilot; otherwise, important details will be missed and may not be recordable after the fact. This recorded information from the pilot is used for checking planning decisions against actual outcomes, and it feeds into the Deploy phase.

Post-Pilot Activities

When the Pilot phase completes, the organization will receive a list of next steps and recommendations that they must complete. The next steps include extending the pilot, planning for the Office 365 service, and planning the organization's environment.

Extend the pilot

After the pilot engagement is complete, the organization is well positioned to gain more value from this effort and has the option to continue extending the pilot to prepare further for future changes. The organization has the following options:

- Extending the pilot
 - Continue user pilot
 - Expand the scope
- Planning for the Office 365 Service
 - Service options
 - Identity planning
 - Mail migration planning
- Planning the customer's environment
 - Raise awareness
 - Plan for transition
- Ending the pilot
 - Returning the environment back to its original state
 - Identifying the reasons for non-conversion

- *Continue user pilot.* The most basic option is simply for the organization to continue with what is in place. Users would continue to use Office 365 on a regular basis. The organization can collect user feedback about Office 365 in their organization and highlight the key benefits. This information also enables the organization to plan future deployments appropriately for each workload. Importantly, the pilot provides data points to best plan the organization's migration and identity needs.
- *Expand the scope.* The trial tenant used for the pilot service allows up to 250 users, so the organization could add more pilot users to prove the service fit for various groups within the organization. Note that users who are moved to the service during the pilot can be transitioned to production after a decision for service use is reached.

Plan for the Office 365 service

The pilot provides the organization with their first look at the Office 365 service. They can take actions now to begin planning how the service will best fit the needs of their company. The following options should be considered:

- *Service options.* The pilot has enabled users to begin using a broad range of Office 365 features. The service provides solutions for mail, collaboration, sharing, and other scenarios. The scope of this pilot has been confined to the core service options; therefore, the organization should determine what additional scenarios are candidates for use in their organization.
- *Identity planning.* The pilot introduced the organization to the concept of identity management in the Office 365 service. The pilot engagement provisions users in the service through cloud identities. The trial tenant shows how this identity management approach works for administrators and users. However, the organization also needs to start thinking about identity management. This planning should consider future plans for additional service scenarios and integration desires for streamlined management. Further planning considerations should determine the future implementation plans for identity management and authentication. The cloud identity approach used in the pilot engagement uses a stand-alone set of credentials for users. Guided by the consultant, the organization should map a plan for the desired authentication plans including plans for single sign-in options.

- *Mail migration planning.* In the pilot, the organization has experienced mail using the Office 365 **connected accounts** feature. This feature enables users to gain access to existing mail items and continue to send and receive mail with their existing email addresses. However, users will expect to bring existing mail, calendar, and contacts to the new service. Office 365 provides a range of migration options to help manage this migration. If customers begin planning now to reduce the content users currently have in place, this migration process is considerably simplified.

Plan the organization's environment

The pilot engagement enabled the Office 365 service and implemented the related components in the organization's environment. Assuming the results of the trial are acceptable, the organization can then perform the following post-pilot activities:

- *Raise awareness.* The Summary Results provided at the end of the pilot assists the organization to share the results to the company leadership and partner teams. They can use these results to help develop and track action on the recommended next steps.
- *Plan for transition.* The pilot uses an Office 365 trial tenant that needs to be transitioned to a live account before the trial expires.

End the pilot

If the organization does not want to move from the pilot to the Deployment phase, then it is necessary to return the environment to how it was before the start of the pilot, and identify the reasons why the pilot was not successful. The organization should always feel that it is possible to return to Office 365 at a later date.

Pilot Planning Resources

The following resources will assist you to get started with the Office 365 FastTrack process:

- **Office 365 FastTrack Deployment Center**



• **Use this site to get the organization facing deployment content. The most updated content is available here:**

<http://go.microsoft.com/fwlink/?LinkId=306546>

- * Office 365 FastTrack Deployment Center
- * Office Ignite Readiness
- * TechNet Center for Office 365
- * TechNet Center for the new Office
- * Office IT Pro Blog
- * Office 365 Trust Center
- * Office 365 Service Descriptions
- * Service Updates for Office 365 for Enterprises
- * Microsoft Planning Services

- **Office Ignite Readiness**



Access to Office technical readiness content, events, and resources.

<http://go.microsoft.com/fwlink/?LinkId=321170>


- **TechNet Center for Office 365**



Get the info IT pros need to deploy, integrate, and manage Office 365 services for enterprises or large organizations.

<http://go.microsoft.com/fwlink/?LinkId=390742>

- **TechNet Center for the new Office**

 **Get the IT pro resources you need to try the new Office (Office 2013 and Office 365 ProPlus), including details about activation, compatibility, and deployment.**

<http://go.microsoft.com/fwlink/?LinkId=321171>

- **Office IT Pro Blog**

 **Provides frequent topics about Office deployment and compatibility issues. Includes articles about Office Telemetry.**

<http://go.microsoft.com/fwlink/?LinkId=195811>

- **Office 365 Trust Center**

 **Information about protecting the privacy and security of customer data.**

<http://go.microsoft.com/fwlink/?LinkId=321172>

- **Office 365 Service Descriptions**

 **The service descriptions provide detailed accounts of the services and features that are available with Office 365.**

<http://go.microsoft.com/fwlink/?LinkId=285516>

- **Service Updates for Office 365 for Enterprises**

 **Here you will find information about the latest features and improvements to Office 365.**

<http://go.microsoft.com/fwlink/?LinkId=195811>

- **Microsoft Planning Services**

 **Planning service site for partners. Learn about engagement options.**

<http://go.microsoft.com/fwlink/?LinkId=321173>

Lesson 4

Enabling Client Connectivity

This final lesson examines the process of checking for connectivity from the client to the Office 365 service. Office 365 provides a number of tools and techniques that you can use to do this, and you can also use general network troubleshooting tools, such as Network Monitor. This lesson concentrates on a subset of those tools and on the general principles that you must address, such as firewall configuration.

Lesson Objectives

After completing this lesson, you should be able to:

- List issues that can prevent clients from connecting to Office 365.
- Describe the requirements for ports, caching, and IPv6 networking to support Office 365.
- Run the Office 365 Best Practices Analyzer to diagnose connectivity issues to Office 365.
- Run the Office 365 OnRamp Tool.
- List other factors that can affect client and network connectivity.

Client Access Blocking Issues

The simplest statement of suitability to connect to Office 365 is that a client computer must be able to make unauthenticated connections to the Internet over ports 80 (HTTP) and 443 (HTTPS). In particular, they must be able to connect to **https://login.microsoftonline.com**.

In consequence, users should simply be able to connect directly to the Office 365 service. Certainly this is the situation when connecting from most domestic Internet connections, where the default rule on the router is to allow all outgoing requests on any port. However, in enterprise environments, routers, switches, firewalls and proxy servers may all conspire to prevent access to one or more Office 365 services.

- No routing to the Internet
- No gateway address
- Gateway address incorrect
- No Internet connection
- Routing errors
- Host firewalls
- Ports blocked
- Authentication
- Latency

The following list is not exhaustive but covers the main reasons why users cannot access Office 365:

Issue	Factor	Remediation
No routing to the Internet	Client using non-routable address, such as 169.254.0.0/16.	Change to either static or dynamically assigned routable address.
No gateway address	Without a default gateway address, clients cannot route packets that are not for the client's subnet.	Add default gateway address and check that default gateway is accessible.
Gateway address incorrect	Default gateway is on a different subnet.	Change gateway address to one on the local subnet.

Issue	Factor	Remediation
No Internet connection	Client has fully routed IP network but no connection to the Internet.	Install Internet connection.
Routing errors	Route to the Internet is not configured correctly.	Reboot and/or reconfigure routers. Check routing tables.
Host firewalls	Host firewalls are blocking outgoing connections.	Configure host firewalls to allow programs or ports using group policy.
Ports blocked	The required ports on the external-facing firewalls are not open for outgoing requests on the required ports.	Open required ports for connection to Office 365 services.
Authentication	Proxy servers require authentication.	Change to unauthenticated access.
Latency	Latency (round-trip time) is too high and breaks encryption.	Can happen with satellite Internet connections. Change to another type of Internet connection or a better Internet Service Provider.

Port, Caching, and IPv6 Requirements

In addition to client connection requirements, the Office 365 service may need further ports to be opened. These ports are as shown in the following table.

- Ports and protocols
 - Ensure correct ports are open
 - Check for network traffic
- Third-party caching and filtering rules
 - Office 365 uses third-party caching for non-SSL traffic
 - IP-based filtering on these caches is not possible or supported
 - Check access to *r3.res.outlook.com for non-SSL traffic
- IPv6-capable devices
 - Check for end-to-end IPv6 support
 - Check for hardware emulation at the perimeter

Protocol	Port	Usage
TCP	443	Office 365 portal (admin and user), Outlook, OWA, SharePoint Online, Lync client, ADFS federation and proxy
TCP	25	Mail routing
TCP	587	SMTP relay
TCP	143/993	IMAP Simple Migration Tool

MCIT USE ONLY. STUDENT USE PROHIBITED

Protocol	Port	Usage
TCP	80/443	Microsoft Azure Active Directory Sync tool, mail migration tools, Exchange Management Console, Exchange Management Shell
TCP	995	POP3(S)
PSOM/TLS	443	Lync Online – outbound data sharing
STUN/TCP	443	Lync Online (outbound audio, video, and application sharing sessions)
STUN/UDP	3478	Lync Online (outbound audio and video sessions)
TCP	5223	Lync mobile client push notifications
UDP	20000-45000	Lync-to-phone outbound
RTC/UDP	50000-59000	Lync (outbound audio and video sessions)



This list of ports is available at the following location:

<http://go.microsoft.com/fwlink/?LinkId=401128>


Third-party caching and filtering rules

Office 365 improves performance and reduces response times by relying on third-party, content-caching engines. These third-party devices cache non-SSL resources, such as the downloaded images that create the Outlook Web App user interface.

Microsoft Office 365 relies on third-party content caching engines to achieve good performance and response times. The types of content cached with these third parties are non-SSL resources, such as the images downloaded to draw the Outlook Web App user interface. As stated above, it's possible and supported to use IP-based filtering for the SSL content downloaded from Office 365 and for the Office 365 endpoints that make in-bound calls to an on-premises environment. However, it isn't possible or supported to use IP-based filtering for the non-SSL resources hosted on third-party content caching engines. To express filtering rules that allow those non-SSL resources to be downloaded to clients on your intranet, you need to use hostname-based filtering (as opposed to IP-based filtering). This is because the IPs used by the third-party content caching engines change frequently in a manner which makes it impractical to track each individual IP change. Allow the following hostnames for these non-SSL resources:

- r3.res.outlook.com
- r4.res.outlook.com
- prod.msocdn.com

Using IP-based filtering for the non-SSL resources that are hosted on third-party, content-caching engines are neither possible nor supported. To express filtering rules that allow these non-SSL resources to be downloaded to clients on your intranet, you need to use host-name-based filtering (as opposed to IP-based filtering). The IP addresses that are used by the third-party, content-caching engines change frequently, making it impractical to track each individual IP change. To accommodate this, you should check whether you have access from the network to * r3.res.outlook.com for these non-SSL resources.

 If you must use IP-based filtering, see the Help topic “Office 365 URLs and IP address ranges” shown here:

<http://go.microsoft.com/fwlink/p/?LinkID=243567>

IPv6-capable devices

If the organization is connecting to Office 365 with IPv6-capable network equipment, you must ensure the following:

- The network equipment can support IPv4 and IPv6.
- The perimeter emulates any hardware solution that has been configured to allow IPv6 clients to connect to the Exchange Online services.

For example, if the organization uses a web proxy, it must be configured as an IPv6-capable web proxy.

Office 365 Best Practices Analyzer

There are a number of tools that you can use for diagnosing client connectivity, but the most suitable is the Office 365 Best Practices Analyzer, which is available from the tools menu in the Office 365 admin center.

The requirements for this tool are as follows:

- Windows 7 with Service Pack 1 or later, 64-bit version
- Internet Explorer 9.0 or later
- Screen resolution: 1024 x 768 minimum

When you run a new scan with the tool, you are presented with the following screen under **View details**:

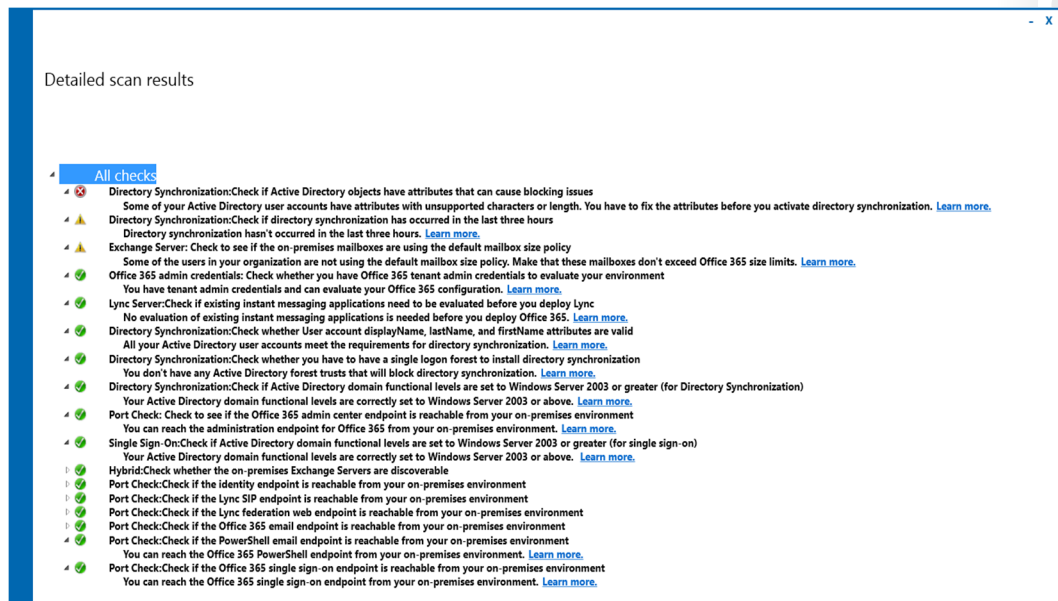
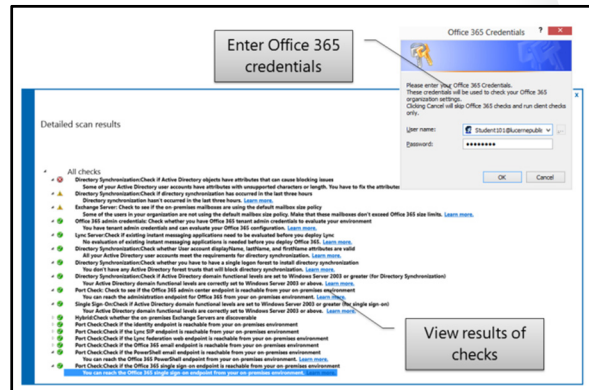


FIGURE 1.1: RESULTS OF THE OFFICE 365 BEST PRACTICES TOOL

MCT USE ONLY. STRICTLY UNAUTHORIZED

This information then enables you to identify what issues might cause the client connection to Office 365 to fail.

Office 365 OnRamp Tool

OnRamp for Office 365 is an automated assistance tool that helps you gather configuration requirements and perform deployment readiness checks against your on-premises environment. It can also speed up your deployment process and help identify blocking issues, particularly:

- Before deploying Office 365, especially for organizations with requirements such as identity federation or hybrid deployment.
- When you are adding new features or complexity, or before proceeding to the next phase of a phased deployment approach.
- When you are testing client connectivity.



In consequence, you may end up running Office 365 at a number of points during the deployment process.

You can start the OnRamp tool either by going to **onramp.office365.com**, or from the tools menu in the Office 365 admin console, which takes you to the same address.

Options that you select in the OnRamp tool include:

- *Feature selection* – which features in Office 365 you are going to deploy.
- *User management* – how you plan to manage user accounts.
- *Email migration* – what option you want to migrate your user's email accounts.
- *Readiness* – reviews your on-premises environment for connecting to Office 365.
- *Automatic checks* – uses an add-in to confirm that your environment is ready.
- *Feature review* – assist with aligning your deployment goals with Office 365 capabilities.

What you end up with is a report that details the features you are going to install and a readiness checklist.

OnRamp for Office 365 Report

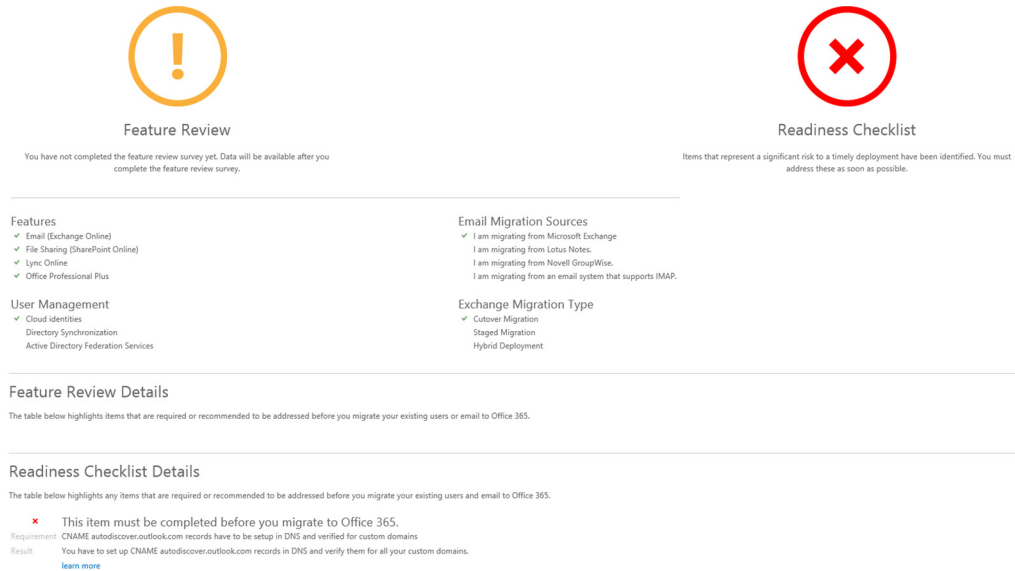


Figure 1.2: OnRamp for Office 365 Report

Network Connectivity Factors

Not surprisingly, using Office 365 service offerings will increase Internet traffic, so it is important for you to evaluate and assess the network impact of the services. Directory synchronization and email traffic in Exchange hybrid deployments have the greatest effect on bandwidth, but organizations should notice a general increase in Internet traffic after migrating users to the Office 365 suite.

When looking at deploying Office 365, you must consider the effect on bandwidth of the following items:

- The Office 365 service offerings to which the organization has subscribed.
- The number of client computers in use at one time.
- The type of task each client computer is performing.
- The performance of the Internet browser software in use.
- The capacity of the network connections and network segments associated with each client computer.
- The organization’s network topology and the capacity of the network hardware.
- Number of simultaneous mailbox migrations.
- Office 365 ProPlus installation and desktop setup.

- Subscribed Office 365 services
- Simultaneous client computer numbers
- Client computer tasks
- Internet browser performance
- Network segment and connection capacity
- Network topology and hardware capacity
- Number of simultaneous mailbox migrations
- Office 365 ProPlus installation and desktop setup
- Network Address Translation limitations

MCT USE ONLY. STUDENT USE PROHIBITED

- Network Address Translation (NAT) limitations.

Testing and validating your Internet bandwidth (download, upload, and latency constraints) are vital to achieving satisfactory experiences for users. It also affects the speed of migration of on-premises mailbox content to Exchange Online. Slow or latent connectivity reduces the number of mailbox migrations that can be completed during a migration window. Later modules will cover this consideration.

Office 365 ProPlus installation is another major user of bandwidth, although the sizing factors here are the same as for any other large application install.

The following tools can help with the process of estimating network bandwidth:



Reference Links: Exchange Client Network Bandwidth Calculator, at <http://go.microsoft.com/fwlink/?LinkId=401130>

Lync 2010 and 2013 Bandwidth Calculator, at <http://go.microsoft.com/fwlink/?LinkId=401131>

NAT limitations

Network address translation (NAT) limitations must be considered. Most users on corporate networks access the Internet through a private (RFC1918) IP address space. Organizations then use gateway technologies such as firewalls and proxies that provide NAT or port address translation (PAT) services to translate from the internal private address space to an external IP address or address range. Each outbound connection from an internal device translates to a different source TCP port on the public IP address. Therefore, thousands of users on a corporate network can “share” a few publicly routable IP addresses.

Just one Outlook client can potentially consume eight or more connections. Because there are a maximum of 64,000 ports available on a Windows-based NAT device, there would typically be a maximum of 8,000 users behind an IP address before the ports are exhausted. If customers are using NAT devices that are not running a Windows operating system, the total available ports could be less than 64,000.

To determine the maximum number of devices behind a single public IP address, monitor the network traffic to determine peak port consumption per client. Also, set a peak factor for the port usage (minimum four). You can then use the following formula to calculate the number of supported devices per IP address:

Maximum supported devices behind a single public IP address = (64,000 – restricted ports)/(Peak port consumption + peak factor).

For instance, if 4,000 ports were restricted for use by Windows and six ports were needed per device with a peak factor of four:

Maximum supported devices behind a single public IP address = (64,000 – 4,000)/(6 + 4) = 6,000.

To support more than 2,000 devices behind a single public IP address, follow these calculations to assess the maximum number of devices that can be supported:

Monitor network traffic to determine peak port consumption per client. This data should be collected from multiple locations, from multiple devices, and at multiple times. Then use the preceding formula to calculate the maximum users per IP address that can be supported in their environment.

Lab B: Preparing for Office 365

Scenario

The labs in this course involve Lucerne Publishing, a global media corporation based in Geneva, Switzerland. Lucerne Publishing currently uses a dedicated data center to run its on-premises environment but is looking to move to Office 365 over the next three months. Remi Desforges, the long-serving Chief Information Officer (CIO), has been instructed to ensure the migration project goes smoothly. He has appointed Justin Muller, the Chief Technology Officer, to head up the team. Justin has engaged Alain Richer as the partner Office 365 implementation consultant.

Objectives

By the end of this lab, you should be able to:

- Plan for a FastTrack Pilot of Office 365.
- Provision tenant accounts in Office 365.
- Set up a management computer.
- Check client connectivity to Office 365.

Lab Setup

Estimated Time: 75 minutes

Virtual machine: 20346C-LUC-CL1

Username: **Student1**

Password: **Pa\$\$w0rd**

This lab is partly a paper-based planning lab and partly hands-on. You should check your answers against the lab instruction to ensure that you have the right answers for a particular section before moving onto the next one.

Where you see references in the steps to **lucernepublishingXXXX.onmicrosoft.com**, you should replace **XXXX** with the unique Lucerne Publishing code that you assigned when you set up your Office 365 accounts in Module 1, Lab 1B, Exercise 2, Task 3, Step 5.

Exercise 1: Planning a FastTrack Pilot

Scenario

Alain Richer needs to create a plan for the FastTrack pilot at Lucerne Publishing; therefore, he needs to ask Justin and his team some questions. He sets up a meeting with Justin Muller, Heidi Leitner (the Network Manager), and Coralie Emond from the IT Department. Heidi has been assigned the task of working with Alain to set up the company account on Office 365, and Coralie will be involved in the day-to-day administration.

The main tasks for this exercise are as follows:

1. Extracting Customer Information
2. Extracting Customer Information - Answers
3. Identifying Activities within the FastTrack Pilot
4. Identifying Activities within the FastTrack Pilot – Answers

► **Task 1: Extracting Customer Information**

1. You are Alain. What discussion headings should you bring to this meeting to ensure you extract the information that you need from Lucerne Publishing to start planning the FastTrack Pilot?
2. When you have listed your questions, go to the next Task for the answers.

► **Task 2: Extracting Customer Information - Answers**

This task provides the answers to the question from the prior task.

1. The headings that Alain would use are as follows.
 - a. **Services** – what Office 365 services do you want to Pilot?
 - b. **Users** – what do they do and where do they work?
 - c. **Devices** – what devices do users have and is there a bring-your-own-device policy in place?
 - d. **IT delivery** – how does the company currently deliver IT and how is this service viewed and managed?
 - e. **Workloads** – what workloads does the company have that can't be migrated to Office 365?
 - f. **Pilot users** – how many do there need to be and in which departments?
 - g. **Management support** – what is the attitude to the cloud within the company and do we have executive support?
 - h. **Success Criteria** – how will you define success and how will you measure it?
 - i. **Feedback** – how are you going to capture feedback about the pilot?
2. The answers from the Lucerne Publishing team are set out below.
 - a. **Services** – what Office 365 services do you want to Pilot?
 - Everything except Project and Visio.
 - Definitely moving from Exchange Server on-premises to Exchange Online.
 - Keep in-house document management but evaluate SharePoint Online.
 - Very interested in Lync – don't currently have it.
 - Yes to OneDrive for Business.
 - Yes to Yammer.
 - b. **Users** – what do they do and where do they work?
 - Executive team of 50, spread all over the world, including the heads of the remote headquarters.
 - Below them are 255 management level personnel, who work either here at HQ or in the regional offices.
 - Around 1,600 employees, some at HQ, some in the regional offices, and a few working from home occasionally.
 - More than 2,500 freelancers who work from home, but they're not going to be part of this phase.
 - c. **Devices** – what devices do users have and is there a bring-your-own-device policy in place?
 - Senior Execs can use whatever they like.

- Some of them are on iPads, some on Android tablets, a few more on Windows RT devices and some with PCs.
 - Same BYOD policy for management, although they do tend to be more PC-based and more static in terms of their locations.
 - Employees are all provided with PCs, either workstations or laptops.
 - Associates use whatever they want as long as it is compatible with the company's file formats.
- d. **IT delivery** – how does the company currently deliver IT and how is this service viewed and managed?
- IT is very much a centralized function.
 - Main corporate data center here in Switzerland. The company doesn't actually say where it's physically located, but they do have very good network connectivity from HQ. The architecture is based on Microsoft's private cloud design, although they haven't fully virtualized all the workloads yet.
- e. **Workloads** – what workloads does the company have that can't be migrated to Office 365?
- The company has the following workloads that cannot be migrated at the moment:
 - Content management system (although that may migrate to SharePoint later) together with its SQL Server database.
 - The ERP system.
 - The HR system and database.
 - Everything else could potentially migrate to the cloud.
- f. **Pilot users** – how many do there need to be and in which departments?
- Five percent of users results in around 100 pilot users. These should be a representative sample from the departments, but not include mission-critical users such as Helpdesk staff.
- g. **Management support** – what is the attitude to the cloud within the company and do we have executive support?
- The CEO does not deal with that level of technical detail any more. However, the COO is keen to move the project forward.
- h. **Success Criteria** – how will you define success and how will you measure it?
- Success will come from the pilot users. If they like the experience of using Office 365 and let the company know, then the company will consider the pilot a success.
- i. **Feedback** - how are you going to capture feedback about the pilot?
- The company already has a web-based feedback system setup. This internally-designed system records and collates the information on the pilot.

► **Task 3: Identifying Activities within the FastTrack Pilot**

1. You are assembling the information into a FastTrack Pilot phase plan. Outline the activities that need to take place and highlight any factors that should be included in your planning.
2. When you have listed the activities in the Pilot phase, go to the next Task to review the answers.

► Task 4: Identifying Activities within the FastTrack Pilot – Answers

This task provides the answers to the question from the prior task.


1. A FastTrack Pilot should include the following activities:
 - a. Sign up for Office 365.
 - b. Set up the pilot domain for Lucerne Publishing (for example, lucernepublishing.onmicrosoft.com).
 - c. Add the pilot users.
 - d. Connect their existing email accounts.
 - e. Set up a team collaboration site for your pilot.
 - f. Prepare the pilot users.
 - g. Test the pilot configuration with the pre-pilot users.
 - h. Run the pilot.
2. Complete the pilot and prepare to move to the Deploy phase.

Results: Lucerne Publishing has signed off on the FastTrack Pilot and wants to test Office 365 in its environment. The company has been provided with a connectivity testing plan and a deployment timetable for the Office 365 implementation.

Exercise 2: Provisioning the Tenant Account

Scenario

The day before the pilot is due to start, Alain meets with Heidi to set up the organization's Office 365 account. He needs to ensure that they have the right information to set up the Pilot tenant account.

 **Note:** For simplicity, this lab uses an ordinary Office 365 trial account, not a FastTrack pilot extended tenant account. Also note that you need to create an account with a unique name in the form: **lucernepublishingXXXX.onmicrosoft.com**. You can use any alphanumeric value for XXXX that the Office 365 website accepts.

When you set up the tenant account for Lucerne Publishing, you will be allocated a **lucernepublishingXXXX.onmicrosoft.com** domain, where **XXXX** is a four character alphanumeric code that you assign.

Make note of this XXXX code as you will need it to complete the remaining labs in this course.

The main tasks for this exercise are as follows:

1. Gathering the Required Information
2. Gathering the Required Information - Answers
3. Creating the Tenant Account
4. Checking the Office 365 Service Status

► Task 1: Gathering the Required Information

1. You are Alain. List the fields that Heidi will need to complete when setting up the tenant administrator account in her name.

2. When you have listed the fields, go to the next Task to see the information that Heidi has provided for each field.

► **Task 2: Gathering the Required Information - Answers**

This task provides the answers to the question from the prior task.

1. Heidi needs to provide the following information to set up the tenant account:
 - a. Country
 - b. First name
 - c. Last name
 - d. Email
 - e. Address 1
 - f. Postal code
 - g. City
 - h. Canton abbreviation
 - i. Phone:
 - j. Organization name
 - k. User ID
 - l. Administrator Password
 - m. Text verification option
2. In response, Heidi provides the following information:
 - a. Country: **Switzerland**
 - b. First name: **Heidi**
 - c. Last name: **Leitner**
 - d. Email: **Heidi's Windows Live account**
 - e. Address 1: **Rue Le-Royer**
 - f. Postal code: **1211**
 - g. City: **Geneva**
 - h. Canton abbreviation: **GE**
 - i. Phone: **Heidi's mobile phone number, including international code**
 - j. Organization name: **Lucerne Publishing**
 - k. User ID: **hleitner@LucernepublishingXXXX.onmicrosoft.com**
 - l. Administrator Password: **Pa\$\$w0rd**
 - m. Text verification options: **Your mobile phone number**

► **Task 3: Creating the Tenant Account**

1. On LUC-CL1, logged on as **Student 1**, on the Task bar, click **Internet Explorer**.
2. In the Address bar, type **http://aka.ms/20346** and press Enter.

3. For Step 1, in the **Start your free 30-day trial** page, complete the following fields. Regardless of your location, use the following information:
 - a. **Country:** Switzerland
 - b. **First name:** Heidi
 - c. **Last name:** Leitner
 - d. **Business email address:** (use your new Windows Live account that you created for this course)
 - e. **Business phone number:** Your mobile phone number, including international code for your current country
 - f. **Company name:** Lucerne Publishing
4. Click **Next**.
5. For Step 2, you have to create a unique domain for the Company name to use in the course. It is recommended that you choose a four character alphanumeric code and append it after **lucernepublishing**. You may have to try a few numeric or alphanumeric combinations to create a unique domain value. For the rest of the fields use the following information:
 - a. **User name:** hleitner
 - b. **Company name:** lucernepublishingXXXX (where XXXX is your unique Lucerne Publishing number)
 - c. **Password:** Pa\$\$w0rd
 - d. **Confirm password:** Pa\$\$w0rd

MAKE A NOTE OF THE XXXX CODE AFTER LUCERNEPUBLISHING. You will use this in all subsequent labs and enter it whenever you are asked to supply a **@lucernepublishingXXXX.onmicrosoft.com** logon or web site URL.
6. Click **Next**.
7. For Step 3, you have to confirm your identity using your mobile phone. Under **Send text message**, from the drop-down box, select the code for the country that you are now in.
8. In the **Mobile phone number** box, enter your correct mobile phone number.
9. Ensure that the **Send text message** option is selected, and then click **Text me**.
10. When you receive the confirmatory text on your mobile phone, enter that in the **Enter your verification code** box.
11. Under **Microsoft Online Services may contact me with information about their products, services and events**, clear the **Email** and **Phone** options.
12. Click **Create my account**.
13. Wait until the Office 365 tenant is provisioned and then click on **You're ready to go...**
14. On the **Don't lose access to your account** page, the **Mobile phone number** and **Alternate email address** fields are required. If either field is blank, enter the appropriate information. Click **Save** and **continue**.
15. Click on the **Admin** tile to go to the Office 365 administrative portal.

► Task 4: Checking the Office 365 Service Status

1. Click on **Service Health** on the left-hand menu, then click on **Service Health** again to display the Service Health Dashboard.
2. Click on **View details and history**.
3. Review the information under **Current status**. Note that at this point, services will still be initializing.
4. Review any service interruption records or additional information in the status page.
Note: During Microsoft's testing, on rare occasions Office 365 did not create the trial tenant properly; as a result, the tenant did not have all the services available to it. If this happens to you, you should create a new trial tenant using a different business email (Windows Live account).
5. Click the **RSS** button. A new Internet Explorer tab opens.
6. Click **Subscribe to this feed**.
7. In the **Subscribe to this feed** dialog box, click **Add to Favorites Bar** and click **Subscribe**. Click **View my feeds** and confirm that **Office 365 Service Health RSS Notifications** has been added to your feeds.
8. Close Internet Explorer.
9. If prompted, click **Close all tabs**.

Results: You have successfully provisioned the Office 365 tenant account for Lucerne Publishing.

Exercise 3: Preparing to Manage Office 365

Scenario

Lucerne Publishing has accepted the pilot plan but the implementation team feels there is a lack of clarity about how to manage Office 365, the effectiveness of client connectivity to Office 365, and the changes that might need to be made to provide this connectivity.

Following a tense meeting between Remi, Justin, Heidi, and Alain, Lucerne Publishing provides the necessary information. Alain needs to confirm that the management computers meet certain requirements, the right ports are open, and that users can connect from those locations to the Office 365 service centers in each country. Heidi is pretty sure connectivity will not be a problem but decides to check anyway.

The main tasks for this exercise are as follows:

1. Configuring a Management Computer
2. Checking Client Connectivity

► Task 1: Configuring a Management Computer

1. Switch to the LUC-CL1 virtual machine.
2. Press the Windows key, and click **File Explorer**.
3. In File Explorer, navigate to **E:\Labfiles\Lab01**.
4. Double-click **msoidcli_64**.
5. In the **Microsoft Online Services Sign-in Assistant Setup** wizard, on the **License Terms** page, click **I accept the terms in the License Agreement and Privacy Statement**, and click **Install**.

6. In the **User Account Control** dialog box, click **Yes**.
7. On the **Completed the Microsoft Online Services Sign-in Assistant Setup Wizard** page, click **Finish**.
8. In File Explorer, in **E:\Labfiles\Lab01**, double-click **AdministrationConfig-EN**.
9. In the **Microsoft Azure Active Directory Module for Windows PowerShell Setup** wizard, on the **Welcome** page, click **Next**.
10. On the **License Terms** page, click **I accept the terms in the License**, and click **Next**.
11. On the **Install Location** page, click **Next**.
12. On the **Ready to Install** page, click **Install**.
13. In the **User Account Control** dialog box, click **Yes**.
14. On the **Completing the Microsoft Azure Active Directory Module for Windows PowerShell Setup** page, click **Finish**.

► Task 2: Checking Client Connectivity

1. On LUC-CL1, on the Task Bar, click **Internet Explorer**.
2. In the Address bar, enter **https://testconnectivity.microsoft.com/**.
3. In the **Microsoft Remote Connectivity Analyzer** page, click the **Office 365** tab.
4. In the Office 365 tab, click **Office 365 Exchange Domain Name Server (DNS) Connectivity Test**, and click **Next**.
5. Under **Domain Name**, enter **lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number).
6. Under **Verification**, enter the characters that you can see into the verification field, and click **Verify**. Note that the verification code is not case-sensitive.
7. Click **Perform Test**.
Note: If you receive a message about having performed too many tests in 60 seconds, wait for a minute and then repeat the test.
8. When you see **Connectivity Test Successful**, under **Test Details**, expand **Test Steps** and review the checks that have been made against the Exchange Online domain.
9. Click **Start Over**.
10. In the **Office 365** tab, click **Office 365 Lync Domain Name Server (DNS) Connectivity Test**, then click **Next**.
11. In the **Sign-in address** field, enter **hleitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number), then click **Perform Test**.
Note: If you receive a message about having performed too many tests in 60 seconds, wait for a minute and then repeat the test.
12. When you see **Connectivity Test Successful**, under **Test Details**, expand **Test Steps** and review the checks that have been made against the Lync Online domain.
13. Click **Start Over**.
14. In the **Office 365** tab, under **Microsoft Exchange ActiveSync Connectivity Tests**, click **Exchange ActiveSync**, then click **Next**.

15. In **Exchange ActiveSync**, select **Use Autodiscover to detect server settings**, then under **Email Address**, enter **hleitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number).
16. In **Microsoft Account**, enter **hleitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number).
17. In **Password** and **Confirm password**, enter **Pa\$\$w0rd**.
18. Check **Ignore Trust for SSL**.
19. Check **I understand that I must use the credentials of a working account from my Exchange domain to be able to test connectivity to it remotely. I also acknowledge that I am responsible for the management and security of this account**.
20. Click **Perform Test**.
21. When you see **Connectivity Test Successful**, under **Test Details**, expand **Test Steps** and review the checks that have been made against Exchange ActiveSync.
22. Click **Start Over**.
23. Under **Microsoft Office Outlook Connectivity Tests**, click **Outlook Connectivity**, then click **Next**.
24. In **Outlook Anywhere (RPC over HTTP)**, in **Email Address** and **Microsoft Account**, enter **hleitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number).
25. In **Password** and **Confirm password**, enter **Pa\$\$w0rd**.
26. Select **Use Autodiscover to detect server settings**.
27. Check **I understand that I must use the credentials of a working account from my Exchange domain to be able to test connectivity to it remotely. I also acknowledge that I am responsible for the management and security of this account**.
28. Click **Perform Test**.
29. When you see **Connectivity Test Successful with Warnings**, under **Test Details**, expand **Test Steps** and review the checks that have been made against **Outlook Anywhere**. Note in particular the **Autodiscover** steps that fail.
30. Under **Run Test Again** at the top right, note that you can copy this test to the clipboard, or save it as XML or HTML.
31. Close Internet Explorer.

Results: Lucerne Publishing has installed the management tools on a client computer and tested client connectivity.

Lab Discussion Questions

Why is it important to specify the correct country when you set up an Office 365 account?

It is important to specify the correct country as some facilities are restricted on a country-by-country basis and you cannot change the country after you have set up the account.

What ports need to be open to ensure client communications with the Office 365 environment and what are those ports and protocols used for?

- Why is it important to specify the correct country when you set up an Office 365 account?
- What ports need to be open to ensure client communications with the Office 365 environment and what are those ports and protocols used for?

Protocol /Port	Usage
TCP 443	Office 365 My Company Portal Outlook 2010 and Office Outlook 2007 Microsoft Entourage 2008 for Mac Exchange Web Services/Outlook for Mac 2011 Outlook Web App SharePoint Online
PSOM/TLS 443	Lync Online (outbound data sharing sessions)
STUN/TCP 443	Lync Online (outbound audio, video, and application sharing sessions)
TCP 10106***	Connects to xsi.outlook.com for Outlook Web App (not essential)
TCP 995	POP3(S)
TCP 587	SMTP(S) Relay with POP3
STUN/UDP 3478	Lync Online (outbound audio and video sessions)
TCP 5223	Lync mobile client push notifications
RTP/UDP 50000-50019	Outbound Lync (outbound audio sessions)
RTP/UDP 50020-50039	Outbound Lync (outbound video sessions)
TCP 50040-50059	Outbound Lync Application sharing and file transfer

The main port that must be open is 443 for encrypted web traffic.

Module Review and Takeaways

Having completed this module, you can now describe the features and benefits of Office 365, plan a pilot deployment of Office 365, provision new tenant accounts, and check that clients can connect to the Office 365 service.



Best Practice: Best practices for this stage of the Office 365 deployment process are as follows:

- Ensure that you understand the organization's need for Office 365.
- Identify any in-house services that are not going to transition to Office 365.
- Recruit the right people to be pilot users.
- Check that you have suitable infrastructure to support a connection to Office 365.

MCT USE ONLY. STUDENT USE PROHIBITED

Module 2

Managing Users, Groups, and Licenses

Contents:

Module Overview	2-1
Lesson 1: Manage Users and Licenses by Using the Administration Center	2-2
Lesson 2: Manage Security and Distribution Groups	2-8
Lesson 3: Manage Cloud Identities with Windows PowerShell	2-12
Lab A: Managing Users, Groups, and Licenses	2-21
Lab B: Continue Lucerne Publishing Datacenter Setup	2-32
Module Review and Takeaways	2-36

Module Overview

In this module, students learn about managing users, groups, and licenses by using the Office 365™ console and Microsoft® PowerShell®.

Objectives

After completing this module, you should be able to:

- Manage users and licenses by using the Office 365 admin center.
- Manage security and distribution groups by using the Office 365 admin center.
- Manage users, licenses, and groups by using Windows® PowerShell.

Lesson 1

Manage Users and Licenses by Using the Administration Center

In this lesson, students learn about assigning licenses to users, creating users, setting user location, updating users, deleting users, and setting sign-in status.

Lesson Objectives

After completing this lesson, you should be able to:

- Create users by using the Office 365 admin center.
- Manage users and licenses by using the Office 365 admin center.
- Delete and restore users by using the Office 365 admin center.
- Describe common errors and best practices for managing users and licenses.

Create Users

As the administrator of your organization's Office 365 environment, it is your responsibility to create and manage user accounts for all its users. There are essentially two ways to create and manage your users:

- *As cloud identities by using only Office 365.* This is the quickest and most straightforward method.
- *As directory synchronized identities by using an on-premises directory service to synchronize with Office 365.* This method has the added complexity of installing and configuring synchronization software to ensure that directory objects synchronize successfully with Office 365.

- Two ways to create and manage users:
 - Using only Office 365 (Cloud-only)
 - Synchronizing Office 365 with a local directory service
- User provisioning options:
 - Office 365 Administration Portal
 - Windows PowerShell
 - Bulk Import (CSV file)
 - Directory Synchronization



Note: Later modules will cover the use of *federated identities that use Active Directory Federation Services (AD FS) for single sign-on (SSO)*. This method involves installing identity federation software to extend the directory synchronization used in the second method but the user management process is carried out by DirSync.

User Provisioning Options

Depending on your needs, skills, and environment, there are also several options you can choose from to provision your users:

- *Office 365 admin center.* This provides a simple web interface for individually creating and managing users.
- *Bulk Import.* This provides a method for the bulk import of multiple users into the Office 365 Administration Portal through a comma-separated value (CSV) file.

- *Windows PowerShell*. This provides a cmdlet- and script-based interface to create and manage single and multiple users.
- *Directory Synchronization*. This provides the only option for provisioning and managing users in a single sign-on (SSO) environment by synchronizing Office 365 with an on-premises directory service through the use of either password synchronization or AD FS. Password synchronization is covered in Module 10.



Note: Provisioning users with Windows PowerShell is covered in a later lesson in this module. Provisioning users with directory synchronization is outside the scope of this module and is covered in a later module in this course.

Creating Users with the Office 365 Admin Center

Using the Office 365 admin center is the simplest method for creating single or small numbers of user accounts.

To create a single user:

1. In the portal, click **Admin, Office 365**.
2. Click **Users**, and then click **Active Users**.
3. Click the + (Add) symbol.
4. Fill in the user information.
5. Specify whether the user is an administrator or not.
6. Specify the user's location.
7. Select which user licenses to assign.
8. Specify whether to send a confirmation email containing the temporary password.
9. Create the user.



Note: The password is sent as clear text in the email. If this is a concern, you need to use another method to inform the user of their temporary password, such as in person, or through a phone call or instant message.

Creating Users with Bulk Import

You can use the bulk add option in the Office 365 admin center to import large numbers of users in one operation using a CSV file. A CSV file is a plain-text file used for storing a large amount of record information in a specific format. Office 365 provides both an empty template and a sample CSV file to make the process easier. You can use a simple text-editing tool such as Notepad to edit these files.

To create users using bulk import:

1. In the portal, click **Admin, Office 365**.
2. Click **Users**, and then click **Active Users**.
3. Click the Bulk add symbol.
4. Browse for the CSV file containing your users.
5. The verification result informs you if there are any errors in your file – you can view the results in the linked log file.

6. On the **Settings** page, set the new users' sign-in status and user location.
7. On the **Assign Licenses** page, specify which licenses the new users should have assigned to them.
8. Specify who to email the results to. It is always a good idea to include your own email address at a minimum so that you can provide the temporary passwords to your new users.


Manage Users and Licenses

Whichever method you use to provision your users, there are several account settings you also need to manage. These include assigning administrator roles, setting the user's sign-in status, specifying user location settings, and assigning licenses. You can manage these user settings using the web portal or Windows PowerShell cmdlets; however, in this lesson we will only use the portal to manage users and their licenses.

Editing Users

You can use the Office 365 admin center to edit single or multiple users.

To edit multiple users:

1. In the portal click **Admin, Office 365**.
2. Click **Users**, and then click **Active Users**.
3. Select the users you want to edit.
4. Click the  (Edit) symbol.
5. On the **Details** page you can make changes to the selected users' domain, and to organizational information, such as department and company contact information.
6. On the **Settings** page you can:
 - a. Specify whether the selected users should have administrator permissions. The different administrator roles are discussed in a later module in this course.
 - b. Specify the sign-in status of the selected users. You can set this to either Allowed or Blocked. If this is set to Blocked, the user cannot log in to Office 365. The user is not immediately blocked from accessing services but they will be blocked at the next login attempt. Typical reasons for blocking a user might be that they are a contract worker or they have left the company but you wish to retain their email details.
 - c. Set the user location. As some services are not allowed in certain countries, Microsoft is required to know the location of each user using its Office 365 services, so that only the permitted services are offered to that user. For example, Jamaica does not permit hosted voicemail in Exchange Online or audio/video in Lync Online.
7. On the **Assign Licenses** page you can either leave the assigned licenses as they are, replace the existing license assignments with new ones, or add new licenses to the existing license assignments.
8. The **Results** page confirms your changes.


- Edit single or multiple users in Office 365 admin center
 - Domain and company information
 - Administrator roles
 - Sign-in status
 - User location
- Assign Office 365 service licenses to users
 - Replace existing licenses
 - Add to existing licenses
- View license information
 - Number of licenses used
 - Unlicensed users

Assigning Licenses to Users

Your organization's users need licenses to use Office 365 services such as Outlook, SharePoint Online and Lync Online. When you assign a license to a user, the service is automatically set up for that user. For example, when you assign a license for SharePoint Online, the user is assigned edit permissions on the default team site. Only members of the Global admin and User management admin roles can assign or remove licenses.

You can assign or remove a license for single or multiple users – you can use the Office 365 admin center or Windows PowerShell.

To assign or remove licenses for multiple users in the Office 365 admin center:

1. In the portal click **Admin, Office 365**.
2. Click **Users**, and then click **Active Users**.
3. Select the users you want to assign or remove licenses for.
4. Click the  (Edit) symbol.
5. On the **Details** and **Settings** pages, click **Next**.
6. On the **Assign Licenses** page, specify whether to replace or add to existing licenses and select the check boxes for the licenses you want to modify.



Note: When you remove a license from one of your users, any service data that is associated with that user is deleted. You then have a 30-day grace period in which you can recover that data, but after that it is gone forever.

Viewing License Information

You can use the Office 365 admin center to view important information about your users' license usage, such as how many licenses you have used and how many are remaining, and which users are currently unlicensed.

To view the number of licenses remaining:

1. In the portal click **Admin, Office 365**.
2. Choose **Licensing**.
3. Choose **Licenses**.
4. Note how many licenses are valid and how many licenses have been assigned.


To view any unlicensed users:

1. In the portal click **Admin, Office 365**.
2. Click **Users**, and then click **Active Users**.
3. Click the Filter symbol.
4. In the drop-down list click **Unlicensed users**.

Delete and Restore Users

When users leave your organization they will no longer require a user account in Office 365. It will be your responsibility to delete their user accounts to ensure they can no longer access Office 365. When you delete a user account, the Office 365 license assigned to that user becomes available to be assigned to another user.

To delete one or more users:

1. In the portal click **Admin, Office 365**.
2. Click **Users**, and then click **Active Users**.
3. Select the users you want to delete.
4. Click the  (Delete) symbol.
5. On the message box click **Yes** to delete the selected users.
6. When they have been successfully deleted, click **Close**.

You can also use Windows PowerShell to delete user accounts by using the **Remove-MsolUser** command with either the **-ObjectId <Guid>** or the **-UserPrincipalName <string>** parameters.

When you delete a user account, the account becomes inactive and the user cannot log in to access Office 365 services. However, there may be occasions when it will be necessary to restore the user's account. Office 365 retains the account as a "soft deleted" inactive account for 30 days after deletion; this enables you to restore the account in such situations.

To restore one or more users:

1. In the portal click **Admin, Office 365**.
2. Click **Users**, and then click **Active Users**.
3. Choose **Deleted users**.
4. Select the users you want to restore.
5. Click **Restore users**.
6. After the user accounts have been restored, you can view a log to display the results of the restoration process.

You can also use Windows PowerShell to restore deleted user accounts by using the **Restore-MsolUser** cmdlet. This is covered in a later lesson in this module.

 **For information on troubleshooting deleted user accounts, see: "How to troubleshoot deleted user accounts in Office 365."**

<http://go.microsoft.com/fwlink/?LinkId=401132>

- Delete single or multiple users
 - Office 365 admin center portal
 - Windows Azure Active Directory Module for Windows PowerShell - *Remove-MsolUser*
 - Deleted users are "inactive" for 30 days ("soft delete")
- Restore deleted users before 30-day grace period
 - Office 365 admin center portal
 - Windows Azure Active Directory Module for Windows PowerShell - *Restore-MsolUser*

Common Errors and Best Practice Guidelines

When managing users and licenses in Office 365, there are some common errors that you should avoid, and some best practices you should follow.

These common errors include:

- When creating cloud users, many small organizations do not have a default password policy; users therefore cannot use the same password with Office 365 and will not understand why.
- A user leaves your organization and you delete his or her account, which deletes the associated mailbox data. To avoid this, you can use the *inactive mailbox* feature which enables you to place an In-Place Hold on the mailbox before you delete the user's Office 365 account and mailbox. This makes the mailbox inactive, which means the mailbox data is available indefinitely. This enables you to use the In-Place eDiscovery feature of Exchange Online to search and access the mailbox contents.

- Common errors
 - Customer domain has no password policy defined and so users cannot use the same password with Office 365 as it does not meet complexity requirements
 - User leaves the organization and when his or her account is deleted, the user's mailbox is also deleted
- Best practices
 - Design user account plan for the future
 - Standardize user naming conventions
 - Ensure accuracy when entering names
 - Look for duplicate accounts when using directory sync



For more information, see “Manage Inactive Mailboxes in Exchange Online.”

<http://go.microsoft.com/fwlink/?LinkId=390865>

To ensure that you create and manage your Office 365 users correctly, follow these best practices:

- Design your user account plan with the future in mind.
- Standardize your organizational user naming convention.
- Ensure you enter correct names for the display name when creating accounts.
- If you decide to start using directory synchronization in the future, ensure you look for potential duplicate names and account details before you synchronize.

Lesson 2

Manage Security and Distribution Groups

In this lesson, students cover the bulk import process, the Azure™ Active Directory® Graph API, the soft delete function, and use of the Office 365 Administration Center for user and group management.


Lesson Objectives

After completing this lesson, you should be able to:

- Create and edit security groups by using the Office 365 admin center.
- Delete security groups by using the Office 365 admin center.
- Describe Exchange Online groups and SharePoint® Online groups.
- Describe common errors and best practices for managing security and distribution groups.

Create and Edit Office 365 Security Groups

The groups you create in the Office 365 admin center are security groups and you should note that these are not mail-enabled.

 **Note:** Mail-enabled groups such as distribution and mail-enabled security groups are created and edited in the Exchange admin center, not in the Office 365 admin center.

Creating Office 365 Security Groups

You can use the Office 365 admin center to organize your users into logical groupings that you can use to assign permissions to in SharePoint Online. For example, you could create a security group containing all users from the Sales department to allow them Full Control access to a sales SharePoint site collection.

You can add and grant permissions to individual users or security groups, and you can also add them directly to the default SharePoint groups which already have pre-defined permissions. However, it is recommended to add your users into Office 365 security groups, and then assign SharePoint site permissions to the groups rather than individual users. Once you have set up your security group structure in Office 365 and granted permissions to those security groups to sites in SharePoint Online, you can add your users to the appropriate security groups in Office 365. This provides your users with the necessary rights to the SharePoint sites.

To create a security group in the Office 365 admin center:

1. In the portal click **Admin, Office 365**.
2. Click **Users**, and then click **Active Users**.
3. Choose **Security groups**.
4. Click the **+** (Add) symbol.
5. Provide a display name and description for the group.

- Office 365 security groups are not mail-enabled
 - Mail-enabled groups do not appear in the Office 365 admin center portal
- Security groups are used to grant permissions to sites and resources in SharePoint Online
- Create groups with admin center portal or through Windows PowerShell – *New-MsolGroup*
- Security groups can be nested to improve organization

6. Select the users you want to add to the security group.
7. Add the selected users.
8. Save and close.

You can also use Windows PowerShell to create security groups for Office 365 by using the **New-MsolGroup** cmdlet; however, this is covered in a later lesson in this module.

Nesting Security Groups

You can optionally nest security groups to improve their organization. Security groups can be nested by adding one security group to another. To do this, simply add a group to another group by clicking the Filter symbol when adding group members and selecting **Groups** from the drop-down list.

Editing Security Groups

The items you can edit on an existing security group are its name, description and members.



Note: You cannot use the Office 365 admin center to edit security groups if they are synchronized with your on-premises Active Directory; you must use local Active Directory management tools.

Delete Office 365 Security Groups

When you no longer need a security group, you can delete it using either the Office 365 admin center or Windows PowerShell. Unlike user accounts, when you delete a security group, it is permanently deleted and cannot be restored. User accounts that were members of the deleted security group remain intact.

To delete a security group in the Office 365 admin center:

1. In the portal click **Admin, Office 365**.
2. Click **Users**, and then click **Active Users**.
3. Choose the security group or groups you want to delete.
4. Click the (Delete) symbol.
5. Confirm that you want to delete the group.

To delete a security group with Windows PowerShell:

1. Open Windows Azure Active Directory Module for Windows PowerShell.
2. At the prompt type the following command, where *groupname* is the name of the group you want to delete, and press Enter:

```
$groupId = Get-MsolGroup -searchString "groupname"
```

3. At the prompt type the following command and press Enter:

```
Remove-MsolGroup -objectid $groupId.ObjectId
```

- Deleted security groups are permanently deleted
 - Its members are not deleted
- Delete security groups
 - Admin center portal
 - Windows PowerShell – *Remove-MsolGroup*

4. At the prompt type **Y** and press Enter.

Exchange Online and SharePoint Online Groups

While the Office 365 admin center uses security groups to organize users, Office 365 includes the following groups:

- *Exchange Online groups*. Can be used to send email messages or assign permissions to a group of users.
- *SharePoint Online groups*. Can be used to grant users permissions to access sites and site resources.


- Exchange Online groups
 - Distribution groups
 - Mail-enabled security groups
 - Dynamic distribution groups
- SharePoint Online groups
 - Collection of users with same permission level
 - Typically contain Office 365 security groups
- Default SharePoint groups
 - Dependent on site template used

Exchange Online Groups

The following three types of mail-enabled groups can be created and managed in the Exchange admin center (EAC) portal:


- *Distribution groups*. These groups can only be used to distribute messages to a set of recipients.
- *Security groups*. These groups can be used to distribute messages and to provide access to resources.
- *Dynamic distribution groups*. These groups do not have a predefined member list because they use recipient filters and conditions that you define to dynamically determine membership at the time that messages are sent.

When you create groups in the EAC, they cannot be edited using the Office 365 admin center, even though the groups appear in the Security Groups list of the portal's Users and Groups section.

 **Note:** Only Exchange distribution groups and mail-enabled security groups appear in the Office 365 admin center; dynamic distribution groups do not appear in the portal.

SharePoint Online Groups

The groups used in SharePoint Online are collections of users who have the same permission level, allowing you to grant access to your SharePoint Online sites to multiple users. SharePoint Online groups greatly enhance and simplify the permissions management process for administrators. Although SharePoint groups can contain individual users, it is better to populate them with security groups from Office 365.

 **Note:** SharePoint Online groups cannot contain distribution groups.

Default SharePoint Groups

There are several built-in groups that are created when you create a site collection in SharePoint Online. These are referred to as default SharePoint groups. The default SharePoint groups created depend on the site template used to create the site. For example, the Team Site template contains three different SharePoint groups: Visitors, Members, and Owners.

Determining Group Types

The different types of groups can become confusing, especially if the display names are similar. However, when you view the groups in Users and Groups under Security Groups, the **type** column informs you of the group type. You can also use the **Get-MsolGroup | Select DisplayName, GroupType** command in Windows Azure Active Directory Module for Windows PowerShell to display the group type information.

Common Errors and Best Practice Guidelines

When managing security groups in Office 365, there are some common errors that you should avoid, and there are some best practices you should follow.

The common errors include:

- Not accurately documenting the Office 365 security group structure, which can lead to poor group management.
- Having an overly complex security group structure, which can lead to confusion and security lapses.
- A user inadvertently becomes a member of a dynamic distribution group. This can occur if a user's account properties are changed to match the dynamic distribution group filters or conditions. In this case the user would unknowingly become a valid recipient as well as becoming a member of a dynamic distribution group and beginning to receive messages sent to that group.

To ensure that you create and manage your Office 365 security groups correctly, you are recommended to follow these best practices:

- Organize users into logical groups who have similar access needs.
- Add users to security groups and then add those security groups to SharePoint default groups, rather than adding individual users to the groups.
- Keep your group naming convention simple but clear.
- Maintain a consistent and well-defined account provisioning process.
- Create policies and procedures for ongoing group maintenance.

- Common errors
 - Poorly documented security group structure
 - Overly complex security group structure
 - User unintentionally becomes a member of a dynamic distribution group
- Best practices
 - Organize users logically based on access needs
 - Add groups to SharePoint groups rather than users
 - Keep naming convention simple and clear
 - Maintain a well-defined account provisioning process
 - Create policies and procedures for group maintenance

Lesson 3

Manage Cloud Identities with Windows PowerShell

In this lesson, students cover how to use Windows PowerShell to configure passwords never to expire; how to carry out a bulk update of user properties; how to create users in bulk by using the Windows Azure Active Directory Module for Windows PowerShell cmdlets, together with bulk user license management; and how to hard delete users.

Lesson Objectives

After completing this lesson, you should be able to:

- Describe how to use Windows PowerShell with Office 365.
- Manage users and licenses by using Windows PowerShell.
- Manage security groups by using Windows PowerShell.
- Describe common errors and best practices for managing users, licenses, and groups with Windows PowerShell.

Using Windows PowerShell with Office 365

Using the Windows Azure Active Directory Module for Windows PowerShell enables you to connect to Office 365 to perform administrative tasks that are not practical, or even possible, using the Office 365 admin center web portal. For example, you can use the Windows Azure Active Directory Module for Windows PowerShell to automate mundane, repetitive tasks such as creating large numbers of user accounts, adding users to groups, and updating multiple user properties.

Using Windows Azure Active Directory Module for Windows PowerShell cmdlets, combined with powerful scripts, means you can drastically reduce the time and effort required to perform repetitive administrative tasks. The following is a list of typical management tasks that can be performed using Windows Azure Active Directory Module for Windows PowerShell with Office 365:

- User management
- License assignment
- Security group management
- Password management
- Domain management
- Admin role assignments

- WAAD Module for PowerShell
 - Connects to Office 365 to perform common and repetitive administrative tasks
- Ensure your environment meets requirements
- Using WAAD Module for PowerShell to manage Office 365
 1. Install the module
 2. Connect to the service
 3. Get help

Windows Azure Active Directory Module for Windows PowerShell Requirements

The following items are required to run the Windows Azure Active Directory Module:

- *Operating system.* You must be running either Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012.
- *Microsoft .NET Framework.* You must install the Microsoft .NET Framework 3.51 feature.
- *Software updates.* You must have installed all the updates required by the Microsoft cloud services to which you have subscribed.
- *Microsoft Online Services Sign-in Assistant.* You must install the appropriate version of the Microsoft Online Services Sign-in Assistant for your operating system from the Microsoft Download Center.

Install the Windows Azure Active Directory Module for Windows PowerShell and Connect to Windows Azure Active Directory

To harness the power of the Windows Azure cmdlets for Windows PowerShell you need to download and install the relevant PowerShell module for Windows Azure for your operating system.



Note: The 64-bit version of the Windows Azure Active Directory Module for Windows PowerShell can be downloaded from the Microsoft Download Center at go.microsoft.com/fwlink/p/?linkid=236297, and the 32-bit version can be downloaded at go.microsoft.com/fwlink/p/?linkid=236298.

After you install the PowerShell module for Windows Azure, you need to connect to your online service through your subscription. To connect to your online service:

- Open the new Windows Azure Active Directory Module for Windows PowerShell console from the desktop shortcut.
- At the prompt, type the following command and press Enter:

```
connect-msolservice
```

- You will be prompted for your credentials.

Get Help on Cmdlets

There are numerous Windows Azure PowerShell cmdlets that can do a multitude of things to different object types, such as users, groups, licenses, passwords, and domains.



For a detailed list of management cmdlets for Windows Azure see “Manage Windows Azure AD using Windows PowerShell.”

<http://go.microsoft.com/fwlink/?LinkId=390866>

To get basic help on a specific cmdlet:

- Open Windows Azure Active Directory Module for Windows PowerShell.
- At the prompt, type the following command and press Enter:

```
Get-Help "cmdletname"
```

For example, **Get-Help set-msoluser**.

To get more detailed help on a specific cmdlet:

- At the prompt, type one of the following commands and press Enter:

```
Get-Help "cmdletname" -examples
```

```
Get-Help "cmdletname" -detailed
Get-Help "cmdletname" -full
```

For example, **Get-Help set-msoluser-detailed**.

Managing Users and Licenses with PowerShell

There are several Windows PowerShell cmdlets you can use to perform tasks related to user management and license management in Office 365.

Add users and licenses

When a new user joins the organization, you can use the **New-MsolUser** cmdlet to create an account in Office 365. This cmdlet can also assign a user license at the same time, so the user can start accessing online services.

To create a user without a license:

- Open Windows Azure Active Directory Module for Windows PowerShell.
- At the prompt, type the following command and press Enter:

```
New-MsolUser -UserPrincipalName username@domainname -DisplayName "Firstname Lastname"
-FirstName "Firstname" -LastName "Lastname"
```

For example:

```
New-MsolUser -UserPrincipalName melissa@lucernepublishing.onmicrosoft.com -
DisplayName "Melissa MacBeth" - FirstName "Melissa" -LastName "MacBeth"
```

To create a user and assign them a license:

- At the prompt, type the following command and press Enter:

```
New-MsolUser -UserPrincipalName username@domainname -DisplayName "Firstname Lastname"
-FirstName "Firstname" -LastName "Lastname" -UsageLocation "2-letter location code" -
LicenseAssignment "license"
```

For example:

```
New-MsolUser -UserPrincipalName melissa@lucernepublishing.onmicrosoft.com -
DisplayName "Melissa MacBeth" - FirstName "Melissa" -LastName "MacBeth" -
UsageLocation "US" -LicenseAssignment "LucernePublishing:ENTERPRISEPACK"
```

Bulk user provisioning

If you need to provision multiple accounts in Office 365, you can use the **Import-Csv** cmdlet with a CSV file. This CSV file should contain a list of all the user accounts you want to create, as well as a column for each of the following user properties:

- FirstName
- LastName
- DisplayName

- Add users and licenses - **New-MsolUser**
 - -LicenseAssignment switch to assign licenses
- Manage licenses - **Set-MsolUserLicense**
 - Use scripts to bulk update licenses
 - -LicenseOptions switch to assign subset of licenses
- Delete users - **Remove-MsolUser**
 - Soft delete – remains in recycle bin for 30 days
 - Hard delete – permanently deleted from recycle bin
- Restore users - **Restore-MsolUser**
 - Within 30 days

- UserPrincipalName
- LicenseAssignment (if you want to assign licenses at the same time)
- UsageLocation

The **Import-Csv** cmdlet will then read through the CSV file and create and license an Office 365 user for each user in the list.

Example:

```
Import-Csv -Path c:\users.csv | ForEach-Object {
    New-MsolUser -FirstName $_.FirstName -LastName $_.LastName `
    -UserPrincipalName $_.UserPrincipalName `
    -DisplayName "$($_.FirstName) $($_.LastName)" `
    -LicenseAssignment 'LucernePublishing:ENTERPRISEPACK' `
    -UsageLocation US
}
```



Note: This cmdlet will generate random passwords for each user; if you want to predefine your own passwords, you could add an extra column to the CSV file with the passwords in it, and update the script to include the **-Password** parameter.

Manage user licenses

You can use the **Get-MsolAccountSku** cmdlet to view the current licensing information for your Office 365 tenant, which includes the number currently available and how many are being used. You can use the **Get-MsolUser** cmdlet with the **-UnlicensedUsersOnly** switch to view a list of users currently without a license.

Additionally, although in the Office 365 admin center you can view how many licenses your organization has purchased and how many remain that can be used, you cannot easily tell which licenses are assigned to which user.

You can, however, use PowerShell to get a list of all your Office 365 tenant users with the licenses that are assigned to each of them and output the result to a CSV file.

To get a list of users and their licenses:

- At the prompt, type the following command and press Enter:

```
Get-MsolUser -All | ft displayname , Licenses | Out-File "filelocation"
```

For example:

```
Get-MsolUser -All | ft displayname , Licenses | Out-File "c:\userlicenses.csv"
```

The **Set-MsolUserLicense** cmdlet enables you to add user licenses, remove user licenses, and update licensing options.

To add a license to a user:

- At the prompt, type the following command and press Enter:

```
Set-MsolUserLicense -UserPrincipalName username@domainname -AddLicenses "license"
```

For example:

```
Set-MsolUserLicense -UserPrincipalName melissa@lucernepublishing.onmicrosoft.com -
AddLicenses "LucernePublishing:ENTERPRISEPACK"
```

To remove a license from a user:

- At the prompt, type the following command and press Enter:

```
Set-MsolUserLicense -UserPrincipalName username@domainname -RemoveLicenses "license"
```

For example:

```
Set-MsolUserLicense -UserPrincipalName melissa@lucernepublishing.onmicrosoft.com -
RemoveLicenses "LucernePublishing:ENTERPRISEPACK"
```

If you want to replace one license with another, you can do this as a single operation so that your user is not left in an intermediate state. For example, you may want to change from a deskless license to an enterprise license, or upgrade from a standard license (E1) to an enterprise license (E3).

To add and remove licenses in one operation:

- At the prompt, type the following command and press Enter:

```
Set-MsolUserLicense -UserPrincipalName username@domainname -AddLicenses "newlicense" -
RemoveLicenses "oldlicense"
```

For example:

```
Set-MsolUserLicense -UserPrincipalName melissa@lucernepublishing.onmicrosoft.com -
AddLicenses "LucernePublishing:ENTERPRISEPACK" -RemoveLicenses
"LucernePublishing:STANDARDPACK"
```

This would upgrade the user's license from an E1 plan to an E3 plan.

Bulk license updates

If you need to update licenses for a large number of users, you can use a PowerShell script to add and remove licenses in one operation, as mentioned above. If you need to upgrade users from an E1 license to an E3 license, you must first generate a CSV file with the list of users currently with an E1 license, and then import that CSV file using the **Import-Csv** cmdlet. You will also need to include a script that will add and remove the required licenses for each user identified by its **UserPrincipalName** in the imported CSV file.



Note: The writing of these scripts is outside the scope of this course.

Assign a subset of licenses

If you want to only assign a subset of service plans from an enterprise license to a user, you can use the **Set-MsolUserLicense** cmdlet combined with the **-LicenseOptions** switch. In order to do this, you need to determine the individual names of each of the service plans in the enterprise license pack.

To view the individual service plans:

- At the prompt, type the following command and press Enter:

```
Get-MsolAccountSku | Where-Object {$_.SkuPartNumber -eq 'ENTERPRISEPACK'} | ForEach-
Object {$_.ServiceStatus})
```

The above command returns a list of the individual service plans; however, a number of the service plan names are difficult to interpret. The following list provides a description of each abbreviated service plan name:

- YAMMER_ENTERPRISE = Yammer
- RMS_S_ENTERPRISE = Rights Management Services
- OFFICESUBSCRIPTION = Office Professional Plus
- MCOSTANDARD = Lync Online
- SHAREPOINTWAC = Microsoft Office Web Apps
- SHAREPOINTENTERPRISE = SharePoint Online
- EXCHANGE_S_ENTERPRISE = Exchange Online

Now that you know what the service plans are called, you can use the **Get-MsolUserLicense** cmdlet with the **-LicenseOptions** switch to assign a subset of service plans from the enterprise license pack. You must specify the tenant account SKU ID, and then disable the service plans you do not want to include.

For example, to assign only the Office Professional Plus, Lync Online, and SharePoint Online licenses to a user:

- At the prompt, type the following command and press Enter:

```
$options = New-MsolLicenseOptions -AccountSkuld tenantname:ENTERPRISEPACK -DisabledPlans
YAMMER_ENTERPRISE, RMS_S_ENTERPRISE, SHAREPOINTWAC, EXCHANGE_S_ENTERPRISE
```

This saves the resulting license options to the **\$options** variable, which you can then assign to the **-LicenseOptions** parameter when assigning licenses to the user.

- At the prompt, type the following command and press Enter:

```
Set-MsolUserLicense -UserPrincipalName username@domainname -LicenseOptions $options
```

For example:

```
Set-MsolUserLicense -UserPrincipalName melissa@lucernepublishing.onmicrosoft.com -
LicenseOptions $options
```

Delete users

When a user leaves the organization, you can use the **Remove-MsolUser** cmdlet to detach the user from Office 365. This cmdlet deletes the user, the user's licenses, and any other associated data. This type of deletion is also known as a soft delete.

To delete a user without needing to confirm the operation:

- At the prompt, type the following command and press Enter:

```
Remove-MsolUser -UserPrincipalName username@domainname -Force
```

For example:

```
Remove-MsolUser -UserPrincipalName melissa@lucernepublishing.onmicrosoft.com -Force
```



Note: The **-Force** switch performs the deletion without requiring you to confirm the operation at the prompt. While this speeds up the operation, it does open it to human error.

By default, when you delete a user, his or her account remains in the Deleted Users view (recycle bin) for 30 days before it is permanently deleted. This allows you some time to retrieve accounts that have perhaps been deleted in error. However, if you wish to remove an already deleted account permanently from the recycle bin you can use the **-RemoveFromRecycleBin** switch. This type of deletion is also known as a *hard delete*.

To permanently delete a user from the recycle bin:

- At the prompt, type the following command and press Enter:

```
Remove-MsolUser -UserPrincipalName username@domainname -RemoveFromRecycleBin
```

For example:

```
Remove-MsolUser -UserPrincipalName melissa@lucernepublishing.onmicrosoft.com -
RemoveFromRecycleBin
```

Restore users

If you have deleted a user in error, you can use the **Restore-MsolUser** cmdlet to restore the user account from the recycle bin back to its original state, as long as you do this within 30 days of the deletion.

To restore a user account from the recycle bin:

- At the prompt, type the following command and press Enter:

```
Get-MsolUser -ReturnDeletedUsers
```

- Note the **UserPrincipalName** of the user you want to restore, and at the prompt, type the following command and press Enter:

```
Restore-MsolUser -UserPrincipalName userprincipalnameofusertorestore
```



For more information on troubleshooting deleted user accounts, see “How to troubleshoot deleted user accounts in Office 365.”

<http://go.microsoft.com/fwlink/?LinkId=401132>

Managing Security Groups with PowerShell

There are several Windows PowerShell cmdlets you can use to perform tasks related to security group management in Office 365.

Create security groups

You use security groups in Office 365 to logically organize your users. You can use the **Get-MsolGroup** cmdlet to return a detailed list of all the security groups that exist for your tenant, up to a maximum of 250 groups. The information returned in the list includes the following:

- Object Id (this is useful when running other cmdlets such as those used below)
- Display name

- Create security groups
 - New-MsolGroup
- Delete security groups
 - Remove-MsolGroup
- Add users to and remove users from a security group
 - Get-MsolUser (to retrieve objectId)
 - Add-MsolGroupMember
 - Remove-MsolGroupMember

- Group type
- Description

To create a security group:

- Open Windows Azure Active Directory Module for Windows PowerShell.
- At the prompt, type the following command and press Enter:

```
New-MsolGroup -DisplayName "displayname" -Description "description"
```

For example:

```
New-MsolGroup -DisplayName "Sales" -Description "Sales Team"
```

Delete security groups

You use the **Remove-MsolGroup** cmdlet to delete a security group from your Office 365 tenant.

To delete a security group:

- At the prompt, type the following command and press Enter:

```
Remove-MsolGroup -ObjectId objectid -Force
```

For example:

```
Remove-MsolGroup -ObjectId 6146df44-dfec-4a88-958b-f5627deb0b1a -Force
```



Note: Rather than having to determine and use the **-ObjectId** parameter when deleting a group, you can use a variable such as **\$groupid** and the **Get-MsolGroup** cmdlet with the **-searchString** parameter.

Add users to and remove users from a security group

You use the **Add-MsolGroupMember** cmdlet to add members to a security group. The new members you add can either be users or other security groups, if you nest your security groups.

To determine the **objectId** of a user:

- At the prompt, type the following command and press Enter:

```
Get-MsolUser -All | Select UserPrincipalName, ObjectId
```

This returns a list of all users with their UPN and their **objectId**, which you can use in the next series of commands.

To add a user to a security group:

- At the prompt, type the following command and press Enter:

```
Add-MsolGroupMember -GroupMemberObjectId groupmemberobjectid -GroupObjectId groupobjectid
```

For example:

```
Add-MsolGroupMember -GroupMemberObjectId f62298ad-6ec1-4da3-8b47-4b84d1cc5941 -GroupObjectId 6146df44-dfec-4a88-958b-f5627deb0b1a
```

To remove a user from a security group:

- At the prompt, type the following command and press Enter:

```
Remove-Mso1GroupMember -GroupMemberObjectId groupmemberobjectid -GroupObjectId groupobjectid
```

For example:

```
Remove-Mso1GroupMember -GroupMemberObjectId f62298ad-6ec1-4da3-8b47-4b84d1cc5941 -  
GroupObjectId 6146df44-dfec-4a88-958b-f5627deb0b1a
```

Common Errors and Best Practice Guidelines

When managing cloud identities in Office 365 with Microsoft PowerShell, there are some common errors that you should avoid, and some best practices you would be well advised to follow.

The common errors include:

- Changing a license incorrectly disconnects the mailbox (E3 customers with archive data lose the archive).
- Deleting groups and users by mistake.
- Not reviewing or testing PowerShell scripts.
- Not knowing the difference between connecting to the Windows Azure Active Directory and the tenant (syntax of the command is incorrect).
- Not having a usage location set for your users.

- Common errors
 - Changing a license incorrectly disconnects the mailbox
 - Deleting groups and users by mistake
 - Not reviewing or testing PowerShell scripts
 - Not knowing the difference between connecting to the Windows Azure Active Directory and the tenant
 - Not having a usage location set for users
- Best practices
 - Review and test PowerShell scripts thoroughly
 - Validate changes made by PowerShell scripts
 - Only provide permissions to the appropriate people

To ensure that you manage your Office 365 identities with Windows PowerShell correctly, you are recommended to follow these best practices:

- Review and test PowerShell scripts thoroughly before deploying in your production environment.
- Validate changes have been made correctly after running PowerShell scripts.
- Only provide permissions to the appropriate people.

Lab A: Managing Users, Groups, and Licenses

Scenario

Now that Heidi Leitner has set up a Lucerne Publishing trial tenant account and successfully registered the `lucernepublishingXXXX.onmicrosoft.com` domain, the company's staff need to use the Office 365 interface during the pilot phase. As there has not yet been a decision on the final design, Heidi and the other Lucerne Publishing pilot users and IT staff are becoming familiar with the interface and the various administrative tasks. Chief among those tasks is the creation of users and groups, together with Office 365 and individual service license administration.

Objectives

To provide the students with practical experience of managing users, licenses, and groups by using both the Office 365 admin center and Windows PowerShell.

Lab Setup

Estimated Time: 75 minutes

Virtual machine: 20346C-LUC-CL1

Username: **Student1**

Password: **Pa\$\$w0rd**

Where you see references in the steps to `lucernepublishingXXXX.onmicrosoft.com`, you should replace XXXX with the unique Lucerne Publishing number that you entered when you set up your Office 365 accounts in Module 1, Lab 1B, Exercise 2, Task 3, Step 5.

Where you see references to `labXXXXXX.o365ready.com`, you should replace XXXXX with the unique O365ready.com number you were assigned when you registered your IP address at `www.o365ready.com` in Module 2, Lab 2B, Exercise 1, Task 2, Step 6.

Exercise 1: Manage Users and Licenses by Using the Administration Center

Scenario

Heidi is learning about the practicalities of managing users and licenses in the Office 365 Admin Center. Her first task is to set up user accounts for the other Office 365 pilot users.

The main tasks for this exercise are as follows:


1. Creating Office 365 Users
2. Editing Office 365 Users
3. Verifying the Office 365 User Accounts


► Task 1: Creating Office 365 Users

1. On your host (classroom) computer, ensure you are logged into the **20346C-LUC-CL1** virtual machine as **Student1** with a password of **Pa\$\$word**.
2. On LUC-CL1, open Internet Explorer and browse to **<https://portal.office.com/>**.
3. Sign in as **hleitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number) with a password of **Pa\$\$w0rd**.
4. In the **Office 365 admin center**, click **Admin**, then click **Office 365**.
5. On the left-hand side, click **Users** and then click on **Active Users** after it expands.

6. Click the + (New) symbol.
7. On the **Create new user account** page, in the **First name** box, type **Robert**.
8. In the **Last name** box, type **Schmid**.
9. In the **Display name** box, type the user's first and last names if the default name does not appear; in this case, type **Robert Schmid**.
10. In the **User name** box, type **rschmid**.
11. Verify that **LucernepublishingXXXX.onmicrosoft.com** is listed in the text box after the '@' sign (where XXXX is your unique Lucerne Publishing number).
12. Click **Create**.
13. On the **Create new user account results** page, note the temporary password here
14. Click **Close**.
15. Repeat steps 6 to 12 to create the following users: (using the first letter of the **First name** and all of the **Last name** as the **User name**; for example, **wdouglas** for William Douglas):
 - William Douglas
 - Justin Muller
 - Rick Torres
 - Mario Ledford
16. Note their temporary passwords here:
 - William Douglas
 - Justin Muller
 - Rick Torres
 - Mario Ledford

► Task 2: Editing Office 365 Users

1. In the Office 365 admin console, in the **Active Users** list, select the check boxes for **Mario Ledford** and **Rick Torres**.
2. On the right-hand side, click the  (Edit) symbol.
3. On the **Details** page, in the **Department** box, type **Accounts**.
4. Click **Next**.
5. On the **Settings** page, in the **Set sign-in status** section, select **Blocked**.
6. Click **Next**.
7. On the **Assign license** page, click **Submit**.
8. On the **Results** page, click **Finish**.
9. In the **Active users** list, under **DISPLAY NAME**, double click **Mario Ledford**.
10. On the left-hand side, click **Details**.
11. Click **Additional details**.
12. Verify that the **Department** box specifies **Accounts**.


13. On the left-hand side, click **Settings**.
14. Verify that **Set sign-in status** is set to **Blocked**.
15. Click **Cancel**.
16. In the **Active Users** list, under **DISPLAY NAME**, double click **Rick Torres**.
17. Repeat steps 10 to 15 to verify that this user has the same settings defined.
18. In the **Active Users** list, select the check box for **Robert Schmid**.
19. On the right-hand side, click the  (Delete) symbol.
20. In the **Warning** dialog box, click **Yes**.
21. In **Users**, click **Deleted users**.
22. Verify that Robert Schmid is in this list.
23. In the **Deleted users** list, select the check box for **Robert Schmid**.
24. On the right-hand side, click **Restore users**.
25. Click **Close**.
26. Click **Active users**.
27. Verify that Robert Schmid is in this list.
28. In the top right-hand corner of the screen, click the drop-down arrow next to **Heidi Leitner**, then click **Sign out**.
29. Close Internet Explorer.

► **Task 3: Verifying the Office 365 User Accounts**

1. On LUC-CL1, open Internet Explorer and browse to **https://login.microsoftonline.com/**.
2. Sign in as **rschmid@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number), with the temporary password noted in the previous task.
3. On the **Update password** page, in the **Old password box**, type Robert's temporary password.
4. In the **New password** and **Confirm new password** boxes, type **Pa\$\$w0rd**.
5. Click **Save**.
6. If prompted, re-enter your new password, and click **Sign in**.
7. Verify that you can access the **Get started with Office 365** page.
8. At the top right-hand of the page, click the drop-down box next to **Robert Schmid**, and then click **Sign out**.

Note: If you have trouble signing out at any point, close and reopen Internet Explorer.

9. Open Internet Explorer and browse to **https://login.microsoftonline.com/**.
10. Sign in as **rtorres@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number), with the temporary password noted in the previous task.
11. Verify that you cannot log in and the message states that your account has been blocked.
12. Close Internet Explorer.
13. Open Internet Explorer and browse to **https://login.microsoftonline.com/**.

14. Sign in as **hleitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number), with a password of **Pa\$\$w0rd**.
15. In the Office 365 admin center, click **Admin**, then click **Office 365**.
16. Click **Users** and then click **Active Users**.
17. In the **Active users** list, select the check boxes for **Mario Ledford** and **Rick Torres**.
18. On the right-hand side, click the  (Edit) symbol.
19. On the **Details** page, click **Next**.
20. On the **Settings** page, in the **Set sign-in status** section, select **Allowed**.
21. Click **Next**.
22. On the **Licenses** page, click **Submit**.
23. On the **Results** page, click **Finish**.
24. At the top right-hand of the page, click the drop-down box next to **Heidi Leitner**, then click **Sign out**.
25. Open Internet Explorer and browse to **https://login.microsoftonline.com/**.
26. Sign in as **rtorres@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number), with the temporary password noted in the previous task.
27. On the **Update password** page, in the **Old password** box, type Rick's temporary password.
28. In the **New password** and **Confirm new password** boxes, type **Pa\$\$w0rd**.
29. Click **Save**.
30. If prompted, re-enter your new password, and click **Sign in**.
31. Verify that you can access the **Get started with Office 365** page.
32. At the top right-hand of the page, click the drop-down box next to **Rick Torres**, and then click **Sign out**.

Results: User accounts and licenses are created and managed according to business needs.

Exercise 2: Manage Security and Distribution Groups

Scenario



Heidi is satisfied with the process of creating user accounts and assigning them licenses. She now wants to practice managing those users through security and distribution group membership.

The main tasks for this exercise are as follows:

1. Creating Office 365 Security Groups
2. Creating Exchange Online Security and Distribution Groups
3. Managing Security Groups

► Task 1: Creating Office 365 Security Groups




1. On LUC-CL1, open Internet Explorer and browse to: **https://login.microsoftonline.com/**

2. Sign in as **hleitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number), with a password of **Pa\$\$w0rd**.
 3. In the **Office 365 admin center**, click **Admin**, and then click **Office 365**.
 4. On the left-hand side, click **Groups**.
 5. Click the + **(Add)** symbol.
 6. On the **New Group** page, in the **Group name** box, type **Sales**.
 7. In the **Description** box, type **Sales department users**.
 8. Click **Create**.
 9. Click **Edit members**, which appears below **Created Sales group successfully**.
 10. Under the **Members** section, click the  **ADD MEMBER** option.
 11. In the **Group Member Picker** window, enter **Robert Schmid** in the search box and select it, enter **William Douglas** in the search box and select it, and then click **Add**.
 12. Click on **Close** and then click on **Back**.
 13. Click the + **(Add)** symbol.
 14. On the **New Group** page, in the **Group name** box, type **Accounts**.
 15. In the **Description** box, type **Accounts department users**.
 16. Click **Create**.
 17. Click **Edit members**, which appears below **Created Accounts group successfully**.
 18. Under the **Members** section, click the  **ADD MEMBER** option.
 19. In the **Group Member Picker** window, enter **Mario Ledford** in the search box and select it, enter **Rick Torres** in the search box and select it, and then click **Add**.
 20. Click on **Close** and then click on **Back**.
- **Task 2: Creating Exchange Online Security and Distribution Groups**
1. In the **Office 365 admin center**, click **Admin**, and then click **Exchange**.
 2. On the left-hand side, click **Recipients**.
 3. In **Recipients**, click **Groups**.
 4. Click the + **(New)** symbol.
 5. In the drop-down list, click **Distribution group**.
 6. In the **Distribution Group** window, in the **Display name** box, type **Sales Distribution**.
 7. In the **Alias** box, type **salesdist**.
 8. In the **Email address** box, accept the default address.
 9. In the **Description** box, type **Distribution group for sales department**.
 10. Scroll down the form, then under **Members**, uncheck the **Add group owners as members** check box.
 11. Click the + **(Add)** symbol.
 12. In the **Select Members** window, select **Robert Schmid** and click **Add**.

13. In the **Select Members** window, select **William Douglas** and click **Add**.
14. Click **OK**.
15. In the **Distribution Group** window, click **Save**.
16. Click the + (New) symbol.
17. In the drop-down list, click **Distribution group**.
18. In the **Distribution Group** window, in the **Display name** box, type **Accounts Distribution**.
19. In the **Alias** box, type **accountsdist**.
20. In the **Email address** box, accept the default address.
21. In the **Description** box, type **Distribution group for accounts department**.
22. Under **Members**, clear the **Add group owners as members** check box.
23. Click the + (**Add**) symbol.
24. In the **Select Members** window, select **Rick Torres** and click **Add**.
25. In the **Select Members** window, select **Mario Ledford** and click **Add**.
26. Click **OK**.
27. In the **Distribution Group** window, click **Save**.
28. In the **Exchange admin center** console, click **Groups**, and then click the + (**New**) symbol.
29. In the drop-down list, click **Security group**.
30. In the **Security Group** window, in the **Display name** box, type **Sales Security**.
31. In the **Alias** box, type **salessec**.
32. In the **Email address** box, accept the default address.
33. In the **Description** box, type **Exchange security group for sales**.
34. Under **Members**, clear the **Add group owners as members** check box.
35. Click the + (**Add**) symbol.
36. In the **Select Members** window, select **Robert Schmid** and click **Add**.
37. In the **Select Members** window, select **William Douglas** and click **Add**.
38. Click **OK**.
39. In the **Security Group** window, click **Save**.
40. Click the + (**New**) symbol.
41. In the drop-down list, click **Dynamic distribution group**.
42. In the **Dynamic Distribution Group** window, in the **Display name** box, type **Accounts Dynamic**.
43. In the **Alias** box, type **acctsdynamic**.
44. In the **Description** box, type **Dynamic distribution group for accounts**.
45. Under **Owner**, click **Browse**.
46. In the **Select Owner** window, click **Heidi Leitner** and click **OK**.
47. Under **Members**, click **Only the following recipient types**.

48. Select the **Users with Exchange mailboxes** check box.
49. Click **Add a rule**.
50. In the drop-down list select **Department**.
51. In the **Specify words or phrases** dialog box, type **Accounts**.
52. Click the + (**Add**) symbol.
53. Click **OK**.
54. In the **Dynamic Distribution Group** window, click **Save**.
55. Verify that the following groups now exist in the Groups list:
 - Sales Distribution
 - Accounts Distribution
 - Sales Security
 - Accounts Dynamic

► Task 3: Managing Security Groups

1. In the **Exchange admin center**, click **Admin**, and then click **Office 365**.
2. On the left-hand side, click **Groups**.
3. Verify that you can see the following groups:
 - Sales Distribution
 - Accounts Distribution
 - Sales Security
4. Verify that you cannot see the Accounts Dynamic group.
5. In the **Security groups** list, clear the check box for **Accounts** (if it was selected by default), and select the check box for the **Accounts Distribution** group.
6. To the right of **Security groups** list, click the  (**Edit**) symbol.
7. Note the message stating that system security groups, distribution groups, and mail-enabled security groups cannot be edited.
8. Click **Cancel**.
9. In the **Security groups** list, select the check box for the **Sales** group.
10. To the right of **Security groups** list, click the  (**Edit**) symbol.
11. Note that you can edit the properties of this Office 365 security group.
12. Under the **Members** section, click **Add Member**.
13. In the **Group Member Picker** window, enter **Justin Muller** in the search box and select it, click **Add**, and then click **Close**.
14. Ensure that Justin Muller is now listed under the **DISPLAY NAME** list, and then click **Back**.
15. In the **Security groups** list, select the check box for the **Sales Security** group.
16. To the right of the groups list, click the  (**Delete**) symbol.
17. In the **Warning** box click **Yes**.

18. Click **Active users**.
19. Confirm that Justin Muller's account still exists in the list of users.

Results: You have created a group structure based on the security need within Lucerne Publishing.

Exercise 3: Manage Cloud Identities with Microsoft PowerShell

Scenario

Heidi is not a PowerShell expert, but she is determined to become more familiar with it and find out how it can help automate the processes of administering Office 365 user and group accounts. The Pilot Phase of the FastTrack process is a good time to learn these new skills and PowerShell syntax.

PowerShell Tip

Throughout this course, you will be tasked with entering a number of PowerShell commands. If you are able to work from a digital version of the course manual during the lab exercises and you are running virtual machines in Hyper-V, you can leverage the Hyper-V clipboard integration feature to paste commands. This will not only save you a lot of time and effort, but it will minimize potential errors should you accidentally mistype command strings.

Perform the following steps to copy and paste PowerShell commands using the Hyper-V clipboard integration feature:

1. Highlight and right-click the command that you must enter in the lab.
2. Click **Copy**.
3. From the virtual machine menu bar, click **Clipboard**, and then click **Type clipboard text**.

The main tasks for this exercise are as follows:

1. Managing Users, Groups, and Licenses with Windows PowerShell
2. Bulk Provision Users with Windows PowerShell

► Task 1: Managing Users, Groups, and Licenses with Windows PowerShell

1. On LUC-CL1, on the desktop, right-click the **Windows Azure Active Directory Module for Windows PowerShell** shortcut and click **Run as administrator**.
2. If a **User Account Control** dialog box appears, click **Yes**.
3. At the prompt, type the following command and press Enter:

```
Connect-mso1service
```

4. In the **Enter Credentials** dialog box log in as **hleitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number), with a password of **Pa\$\$w0rd**.
5. At the prompt, type the following command and press Enter (where XXXX is your unique Lucerne Publishing number):

```
New-Mso1User -UserPrincipalName elabrecque@LucernePublishingXXXX.onmicrosoft.com -
DisplayName "Elisabeth Labrecque" -FirstName "Elisabeth" -LastName "Labrecque" -
Password 'Pa$$w0rd' -ForceChangePassword $false -UsageLocation "CH"
```


- At the prompt, type the following command and press Enter (where XXXX is your unique Lucerne Publishing number).

```
New-MsolUser -UserPrincipalName lmartin@LucernePublishingXXXX.onmicrosoft.com -
DisplayName "Liane Martin" -FirstName "Liane" -LastName "Martin" -Password 'Pa$$w0rd'
-ForceChangePassword $false -UsageLocation "CH"
```

- To create a Marketing group, at the prompt type the following command and press Enter:

```
New-MsolGroup -DisplayName "Marketing" -Description "Marketing department users"
```

- To configure a variable for the group, at the prompt type the following command and press Enter:

```
$MktGrp = Get-MsolGroup | Where-Object {$_.DisplayName -eq "Marketing"}
```

- To configure a variable for the first user account, at the prompt type the following command and press Enter:

```
$ELabrecque = Get-MsolUser | Where-Object {$_.DisplayName -eq "Elisabeth Labrecque"}
```

- To configure a variable for the second user account, at the prompt type the following command and press Enter:

```
$LMartin = Get-MsolUser | Where-Object {$_.DisplayName -eq "Liane Martin"}
```

- To add Elisabeth Labrecque to the Marketing group, at the prompt type the following command and press Enter:

```
Add-MsolGroupMember -GroupObjectId $MktGrp.ObjectId -GroupMemberType "User" -
GroupMemberObjectId $ELabrecque.ObjectId
```

- To add Liane Martin to the Marketing group, at the prompt type the following command and press Enter:

```
Add-MsolGroupMember -GroupObjectId $MktGrp.ObjectId -GroupMemberType "User" -
GroupMemberObjectId $LMartin.ObjectId
```

- To verify the members of the Marketing group, at the prompt type the following command and press Enter:

```
Get-MsolGroupMember -GroupObjectId $MktGrp.ObjectId
```

- To determine which users are unlicensed, at the prompt type the following command and press Enter:

```
Get-MsolUser -UnlicensedUsersOnly
```

- To license Elizabeth Labrecque, at the prompt type the following command and press Enter (where XXXX is your unique Lucerne Publishing number):

```
Set-MsolUserLicense -UserPrincipalName elabrecque@LucernePublishingXXXX.onmicrosoft.com -
AddLicenses "LucernePublishingXXXX:ENTERPRISEPACK"
```

- To license Liane Martin, at the prompt type the following command and press Enter (where XXXX is your unique Lucerne Publishing number):

```
Set-MsolUserLicense -UserPrincipalName lmartin@LucernePublishingXXXX.onmicrosoft.com -
AddLicenses "LucernePublishingXXXX:ENTERPRISEPACK"
```

17. To prevent a user from signing in, at the prompt type the following command and press Enter (where XXXX is your unique Lucerne Publishing number):

```
Set-MsolUser -UserPrincipalName elabrecque@LucernePublishingXXXX.onmicrosoft.com -  
blockcredential $true
```

18. To delete a user, at the prompt type the following command and press Enter (where XXXX is your unique Lucerne Publishing number):

```
Remove-MsolUser -UserPrincipalName elabrecque@lucernepublishingXXXX.onmicrosoft.com -  
Force
```

19. To view the **Deleted Users** list, at the prompt type the following command and press Enter:

```
Get-MsolUser -ReturnDeletedUsers
```

20. Verify that **Elisabeth Labrecque** is included in the **Deleted Users** list. Note that it specifies that she is still licensed.

21. To restore a deleted user, at the prompt type the following command and press Enter (where XXXX is your unique Lucerne Publishing number):

```
Restore-MsolUser -UserPrincipalName elabrecque@lucernepublishingXXXX.onmicrosoft.com
```

22. To view the **Deleted Users** list, at the prompt type the following command and press Enter:

```
Get-MsolUser -ReturnDeletedUsers
```

23. Verify that **Elisabeth Labrecque** is no longer in the **Deleted Users** list.

24. To view the **Active Users** list, at the prompt type the following command and press Enter:

```
Get-MsolUser
```

25. Verify that **Elisabeth Labrecque** is included in the **Active Users** list.

26. To allow a user to sign in, at the prompt type the following command and press Enter (where XXXX is your unique Lucerne Publishing number):

```
Set-MsolUser -UserPrincipalName elabrecque@LucernePublishingXXXX.onmicrosoft.com -  
blockcredential $false
```

► Task 2: Bulk Provision Users with Windows PowerShell

1. On LUC-CL1, on the Task bar, click File Explorer.
2. Navigate to **E:\labfiles\Lab02**.
3. Right-click **O365users.csv**, point to **Open with**, and click **Notepad**.
4. Click **Edit**, and then click **Replace**.
5. In **Find what**, enter **XXX**.
6. In **Replace with**, enter your unique four character number from your Office 365 domain (as in lucernepublishingXXXX.onmicrosoft.com).
7. Click **Replace All**.
8. Click **Cancel**.

9. Check that the XXXX entries have been replaced with your unique Lucerne Publishing number.
10. Close O365Users.csv and in the **Notepad** message box, click **Save**.
11. To bulk import several users from a CSV file, copy and paste this code into the **Administrator: Windows Azure Active Directory Module for Windows PowerShell** window on LUC-CL1 and press Enter:

```
Import-Csv -Path e:\labfiles\lab02\O365Users.csv | ForEach-Object { New-MsolUser -
UserPrincipalName $_.UPN -AlternateEmailAddresses $_.AltEmail -FirstName
$_.FirstName -LastName $_.LastName -DisplayName $_.DisplayName -BlockCredential
$False -ForceChangePassword $False -LicenseAssignment $_.LicenseAssignment -
Password $_.Password -PasswordNeverExpires $True -Title $_.Title -Department
$_.Department -Office $_.Office -PhoneNumber $_.PhoneNumber -MobilePhone
$_.MobilePhone -Fax $_.Fax -StreetAddress $_.StreetAddress -City $_.City -
State $_.State -PostalCode $_.PostalCode -Country $_.Country -UsageLocation
$_.UsageLocation }
```

12. To view the **Active Users** list, at the prompt type the following command and press Enter:

```
Get-MsolUser
```

13. Switch back to Internet Explorer, click **Admin**, and then click **Office 365**.
14. On the left column, click **Users** and then click **Active users**.
15. Review the active users that you have just imported.
16. Click **Admin** and then click **Exchange**.
17. Under **Recipients**, review the mailboxes and associated email addresses that have been created.

Results: Heidi can use Windows Azure PowerShell to manage Lucerne Publishing user and group accounts in Office 365.

Lab Discussion Questions

What process do you need to go through before you can use PowerShell to administer users and groups in Office 365?

Run Windows Azure Active Directory PowerShell with administrative rights, then execute the Connect-MSOL command. Provide the credentials of an account that has Global Admin or User Management Admin rights.

How would you design your group structure to minimize adding and removing people from groups?

- What process do you need to go through before you can use PowerShell to administer users and groups in Office 365?
- How would you design your group structure to minimize adding and removing people from groups?

Use nested groups and assign permissions to the group rather than to individuals.

Lab B: Continue Lucerne Publishing Datacenter Setup

Scenario

This lab continues setting up the Lucerne Publishing Datacenter, which you started in Lab 1A.

Objectives

By the end of this lab, you will have:

- Installed and configured Exchange Server.
- Checked that the datacenter environment is working correctly.

Lab Setup

Estimated Time: 90 minutes

Virtual machine: 20346C-LUC-CL1

Username: **Student1**

Password: **Pa\$\$w0rd**

You should continue this setup using the same Windows Azure session that you used in Lab 1A.

Exercise 1: Set Up the Exchange Server

Scenario

This exercise continues setting up the Lucerne Publishing Datacenter by installing Exchange Server 2013 into your domain.

The main tasks for this exercise are as follows:

1. Obtain Your Student DNS Domain Name
2. Install Exchange 2013 into your Domain
3. Verify the Exchange Server Installation

► Task 1: Obtain Your Student DNS Domain Name

1. On LUC-CL1, at the **Windows Azure PowerShell** prompt, type the following command and press Enter:

```
CD E:\Setupfiles
```

2. At the **Windows Azure PowerShell** prompt type the following command and press Enter:

```
.\GetIPAddress.ps1
```

3. Write down the public IP address of the Lucerne Publishing datacenter for future reference:

Note: You will require this address in several of the following labs, so it is recommended that you save it in a text file on to your desktop.

4. On LUC-CL1, on the taskbar, click **Internet Explorer**.
5. In the address box, type **http://www.O365Ready.com** and then press Enter.
6. Under **Generate Student Lab Number**, type in your public IP address from Step 3 above, and then click **Submit**.

7. Write down your five-digit O365Ready Lab domain for future reference:

lab_____o365ready.com

Note: This is your DNS sub-domain. You should use this in all subsequent labs wherever you see **labXXXXX.o365ready.com** in the instructions.

8. Press the Windows key, type **PowerShell**, and then click **Windows PowerShell**.
9. At the Windows PowerShell prompt, type **nslookup labXXXXX.o365ready.com** (replacing XXXXX with the number from Step 6 above) and press Enter.

Note: You may get a failure message at this point which is caused by DNS propagation delays. If so, return to this step after you have completed the next task, "Install Exchange 2013 into your Domain".

10. Verify that the returned IP address value matches the one you recorded in Step 3.

► Task 2: Install Exchange 2013 into your Domain

1. On **LUC-CL1**, in **File Explorer**, in **E:\RDP_files**, double-click **LUC-EX1.rdp**.
2. If a Remote Desktop Connection warning message appears, click **Don't ask me again for connections to this computer** and click **Connect**.
3. Connect as **LUCERNE\LucAdmin**, password: **Pa\$\$w0rd**.
4. If another Remote Desktop Message appears, click **Don't ask me again for connections to this computer** and click **Yes**.
5. Press the Windows key to go to the Start screen.
6. Right-click **Exchange Management Shell**, and then click **Run as administrator**.
7. At the Windows PowerShell prompt, type the following command and press Enter:
CD C:\Temp
8. At the Windows PowerShell prompt, type the following command and press Enter:
Set-ExecutionPolicy Unrestricted
9. Type **Y** and then press Enter to confirm the execution policy change.
10. At the Windows PowerShell prompt, type the following command, and press Enter:
.\SetupExchange.ps1
11. At the **What is your 5 digit O365Ready Lab UPN number** prompt, enter the number you were assigned in the previous task (where XXXXX is your unique O365ready.com number).
12. Your lab UPN is displayed.
13. Wait until you see the **Exchange setup is complete** message before proceeding.
14. Close the RDP session.
15. On **LUC-CL1**, switch to the **Windows Azure PowerShell** prompt.
16. At the Windows Azure PowerShell prompt, type the following command and press Enter:
.\RestartExchange.ps1
17. Wait until you see the **Exchange environment is ready** message before proceeding

► Task 3: Verify the Exchange Server Installation

1. On **LUC-CL1**, switch to the RDP connection to **LUC-DC1**.

2. In **Server Manager**, click **Tools**, and then click **Active Directory Domains and Trusts**.
3. In Active Directory Domains and Trusts, in the console tree, right-click **Active Directory Domains and Trusts**, and click **Properties**.
4. In the **Active Directory Domains and Trusts** dialog box, verify that the **UPN suffix** is **LabXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number).
5. Close the **Active Directory Domains and Trusts** dialog box, and then close Active Directory Domains and Trusts.
6. In **Server Manager**, click **Tools** and click **Active Directory Users and Computers**.
7. In the **Accounts** OU, verify that there are 15 user accounts.
8. In the **Sales** OU, verify that there are two accounts.
9. Double-click one of the user accounts, and on the **Account** tab, verify that the logon name is in the form **<name>@LabXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number).
10. Close the **User Properties** dialog box, and then close **Active Directory Users and Computers**.
11. Minimize the LUC-DC1 RDP session.
12. On **LUC-CL1**, double-click **LUC-EX1.rdp**, and connect as **LUCERNE\LucAdmin**, password: **Pa\$\$w0rd**.
13. On the Start screen, click **Exchange Management Shell**.
14. At the Exchange Management Shell prompt, type the following command and press Enter:
Get-ExchangeServer |Select Name, ServerRole
15. Verify that the **Mailbox** and **ClientAccess** roles are enabled on this server.
16. At the Exchange Management Shell prompt, type the following command and press Enter:
Get-Mailbox -OrganizationalUnit Accounts
17. Verify that there are 15 mail-enabled users.
18. On LUC-EX1, on the Start screen, start Internet Explorer, and in the Address bar, type **https://luc-ex1/ecp**.
19. Log in as **LUCERNE\LucAdmin** with a password of **Pa\$\$w0rd**.
20. If the **Outlook Web App Language and Time Zone** page appears, then under **Language**, select **English (United States)**, and under **Time zone**, select **(UTC) Coordinated Universal Time**, and then click **Save**.
21. Confirm that you can see the Exchange Admin Center.
22. Minimize the LUC-EX1 RDP session.
23. On LUC-CL1, switch to Internet Explorer.
24. In the **Address** box, type **https://IPaddress/owa** (where IPaddress is the public IP address you obtained in step 3 of the Obtain your Student DNS Domain Name task), and then press Enter.
25. On the **There is a problem with this website's security certificate** page, click **Continue to this website**.
26. Log in as **LUCERNE\LucAdmin** with a password of **Pa\$\$w0rd**.
27. Click **New mail** and in the **To** box, type **username@outlook.com**, (where username@outlook.com is the email address you used to sign up for the Office 365 trial in Module 1, Lab A, Exercise 1, Task 1).

28. Add a subject line and some text to the body of the message.
29. Click **SEND**.
30. If the message bounces back, forward it to **delist.forefront@messaging.microsoft.com** and your IP address should be delisted within 24 hours.

Note: You will not get a response to the delisting request as incoming DNS has not yet been configured. Also, the address for delisting may be different to that shown above.

Results: You have a working Exchange Server.

Module Review and Takeaways

Having completed this module, you can now use the Office 365 admin center and Windows PowerShell to manage users, licenses, and groups in Office 365.

Module 3

Administering Office 365

Contents:

Module Overview	3-1
Lesson 1: Manage Administrator Roles in Office 365	3-2
Lesson 2: Configure Password Management	3-8
Lesson 3: Administer Rights Management	3-13
Lab: Administering Office 365	3-25
Module Review and Takeaways	3-37

Module Overview

In this module, students learn about more complex administration functions, such as the management of administrators themselves, how to configure and set password policies in Office 365™ and how to enable and administer rights management to protect confidential documents.

Objectives

After completing this module, you should be able to:

- Manage users and licenses by using the Office 365 admin center.
- Manage security and distribution groups by using the Office 365 admin center.
- Manage users, licenses, and groups by using Windows PowerShell®.

Lesson 1

Manage Administrator Roles in Office 365

In this lesson, students learn about the permission model in Office 365 and how to create or revoke assignment of administrative roles. They also cover how to determine and assign roles such as the global administrator, billing administrator and user account administrator. They finish off reviewing delegated administration for operating with a managing partner.

Lesson Objectives

After completing this lesson, you should be able to:

- Describe the Office 365 administrator roles.
- Assign Office 365 administrator roles.
- Describe delegated administration.
- Describe common errors and best practices for managing administrator roles.

Office 365 Administrator Roles

Office 365 provides several ready-made administrator roles that you can assign to other users in your organization to ease the administrative burden. Because of the nature of the tasks that these roles can perform, you need to think carefully about who you assign them to, ensuring that those people are responsible and trustworthy.

Permission Model in Office 365

The permission model in Office 365 on which these administrator roles are based is referred to as Role-Based Access Control (RBAC). The RBAC model makes it easier to assign permissions to a user by giving that user a role which has pre-defined permissions assigned to it.

Other online services have their own permission models. For example, Exchange Online uses a similar RBAC model to define administrator roles, but it also utilizes a security model, based on individual permissions for its mailboxes. However, SharePoint® Online has its own completely separate security permissions model, based on security groups, permissions, and permission levels. This allows administrators to assign individual permissions or groups of permission to its resources, such as site collections, sites, and documents.


Office 365 Administrator Roles

Whereas the administrator has full access to all tasks that can be undertaken in the Office 365 admin center, the administrator roles can only carry out a defined subset of these administrative tasks, dependent on the role granted.


The administrator roles that can be assigned are:

- *Billing administrator*. This role can make purchases, manage subscriptions, manage support tickets, and monitor the health of the online service.

Office 365 Administrator Role	PowerShell Administrator Role	Role Tasks
Billing administrator	Company Administrator	Make purchases, manage subscriptions, manage support tickets, and monitor service health
Global administrator	Billing Administrator	Perform all administrative tasks
Password administrator	Helpdesk Administrator	Change/reset passwords, manage service requests, and monitor service health
Service administrator	Service Support Administrator	Manage service requests and monitor service health
User management administrator	User Account Administrator	Create and delete users and groups, reset passwords, manage service requests, and monitor service health

 **Note:** If your organization did not purchase Office 365 directly from Microsoft®, but instead purchased through a partner, then you cannot make billing changes and therefore you can't be assigned the billing administrator role.

- *Global administrator.* This role has the same access as the initial administrator and can perform all the available administrative tasks in the Office 365 admin center, including assigning administrator roles to other users. You can have more than one global administrator role.
- *Password administrator.* This role can change and reset passwords, manage service requests, and monitor the health of the online service. Password administrators can only change and reset passwords for standard users and other password administrators – not other administrator roles.
- *Service administrator.* This role can manage service requests and monitor the health of the online service. You need to first assign administrative permission to a service such as Exchange Online before you assign this role to a user.
- *User management administrator.* This role can create and delete users and groups, and can also reset passwords, manage service requests, and monitor the health of the online service. Although they can create and delete users, user management administrators are restricted from the following:
 - They cannot create other administrator roles.
 - They cannot delete global administrators.
 - They cannot reset passwords for billing administrators, global administrators, or service administrators.

 **Note:** In Office 365 for Small Business, there is only one administrator role. An administrator can assign other users this same administration role, but there are no other sub-roles that can be assigned.

In Windows PowerShell not all administrator roles have the same names as specified in the admin center user interface. The equivalent role names are as follows:

Admin Center Role Name	Windows PowerShell Equivalent Role Name
Global administrator	Company Administrator
Billing administrator	Billing Administrator
Password administrator	Helpdesk Administrator
Service administrator	Service Support Administrator
User management administrator	User Account Administrator

To view the available administrator roles in Windows Azure™ Active Directory Module for Windows PowerShell, at the prompt type the following command and press Enter:

```
Get-MsolRole
```

Global Administrator-Only Tasks

The following tasks can only be performed by the Global administrator:

- Manage domains.
- Manage organization information.
- Delegate administrator roles to other users.
- Use directory synchronization.

Assign Administrator Roles

You can use either the Office 365 admin center or Windows PowerShell to assign the various administrator roles to your users in Office 365.

To assign an administrator role in the admin center, perform the following steps:

1. In the portal, click **Admin, Office 365**.
2. Click **Users** and then click **Active users**.
3. Click the name of the user you want to assign an administrator role to.
4. In the left-hand side, click **Settings**.
5. Under **Assign role**, click **Yes** and then select a role from the drop-down list.
6. Provide an alternate email address.
7. Save your changes.

- In the Office 365 admin center
 - Admin>Office 365>users and groups
 - Select user>edit
 - On settings page, assign role, select admin role and provide alternate email address
- In Windows PowerShell
 - Get-MsolRole
 - Get-MsolUserRole
 - Get-MsolUserRoleMember
 - Add-MsolRoleMember
 - Remove-MsolRoleMember



Note: You can assign the same administrator role to more than one user at the same time by selecting the users first in the users and groups list.

To assign an administrator role in Windows PowerShell, at the prompt type the following command and press Enter:

```
Add-MsolRoleMember -RoleName "nameofrole" -RoleMemberEmailAddress "useremailaddress"
```

For example:

```
Add-MsolRoleMember -RoleName "Helpdesk Administrator" -RoleMemberEmailAddress "melissaf@lucernepublishing.onmicrosoft.com"
```

End of List

To view a user's assigned administrator role, at the prompt type the following command and press Enter:

```
Get-MsolUserRole -UserPrincipalName "userprincipalname"
```

To view all users assigned to a specific administrator role, at the prompt type the following commands and press Enter:

```
$role = Get-MsolRole -RoleName "Helpdesk Administrator"
Get-MsolRoleMember -RoleObjectId $role.ObjectId
```

To remove an administrator role in Windows PowerShell, at the prompt type the following command and press Enter:

```
Remove-MsolRoleMember -RoleName "nameofrole" -RoleMemberEmailAddress
"useremailaddress"
```

For example:

```
Remove-MsolRoleMember -RoleName "Helpdesk Administrator" -RoleMemberEmailAddress
"melissaf@lucernepublishing.onmicrosoft.com"
```

Corresponding Online Service Roles

The administrator roles in Office 365 have some corresponding roles in other online services, such as Exchange Online and SharePoint Online.

Office 365 Role	Exchange Online Role	SharePoint Online Role	Lync Online Role
Global administrator	Exchange Online administrator Company administrator	SharePoint Online administrator	Lync Online administrator
Billing administrator	n/a	n/a	Lync Online administrator
Password administrator	Helpdesk administrator	n/a	Lync Online administrator
Service administrator	n/a	n/a	Lync Online administrator
User management administrator	n/a	n/a	Lync Online administrator

Delegated Administration

If you do not have in-house administrators, you can outsource your administration to a Microsoft partner. For example, if you are a small company without the need for specialized IT administration roles, you may rely on a Microsoft partner to provide IT administrative functionality.

In Office 365, this is called delegated admin, and is initiated by a partner sending your organization an email message requesting that you give them permission to act as administrator on your behalf.

- Delegated administration process
 - Open offer email message from partner
 - Navigate to authorization page in Office 365
 - Authorize the partner
 - Start the trial or subscription
- Partner assigned administration roles
 - Full administration = Global administrator
 - Limited administration = Password administrator

Delegated Administration Process

To accept the offer of delegated administration:

1. Open the email message from your partner and read the terms of the offer.

MCT USE ONLY. STUDENT USE PROHIBITED

2. Click the link to authorize the agreement which takes you to an authorization page in Office 365.
3. Under Delegated administration, click **Yes** to authorize the partner to be your delegated admin.
4. If the delegated administration offer came with a trial subscription or a purchase offer, create the trial or subscription tenant account.


To view the delegated admins:

1. In the Office 365 admin center, click **Admin**.
2. Click **Office 365**.
3. Click **Users**, click **Active users**, and then click **Delegated admins**.



Note: If you do not have a delegated admin, the message on that page will read: "There are no delegated administrators associated with your account."

To delete a delegated admin:

1. In the Office 365 admin center, click **Admin**.
2. Click **Office 365**.
3. Click **Users**, click **Active users**, and then click **Delegated admins**.
4. On the **Delegated admins** page, select the partner you want to delete and click the  (Delete) symbol.
5. Click **Yes** and confirm the deletion.

Administrator Roles Set by Partners

When you delegate administration to a partner, they receive the ability to specify administration roles for your company when they create users on your behalf. They can assign these roles to support agents in their own organization or to users in your organization. However the options are limited to just two roles:

- *Full administration.* This role has the same privileges as a Global administrator role in Office 365.
- *Limited administration.* This role has the same privileges as a Password administrator role in Office 365.

Common Errors and Best Practice Guidelines

When managing administrator roles in Office 365, there are some common errors that you should avoid, and there are some best practices you should follow.

The common errors include:

- Granting more access than is necessary.
- Not planning administration roles.
- Not following a reference model, such as an organizational chart.

To ensure that you manage Office 365

administrator roles correctly, it is recommended that you perform the following best practices:

- | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • Common errors <ul style="list-style-type: none"> • Granting more access than is necessary • Not planning administration roles • Not following a reference model • Best practices <ul style="list-style-type: none"> • Ensure that administrator roles are carefully planned • Document and audit administration roles/privileges • Keep administration roles up to date • Get approval/sign off on administration role design |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

- Ensure that administrator roles are carefully planned, by creating a matrix to distribute roles based on the organization's operational model.
- Document and audit administration roles and their privileges.
- Ensure you keep your administration roles up to date by changing or removing roles as necessary.
- Ensure you get approval and sign off for final administration role design.

Lesson 2

Configure Password Management

In this lesson, students learn how to use the Office 365 administration console and Windows PowerShell to manage user account expiration policy and password complexity. They also explore the options for managing password resets through the self-service options and by the administrator.

Lesson Objectives

After completing this lesson, you should be able to:

- Manage passwords and password policies by using the Office 365 admin center.
- Manage passwords and password policies by using Windows PowerShell.
- Describe common errors and best practices for managing passwords.

Manage Passwords and Password Policies

One method that Office 365 provides to protect users is the requirement to sign in with a password. It is the Office 365 administrator's responsibility to carry out the various tasks involved in managing these passwords for the organization's users. These tasks may include changing passwords, setting password expiration, and resetting passwords.

Setting Password Expiration

By default in Office 365, users' passwords do not expire until 90 days have passed, and users are notified of the impending password expiration 14 days before it occurs.

You can use the Office 365 admin center to change this setting for your organization.

To change the password expiration policy, perform the following steps:

1. In the portal click **Admin, Office 365**.
2. Choose **Service settings**.
3. Choose **Passwords**.
4. Specify a number of days between 14 and 730 for the password expiry.
5. Specify a number of days between 1 and 30 for the password expiry user notification warning.
6. Save your settings.



Note: If you want to change the setting for a user or users so that their password never expires, you need to use the Windows Azure Active Directory Module for Windows PowerShell. This will be covered later in this module.

- Password expiry policy
 - Number of days before it expires
 - Number of days warning prior to expiry
- Resetting user passwords
 - Creates new temporary password
- Resetting admin passwords
 - Reset it yourself
 - Get another admin to reset for you

If a user does not change his or her password before the expiration time has elapsed, he or she can still change it using the password update page that appears the next time they log in. Alternatively, you can reset their password for them.

Resetting User Passwords

If you need to reset a password on behalf of a user, you can reset it for one or more users on the Active Users page. The selected users will be given a new temporary password, which they will need to change when they next sign in.

Resetting Admin Passwords

If you forget your own administrator password there are two options available:

- *Ask another administrator to reset it for you.* In this case, the other administrator must be either a global admin, user management admin, or password admin. However, if your account is a global admin account you must get another global admin to reset it for you.
- *Reset the password yourself.* In this case, as an administrator of the Office 365 cloud service, you can reset your password using the Reset Your Password web page, by performing the following steps:
 - a. On the Office 365 sign-in page, click the **Can't access your account?** link.
 - b. On the **User verification** page, provide your user ID and the verification characters required.
 - c. Open your email inbox and look for an email message from Microsoft Online Services.
 - d. Click the **Reset your password now** link in the email.
 - e. On the **Create a new password** page, type in and confirm a new password.
 - f. When the password has been reset, click the link provided to return to the sign-in page.

For this to work, you must have already supplied an alternate email address in your account settings; this must not be your Office 365 email address. Additionally, if you use a custom domain name or you are using directory synchronization, you must have also supplied a phone number in your account details that is capable of receiving text notifications. In this case, a code will be automatically generated and sent in a text to your mobile phone, and you will need to enter this code on the Mobile phone verification page.



Note: You must complete the admin password reset process within 10 minutes; otherwise, you will need to start the process again.

Manage Passwords and Password Policies with PowerShell

While you can manage password policies using the Office 365 admin center, you can also use the power of the Windows Azure Active Directory Module for Windows PowerShell to manage password policies; in fact, PowerShell provides more functionality than is available within the portal.

- Change/reset a user's password
- Set tenant password policy
 - Password expiry
 - Password expiry notification warning
- Configure user password to never expire
- Remove the never-expires setting
- View which user passwords are set to never expire
 - All these settings are for single user or all users
- Remove strong password complexity requirements
 - Single user only

You can use Windows Azure Active Directory Module for Windows PowerShell to accomplish the following tasks:

- Change a user's password.
- Set the password policy for the tenant.
- Configure user passwords to never expire.
- Remove the never-expires setting.
- View which user passwords have been set to never expire.
- Remove strong password complexity requirements on a per-user basis.

Change a User's Password

Users are automatically given a temporary password when their user account is created. When they first log in, they are required to change their temporary password to a new one that conforms to the Office 365 password policy.

You can also reset the password for them in the admin center, or you can change their password by using a Windows PowerShell cmdlet.

To change a user's password in Windows PowerShell, at the prompt type the following command and press Enter:

```
Set-MsolUserPassword -UserPrincipalName "userprincipalname" -NewPassword "newpassword"
```



Note: If you omit the **-NewPassword** parameter, then it is considered a password reset rather than a password change; in this case, the user will be given a random password and must change it themselves at the next sign-in attempt.

Set Password Policy for a Tenant

You can use the **Set-MsolPasswordPolicy** cmdlet to set the same password policy settings as you can in the admin center. This cmdlet allows you to specify the password expiry time and the password expiry notification settings.

To configure the password policy for a tenant in Windows PowerShell, at the prompt type the following command and press Enter:

```
Set-MsolPasswordPolicy -DomainName "domainname" -ValidityPeriod "numberofdays" -NotificationDays "numberofdays"
```

You can also view the current password policy settings by using the **Get-MsolPasswordPolicy** cmdlet.

Configure Passwords to Never Expire

You can use Windows Azure Active Directory Module for Windows PowerShell commands to configure either one or all users so that their password does not expire.

To configure the password to never expire for a single user, at the prompt type the following command and press Enter:

```
Set-MsolUser -UserPrincipalName "userprincipalname" -PasswordNeverExpires $true
```

To configure the password to never expire for all users, at the prompt type the following command and press Enter:

```
Get-MsolUser | Set-MsolUser -PasswordNeverExpires $true
```

Remove Never Expire Setting

You can also turn off the **Password Never Expires** setting for individual users or all users with Windows Azure Active Directory Module for Windows PowerShell.

To configure the password to expire for a single user, at the prompt type the following command and press Enter:

```
Set-MsolUser -UserPrincipalName "userprincipalname" -PasswordNeverExpires $false
```

To configure the password to expire for all users, at the prompt type the following command and press Enter:

```
Get-MsolUser | Set-MsolUser -PasswordNeverExpires $false
```

View Passwords Set to Never Expire

You can use Windows PowerShell to determine which users have their password set to never expire.

To view whether a single user is set to never expire, at the prompt type the following command and press Enter:

```
Get-MsolUser -UserPrincipalName "userprincipalname" | Select PasswordNeverExpires
```

To view the **Password Never Expires** setting for all users, at the prompt type the following command and press Enter:

```
Get-MsolUser | Select UserPrincipalName, PasswordNeverExpires
```



Note: You can only set passwords to never expire on user accounts that have not been synchronized with a directory service.

Remove Strong Password Requirements

The default setting in Office 365 requires that all user passwords must comply with the complexity requirements, which include the following criteria:

- The password must contain at least one lowercase character.
- The password must contain at least one uppercase character.
- The password must contain at least one non-alphanumeric character (symbol).
- The password cannot contain any spaces, tabs, or line breaks.
- The password must be between 8 and 16 characters in length.
- The password cannot contain the user name.

However, you can use Windows PowerShell to change that behavior on a user-by-user basis.

To remove the strong password requirements for a single user, at the prompt type the following command and press Enter:

```
Set-MsolUser -UserPrincipalName "userprincipalname" -StrongPasswordRequired $false
```



Note: Removing the strong password requirement is not recommended and should only be used if specific circumstances require it.

Common Errors and Best Practice Guidelines

When managing passwords and password policies in Office 365, there are some common errors that you should avoid, and there are some best practices you should follow.

The common errors include:

- Not having a standardized password policy.
- Not aligning cloud policies with on-premises policies.

To ensure that you manage Office 365 passwords and password policies correctly, it is recommended that you perform the following best practices:

- Ensure that administrator roles are correctly defined.
- Ensure that users and administrators are aware of the password reset process.
- Create standardized password policies.
- Enforce the use of strong passwords.

- Common errors
 - Not standardizing password policies
 - Not aligning cloud policies with on-premise policies
- Best practices
 - Ensure administrator roles are correctly defined.
 - Ensure users and administrators know the password reset process
 - Create standard password policies
 - Enforce strong passwords

Lesson 3

Administer Rights Management

In this lesson, students learn how to activate Rights Management Services (RMS) in Office 365. They then explore Exchange, SharePoint, and Office 365 ProPlus integration with RMS, assign roles for Windows Azure AD Rights Management and enable recovery of protected documents.

Lesson Objectives

After completing this lesson, you should be able to:

- Describe rights management in Office 365.
- Plan for rights management in Office 365.
- Activate and configure rights management in Office 365.
- Describe rights management integration with Exchange Online.
- Describe rights management integration with SharePoint Online.
- Describe rights management integration with Office.
- Describe common errors and best practices for managing rights management in Office 365.

RMS in Office 365 Overview

Windows Azure AD Rights Management enables you to protect sensitive Office 365 application and service data including email, document libraries, and other confidential documents. It also enables users to share this data with other users in the organization. You assign rights to your content when you publish it, and the content is then encrypted, regardless of how or where it is distributed.

Rights management provides the following functionality:

- *Protects sensitive data.* Administrators and users can assign several rights to your content using policies, and these enable you to assign rights that include the ability to allow or deny reading, editing, forwarding, printing, and copying of email or documents as needed.
- *Offers persistent protection.* Rights Management provides data protection continuously, so that once the sensitive content is protected, only people who were granted usage rights can decrypt the information, whether it is static or in transit.
- *Integrates with Office 365.* Rights Management integrates with Exchange Online, SharePoint Online, and Office Professional Plus 2013 to provide rights management capabilities across the Microsoft Office suite.

The key information rights management (IRM) features within Windows Azure AD Rights Management that are available in Microsoft Office 365 Enterprise E3 and Microsoft Office 365 ProPlus include:

- Protects sensitive data
 - Email
 - Documents
- Offers persistent protection
 - Static or in transit
- Integrates with Office 365
 - Office integration
 - Exchange Online
 - SharePoint Online

- *Office IRM Integration.* Rights Management enables Microsoft Office Professional Plus 2013 and Microsoft Office 2010 users to protect content using predefined IRM policies provided by the service within a company. Office applications that include these capabilities are Word®, Excel®, PowerPoint®, Outlook®, and InfoPath®.



For more information on how to get started configuring Office client computers to use Rights Management, go to:

<http://go.microsoft.com/fwlink/?LinkId=390867>

- *Exchange Online IRM Integration.* Rights Management enables Exchange Online users to IRM-protect email messages in Outlook Web Access and access IRM-protected messages through Exchange Active Sync for devices that have implemented IRM support including Windows Phone® 7. Administrators of Exchange Online can also enable other IRM features, such as Outlook protection rules and transport rules for protection and decryption. These help to ensure that sensitive content is not accidentally leaked outside of the organization, and edit the message content to include disclaimers.
- *SharePoint Online IRM Integration.* Rights Management enables administrators of SharePoint Online to create IRM-protected document libraries. Therefore, when a user checks out a document from the IRM-protected document library, IRM is applied to the document and the user has the rights to it as specified in the document library IRM settings configured by the SharePoint Online administrator.



Note: Integration with these products will be covered in more detail later in this lesson.

Plan RMS in Office 365

There are several steps that an organization must complete in order to configure and enable Windows Azure AD Rights Management for use.

Before you can begin to use Rights Management, you must perform the following preparation tasks:

1. Prepare your Office 365 tenant by creating new security groups and mail-enabled security groups as needed for administration of the Rights Management service.
2. Decide whether you want Microsoft to manage your tenant key, which is the default, or generate and manage your own tenant key (known as bring your own key, or BYOK).
3. Install the Windows PowerShell module for Rights Management.
4. Activate Rights Management so that you can begin to use the service.

1. Create Office 365 tenant security groups and mail-enabled groups
2. Decide who will manage the tenant key – you or Microsoft
3. Download and install the Rights Management module for Windows PowerShell
4. Activate Rights Management

These last two steps are covered in detail in the next topic.



For more information on how to manage your Rights Management tenant key, go to:

<http://go.microsoft.com/fwlink/?LinkId=390868>

Activate and Configure RMS in Office 365

When you activate Windows Azure AD Rights Management services, you enable the feature for all rights-enabled services and applications. You must activate Rights Management before you can start using the IRM features available in Office, Exchange Online, and SharePoint Online.

Activate Rights Management in Office 365 Admin Center

Before you activate Rights Management, first confirm that your service plan or product version and edition support the Rights Management service.

To activate Rights Management in the Office 365 admin center:

1. In the left-hand side, click **Service settings**.
2. From the Service settings page, click **Rights management**.



Note: If you do not see the rights management option, it might be because your service plan or product version does not support Rights Management, or it has not yet been upgraded to support it.

3. Under **Protect your information**, click **Manage**.
4. Under **Rights management**, click **Activate**.
5. When prompted, click **Activate**.
6. You will now see that Rights Management is activated and you have the option to deactivate it.

Activate Rights Management for Office 365 using Windows PowerShell

You can also use the Windows PowerShell cmdlet, **Enable-Aadrm**, to activate Rights Management for Office 365. However, before you can activate Rights Management in Office 365 using Windows PowerShell, you need to download and install the Windows PowerShell module for Rights Management.



To download the Windows Azure AD Rights Management module for Windows PowerShell, go to:

<http://go.microsoft.com/fwlink/?LinkId=390869>

To install the Rights Management administration module:

1. Double-click **WindowsAzureADRightsManagementAdministration_x64.exe**.
2. In the **User Account Control** dialog box, click **Yes**.
3. On the **Welcome** page, click **Next**.
4. Accept the license terms and click **Next**.
5. Click **Install**.
6. When complete, click **Finish**.

- Activate using admin center portal
 - Service settings>rights management>manage>activate
- Activate using Windows PowerShell
 - Import-Module aadrm
 - Connect-aadrmService
 - Enable-aadrm
- Manage RMS administrator roles
 - Add-AadrmRoleBasedAdministrator
 - Get-AadrmRoleBasedAdministrator
 - Remove-AadrmRoleBasedAdministrator

The next thing you need to do is import the Rights Management module for Windows PowerShell and connect to the Rights Management service.

To import the Rights Management Module for Windows PowerShell and connect to the service:

1. Open Windows Azure Active Directory Module for Windows PowerShell.
2. At the prompt, type the following command and press Enter:

```
Import-Module aadrm
```

3. At the prompt, type the following command and press Enter:

```
Connect-aadrmService -Verbose
```

4. Enter your Office 365 Global administrator credentials.



Note: By default, Global administrators have access to administer Rights Management.

Finally, you need to perform the following steps to enable Rights Management for your tenant using Windows PowerShell:

1. At the prompt, type the following command and press Enter:

```
Enable-aadrm
```

2. At the prompt, type the following command and press Enter:

```
Disconnect-aadrmService
```



Note: The **Enable-Aadrm** cmdlet must be run for all new Office 365 tenant accounts before Rights Management services are available for you to use in implementing rights protection of your content.

Manage Role-Based Administrators for Rights Management

By default, all Global administrators in Office 365 can use all the Rights Management PowerShell cmdlets. However, if you need to delegate Rights Management administrator privileges to another user or group in your organization, you can use the **Add-AadrmRoleBasedAdministrator** cmdlet to add this user (or a group that the user is a member of) to the list of users allowed to administer Rights Management.

To add a role-based administrator for Rights Management, at the prompt type the following command and press Enter, where *user@domainname* is the email address of a user or a group:

```
Add-AadrmRoleBasedAdministrator -EmailAddress "user@domainname"
```

Alternatively you can specify the group name as follows:

```
Add-AadrmRoleBasedAdministrator -SecurityGroupDisplayName "Sales Dept"
```

To view a list of role-based administrators for Rights Management, at the prompt type the following command and press Enter:

```
Get-AadrmRoleBasedAdministrator
```


To remove a role-based administrator for Rights Management, at the prompt type the following command and press Enter, where *user@domainname* is the email address of a user or a group:

```
Remove-AadrmRoleBasedAdministrator -EmailAddress "user@domainname"
```

Alternatively you can specify the group name as follows:

```
Remove-AadrmRoleBasedAdministrator -SecurityGroupDisplayName "Sales Dept"
```

RMS Integration with Exchange Online

Users will often send email messages which contain sensitive data, such as legal documents, employee and payroll information, sales reports, and confidential product details. Accidentally leaking sensitive information such as this can have very serious ramifications for your company. To help mitigate this risk, Exchange Online provides IRM capabilities to protect these sensitive email messages and their attachments.

Users can apply IRM protection to their email messages whether they are in Outlook or Outlook Web App. Exchange Online administrators can also use Outlook protection rules and transport protection rules to apply IRM protection to users' email messages. When IRM protection is applied to an email, the usage rights are embedded in the message itself so that protection applies regardless of whether the user accesses the message content online or offline.

- Enable IRM Services in Exchange Online
 1. Enable Rights Management in Office 365
 2. Connect to Exchange Online with Remote PowerShell
 3. Configure RMS Online Key Sharing Location
 4. Import TPD from RMS Online
 5. Enable IRM in Exchange Online
 6. Test IRM configuration
- Apply IRM to emails in OWA
- Administrator-defined IRM in Exchange Online
 - Transport protection rules (Outlook and OWA)
 - Outlook protection rules (Outlook)

Enable IRM Services with Exchange Online

There are several required configuration steps you must take before you can start implementing IRM with Exchange Online.

1. Activate Rights Management

Windows Azure Active Directory Rights Management is disabled by default in Office 365. In consequence, you need to activate it either by using Windows PowerShell or the Rights Management settings in the Office 365 admin center.



Note: This step was covered in the previous topic.

2. Connect to Exchange Online Using Remote PowerShell

Remote PowerShell is the administrative shell that enables you to administer Exchange Online from a command prompt. To do this, you need to create a remote shell session to connect to your Exchange Online organization.

To connect to Exchange Online using Remote PowerShell:

- a. Open Windows Azure Active Directory Module for Windows PowerShell.
- b. At the prompt, type the following command and press Enter:

```
Set-ExecutionPolicy RemoteSigned
```

- c. At the prompt, type the following command and press Enter:

```
$UserCredential = Get-Credential
```

- d. Enter your Office 365 Global administrator credentials.

- e. At the prompt, type the following command and press Enter:

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

- f. At the prompt, type the following command and press Enter:

```
Import-PSSession $Session
```

3. Configure the RMS Online Key Sharing Location

To configure the sharing location for the RMS Online key for Exchange Online in the European Union, at the prompt type the following command and press Enter:

```
Set-IRMConfiguration -RMSOnlineKeySharingLocation "https://sp-  
rms.eu.aadrm.com/TenantManagement/ServicePartner.svc"
```



Note: Depending on your location in the world, in the above command, you should replace the *eu* part of the URL with *na* for North America or *ap* for Asia.

4. Import the Trusted Publishing Domain from RMS Online

To import the Trusted Publishing Domain from RMS Online, at the prompt type the following command and press Enter:

```
Import-RMSTrustedPublishingDomain -RMSOnline -name "RMS Online"
```

5. Enable IRM in Exchange Online

To enable IRM for your Exchange Online tenant, at the prompt type the following command and press Enter:

```
Set-IRMConfiguration -InternalLicensingEnabled $True
```

6. Test the IRM Configuration

You need to check that you have configured IRM correctly for Exchange Online by running the Test-IRMConfiguration cmdlet.

To test IRM Configuration for Exchange Online:

- a. At the prompt, type the following command and press Enter:

```
Test-IRMConfiguration -RMSOnline
```

This test checks connectivity from Exchange Online to RMS Online service, obtains your organization's Trusted Publishing Domain, and verifies that it is valid.

- b. At the prompt, type the following command and press Enter:

```
Test-IRMConfiguration -Sender user@domainname
```

This tests that a specified user is able to send messages successfully using IRM.

7. Disconnect from Exchange Online

Lastly, you need to disconnect from the Remote PowerShell session after you complete these steps. If you do not disconnect from the session, you will still be using one of your three allowed concurrent Remote PowerShell sessions at the time you close it.

To disconnect from the Exchange Online Remote PowerShell session, at the prompt type the following command and press Enter:

```
Remove-PSSession $Session
```



For more information on how to implement and configure IRM in Exchange Online go to:

<http://go.microsoft.com/fwlink/?LinkId=390870>

Apply IRM to Emails in Outlook Web App

After you configure and enable IRM for use with Exchange Online, your users can start to apply IRM policies to their email messages in Outlook and Outlook Web App. When a user uses IRM to protect an email message, any IRM-supported attachments are also protected.

When a user sends an email message in Outlook Web App, they will see a new option on the ... menu, called **set permissions**. This new menu item provides the following IRM templates that users can select from:

- *No Restrictions*. As the name suggests, this has no IRM restrictions associated with it.
- *Do Not Forward*. This allows a recipient to read the message, but they cannot forward it, print it, or copy content from it.
- *Company name – Confidential*. This specifies that the message content is proprietary information and is intended for internal consumption only. The content may be modified but it cannot be copied or printed.
- *Company name – Confidential View Only*. This is the same as above except that the content is read-only and therefore cannot be modified either.



Note: IRM protection is applied to attached email messages and document attachments from Word, Excel, PowerPoint, InfoPath, as well as XPS files.

To send an IRM-protected email message with an attachment in Outlook Web App:

1. In the Office 365 admin center, click **Outlook**.
2. Click **New mail**.
3. Provide the name of a recipient in the **To:** box.
4. Provide a subject for your email in the **Subject:** box.
5. Click **INSERT** and choose attachment.
6. Browse to the file you want to attach and click **Open**.
7. Click the ... on the top menu, and point to **Set permissions**.

8. Choose one of the four template options.
9. Send the message.



Note: Although IRM protects the email message and its attachment using access and usage rights, IRM cannot prevent content from being erased, stolen, corrupted or captured and transmitted by malware or viruses. It will also not prevent content being manually retyped or screen captured.

Administrator-Defined IRM Protection for Exchange Online

After you enable IRM for Exchange Online, administrators can use either of two methods to apply IRM protection to email messages:

- Transport protection rules can be used to automatically apply IRM protection in Outlook and Outlook Web App. Administrators configure the transport protection rule action to apply an RMS rights policy template to messages that meet the conditions of the rule. The RMS rights policy templates are available to use with the transport protection rule action called *Apply rights protection to message with*. In the Exchange admin center this can be found in **mail flow**, under **rules**, then **Apply rights protection to messages**.
- Administrators can create Outlook protection rules to automatically apply IRM protection to messages in Outlook (but not Outlook Web App), based on conditions that include the sender's department, the recipient's name, the subject or body of the message, and the location of the recipient (internal or external to your organization).

To create a transport protection rule in Exchange Online:

1. In the Office 365 admin center, choose **Admin**, then **Exchange**.
2. Choose **Mail flow**.
3. Choose **Rules**.
4. Create a new rule and choose **Apply rights protection to messages**.
5. Provide a name for the rule.
6. Under Apply this rule if, click the arrow and choose **Apply to all messages**.
7. Under **Do the following**, choose **Select one**.
8. In the **Select RMS template** dialog box, choose one of the three available templates.
9. Add rule actions, exceptions, and other rule settings as required.

RMS Integration with SharePoint Online

Rights Management enables administrators of SharePoint Online to protect document libraries (and lists) with IRM so that, when a user downloads a document from the IRM document library (or a list item), IRM protection is applied to the document (or list item) and only the usage rights specified by the administrator in an IRM policy are available to that user.

SharePoint Online users will be able to access documents in a library once a user has configured it so that it is shared across organizations. Office 365 users will be able to download the document in the shared library and access them according to the specified IRM document usage rights. However, non-Office 365 users will only get a read-only view of documents in the shared library.

- Enable IRM Services in SharePoint Online
 - SharePoint admin center>settings>Information Rights Management>Use the IRM service specified in your configuration
 - Refresh IRM settings
- Apply IRM to document libraries or lists in SharePoint Online
 - Library>Library Settings>Permissions and Management>Information Rights Management>Restrict permissions on this library on download
 - Configure document access rights

Enable IRM Services in SharePoint Online

SharePoint Online includes IRM feature support using Windows Azure AD Rights Management.


To configure SharePoint Online to use Rights Management:

1. In the Office 365 admin center, choose **Admin**, then **SharePoint**; this opens the SharePoint admin center.
2. In the left-hand side, choose **Settings**.
3. On the **Settings** page, in the IRM section, select **Use the IRM service** specified in your configuration.
4. Choose **Refresh IRM Settings** which will now allow users in your organization to protect their SharePoint lists and document libraries.

Apply IRM to a List or Library in SharePoint Online

As a SharePoint Online user you can use IRM to help regulate and safeguard files that can be downloaded by users from lists or document libraries. By default, RMS supports IRM for sites; therefore, there are no separate software or additional installation requirements.

Before users can apply IRM to a document library or list in SharePoint Online, it must have already been enabled for your site by a SharePoint Online administrator.

 **Note:** In order for a user to apply IRM protection to a document library or list, they must have at least Design level permissions on that library or list.

To apply IRM protection for a SharePoint document library:

1. Navigate to the library for which you want to configure IRM.
2. On the ribbon, choose the **Library** tab, and then choose **Library Settings**.
3. Under **Permissions and Management**, choose **Information Rights Management**.
4. On the **Information Rights Management Settings** page, select the **Restrict permissions on this library on download** check box.
5. Provide a descriptive name for the permission policy that will help you to distinguish it from other policies.

6. Provide a description for the permission policy that will appear to users who access this library; this description will help explain how they should handle the documents in this library.
7. To apply more restrictions to the documents in this library, choose **SHOW OPTIONS** and then select any of the following:
 - *Set additional IRM library settings.* This setting enables you to specify that users are not allowed to upload documents which do not support the IRM feature. This prevents users from opening documents in the browser for this document library, and disables restricting access to the document library on a specified date.
 - *Configure document access rights.* This setting enables you to configure which document access rights are allowed. These include allowing users to print, to run scripts, and to write to the copy of the downloaded documents. You can also set the expiry of the access rights to the downloaded documents by specifying a number of days between 1 and 365.
 - *Set group protection and credentials interval.* This setting controls the interval that credentials are cached for in the application that is licensed to open the document, and enables you to specify a group to share the documents in this library with.



Note: When you enable IRM on a list in SharePoint Online, rights management applies only to the files that are attached to list items, not the list items themselves.

RMS Integration with Office

Rights Management that is integrated with Microsoft Office Professional Plus 2013 and Microsoft Office 2010 provides users with the ability to protect their content with predefined IRM policies. Office applications that support and provide these capabilities are Word, Excel, PowerPoint, Outlook, and InfoPath.

Office Support for Rights Management

To create or use IRM protected content in Office, your version of Office must support the RMS in Office 365. The following table indicates which Office versions are supported:


- Office support for Rights Management
 - Office Pro Plus 2013 and Office 2010 – supported
 - Office 2007 – not supported
- Office Professional Plus 2013 Client Configuration
 - Install Office and login with Office 365 credentials
- Office 2010 Client Configuration
 - Install Office
 - Install RMS sharing application
 - Login with Office 365 credentials
- Protecting Office Content with Rights Management
 - Templates
 - User defined rights

Office Product Family	Restrictions for Rights Management
Microsoft Office Professional Plus 2013	Supported for this release
Microsoft Office 2010	Supported for this release: <ul style="list-style-type: none"> • You must have at least Office 2010 Professional Plus to publish rights-protected content. • All versions of Office 2010 can access rights-protected content if the user has the correct permissions.

Office Product Family	Restrictions for Rights Management
Microsoft Office 2007	Not supported for this release
Office for Mac 2011	Not currently supported

Office Professional Plus 2013 Client Configuration

In order to use IRM capabilities in Office Professional Plus 2013, you need to install Office and then sign in to your Office applications using your Office 365 credentials.

 **Note:** You can also download and use the Microsoft Rights Management sharing application to get more functionality, but it is not required. The RMS sharing application adds an RMS-specific toolbar to the Office ribbon.

Office 2010 Client Configuration

In order to use IRM capabilities in Office 2010, you need to install Office, download and install the Microsoft Rights Management sharing application, and then sign in to your Office applications using your Office 365 credentials through the Rights Management sharing application.

 **To download the Microsoft Rights Management sharing application go to:**

<http://go.microsoft.com/fwlink/?LinkId=303970>


 **To read the Microsoft Rights Management sharing application user's guide go to:**

<http://go.microsoft.com/fwlink/?LinkId=390871>

Protecting Office Content with Rights Management

There are two methods for providing content protection using Rights Management in Office:

- *Templates.* These contain predefined rights that can be applied to provide IRM protection for content. The following templates are provided in Microsoft Office 2013:
 - *Company Confidential.* This template allows users to read and modify the content, but does not allow them to print or copy the document content.
 - *Company Confidential Read Only.* This template allows users to only read the content, but does not allow them to edit, print, or copy the document content.

 **Note:** Only users within your organization can open documents to which this template has been applied.

- *User defined rights.* These settings enable you to configure more granular control of content access. Users can apply their own usage rights and specify which users and groups they apply to.

Common Errors and Best Practice Guidelines

When administering Rights Management in Office 365, there are some common errors that you should avoid, and there are some best practices you should follow.

The common errors include:

- Lack of administrator knowledge can lead to confusion when implementing and configuring RMS.
- Lack of user training can lead to expectations being set too high, and confusion over how RMS restrictions work.
- If your RMS policies are too complex, it can make managing them very difficult, so try to avoid having too many policies.
- IRM feature support is provided by Microsoft for Windows Mobile devices such as Windows Mobile 6.x and Windows 7.5+ devices. However, IRM features are not supported by Microsoft for Android, BlackBerry OS, Apple iOS, or Nokia Symbian OS devices. Third-party products providing IRM-enabled applications for the unsupported devices may exist. Windows Phone versions 7.5 and later versions all include built-in functionality that allows users to access email messages and Microsoft Office documents protected by IRM.

To ensure that you administer Rights Management correctly in Office 365, you are recommended to follow these best practices:

- Use the Keep It Simple, Stupid (KISS) principle when planning and implementing RMS policies to avoid confusion and sensitive content leakage.
- Ensure you make your users aware that IRM is only available for Office 2010 and 2013 clients in your on-premises deployment.

- Common errors
 - Lack of administrator knowledge
 - Lack of end-user training
 - RMS policies too complex
 - Non-MS device compatibility
- Best practices
 - Use KISS principle
 - Ensure users are aware that IRM is only for Office 2010/2013 clients

Lab: Administering Office 365

Scenario

Lucerne Publishing is now well into the Pilot Phase of its FastTrack deployment of Office 365. Justin has asked Heidi to review how administrator accounts are created. In addition, because the company is increasingly seeing its publications plagiarized or stolen outright, it needs to implement RMS in Office 365 to protect its intellectual property. However, Justin needs to ensure that they still have the ability to recover documents if required.

Objectives

To provide the students with practical experience of administering Office 365 administrator roles, passwords and password policies, and rights management by using both the Office 365 admin center and Windows PowerShell.

Lab Setup

Estimated Time: 75 minutes

Virtual machine: 20346C-LUC-CL1

Username: **Student1**

Password: **Pa\$\$w0rd**

In all tasks, where you see references to **lucernepublishingXXXX.onmicrosoft.com**, replace the **XXXX** with the unique Lucerne Publishing number that you were assigned when you set up your Office 365 account in Module 1, Lab 1B, Exercise 2, Task 3, Step 5.

Where you see references to **labXXXXX.o365ready.com**, replace the **XXXXX** with the unique O365ready.com number you were assigned when you registered your IP address at www.o365ready.com in Module 2, Lab 2B, Exercise 1, Task 2, Step 6.

Exercise 1: Manage Administrator Roles in Office 365

Scenario

Justin and Heidi have drawn up a list of the pilot users that they want to assign administrative rights. Liane Martin is to be the Password Administrator, while Odessa Brunner will be the User Management Administrator.

In this exercise, Heidi assigns administrative rights to additional user accounts using both the Office 365 admin center and PowerShell. She establishes the scope of the assigned rights and manages those accounts to meet the business needs of the organization.

The main tasks for this exercise are as follows:

1. Managing Administrator Roles in the Admin Center
2. Testing Administrator Roles in the Admin Center
3. Managing Administrator Roles in Windows Azure Active Directory Module for Windows PowerShell
4. Testing Administrator Roles in Windows Azure Active Directory Module for Windows PowerShell

► Task 1: Managing Administrator Roles in the Admin Center


1. On your host computer, ensure you are logged into the **20346C-LUC-CL1** virtual machine as **Student1** with a password of **Pa\$\$word**.
2. On LUC-CL1, open Internet Explorer and browse to **<https://login.microsoftonline.com/>**.

3. Sign in as **hleitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number), with a password of **Pa\$\$w0rd**.
4. In the **Office 365 admin center**, click **Admin** in the top right, then click **Office 365**.
5. On the left-hand side, click **Users**, and then click **Active Users**.
6. Double-click **Mario Ledford**.
7. In the **Mario Ledford** page, click **Settings**.
8. Under **Assign role**, click **Yes**, then select **Billing administrator** from the list.
9. **user@alt.none** is the default alternate email address and should be displayed in the **Alternate email address** box; if it does not appear, then type **user@alt.none** in this field.
10. Click **Save**.
11. Double-click **Luc Cartier**.
12. In the **Luc Cartier** page, click **Settings**.
13. Under **Assign role**, click **Yes**, then select **Billing administrator** from the list.
14. In the **Alternate email address** box, type **user@alt.none**.
15. Click **Save**.
16. Double-click **Liane Martin**.
17. In the **Liane Martin** page, click **Settings**.
18. Under **Assign role**, click **Yes**, then select **Password administrator** from the list.
19. In the **Alternate email address** box, type **user@alt.none**.
20. Click **Save**.
21. Double-click **Odessa Brunner**.
22. In the **Odessa Brunner** page, click **Settings**.
23. Under **Assign role**, click **Yes**, then select **User management administrator** from the list.
24. In the **Alternate email address** box, type **user@alt.none**.
25. Click **Save**.
26. In the top right menu, click **Heidi Leitner**, then click **Sign out**.

► Task 2: Testing Administrator Roles in the Admin Center

1. On the **Office 365** page, sign in as **lmartin@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number), with a password of **Pa\$\$w0rd**.
2. On the **Don't lose access to your account** page, in the **Country or region** box, select **Switzerland**.
3. In the **Mobile phone number** box, type **5551234**.
4. In the **Alternate email address** field, enter **username@outlook.com** (where username@outlook.com is the Windows Live address you registered in Lab 1A, Ex 1 Task 1).
5. Click **Save and continue**.
6. In the **Office 365 admin center**, click **Admin** in the top right, then click **Office 365**.
7. On the left-hand side, click **Users**, and then click **Active Users**.

8. Double-click **Thomas Lanctot**.
 9. Note that you cannot perform any administrative tasks.
 10. Click **Close**.
 11. In the list of **Users** select the check box for **Thomas Lanctot**.
 12. On the right-hand side, click **Reset Password**.
 13. On the Send results in email, clear **Send email**.
 14. Click **Reset password**.
 15. Write down the temporary password here for future reference:

 16. Click **Finish**.
 17. In the top right menu, click **Liane Martin**, then click **Sign out**.
 18. On the **Office 365** page, sign in as **obrunner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number), with a password of **Pa\$\$w0rd**.
 19. On the **Don't lose access to your account** page, in the **Country or region** box, select **Switzerland**.
 20. In the **Mobile phone number** box, type **5551234**.
 21. Click **Save and continue**.
 22. In the **Office 365 admin center**, on the left-hand side, click **Users**, and then click **Active Users**.
 23. Double-click **Thomas Lanctot**.
 24. On the **Thomas Lanctot** page, click **Details**.
 25. Click **Additional details**.
 26. In the **Office Phone** box, type **555-1234**.
 27. On the left-hand side click **Settings**.
 28. Note that you do not have the rights to assign an administrator role.
 29. Under **Set sign-in status**, click **Blocked**.
 30. Click **Save**.
 31. In the **Office 365 admin center**, click **Active Users**, and then click the + (New) symbol.
 32. In the **First name** box, type **Alfredo**.
 33. In the **Last name** box, type **Abner**.
 34. In the **User name** box, type **aabner**.
 35. Click **Create**.
 36. Click **Close**.
- Note:** If Alfredo is let go, a user management administrator can also delete accounts.
37. In the list of **Active Users**, select the check box for **Alfredo Abner**.
 38. On the right-hand side, click the  (Delete) symbol.
 39. In the **Message** box, click **Yes**.

40. In the top right menu, click on the profile photo icon of **Odessa Brunner**, and then click **Sign out**.

► **Task 3: Managing Administrator Roles in Windows Azure Active Directory Module for Windows PowerShell**

1. On the desktop, right-click the **Windows Azure Active Directory Module for Windows PowerShell** shortcut and click **Run as administrator**.
2. If a **User Account Control** dialog box appears, click **Yes**.
3. At the prompt, type the following command and press Enter:

```
Connect-msolservice
```

4. In the **Enter Credentials** dialog box, log in as **hleitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number) with a password of **Pa\$\$wOrd**.
5. At the prompt, type the following command and press Enter (where XXXX is your unique Lucerne Publishing number):

```
Add-MsolRoleMember -RoleName "Service Support Administrator" -RoleMemberEmailAddress "rtorres@lucernepublishingXXXX.onmicrosoft.com"
```

6. At the prompt, type the following command and press Enter (where XXXX is your unique Lucerne Publishing number):

```
Add-MsolRoleMember -RoleName "Billing Administrator" -RoleMemberEmailAddress "wdouglas@lucernepublishingXXXX.onmicrosoft.com"
```

7. At the prompt, type the following command and press Enter (where XXXX is your unique Lucerne Publishing number):

```
Add-MsolRoleMember -RoleName "Company Administrator" -RoleMemberEmailAddress "jmuller@lucernepublishingXXXX.onmicrosoft.com"
```

8. At the prompt, type the following command and press Enter:

```
$role = Get-MsolRole -RoleName "Service Support Administrator"
```

9. At the prompt, type the following command and press Enter:

```
Get-MsolRoleMember -RoleObjectId $role.ObjectId
```

10. Verify that **Rick Torres** is included in the list of users who have the **Service Support Administrator** role.

11. At the prompt, type the following command and press Enter:

```
$role = Get-MsolRole -RoleName "Billing Administrator"
```

12. At the prompt, type the following command and press Enter:

```
Get-MsolRoleMember -RoleObjectId $role.ObjectId
```

13. Verify that **William Douglas** is included in the list of users who have the **Billing Administrator** role.

14. At the prompt, type the following command and press Enter:

```
$role = Get-MsolRole -RoleName "Company Administrator"
```

15. At the prompt, type the following command and press Enter:

```
Get-MsolRoleMember -RoleObjectId $role.ObjectId
```

16. Verify that **Justin Muller** is included in the list of users who have the **Company Administrator** role.
17. At the prompt, type the following command and press Enter:

```
Exit
```

► Task 4: Testing Administrator Roles in Windows Azure Active Directory Module for Windows PowerShell

1. On LUC-CL1, open Internet Explorer and browse to <https://login.microsoftonline.com/>.
2. Sign in as **jmuller@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number), with the temporary password you recorded for his account in Lab 2.
3. When prompted, change his password to **Pa\$\$w0rd**.
4. If prompted, re-enter the new password, and click **Sign in**.
5. On the **Don't lose access to your account** page, in the **Country or region** box, select **Switzerland**.
6. In the **Mobile phone number** box, type **5551234**.
7. In the **Alternate email address** field, enter **username@outlook.com** (where username@outlook.com is the Windows Live address you registered in Lab 1A, Ex 1 Task 1).
8. Click **Save and continue**.
9. On the **Welcome** page, click **Admin** and then click **Office 365**.
10. In the top-right menu, click **Justin Muller**, then click **Sign out**.
11. On the desktop, right-click the **Windows Azure Active Directory Module for Windows PowerShell** shortcut and click **Run as administrator**.
12. If a **User Account Control** dialog box appears, click **Yes**.
13. At the prompt, type the following command and press Enter:

```
Connect-msolservice
```

14. In the **Enter Credentials** dialog box, log in as **jmuller@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number) with a password of **Pa\$\$w0rd**.
15. At the prompt, type the following command and press Enter (where XXXX is your unique Lucerne Publishing number):

```
Add-MsolRoleMember -RoleName "Service Support Administrator" -RoleMemberEmailAddress "rschmid@lucernepublishingXXXX.onmicrosoft.com"
```

16. At the prompt, type the following command and press Enter:

```
$role = Get-MsolRole -RoleName "Service Support Administrator"
```

17. At the prompt, type the following command and press Enter:

```
Get-MsolRoleMember -RoleObjectId $role.ObjectId
```

18. Verify that **Robert Schmid** is now included in the list of users who have the **Service Support Administrator** role.
19. At the prompt, type the following command and press Enter:

```
Exit
```

Results: The designated administrators have the access rights they require to carry out their roles.

Exercise 2: Configure Password Management

Scenario

Justin does not want Office 365 password resets to burden the Helpdesk; therefore, he is concerned about the approach that the team is taking to password management in Office 365. He works with Heidi to find out how easy the process is for resetting passwords on his own account.

In discussions with Remi, Justin and Heidi have decided to implement the same password policy in Office 365 as they have in the internal network; this involves a password lifetime of 90 days and a notification period of 14 days prior to the change. Heidi is tasked to set up this policy and to discover how the company can use Windows Azure Active Directory Module for PowerShell to set and manage user passwords.

The main tasks for this exercise are as follows:

1. Configuring the Password Expiration Policy
2. Resetting an Administrator Password
3. Managing Passwords and Password Policy with Windows PowerShell

► Task 1: Configuring the Password Expiration Policy

1. Open Internet Explorer and browse to <https://login.microsoftonline.com/>.
2. Sign in as **hleitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number) with a password of **Pa\$\$w0rd**.
3. In the **Office 365 admin center**, click **Admin**, then click **Office 365**.
4. On the left-hand side, click **Service settings**.
5. Click **Passwords**.
6. Under **Set the password expiration policy**, in the **Days before passwords expire** box, type **60**.
7. In the **Days before a user is notified that their password will expire** box, type **7**.
8. Click **Save**.
9. Verify that the message **Your password expiration policy has been saved** appears at the top of the page.

► Task 2: Resetting an Administrator Password

1. In the **Office 365 admin center**, on the left-hand side, click **Users** and then click **Active users**.
2. Double click **Justin Muller**.
3. In the **Justin Muller** page, click **Settings**.

4. In the **Alternate email address** box, type **username@outlook.com**, (where username@outlook.com is the Windows Live address you registered in Lab 1A, Ex 1 Task 1).
5. Click **Save**.
6. In the top-right menu, click **Heidi Leitner**, then click **Sign out**.
7. On the **Office 365** page, click **Use another account** (if showing) and then click **Can't access your account?**
8. On the **User verification** page, in the **User ID** box, type **jmuller@lucernepublishingXXXX.onmicrosoft.com**, (where XXXX is your unique Lucerne Publishing number).
9. Enter the characters in the picture, and click **Next**.
10. Click **Email**.
11. Open the email inbox for your **username@outlook.com** address (where username@outlook.com is the Windows Live address you registered in Lab 1A, Ex 1 Task 1) and look for an email message from **Microsoft Online Services**.
12. Enter the verification code that is included in the email message, and then click **Next**.
13. Click **Reset your password now** in the email message.
14. On the **Create a new password** page, type in and confirm **Pa\$\$w0rd** as your new password.
15. Click **Finish**.
16. On the **Reset your password** page, note the **Your password has been reset** message.
17. In Internet Explorer, go to **login.microsoftonline.com** and sign in to Office 365 as **jmuller@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number), with a password of **Pa\$\$w0rd**.
18. In the top-right menu, click **Justin Muller**, then click **Sign out**.

► Task 3: Managing Passwords and Password Policy with Windows PowerShell

1. On the desktop, right-click the **Windows Azure Active Directory Module for Windows PowerShell** shortcut and click **Run as administrator**.
2. If a **User Account Control** dialog box appears, click **Yes**.
3. At the prompt, type the following command and press Enter:

```
Connect-mso1service
```

4. In the **Enter Credentials** dialog box, log in as **hleitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number) with a password of **Pa\$\$w0rd**.
5. At the prompt, type the following command and press Enter (where XXXX is your unique Lucerne Publishing number):

```
Set-MsolPasswordPolicy -DomainName "lucernepublishingXXXX.onmicrosoft.com" -ValidityPeriod "90" -NotificationDays "14"
```

6. At the prompt, type the following command and press Enter (where XXXX is your unique Lucerne Publishing number):

```
Set-MsolUserPassword -UserPrincipalName "t1ancot@lucernepublishingXXXX.onmicrosoft.com" -NewPassword "L3tme!nNow"
```

- At the prompt, type the following command and press Enter:

```
Get-MsolUser | Set-MsolUser -PasswordNeverExpires $false
```

Results: Lucerne Publishing administrators can reset their passwords, and Heidi has verified that they can now use the Windows Azure Active Directory Module for PowerShell to set passwords and modify password policy.

Exercise 3: Administer Rights Management

Scenario

Jesse Wagner, the COO of Lucerne Publishing, and her husband James, the CEO, are both very concerned with the increasing attempts to plagiarize Lucerne Publishing's content. There is considerable interest in how Office 365 implements RMS protection to complement the existing RMS environment that operates internally. Heidi decides to do some experimentation; she plans to work with Rick Torres to use the Office 365 admin console and PowerShell to configure RMS, then view the results of applying RMS policies.

The main tasks for this exercise are as follows:

- Activating Rights Management in Office 365
- Activating Rights Management with Windows PowerShell
- Integrating Rights Management with Exchange Online
- Integrating Rights Management with SharePoint Online

► Task 1: Activating Rights Management in Office 365

- Open Internet Explorer and browse to <https://login.microsoftonline.com/>.
- Sign in as **hleitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number) with a password of **Pa\$\$w0rd**.
- In the **Office 365 admin center**, on the left-hand side, click **Service settings**.
- Click **Rights management**.
- Under **Protect your information**, click **Manage**.
- On the **Rights Management** page, click **Activate**.
- In the **Confirmation message** box, click **Activate**.
- Press F5 to refresh the page.
- On the **Rights Management** page, click **Deactivate**.
- In the **Confirmation message** box, click **Deactivate**.

► Task 2: Activating Rights Management with Windows PowerShell

- On LUC-CL1, open Internet Explorer and browse to <http://go.microsoft.com/fwlink/?LinkId=390869>.
- Click **Download**.
- Select the checkbox next to **WindowsAzureADRightsManagementAdministration_x64.exe** and click **Next**.
- If you receive a pop-up message, click **Allow once**.

5. Click **Save**, then click **Run**.
6. In the **User Account Control** box, click **Yes**.
7. In the **Welcome** page, click **Next**.
8. Accept the license terms, and click **Next**.
9. Click **Install**.
10. Click **Finish**.
11. Switch back to the Windows Azure Active Directory Module for Windows PowerShell session.
12. At the prompt, type the following command and press Enter:

```
Connect-mso1service
```

13. In the **Enter Credentials** dialog box, log in as `hleitner@lucernepublishingXXXX.onmicrosoft.com` (with a password of **Pa\$\$w0rd**).
14. At the prompt, type the following command and press Enter:

```
Import-Module aadrm
```

15. At the prompt, type the following command and press Enter:

```
Connect-aadrm service -Verbose
```

16. In the **Enter your credentials** dialog box, log in as **hleitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number), with a password of **Pa\$\$w0rd**.
17. At the prompt, type the following command and press Enter:

```
Enable-aadrm
```

18. At the prompt, type the following command and press Enter:

```
Disconnect-aadrm service
```

► Task 3: Integrating Rights Management with Exchange Online

1. At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command and press Enter:

```
Set-ExecutionPolicy RemoteSigned
```

2. Type **Y** to confirm and press Enter.
3. At the prompt, type the following command and press Enter:

```
$UserCredential = Get-Credential
```

4. Enter **hleitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number), with a password of **Pa\$\$w0rd**.
5. At the prompt, type the following command and press Enter:

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

6. At the prompt, type the following command and press Enter:

```
Import-PSSession $Session
```

7. At the prompt, type the following command and press Enter:

Important: In the following command, replace the “**eu**” (Europe) in the URL with “**na**” (North America) or “**ap**” (Asia Pacific), depending on your tenant’s current location in the world. Ask your instructor if you are not sure which location to use. Please note that Microsoft’s testing has found that on some occasions, the specified location does not work (for example, “na” may not work for a North American tenant). If this occurs, use either of the other two locations.

```
Set-IRMConfiguration -RMSOnlineKeySharingLocation “https://sp-
rms.eu.aadrm.com/TenantManagement/ServicePartner.svc”
```

8. At the prompt, type the following command and press Enter:

```
Import-RMSTrustedPublishingDomain -RMSOnline -name “RMS Online”
```

9. At the prompt, type the following command and press Enter:

```
Set-IRMConfiguration -InternalLicensingEnabled $True
```

10. At the prompt, type the following command and press Enter:

```
Test-IRMConfiguration -RMSOnline
```

You should receive a message that the IRM configuration has been correctly configured.

11. At the prompt, type the following command and press Enter:

```
Remove-PSSession $Session
```

12. In **Office 365 admin center**, logged in as **Heidi Leitner**, click **Outlook**.
13. Click **New**.
14. In the **To** box, type **Rick Torres**, and then click **Search Contacts & Directory**.
15. In the **Subject** box, type **RMS Test**.
16. Click **INSERT** and then click **Attachments or OneDrive files** from the drop-down menu.
17. Click **Computer**.
18. Browse to the **E:\Labfiles\Lab03\Sales Proposal.docx** file, and click **Open**.
19. Click **Send as attachment**.
20. Click the ellipsis (...) in the top menu, and point to **Set permissions**.
21. Click **Do Not Forward**.
22. Click **SEND**.
23. Repeat steps 13 to 22 to send the **Company Profile.docx** file to **Rick Torres** but this time choose the **Lucerne Publishing – Confidential View Only** template.

24. In the top-right menu, click **Heidi Leitner**, then click **Sign out**.
25. On the **Office 365** page, click **Use another account** and sign in as **rtorres@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number) with a password of **Pa\$\$w0rd**.
26. If the **Don't lose access to your account** page appears, then enter the following information:
 - a. In the **Country or region** box, select **Switzerland**.
 - b. In the **Mobile phone number** box, type **5551234**.
 - c. In the **Alternate email address** field, enter **username@outlook.com** (where username@outlook.com is the Windows Live address you registered in Lab 1A, Ex 1 Task 1).
 - d. Click **Save and continue**.
27. In the **Office 365 admin center** click **Outlook**.
28. If the **Outlook Web App** page appears, then enter the following information:
 - a. In **Language**, select your preferred display language.
 - b. In **Time zone**, select your local time zone.
 - c. Click **Save**.
29. Open the first email message from **Heidi Leitner**.
30. Note that the **FORWARD** option is greyed out.
31. Close that email message and open the second one from **Heidi Leitner**.
32. Note that the content is intended for internal users only and cannot be modified.
33. Close the email message.
34. In the top-right menu, click **Rick Torres**, then click **Sign out**.

► **Task 4: Integrating Rights Management with SharePoint Online**

1. On the **Office 365** page, sign in as **hleitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number) with a password of **Pa\$\$w0rd**.
2. In the **Office 365 admin center** click **Admin**, and then click **SharePoint**.
3. In the left-hand side, click **Settings**.
4. On the **Settings** page, in the **Information Rights Management (IRM)** section, select **Use the IRM service specified in your configuration**.
5. Click **Refresh IRM Settings**.
6. In the left-hand side, click **Site collections**.
7. Under **Site Collections**, click **http://lucernepublishingXXXX.sharepoint.com**, (where XXXX is your unique Lucerne Publishing number).
8. On the **Site Collection Properties** page, next to **Web Site Address**, click **http://lucernepublishingXXXX.sharepoint.com**, (where XXXX is your unique Lucerne Publishing number).
9. In the top ribbon, click **PAGE**, and then click **View All Pages**.
10. In **Pages**, on the ribbon, click the **LIBRARY** tab, and then click **Library Settings**.
11. Under the **Permissions and Management** column, click **Information Rights Management**.

12. On the **IRM** page, click the **Restrict permissions on this library on download** check box.
13. In the **Create a permission policy title** box, type **My RMS Policy**.
14. In the **Add a permission policy description** box, type **A test policy for RMS in SharePoint Online**.
15. Click **SHOW OPTIONS**.
16. Under **Set additional IRM library settings**, click **Do not allow users to upload documents that do not support IRM**.
17. Under **Configure document access rights**, click **Allow viewers to print**, and **Allow viewers to write on a copy of the downloaded document**.
18. Click **After download, document access rights will expire after these number of days**, and type **30** in the box.
19. Under **Set group protection and credentials interval**, click **Allow group protection. Default group**; and in the text box, type **Sales**, and then click **Sales Distribution** in the pop-up list.
20. Click **OK**.
21. Close Internet Explorer.

Results: Lucerne Publishing can better protect its confidential data throughout the organization.

Lab Discussion Questions

In the PowerShell sections, why did you need to run two separate connection commands in this lab?

Connect-MSOL connects to Office 365, whereas the second connection is to Exchange Online.

What is the purpose of downloading WindowsAzureADRightsManagementAdministration_x64.exe and importing the Azure Active Directory Rights Management (AADRM) module?

The AADRM module provides the cmdlets for managing Active Directory Rights Management in Office 365.

WindowsAzureADRightsManagementAdministration_x64.exe contains this module.

- In the PowerShell sections, why did you need to run two connection commands in this lab?
- What is the purpose of downloading WindowsAzureADRightsManagementAdministration_x64.exe and importing the aadrm module?

Module Review and Takeaways

Having completed this module, you can now manage the Office 365 administrator roles, manage passwords and password policies, and administer rights management in Office 365.

MCT USE ONLY. STUDENT USE PROHIBITED

Module 4

Planning and Managing Clients

Contents:

Module Overview	4-1
Lesson 1: Plan for Office Clients	4-2
Lesson 2: Manage User-driven Client Deployments	4-12
Lesson 3: Manage IT Deployments of Office 365 ProPlus	4-16
Lesson 4: Office Telemetry and Reporting	4-22
Lab: Managing Clients	4-28
Module Review and Takeaways	4-41

Module Overview

In this module, students learn how to plan for a client deployment and ensure that users get the tools they need to interact with Office 365™ effectively. This module covers the planning process, how to make Office 365 ProPlus directly available to end users, and how to deploy it as a managed package. Finally, this module covers how to set up Office telemetry so that administrators can keep track of how users are interacting with Microsoft® Office.

Objectives

After completing this module, you should be able to:

- Plan for deploying Office 365 clients.
- Prepare for user-driven client deployments.
- Prepare for managed IT deployments of Office 365 clients.
- Implement and use Office Telemetry with Office 365 clients.

Lesson 1

Plan for Office Clients

This lesson examines how to plan for an Office 365 client deployment. This includes planning for Microsoft Outlook®, the Lync® client, and Office Online. This lesson also covers the process of activation and revoking activation, and how activation relates to licensing. Finally, it covers the differences between click-to-run and Microsoft installer applications.

Lesson Objectives

After completing this lesson, you should be able to:

- List the types of Office 365 client software.
- Describe some of the important planning issues for Office 365 clients.
- Describe the key features and usage scenarios for Office 365 ProPlus.
- Describe the key features and usage scenarios for Office Online.
- Explain how Office 365 clients are licensed and activated.
- Describe the key technologies used for deploying Office clients.
- List some best practices for Office clients.

Introduction to Office 365 Clients

Depending on the Office 365 plan, there are several client packages that can be deployed to users.

Office 365 ProPlus

Office 365 ProPlus is a downloadable version of the Microsoft productivity suite, and includes Word® 2013, Excel® 2013, PowerPoint® 2013, Outlook® 2013, Access® 2013, Publisher 2013, OneNote® 2013, InfoPath®, and the Lync 2013 client.

Office 365 ProPlus supports streaming deployment, using Click to Run (C2R) technology; this enables users to click the application installation icon, and start using the application itself, while the program installs in the background. It is important to emphasize that, although an Internet connection is required during deployment, Office 365 ProPlus is installed and runs locally on the user's computer. Office 365 ProPlus is not a web-based version of Office, and users do not have to be permanently connected to the Internet to use it.

- Office 365 ProPlus
- SharePoint Designer, Visio, Project
- Office Online
- Office for Mac
- Office for iPad

SharePoint® Designer, Visio®, and Project

Some Office 365 plans also include SharePoint Designer, Visio and Project; these applications are not part of Office 365 ProPlus.



Note: SharePoint Designer 2013 is also available as a download from the Microsoft Download Center.

Office Online

There are also Office Online versions of Word, Excel, PowerPoint, and OneNote. Office Online is streamed from the cloud and cannot be used offline.

To use Office Online, users must be enrolled in an Office 365 plan that includes SharePoint Online.

Office for Mac 2011

Office for Mac 2011 can be downloaded from the service settings section of the Office 365 website. Office 2011 for Mac integrates with Office 365.

Office for iPad

The new Office for iPad app can be used to view, create, and edit documents on an iPad. This application can be installed from the App Store and consists of touch-friendly versions of Word, Excel, and PowerPoint. There is also a separate OneNote for iPad, as well as OWA for iPad, a SharePoint Newsfeed app, a OneDrive for Business client, and a Yammer app for iPad.

Planning for Office 365 Clients

The following issues should be taken into account when planning for Office 2013 client deployments.

Office Isolation

The Office C2R deployment technology provides very specific application isolation. Specifically, isolation is only applicable to previous versions of Office, and the virtual application packages used by Office 365 ProPlus still provide full communications with all other native applications.

- Office Isolation
- Office Customization Support
- Planning for Outlook
- Planning for Lync

Office Customization Support

When planning for Office 365 ProPlus deployment, it is important to note that C2R is designed to work with existing Office add-ins, customizations, and macros. This includes add-ins, Simple and Extended MAPI, ActiveX controls, and Browser Helper Objects. Office 365 ProPlus also works with legacy Office file formats.

Planning for Outlook

If Office 365 is being used with existing installations of Outlook 2010 or 2013, Outlook will need to be configured to enable access to Office 365 online services. However, when Office 365 ProPlus provides the Outlook client, users will just need to provide their Office 365 email address when first starting Outlook. Outlook should then be automatically configured for use with Office 365, provided that all the required DNS records have been set up.

Planning for Lync

When planning for a Lync deployment, it is important to determine whether dial-in conferencing must be available, and if so, which provider will be used, and which users must have access to the conference bridge.

Office 365 ProPlus

Office 365 ProPlus includes all the standard Office applications: Word 2013, Excel 2013, PowerPoint 2013, Outlook 2013, Access 2013, Publisher 2013, OneNote 2013, InfoPath, and the Lync 2013 client. Project Pro for Office 365 and Visio Pro for Office 365 are not part of Office 365 ProPlus; they are licensed separately and are available as separate applications for some Office 365 subscription plans. SharePoint Designer is also available for deployment with particular plans. Office 365 ProPlus is licensed per user, not per computer, and permits Office to be used on up to five PCs or Macs, as well as on mobile devices.

- Office 365 ProPlus vs. Office 2013 Professional Plus
- Office 365 ProPlus System requirements
- Internet requirements

Office 365 ProPlus vs. Office 2013 Professional Plus

While Office 365 ProPlus includes the standard Office applications, there is a basic difference between it and Office 2013 Professional Plus. Office Pro Plus is the desktop version of Office. It is installed in the traditional way (through an MSI) from volume license (VL) media and requires a VL product key. Office Professional Plus is the full desktop-installed version of Office and includes Office Online in the license. It does not use Click-to-Run, so installations are not streamed, and updates are not automatically pushed out to the applications.

Office 365 ProPlus System requirements

The Office (365) ProPlus System Requirements include:

Component	Requirement
Computer and processor	1 gigahertz (GHz) or faster x86- or x64-bit processor with SSE2; Intel processor (Mac).
Memory	1 GB RAM (32-bit or Mac) /2 GB RAM (64-bit).
Hard disk	3.0 GB of available disk space (PC); 2.5 GB HFS+ hard disk format (Mac).
Display	1366x768 minimum resolution.
Operating system	Windows Server 2008R2, Windows 7, Windows Server 2012, Windows 8; Mac OS X 10.6 or later (Mac).
Graphics	Graphics hardware acceleration requires a DirectX 10 graphics card with 1366x768 resolution.
Browser	Microsoft Internet Explorer 8, 9, or 10; Mozilla Firefox 10.x or a later version; Apple Safari 5; or Google Chrome 17.x.
Network	Internet functionality requires an Internet connection.

Internet requirements

Users must be able to connect to Office Licensing Service through the Internet at least once every 30 days.

The following list identifies the ports, protocols, and URLs that Click-to-Run for Office 365 uses for downloads, installation, automatic updates, subscription maintenance, and activation:

- *Download and installation from the portal; Automatic updates.* TCP (80), target URL: <http://officecdn.microsoft.com>.
- *Subscription maintenance.* TCP (443), target URL: <https://ols.officeapps.live.com/olsc>.
- *Office 365 ProPlus activation.* TCP (443), target URL: <https://activation.sls.microsoft.com>.
- *Office 365 ProPlus activation.* TCP (80), target URLs: <http://crl.microsoft.com/pki/crl/products/MicrosoftProductSecureCommunicationsPCA.crl>, <http://www.microsoft.com/pki/crl/products/MicrosoftProductSecureCommunicationsPCA>.



Note: These URLs are not end-user accessible and will generate 403 Access Denied errors.

Office Online

Office Online provides an alternative way to use Office applications online. Office Online is either streamed from Office 365 or from on premises servers (not covered in this course), and requires Internet or network access; Office Online cannot be used offline.

To use Office Online, users must be enrolled in an Office 365 plan that includes SharePoint Online. The following Office Online apps are available for viewing and editing documents online:

- Microsoft Excel Online
- Microsoft OneNote Online
- Microsoft PowerPoint Online
- Microsoft Word Online

- Office Online overview
- Using Office Online
- Office Online versus Office 365 ProPlus/Office 2013 Professional Plus
- Office Online save locations
- System requirements

Strictly speaking, Outlook Web App is not an Office Online App; Outlook Web App provides online access to email through the Office 365 webmail site. Similarly, the Lync Web App and the Project Web App may be available, depending on the subscription plan.

The Outlook Web App supports attachment viewing, and can convert documents and PDF files into HTML for read-only viewing in a web browser window, or convert PDFs into Word document format. The Outlook Web App can interoperate with Lync Online and Lync Server on-premises to provide users with instant messaging (IM) and presence within the Outlook Web App interface, and can also display users' photos, as stored in Active Directory®, within the interface.

Using Office Online

Office Online apps are launched by selecting a document to view or edit from the OneDrive page in the Office 365 portal, or from locally-hosted enterprise versions of the Office web apps on a SharePoint 2013 site. Selecting a document automatically starts the Office Online App that is associated with the file. Office Online includes commonly-used edit functions. To access more advanced features, users must either edit the document in an already existing Office installation, such as Office 365 ProPlus.

Office Online vs. Office 365 ProPlus/Office 2013 Professional Plus

Office Online provides a subset of the full feature set available in Office 365 ProPlus and Office 2013 Professional Plus; however, this subset does include all the most commonly-used editing and formatting features.



For information on the differences between using a document in the browser and in Word, see the following link:

<http://go.microsoft.com/fwlink/?LinkId=400799>



For information on the differences between using a notebook in the browser and in OneNote, see the following link:

<http://go.microsoft.com/fwlink/?LinkId=400798>



For information on feature support in PowerPoint Online App, see the following link:

<http://go.microsoft.com/fwlink/?LinkId=390874>



For information on the differences between using a workbook in the browser and in Excel, see the following link:

<http://go.microsoft.com/fwlink/?LinkId=390875>

Office Online Save Locations

Office Online apps differ slightly in their default save behaviors:

- *Word Online.* Documents must be manually saved, as there is no auto-save feature. Documents can be saved locally.
- *Excel Online.* Worksheets must be manually saved; the download command is used to send a copy to the local computer.
- *OneNote Online.* If a OneNote notebook is saved to a SharePoint document library, then the OneNote notebook is online. This allows the notebook to be shared by sending a link instead of an email attachment. By clicking the link, recipients can read notes in their web browser.
- *PowerPoint Online.* All changes are automatically saved; there is no Save command. To download a copy, the user must have the Microsoft PowerPoint desktop app. If the presentation is saved in a SharePoint document library, then the presentation is online and it can be shared by sending a link instead of an email attachment. Recipients with proper permissions can view it in their web browser or mobile device.



For more information on Office Online save locations, see the following link:

<http://go.microsoft.com/fwlink/?LinkId=400797>

System requirements

Office Online requires a browser that supports HTML 5 and JavaScript 5, such as:

- Internet Explorer 9 with at least MS12-037: Cumulative Security Update for Internet Explorer: June 12, 2012 installed
- Internet Explorer 10 or later (strongly recommended)
- At least Mozilla Firefox 12
- At least Apple Safari 5
- At least Google Chrome 18



For more information on browser requirements, see the following link:

<http://go.microsoft.com/fwlink/?LinkId=400795>

Office 365 ProPlus Licensing and Activation

In order to install Office 365 ProPlus, each user must have:

- An Office 365 user account and password, to sign in to Office 365.
- An Office 365 license, which must be assigned to the user by the organization's administrator.

An Office 365 license is assigned to a specific user, but a single Office 365 license enables a user to deploy Office 365 ProPlus on up to five different computers. The user manages these installations in the Office 365 portal, and can deactivate Office 365 on a specific device, if necessary.

- User requirements
- Licensing and activation process
- Reduced functionality mode

Licensing and activation process

As part of the installation process, Office 365 ProPlus communicates with the Office Licensing Service and the Activation and Validation Service to obtain and activate a product key. Each day, or each time the user logs on to their computer, it connects to the Activation and Validation Service to verify the license status and extend the product key. As long as the computer can connect to the Internet at least once every 30 days, Office remains fully functional. If the computer goes offline for more than 30 days, Office enters reduced functionality mode until the next time a connection can be made. To get Office fully functional again, a user can simply connect to the Internet and let the Activation and Validation Service reactivate the installation.

The activation status can be checked within Office applications by clicking **File** (to go to the **Backstage** view) and then clicking **Account**. If "Product Activated" appears on the page, the Office Subscription license is successfully activated. If Office 365 Professional Plus is already running when activation occurs, the Backstage view may not reflect the licensed status. In this case, the Office application will need to be restarted in order to see the updated license status.

Office 365 administrators cannot see which computers a user has installed Office on and cannot deactivate an Office installation on a user's computer. However, administrators do control the assignment of Office 365 licenses to users. Therefore, when a user leaves an organization, an administrator can re-

assign that user's Office 365 license to a different user, and any of that user's Office installations will end up in reduced functionality mode.

Reduced functionality mode

If a user attempts to install Office 365 ProPlus on a sixth computer, they will need to deactivate one of the first five installations. Office 365 ProPlus will then go into reduced functionality mode on the deactivated computer. Office 365 ProPlus also enters reduced functionality mode if the administrator revokes the user's license to use ProPlus from the portal, or if the Office 365 subscription expires.

In reduced functionality mode, Office 365 ProPlus remains installed on the computer, but users can only view and print their documents. All features for editing or creating new documents are disabled, and the user sees a message with the following options to reactivate:

- Enter product key
- Sign in to O365

As long as the Office 365 subscription is current and the user has been granted a license, the user can then choose one of the available options to reactivate Office 365 ProPlus on that computer.

Office 365 Deployment Overview

The deployment methods discussed in this topic can be used with whichever applications are included with the Office 365 subscription. Note, however, that this topic specifically covers Office 365 ProPlus; on-premises deployment of Office Online to the organization's own SharePoint Online servers is not covered in this course.



Note: Due to its online activation requirement, Office 365 ProPlus is unable to be deployed to computers that cannot or do not have an Internet connection. For disconnected computers, Office Professional Plus 2013 and a traditional activation method, such as Key Management Service (KMS) or Active Directory Domain Services, should be deployed.

- Deployment and Bandwidth Planning
- Removing previous versions
- User Communications and Guidance
- Deployment Methods
- Benefits of C2R
- C2R technology
- Limitations of C2R

Deployment and Bandwidth Planning

The Office 365 ProPlus desktop setup must be run on each computer. If setup is initiated without first installing any necessary operating system service packs and updates, a significant amount of download bandwidth may be taken up as each computer separately connects to the Internet, then downloads, and installs service packs or updates. To prevent bandwidth saturation, updates should be deployed prior to deploying the Office 365 ProPlus setup. A package deployment tool, such as Microsoft System Center Configuration Manager, should also be used so that updates are only downloaded once, but are then distributed as part of a planned and scheduled deployment.

If updates cannot be deployed prior to Office 365 ProPlus setup, Active Directory group policy can be used to throttle the deployment of the Office 365 ProPlus by deploying the setup package to a subset of users at a time, such as by OU or site/location. In this way, although updates are being downloaded by all users, the download activity is spread across days or weeks.

Removing Previous Versions

As part of deployment planning, it is important to consider how to remove any previous Office versions or previous installations; for example, when Office 2013 Professional Plus is being replaced with Office 365 ProPlus.

Microsoft Office 2013 suites or Office 365 Home Premium can be automatically removed using a Fix it, through the Windows Control Panel, or manually.

 **For more information, see the Uninstall Microsoft Office 2013 or Office 365 page on Microsoft Support at the following link:**

<http://go.microsoft.com/fwlink/?LinkId=390878>

User Communications and Guidance

As part of deployment planning, it is essential to maintain active communications with users. These communications include advanced notices of planned deployments of Office 365 ProPlus, help and guidance on using Office 365 ProPlus, and links and pointers to resources and learning tools.

If users are expected to use some form of self-service to install Office 365 ProPlus, additional information will also be required, such as:

- Informing users of the download location to use for Office 365 ProPlus setup, as this location varies, depending on the Office 365 subscription plan (for example, E1 vs. E3).
- Using correct wording in all communications – for example, depending on subscription level, users may be accessing the "Office 365 Portal" or the "Office 365 Admin Center".
- Pointing out to advanced users that Office 365 ProPlus uses C2R, and that users should not use any existing VL media location that they may have in the past to self-service install Office 2013 Professional Plus or prior versions.

This information is covered in greater detail in the next lesson.

Deployment Methods

The two most common ways in which Office 365 ProPlus is deployed to users include:

- User-driven (self-service) installation of Office 365 ProPlus directly from the Office 365 portal. This type of deployment is described in Lesson 2 of this module.
- Managed deployments, by first downloading the Office 365 ProPlus software to the local network and then push deploying it to users. This type of deployment is described later in this module.

Office 365 ProPlus could also be deployed by users starting an installation from media in a network share. Office 365 ProPlus can also be deployed using application virtualization, although this method is beyond the scope of this course.

Office 365 ProPlus uses C2R technologies for deployment. C2R is now the default installation technology for Office 2013 Professional Plus, except for Volume Licensed editions. Volume Licensed Office 2013 Professional Plus and older Office versions use MSI-based deployment and support the following options:

- User-driven deployment from Volume Licensed media in a network share
- IT managed deployments
- Application virtualization
- Presentation virtualization (Office 365 ProPlus does not support this option, as C2R installations are not supported in such environments)

C2R supports both user-driven self-service "pull" installations, and managed "push" installations using software distribution tools such as System Center Configuration Manager, Windows Intune™, third-party software distribution, Group Policy login scripts, and scripted installation.

Benefits of C2R

With C2R, the time to first launch an Office application is about two minutes; by contrast, MSI-based installations may take 30 minutes or more to complete. C2R's fast launch time is because the Office payload is streamed from the installation source, and parts of this can be used before the entire payload is streamed. Additional features are then downloaded as required.

Office 365 ProPlusC2R is tightly integrated with Office 365, and provides for five simultaneous installations per user, through user-based activation. Because the source binaries are kept patched in the cloud, Office 365 ProPlusC2R is up-to-date from the start and this is maintained automatically; there is no need to download and install updates manually. C2R also enables the roaming of Office settings, such as recent files, and custom dictionaries.

By contrast, during the 30 minutes that it takes MSI-based installations to complete, users are unable to use any of their Office applications; service packs and updates will then need to be installed. Using MSI requires KMS or MAK management for activations – these are tied to a device rather than being user-based.

C2R technology

Click-to-Run uses Dynamic Feature Prioritization with App-V technology; the first 5-10 percent of the download is the App-V agent, and after the agent is ready, Office shortcuts appear on the desktop. By clicking a shortcut, such as **Word 2013**, the main Word features are then downloaded immediately. If more specific features are requested that have not yet been downloaded (such as mail merge), Click-to-Run will stream these on demand.

Click-to-Run is based on App-V technology, but does not require an App-V infrastructure or MDOP. The enhanced App-V in Click-to-Run enables other applications, ActiveX controls, add-ins, and Office Online apps to integrate with Office. End users will not see any difference in how Office interacts with other software on their computer. However, while other applications can fully integrate with Office, Click-to-Run is isolated enough to support side-by-side Office. This feature means Office 365 ProPlus can coexist with Office 2003, 2007, or 2010.



Note: Previous versions of App-V isolated the application against the operating system and against other applications; as a result, an App-V deployment of Office 2010, for example, would not be able to work with a Line of Business (LoB) application.

Limitations of C2R

C2R must authenticate with Office 365, requiring the computer to be able to connect to the Internet during deployment, for activation, and periodically after that to maintain activation. Therefore, C2R is not appropriate in every scenario. For example, C2R cannot be used in "session sharing" environments (such as Terminal Services, Remote Desktop Services, or Citrix XenApp), as Office subscription media is user-based, and this would allow a license that is installed for one user to be used by multiple users. To use Remote Desktop Services, you must use a volume license version of Office Professional Plus 2013, which is available from the Volume Licensing Service Center (VLSC). You can deploy Office 365 ProPlus to a virtual desktop, but that must be assigned to a single user.

Click-to-Run also requires administrative rights during installation; if this requirement cannot be met, a volume license version of Office Professional Plus 2013 must be deployed using a software distribution

method such as System Center Configuration Manager, where the agents used run within the system context of the local computer.

Best Practices for Office 365 Clients

Obstacles to a successful client deployment include incomplete data, custom application incompatibilities, and not gathering enough or important information from existing implementations and running into compatibility issues later.

When preparing an Office 365 client deployment, best practices include:

- Planning
- Consulting
- Strategy for installation/uninstallation of Office
- End-user training and user communication
- Training for help desk/desktop support staff

- Planning
- Consulting
- Strategy for installation/uninstallation of Office
- End-user training and user communication
- Training for help desk/desktop support staff

Discussion: How should Lucerne Publishing be deploying Office to users?

Based on the Lucerne Publishing scenario, how do you think Lucerne Publishing should deploy Office to its users?

- Which Office clients to use?
- Which deployment methods to use?
- How to manage activation and licensing?

- Based on the Lucerne Publishing scenario, how do you think Lucerne Publishing should deploy Office to its users?
 - Which Office clients to use?
 - Which deployment methods to use?
 - How to manage activation and licensing?

Lesson 2

Manage User-driven Client Deployments

In this lesson, you will learn how to control the self-service provision of Office 365 ProPlus and other apps that work with Office 365, such as Windows Store Apps, and Mobile Apps.

Lesson Objectives

After completing this lesson, you should be able to:

- Describe the user-driven (self-service) process for deploying Office 365 clients.
- Explain how to manage and control user-driven client deployments.
- Describe some important considerations for user-driven client deployments.
- List some best practices for user-driven client deployments.

Introduction to User-driven Deployment

User-driven (self-service) installation from the Office 365 portal is where Click-to-Run is initiated by the user by logging on to the Office 365 portal, and then selecting **Install Software**. This approach does not require much administrative setup, but provides for limited control over the deployment (by contrast with managed deployments). For example, administrators cannot control where computers users install Office 365 ProPlus, but they can disable all Office 365 ProPlus deployments for a specific user.

In a user-driven deployment:

- Office is always streamed from the Internet to the computer; local source locations are not supported.
- Users must have an Office 365 account and be provisioned for ProPlus.
- Users must have administrative rights to the local computer.
- Office 365 ProPlus installs Office 365 updates automatically in the background from the Internet; this behavior cannot be changed.

User-driven deployments:

- Office is always streamed from the Internet
- Users must have an Office 365 account and be provisioned for ProPlus
- Users must have administrative rights to the local computer
- Office 365 ProPlus installs updates from Office 365 automatically in the background from the Internet

Managing User-driven Deployments

For user-driven deployments of Office 365 ProPlus, there are limited management options. Users can be prevented from installing Office 365 ProPlus from the Office 365 portal; this can be useful if the organization's policy is to deploy Office 365 ProPlus from an on-premises location in a managed deployment.

Similarly, administrators cannot control whether users install the 32-bit or 64-bit version of Office 365 ProPlus in a user-driven deployment. The 32-bit version is recommended, even on computers that have 64-bit operating systems. If users are installing from the Office 365 portal, it is important that they are clearly instructed on which version to install.

User software page:

- Office and Lync
- SharePoint Designer

Controlling specific application:

- AppLocker policies
- Microsoft Application Virtualization (App-V) 5.0

 **For more information on 64-bit editions of Office 2013, refer to the following page:**

<http://go.microsoft.com/fwlink/?LinkId=390879>

Controlling application deployment

Office 365 administrators can use the **user software** page in the Office 365 admin center to control whether or not users can install Office software from the Office 365 portal. For example, depending on the subscription plan, an administrator could permit users to install Office 365 ProPlus packages (Word, Excel, and PowerPoint), but not Visio. It is important to note, however, that this setting applies to all users. If an administrator disables Office software installations for users, they will see the following message on their software page:

The administrator has disabled Office installations. Contact your administrator for information about how to install Office.

Office 365 ProPlus installs as one package and, from the portal, it is not possible to select particular applications, such as Word and PowerPoint – but not Access. If an administrator wants to control installations down to application level, there are two options:

- AppLocker policies can be used to prevent a Click-to-Run application from running.
- Microsoft Application Virtualization (App-V) 5.0 can be used to customize the Office 365 configuration, so that only specific apps are included.

Considerations for User-driven Deployments

When planning for user-driven deployments, it is important to consider typical obstacles to success. These obstacles include the following.

- Users do not have admin rights – this is a requirement of user-driven deployment.
- Bandwidth limitations during deployment that prevent success streaming of Office 365 ProPlus binaries.
- Incorrect licenses that prevent successful user activation.
- Windows XP requires SP3 and the Windows Update Agent; otherwise, Office 365 ProPlus setup fails.

- Obstacles to success
- Office for Mac
- Mobile devices

Office for Mac

When Mac users select software deployment, Office for Mac 2011 can be downloaded and installed. For PC users, this software can be installed on up to five computers. Also keep in mind that Office Online is fully supported on Macs, as long as the browser requirements are met. Office 365 can also be used with existing Microsoft Office for Mac 2011 Service Pack 3, and Microsoft Office 2008 for Mac 12.2.9 Update or a later version with Microsoft Entourage 2008 for Mac, Web Services Edition.

Mobile devices

Office 365 can be used on a wide range of mobile devices, including phones and tablets. Office Online is available for Surface with Windows RT, Windows Phone, iPhone, iPad, with light versions available for Android phones, BlackBerry devices, and Nokia (Symbian OS). Surface with Windows RT, and Windows Phone devices also include built-in Office apps. Users can use Office 365 on up to five mobile devices and five PCs.



There is a new version of Office for iPad. For more information, see the following link:

<http://go.microsoft.com/fwlink/?LinkId=400796>



The following page compares how different mobile devices work with Office 365:

<http://go.microsoft.com/fwlink/?LinkId=390880>

Best Practices for User-driven Deployments

The chances for a successful user-driven deployment can be jeopardized when there is lack of planning or testing, deploying the incorrect plan, or not understanding what happens when you revoke a license.

Best practices for successful user-driven deployments include:

- Setting up a communication package to inform users of a new version of Office and how to use it.
- Planning, planning, planning.
- Specifying the platforms and devices that will be supported.
- Deploying the plan – who the plan will be rolled out to, when, and so on.
- Creating a proper training plan for Office.

- Setting up a communication package to inform users of a new version of Office and how to use it
- Planning, planning, planning
- Specifying the platforms and devices that will be supported
- Deploying the plan – who the plan will be rolled out to, when, and so on
- Creating a proper training plan for Office

Lesson 3

Manage IT Deployments of Office 365 ProPlus

In this lesson, students learn how to manage an Office 365 ProPlus deployment, manage streaming updates, use the Office deployment tool, and customize the Office 365 deployment.

Lesson Objectives

After completing this lesson, you should be able to:

- Describe the process for deploying Office 365 clients using a managed approach.
- Describe how to use the Office Deployment Tool.
- Explain how Group Policy is used to enable managed client deployments.
- Describe how client software updates are managed.
- Describe some important considerations for managed client deployments.
- List some best practices for managed client deployments.

Introduction to Managed Deployments

In a managed deployment, the Office 365 ProPlus software is first downloaded to the local network, and then some form of push mechanism is used to deploy it to users. The following software distribution tools are examples of mechanisms that can be used to manage "push" installations:

- System Center Configuration Manager
- Windows Intune
- Third-party software distribution
- Group Policy login scripts
- Scripted installation

Software downloaded to local network, then distributed through any of the following tools:

- System Center Configuration Manager
- Windows Intune
- Third party software distribution
- Group Policy login scripts
- Scripted installation

Office Deployment Tool:

- Configuration.xml
 - Group Policy
- (Office Customization Tool (OCT) not used)

In the lab for this module, Group Policy computer startup scripts are used to deploy Office 365 ProPlus. However, similar command-lines and scripts can also be used as part of an Electronic Software Distribution (ESD), and can be built in to System Center or Microsoft Deployment Toolkit (MDT) task sequences.

Whatever mechanism is used, it is important to remember that C2R installations must be run as local admin. For example, in the case of Group Policy startup scripts, they must be run from the computer context and not the user context.

Performing Managed Deployments

For Click-to-Run, all configuration of the Office client is performed through Group Policy. The Office Customization Tool (OCT), as used with VL-licensed Office 2013 Professional Plus media, is not used. Instead, C2R is managed using the OCT, which is configured using the following tools:

- *Configuration.xml*. To customize the deployment experience.
- *Group Policy*. To manage all other Office settings.

Office Deployment Tool

The Office Deployment Tool (ODT) is downloadable from the Office 365 admin center, or directly from Microsoft Download Center.

ODT is used to:

- Download Office source files (source URL: <http://officecdn.microsoft.com>).
- Install or remove Click-to-Run/customize installations.
- Apply software update policies.

ODT supports three command-line switches:

- **/download** **<path to configuration.xml>** to specify the download.
- **/configure** **<path to configuration.xml>** to specify the Office source file location.
- **/packager** to prepare Office source files so that Click-to-Run can be used in an App-V infrastructure.

The ODT process involves the following key steps:

1. Edit Configuration.xml to specify the Office 365 software to download, such as Office 365 ProPlus, and Visio, and to specify the shared location to use.
2. Use ODT with the download option to place source files in a software distribution infrastructure; for example, **setup.exe /download \\LUC-SV1\Office15\Configuration.xml**.
3. Use ODT with the configure option to deploy the Office download tool and the configuration file to clients; for example, **setup.exe /configure \\LUC-SV1\Office15\Configuration.xml**.
4. When the ODT is executed by client machines, ODT reads the configuration file, and then streams C2R from the specified location (for example, where the source files were downloaded internally).



Note: It is the ODT and not the Office source files that are deployed using this method. The ODT is a 1 MB executable.



For more information on the ODT, see Office Deployment Tool for Click-to-Run at the following link:

<http://go.microsoft.com/fwlink/?LinkId=390881>



For more information on configuration.xml options, see Reference for Click-to-Run configuration.xml at the following link:

<http://go.microsoft.com/fwlink/?LinkId=390882>

```
<Configuration>
<Add SourcePath="\\Server\Share\Office*" OfficeClientEdition="32" >
  <Product ID="O365ProPlusRetail">
    <Language ID="en-us" />
  </Product>
  <Product ID="VisioProRetail">
    <Language ID="en-us" />
  </Product>
</Add>

<Updates Enabled="TRUE" UpdatePath="\\Server\Share\Office*" />

<Display Level="None" AcceptEULA="TRUE" />

Logging Name="OfficeSetup.txt" Path="%temp%" />

<Property Name="AUTOACTIVATE" Value="1" />
</Configuration>
```

Using Group Policy to Configure Deployments

Group Policy is used to manage general Office settings, as well as application-specific settings such as managed add-ins. At the Office level, group policy is used to control the user's first run experience (FRE), or to remove all FRE features for "no prompt" deployment, as in the following example:

User Configuration\Administrative Templates\Microsoft Office 2013\First Run:

- Disable First Run Movie - **Enabled**
- Disable Office First Run on application boot - **Enabled**


Group Policy:

- General Office settings
- Application-specific settings

User Configuration\Administrative Templates\Microsoft Office 2013

User Configuration\Administrative Templates\Microsoft Office 2013\Privacy\Trust Center:

- Disable Opt-in Wizard on first run - **Enabled**
- Enable Customer Experience Improvement Program - **Disabled**
- Allow, including screenshot with Office Feedback - **Disabled**
- Send Office Feedback - **Disabled**
- Automatically receive small updates to improve reliability - **Disabled**

 **For more information on policy settings, see Group Policy Administrative Template files (ADMX, ADML) and Office Customization Tool (OCT) files for Office 2013.**

<http://go.microsoft.com/fwlink/?LinkId=390883>

Managing Updates

C2R uses an optimized software update model that provides unobtrusive background updates. The first consequence of this model is simpler and smaller updates. Every month, on "Patch Tuesday" (the second Tuesday of the month), an updated Office build is released, comprising a full set of source files. Unlike with traditional MSI-based installations, separate security fixes, private hotfixes, cumulative updates, and service packs will not be provided. The updated full set of source files is used for new installations; for existing installations, during the update process, the client performs a delta comparison between the current and updated build, and only the deltas are downloaded.

The second consequence of this model is that users are not impacted, even if they are using an Office application when an update is being performed. When they close and reopen the Office application, they will automatically be using the newer build.

Optimized software update model:

- Smaller updates
- Background updates

Update options:

- Automatic from cloud
- Automatic from network
- Rerun setup.exe using ESD

Using Configuration.xml file to manage updates


Update options

Updating options include:

1. *Automatic from cloud.* This is the default mode (typically used for home or small office installations) where updates are downloaded from the cloud. A daily task checks for updates, and when a new build is available, the client automatically receives the deltas.
2. *Automatic from network.* In managed deployments, administrators can specify (using group policy or the configuration.xml file during setup) to check for updated builds from an internal source; this is typically used in small/medium organizations.
3. *Rerun setup.exe using ESD.* In large organizations, using an ESD such as Configuration Manager enables even more fine-grained control of update scheduling. Scripts or task sequences in the ESD are used to re-execute "setup.exe /configure," again comparing the current version with the source (defined in the SourcePath attribute in the config.xml) and only install deltas. Using an ESD, administrators can specify how many users receive a new build in a given time period.

Options 2 and 3 enable administrators to control when users receive updated builds. For these two options, a best practice is to initially download the updated build to a test share, and to apply updates to test/pilot machines only (as these computers are configured to get updates from \\Server\Testing\$, for example).

After the testing period, the updated build is moved to a production update share, and to automatically update production machines (as they are configured to get updates from \\Server\Production\$, for example).

 **Note:** Although administrators can choose not to receive updates, it is important to note that clients can only be on an "outdated" build for 12 months. After 12 months, clients will need to download a newer build to be covered by Microsoft support.

Using Configuration.xml file to manage updates

Administrators can configure update behavior by using the ODT configuration.xml file options. For example:

```
<Updates Enabled="TRUE" UpdatePath="\\Server\Share\Office\" />
```

- *Enabled.* If set to TRUE (default), C2R will automatically detect, download, and install updates.
- *UpdatePath.* Used to specify a network, local, or HTTP path for a C2R installation source to use for updates. If not set, or set to "default", the Microsoft C2R source on the Internet will be used.
- *TargetVersion.* Can be used to set a specific product build number, for example, 15.1.2.3, that will be updated in the next update cycle. If not set or set to "default," C2R will update to the latest version advertised at the C2R source.

Considerations for Managed Deployments

When planning for managed deployments, it is important to consider typical obstacles to success. These obstacles include the following:

- *Users do not have admin rights.* This is a requirement of managed deployments.
- *Bandwidth limitations during deployment.* Prevents success streaming of Office 365 ProPlus binaries.
- *Incorrect licenses.* Prevents successful user activation.
- *Windows XP.* Requires SP3, and the Windows Update Agent; otherwise Office 365 ProPlus setup fails.
- *Lack of IT expertise in enterprise software deployment.* Tools such as Group Policy and System Center Configuration Manager need to be fully understood before being used as part of enterprise Office 365 client rollouts.

- Users do not have admin rights
- Bandwidth limitations during deployment
- Incorrect licenses
- Windows XP issues
- Lack of ESD expertise

Best Practices for Managed Deployments

Things can go wrong when there is lack of planning, or testing, perhaps leading to installations flooding the network. Issues can also arise when incorrectly specifying 64-bit versus 32-bit Office, or when compatibility issues of Office with other apps have not been properly tested; or issues such as with Office templates (for example, Word 95 template does not work with Office 2013). Where users do not all use the same first language, it is also easy to overlook the steps needed to ensure that each user has access to software in their preferred language.

- Proper planning and design and testing
- User acceptance testing (piloting)
- Awareness program of the new app
- Have a proper training plan for Office



Note: It is important to prepare a thorough support plan for users, to help guide them through the transition to Office 365 applications.

Best practices for managed deployments include:

- Proper planning, design and testing.
- User acceptance testing (piloting).
- Awareness program of the new app.
- Have a proper training plan for Office.

Discussion: Planning for a Managed Office 365 Deployment

Based on the Lucerne Publishing scenario, what factors should Lucerne Publishing take into account when planning for a managed Office deployment?

- Software distribution tool(s) to use?
- Group Policies to create?
- Office configuration(s) to use?
- How to manage updates?

- Based on the Lucerne Publishing scenario, what factors should Lucerne Publishing take into account when planning for a managed Office deployment?
 - Software distribution tool(s) to use?
 - Group Policies to create?
 - Office configuration(s) to use?
 - How to manage updates?

Lesson 4

Office Telemetry and Reporting

In this lesson, students learn how to set up the telemetry service, enable telemetry through Group Policy, report user issues, and deploy the telemetry agent.

Lesson Objectives

After completing this lesson, you should be able to:

- Describe Office Telemetry and how it is used with Office 365 clients.
- Explain how to install and configure Office Telemetry for use with Office 365 clients.
- Describe how to use Office Telemetry data.
- Describe some important considerations for using Office Telemetry.
- List some best practices for deploying and using Office Telemetry.

Introduction to Office Telemetry

Office Telemetry provides inventory, usage, and monitoring tools for Office 2013, Office 2010, Office 2007, and Office 2003. Data is collected whenever a monitored document is opened, edited, or closed. This data can then be aggregated in a central database for reporting and viewing. Data can be viewed using an Excel solution, the Telemetry Dashboard, and through the Telemetry Log.

For Office 2013 applications, records may also be created if certain error situations occur, including a description of the problem and a link to more information.

Office Telemetry is built into Office 2013, and, if data collection is enabled, information about installed add-ins, the most recently-used documents, and application event data will be sent to the telemetry database. However, for Office 2003, Office 2007, and Office 2010, an agent must first be deployed; this agent collects information about add-ins and recently-used documents, but does not provide application event data.

What is Office Telemetry Used For?

A key function of Office Telemetry is to help when planning an upgrade to Office 365 ProPlus. By deploying agents to computers running existing Office editions, data can be collected to provide inventory information, and to identify the business-critical Office documents and solutions in the organization. These solutions should then be prioritized for compatibility testing with ProPlus.

Collecting this data prior to an Office 365 ProPlus rollout provides the information needed to help with capacity planning, and to ensure that ProPlus network and storage performance will be within acceptable limits.

Office Telemetry can also be used post-ProPlus rollout to monitor performance against targets, and to identify errors and problems with Office solutions.

- What is Office Telemetry Used For?
- Telemetry operations
- Telemetry management

Telemetry operations

Before data collection can begin, Office Telemetry client functionality, whether built into Office 2013 or deployed to previous versions of Office, must be enabled through Group Policy or by editing the local registry. Data collection runs as a scheduled task and requires domain membership.

Office client data is first sent to a shared folder on the network (it cannot be stored in the cloud); this folder must be accessible to all clients and users. The Office Telemetry processing service, known as the Office Telemetry Processor, runs on a domain-joined Windows Server 2008 or later computer; this service then reads the data and sends it to the Office Telemetry database.



Note: The telemetry processor can run on Windows 7 and Windows 8 in test or small environments; it is also possible to run the processor on a workgroup computer by using a workaround.

The Office Telemetry database requires SQL Server 2005 and later versions, and can be run on SQL Express editions in test or small environments.



Note: A single computer can be used for all the Office Telemetry components: database, share, and processor.

The Telemetry Dashboard is an Excel 2013 tool that is installed automatically as part of Office Professional Plus 2013 and Office 365 ProPlus installations. The dashboard connects to the database to enable consolidated views of telemetry data, and multiple users can use the dashboard to view the data.

The Telemetry Log is an additional tool that is designed for developers and experienced users to diagnose compatibility issues on a specific Office 2013 client. As with the dashboard, the telemetry log requires Excel 2013, and is automatically installed with Office Professional Plus 2013 and Office 365 ProPlus. However, unlike the dashboard, the telemetry log connects to the local data store on the client, and not the central database.

Telemetry management

Telemetry data collection is managed separately for each client through Group Policy settings. These settings are provided with Office 2013 administrative templates, as part of Office15.admx and Office15.adml, and the settings are located under the **User Configuration\Administrative Templates\Microsoft Office 2013\Telemetry Dashboard** node. If group policy cannot be used, these settings can also be configured on the local computer by editing the registry, or by deploying registry files. There are also several telemetry test settings that can only be updated through registry edit.

Installing and Configuring Telemetry

The telemetry dashboard and components are first deployed on user computers; these components are part of Office Professional Plus 2013 and Office 365 ProPlus installations, and do not require additional installation. The dashboard **Getting Started** worksheet then provides a step-by-step guide and links to configure all the required Office Telemetry components.

The following steps are required to install and configure Office Telemetry:

Configuration steps:

1. Database preparation
2. Telemetry processor setup
3. Deploy agents
4. Configure telemetry agents

Post-Configuration steps:

5. Connect the dashboard to the database
6. Configure privacy

1. *Database preparation.* The first step is to deploy SQL Server (Express or full version), or to connect to an existing SQL Server installation. If a new database is required, the **Getting Started** worksheet provides download links for SQL Server Express.



Note: When configuring the database, **Mixed Mode** authentication must not be selected because the Telemetry Dashboard does not support SQL Server authentication.

2. *Telemetry processor setup.* The second step is to set up the telemetry processor, which reads information stored in the shared folder by telemetry agents then connects and adds records to the telemetry database. The Office Telemetry Processor setup wizard provides guidance for installing the processor, setting up the share, and making the database connection.
3. *Deploy telemetry agents.* The third step is to deploy any required agents for pre-Office 213 versions. The dashboard **Getting Started** worksheet provides download links for x86 and x64 telemetry agents. Agents can be deployed using scripts, Group Policy, or by electronic software distribution (ESD), such as System Center Configuration Manager.
4. *Configure telemetry agents.* The fourth step is to configure telemetry agents and enable data logging. The dashboard **Getting Started** worksheet provides a download link for the Office 2013 Administrative Template files. The **office15.admx** file and language-specific **office15.adml** file should then be imported into Active Directory for use with Group Policy Management tools.

The Office Telemetry Group Policy settings cover the following options:

- Enabling data collection.
- Enabling data upload to the shared folder.
- Location (UNC path) of the shared folder that the client will use to store its data.
- Any applications or solutions to ignore during data collection.
- Custom tags to use to help during data viewing; these tags can include user location, department, and AD security group. More information on tagging is provided in the next topic.
- Enabling privacy settings.

When the Group Policy settings have been deployed to Office clients, the telemetry configuration is complete, and data collection will begin.

Post-Configuration Steps

The dashboard **Getting Started** worksheet provides two additional post-configuration steps:

5. *Connect the dashboard to the database.* The fifth step on the dashboard **Getting Started** worksheet is to connect the dashboard to the database to enable viewing of the data. This step creates and populates additional worksheets, and is covered in a later topic.
6. *Configure any required privacy settings.* The final configuration step is to optionally configure any required privacy settings. By default, data collection includes full file names, file paths, and document titles. Detailed information such as this should not always be viewable by administrators. If the **Turn on privacy settings in Telemetry Agent** Group Policy setting is enabled, file names, file paths, and titles will be obscured. For example, a document named `Merger_Contoso.docx`, will be recorded as `Me*****.docx` in the shared folder, and the document's location and title will be `<location>***** and *****`.

Threshold limits can also be set to prevent certain data from being sent to the shared folder; for example, to exclude documents and applications that are only used by small numbers of users. Data thresholds are set by using the Telemetry Dashboard Administration Tool (Tdadm.exe), which must be downloaded from the Microsoft Download Center.

 **More information on managing privacy settings in Telemetry Dashboard can be found here:**

<http://go.microsoft.com/fwlink/?LinkId=390884>


Using Telemetry Data

After information has been collected in the file share and the telemetry processor has stored records in the database, the data is ready for viewing through the dashboard.

Deciphering and analyzing the data

The fifth step on the dashboard **Getting Started** worksheet provides the **Connect to Database** option. When this option is selected, additional worksheets are created and populated. For example, the **Overview** worksheet provides a summary of the stability and deployment status of Office within the organization. The Documents and Solutions worksheets provide more detail on individual documents and solutions. All worksheets provide options for filtering based on labels (tags), date range, or by view, such as most frequently-used documents.

Setting up tags requires use of Group Policy or direct editing of the local registry. Tags can be based around an Active Directory structure, such as a domain and OU, security group membership (by using security filtering of GPOs, or user information stored in Active Directory, such as Manager, Office Location, and so on.

 **Note:** The use of multiple tags can require the creation and management of a large numbers of GPOs. Creating GPOs can be simplified by using a scripted approach, such as using PowerShell®.

- Deciphering and analyzing the data
- Multiple viewer access
- Removing data



More information on deploying labels (tags) to aid analysis in Telemetry Dashboard is provided here:

<http://go.microsoft.com/fwlink/?LinkId=390885>

Multiple viewer access

For multiple administrators to view telemetry reports, all admins must be added to the `td_readonly` role on the database. The account used to initially set up and configure Office Telemetry is added to this role by default. New users can be added to the `td_readonly` role by using OSQL, SQLCMD, Enterprise Manager, or the Telemetry Dashboard Administration Tool (Tadm).

Removing data

The Telemetry Dashboard Admin Tool can be used to copy or move data from old events to a separate database, such as for archiving; this tool can also be used to delete specific data in the database, based on user name, department, or file name.



For more information, see Telemetry Dashboard Administration Tool References, using the following link:

<http://go.microsoft.com/fwlink/?LinkId=390886>

Disabling logging does not delete the data that has already been collected. To delete this data on the local client computer, delete the files `evt.tbl`, `sln.tbl`, `user.tbl` that are located under `%LocalAppData%\Microsoft\Office15.0\Telemetry\Microsoft\Office\15.0\Telemetry\`.

Considerations for using Office Telemetry

When planning for Office Telemetry it is important to consider typical obstacles to success.

Permissions

The computers that run the Telemetry Processor, shared folder, and SQL database must be joined to a domain so that the appropriate security settings can be configured. If there is a firewall between the dashboard and the telemetry database, the SQL port must be enabled in the firewall configuration; the default port for SQL Server is 1433.

Common obstacles to a successful deployment of Office Telemetry include:

- Permissions
- Infrastructure issues
- Unreported data
- Missing data
- Performance and capacity planning



Note: It is important to check the user permission role for the Telemetry Dashboard, and that the user has been added to the `td_readonly` role.

Infrastructure issues

Various telemetry infrastructure issues can affect successful deployment; for example, a corrupt telemetry database, or connectivity issues between agent and shared folder, between the telemetry processor and the database, or between the telemetry dashboard and the database.

Unreported data

For various reasons, there may be Office data that is never sent to the shared folder, and therefore never stored in the database. For example, offline machines or mobile machines that cannot receive Group Policy may never be enabled for data logging, or be able to report back their data.

If pre-Office 2013 computers are overlooked, it may be assumed that all Office computers are reporting data; however, if agents have not been deployed, data will never be sent.

Windows XP computers do not support the telemetry agent scheduled task; therefore, they only report data at each user logon.

Missing data

It is important to remember that data reporting is a background activity, and that after the random initial upload interval, data is only collected every eight hours. Therefore, it may take some time before all computers are reporting data.


Performance and capacity planning

Telemetry performance can be maximized by setting data thresholds, so that only essential information is reported. Thresholds are set by using the Telemetry Dashboard Administration Tool (Tdadm.exe).

When planning for capacity, note the following data collection upload sizes:

- Office 365 ProPlus - typically 64kb at each upload
- Office 2003+ - typically 50kb at each upload

Even with these small upload sizes, significant data collections can result for larger organizations. For example, 25,000 users reporting data over an eight-hour period can result in 11 GB of data.

 **For more information on issues related to telemetry operations, see the Troubleshooting Telemetry Dashboard deployments section of the Deploy Telemetry Dashboard page at the following link:**

<http://go.microsoft.com/fwlink/?LinkId=390887>

Best Practices for Office Telemetry

To help ensure a successful deployment of Office Telemetry, consider the following best practices:

- Design for reports and dashboard
- Capacity planning
- Consult an expert
- Pilot and test

- Design for reports and dashboard
- Capacity planning
- Consult an expert
- Pilot and test

Lab: Managing Clients

Scenario

Despite Remi's reservations about Office 365, the FastTrack Pilot has proceeded well. Justin's excellent project management skills, combined with Heidi's enthusiasm for the new technology, has generated positive feedback from the pilot users. Because the pilot has received enthusiastic support from the COO and no objections from the CEO, Alain Richer is hopeful that the company will adopt the new platform and move directly from the Pilot Phase to the Deploy Phase.

Before they enter the final phase of the pilot, Heidi has been asked to review the deployment options for Office 365 ProPlus, as well as the management options available with this software.

Objectives

To provide the students with practical experience of planning and deploying Office 365 ProPlus clients.

Lab Setup

Estimated Time: 60 minutes

Virtual machine: 20346C-LUC-CL1

Username: **Student2**

Password: **Pa\$\$w0rd**

In all tasks, where you see references to lucernepublishingXXXX.onmicrosoft.com, replace the XXXX with the unique Lucerne Publishing number that you were assigned when you set up your Office 365 account in Module 1, Lab 1B, Exercise 2, Task 3, Step 5.

Where you see references to labXXXXX.o365ready.com, replace the XXXXX with the unique O365ready.com number you were assigned when you registered your IP address at www.o365ready.com in Module 2, Lab 2B, Exercise 1, Task 2, Step 6.

Exercise 1: Manage user-driven client deployments

Scenario

Lucerne Publishing plans to use a combination of user-driven and managed deployments, depending on the employment relationship and working practices of individual users. Associates, those who have brought their own devices, and home workers will all install Office 365 ProPlus manually from the Office 365 website. Heidi then wants to see what happens to users when she activates and deactivates Office 365 ProPlus subscriptions.



The main tasks for this exercise are as follows:


1. Managing Software and Licenses
2. Performing User-driven Installation
3. Deactivating Office 365 ProPlus
4. Reactivating Office 365 ProPlus



► Task 1: Managing Software and Licenses

1. On your host computer, switch to the **20346C-LUC-CL1** virtual machine.
2. Ensure you are logged on as **Student2** with a password of **Pa\$\$word**.

Note: This is the first lab in which you are logging on as **Student2**. Make sure you logged on as Student2 rather than Student1.

3. On the Desktop run Internet Explorer.
4. Browse to <http://login.microsoftonline.com> and on the **Sign in** page, in the **Name** box, type **hleitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number).
5. In the **Office 365 admin center**, click **Users** on the left and then click **Active Users**.
6. Select **Shirley Mayer**, and then under **Assigned License**, click **Edit**.
7. Click on the down arrow next to the assigned **Microsoft Office 365 Plan E3** to reveal the individual license components.
8. Clear the check box for **Office 365 ProPlus** to remove the license from **Shirley**.
9. Click **Save**.
10. In the **Office 365 admin center**, under **Active users**, click **Robert Schmid**.
11. Click on **Edit**, which appears next to **Assigned license Microsoft Office 365 E3** on the right side.
12. Click on the down arrow next to the assigned **Microsoft Office 365 Plan E3** to reveal the individual license components.
13. Note the licenses for Robert – he has rights to everything.
14. Click the **DISCARD** button.
15. Repeat steps 10-14 for **Karen Gruber**.
16. In the **Office 365 admin center**, click **Service settings**, and then click **User software**.
17. In the **Manage user software through Office 365** section, click to clear **Office and Lync**, and **SharePoint Designer** (by default, both check boxes are selected).
18. Click **Save**.
19. On the **Admin** page, click **Heidi Leitner's** photo profile icon  in the top right screen and then click **Sign Out**.
20. On the **Sign in** page at <https://portal.microsoftonline.com>, in the **Name** box, type **smayer@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number).
21. In the **Password** box, type **Pa\$\$w0rd**, and then click **Sign in**.
22. On the **Collaborate with Office Online** page, click the small Gear icon  in the top right corner, and then click the **Office 365 settings** option.
23. On the **Office 365 settings** page, click on the **Software** option.

Note: This user has no license, and Office is not available for download; only desktop setup is available for Office.
24. Software options for **Lync** will be displayed automatically.
25. On the **Software** page, click **Shirley Mayer's** photo profile icon, and then click **Sign Out**.
26. On the **Sign in** page, in the **Name** box, type **kgruber@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number).
27. In the **Password** box, type **Pa\$\$w0rd**, and then click **Sign in**.
28. On the **Collaborate with Office Online** page, click the small Gear icon  in the top right corner, and then click the **Office 365 settings** option.

29. On the **Office 365 settings** page, click on the **Software** option.
Note: This user has a license, but Office is not available for download.
30. Note the message: The administrator has disabled Office installations. Contact your administrator for information about how to install Office.
31. Verify that Phone and tablet apps are available.
32. Click **Karen Gruber's** photo profile icon in the top right-hand side of the screen and click **Sign out**.
33. Press the **Windows** key to go to the Start screen, and then click **Internet Explorer**.
34. In the **Address** box, type **http://portal.microsoftonline.com**, and press Enter.
35. On the **Sign in** page, in the **Name** box, type **hleitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number).
36. In the **Password** box, type **Pa\$\$w0rd**, and then click **Sign in**.
37. Click on the grey **Admin** icon on the initial **Welcome** screen.
38. In the **Office 365 admin center**, click **Service settings**, and then click **User software**.
39. In the **Manage user software through Office 365** section, select **Office** and **Lync**.
40. Click **Save**.
41. Press the **Windows** key and click **Desktop**.
42. In Internet Explorer, on the **Software** page, click Heidi Leitner's photo profile icon, and then click **Sign Out**.
43. On the **Sign in** page, in the **Name** box, type **smayer@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number).
44. In the **Password** box, type **Pa\$\$w0rd**, and then click **Sign in**.
45. On the **Collaborate with Office Online** page, click the small Gear icon  in the top right corner.
46. Click on the **Office 365 settings** option.
47. On the **Office 365 settings** page, click on the **Software** option.
Note: This user has no license for Office 365 ProPlus.
48. Verify that only desktop setup is available for Office.
49. Click **Lync**, and verify that desktop and app software is available.
50. On the **Get started with Office 365** page, click Shirley Mayer's photo profile icon, and then click **Sign Out**.
51. On the **Sign in** page, in the **Name** box, type **kgruber@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number).
52. In the **Password** box, type **Pa\$\$w0rd**, and then click **Sign in**.
53. On the **Collaborate with Office Online** page, click the small Gear icon  in the top right corner, and then click the **Office 365 settings** option.
54. On the **Office 365 settings** page, click on the **Software** option.
Note: This user has a license, and Office is available for download.
55. Verify that **Office** and **Lync** desktop software is available to install.

56. This user can now select whether to install the 32-bit or 64-bit version of Office 365 ProPlus and which language they want to install.

57. Note also that Phone and tablet apps are available.

► **Task 2: Performing User-driven Installation**

1. Under **Language**, select the language to install.

2. Leave **32-bit (recommended)** selected.

3. Click **Install**.

4. In the Internet Explorer notification bar, click **Run**.

5. In the **User Account Control** dialog box, select **Student1**, and in the **Password** box, type **Pa\$\$w0rd**, and click **Yes**.

Note: This step is required because the local user is not an administrator.

6. On the **Welcome to your new Office** page, click **Next**.

7. If you get the **First things first** page, click **No thanks**, and then click **Accept**.

8. After the video has played, click **Sign in**. Alternatively, click **Next** to skip the video.

9. On the **Sign in** page, in the **E-mail address** box, type **kgruber@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number), and then click **Next**.

10. On the **Sign in** page, in the **Password** box, type **Pa\$\$w0rd**, and then click **Sign in**.

11. Close the **Office** page.

12. On the taskbar, click the **Office** icon, and note the status of the download.

Note: It will take several minutes to complete, but applications are now available.

13. Press the Windows key to go to the Start screen.

14. Note that Office applications are now available.

15. On the Start screen, click **Word 2013**.

16. If you get the **First things first** dialog box, click **No thanks**, and then click **Accept**.

17. Click **Blank document**.

18. Type some text.

19. Click **File**, then click **Save**.

20. Click **Browse**, and save the file to the **Lucerne Publishing Team Site** in the **Documents** folder as **Meeting Agenda**.

21. Click **Save**.

You may see a "streaming features" message.

22. Close Word.

23. Switch back to **Karen Gruber's** Office 365 session in Internet Explorer.

24. In the top-right corner, click the **Settings** icon, and then click **Office 365 settings**.

25. On the **Office 365 settings** page, click **Software**.

26. Note that the installation is listed together with the computer name.

Note also the option to deactivate this installation (for example, if this user wanted to activate on another computer and already had four other activations – five concurrent is allowed).

27. Click **Tools & Add-ins**.
28. Note the following message under Install SharePoint Designer 2013: **The administrator has disabled SharePoint Designer 2013 installations. Contact your administrator for information about how to install SharePoint Designer 2013.**

This message is displayed because you have not yet re-enabled SharePoint Designer 2013 installations from the portal.

► Task 3: Deactivating Office 365 ProPlus

1. Press the Windows key to go to the Start screen, and then click **Internet Explorer**, to switch to **Heidi Leitner's** session in the **Modern apps** browser.
2. In the **Office 365 admin center**, click **Users** on the left, click **Active users**, and then click **Karen Gruber**.
3. Clear the check box for **Office 365 ProPlus**, to remove the license from Karen's account.
4. Click **Save**.
5. Press the Windows key to go to the Start screen, then click **Desktop**.
6. In Internet Explorer, at top-right, click **Karen Gruber**, and then click **Sign out**.
7. On the **Sign** page, in the **Name** box, type **kgruber@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number).
8. In the **Password** box, type **Pa\$\$w0rd**, and then click **Sign in**.
9. In the top-right corner, click the **Settings** icon, and then click **Office 365 settings**.
10. On the **Office 365 Settings** page, click **Software**.
11. Note that the Office installation is no longer listed, as this user no longer has an active license (although software is available).

► Task 4: Reactivating Office 365 ProPlus

1. Press the Windows key to go to the Start screen, and then click **Internet Explorer** to switch to the Heidi's session in the modern apps browser.
2. In the **Office 365 admin center**, click **Users**, click **Active users**, and then click **Karen Gruber**.
3. Select the check box for **Office 365 ProPlus** to restore the license for **Karen**.
4. Click **Save**.
5. Press the Windows key to go to the Start screen, click **Desktop**, and then click **Internet Explorer**, to switch to the user session (Desktop browser).
6. At the top-right corner, click **Karen Gruber**, and then click **Sign out**.
7. On the **Sign** page, in the **Name** box, type **kgruber@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number).
8. In the **Password** box, type **Pa\$\$w0rd**, and then click **Sign in**.
9. In the top-right corner, click the **Settings** icon, and then click **Office 365 settings**.
10. On the **Office 365 settings** page, click **Software**.

11. Note under Office, you may get a "**Setting up Office**" progress message while the license is being provisioned (which may take several hours).
12. Press the Windows key and on the Start screen, click **Word 2013**. If you cannot see the icon for Word 2013, type "**Word**" and then click the icon.
13. In **Microsoft Word**, click **Blank document**, click **File**, and then click **Account**.
14. In the pop-up message, click **Enable**.
15. Under **Subscription Product**, click **Manage Account**.
16. Under **Software**, click **Lync**.
17. Note that the full Lync client is not available to be installed until the Office license is ready.
18. Click **Get app**.
19. In the **Windows Store** page, click **Install**.
20. On the **Add your Microsoft account** dialog box, in the **E-mail address** box, type **username@outlook.com**, (where username@outlook.com is the Windows Live address you registered in Lab 1A, Ex 1 Task 1), in the **Password** box, type **<password>**, (where <password> is the password you used to sign up for the Office 365 trial in Module 1, Lab A, Exercise 1, Task 1), and then click **Save**.
Note: This Office 365 user does not have an associated Microsoft Account at this stage.
21. In the **Windows Store** page, click the left arrow to return to the **Lync app** page.
22. Press the Windows key to go to the Start screen.
23. Verify that the Lync 2013 app is now available. If you cannot see the icon, type **Lync**.
24. On the **Windows Start** page, click **Internet Explorer**, to switch to Heidi's session on the Modern Apps browser.
25. In the top-right corner, click the **Settings** icon, and then click **Office 365 settings**.
26. On the **Office 365 settings** page, click **Software**.
27. Note that under Office, Office installation should now be available again (if not, wait a few minutes and refresh the page).

Results: Lucerne Publishing can control user access to Office 365 ProPlus and demonstrate a simplified, distributed installation of Office 365 ProPlus.

Exercise 2: Manage IT deployments of Office 365 ProPlus

Scenario

For users who work on domain-joined computers at Lucerne Publishing office locations either in Switzerland or around the world, self-service deployment is not suitable. This restriction is due to the users' lack of administrative rights, as well as the additional download traffic that would be generated. As a result, Heidi wants to analyze both group policy management and scripting to enable deployment of Office 365 to multiple computers within a managed network.

The main tasks for this exercise are as follows:

1. Using the Office Deployment Tool

2. Creating Deployment GPOs
3. Verifying a Managed Deployment
4. Using GPOs to Modify First Run Experience

► **Task 1: Using the Office Deployment Tool**

1. On **LUC-CL1**, press the Windows key to go to the Start screen.
2. On the Start screen, click **Student2**, and then click **Student1**.
3. On the **Login** page, type **Pa\$\$w0rd** as the password, and then press Enter.
4. Click **Desktop**, then in the Taskbar, click **File Explorer**.
5. Navigate to **E:\RDP_files**.
6. Double-click **LUC-SV1.rdp**, and connect as **LUCERNE\LucAdmin**, with a password of **Pa\$\$w0rd**.
7. If you get a Remote Desktop Connection warning, select the **Don't ask me again for connections to this computer** check box, and then click **Yes**.
8. On the taskbar, click **File Explorer**.
9. In File Explorer, expand **Computer**, and then click **Local Disk (C:)**.
10. In File Explorer, click the **Home** tab, and then click **New Folder**.
11. Type **Office15**, and then press Enter.
12. In File Explorer, right-click **Office15**, then click **Share with**, and then click **Specific people**.
13. In the **File Sharing** dialog box, click the drop-down list, select **Everyone** from the list, click **Add**, and then click **Share**.
14. In the **File Sharing** dialog box, click **Done**.
15. In **Server Manager**, in the navigation pane, click **Local Server**.
16. In the **Properties for LUC-SV1**, next to IE Enhanced Security Configuration, click **On**.
17. In the **Internet Explorer Enhanced Security Configuration** dialog box, select **Off** for **Administrators**, and then click **OK**.
18. Close Server Manager.
19. Press the Windows key to go to the Start screen.
20. On the Start screen, click **Internet Explorer**.
21. At the **Windows Internet Explorer 10** dialog box, select **Use recommended security and compatibility settings**, and then click **OK**.
22. In the **Address** box, type **http://portal.microsoftonline.com**, and then press Enter.
23. Log on as **hleitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number) and a password of **Pa\$\$w0rd**.
24. If the **Don't lose access to your account** dialog box appears, select your **Country or region**, enter your mobile phone number, then click **Save and continue**.
25. In the **Office 365 admin center**, click **Service settings**, and then click **User software**.
26. In the **Manually deploy** section, expand **The latest version of Office**, and then click **Download and customize**.

27. In the **Microsoft Download Center**, on the **Office Deployment Tool for Click-to-Run** page, click **Download**.
28. In the Internet Explorer bar, click **Run**.
29. In the **The Microsoft Office 2013 Click-to-Run Administrator Tool** dialog box, select the **Click here to accept the Microsoft Software License Terms** check box, and then click **Continue**.
30. In the **Browse For Folder** dialog box, navigate to **C:\Office15**, and click **OK**.
31. In the **The Microsoft Office 2013 Click-to-Run Administrator Tool** dialog box, click **OK**.
32. On the taskbar, click **File Explorer**.
33. In this step, you will back up the Office 15 **configuration.xml** file and then open it so that you can edit it in the next step. To do this, perform the following steps:
 - a. In File Explorer, double-click **C:\Office15**.
 - b. As a best practice, you should back up configuration files before editing them; therefore, copy the **configuration.xml** file, paste it in this same folder, and then rename it so that you have a backup copy.
 - c. Right-click the **configuration.xml** file, click **Open with**, and then click **Notepad**.
34. In Notepad, replace all occurrences of **\\Server\Share** with **\\LUC-SV1\Office15**.
35. In Notepad, remove all the remaining comment codes (lines that start with **<!--** and end with **-->**), and save the file as **LucerneConfiguration.xml**.
36. Comment out Visio to make the download quicker, by replacing this code:

```
</Product>
  <Product ID="VisioProRetail">
    <Language ID="en-us" />
  </Product>
```

with this code:

```
</Product>
<!--
  <Product ID="VisioProRetail">
    <Language ID="en-us" />
  </Product>
-->
```

37. Save the file.
38. Switch to File Explorer, press **SHIFT**, and then right-click any white space below the file list, and then click **Open command window here**.
39. At the Command Prompt, type the following command, and then press Enter:

Setup /?
40. Note the Office Deployment Tool command-line options.
41. At the Command Prompt, type the following command, and then press Enter:

setup.exe /download \\LUC-SV1\Office15\LucerneConfiguration.xml
42. The download will take several minutes to complete.
43. Switch to File Explorer, and verify the download.

► Task 2: Creating Deployment GPOs

1. Switch to the LUC-CL1 virtual machine session.
2. On the Desktop, on the Taskbar, click **File Explorer**.
3. Navigate to **E:\RDP_files**.
4. Double-click **LUC-DC1.rdp**, and connect as **LUCERNE\LucAdmin**, password: **Pa\$\$w0rd**.
5. If you get a Remote Desktop Connection warning, select the **Don't ask me again for connections to this computer** check box, and click **Yes**.
6. On **LUC-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
7. In the console tree, right-click **lucernepublishing.local**, point to **New**, and then click **Organizational Unit**.
8. Type **Lucerne_Computers**, and then click **OK**.
9. In the console tree, under **lucernepublishing.local**, click **Computers**.
10. Click **LUC-CL2** and holding the shift key, click **LUC-CL3**. Right-click the selection, click **Move**, click **Lucerne_Computers**, and then click **OK**.
11. In **Server Manager**, click **Tools**, and then click **Group Policy Management**.
12. In **Group Policy Management**, expand **Forest: lucernepublishing.local**, expand **Domains**, expand **Lucernepublishing.local**, and then click **Lucerne_Computers**.
13. Right-click **Lucerne_Computers**, and then click **Create a GPO in this domain, and Link it here**.
14. In the **New GPO** dialog box, in the **Name** box, type **DeployO365**, and click **OK**.
15. In **Group Policy Management**, click **Lucerne_Computers**, then in the right-hand pane, right-click **DeployO365** and click **Edit**.
16. In **Group Policy Management Editor**, expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, and then click **Scripts (Startup/Shutdown)**.
17. Double-click **Startup**, and then click **Show Files**.
18. In Windows Explorer, click **Home**, then click **New item**, and click **Text Document**.
19. Double-click **New Text Document**.
20. In Notepad, add the following line:

```
\\LUC-SV1\Office15\setup.exe /configure \\LUC-SV1\Office15\LucerneConfiguration.xml.
```
21. Save the file as **DeployO365.cmd**. Ensure that in **Save as type**, you select **All Files** and that the file extension is **.CMD**.
22. Close Notepad.
23. Delete **New Text Document**.
24. Switch back to the **Group Policy Management Editor, Startup Properties** dialog box.
25. Click **Add**.
26. In the **Add a Script** dialog box, click **Browse**.
27. In the **Browse** dialog box, select **DeployO365.cmd**, and click **Open**.
28. In the **Add a Script** dialog box, click **OK**.

29. In the **Startup Properties** dialog box, click **OK**.
30. Close Group Policy Management Editor.
31. Note that this script could also be deployed using Intune, SCCM, or other ESD.

► **Task 3: Verifying a Managed Deployment**

1. Switch to the **LUC-CL1** virtual machine session.
2. On the Desktop, on the Taskbar, click **File Explorer**.
3. Navigate to **E:\RDP_files**.
4. Double-click **LUC-CL2.rdp**, and connect as **LUCERNE\LucAdmin**, password: **Pa\$\$w0rd**.
5. If you get a Remote Desktop Connection warning, select the **Don't ask me again for connections to this computer** check box, and click **Yes**.
6. On the Start screen, click **Server Manager**.
7. In **Server Manager**, in the navigation pane, click **Local Server**.
8. In the **Properties for LUC-CL2**, next to IE Enhanced Security Configuration, click **On**.
9. In the **Internet Explorer Enhanced Security Configuration** dialog box, select **Off** for **Administrators** and for **Users**, and then click **OK**.
10. Close Server Manager.
11. On **LUC-CL2**, on the Start screen, point to the bottom-right corner of the screen, move the mouse pointer up, then click **Settings**.
12. Click **Power**, then click **Restart**, and then click **Continue**.
Note: If any updates have downloaded, click **Update and restart** instead.
13. Wait a few minutes for LUC-CL2 to restart before continuing.
14. On the **LUC-CL1** virtual machine session, in **File Explorer**, in **E:\RDP_files**, double-click **LUC-CL2.rdp**, and connect to LUC-CL2 as **LUCERNE\wdouglas**, password: **Pa\$\$w0rd**.
15. If you get a Remote Desktop Connection warning, select the **Don't ask me again for connections to this computer** check box, and click **Yes**.
16. Press Ctrl+Tab, and note that Office 2013 is installed.
17. Click **Word 2013** and click **Sign in**.
Note: If you get an error message, try closing down Word 2013 using Task Manager if required, and restarting at step 17.
18. On the **Sign in** page, in the **E-mail address** box, type **wdouglas@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number), and then click **Next**.
19. On the **Sign in** page, in the **Password** box, type the temporary Office 365 password from Lab 3 for **William Douglas**, and then click **Sign in**.
20. In the **Update password** dialog box, under **Old password**, enter William Douglas's temporary password.
21. In the **New password** and **Confirm new password** boxes, enter **Pa\$\$w0rd**, then click **Save**.
22. In the **Office 365 logon** dialog box, re-enter the new password and click **Sign in**.

23. If you get an Internet Explorer dialog box, click **Close**, and then re-enter your password to sign in again.
24. In the **Account Updated** dialog box, click **OK**.
25. In the **First things first** dialog box, click **No thanks**, and then click **Accept**.
26. Close the Welcome to your new Office dialog box.
27. In the templates list, click **Blank document**.
28. Type some text.
29. Click **File**, then click **Save**.
30. Click **Lucerne Publishing Team Site**.
31. Under **Document Libraries**, double-click **Documents**.
32. In **File** name, enter **Meeting Report** and click **Save**.
33. Right-click on the taskbar, and click **Task Manager**.
34. In **Task Manager**, click **More details**.
35. In the **Processes** tab, under **Background processes**, note **Microsoft Office Click-to-Run**.
36. Click the **Details** tab, and note **officeclicktorun.exe** in the task list.
37. Close Task Manager.
38. Close Word 2013.

► **Task 4: Using GPOs to Modify First Run Experience**

1. Switch to the **LUC-CL1** virtual machine session.
2. On the Desktop, on the Taskbar, click the **LUC-DC1 RDP** session.
3. Log on as **LUCERNE\LucAdmin** with a password of **Pa\$\$w0rd**.
4. If you get a Remote Desktop Connection warning, select the **Don't ask me again for connections to this computer** check box, and click **Yes**.
5. On **LUC-DC1**, on the Task Bar, click **File Explorer** and navigate to the **C:\Labfiles\Lab04** folder.
6. In File Explorer, double-click **admintemplates_32**.
7. In the **The Microsoft Office 2013 Administrative Templates** dialog box, select the **Click here to accept the Microsoft Software License Terms** check box, and then click **Continue**.
8. In the **Browse For Folder** dialog box, expand **Computer**, and then click **Local Disk (C:)**, then click **Make New Folder**, type **Office Templates**, then press Enter, and then click **OK**.
9. In the **Microsoft Office 2013 Administrative Templates** dialog box, click **OK**.
10. In File Explorer, navigate to **C:\Office Templates\admx**, right-click **office15.admx**, and click **Copy**.
11. In File Explorer, navigate to **C:\Windows\PolicyDefinitions**, click **Home**, and then click **Paste**.
12. In File Explorer, navigate to **C:\Office Templates\admx\en-us**, right-click **office15.adml**, and then click **Copy**.
13. In File Explorer, navigate to **C:\Windows\PolicyDefinitions\en-US**, click **Home**, and then click **Paste**.

Note: If the ADMX file is not in the EN-US folder, group policy cannot see the Office policies in the file.

14. Switch back to the **Group Policy Management** window, expand **lucernepublishing.local**, and then expand **Lucerne_Computers**.
15. Under **Lucerne_Computers**, right-click **DeployO365**, and then click **Edit**.
16. In **Group Policy Management Editor**, expand **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, expand **System**, and then click **Group Policy**.
17. Right-click **Configure user Group Policy loopback processing mode**, and click **Edit**.
18. In the **Configure user Group Policy loopback processing mode** dialog box, click **Enabled**, then under **Options**, in the **Mode** list, select **Merge**, and then click **OK**.
19. In **Group Policy Management Editor**, expand **User Configuration**, expand **Policies**, expand **b**, expand **Microsoft Office 2013**, and then click **First Run**.
20. Right-click **Disable First Run Movie**, select **Edit**, click **Enabled** and click **OK**.
21. Right-click **Disable Office First Run on application boot**, select **Edit**, click **Enabled**, and then click **OK**.
22. On **LUC-CL1**, go to the Desktop and on the Taskbar, click **File Explorer**.
23. Navigate to **E:\RDP_files**.
24. Double-click **LUC-CL3.rdp**, and connect as **LUCERNE\LucAdmin** with a password of **Pa\$\$w0rd**.
25. If you get a Remote Desktop Connection warning, select the **Don't ask me again for connections to this computer** check box, and click **Yes**.
26. On the Start screen, right-click **Windows PowerShell** and click **Run as administrator**.
27. At the Windows PowerShell command prompt, type the following command, and press Enter:

```
gpupdate /force
```
28. On the Start screen, point to the bottom-right corner of the screen, move the mouse pointer up, then click **Settings**.
29. Click **Power**, then click **Restart**, and then click **Continue**.

Note: If any updates have downloaded, click **Update and restart** instead. Then wait a few minutes for LUC-CL3 to restart before continuing.
30. In File Explorer on **LUC-CL1**, double-click **LUC-CL3.rdp**.
31. Log on as **LUCERNE\elabrecque**, with a password of **Pa\$\$w0rd**.
32. On the Windows Start screen, press Ctrl+Tab, and click **Word 2013**.
33. Wait for the **Sign In** dialog box, and then activate Office using **elabrecque@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number), and a password of **Pa\$\$w0rd**.
34. On the **Account Updated** message box, click **OK**.
35. Note that the Word video does not appear.
36. On the **First things first** page, click **No thanks**, and then click **Accept**.
37. Close the browser window, then close Word 2013.

38. Press the Windows key to go to the Start screen.
39. On the Start screen, click **Elisabeth Labrecque**, and then click **Sign out**.

Results: Lucerne Publishing has enabled centralized managed deployment of Office 365 clients and implemented a standardized MS Office configuration using one version of Office.

Lab Review Discussion Questions

Why do you need to edit the configuration xml file when preparing to use managed deployments of Office 365 Pro Plus?

This configuration file is used to specify the UNC path to the shared folder containing the Office 365 Pro Plus source files, and also to specify products and languages to install.

How can you verify that the Click-to-Run service is running?

Use Task Manager, and in the Processes list, under Background processes, look for Microsoft Office Click-to-Run. You can also click the Details tab, and look for officeclicktorun.exe in the task list.

- Why do you need to edit the configuration xml file when preparing to use managed deployments of Office 365 Pro Plus?
- How can you verify that the Click-to-Run service is running?

Module Review and Takeaways

Having completed this module, you can now plan for deploying Office 365 clients, prepare for user-driven client deployments, prepare for managed IT deployments of Office 365 clients, and implement and use Office Telemetry with Office 365 clients.



Best Practice: Obstacles to a successful client deployment include incomplete data, custom application incompatibilities, and not gathering enough or important information from existing implementations and running into compatibility issues later.

The chances for a successful user-driven deployment can be jeopardized when there is lack of planning or testing, deploying the incorrect plan, or not understanding what happens when you revoke a license.

For managed deployments, it is important to prepare a thorough support plan for users, to help guide them through the transition to Office 365 applications.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Users do not all use the same first language.	

MCT USE ONLY. STUDENT USE PROHIBITED

Module 5

Planning DNS and Exchange Migration

Contents:

Module Overview	5-1
Lesson 1: Add and Configure Custom Domains	5-2
Lesson 2: Recommend a Mailbox Migration Strategy	5-12
Lab: Preparing for Exchange Migration	5-30
Module Review and Takeaways	5-39

Module Overview

In this module, you move on learn about the factors that cover DNS domain configuration for Office 365™, where you need to add the customer's existing domain or domains to Office 365. This module also covers the individual settings that you need to configure so that each Office 365 service works correctly and fully supports client access. These activities typically happen in the Deploy phase of the FastTrack process.

So far, you have been looking at Office 365 on its own. In this module, you move on to considering what you have to cover when migrating services from your on-premises environment, starting with your email system. This module addresses the key issues of migrating email accounts to Exchange Online and the planning involved in that process. In the lab, you will practice that planning, and then carry out a cutover migration from your on-premises environment to Exchange Online.

Objectives

After completing this module, you should be able to:

- Explain how to add custom domains to Office 365 and customize them to the organization's requirements.
- Recommend a mailbox migration strategy for moving to Exchange Online.

Lesson 1

Add and Configure Custom Domains

As Office 365 is a Microsoft-hosted, Internet-based cloud service, it should come as no surprise that DNS is an important part of Office 365. In particular, you need to be able to provide an organization with the option to register its own DNS domain with Office 365, thus enabling that company to use email addresses in the form `username@customdomain.com` or SharePoint sites in the form of `http://sharepoint.customdomain.com`.

In this lesson, you will review the prerequisites, requirements, and process for registering and confirming ownership of DNS domains with Office 365, including sub-domains, alternate domains and matching domain names to User Principal Names in an on-premises Active Directory®.

Lesson Objectives

After completing this lesson, you should be able to:

- List the DNS record types that Office 365 uses.
- Explain how DNS functions and why it is important in Office 365.
- Describe the function of split-brain DNS.
- Plan for custom domains in Office 365.
- Describe the process of adding and verifying domains to Office 365.
- Explain how to add and verify a custom domain.
- Locate instructions on adding custom domains to listed DNS hosters.
- Troubleshoot the domain verification process.
- List best practice guidelines for configuring custom domains.

DNS and Office 365

DNS is a hierarchical, distributed global naming scheme that maps human-readable host, machine or service names to Internet Protocol (IP) addresses. So when you attempt to connect to a host name using the PING or TELNET commands, it is DNS that resolves the host address to a unique IP address. For example, the command PING `www.microsoft.com` returns the IPv4 address `64.4.11.42`.

DNS provides mapping to both IPv4 and IPv6 addresses. It can also provide the reverse service, mapping IP addresses to host names.


Although DNS is the primary naming service on the Internet, where names are globally unique, organizations may also have their own internal DNS domains, where name mappings are local and the mapped IP addresses belong to private address ranges, such as `10.0.0.0/8`, `172.16.0.0/16`, or `192.168.X.X/24`.

- DNS maps host names to IP addresses and back again
- DNS works on both the Internet and internal networks
- Default Office 365 domain is companyname.onmicrosoft.com
- Adding a domain like `lucernepublishing.com` enables:
 - A mail address of user@lucernepublishing.com
 - A SharePoint site at sharepoint.lucernepublishing.com
 - A SIP domain for Lync Online of `sip.lucernepublishing.com`

When you set up an Office 365 pilot, the default DNS domain is <companyname>.onmicrosoft.com, so email addresses within Office 365 are user@companyname.onmicrosoft.com and SharePoint® sites point to companyname.sharepoint.com. In the Deploy phase, the organization is likely to require the addition of one or more domains into Office 365 so that the online services can use that domain name for configuration.

For example, if the domain lucernepublishing.com is added, this external domain can be used as follows:

- *Exchange Online.* Provide email addresses and distribution lists in the form user@lucernepublishing.com or sales@lucernepublishing.com.
- *Lync Online.* Provide Session Initiation Protocol (SIP) name resolution.

 **Note:** There are some noticeable differences between the Office 365 versions in how they can manage domains. Later topics in this module cover some of these differences.

It is important that you can prove you do own a particular DNS domain, otherwise anyone else could register it and impersonate your organization, even to the extent of being able to read all the company's email messages.

DNS Record Types

A DNS server will typically be configured with one or more DNS zones, such as lucernepublishing.org, the exception being if the DNS server is used only for caching requests.

When the DNS server receives a request for a host name, such as mail.lucernepublishing.org, it then looks up its records in the lucernepublishing.com zone and checks to see what IP address is registered against the value for "mail" and returns that IP address back to the requesting client.

Each DNS zone can contain a number of different DNS record types which provide differing name resolution services. Office 365 uses the following subset of DNS records:

Type	Full Name	Function
A (IPv4)	Address	Maps a host name such as mail.lucernepublishing.com to an IP address, such as 131.107.10.10
AAAA (IPv6)		
CNAME	Canonical Name	Points one host record, such as ftp.lucernepublishing.com to another host record, such as mail.lucernepublishing.com or even another host record in another domain, such as www.contoso.com
MX	Mail Exchanger	Points to the host that will receive mail for that domain
NS	Name Server	Delegates a DNS zone to the specified authoritative name server
PTR	Pointer	Points to another record, like a CNAME
SPF	Sender Policy Framework	SPF provides limited anti-spam services
SRV	Service locator	Locates hosts that are providing specific services, such as the SIP endpoint in Lync Online
TXT	Text	Records a human-readable text field in DNS

Record Type	Full Name	Function
A (IPv4) AAAA (IPv6)	Address	Maps a host name such as mail.lucernepublishing.com to an IP address, such as 131.107.10.10.
CNAME	Canonical Name	Points one host record, such as ftp.lucernepublishing.com to another host record, such as mail.lucernepublishing.com or even another host record in another domain, such as www.contoso.com.
MX	Mail Exchanger	Points to the host that will receive mail for that domain. MX records must point to an A record, not a CNAME record.
NS	Name Server	Delegates a DNS zone to the specified authoritative name server.

MCT USE ONLY. STUDENT USE PROHIBITED

Record Type	Full Name	Function
PTR	Pointer	Points to another record, like a CNAME. Typically used for reverse DNS lookups, where querying for an IP address returns a host name.
SPF	Sender Policy Framework	Sender Policy Framework provides limited anti-spam protection by specifying which hosts are and are not authorized to use a domain name for "HELO" and "MAIL FROM" commands.
SRV	Service locator	Locates hosts that are providing specific services, such as the SIP endpoint in Lync Online.
TXT	Text	Records a human-readable text field in DNS.

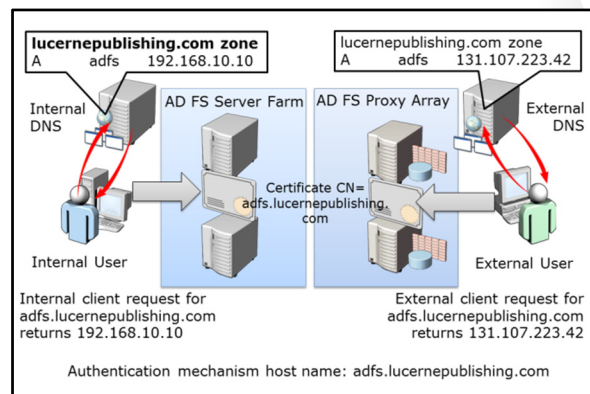


The following link provides more information on DNS record types:

<http://go.microsoft.com/fwlink/?LinkId=390888>

Split-Brain DNS

As the Internet has become more pervasive and the global DNS hierarchy now encompasses all external host names, organizations have started configuring DNS for their internal networks as well, replacing older or more restricted naming systems, such as NetBIOS. Therefore, a company might set up its own internal DNS for its internal domain – say `lucernepublishing.local` – and then use a DNS forwarder on the internal DNS servers to redirect name resolution requests for external domains to an external name server. For example, a request for `mail.lucernepublishing.local` would be redirected to an internal IP address, such as `192.168.20.10`, whereas a request for `mail.lucernepublishing.com` might go to `131.107.43.19`, the company's external IP address for that host name.



Split-brain DNS is a configuration where the internal and external DNS environments provide different IP addresses to requests for the same host name, depending on where the request comes from. If a request for `mail.lucernepublishing.com` comes from inside the `lucernepublishing.com` network, the address returned might be `192.168.20.10` on the internal network, whereas if a user directly connected to the Internet made the same request to `mail.lucernepublishing.com`, the IP address returned might be `131.107.43.19`. This configuration is achieved by creating a zone on the internal DNS server for `lucernepublishing.com`.

When a client on the internal network makes a request for `mail.lucernepublishing.com`, the internal DNS server responds with the IP address for that host, using the A (Address) or CNAME (common name) records that the server maintains for that zone. There is no requirement to forward on the name resolution request to the external DNS servers. However, external clients who try to contact `mail.lucernepublishing.com` receive a response from the external DNS server that is authoritative for that zone.

Split-brain DNS configuration is important in certain situations in Office 365, such as when configuring single sign-on with Active Directory Federation Services (AD FS). In this case, the address for connecting to AD FS might be adfs.lucernepublishing.com. In addition, because the authentication process needs to be protected using Secure Sockets Layer (SSL) encryption, the common name (cn) or one of the subject alternate names (SANs) on the certificate must match the host name of the communication endpoint of the service. The challenge here is that, in order to ensure a consistent experience for users, both internal and external clients will be connecting using the same host name.

In the case of AD FS, there is an additional complication, in that internal clients connect directly to the AD FS server farm, whereas external clients connect to the AD FS proxy array. Hence, DNS needs to return a different IP address for internal and external clients.

The following diagram shows how split-brain DNS works:

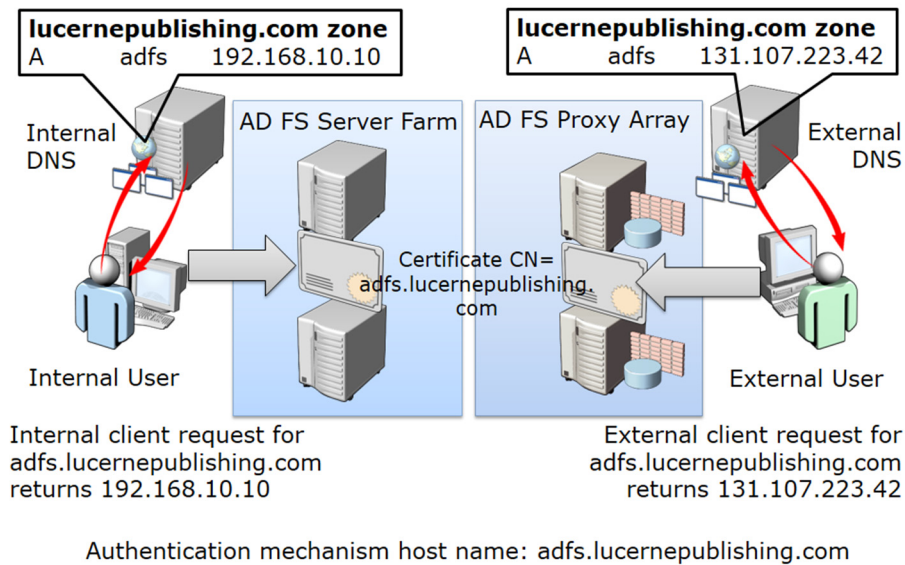


FIGURE 5.1: SPLIT-BRAIN DNS PROVIDING DIFFERENT IP ADDRESSES FOR ADFS.LUCERNEPUBLISHING.COM.

Planning Custom Domains

When planning to add custom domains to Office 365, there are a number of factors you need to consider. These factors can differ with the Office 365 subscription selected. The following table sets out these planning factors:

- Additional Root domains
- Subdomains
- Domain adding order
- DNS record hosting
- Domain numbers
- DNS console access
- Not registering DNS
- Not changing all records
- DNS record propagation

MCT USE ONLY. STUDENT USE PROHIBITED

Factor	Considerations
Multiple Domains	Plan to add the main domain that your company currently uses along with any other domain that is used for email messages within the organization. This scenario is common where the overall company is a business group or the organization has been through a merger process and some employees still have alternative domain addresses.
Subdomains	You may want to register subdomains such as <code>content.lucernepublishing.com</code> within the account for Lucerne Publishing. Note that Office 365 Midsize Business and Enterprise plans allow you to add sub-domains under your root domain, whereas the Office 365 Small Business plans do not.
Domain numbers	You can register up to 600 domains with Office 365.
Domain adding order	Root domains must be added before sub-domains, so you need to register <code>lucernepublishing.com</code> before you add <code>content.lucernepublishing.com</code> .
DNS record hosting	With Office 365 Midsize Business and Enterprise plans, you host your DNS records with your current hosting provider. With the Small Business Plan, there is the option to use Office 365 to host your DNS records.
Access to the DNS console	Check with your DNS hosting organization as to what access you get to the DNS console. You need to be able to add A, CNAME, TXT and MX records to configure Office 365 services. If your DNS hosting provider does not give that level of access, you may have to change providers.
Not registering DNS	It is rare that you should not want to register a DNS domain with Office 365 but it is a possible option – for example, if you want to have a completely separate email and directory service for your Office 365 users. For example, a university might want to host its faculty members in the on-premises environment and have the students in Office 365 with a different domain name.
Not changing all records	You may not want to change all the DNS records to point to Office 365. The setup topic later in this lesson identifies how to handle the verification process when not changing all DNS records.
DNS record propagation timings	DNS records can take up to 72 hours to propagate. Reducing the Time to Live (TTL) value can speed up this process, but you still need to plan for the replication time.

Process for Adding Domains to Office 365

If an organization has a domain name that needs to be added to Office 365, then there is a specific process that the administrator or Microsoft Partner must go through.

1. Check that you have ownership of the domain. Who owns a domain can sometimes be problematic, particularly if a former employee registered the domain with their information and has now left the organization. Check the WHOIS record for that domain using an Internet WHOIS register, such as who.is to find out who originally registered it.
2. Check that you have access to the DNS console for the domain. Different DNS hosting organizations provide varying levels of access to DNS records for a hosted domain.
3. Check that you can make changes to the DNS records for the domain.
4. Log onto the Office 365 admin center and go to the domains tab.
5. Confirm domain ownership for the domain:
 - a. Enter the domain name for which you want to confirm ownership of the domain.
 - b. Add text (TXT) or mail exchanger (MX) records to the DNS record for the domain.
 - c. Confirm ownership by getting Office 365 to verify that you could make that change to the DNS records.
6. Change the default domain to the new domain, so that any new accounts use this domain value rather than the one originally assigned when you set up Office 365.
7. Add users and assign licenses (this is part of the Office 365 setup rather than a DNS specific operation).
8. Set the domain purpose and finish configuring DNS (covered in the next lesson).



1. Check ownership of the domain
2. Check you have access to the DNS console
3. Check that you can make the required changes to DNS records
4. Log onto Admin Center in Office 365
5. Confirm domain ownership in Office 365 by adding an MX or TXT record to DNS
6. Change the default domain to the new domain
7. Add users and assign licenses
8. Set the domain purpose and finish configuring DNS

You can cancel out of the domain setup process but still verify that you own the domain. In the Office 365 admin console, you will see the message “setup in progress”.

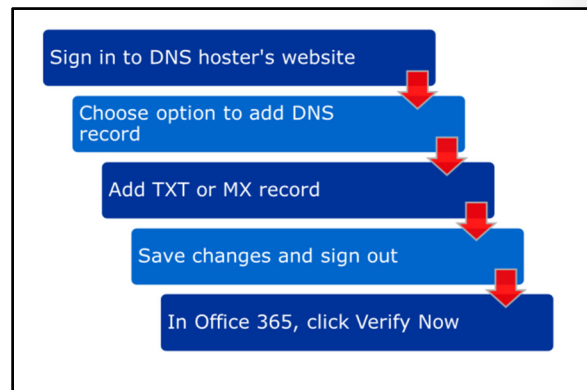



Note: After you have verified a domain, you can delete the verification TXT record. You should also be aware that you can only validate each domain (with any attendant sub-domains) to a single Office 365 tenant account.

Generic DNS Verification Procedure

The following generic steps should be used to verify a custom DNS domain:

1. Sign in to your domain registrar's website, and then select the domain that you're verifying.
2. In the DNS management area for your account, choose the option to add a DNS record for your domain.
3. Use the values shown in the table below to create either a TXT or MX record.
4. Save your changes, and then sign out of your DNS hosting provider's website.
5. Wait 15 minutes for DNS replication to take place.
6. In the Office 365 portal, click **Verify now**.



 **Note:** With regard to step #3, you only have to create one of the records shown. TXT is the preferred method, but some DNS hosting providers do not support creation of TXT records; in this case, you can create an MX record instead.

Record type (only one required)	Alias or Hostname	Destination or Points to Address	TTL
TXT	@ or customdomainname.com	MS=ms14478881	1 Hour
MX	@ or customdomainname.com	ms14478881.msv1.invalid.outlook.com	1 Hour

If you are not familiar with DNS, you could email your DNS hoster and ask them to create the record for you, using a message like this:

Hi,

I'm using Microsoft Office 365 and would like to register my domain with this service, but Office 365 must be able to verify that I own the domain name. To do this, please could you create a TXT or an MX record for my domain using the information in the following table?

Record type (only one required)	Alias or Hostname	Destination or Points to Address	TTL
TXT	@ or customdomainname.com	MS=ms14478881	1 Hour
MX	@ or customdomainname.com	ms14478881.msv1.invalid.outlook.com	1 Hour

DNS Verification with Specified DNS Hosters

In addition to the generic instructions for DNS registration from the previous topic, Office 365 provides specific steps and screenshots for the following DNS hosters:

- eNom
- GoDaddy
- 1&1 Internet
- Hover
- Melbourne IT
- Network Solutions
- Register.com
- DNSPod
- HiChina

You can access the steps and accompanying screenshots for each of these providers in the Office 365 admin center.

To access the step-by-step instructions for these providers, click the drop-down list during the confirm ownership process.

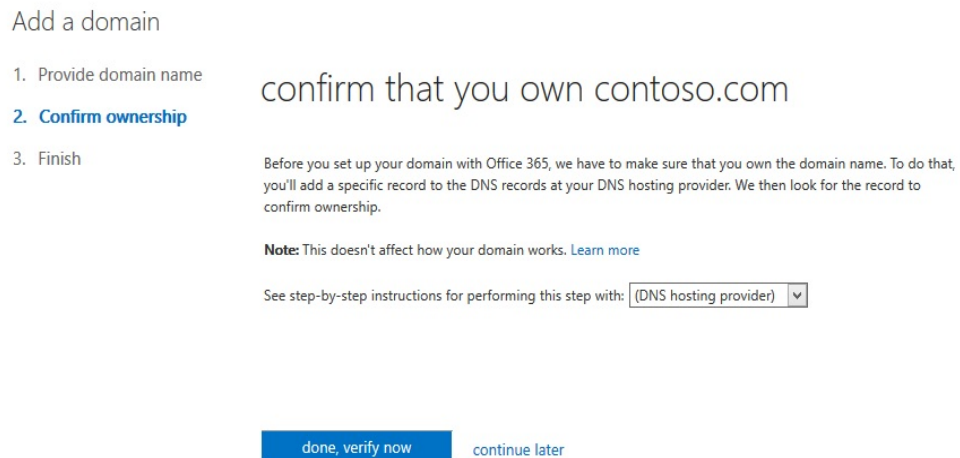
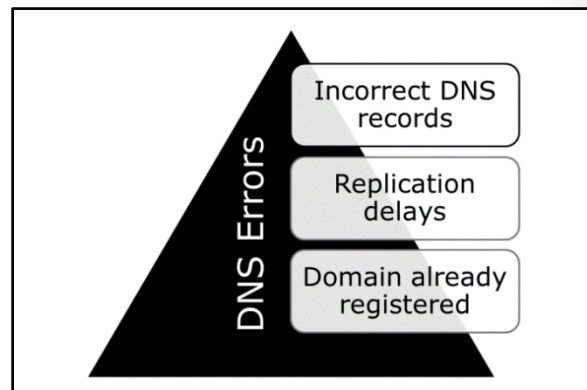


FIGURE 5.2: THIS IMAGE SHOWS THE INTERFACE FOR SELECTING SPECIFIC DNS HOSTERS.

Troubleshoot Domain Addition

As long as you have ownership of your DNS domain and can add TXT or MX records to it, you should be able to register and configure DNS domains with Office 365. However, it may be possible that Office 365 cannot verify that you own the domain.

The most common reason for this is that it can be tricky to ensure that you add the TXT or MX DNS record correctly into your hoster's DNS interface. DNS hosters do not always provide particularly intuitive user experiences, so the required values may end up in the wrong fields.



The following table summarizes the typical troubleshooting issues:

Issue	Cause	Remedy
<i>Incorrect DNS record</i>	During the verification process, Office 365 checks for the exact values for the records. If the values that you enter do not match, then the domain will not be verified.	Ensure that MX or TXT records are entered correctly. Use <code>nslookup msxxxxxxx.yourdomain.com</code> to check that the record exists, where <code>msxxxxxxx</code> is the TXT record that you added to DNS. Request assistance from your DNS hosting provider to enter information into the correct fields. Use one of the supported DNS providers.
<i>Replication delays</i>	It can take up to 72 hours for the DNS record to propagate. Changing the TTL value to 1 hour can help speed up this update process but that is not guaranteed.	Wait up to 72 hours for replication to happen. If 72 hours have elapsed, try removing and readding the verification record. Run the domain troubleshooter from the admin center.
<i>Domain already registered</i>	If you created another account for Office 365 and registered the domain with that account, you will not be able to register that domain with your new account. This issue can arise where you are migrating Office 365 accounts, for example from a midsized business account to an enterprise account.	Log onto the original account and remove the domain. You must ensure that the domain is not being used for any purpose in Office 365.



More information about removing a domain from Office 365 is available at the following link:

<http://go.microsoft.com/fwlink/?LinkId=390889>

Note that you can cause errors if you update DNS records after provisioning a domain in Office 365.

Recommendations for Domain Configuration

When you are registering domains with Office 365, you should apply the following best practices.

- Identify the domains you need to register with Office 365, along with any subdomains.
- Check that none of these domains are currently registered with Office 365.
- Check that you can make the required changes to your current DNS provider.
- Register root domains first, followed by subdomains.
- Ensure that the root domain registration completes before registering the subdomain.
- Use NSLOOKUP to check that each added DNS record exists and is correct.
- Allow for DNS replication time.
- After registration, move on to configuring DNS settings.
- Document all the changes you have made, both in Office 365 and at the DNS provider's site.

- Identify domains to register
- Check none are currently registered with Office 365
- Check that you can add DNS records to the domain
- Complete root domain registration before registering subdomains
- Use NSLOOKUP to check DNS entries
- Allow for replication
- Move on to configuring DNS settings
- Document the changes you have made

Lesson 2

Recommend a Mailbox Migration Strategy

Because email is seen as a mission-critical service for businesses of all sizes, it is not surprising that the migration of an organization's messaging system to Exchange Online is the highest profile change to make as part of the move to Office 365. You should remember that, while the FastTrack approach takes a more direct route to service adoption, it does not provide a shortcut in terms of analyzing an organization's needs and ensuring that the migration approach fits these needs.

This lesson covers approaches to email migration, which include cutover, staged, and IMAP. It also briefly touches on hybrid and long-term coexistence, although these mechanisms are beyond the scope of this course.

Lesson Objectives

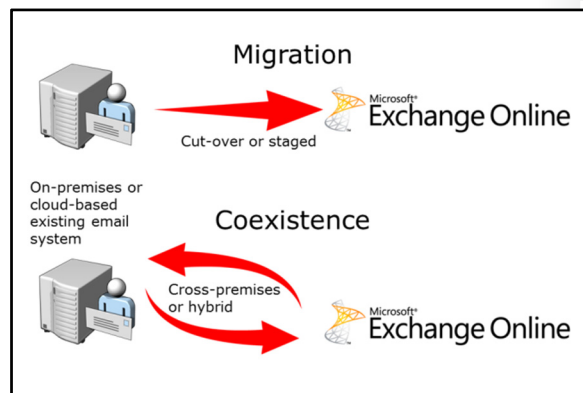
After completing this lesson, you should be able to:

- Provide an overview of the migration and coexistence approaches with Exchange Online.
- List the migration options and summarize the factors for each approach.
- Explain the cutover migration approach and highlight the planning factors for that method.
- Describe staged migration.
- Outline hybrid Exchange deployments and identify when they are useful.
- Describe IMAP migration.
- Describe PST migration.
- Explain the public folder migration process.
- Identify the planning decisions that indicate which option you should select.
- List additional planning factors with Exchange Online migrations.


Mail Migration and Coexistence Overview

Part of the value that Exchange Online delivers within Office 365 is the flexibility that it gives to organizations in terms of migration and coexistence options. Exchange Online provides the class-leading features of Exchange Server 2013 in a public cloud environment and the migration and coexistence options facilitate implementation of this service. The two main approaches for moving to or integrating Exchange Online are:

- **Migration.** Your organization currently has either Exchange Server on-premises, a third-party email system, or another vendor's cloud-based mail service and you want to move them to Exchange Online before decommissioning their current system completely. The result is that only Exchange Online handles messaging for the organization. Migrations can be either cut-over, which moves the entire organization in one pass, or staged, where the users are moved in batches and there is a temporary coexistence phase.

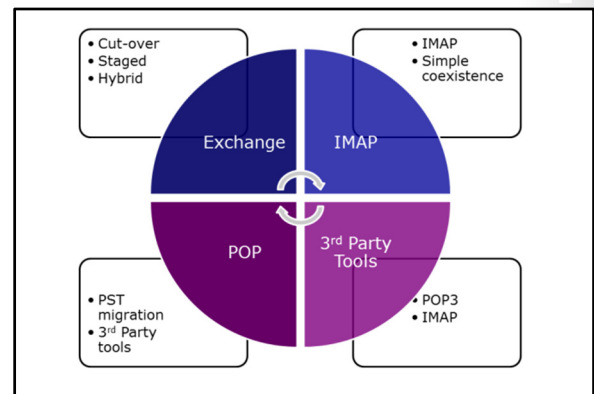


- Coexistence.** Your organization currently has an on-premises mail system and you want to integrate that environment with Exchange Online. Coexistence can either be cross-premises, supporting basic features such as a shared global address list, or hybrid, where there is full interoperability between the online and on-premises environments, including onboarding and offboarding facilities, free/busy integration, and delegation. Hybrid coexistence requires Directory Synchronization and typically would use single sign-on (SSO) for authentication.

 **Note:** Exchange Server long-term hybrid deployments are not covered in detail in this course.

Migration Options

The following topic summarizes the migration and co-existence options and highlights for each approach when that option is most likely to be suitable.



Migration Approach	Source Email	Mechanism	Advantages	Disadvantages
Cutover Exchange Migration	Exchange 2003 or later	Outlook Anywhere connection to mailboxes	<ul style="list-style-type: none"> Simple and most direct approach Migrates all users in a weekend Migrates all user mailbox information 	<ul style="list-style-type: none"> Max 2,000 users
Staged Exchange Migration	Exchange 2003 or 2007	Outlook Anywhere connection to mailboxes	<ul style="list-style-type: none"> Relatively simple No hybrid Exchange requirement Works with more than 2,000 users Migrates all user mailbox information 	<ul style="list-style-type: none"> Requires a co-existence period with users on old and new systems
Hybrid Migration (co-existence)	Exchange 2010 or 2013	Hybrid Exchange federation between on-premises and Exchange Online	<ul style="list-style-type: none"> Allows for longer migration time Maintains full Exchange usability during migration Works with more than 	<ul style="list-style-type: none"> Requires configuration of Hybrid Exchange wizard

Migration Approach	Source Email	Mechanism	Advantages	Disadvantages
		organizations	2,000 users <ul style="list-style-type: none"> Migrates all user mailbox information 	
IMAP Migration	Any IMAP-accessible email server	IMAP connection to user mailboxes	<ul style="list-style-type: none"> Compatible with most email servers, including Exchange Server 2000 and 5.5 	<ul style="list-style-type: none"> Only migrates the user's inbox
PST migration	POP3 email server with PST mail storage	Migration tool to connect to PST files	<ul style="list-style-type: none"> Works with third-party POP3 servers using Outlook client Migrates all mailbox folders 	<ul style="list-style-type: none"> Only works with Outlook clients
Third-party migration	POP3/IMAP servers	Custom migration tool to connect to user mailboxes	<ul style="list-style-type: none"> Works with email servers not covered by other methods 	<ul style="list-style-type: none"> Variable levels of information migration

In addition to these mechanisms, there is also cross-premises or simple co-existence. However, this is not a migration approach, as you would use either IMAP migration or staged IMAP migration to move to Exchange Online.


Cutover Exchange Migration

If your organization has Exchange Server 2003 or later and fewer than 2,000 users, a cutover Exchange migration is the preferred option. When contemplating this move, you should plan for the following factors before starting the migration process:

- Mailbox access.** Exchange Online uses Outlook Anywhere (formerly known as Remote Procedure Calls over HyperText Transfer Protocol, or RPC over HTTP) to connect to the Exchange Server organization. If Outlook Anywhere is not enabled you need to plan to add that service.
- Certificates.** Outlook Anywhere requires a third-party trusted SSL certificate with a principal name that matches the external host name of the published service. Self-signed certificates cannot be used. You can use the Exchange Remote Connectivity Analyzer to check the connection to Outlook Anywhere. Alternatively, you can simply check that you can connect to a mailbox over Outlook.

- Mailbox access
- Certificates
- Permissions
- Domains
- Unified Messaging

- *Permissions.* To perform the migration, you need to connect with an account that has sufficient access rights on the mailbox database. These permission settings depend on which version of Exchange you are connecting to.
- *Domains.* You must have previously added your existing SMTP domain as a managed domain in Office 365. This is a requirement because the migration process uses the SMTP address of the on-premises mailbox to create the Office 365 cloud-based identity and email address. Migration will fail if your Exchange domain is not an accepted domain (or the primary domain) of your cloud-based organization.
- *Unified Messaging.* If the mailboxes you are migrating are enabled for Unified Messaging (UM) you have to disable UM on the mailboxes before you migrate them. You can enable UM on the mailboxes after the migration is complete. This planning is covered in the next module.
- *Public folders.* The latest service update to Office 365 now supports Public Folders. Public folder migration is covered in a later topic.


 **Note:** If you have activated and installed the Microsoft Online Services Directory Synchronization tool, you cannot run a cutover Exchange Migration. If you have already installed the directory synchronization tool, you can deactivate directory synchronization and then run a cutover Exchange migration.

After planning is complete, the steps you must perform to complete the migration process are relatively simple. They include:

1. Create the migration batch.
2. Configure the connection settings.
3. Name the migration batch.
4. Start the migration batch.
5. Configure your MX record to point to Office 365.
6. Delete the migration batch.

After you complete the migration process, you must:

- Assign licenses to users.
- Create an autodiscover DNS record.
- Implement SSO if required.
- Decommission the on-premises Exchange Server computers.

 **Best Practice:** If you implement a single sign-on solution, you are strongly recommended to maintain at least one Exchange server so that you can access Exchange System Manager (Exchange 2003) or Exchange Management Console/Exchange Management Shell (Exchange 2007 and Exchange 2010) to manage mail-related attributes on the on-premises mail-enabled users. For Exchange 2007 and Exchange 2010, the Exchange server that you maintain should have the Hub Transport, Client Access, and Mailbox server roles installed.

 **For more information about performing an Exchange cutover migration, see the following:**

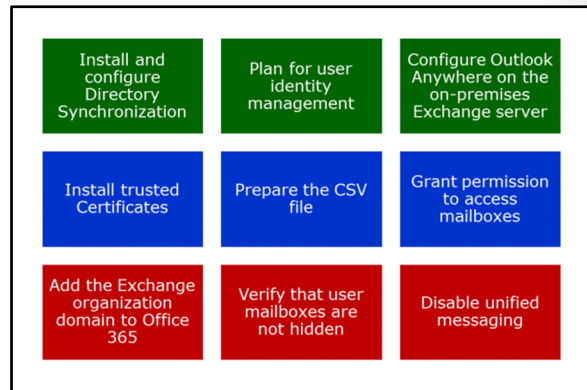
<http://go.microsoft.com/fwlink/?LinkId=321125>

Staged Exchange Migration

If your organization has Exchange Server 2003 or Exchange 2007 with 2,000 users or more, you will need to plan for a staged Exchange migration. However, a staged Exchange migration is more than just a series of cutover migrations because you need to establish cross-premises coexistence for the period of the migration. The remaining factors are the same as for a cutover migration.



Note: There is no limit to the number of mailboxes that you can migrate to the cloud using a staged Exchange migration. However, the CSV file for a migration batch can contain a maximum of 2,000 rows. To migrate more than 2,000 mailboxes, you have to submit additional CSV files.



The staged migration is intended for organizations that desire a shorter period of coexistence from their existing Exchange mail environment to Exchange Online. User identities will automatically be provisioned by the Windows Azure Active Directory Sync tool. After all the users are migrated to Exchange Online you can then deploy single sign-on.

This type of migration also enables you to maintain coexistence between your on-premises and Office 365 email organizations. In this scenario, you can move some mailboxes to Exchange Online while maintaining the rest of the mailboxes in your on-premises mail environment.

The email migration itself is performed through the Exchange Control Panel and a CSV file. You must also use the Windows Azure Active Directory Sync tool to keep your on-premises Active Directory synchronized with Office 365 and Exchange Online.

Migration process

When you use a staged Exchange migration and CSV file to migrate on-premises Exchange mailboxes to the cloud, the migration service performs the following tasks for each migration batch that you run:

- It verifies that OLSync or the Directory Synchronization tool is enabled for your cloud-based organization.
- It checks that a mail-enabled user exists in the cloud-based email organization for each entry in the CSV file.
- It converts the mail-enabled user to a mailbox.
- It configures mail forwarding by populating the TargetAddress property on the on-premises mailbox with the email address of the cloud-based mailbox. This enables email sent to an on-premises mailbox to be forwarded to the corresponding cloud-based mailbox.
- It migrates email messages, contacts, and calendar items from the Exchange mailboxes to the corresponding cloud-based mailboxes. After mailbox items are migrated, the Exchange and cloud-based mailboxes are not synchronized. New email sent to the on-premises Exchange mailbox is forwarded to the corresponding cloud-based mailbox.
- It sends an email message to the administrator when the migration batch is complete. This message lists the number of mailboxes that were successfully migrated and how many could not be migrated. The message also includes links to migration statistics and error reports that contain more detailed information.

Monitoring of the migration batches is carried out through the Office 365 Admin console.

Planning activities

You must plan for the following activities before starting a staged Exchange migration:

- *Install and configure directory synchronization.* The Directory Sync tool must be running to perform a staged email migration. The directory synchronization tool creates the mail-enabled users in the organization's tenant account that are converted to mailboxes during the migration.
- *Plan for user identity management.* After the on-premises mailboxes are migrated to the cloud, the synchronization process continues to update the user attributes on the mailbox according to changes made in the on-premises Active Directory. Because of this, the "source of authority" for managing user objects is the on-premises directory; therefore, you cannot manage user mailbox properties in Exchange Online. However, after running a staged Exchange migration you can configure directory synchronization so that the source of authority is the Office 365 directory, which will enable management of mailbox properties in Exchange Online.
- *Configure Outlook Anywhere on the on-premises Exchange server.* As with a cutover migration, the migration service uses RPC over HTTP, or Outlook Anywhere, to connect to the on-premises Exchange server.
- *Install trusted certificates.* The Outlook Anywhere configuration must be configured with a certificate issued by a trusted third-party certification authority (CA). It cannot be configured with a self-signed certificate. Also, the principal name on the certificate must match the host name of the external IP for the on-premises server.
- *Prepare the CSV file.* Identify the group of users whose on-premises mailboxes are to be migrated to the cloud. Include these users in the CSV file that will make up the migration batch. Mailboxes are migrated in the same sequence listed in the CSV file. The attributes in the CSV file are **EmailAddress** (required), **Password** (optional), and **ForceChangePassword** (optional).
- *Grant permission to access mailboxes.* The on-premises migration account must have the necessary permissions to access all user mailboxes. You can assign the Full Access permission for individual mailboxes or assign the Receive As permission for a mailbox database.
- *Add the Exchange organization domain to Office 365.* The migration service uses the SMTP address of the on-premises mailboxes to create email addresses for the new cloud-based mailboxes.
- *Verify that user mailboxes are not hidden in on-premises address lists.* Migration will fail for on-premises mailboxes that are hidden from address lists.
- *Disable Unified Messaging.* If mailboxes are enabled for Unified Messaging (UM), disable UM before the migration. You can then enable UM on the mailboxes after the migration is complete.

Migration steps

The migration steps are very similar to that with a cutover migration, except that there are multiple batches:

1. Create a migration batch.
2. Configure the connection settings.
3. Upload the CSV file and name the migration batch.
4. Start a migration batch.
5. Convert on-premises mailboxes to mail-enabled users.
6. Create and start additional migration batches.

7. Delete the migration batches.



For more information about performing a staged migration, see the following:

<http://go.microsoft.com/fwlink/?LinkId=321126>

Hybrid Exchange

A hybrid Exchange implementation is different in the two previous examples, in that it can be used as both a migration path and a permanent arrangement. A hybrid Exchange environment can provide the smoothest migration to Office 365, or it can be used to keep a mix of on-premises mail users and Office 365 mail users for an extended period of time. A hybrid deployment provides a unified email experience for the organization, enabling users with mailboxes in the on-premises Exchange Server environment and users with Exchange Online mailboxes to find each other in the global address list, and to send, receive, and reply to email regardless of which system is hosting their mailbox.

Feature	Cross-Premises	Hybrid
Mail routing between on-premises and online	✓	✓
Unified global address list	✓	✓
Free/Busy and calendar sharing cross-premise	✗	✓
Out of Office understands that cross-premises is "internal"	✗	✓
Mail-tips, messaging tracking, and mailbox search cross-premises	✗	✓
Outlook Web App redirection cross-premises (single Outlook Web App URL)	✗	✓
Can route outbound mail through on-premises (allows address rewrite, transport agents)	✗	✓
Secure mail routing (TLS plus Mutual Authentication) cross-premises	✗	✓
Exchange Management Console (on-premises) used to manage cross-premises mailbox migrations	✗	✓
Mailbox moves support for onboarding and offboarding	✗	✓
No OST re-sync after mailbox migration	✗	✓



Note: A hybrid Exchange implementation is also required where you have an organization with more than 2,000 users and Exchange 2010 or Exchange 2013 and you want to migrate completely to Exchange Online. The hybrid Exchange wizard considerably simplifies the process of configuring this federated environment.

A hybrid deployment offers organizations the ability to extend the feature-rich experience and administrative control they have with their existing on-premises Microsoft Exchange organization to the cloud. A hybrid deployment also provides the seamless look and feel of a single Exchange organization between an on-premises Exchange Server 2013 organization and Exchange Online in Microsoft Office 365. As mentioned earlier, a hybrid deployment can serve as an intermediate step to moving completely to an Exchange Online organization.

A hybrid deployment provides the following advantages:

- Exchange Online and on-premises users can share free/busy calendar data.
- Administrators can use the Exchange Administration Center (EAC) to manage both the Exchange Online and on-premises Exchange mail environments.
- Administrators can use powerful and familiar Exchange management tools to move users to Exchange Online.
- Outlook profiles for users are automatically updated to the Exchange Online environment when the Exchange hybrid deployment and Autodiscover are configured appropriately. Administrators do not need to manually reconfigure Outlook profiles or resynchronize .OST files after moving users' mailboxes.
- Outlook Web App redirection allows for redirection from the on-premises Outlook Web App environment to the Office 365 Outlook Web App environment. You specify a target URL for your organization (for example, www.outlook.com/contoso.com).

- MailTips, out-of-office messages, and similar features understand that Office 365 and on-premises users are part of the same organization.
- Delivery reports and multi-mailbox search work with users who are on-premises and those working in Exchange Online.
- Authentication headers are preserved during cross-premises mail flow, so all mail looks and feels like it is internal to the company (for example, recipient names resolve in the global address list).
- If necessary, administrators can easily move mailboxes back to the on-premises Exchange environment.

The following table summarizes these benefits and compares hybrid Exchange with cross-premises (simple) coexistence:

Feature	Cross-Premises	Hybrid
Mail routing between on-premises and online	✓	✓
Unified global address list	✓	✓
Free/Busy and calendar sharing cross-premise	✗	✓
Out of Office understands that cross-premises is "internal"	✗	✓
Mail-tips, messaging tracking, and mailbox search cross-premises	✗	✓
Outlook Web App redirection cross-premises (single Outlook Web App URL)	✗	✓
Can route outbound mail through on-premises (allows address rewrite, transport agents)	✗	✓
Secure mail routing (TLS plus Mutual Authentication) cross-premises	✗	✓
Exchange Management Console (on-premises) used to manage cross-premises mailbox migrations	✗	✓
Mailbox moves support for onboarding and offboarding	✗	✓
No OST re-sync after mailbox migration	✗	✓

IMAP Migration

If your company is a small organization with an email environment that supports IMAP connections, a quick cutover to Exchange Online services with no coexistence is the recommended approach. User identities are automatically provisioned with the IMAP migration tool available from the Exchange Control Panel. Note that you will need to create Exchange Online mailboxes before beginning this process. After the cutover is complete, single sign-on may be deployed as part of the Enhance phase.

- Courier-IMAP
- Cyrus
- Dovecot
- UW-IMAP
- Exchange 2010
- Exchange 2007
- Exchange 2003
- Exchange 2000
- Exchange 5.5



Note: IMAP migration does not migrate contacts and calendar items. If the organization requires migration of contact and calendar items, use either PST migration or a third-party migration tool.

You can use the Email Migration tool in the Exchange Control Panel and a CSV file to migrate the contents of users' mailboxes from an IMAP messaging system to their Exchange Online mailbox. Supported IMAP servers include the following:

- Courier-IMAP
- Cyrus
- Dovecot
- UW-IMAP
- Exchange 2010
- Exchange 2007
- Exchange 2003

Exchange 2000 and Exchange 5.5 also support IMAP connections, and you can use IMAP as a migration approach with these platforms.



For more information about performing an IMAP migration, see:

<http://go.microsoft.com/fwlink/?LinkId=524335>

With larger IMAP migrations a temporary coexistence phase may be required. It is also possible to have permanent coexistence with non-Exchange Server systems.



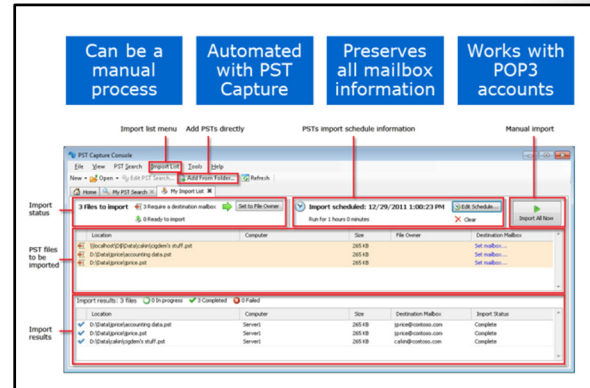
Note: During the migration, Exchange Online creates fewer than 10 connections to the IMAP server to avoid overusing the remote server's resources and bandwidth.

PST Migration

PST Migration is a method for getting user email, calendar items, contacts, and tasks into Exchange Online. It is most likely to be used with a third-party email system in which users employ Outlook to connect to the mail server over POP3.

Manual import

PST migration can be performed entirely as a user-driven migration. Here, you create a new Office 365 account and an Exchange Online mailbox for the user and provide them with the credentials to connect. The user then attaches his or her old .PST file to the new Exchange Online account; this allows the user to access all emails, calendar items, contacts, and tasks.



PST Capture

Microsoft Exchange PST Capture enables a network administrator to search for PST files on computers in an organization and then import those files into mailboxes hosted in Exchange Online. PST Capture is comprised of the following components:

- *PST Capture Central Service.* At the heart of PST Capture is the PST Capture Central Service. The Central Service maintains the list of all PST files found in an organization and manages the data as it is moved to Exchange Online.
- *PST Capture Agent.* Discovery of the PST files is performed by PST Capture agents that are installed on client computers. The agents also send the PST files they find to the host computer when an import operation is started on the PST Capture Console.
- *PST Capture Console.* The PST Capture Console is the interface used to configure PST searches, specify the target mailboxes for PST files, and track the status of PST import operations and reports. The administrator can also use the console to import PST files stored on network-attached storage (NAS) devices, since PST agents cannot be installed on NAS devices.

For optimal operation, the PST Capture Central Service and the PST Capture Console should run on a dedicated computer, known as the PST Capture host computer.

The following image shows the PST Capture Console user interface:

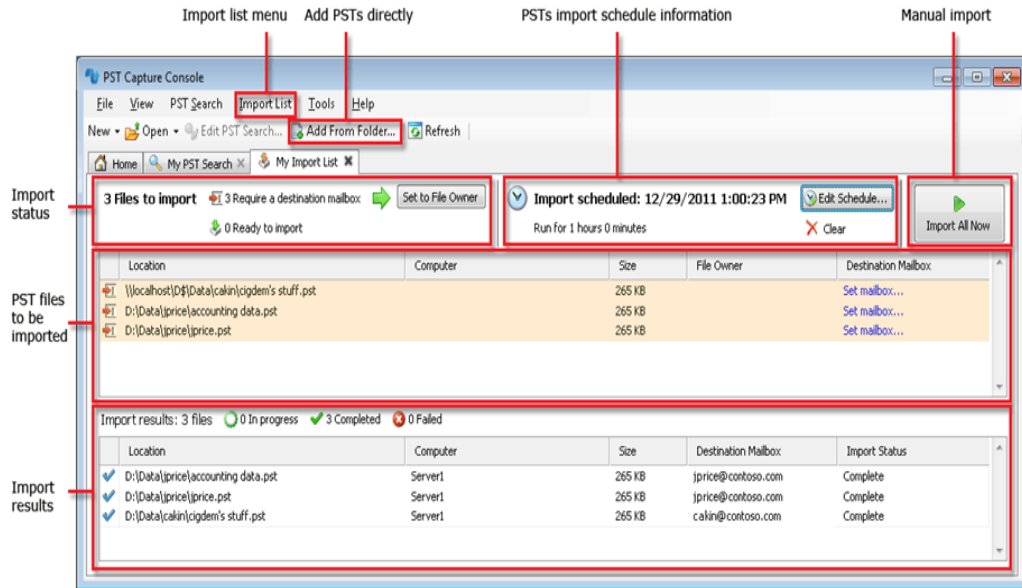



FIGURE 5.3: PST CAPTURE CONSOLE USER INTERFACE

If using PST Capture, you must consider the following planning factors:

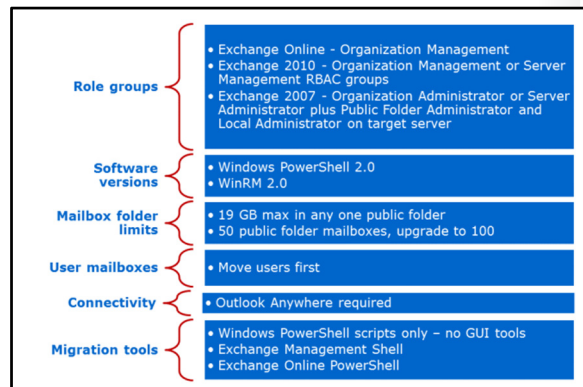
- *Network utilization.* PST Capture has considerable impact on network utilization when transferring PST data over the network. The PST files are copied from the clients to the host computer and from there to Exchange Online. Therefore, you must plan for this additional traffic and the effect it will have on the Internet connection.
- *Permissions.* PST Capture requires a service account. Depending on how you use PST Capture, a different set of permissions is required for the service account. Typically, the requirement is to be logged on with Local Administrator permissions. Other connecting accounts must either have the Organization Management role or be an Exchange Online Administrator account.

 **Additional Reading:** For more information about PST Capture, see the following article: <http://go.microsoft.com/fwlink/?LinkId=321127>

Public Folder Migration

Exchange Online, with the version 15 tenant of Office 365, now supports public folders. If your organization is using public folders, this factor requires additional planning and extra steps in the migration.

Public folders in Exchange Online have a fundamentally different architecture to those in other versions of Exchange. In essence, Exchange Online holds public folder data in a series of mailboxes. The first public folder mailbox you create holds the folder hierarchy while the remaining mailboxes store the data.





Note: A key factor with migrating public folders is that Exchange 2003 SP3 is not a supported platform for this migration process. Therefore, if you are planning to migrate public folder data to Exchange Online where the organization is running Exchange 2003, they must introduce one or more Exchange 2010 SP3 or Exchange 2007 SP3 RU10 servers, moving the public folders and all replicas to those servers.

The following sections outline the planning factors that you must consider when migrating public folders:

Role groups

In Exchange Online, you must be a member of the Organization Management role group. This role group is different from the permissions assigned to you when you subscribe to Exchange Online. In Exchange 2010, you must be a member of the Organization Management or Server Management RBAC role groups. In Exchange 2007, you need to be assigned the Exchange Organization Administrator role or the Exchange Server Administrator role. In addition, you must be assigned the Public Folder Administrator role and local Administrators group for the target server.

Software versions

If migrating from an Exchange 2007 server, upgrade to Windows PowerShell® 2.0 and WinRM 2.0 for Windows Server 2008 x64 Edition.

Mailbox folder size and limits

Before migration, if any public folder in your organization is greater than 19 GB, we recommend either deleting content from that folder or splitting it up into multiple public folders. If either of these options is not feasible, we recommend that you do not move your public folders to Exchange Online.

In Exchange Online, the default limit is 50 public folder mailboxes. Exchange Online will allow you to automatically upgrade to 100 public folder mailboxes if you exceed this amount. If you need to exceed 100 public folder mailboxes, contact Exchange Online support to request additional public folder mailboxes and your request will be evaluated.

User mailboxes

Before you migrate your public folders, we recommend that you first move all user mailboxes to Exchange Online.

Connectivity

Outlook Anywhere must be enabled on the legacy Exchange server.

Migration tools

You have to use Windows PowerShell cmdlets with either Exchange Management Shell (EMS) for on-premises servers or Exchange Online PowerShell for this migration, because the Exchange Admin Center (EAC) and Exchange Management Console (EMC) are not supported.

The overall process that you need to introduce into your migration plan is as follows:

1. Download the migration scripts.
2. Prepare for the migration.
3. Generate the .csv files.
4. Create the public folder mailboxes in Exchange Online.
5. Start the migration request.
6. Lock down the public folders on the legacy Exchange server for final migration (downtime required).

7. Finalize the public folder migration (downtime required).
8. Test and unlock the public folder migration.

Discussion: Email Migration

Discuss the following topics related to email migration:

What types of email migration have you already implemented?

If you have already implemented a mail migration to Exchange Online, what type and size was it? If you can, please provide information about:

- Initial messaging environment
- Directory service type
- Selected migration path
- Number of users
- Mailbox size
- Bandwidth
- Time to migrate

What were the challenges?

Describe any particular challenges you experienced. Challenges can fall into one or more of the following categories:

- Organizational
- Technical
- Business
- Political
- Personal

What were the lessons you learned from this process?

List any items that you learned from the deployment process, highlighting anything that you wished you had known before the start of the project.

- What types of email migration have you already implemented?
- What were the challenges?
- What were the lessons you learned from this process?

Exchange Online Migration Planning Factors

When considering what approach suits your organization best, you need to identify information about the following factors:

- What is their current email system?
 - On-premises or cloud-based
 - Exchange Server or third-party
 - Which version?
 - What service packs?
 - What is their system performance?
- How many users do they have?
 - Under 2,000
 - Over 2,000
- How do those users access their mailboxes?
 - POP3
 - IMAP
 - MAPI
 - Outlook Anywhere
 - Web/Outlook Web Access
- What features are they currently using?
 - Global address lists
 - Mailbox delegation
 - Free/busy
 - Public folders
 - Custom applications, such as Contact Relationship Management integration
- How much mail data is there?
 - Average mailbox size
 - Total mailbox data
 - Public folder data
- What is the quality of the organization's Internet connection?
 - Download and upload speeds
 - Latency
 - Reliability
 - Supplier

- Current email system
- User numbers
- Access mechanism
- Feature usage
- Mail data volume
- Internet connection

With this information, you can identify possible migration routes and remove others from consideration.

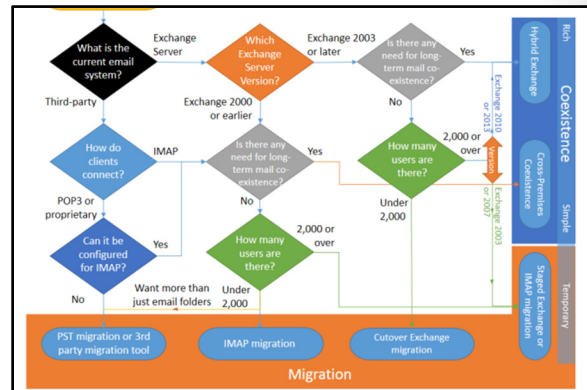
Email Migration Flowchart

With answers to the Exchange Online planning factors, you can now start to triage the possible options, eliminating from further consideration those that will not work for your organization. You should note that this triage process only highlights the main choices in selecting the correct option for Exchange Online migration or coexistence.

You should analyze the following options when identifying the best method for email migration:

- **Current email system.** If your organization has some version of Exchange Server on-premises, and depending on the version of Exchange, you can look at the full range of migration options. If it currently runs a third-party mail system then the Exchange Server options are not available, and you need to identify the connection mechanism.
- **Exchange Server version.** If the organization has Exchange Server on-premises then you need to identify the version. If it is Exchange Server 2000 or earlier, IMAP, PST, or third-party tools are the available migration routes. If it has Exchange 2003 or later then there are options for hybrid coexistence or staged Exchange migration.
- **Long-term coexistence with Exchange.** If the organization wants to keep its on-premises Exchange server, the recommended route is for the Hybrid Exchange server. This approach also works with Exchange Server 2003 (running SP2) and Exchange Server 2007 SP3 RU10 if there is an Exchange 2010 SP3 gateway server on-premises.
- **User numbers.** If the organization has Exchange, but does not want long-term coexistence, the final deciding factor is the number of users. If there are fewer than 2,000 users, the recommendation is an Exchange cutover migration. However, if there are 2,000 or more mailboxes to migrate, then you need to review the version of Exchange Server again. If it is Exchange 2003 or 2007, then staged migration is the answer. If the organization is using Exchange 2010 or Exchange 2013, then you need to implement a temporary hybrid Exchange arrangement while mailboxes are migrated.
- **IMAP connections.** If IMAP is or can be made available as a protocol to connect to the existing email system, an IMAP migration is possible. However, if IMAP is not available on non-Exchange Server systems, migration will need to be PST-based or use a third-party tool.
- **IMAP cross-premises coexistence.** There is a lower probability option with existing IMAP-based mail systems for implementing cross-premises coexistence. This approach might be necessary with third-party email systems where there are more than 2,000 users.
- **POP3 or proprietary connections.** If the third-party email system only provides POP3 or a proprietary protocol over which users connect to their mailboxes, the only migration options are:
 - PST migration if the users have Outlook.
 - Third-party POP3-based migration tool if they do not use Outlook.

The following diagram displays the overall triage process.



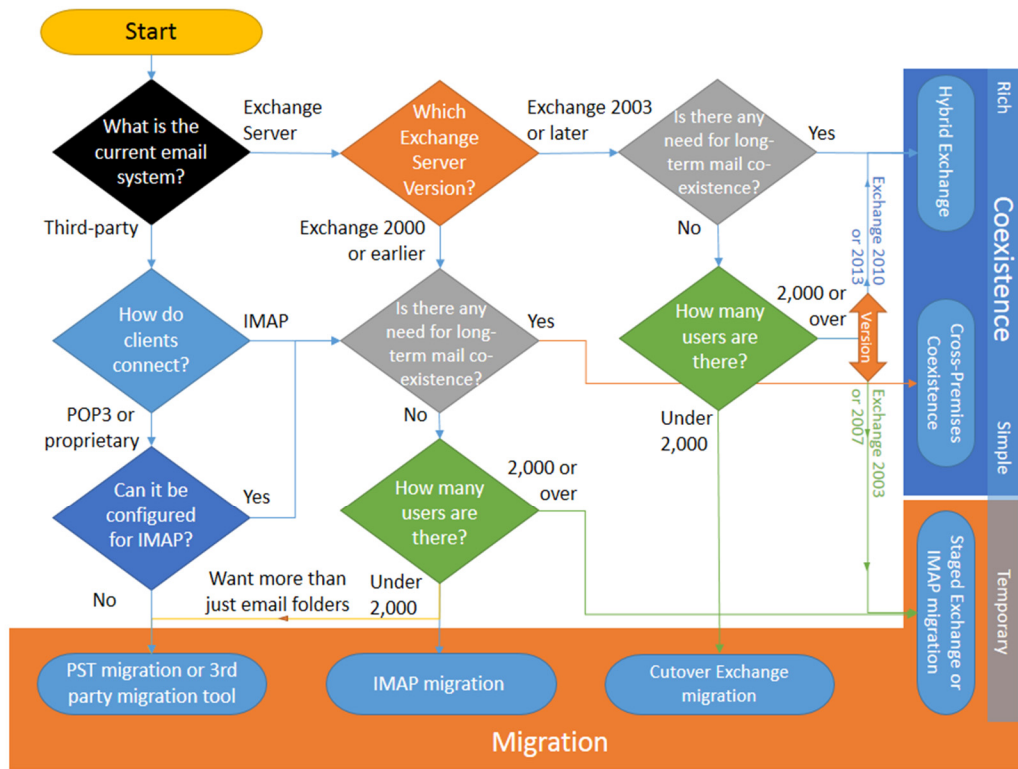
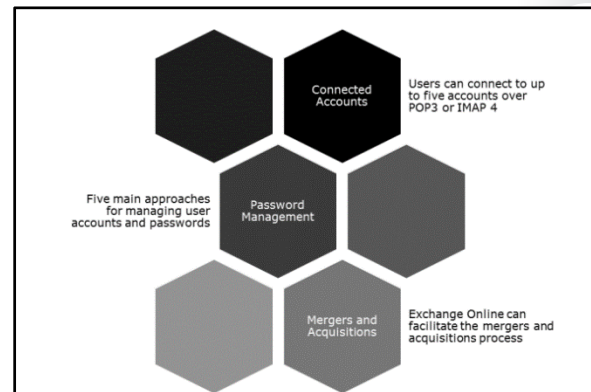


FIGURE 5.4: FLOWCHART TO ASSIST WITH SELECTING THE BEST EMAIL MIGRATION OR CO-EXISTENCE OPTION FOR EXCHANGE ONLINE

Additional Factors with Mailbox Migration

Connected Accounts

The connected accounts feature in Office 365 is a mechanism by which users can configure connections to multiple external accounts over IMAP or POP3 protocols and bring those messages into their Outlook mailbox in Office 365. This feature also enables organizations to implement Exchange Online during the Pilot Phase of a FastTrack deployment, providing users with the experience of receiving and managing email in their mailboxes, yet reverting to the existing email system if the organization does not decide to go ahead with the deployment. However, if you carry out a mail migration to Exchange Online, the connected account is merged into the new Exchange online mailbox.



Connected accounts are set up on a per-user basis and not by administrators. It is necessary, therefore, to train the users in the process of setting up the connection in their Office 365 administration console. Each user can connect to up to five different external email accounts.



The following link provides instructions on how to set up connected accounts:

<http://go.microsoft.com/fwlink/?LinkId=390890>

The lab practice at the end of this module takes you through this process.

Connected accounts are checked for new mail every hour and you can use inbox rules to sort incoming mail into different folders based on the recipient email address. So you can sort work email into one folder and Outlook.com personal messages into another.

Password Management

Password management during and after Exchange Online migration is an important factor to consider. Although later modules deal with this issue in greater detail, you have five main options in terms of managing passwords for Exchange Online.

Approach	Implications
Manage passwords only in Office 365	Requires removal of on-premises Active Directory. Only practicable with smaller organizations
Manage passwords both on-premises and in Office 365	Users may have two different sets of credentials to manage
Implement DirSync without password sync	Users log on with one user name but potentially different passwords in on-premises and in Office 365
Implement DirSync with password sync	Users log on with one set of credentials with passwords managed in Active Directory
Implement Single Sign-On (SSO)	Users log on with one set of credentials or two-factor authentication (for example, smartcard) with passwords managed in Active Directory

If you are implementing hybrid Exchange, then you must use DirSync. You are also recommended either to use password sync or SSO so that users only have to provide one set of credentials and password management takes place in Active Directory.

Mergers and Acquisitions

Exchange Online offers a range of options that can assist during a merger or acquisition process between two organizations. These options include:

- Migrating both organizations to Exchange Online, while creating new email accounts and maintaining the old ones.
- Keeping one organization in its on-premises environment and moving the other organization to Exchange online separately.
- Keeping one organization in its on-premises environment and moving the other organization to Exchange Online in a hybrid Exchange arrangement, then onboarding the other organization to on-premises before decommissioning Exchange Online.
- Setting up hybrid Exchange and moving users from both organizations either to on-premises or Exchange Online as their job function dictates.

Discussion: Identify a Migration Strategy for Lucerne Publishing

As a class, discuss the most appropriate strategy for Lucerne Publishing to migrate to Exchange Online.

- Review the factors in the Lucerne Publishing environment
- Triage the possible migration routes and discard those that are not appropriate
- Identify the best approach for an organization of this size

Lab: Preparing for Exchange Migration

Scenario

After a successful Fast Track pilot, Lucerne Publishing has given approval to move on to the Deploy phase and is in the process of adopting Office 365. The team is the same, with Alain Richer providing partner support, Justin as the Project Manager, and Heidi as the main implementer.

The company now needs to ensure that:

- its DNS domains are registered with Office 365
- the DNS records are correctly configured
- all parent and subdomains are added
- the service records for different Office 365 services are configured

Objectives

The objectives of this lab are to:

- Add and configure domains and subdomains in Office 365.
- Configure certificates for use with Exchange Server and Active Directory Federation Services.
- Check that Outlook Anywhere is working for Office 365 to connect to on-premises Exchange Server.

Lab Setup

Estimated Time: 90 minutes

Virtual machine: 20346C-LUC-CL1

Username: **Student1**

Password: **Pa\$\$w0rd**

Where you see references in the steps to `lucernepublishingXXXX.onmicrosoft.com`, you should replace `XXXX` with the unique Lucerne Publishing number that you were assigned when you set up your Office 365 accounts in Module 1, Lab 1B, Exercise 2, Task 3, Step 5.

Where you see references to `labXXXXX.o365ready.com`, you should replace `XXXXX` with the unique `o365ready.com` number you were assigned when you registered your IP address at `www.o365ready.com` in Module 2, Lab 2B, Exercise 1, Task 2, Step 6.

Exercise 1: Configure Exchange Server for Cutover Migration

Scenario

Alain's planning sessions with Justin and Heidi have established that the most appropriate approach for Lucerne Publishing is to carry out a cutover migration from their on-premises Exchange Server to Exchange Online. This decision is based on the fact that Lucerne Publishing has Exchange Server 2013 and fewer than 2,000 users.

To prepare for this migration, Heidi verifies that all the DNS settings and security certificates are in place for the on-premises Exchange Server. By the end of this process, on-premises Exchange is properly configured for connections from Office 365.

The main tasks for this exercise are as follows:

1. Create the External DNS Zone in the DNS Console
2. Test that DNS Delegation is Working

3. Configure DNS Records for the On-Premises Exchange Server
4. Create a Certificate Signing Request for a Third-Party SSL Certificate
5. Request and Download a Certificate from a Public Certificate Authority
6. Install the Third-Party SSL Certificate
7. Configure Exchange Server To Use the Lab Certificate for Mail Services
8. Verify the Lab Certificate is Correctly Installed
9. Verify that Outlook Anywhere Works with On-Premises Exchange

► **Task 1: Create the External DNS Zone in the DNS Console**

1. On the **LUC-CL1** desktop, click **File Explorer** and navigate to **E:\Rdp_files**.
2. Double-click on **LUC-DC1.rdp** and log on as **LUCERNE\LucAdmin** with a password of **Pa\$\$w0rd**.
3. In **LUC-DC1**, press the Windows Key, and on the Start screen, click **Server Manager**.
4. In **Server Manager**, click the **Tools** menu and then click **DNS**.
5. In **DNS Manager**, expand **LUC-DC1**.
6. Click **Forward Lookup Zones**, then right-click and click **New Zone**.
7. In the **New Zone Wizard**, click **Next**.
8. In **Zone Type**, ensure the zone type is **Primary zone** and that **Store the zone in Active Directory** is not selected and click **Next**.
9. In the **Zone Name** page, enter your student DNS domain name in the form of **labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number) and click **Next**.
10. Select to **Create a new file** with a name of **labXXXXX.o365ready.com.dns** and click **Next**.
11. In the **Dynamic Update** page, ensure that **Do not allow dynamic updates** is selected, then click **Next**.
12. On the **Completing the New Zone Wizard** page, click **Finish**.
13. In **DNS Manager**, on the **View** menu, click **Advanced** to display the TTL value on records.

► **Task 2: Test that DNS Delegation is Working**

1. In **DNS Manager**, right-click **labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number) and click **New Alias (CNAME)**.
2. In the **Alias name** field, enter **www** as the alias name.
3. In the **Fully qualified domain name (FQDN) for target host** field, enter **www.microsoft.com**.
4. Click **OK** to close the **New Resource Record** dialog box.
5. Press the Windows key and on the **Start** screen, click **Windows PowerShell**.
6. In the Windows PowerShell window, type **NSLOOKUP** and press Enter.
7. At the NSLOOKUP arrow prompt, type **www.labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number) and press **ENTER**.

You should see a response such as:

Name: lb1.www.ms.akadns.net

Address: 134.170.188.84 (this will vary based on location)

Aliases: www.labXXXXX.o365ready.com

www.microsoft.com

toggle.www.ms.akadns.net

g.www.ms.akadns.net

8. Press the Windows key and on the **Start** screen, click **Internet Explorer**.
9. If the **Set up Internet Explorer** dialog box appears, click **Use recommended security and compatibility settings** and click **OK**.
10. In the **Address** field, enter **www.labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number).
11. If the **Internet Explorer security warning** appears, click **Close**.
12. Confirm that the web request redirects to the Microsoft website.
13. Close Internet Explorer.
14. Switch back to **DNS Manager**.
15. In the **labXXXXX.o365ready.com** zone (where XXXXX is your unique o365ready.com number), right-click the **www - Alias (CNAME)** record and click **Delete**.
16. In the **DNS** confirmation box, click **Yes**.

► **Task 3: Configure DNS Records for the On-Premises Exchange Server**

1. On **LUC-DC1**, in **DNS Manager**, right-click on the **labXXXXX.o365ready.com zone** (where XXXXX is your unique o365ready.com number) and select **New Host**.
2. In the **New Host** dialog box, in the **Name** field, enter **mail**.
3. In the **IP address** field, enter the external IP address for the Lucerne Publishing datacenter that you recorded in Module 2, Lab B, Exercise 1, Task 2, Step 2.
4. Click **Add Host**, and then in the **DNS message** box, click **OK**.
5. Click **Done**.
6. Switch to Windows PowerShell.
7. Enter the following command and press Enter:
PING mail.labXXXXX.o365ready.com (where XXXXX is your unique o365ready.com number).
8. Confirm that **mail.labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number) resolves to the external IP address of the Lucerne Datacenter.
Note: You will not get a response from the PING command.
9. In **DNS Manager**, right-click the **labXXXXX.o365ready.com** zone (where XXXXX is your unique o365ready.com number) and click **New Mail Exchanger**.
10. In the **Mail Exchanger (MX)** tab, leave the **Host or child domain** field blank.
11. In the **Fully qualified domain name (FQDN) of mail server**, enter **mail.labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number).
12. Leave the **Mail server priority** as **10**.
13. Click **OK** to create the mail server record.

14. In DNS Manager, right-click the **labXXXXX.o365ready.com zone** (where XXXXX is your unique o365ready.com number) and click **New Alias (CNAME)**.
15. In the **Alias (CNAME)** tab in the **Alias name** field, enter **autodiscover**.
16. In the **Fully qualified domain name (FQDN) for target host**, enter **mail.labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number).
17. Click **OK**.
18. Switch to Windows PowerShell.
19. Enter the following command and press Enter:
PING autodiscover.labXXXXX.o365ready.com (where XXXXX is your unique o365ready.com number).
20. Confirm that this request resolves to **mail.labXXXXX.o365ready.com**.
Note: You will not get a response from the PING command.
21. Switch to **LUC-CL1**.
22. Press the Windows key and in the **Start** screen, type Control and click **Control Panel**.
23. In **Control Panel**, click **Programs**.
24. Under **Programs and Features**, click **Turn Windows features on or off**.
25. In the **Windows Features** dialog box, select the **Telnet Client** check box, then click **OK**.
26. On the **Windows completed the requested changes** page, click **Close**.
27. Press the Windows key and in the **Start** screen, type **Command** and click **Command Prompt**.
28. In the **Command Prompt**, type **telnet** and press Enter.
29. At the Telnet prompt, type the following on one line and press Enter (where XXXXX is your unique o365ready.com number):
Open mail.labXXXXX.o365ready.com 25
30. You should receive a response similar to the following:
220 LUC-EX1.lucernepublishing.local Microsoft ESMTTP MAIL Service ready at (date),(time).
31. Type **EHLO** and press enter.
32. A list of commands starting with 250 should appear.
33. Close the command prompt window.

► **Task 4: Create a Certificate Signing Request for a Third-Party SSL Certificate**

1. On **LUC-CL1**, in the **E:\RDP_files** folder, double-click **LUC-EX1.rdp** and log on as **LUCERNE\LucAdmin** with a password of **Pa\$\$w0rd**.
2. On the **Do not ask me again for connections to this computer** message, click **Yes**.
3. On **LUC-EX1**, on the Start screen, click **Exchange Management Shell**.
4. To create a new certificate request for the on-premises services, at the Exchange Management Shell command prompt type the following command, and press Enter.

```
$Data = New-ExchangeCertificate -GenerateRequest -SubjectName "c=US,o=Lucerne Publishing, cn=fs.labXXXXX.o365Ready.com" -DomainName
```

mail.labXXXXX.o365Ready.com, autodiscover.labXXXXX.o365Ready.com, labXXXXX.o365Ready.com -PrivateKeyExportable \$true

- To export the new certificate request to a file, at the Exchange Management Shell command prompt type the following command, and press Enter.

Set-Content -path "C:\Temp\LabCertReq.txt" -Value \$Data

(where XXXXX is your unique o365ready.com number)

► **Task 5: Request and Download a Certificate from a Public Certificate Authority**

- On **LUC-EX1**, on the taskbar, click **File Explorer**, and browse to **C:\Temp**.
- Double-click **LabCertReq.txt**, to open it in Notepad.
- In Notepad, press CTRL+A, to select all the contents of the file, and then press CTRL+C to copy the contents.
- Close Notepad.
- Press the Windows key to go to the Start screen, and then click **Internet Explorer**.
- If you get a **Windows Internet Explorer 10** dialog box, select **Use recommended security and compatibility settings**, and then click **OK**.
- In the Address box, type **https://www.digicert.com/friends/exchange.php**, and press Enter.
- On the **Exchange Ignite CSR Submission** page, in the **Paste CSR** box, right-click inside the box, and then click **Paste**.
- Under **Certificate Details**, in the **Common Name** box, verify the common name is **fs.labXXXXX.O365Ready.com**, (where XXXXX is your unique o365ready.com number).
- Review the **Subject Alternative Names** information and verify the names are correct for **mail.labXXXXX.o365ready.com**, **autodiscover.labXXXXX.o365ready.com**, and **labXXXXX.o365ready.com**.

WARNING: If ANY of the subject alternative names are missing, then something went wrong in the prior task. If this occurs, you must: 1) go back and repeat the prior task (Create a Certificate Signing Request for a Third-Party SSL Certificate), and then 2) restart the steps in this task.

All the subject alternative names listed here must be correct before you can proceed; otherwise, future lab steps will fail.

- Under **Certificate Delivery**, in the **Email Address and Email Address (again)** boxes, type **hleitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number).
- Select the **I agree to the Terms of Service above** check box, and then click **Submit**.

Note: You may have to wait a few minutes for the email message with the compressed certificate file to arrive.

- In Internet Explorer, click the **New Tab** button.
- In the new tab, type **http://mail.Office365.com**, and press Enter.
- Sign in to Office 365 as **hleitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number) and a password of **Pa\$\$w0rd**.
- In the **Inbox**, locate the email message from **DigiCert** with the zip file attachment.

Note: It may take up to 15 minutes for the message with the certificate to arrive.

17. Click the **DigiCertSSL zip** file attachment.
18. In the Internet Explorer notification bar, click **Save**, then click **Save as**, then browse to **C:\temp**, and then click **Save**.
19. In Internet Explorer, click **Open folder**, then right-click **DigiCert_certs.zip**, and click **Extract All**.
20. In the **Extract Compressed (Zipped) Folders** dialog box, click **Extract**.

► Task 6: Install the Third-Party SSL Certificate

1. On **LUC-EX1**, switch to **Exchange Management Shell command prompt**.
2. To import a new certificate for the on-premises services, at the Exchange Management Shell command prompt type the following command, and press Enter.

```
Import-ExchangeCertificate -FileData ([Byte[]](Get-Content -Path C:\Temp\DigiCert_certs\certs\fs_labXXXXX_o365ready_com.cer -Encoding byte -ReadCount 0))
```

(where XXXXX is your unique o365ready.com number)

3. To export the a new certificate with the private key for the on-premises services, at the Exchange Management Shell command prompt type the following command, and press Enter.

```
$file = Get-ExchangeCertificate | Where-Object { $_.RootCAType -eq "ThirdParty" } | Export-ExchangeCertificate -BinaryEncoded:$true -Password (Get-Credential).password
```

(where XXXXX is your unique o365ready.com number)

4. In the **Username and Password** dialog box, type **Admin** for the **Username** and **Pa\$\$w0rd** for the **Password**, and then click **OK**.
5. To export the new certificate data to a file, at the Exchange Management Shell command prompt type the following command, and press Enter.

```
Set-Content -Path "C:\Temp\Labcert.pfx" -Value $file.FileData -Encoding Byte
```

► Task 7: Configure Exchange Server To Use the Lab Certificate for Mail Services

1. On **LUC-CL1**, on the Task Bar, right-click Internet Explorer and click **Start InPrivate Browsing**.
2. In the Address bar, enter **https://mail.labXXXXX.O365Ready.com/owa** (where XXXXX is your unique o365ready.com number) and press Enter.

Note the There is a problem with this website's security certificate message.

3. Click **Continue to this Web site**. Remain at the **Outlook Web App** logon screen and note the certificate error message in the Address bar.
4. Switch to **LUC-EX1**.
5. On **LUC-EX1**, switch to the **Exchange Management Shell command prompt**.
6. To assign the new certificate for the on-premises services, at the **Exchange Management Shell** command prompt, type the following command and press Enter.

```
Get-ExchangeCertificate | Where-Object { $_.RootCAType -eq "ThirdParty" } | Enable-ExchangeCertificate -Services POP,IMAP,SMTP,IIS
```

7. Press Enter again to confirm the operation in the Exchange Management Shell.

► Task 8: Verify the Lab Certificate is Correctly Installed

1. On **LUC-EX1**, in the Taskbar, click **Server Manager**.
2. In Server Manager, from the **Tools** menu, click **Services**.
3. Scroll down the list of services, then right-click **Microsoft Exchange IMAP 4** and click **Properties**.
4. In the **General** tab, next to startup type, click **Automatic**.
5. Click **Start**.
6. Click **OK** when the service has started.
7. Right-click the **Microsoft Exchange IMAP 4 Backend** service and click **Properties**.
8. In the **General** tab, next to startup type, click **Automatic**.
9. Click **Start**.
10. Click **OK** when the service has started.
11. Close the Microsoft Exchange IMAP 4 backend Properties dialog box.
12. Close the **Services** console.
13. Switch to **LUC-CL1**.
14. In the InPrivate browsing session of Internet Explorer, click the **Refresh** button.
15. Confirm that the certificate error warning message has now disappeared from the **Address** bar.
16. Log on as **LUCERNE\CEmond** with a password of **Pa\$\$w0rd**.
17. If prompted, under **Language**, select **English (United States)**, under **Time zone**, select **Coordinated Universal Time UTC**, and then click **Save**.
18. To the right of the Address bar, click the **padlock symbol**.
19. Confirm that the **Certificate name** is **fs.labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number) and the subject alternate names include **mail.labXXXXX.o365ready.com**.
20. Click **New mail**.
21. In the **To** box, enter **HLeitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number).
22. Add a **Subject** and some body text.
23. Click **SEND**.
24. In Internet Explorer, click the **New Tab** button.
25. In the new tab, type **https://outlook.office365.com/owa** and press Enter.
26. Log on as **HLeitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number) with a password of **Pa\$\$w0rd**.
27. In **Inbox**, click the message that has arrived and click **REPLY**.
28. Enter some text in the body of the message and click **SEND**.
29. Switch back to the tab for **Coralie Emond** and check that the reply message appears.
30. Close all tabs on Internet Explorer.

Note: If the message bounces, follow the instructions in the message for how to unblock the IP address of the Lucerne Publishing data center.

► **Task 9: Verify that Outlook Anywhere Works with On-Premises Exchange**

1. On **LUC-CL1**, on the Task Bar, click **Internet Explorer**, and navigate to **https://testconnectivity.microsoft.com**.
2. In the **Exchange Server** tab, click **Outlook Autodiscover**, and then click **Next**.
3. In the **Outlook Autodiscover** page, in **Email address** enter **hleitner@labXXXXX.o365ready.com** (where **XXXXX** is your unique **o365ready.com** number), in **Domain\User name**, enter **LUCERNE\HLeitner** and in the **Password** and **Confirm Password** boxes, enter **Pa\$\$w0rd**.
4. Check the **I understand that I must use the credentials of a working account** box.
5. Under **Verification**, enter the characters from the Captcha into the box and click **Verify**.
6. Click **Perform Test**.
7. On the **Connectivity Test Successful with Warnings** page, expand the test steps to note that the failure was due to not connecting to the **https://labXXXXX.o365ready.com/AutoDiscover/AutoDiscover.xml** endpoint. However, connection to **https://autodiscover.labXXXXX.o365ready.com/AutoDiscover/AutoDiscover.xml** succeeds.
8. Click **Start Over**.
9. In the **Exchange Server** tab, click **Outlook Connectivity**, and click **Next**.
10. In the **Outlook Connectivity** page, in **Email address**, enter **hleitner@labXXXXX.o365ready.com** (where **XXXXX** is your unique **o365ready.com** number), in **Domain\User name**, enter **LUCERNE\HLeitner** and in the **Password** and **Confirm Password** boxes, enter **Pa\$\$w0rd**.
11. Click **Manually specify server settings**.
12. In **RPC Proxy server**, enter **mail.labXXXXX.o365ready.com** (where **XXXXX** is your unique **o365ready.com** number).
13. In **Exchange server**, enter **LUC-EX1.LUCERNEPUBLISHING.LOCAL**.
14. The **Mutual authentication principal name** will autocomplete to **msstd: mail.labXXXXX.o365ready.com** (where **XXXXX** is your unique **o365ready.com** number).
15. Under **RPC proxy authentication method**, click **Ntlm**.
16. Check the **I understand that I must use the credentials of a working account** box.
17. Verification should still apply from the previous test. If not, repeat Step 5 in the previous set of steps.
18. Click **Perform Test**.
19. On the **Connectivity Test Successful with Warnings** page, expand **Test Steps** to identify the issue.
Note: The failure is due to the certificate common name not matching the mutual authentication string. However, a match was found in the subject alternative name extension.
20. Close Internet Explorer.
21. You have now configured on-premises Exchange Server for migration.

Results: Lucerne Publishing has ensured that Exchange Server is ready for a cutover migration.

Lab Discussion Questions

Why is DNS such a critical dependency in Office 365?

DNS is a critical dependency because this service is essential for clients to locate and connect to each of the Office 365 services.

Why is it important that domains are registered before subdomains?

Office 365 links subdomains to parent domains. This linkage cannot be carried out retrospectively, so you have to register contoso.com before you can register content.contoso.com. Because you have already proved that you own contoso.com, you can then register content.contoso.com and Office 365 knows that you control that subdomain as well.

- Why is DNS such a critical dependency in Office 365?
- Why is it important that domains are registered before subdomains?

Module Review and Takeaways

Having completed this module, you should now be able to:

- Recommend a mailbox migration strategy for moving to Exchange Online.
- Plan for implementing Exchange Online within your organization.



Best Practice: Best practices when planning Exchange Online and migration include:

- Ensure you have considered all the factors when selecting the migration path to Exchange Online.
- Analyze the risks to consider all possible “what-if” scenarios and identify mitigation plans to deal with each risk.
- Ensure you apply a structured change management methodology to the migration plan and adoption process.
- Keep your project sponsor, management team, administrators, and users informed about what is going on, particularly in the lead-up to any switchover.
- Make sure that everyone involved in the project has had sufficient training and is competent to carry out their tasks.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Timing of DNS updates	
MX records	

MCT USE ONLY. STUDENT USE PROHIBITED

Module 6

Planning Exchange Online and Configuring DNS Records

Contents:

Module Overview	6-1
Lesson 1: Plan for Exchange Online	6-2
Lesson 2: Configure DNS Records for Services	6-22
Lab: Configuring DNS Records and Migrating to Exchange Online	6-31
Module Review and Takeaways	6-44

Module Overview

In this module, you learn about the factors that cover DNS domain configuration for Office 365™, where you need to add the customer's existing domain or domains to Office 365. This module also covers the individual settings that you need to configure so that each Office 365 service works correctly and fully supports client access. These activities typically happen in the Deploy phase of the FastTrack process.

So far, you have been looking at Office 365 on its own. In this module, you examine the scenario in which you migrate services from your on-premises environment, starting with your email system. This module addresses the key issues of migrating email accounts to Exchange Online and the planning involved in that process. In the lab, you will practice that planning and then carry out a cutover migration from your on-premises environment to Exchange Online.

Objectives

After completing this module, you should be able to:

- Plan for implementing Exchange Online within your organization.
- Configure DNS records for Office 365 services.

Lesson 1

Plan for Exchange Online

In this lesson, you look at the more general factors covering planning for Exchange Online. These factors include client requirements, feature selection, eDiscovery, legal hold and archiving, and protocol support. This lesson also looks at factors such as Mail Exchanger DNS records, Exchange Online Protection (EOP) and mail delivery to non-ActiveSync mobile devices.

Lesson Objectives

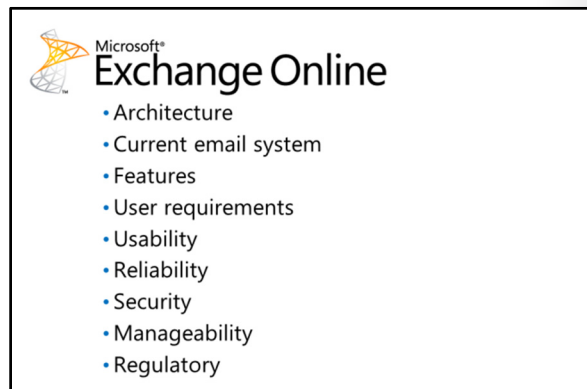
After completing this lesson, you should be able to:

- Identify organizational requirements for Exchange Online features.
- List common Exchange Online planning factors.
- Plan client requirements for Exchange Online.
- Plan for OWA and ActiveSync access, including setting policies.
- Provide OWA on mobile devices that do not use ActiveSync.
- Plan for eDiscovery, legal hold, archiving, and journaling.
- Plan for mail delivery in hybrid email setups.
- Plan for EOP in conjunction with Exchange Online.
- Outline how to run an Exchange Online administrative process.

Exchange Online Feature Requirements

It is now a truism of modern business that email is an essential service for organizations of all sizes. Not surprisingly, Exchange Online is the service that is most likely to interest potential adopters of Office 365.

Microsoft® Exchange Online is a hosted messaging solution that delivers the capabilities of Microsoft Exchange Server as a cloud-based service. It gives users single sign-on access to email, calendar, contacts, and tasks from PCs, the web, and mobile devices. In addition, it integrates fully with Windows Azure™ AD, enabling administrators to use group policies and other administration tools to manage Exchange Online features across their environment. It can also integrate with existing Exchange on-premises installations, either using simple co-existence or as a long-term hybrid deployment.



Feature discovery


Many organizations become interested in Office 365 for the simple fact that it enables the company to outsource its email to an Exchange-based service that offers significant functionality improvements over other cloud-based and on-premises email systems. When planning Exchange Online and determining whether it is the right choice for your organization, you should address the following factors and plan around the expected responses:

- *Architecture*. Email organizations, domains, trusts, multi-forest considerations.
- *Current email system*. Type, version, features, support, mail clients.
- *Features*. Email, calendar, contacts, tasks, public folders.
- *User requirements*. Access, device support, message handling, rule configuration.
- *Usability*. Integration with other services, authentication, ease of connection.
- *Reliability*. Uptime guarantees, mailbox and message protection.
- *Security*. Authentication, authorization, delegation, proxy addresses.
- *Manageability*. Administration, ease of access, policy enforcement, user and group management.
- *Regulatory*. Compliance and eDiscovery.

 **These planning tasks are covered in the Exchange Online Planning Guide, which can be found at the following link. Note that this link refers to material that was developed for the previous deployment methodology. However, the planning factors still apply:**

<http://go.microsoft.com/fwlink/?LinkId=321198>

Service description

 The service description for Exchange Online is available here:

<http://go.microsoft.com/fwlink/?LinkId=321199>

Latest features

The new features in the latest version of Exchange Online are shown here:

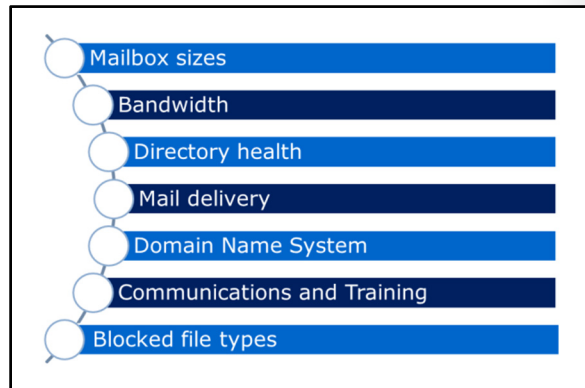
<http://go.microsoft.com/fwlink/?LinkId=271724>

Output

The output from this planning activity is confirmation as to whether Exchange Online can meet your organization's requirements, together with an appreciation of what the organization needs the service to provide.

Common Exchange Online Planning Factors

Regardless of the migration or coexistence option that you identified following your analysis of your organization's environment, there are several common factors that you should plan for. These include:



- *Mailbox sizes.* Create and implement a plan to reduce the size of users' mailboxes. Mailbox sizes are a major factor in determining the time it will take to migrate to Exchange Online. You should discuss options within your organization as to how to reduce mailbox sizes, including clearing out old emails, archiving messages to PST files, deleting sent files (particularly larger ones), and using rules. Review the organization's tools that will assist you in identifying which are the largest mailboxes (and do not be surprised to find that the CxOs are the major culprits).
- *Bandwidth.* Internet bandwidth is the second limiting factor that controls how long it takes to migrate to Exchange Online. In particular, it is the uplink speed that is important. Talk to the IT department about their link speed, its quality, and whether this is a good time to upgrade to a faster link or to a symmetric technology.
- *Directory health.* It is vital that you plan for a healthy directory service before starting the Deploy phase. This is also the time to remove duplicate accounts, old groups, unnecessary organizational units, retired servers, and old client computers, and generally perform housekeeping on the directory service. You should also check for errors in the log files and ensure that replication is functioning correctly.
- *Mail delivery.* If you are implementing coexistence, you must plan where incoming mail will be delivered. Delivery will initially be to the on-premises server, but you will need to determine if this is the best long-term arrangement in a coexistence scenario. You must also identify the point at which you will switch over in a cutover or staged migration.
- *Domain name services (DNS) settings.* You will need to plan for DNS configuration changes during the migration process, such as MX records, CNAMEs, and Autodiscover settings. Remember that DNS settings can take a while to propagate globally and that changing the Time to Live (TTL) setting can help speed up this process.
- *Communications.* It is essential that you communicate relevant and timely information about the migration plan to users. The pilot users can help assure people that the migration should go smoothly, but you must not overlook this factor in your planning.
- *Training.* If your organization's users are moving from one mail client to Outlook 2013 they will require a significant amount of training on this new client. If they are updating from an earlier version of Outlook this training requirement will be diminished, but you must still ensure that you have covered training as a consideration in your plan.
- *File types.* SharePoint Online blocks some file types. Ensure your users appreciate the implications of these blocked file types.



Refer to the following link for a list of blocked file types:

<http://go.microsoft.com/fwlink/?LinkId=321124>

Plan Client Requirements

Exchange Online provides industry-leading email capabilities, including inbox management, calendars, contacts, and to-do lists with the flexibility of the three-screen experience (personal computer, browser, and mobile device). You must provide users with the client software most appropriate for their needs.

The following table lists the supported client types, access protocols, and planning factors:

Consider the following general issues when planning client requirements:

- Versions
- Platform type
- Operating system or mobile operating system
- Client type
- Browser type
- User requirements
- User location
- Connection type
- Bandwidth
- Deployment
- Training
- Management

Client	Protocol	Planning factors
Outlook 2013	Outlook Anywhere (RPC over HTTP)	Richest client experience Client deployment mechanism Training
Outlook 2010 with Service Pack (SP) 1	Outlook Anywhere	Limitations on features compared to Outlook 2013
Outlook 2007 with SP3	Outlook Anywhere	Limitations on features compared to Outlook 2013 or 2010
Microsoft Outlook for Mac 2011	Outlook Anywhere	Limitations on features compared to Outlook 2013 or 2010
Outlook Web App	HTTP(S)	Limitations on features compared to Outlook Offline access may not be available, depending on the browser in use Available bandwidth Training requirements User expectations
Exchange ActiveSync (EAS)	EAS	Limitations on EAS devices
Legacy BlackBerry 7.1 and earlier devices (non-EAS)	Proprietary	Requires optional BlackBerry Enterprise Server (BES) service
Microsoft Entourage® 2008 for Mac, Web Services Edition	HTTP(S) – uses Exchange Web Services	
POP3/IMAP clients including Outlook 2003	POP3 IMAP4	Access to inbox folder only No support for calendar/to do/contact items
SMTP submission	SMTP	Send support only in conjunction with POP3/IMAP
Applications developed with Exchange Web Services	HTTP(S)	



For more information on the Office 365 client requirements, go to the following link:

<http://go.microsoft.com/fwlink/?LinkId=390891>

When planning client requirements, you must also consider the following general issues:

- *Versions:* Current client and version, any planned upgrades.
- *Platform type:* PC, browser, or mobile.
- *Operating system:* Windows 8, Windows 7, Windows Vista, Windows XP, or Mac OS X.
- *Mobile operating system:* Windows Phone, Windows Mobile, iPhone, BlackBerry, Nokia, Android, Palm.
- *Client type:* Rich client, web client, lightweight mail client, Windows 8 mail app.
- *Browser type:* Internet Explorer, Mozilla Firefox, Google Chrome or Safari.
- *User requirements:* Inbox only, full collaboration, lightweight access, mobile access.
- *User location:* Internal network, external or both.
- *Connection type:* Local area network, broadband, virtual private network, mobile broadband, or other connection types.
- *Bandwidth:* Gigabit, Megabit, Kilobit, or slower, latency, utilization levels.
- *Deployment:* Methods, management, restrictions, policies.
- *Training:* Approach, delivery modalities, technical levels, user groups, feedback, helpdesk.
- *Management:* Policies, settings, features enabled/disabled, settings.



For more information on Exchange Online clients, see the following link:

<http://go.microsoft.com/fwlink/?LinkId=390892>



For more information about how mobile devices work with Office 365, see the following link:

<http://go.microsoft.com/fwlink/?LinkId=400793>

Plan for Outlook Web Access

After Outlook Anywhere, Outlook Web Access (OWA) and Exchange ActiveSync (EAS) provide the most popular means for accessing Exchange Online. It is important, therefore, that you plan these features properly.

Outlook Web Access

OWA is now a central part of Office 365 and Exchange Online and integrates directly into each user's Office 365 portal. If the user has a subscription to the Lync Online service, then OWA also displays their Lync Online presence information.

- Do you want OWA enabled or disabled globally?
- Do you want to enable or disable it by user?
- Do you want to enable or disable OWA on mobile devices?
- How many different OWA policies do you need and with what settings?
- Which features do you want to enable or disable by default?
- What browsers will users have to access OWA?
- Do you want to enable or disable offline usage?

In many ways, OWA planning is relatively simple. OWA is always available to an Office 365 or Exchange Online user unless you switch it off. It will work with a range of browsers, including those on mobile platforms. OWA also offers offline reading and composing of email messages on certain browser types (Internet Explorer 10, Safari, and Google Chrome).



Note: Offline access for OWA is not a replacement for the full offline facilities of Microsoft Outlook 2013 when operating with an offline store (OST) file. It also is not available on mobile browsers.

Policy Control in OWA

Office 365 provides extensive controls of OWA through policies, accessed either through the Exchange Online console or Exchange Management Shell. Per-user control options include:

- Enable/disable OWA
- Select and apply defined OWA policies
- Enable/disable OWA on mobile devices
- Select and apply defined OWA for devices policies

Central policy controls you can apply through OWA policies include the ability to enable or disable the following settings:

- Instant, text, and Unified messaging
- Exchange ActiveSync
- Contacts
- LinkedIn contact sync
- Mobile device contact sync
- Journaling
- Themes
- Premium client
- Email signature
- Calendar
- Tasks
- Reminders and notifications
- Public or private computer attachment settings
 - Direct file access or WebReady document viewing
 - Force WebReady access if a viewer is available

In Exchange Management Shell, you can use the **Set-OWAMailboxPolicy** command to set policy options, including those not available through the Exchange Online admin console. For example, to enable or disable offline access over OWA, use the following command:

```
Set-OwaMailboxPolicy -AllowOfflineOn [NoComputers | AllComputers | PrivateComputers]
```

For more information, run **get-help Set-OWAMailboxPolicy** in Exchange Management Shell.

Planning Decisions

When planning for OWA, consider the following questions:

- Do you want OWA enabled or disabled globally?
- Do you want to enable or disable it by user?
- Do you want to enable or disable OWA on mobile devices?
- How many different OWA policies do you need and with what settings?
- Which features do you want to enable or disable by default?
- What browsers will users have to access OWA?
- Do you want to enable or disable offline usage?

Plan for Exchange ActiveSync

EAS is a protocol that enables mobile devices to synchronize email, calendar, contact, to-do items, and notes with an Exchange Server. EAS also provides limited policy control over the mobile device, such as the ability to set a password policy and to wipe the device remotely. EAS uses XML, typically over HTTPS, to communicate with the remote server, which can either be on-premises or Exchange Online.

As with OWA, most organizations will simply want to keep EAS enabled, with some additional configuration, depending on security and user requirements. Configuration options on a per-user basis include:

- Enable/disable ActiveSync on that mailbox.
- Change which ActiveSync policy applies to the mailbox.

Centrally-managed mobile device mailbox policies cover:

- Allow/block access/quarantine mobile devices
- Set quarantine email messages
- Set password requirement for mobile devices
 - Simple/complex
 - Alphanumeric
 - Require device encryption
 - Minimum password length
 - Number of failures before device wipe
 - Inactivity time
 - Enforce password lifetime
 - Password recycle count

- Do you want EAS enabled or disabled globally?
- Do you want to enable or disable it by user?
- How do you want to control security on mobile devices?
- How many different EAS policies do you need and with what settings?
- Which settings do you want to enable or disable by default?
- What policies will apply to users' personal devices?

Windows PowerShell® commands for ActiveSync policies include:

- Set-ActiveSyncDeviceAccessRule
- Set-ActiveSyncDeviceAutoBlockThreshold
- Set-ActiveSyncMailboxPolicy
- Set-ActiveSyncOrganizationSettings
- Set-ActiveSyncVirtualDirectory
- Get-ActiveSyncDevice



Note: The Exchange Management Console PowerShell cmdlets can manage many more settings than the Admin console, including allowing desktop synchronization, use of storage cards, use of the camera, Internet sharing, Bluetooth, and so on.

Planning decisions for EAS should address the following questions:

- Do you want EAS enabled or disabled globally?
- Do you want to enable or disable it by user?
- How do you want to control security on mobile devices?
- How many different EAS policies do you need and with what settings?
- Which settings do you want to enable or disable by default?
- What policies will apply to users' personal devices?

When planning for delivery of mail to non-ActiveSync mobile devices, you should consider the factors in the previous OWA topic. For example, the command **Get-ActiveSyncMailboxPolicy** would return information and configurable settings as follows:

```
RunspaceId                : 83fe6c03-bc63-43af-9f09-
c0cfc3d09c7e
AlphanumericDevicePasswordRequired : False
DevicePasswordEnabled      : False
AllowSimpleDevicePassword  : True
MinDevicePasswordLength    :
MaxInactivityTimeDeviceLock : Unlimited
MaxDevicePasswordFailedAttempts : Unlimited
DevicePasswordExpiration   : Unlimited
DevicePasswordHistory      : 0
MinDevicePasswordComplexCharacters : 1
AllowNonProvisionableDevices : True
AttachmentsEnabled        : True
DeviceEncryptionEnabled    : False
RequireStorageCardEncryption : False
```

PasswordRecoveryEnabled	: False
DevicePolicyRefreshInterval	: Unlimited
MaxAttachmentSize	: Unlimited
WSSAccessEnabled	: True
UNCAccessEnabled	: True
IsDefault	: True
AllowStorageCard	: True
AllowCamera	: True
RequireDeviceEncryption	: False
AllowUnsignedApplications	: True
AllowUnsignedInstallationPackages	: True
AllowWiFi	: True
AllowTextMessaging	: True
AllowPOPIMAPEmail	: True
AllowIrDA	: True
RequireManualSyncWhenRoaming	: False
AllowDesktopSync	: True
AllowHTMLEmail	: True
RequireSignedSMIMEMessages	: False
RequireEncryptedSMIMEMessages	: False
AllowSMIMESoftCerts	: True
AllowBrowser	: True
AllowConsumerEmail	: True
AllowRemoteDesktop	: True
AllowInternetSharing	: True
AllowBluetooth	: Allow
MaxCalendarAgeFilter	: All
MaxEmailAgeFilter	: All
RequireSignedSMIMEAlgorithm	: SHA1
RequireEncryptionSMIMEAlgorithm	: TripleDES
AllowSMIMEEncryptionAlgorithmNegotiation	: AllowAnyAlgorithmNegotiation
MaxEmailBodyTruncationSize	: Unlimited
MaxEmailHTMLBodyTruncationSize	: Unlimited
UnapprovedInROMApplicationList	: {}
ApprovedApplicationList	: {}

```

AllowExternalDeviceManagement      : False
MobileOTAUpdateMode                 : MinorVersionUpdates
AllowMobileOTAUpdate                 : True
IrmEnabled                           : True
AdminDisplayName                     :
ExchangeVersion                      : 0.1 (8.0.535.0)
Name                                  : Default
DistinguishedName                    : CN=Default,CN=Mobile Mailbox
Policies,CN=LUC-ORG,CN=Microsoft

Exchange,CN=Services,CN=Configuration,DC=lucerne,DC=local
Identity                              : Default
Guid                                  : cf0a4c9d-ab72-42f0-b1e3-
403155339b7a
ObjectCategory                       :
lucernepublishing.local/Configuration/Schema/ms-Exch-Mobile-Mailbox-Policy
ObjectClass                           : {top, msExchRecipientTemplate,
msExchMobileMailboxPolicy}
WhenChanged                           : 12/5/2013 6:29:58 PM
WhenCreated                           : 12/5/2013 6:29:58 PM
WhenChangedUTC                        : 12/5/2013 6:29:58 PM
WhenCreatedUTC                        : 12/5/2013 6:29:58 PM
OrganizationId                        :
OriginatingServer                     : LUC-DC1.lucernepublishing.local
IsValid                               : True
ObjectState                           : Unchanged
    
```

Plan for eDiscovery and In-Place Hold

When an organization has a reasonable expectation of litigation in the future, it may be required to preserve electronic communications, such as email and IMs that may be relevant to the case. As this can be a very broad requirement, organizations may need to implement information protection policies from the start.

Exchange Online provides a number of features that enable you to control how information is stored, managed, and transmitted within the organization. eDiscovery and in-place hold

- Are eDiscovery and in-place hold policies required?
- On which mailboxes?
- What information should be harvested?
- How many discovery mailboxes are required?
- Is legal hold supported in the subscription?
- How many days should items be held?
- Who will have rights to view eDiscovery items?

provide a mechanism to search mailboxes for specific words, such as “merger” and “Adatum”, and then specify what happens to the information gathered. Compliance officials and data security managers can then review this information in case of future litigation.

The key point here is that in-place hold preserves information even if users delete it, and that eDiscovery makes that information available to users with the correct role-based access control rights.



For more information on eDiscovery, see the following link:

<http://go.microsoft.com/fwlink/?LinkId=390893>



Note: You have to create a discovery mailbox by using the shell command **New-Mailbox** with the Discovery switch – you cannot create a discovery mailbox in EAC. To create a new discovery mailbox called SearchResults, run the following command:

New-Mailbox SearchResults -Discovery -UserPrincipalName SearchResults@contoso.com.



For more information on in-place hold, see the following link:

<http://go.microsoft.com/fwlink/?LinkId=390894>

You create and configure eDiscovery and legal hold policies through the Exchange Online Admin Center or by using the **New-Mailbox** PowerShell cmdlet. During the planning process, you must consider the following factors and configure the relevant policy settings:

- Are eDiscovery and Legal Hold policies required?
- Which mailboxes should a policy apply to (all or a subset)?
- What information should be harvested (all or a query-based subset)?
- How many Discovery mailboxes are required?
- Is legal hold available in the subscription (In-Place Hold is a premium feature that requires an Exchange Online Plan 2 or Exchange Online Archiving license for each user mailbox)?
- If legal hold is available, how many days to hold items after their received date?
- Who will have the Discovery Management admin role and therefore the administrative rights to view eDiscovery items in EAC?

Plan for Data Loss Prevention (DLP)

DLP is a mechanism for preventing data leaving the organization where that information is likely to contain confidential data, such as credit card numbers or national insurance numbers. In addition, you can create custom rules that cover custom information, such as employee numbers or other definable data. Exchange Online implements this protection by matching the format of blocks of numbers to that in the specified rule. An example of a rule might be US Financial, which applies the formats for 'Credit Card Number' or 'U.S. Bank Account Number' or 'ABA Routing

- What information must we protect?
- How can we best protect that information?
- How is the data formatted?
- What do we want users to be able to do if there is a policy match?
- What levels of auditing must we apply?
- Does the DLP policy need timings defined?

Number'. A message with a number such as 1234 5678 9012 3456 or 1234-5678-9012-3456 would then be picked up.

Depending on the rule settings, the message sender may have the option to override the rule and insist on delivery. If they do that, then the user may see warning messages and auditing options can then specify how the message is audited.

These rules can then be set to test mode, either with or without policy tips, or enforce mode. You can create policy tips with the following actions:

- Notify the sender
- Allow the sender to override
- Block the message
- Link to compliance URL


DLP custom rules enable you to specify multiple settings, such as if the sender is a specified person, the recipient is a member of a group, the subject or body contains particular terms, and so on. You can also configure audit settings and activate and deactivate the rule on specific dates.

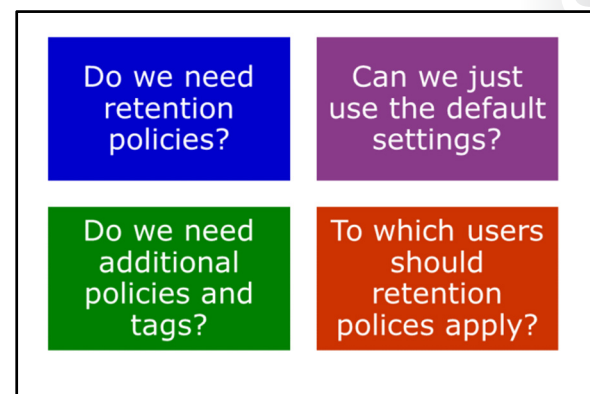
DLP planning factors include:

- What information must we protect?
- How can we best protect that information?
- How is the data formatted?
- What do we want users to be able to do if there is a policy match?
- What levels of auditing must we apply?
- Does the DLP policy need timings defined?

Plan for Retention

Information retention is performed through retention policies and retention tags. Retention policies are collections of retention tags. Retention policies are applied when the Managed Folder Assistant processes a mailbox.

 **Note:** Only Microsoft Outlook 2010 and later and Microsoft Office Outlook Web App users can apply personal tags and view the retention tags applied to their mailbox folders or items.



Retention tags consist of a number pre-defined rules and actions governing what should happen when an item is deleted. For example, the six-month delete tag will delete items in a particular folder after six months but allow recovery. You can define additional retention tags and configure settings, such as what happens to messages after what time – for example, delete or move to archive.

You then assemble bunches of retention tags into a retention policy and apply that retention policy. The users don't actually see the name of the policy – all they see are the individual tag settings which can then

apply to folders in their mailbox. Note that users can create and apply their own personal retention policies (requires an Exchange Enterprise client access license for on-premises users in a hybrid environment).



For more information on retention tags and policies, see the following link:

<http://go.microsoft.com/fwlink/?LinkId=390895>

Planning for retention involves considering the following factors:

- What requirement do we have for retention within the organization?
- Are further retention tags required or do the defined ones meet the organization's needs?
- Are further retention policies required in addition to the default one and what tags should be in that policy?
- Which users require specific retention policies applied to their mailboxes?

Plan for Journaling

Journaling is the process of using journal rules to record all communications in support of your organization's email retention or archival strategy. This process enables organizations to meet compliance requirements while going about their ordinary business, such as complying with the Sarbanes-Oxley Act of 2002 or the Gramm-Leach-Bliley Act (Financial Modernization Act).

Setting up journaling involves defining journal rules that consist of a journal rule scope, a journal recipient, and a journal mailbox. Scope involves specifying whether the journal rule applies to all messages to a specified user or group and whether all messages – or just internal or external ones – will be recorded.

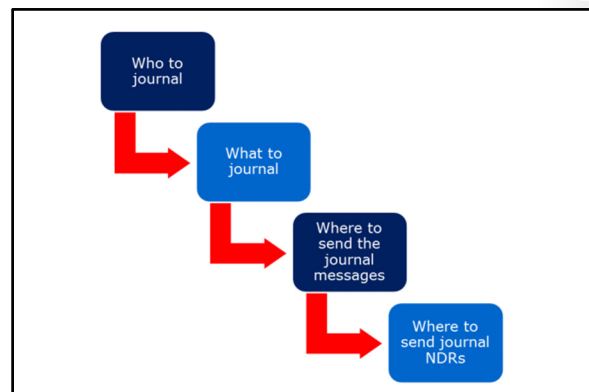
Planning factors to consider with journaling include:

- Who to journal (all users, as specific user or a group).
- What to journal (all messages, all internal ones or all external ones).
- Where to send the journal messages (for example, to an internal mailbox or an external SMTP address).
- Where to send non-deliverable journal reports (ideally this should be a dedicated mailbox, as journal rules do not apply to the journal report NDR mailbox).



More information on journaling is available from this link:

<http://go.microsoft.com/fwlink/?LinkId=390896>



Plan for Archiving

Microsoft Exchange Online Archiving is an Office 365 cloud-based, enterprise-class archiving solution for organizations that have deployed specific Office 365 plans. Exchange Online Archiving assists with archiving, compliance, regulatory, and eDiscovery challenges while simplifying on-premises infrastructure, reducing costs, and easing IT burdens.

Online or personal archives is a service in Office 365 that provides an additional user mailbox for storing older messages, such as calendar items from two or more years ago or sent items that are no longer of immediate importance. The online archive mailbox looks just like an ordinary mailbox and you can create folders in it, search it, and carry out the same administrative tasks as with a regular mailbox. The chief difference between the online archive and the main mailbox is that the online archive can be much larger – useful for CEOs who do not like deleting anything – and the fact that it is not available offline, so does not create a corresponding offline store (.OST) file on the local computer.

Online archiving only applies to certain plan levels in Office 365. The following plans have the service integrated:

- Office 365 Enterprise E3 and E4
- Office 365 Education A3 and A4
- Office 365 Government G3 and G4
- Exchange Online Plan 2

It is also available as an add-on with the following plans:

- Exchange Online Plan 1 and Online Kiosk
- Office 365 Midsize Business
- Office 365 Enterprise E1 and K1
- Office 365 Government G1 and K1
- Office 365 Education A2



Note: Online archives can be of unlimited size but, in fact, have an initial fair use quota of 100 GB. This limit can be raised by calling support.

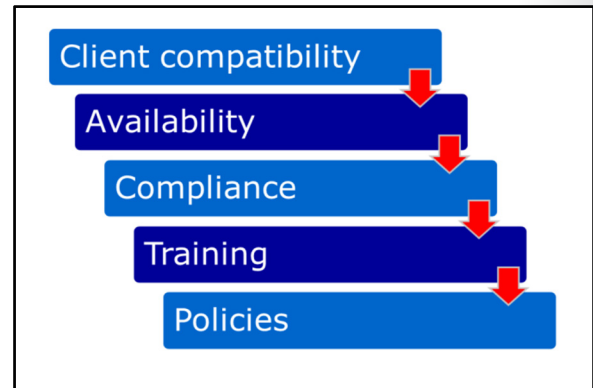


For more information on Exchange Online Archiving, go to the following link:

<http://go.microsoft.com/fwlink/?LinkId=390897>

Archiving is not a difficult concept to get over to users, as the archive mailbox simply appears as another mailbox in their profile. However, there are limitations in its use, so you need to consider the following planning factors when implementing this service:

- Client compatibility – the archive mailbox is only accessible through Outlook and OWA.
- Availability – the archive is for online usage only and is not available offline.



- Compliance – how will archiving integrate with journaling and eDiscovery?
- Training – although not difficult to learn, users need to know how to use the archive mailbox, along with retention policies.
- Policies – identify and apply archive policies so that users can select how items are moved to their archive mailbox.

It is important to remember (and to get over to your users) that archive is NOT backup. It is also not a PST (personal store) file. PSTs are client-based messaging database files that are typically only available on a local computer, whereas archive folders are server-based and do not exist on the local computer.

Plan for Mail Delivery with Hybrid Exchange

Mail delivery with hybrid Exchange is a particular area that requires additional explanation. A feature of hybrid deployments is that there are typically some mailboxes in the on-premises server and others in Exchange Online. However, to the outside world, these mailboxes all appear to be part of one big organization.

Hybrid transport is the service that ensures that messages are correctly routed to the correct environment for each mailbox and that this message delivery is performed in a secure manner using Transport Layer Security (TLS). In addition, this message delivery is treated as being internal to the organization. Anti-spam policies, journaling, and transport rules all use settings that apply to internal messages rather than ones for messages coming in from outside the organization.

Configuring a hybrid organization with the Hybrid Configuration Wizard in Exchange 2013 automatically sets up this TLS transport. The on-premises SMTP endpoint needs to be running on an Exchange 2013 Client Access server or an Exchange 2010 SP3 Edge Transport server. Microsoft EOP then connects to that endpoint.



Note: You cannot have any other form of host, service, or appliance between EOP and the Exchange 2013 or Exchange 2010 SP3 server. Hybrid operation requires specific additional information to be added to messages transiting between the online and on-premises environments, and any other type of intermediary device will remove this information.

Decisions that you need to take when planning hybrid routing include:

- *Incoming mail routing.* Does your organization want to route incoming mail in through Office 365 and EOP or in through their on-premises infrastructure?
 - *On-premises.* In this case, the DNS MX record for the organization remains pointing to the on-premises servers. This option is useful if the customer has strict compliance requirements and must apply journaling to all incoming messages. It is also preferable if the customer has more mailboxes on-premises than online.
 - *Exchange Online.* Here, the messaging administrator changes their DNS MX record for their email domain to point to Exchange Online, and message delivery is to the cloud. This option is

- Incoming routing
 - Through on-premises – no change to DNS MX records and on-premises forwards messages to online mailboxes
 - Through EOP – process depends on whether centralized message handling is enabled
- Outgoing routing
 - Direct to recipient – when centralized message handling is disabled
 - Through on-premises – when centralized message handling is enabled

preferable if your organization has more mailboxes in Exchange Online than in the on-premises environment. However, there is a difference in how this routing is performed, depending on whether centralized mail transport is enabled.

- *Centralized mail transport not enabled (default).* If centralized mail transport is not enabled, incoming messages arrive through EOP and Exchange Online performs the process of copying and routing the messages to cloud-based or on-premises mailboxes.
- *Centralized mail transport enabled.* If centralized mail transport is enabled, EOP routes the incoming mail to the on-premises Exchange 2013 Client Access server, which is then responsible for routing copies of the message, either to Exchange Online or to on-premises mailboxes.
- *Outgoing mail routing.* Does your organization want to route outgoing mail direct to the Internet or through the on-premises environment? Here, the different routes are selected, depending on whether centralized mail transport is enabled.
 - *Direct to recipient.* If centralized mail transport is not enabled, outgoing mail from Exchange Online is sent direct to the recipient's domain using DNS settings. Outgoing mail from the on-premises environment is unaffected.
 - *Through on-premises.* If centralized mail transport is enabled, all outgoing messages from Exchange Online mailboxes are sent to the on-premises environment, and then sent to their destination domains from there. Therefore, organizations with strict compliance requirements can ensure that all outgoing messages go through the corporate gateway and any archiving or journaling of those messages can take place.
- *Edge Transport servers.* Your organization has the option to deploy Exchange Server 2010 SP3 Edge Transport servers, which means that the domain-joined Exchange Server computers are not exposed directly to the Internet.

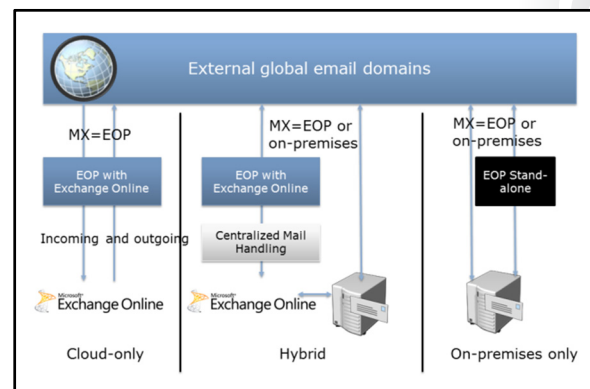
The routing for incoming and outgoing mail has no effect on communications between the on-premises Exchange organization and Exchange Online, which are still made over an encrypted channel.

Plan for Exchange Online Protection

EOP is a low-cost, enterprise class, cloud-based, anti-spam, and anti-malware message sanitizing system. It provides a layer of protection for organizations of all sizes and helps prevent attacks from a range of sources. It is also easy to configure and integrate into your customer's existing environment. EOP is the replacement for Forefront Online Protection for Exchange (FOPE).

EOP provides message sanitation for incoming and, if necessary, outgoing mail. The configuration of this protection differs according to the configuration of messaging within an organization's environment. When planning EOP, you need to configure the environment for one of the following three options:

- Cloud-only
- On-premises only



- Hybrid

If your organization is moving to a cloud-only environment, either as a cutover, IMAP, PST or staged migration, you will be implementing EOP as part of Exchange Online; in this case, you only need to plan for message handling policies in EOP. All the features in EOP with Exchange Online will be available.

If your organization is planning to keep their current on-premises mail setup and use Exchange Online with Office 365, they can optionally route incoming messages through the stand-alone EOP service before delivery to their on-premises mail system. They can also send outgoing messages through this route if required. If using this option, the following services in EOP will not be available:

- Reporting using web services
- Delivery reports
- Data Loss Prevention (DLP)
- DLP Policy Tips
- Remote Windows PowerShell Access

However, users will be able to self-manage spam-quarantined messages, which is not available in EOP with Exchange Online.

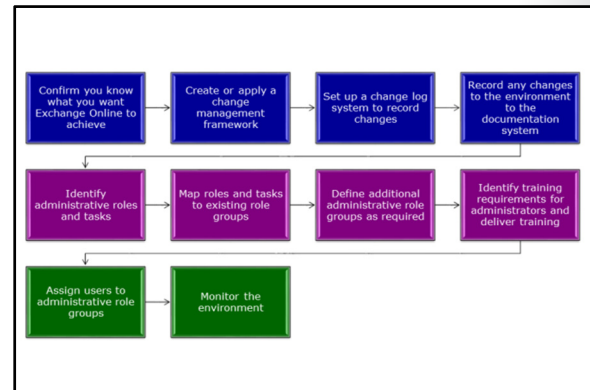
If your organization is planning to implement a hybrid Exchange server environment, they will have users in the on-premises environment and in Exchange Online; therefore, you have more options for integrating EOP. These options are as shown in the following table.

Message Direction	Delivery route	Centralized Message Delivery Off (Default)	Centralized Message Delivery On	Changes to environment
Incoming	On-premises	Direct delivery to on-premises mailboxes and then mail routed through EOP for cloud-based recipients	No change	No change to external MX DNS record. Centralized messaging setting has no effect
Incoming	Office 365	EOP accepts messages, Exchange Online copies and routes on-premises mail back through EOP to the on-premises server	EOP accepts messages then routes to on-premises server, which then copies and routes back through EOP to the cloud-based mailboxes	MX points to EOP. Configure centralized messaging for desired routing
Outgoing	Direct to Internet	Mail from cloud-based mailboxes goes through EOP and direct to recipients. Mail from on-premises users goes direct to recipients	N/A	Do not enable centralized messaging in Hybrid configuration Wizard
Outgoing	Through on-premises servers	N/A	Mail from online users goes through EOP to on-premises server and then out to recipient domains	Enable centralized messaging in Hybrid configuration wizard

Plan for Exchange Online Administration

Planning for Exchange Online administration is an important part of the overall planning process. Only by identifying how you want to administer Exchange Online can you expect to deliver the efficiencies that Exchange Online can potentially deliver. Conversely, if your Exchange Online administration processes are not well defined, you are in danger of failing to meet your requirements for security, feature take-up, and data protection.

To ensure that your Exchange Online administration is working as it should be, you are recommended to apply the following process:



1. Confirm you know what you want Exchange Online to achieve.
2. Create or apply a change management framework.
3. Set up a change log system to record changes.
4. Record any changes to the environment to the documentation system.
5. Identify administrative roles and tasks.
6. Map roles and tasks to existing role groups.
7. Define additional administrative role groups as required.
8. Identify training requirements for administrators and deliver training.
9. Assign users to administrative role groups.
10. Monitor the environment.

Confirm you know what you want Exchange Online to achieve

Before you start administering Exchange Online (or bring in others to do that with you) you must know what you want the new environment to achieve. For example, it may be to reduce administrative costs, in which case you don't want to create an administrative setup that is as complex as your current on-premises one.

Create or apply a change management framework

Regardless of whether you have a change management framework such as Microsoft Operations Framework (MOF) in place, you should implement one with Exchange Online. You need to have a process for identifying, testing, approving, and making changes to the Office 365 configuration.

Set up a change Log system to record changes

It is essential that you have good documentation of your Office 365 settings and that this is maintained and kept up to date. This is probably the most frustrating aspect of systems management, as other administrators (and, if we're frank, ourselves) are very bad at recording information of this type. However, that is no excuse for not setting up a documentation system and specifying that recording configuration changes is an essential part of the change management process.

Identify administrative roles and tasks

You now need to identify what roles and tasks our administrators are required to carry out. For example, you may have people in your organization who have unusual job responsibilities, so require unique combinations of access rights to Office 365.

Map roles and tasks to existing role groups

When you have finished defining the administrative requirements, you now take those roles and map them to the existing role groups. Office 365 provides the following role groups:

- Compliance Management
- Discovery Management
- Help Desk
- Help Desk Administrators (HelpdeskAdmins_ <unique value>)
- Hygiene Management
- Organization Management
- Recipient Management
- Records Management
- Tenant Admins (TenantAdmins <unique value>)
- UM Management
- View-Only Organization Management

There are also the admin roles as defined in Office 365, such as Billing Admin, Global Admin, and so on. In Exchange Online, these administrator types have the following mapping and equivalent rights:

Office 365 Administrator type	Exchange Online equivalent rights
Global Administrator	Organization Management
Password Administrator	Help Desk Administrator

Define additional administrative roles as required

If there are still accounts that can't be mapped to the existing roles, you need to create new ones, combining the role-based access control (RBAC) permissions so that each account has the rights it needs.

Identify training requirements for administrators and deliver training

Now that you know who will be doing what, this is a good time for you to ensure that the people assigned to specific roles have the skills and training they need to carry out those tasks. Look at online training resources and official Microsoft Curriculum training courses that may meet their needs.

Assign users to administrative roles

With your full listing of administrator roles and administrative personnel defined and those users now having the knowledge and skills they need to do their tasks (including documenting their actions), you can now map those people to their respective roles and let them get on with their jobs.

Monitor the environment

You should still ensure that you monitor the Exchange Online environment to check that your team is doing the jobs properly, including recording changes. Remember that one of the best sources of real-time

monitoring will be your users. If you have an Exchange Online service outage, check with the Office 365 console first to eliminate the service itself as a source of failure.

Module 12 in this course covers the components of an effective monitoring environment.

Lesson 2

Configure DNS Records for Services

As you have seen in the first lesson, DNS is an essential service for Office 365 and registering custom domains is an important activity within the Deploy Phase of the FastTrack process. In this next lesson, you move on to specifying the different DNS settings for each Office 365 service and identifying the functions that these settings provide.

Lesson Objectives

After completing this lesson, you should be able to:

- Explain the function of DNS for each Office 365 service.
- Identify the different DNS record types used with Office 365.
- List the differences between cloud-based and hybrid DNS records.
- Describe the consequences of adding or changing records.
- Explain which domain will host the service with multiple domains.
- Explain why you do not always need to update all DNS records.

DNS and Office 365 Services

You have already looked at the process of registering custom domains and the DNS record types that Office 365 uses. You now move on to look at the functionality that DNS provides in more detail.

Office 365 uses DNS at the following levels:

- The Office 365 service level.
- For Exchange Online in both cloud-only and hybrid modes.
- For SharePoint Online in both cloud-only and hybrid modes.
- For Lync Online in both cloud-only and hybrid modes.
- For single sign-on authentication.

Office 365 Service Level

At the service level, Office 365 uses a CNAME record to direct client authentication requests to the right location. This redirection speeds up authentication, otherwise clients will only authenticate to Office 365 in the USA. Office 365 also uses TXT or MX records to verify domain ownership. These records have no other function.

Exchange Online

The Exchange Online service uses three records for cloud-only operation and three for hybrid operation. With cloud-only operation, you require the following records:

Service	Record	Function
Office 365	CNAME	Directs authentication to the right identity platform; speeds up authentication, otherwise clients will authenticate to Office 365 in the USA
Domain verification	TXT	Verifies domain ownership; no other function
Exchange Online	CNAME	Enables autodiscover for Outlook clients
	MX	Routes incoming mail to Exchange online
	SPF (TXT)	Sender Policy Framework anti-spam
Exchange Federation	TXT	Enables Exchange federation in hybrid environments
	CNAME	Provides autodiscover for easy client connection with Exchange federation
SharePoint Lync	CNAME	Redirects to public web site for domain
	SRV	Enables SIP federation
SSO	SRV	Coordinates information flow between clients
	CNAME	Redirects Lync online client sign-in
	Host (A)	Redirects Lync online mobile client sign-in
SSO	Host (A)	Publishes SSO ADFS server address

- The autodiscover CNAME record enables autodiscover for Outlook clients. Users can then simply enter their email address into Outlook to set up Outlook Anywhere access, based on that user's domain suffix.
- With a cloud-only configuration, the MX record routes incoming mail to Exchange Online through the Exchange Online Protection service. This service is available as a stand-alone offering, in which case the MX records will point to the cloud service.
- The SPF (TXT) record provides the Sender Policy Framework anti-spam protection. SPF records ensure that destination email servers trust the messages sent from your domain in Office 365. The SPF record makes all messages from your domain appear to originate from the Office 365 messaging servers.

 **See the following link for more information on Sender IDs and how they use SPF records to combat spoofing:**

<http://go.microsoft.com/fwlink/?LinkId=524347>

With hybrid operation where the organization has some users on Exchange Online and some on Exchange Server on-premises, the following settings apply:

- Two TXT records are required to enable Exchange federation in hybrid environments. One record is for the domain name and one is for exchangedelegation.domainname. Both these text records include a hash text that is unique to the domain.
- An MX record is required to deliver mail for the federated domain. This value may be set to point to Exchange Online or it can be set to point to the on-premises server. The choice will depend on the design decisions and factors, such as whether there are more users on-premises or in the cloud.
- As with the cloud-only environment, a CNAME autodiscover record provides easy client connection with Exchange federation. Again, this CNAME record may point to the on-premises Outlook Anywhere endpoint or to Exchange Online.

SharePoint Online

SharePoint online only requires one DNS entry for the public website. You need to configure a CNAME entry that points the host name for our domain to the subdomain on the SharePoint.com domain.

Lync Online

With Lync Online, DNS records are slightly more complex, consisting of two SRV and two CNAME records.

The first of these SRV records enables SIP federation so that your SIP domain can federate to external domains and to public instant message environments, such as Skype. The second is for coordinating information flow between clients. There are then two CNAME aliases, one for redirecting the Lync online client sign-in, the other for redirecting Lync online mobile client sign-in.

Single Sign-On

If you are implementing single sign-on in conjunction with Office 365, you need an A record to publish the SSO AD FS server address. Note that, in external DNS, this A record will typically point to the external address of the network load balancer for the AD FS Proxy Server array. On the internal DNS, it will point to the AD FS server farm.

DNS Office 365 Service Examples

Moving on from the previous topic, this table shows examples of the records for each DNS entry for the Office 365 services.

Service	Record	Example Values
Office 365	CNAME	Alias: msoid, Target: clientconfig.microsoftonline-p.net
Domain verification	TXT	Host: @ (or, for some DNS hosting providers, your domain name) Value: Text string that the Add a domain Wizard generates.
Exchange Online	CNAME	Alias: Autodiscover Target: autodiscover.outlook.com
	MX	Domain: contoso.com, Target email server: <MX token>.mail.protection.outlook.com, Preference: 10
	SPF (TXT)	TXT Name @ Values: v=spf1 include:spf.protection.outlook.com -all
Exchange Federation	TXT	TXT record 1: contoso.com plus hash text TXT record 2: exchangedelegation.contoso.com hash text
	MX	Domain: service.contoso.com, Target email server: <MX token>.mail.eo.outlook.com, Preference: 10
	CNAME	Alias: Autodiscover.service.contoso.com Target: autodiscover.outlook.com
SharePoint	CNAME	Hostname: www.contoso.com Points to address: contoso.sharepoint.com TTL: 1 hour
Lync	SRV	Service: _sipfederationtls, Protocol: TCP, Priority: 100, Weight: 1, Port: 5061, Target: Sipfed.online.lync.com
	SRV	Service: sip, Protocol: TLS, Priority: 100, Weight: 1, Port: 443 Target: sipdir.online.lync.com
	CNAME	Alias: sip, Target: sipdir.online.lync.com
SSO	Host (A)	Target: sts.contoso.com

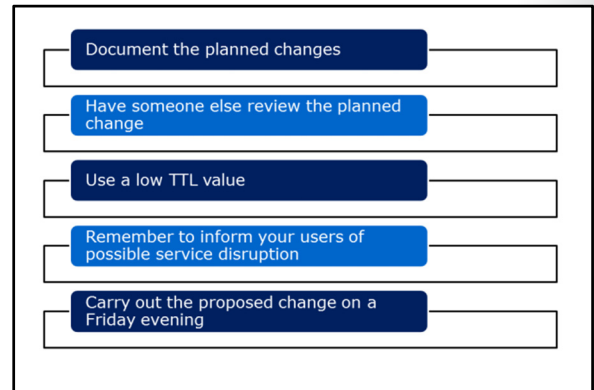
Service	Record	Example Values
Office 365	CNAME	Alias: msoid Target: clientconfig.microsoftonline-p.net
Domain verification	TXT	Host: @ (or, for some DNS hosting providers, your domain name) Value: A text string that the Office 365 Add a domain Wizard generates
Exchange Online	CNAME	Alias: Autodiscover Target: autodiscover.outlook.com
	MX	Domain: contoso.com Target email server: <MX token>.mail.protection.outlook.com Preference: 10
	SPF (TXT)	TXT Name @ Values: v=spf1 include:spf.protection.outlook.com -all Existing Forefront Online Protection for Exchange customers must also add the following record: include: spf.messaging.microsoft.com Note: If the firewall or proxy server blocks TXT lookups on an external DNS, add this record to the internal DNS record
Exchange Federation	TXT	TXT record 1: contoso.com plus hash text (for example, Y96nu89138789315669824) TXT record 2: exchangedelegation.contoso.com hash text (for example, Y3259071352452626169)
	MX	Domain: service.contoso.com Target email server: <MX token>.mail.eo.outlook.com Preference: 10
	CNAME	Alias: Autodiscover.service.contoso.com Target: autodiscover.outlook.com
SharePoint	CNAME	Hostname: www.contoso.com Points to address: contoso.sharepoint.com TTL: 1 hour

Service	Record	Example Values
Lync	SRV	<i>Service:</i> _sipfederationtls <i>Protocol:</i> _TCP <i>Priority:</i> 100 <i>Weight:</i> 1 <i>Port:</i> 5061 <i>Target:</i> Sipfed.online.lync.com <i>Note:</i> If the firewall or proxy server blocks SRV lookups on an external DNS, add this record to the internal DNS record
	SRV	<i>Service:</i> _sip <i>Protocol:</i> _TLS <i>Priority:</i> 100 <i>Weight:</i> 1 <i>Port:</i> 443 <i>Target:</i> sipdir.online.lync.com
	CNAME	<i>Alias:</i> sip <i>Target:</i> sipdir.online.lync.com
	CNAME	<i>Alias:</i> lyncdiscover <i>Target:</i> webdir.online.lync.com
SSO	Host (A)	<i>Target:</i> sts.contoso.com

DNS Record Changes

Before you change the DNS records for services in Office 365, you must be aware of the effects. The two main changes you are likely to make are as follows:

- MX record:** If you are migrating from on-premises email to Exchange Online and want to change the delivery point for incoming mail from the current Simple Mail Transfer Protocol (SMTP) endpoint on your firewall to EOP. The MX record change is the final stage of a cutover or staged migration.
- www.domainname.com record.** If you are moving your public website onto SharePoint, you will change the existing A or CNAME record to point to domain.sharepoint.com.



You should plan changes to DNS settings carefully as incorrect settings can result in service failure. You must also be aware that changes to DNS settings can take some time to propagate around the global network, so it can take time for the reconfiguration to take effect. If you subsequently find that the setting is incorrect, it can take up 72 hours to fix it, so a DNS record setting error could potentially make the service unavailable for your domain for nearly a week.

When changing DNS records for Office 365, you should carry out the following recommendations:

- Make sure you document the planned changes.
- Have someone else review the planned change before you put it into action.
- Use a low TTL value, such as 60 minutes, which should help reduce the time that the planned change takes to propagate through DNS.
- Remember to inform your users of a possible service disruption.
- Carry out the proposed change on a Friday evening so that the DNS replication can occur over the weekend.



The Remote Connectivity Analyzer Tool is the best utility to employ for testing your domain settings for each service.

<http://go.microsoft.com/fwlink/?LinkId=390899>

Additional tools for testing DNS settings include running NSLOOKUP from a command prompt to check for individual name entries in DNS. The syntax is NSLOOKUP hostname.domainname.com.

Hosting Multiple Domains

As pointed out in the previous lesson, you can host multiple domains on Office 365 with up to 600 domains in each account, including subdomains. With Office 365, you have the flexibility to configure the services to be hosted on different domains.

Option	Process
Single Default Domain	Use the domain you get when you sign up for the service
Single custom domain	Add a single external domain that you add after signup or as part of the Deploy Phase of the FastTrack process
Single custom root domain with subdomains	Add the root domain then the subdomains
Multiple custom domains, no subdomains	Add the root domains independently
Multiple root domains with multiple subdomains	Add the root domain then the subdomains from that root. Add other root domains independently followed by their subdomains

Option	Process	Domain format	DNS registered and managed by	Services accessed as:
Single Default Domain	Use the domain you get when you sign up for the service	contoso.onmicrosoft.com	Office 365	Exchange Online: user@contoso.onmicrosoft.com SharePoint: contoso-public.sharepoint.com Lync: user@contoso.onmicrosoft.com
Single custom domain	Add a single external domain after signup or as part of the	contoso.com	Small Business plans – Office 365 or external	Exchange Online: user@contoso.com SharePoint: www.contoso.com (public site)

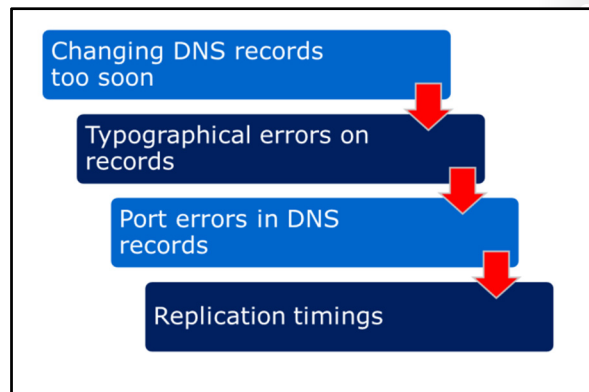
Option	Process	Domain format	DNS registered and managed by	Services accessed as:
	FastTrack Deploy Phase		DNS hoster Medium Business and Enterprise plans – External DNS hoster	Lync: user@contoso.com
Single custom root domain with subdomains	Add the root domain then the subdomains	contoso.com mail.contoso.com content. contoso.com	Small Business plans – subdomains not available Medium Business and Enterprise plans – External DNS hoster	Exchange Online: user1@contoso.com user2@mail.contoso.com user3@content.contoso.com SharePoint: www.contoso.com www.content.contoso.com Lync: user@contoso.com
Multiple custom domains, no subdomains	Add the root domains independently	contoso.com adatum.com fourthcoffee.com	Small Business plans – Office 365 or external DNS hoster Medium Business and Enterprise plans – External DNS hoster	Exchange Online: user1@contoso.com user1@fourthcoffee.com user2@fourthcoffee.com user3@adatum.com SharePoint: www.contoso.com www.fourthcoffee.com www.adatum.com Lync: user1@contoso.com user2@adatum.com user3@fourthcoffee.com
Multiple root domains with multiple subdomains	Add the root domain then the subdomains from that root. Add other root domains independently followed by their subdomains followed by	contoso.com mail.contoso.com content. contoso.com adatum.com data.adatum.com fourthcoffee.com cappuccino. fourthcoffee.com		Exchange Online: user1@mail.contoso.com user1@fourthcoffee.com user2@fourthcoffee.com user3@data.adatum.com SharePoint: www.contoso.com www.content.contoso.com www.fourthcoffee.com www.adatum.com

MCT USE ONLY. STUDENT USE PROHIBITED

Option	Process	Domain format	DNS registered and managed by	Services accessed as:
	their subdomains			www.data.adatum.com Lync: user1@contoso.com user2@adatum.com user3@fourthcoffee.com

Troubleshoot DNS Records

Because of the cloud-based nature of Office 365 and the way in which it interacts with on-premises systems, whenever you are troubleshooting service provision on Office 365 with custom domains, you should investigate DNS records as a priority. Typical errors and prevention or troubleshooting errors are as follows:



Issue	Symptoms	Detection	Correction
Changing DNS records too soon	Service fails Mail not delivered and could be lost irretrievably	Users will complain	Change DNS record back to original value Document all changes before making them
Typographical errors on records	Service fails Mail not delivered and could be lost irretrievably Users cannot log on	NSLOOKUP Remote Connectivity Analyzer Best Practices Analyzer Tool Microsoft Connectivity Analyzer Office 365 DNS Diagnostic Tool MOSDAL Support Toolkit	Check records for errors Get other people to check the records (easy to see what you think you see) Correct records Wait for propagation to occur Recheck service
Port errors in DNS records	Users cannot log on Lync Online service inoperable Note that this can be a	Users cannot connect NSLOOKUP Remote Connectivity Analyzer Best Practices Analyzer Tool Microsoft Connectivity Analyzer	Check records for errors Get other people to check the records Correct records Wait for propagation to occur Recheck service

Issue	Symptoms	Detection	Correction
	difficult issue to detect	Office 365 DNS Diagnostic Tool MOSDAL Support Toolkit	
Replication timings	Service does not transition to Office 365 in a timely fashion	NSLOOKUP and WHOIS still showing records for domain having old settings	Wait for replication to occur Check that the records are actually correct

Other factors that can cause issues with DNS and should be addressed by training are:

- Having a poor understanding of how DNS works.
- Not having a good project plan.
- Failing to identify what your start and end goals are.
- Not understanding the sequence of cutting over to cloud environment.
- Lack of consideration for transition period.

The following XML is an example of the output from the MOSDAL Support Toolkit testing the Lync Online part of the DNS setup. Note the port, IP address and DNS values for the service:

```

<application name="Lync Online">
  <dnsTest name="[SRV]:
_sip._tls.LucernePublishingXXXX.onmicrosoft.com">
    <dnsLookup type="internal">
      <server>server2012.contoso.local</server>
      <address>192.168.20.10</address>
      <result>Non-authoritative answer:</result>
      <result>SRV service location:</result>
      <resultData>
        <pair name="priority" value="100" />
        <pair name="weight" value="1" />
        <pair name="port" value="443" />
        <pair name="svr hostname"
value="sipdir.online.lync.com" />
        <pair name="sipdir.online.lync.com      internet
address" value="132.245.209.21" />
        <pair name="sipdir.online.lync.com      AAAA IPv6
address" value="2a01:111:f404:9401::35" />
      </resultData>
    </dnsLookup>
    <dnsLookup type="external">
      <server>resolver1.opendns.com</server>
      <address>208.67.222.222</address>
      <result>Non-authoritative answer:</result>
      <result>SRV service location:</result>
      <resultData>
        <pair name="priority" value="100" />
        <pair name="weight" value="1" />
        <pair name="port" value="443" />
        <pair name="svr hostname"
value="sipdir.online.lync.com" />
      </resultData>
    </dnsLookup>
  </dnsTest>

```

</application>

Recommendations for Configuring DNS Records

When configuring DNS settings for Office 365 services, you should apply the following guidelines and best practices:

- *Plan every change in detail.* It is vital that, before you go anywhere near the DNS console, you have a clear and detailed design and a project plan for what you intend to do.
- *Take extra care with MX records.* The above requirement is doubly true if you are planning to change MX records. Errors can take some time to fix, during which time your company's email service will be unavailable.
- *Work with a reliable cloud partner.* Working with a competent cloud services partner should help to reduce issues caused by DNS configuration errors.
- *Communicate with users.* Ensure that you notify users about transition or DNS changes that might affect the service. Take particular care to inform them of any configuration changes that have to be made in Outlook or Lync.

- Plan every change to DNS in detail
- Take extra care with MX records
- Work with a reliable cloud partner
- Communicate with users

Remember – DNS propagation can take up to 72 hours, so if you get your DNS settings wrong, it could take more than three days to sort it out – so be warned!

Lab: Configuring DNS Records and Migrating to Exchange Online

Scenario

Lucerne Publishing is now well into the Deploy phase and is in the process of adopting Office 365. The company needs to ensure that the cutover migration to Exchange Online is successful and that the DNS records for Office 365 are correctly configured. In addition, it needs to verify that all parent and subdomains have been added, and that the service records for different Office 365 services have been configured.

Objectives

The objectives of this lab are to:

- Add and configure domains and subdomains in Office 365.
- Carry out the cutover migration to Exchange Online.
- Configure DNS records for Exchange, SharePoint and Lync in Office 365.

Lab Setup

Estimated Time: 60 minutes

Virtual machine: 20346C-LUC-CL1

Username: **Student1**

Password: **Pa\$\$w0rd**

Where you see references in the steps to `lucernepublishingXXXX.onmicrosoft.com`, you should replace `XXXX` with the unique Lucerne Publishing number that you were assigned when you set up your Office 365 accounts in Module 1, Lab 1B, Exercise 2, Task 3, Step 5.

Where you see references to `labXXXXX.o365ready.com`, you should replace `XXXXX` with the unique `o365ready.com` number you were assigned when you registered your IP address at `www.o365ready.com` in Module 2, Lab 2B, Exercise 1, Task 2, Step 6.

Exercise 1: Perform a cutover migration to Exchange Online

Scenario

If Coralie Emond is feeling under pressure, she's trying hard not to let it show. Because Coralie is the Exchange guru at Lucerne Publishing, Heidi has decided that she should perform the Office 365 cutover migration, supported by Alain Richer. Coralie will also need to configure DNS domains with Office 365.

To carry out this process, she needs an administrator account on-premises and a global administrator account on Office 365. She also needs to access the on-premises DNS console and be able to reconfigure mail exchanger, canonical name and address records.

When she has completed the cutover migration, Coralie must configure DNS records for the Office 365 services and verify that those records are accessible.

The main tasks for this exercise are as follows:

1. Connect an Online Account to on-Premises Exchange Account
2. Add a Custom Domain to Office 365
3. Add a Subdomain to Office 365 and Change the Default Domain

4. Appoint a Migration Administrator
5. Create a Migration Endpoint in Office 365
6. Change User Principal Names to Ensure Migration
7. Perform the Batch Migration
8. Clean Up the Batch Migration

► **Task 1: Connect an Online Account to on-Premises Exchange Account**

1. On **LUC-CL1**, on the Task Bar, right-click **Internet Explorer** and click **Start InPrivate Browsing**
2. **Note:** You use an InPrivate browsing session so that you can log on with a separate set of credentials.
3. In the InPrivate session, type **https://mail.labXXXXX.o365ready.com/owa** (where XXXXX is your unique o365ready.com number) and press Enter.
4. In **Domain\user name**, enter **LUCERNE\LCartier** and in the **Password** field, enter **Pa\$\$w0rd**, then click **Sign in**.
5. Click **Continue to this Web site**.
6. If requested, set your language to **US English** and your time zone to **UTC**, and then click **Save**.
7. In **Luc Cartier's** session, click **New mail** and in the **To** field, enter **Coralie Emond**. Add a subject and suitable text and click **Send**.
8. In Internet Explorer, click **New tab** and then navigate to **outlook.office365.com**.
9. Log on as **Cemond@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number) with a password of **Pa\$\$w0rd**.
10. If requested, set your language to **US English** and your time zone to **UTC**, then click **Save**.
11. Review the **Inbox** and confirm that none of the messages from Luc Cartier are there.
12. On the right-hand side, click the **Settings** cog and click **Options**.
13. In **Account**, click **Connected accounts**.
14. In **Connected accounts**, click the + sign.
15. In **New account connection**, enter **cemond@labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number) as the **Email address** and a **Password** of **Pa\$\$w0rd**, and then and click **OK** in the right corner.
16. Click **OK** on the finished page.
17. In the **Connected accounts** page, click **Change default reply address**, select **cemond@labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number), and then click **Save**.
18. Under **Connected accounts**, note the status of the **cemond@labXXXXX.o365ready.com** account is **Downloading**.
19. Click **Options** in the left corner to return to the **Mailbox** page.
20. Note the emails from the on-premises server appearing in Exchange Online.
21. Click one of Luc Cartier's messages and click **REPLY**.
22. **Note:** The **From** field should be displayed. If it does not, click the ellipsis ... button and click **Show from**.

23. Note that the **From** field is set to **cemond@labXXXXX.o365ready.com**, (where XXXXX is your unique o365ready.com number).
24. Enter some text in the body of the message and click **SEND**.
25. Switch to Luc Cartier's session and check that the message has arrived. Note that the message is sent on behalf of **cemond@labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number).
26. Click **Reply** and note that the **Reply address** is **cemond@labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number).
27. Click **DISCARD**.
28. Log off from Luc Cartier's account.

► **Task 2: Add a Custom Domain to Office 365**

1. In **LUC-CL1**, on the Task Bar, right-click **Internet Explorer**, click **Start InPrivate Browsing**, and then navigate to **login.microsoftonline.com**.
2. Log on as **HLeitner@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number) with a password of **Pa\$\$w0rd**.
3. Click **Admin**, then click **Office 365**.
4. In the left-hand navigation, click **Domains**.
5. Click **Add domain**.
6. Click **Let's get started** to begin the process.
7. In the text box on the **Which domain do you want to use?** page, enter your domain name in the form of **labXXXXX.O365Ready.com** (where XXXXX is your unique o365ready.com number).
8. ASK ANOTHER STUDENT TO CONFIRM THAT YOU HAVE TYPED THE NAME IN CORRECTLY.
9. After confirmation, click **Next**.
10. Write down the **TXT** record shown in the **TXT value** column. This entry will be similar to **MS=msXXXXXXXXXX**. Record this value below:
MS=_____
11. Switch to **LUC-DC1**.
12. In **DNS Manager**, right-click **labXXXXX.o365Ready.com** (where XXXXX is your unique o365ready.com number), and click **Other New Records**.
13. Under **Select a resource record type**, scroll down to **Text (TXT)** and click **Create Record**.
14. In the **New Resource Record** box, leave the **Record name** field blank.
15. In the **Text** field, enter **MS=msXXXXXXXXXX** that you recorded in Step 10.
16. Click **OK** to create the record.
17. In the **Resource Record type** dialog box, click **Done**.
18. On **LUC-CL1**, press the **Windows** key, type **Command**, and click **Command Prompt**.
19. In the Command Prompt, type **NSLOOKUP** and press Enter.
20. At the NSLOOKUP prompt, type **server <IPAddress>**, where **<IPAddress>** is the external address of the Lucerne Publishing datacenter that you obtained after running the **GetIPAddress** script in Module 2, Lab B, Exercise 1, Task 1, Step 2. You should see a message saying:

- Default Server: <IPAddress>
- Address: <IPAddress>.

where <IPAddress> is your external address from your data center that you just entered into the **server <IPAddress>** command above.

21. Type **ls -t TXT labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number) and press Enter.
22. You should receive a message that the query was refused. This is expected behavior.
23. Switch to **LUC-DC1**, and in the **DNS Manager** console, right click the **labXXXXX.o365ready.com** domain and then click **Properties**.
24. In the **labXXXXX.o365ready.com Properties** dialog box, click the **Zone Transfers** tab.
25. In the **Zone Transfers** tab, click **To any server**, and then click **Apply**.
26. On **LUC-CL1**, in the NSLOOKUP prompt, type **ls -t TXT labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number) and press Enter.
27. **Note:** If this step and step 28 do not work, check with your instructor as your training location may be blocking TCP Port 53, which is required for DNS zone transfers.
28. Check that the "MS=XXXXXXXX" value is present and is the same as that in the Office 365 Admin Center.
29. Type **ls -d labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number) and press Enter.
30. Note the record(s) from the **labXXXXX.o365ready.com** zone.
31. Switch back to **LUC-DC1**, and in the **Zone Transfers** tab on the **labXXXXX.o365ready.com Properties** dialog box, click the **Only to servers listed on the Name Servers** tab, and then click **OK**.
32. Switch back to **LUC-CL1** and in the **Office 365 Admin** console, click **Okay, I've added the record**.
33. You should receive a message saying **We have verified that you own labXXXXX.o365ready.com**.
34. Click **"X"** to close the page.
35. In the **Add a domain to Office 365** page, click **Cancel**.

► Task 3: Add a Subdomain to Office 365 and Change the Default Domain

1. Switch to **LUC-DC1** and in **DNS Manager**, right-click **labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number) and click **New Domain**.
2. In the **New DNS Domain** dialog box, type **content** and then click **OK**.
3. You should now see a **content** subdomain under **labXXXXX.o365ready.com**.
4. In **LUC-CL1**, in the **Office admin** console, click **Domains**.
5. Click + **Add Domain**.
6. In the text box on the **Which domain do you want to use?** page, enter your **domain name** in the form of **content.labXXXXX.O365Ready.com** (where XXXXX is your unique o365ready.com number), and then click **Next**.
7. You should receive a message saying **We've verified that you own content.labXXXXX.o365ready.com**.
8. Click **Next**.

9. On the **Let's update your current Office 365 users to content.labXXXXX.O365Ready.com** page (where XXXXX is your unique o365ready.com number), scroll to the bottom of the page and click on **Skip this step**.
10. On the next page, click **Skip this step** again.
11. On the **Get ready to update DNS records to work with Office 365** page, click **Next**.
12. On the **Which services do you want to use with content.labXXXXX.O365Ready.com** page (where XXXXX is your unique o365ready.com number), clear **Outlook for email, calendar and contacts**, clear **Lync for instant messaging and online meetings**, then click on **Next**.
13. Click **Finish**.
14. In the top right corner of the **Office 365 admin center**, click **Lucerne Publishing (edit)**.
15. Under **Default domain**, verify that it is set to **labXXXXX.o365ready.com**.
16. Click **Save**.

► **Task 4: Appoint a Migration Administrator**

1. On **LUC-DC1**, click **Server Manager**.
2. In **Tools**, click **Active Directory Users and Computers**.
3. In **Active Directory Users and Computers**, expand **Lucernepublishing.local**, click **Accounts**, right-click **Coralie Emond** and click **Add to a group**.
4. In the **Select Groups** dialog box, under **Enter the object names to select**, enter **Domain Admins** and click **OK**.
5. In the **Active Directory Domain Services** dialog box, click **OK**.
6. On **LUC-CL1**, in the **Office 365 admin** console, click **Admin**, and then click **Office 365**.
7. Click **Users**, click **Active users**, and then click **Coralie Emond**.
8. In the **Details** page, click **Settings**.
9. Under **Assign role**, click **Yes** and from the list, select **Global Administrator**.
10. In the **Alternate email address** field, type **user@alt.none**.
11. Click **Save**.
12. Click **Heidi Leitner** and click **Sign out**.



► **Task 5: Create a Migration Endpoint in Office 365**

1. In the **Office 365 login** page, enter **cemond@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number) and **Pa\$\$w0rd** and click **Sign in**.
2. In the **Don't lose access to your account** page, under **Country or region**, select **Switzerland**. In the **Mobile phone number** field type **5551000**, and then click **Save and continue**.
3. In **Admin**, click **Exchange**.
4. In **Recipients**, click **Migration**.
5. In **Migration**, click the ellipsis ..., then click **Migration endpoints**.
6. In **Migration endpoints**, click the + sign.
7. In new **Migration endpoint**, click **Outlook Anywhere**, and then click **Next**.

8. On the **Enter on-premises account credentials** page, complete the following fields:
 - a. Email address: **cemond@labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number)
 - b. Account with privileges: **LUCERNE\Cemond**
 - c. Password of account with privileges: **Pa\$\$w0rd**
9. Click **Next**.
10. If you receive a failure message, enter the following information:
 - a. Exchange server: **LUC-EX1.LUCERNEPUBLISHING.LOCAL**
 - b. RPC proxy server: **mail.labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number)
11. Click **More options** and select the following settings:
 - a. Authentication: **NTLM**
 - b. Mailbox permission: **Domain Admin**
12. Click **Next**.
13. In the **New migration endpoint** page, enter the following information:
 - a. Migration endpoint name: **Lucerne Migration**
 - b. Maximum concurrent migrations: **10**
 - c. Maximum concurrent incremental syncs: **10**
14. Click **New**.
15. In the **Migration endpoints** page, click **Close**.

► **Task 6: Change User Principal Names to Ensure Migration**


1. In the **Migration** page, click the + sign and then click **Migrate to Exchange Online**.
2. In the **New migration batch** page, click **Cutover migration** and then click **Next**.
3. In the **Confirm the migration endpoint** page, check that the **Exchange server** is **LUC-EX1.LUCERNEPUBLISHING.LOCAL** and the **RPC proxy server** is **mail.labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number), and then click **Next**.
4. In the **New migration batch name**, enter **Lucerne Migration** and then click **Next**.
5. In the **Start the batch** page, check that **Coralie Emond** is the name showing, click **Manually start the batch later**, and then click **New**.
6. In the **Migration dashboard**, note the number of mailboxes to migrate and the current status.
7. Click the **Start** arrow.
8. In the **Warning** dialog box, click **Yes**.
9. Wait until the mailboxes have synced. Mailbox sync at this point typically takes 10-15 minutes.
10. **Note:** All the mailboxes that have a UPN of **lucernepublishingXXXX.onmicrosoft.com** will fail to sync at this point.
11. In the **Office 365 admin center**, click **Admin** then click **Office 365**.
12. Click **Users** and then click **Active Users**.


13. Click the check box to select **All users**.
14. Click the  (**Edit**) symbol.
15. Click **Details**, then under Domain, select **labXXXXX.o365ready.com**.
16. Click **Next**.
17. In **Settings**, click **Next**.
18. In **Assign licenses**, click **Submit**.
19. **Note:** **cemond@labXXXXX.o365ready.com** has the status of **Skipped**. You cannot edit yourself through bulk edit.
20. Click **Finish**.
21. If a message box appears, click **Yes**.
22. In **Active Users**, click the box next to **Coralie Emond** and click the  (**Edit**) symbol.
23. Click **Details**, then under **User name**, after the @ sign, select **labXXXXX.o365ready.com**.
24. Click **Save**.
25. In the warning message **Are you sure you want to make this change?**, click **Yes**.
26. In the **Finish your user ID change** message box, click **OK**.

► Task 7: Perform the Batch Migration

1. Click Internet Explorer and browse to **login.microsoftonline.com**.
2. Log on as **cemond@labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number) with a password of **Pa\$\$w0rd**.
3. Click **Admin** and then click **Exchange**.
4. In **Recipients**, click **Migration**.
5. Click the **Resume** button (it is the same as the Start button).
6. In the warning message, click **Yes**.
7. The status will read **Syncing**.

Note: This synchronization can take anywhere from 10 to 60 minutes. You can continue with the next steps when the user accounts appear.

8. In the **Exchange admin center**, click **Admin** then click **Office 365**.
9. Click **Users** and then click **Active Users**.
10. Check the boxes for all imported users and then click the  (**Edit**) icon.
11. In the **Details** page, click **Next**.
12. In the **Settings** page, under **Set user location**, click **Switzerland** and click **Next**.
13. In the **Assign licenses** page, click **Replace existing license assignments**, click **Microsoft Office 365 Plan E3**, and then click **Submit**.
14. In the **Results** page, click **Finish**.
15. In the **Office 365 admin center**, click **Admin**, then click **Exchange**.
16. In **Recipients**, click **Migration**.

17. Under **Mailbox status**, click **View details**.
18. The number of mailboxes that synced may vary per student. If LucAdmin's account does not sync, ignore this result.
19. Click **Close**.
20. In the **Exchange Admin Center**, in **Recipients**, under **Migration**, click the migration batch, and then click the  (**Delete**) icon.
21. In the **Confirmation** dialog box, click **Yes**.

► Task 8: Clean Up the Batch Migration

1. Switch to **LUC-EX1**.
2. In the Start page or on the Task bar, click **Internet Explorer**.
3. Browse to **https://mail.labXXXXX.o365ready.com/ECP** (where XXXXX is your unique o365ready.com number).
4. In **Domain\user name**, enter **LUCERNE\LucAdmin**, in **Password**, enter **Pa\$\$w0rd** and then click **Sign in**.
5. If prompted, under **Language** select **English (United States)** and under **Time zone**, select **(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna**, and then click **Save**.
6. In the **ECP**, click **Recipients** and click **Mailboxes**.
7. Notice all the current mailboxes.
8. Press the Windows key and in the Start screen, type **notepad**.
9. Click **Notepad**, and in the Notepad window, enter each of the following six commands on a separate line, each starting with the **\$enableusers** command:

```
$enableusers = Get-User -Filter {RecipientType -eq "UserMailbox"} -OrganizationalUnit "Accounts"
$enableusers | foreach { Disable-Mailbox $_.SamAccountName }
$enableusers | foreach { Enable-MailUser $_ -externalEmailAddress $_.UserPrincipalName.toString() }
$enableusers = Get-User -Filter {RecipientType -eq "UserMailbox"} -OrganizationalUnit "Sales"
$enableusers | foreach { Disable-Mailbox $_.SamAccountName }
$enableusers | foreach { Enable-MailUser $_ -externalEmailAddress $_.UserPrincipalName.toString() }
```

10. Click **File** and click **Save**.
11. In the **Save As** dialog box, save the file as **C:\temp\MailUser.ps1**.
12. Ensure that **Save as** type is set to **All Files (*.*)**.
13. Click **Save**.
14. Press the Windows key and click **Exchange Management Shell**.
15. In the **Exchange Management Shell**, type **cd C:\temp** and press Enter.
16. Type **.\MailUser.ps1** and press Enter.
17. Press Enter to disable each mailbox. You should see the users listed as mail-enabled users. The number of users may vary per student.

18. Switch back to **EAC** and click **Contacts**.
19. Click the **Refresh** icon.
20. You should now see the mail-enabled contacts, all with **username@labXXXXX.o365ready.com** addresses. The number of mail-enabled contacts may vary per student.

Results: Lucerne Publishing will have moved their email system to Exchange Online and set up DNS records for the Office 365 services.

Exercise 2: Configure DNS Records for Services

Scenario

With the cutover migration successfully completed and the mailbox content moved across to Exchange Online, Coralie can now set up the DNS records for the Office 365 services. Office 365 generates the correct DNS entries, and then Coralie needs to set up those entries in DNS. When she has completed this task, Office 365 checks that the correct records are in place.

The main tasks for this exercise are as follows:

1. Configure DNS Settings for Exchange Online
2. Check Lync Online functionality
3. Configure DNS Settings for Lync Online

► Task 1: Configure DNS Settings for Exchange Online

1. On **LUC-CL1**, in the **Office 365 admin center**, logged in as **Coralie Emond** (cemond@labXXXXX.o365ready.com) under the **Admin** menu, click **Office 365**.
2. In the left-hand column, click **Domains**.
3. In the list of domains, click **Complete Setup** next to **labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number).
4. In the **Add a new domain to Office 365** page, click **Step 2 Add users**.
5. On the **Add new users** page, click **If you don't want to add any users, you can skip this step** at the bottom of the page.
6. On the **Get ready to update DNS records to work with Office 365** page, click **Next**.
7. On the **Which services do you want to use with labXXXXX.o365ready.com** page, ensure that only **Outlook for Email, calendar, and contacts** is checked, and then click **Next**.
8. Note the settings in the **Add the following DNS records for labXXXXX.o365ready.com** page.

IMPORTANT: DO NOT CLOSE THIS PAGE.

9. Switch to **LUC-DC1**.
10. In **DNS Manager**, on the **View** menu, click **Advanced** to display the TTL value on records.
11. In the **labXXXXX.o365ready.com** zone, double-click the **Mail Exchanger (MX) record**.
12. In the **Mail Exchanger (MX)** tab, leave the **Host or child domain** field blank.
13. The **Fully qualified domain name (FQDN)** should be **labXXXXX.o365ready.com**.

14. In the **Fully qualified domain name (FQDN) of mail server** field, change the value from **mail.labXXXXX.o365ready.com** to the value from POINTS TO ADDRESS from the Office 365 console. The value will be something like **labXXXXX-o365ready-com.mail.protection.outlook.com**.
 15. Leave the default **TTL** value as **1 hour**.
 16. Change the **Mail server priority** to **0** and click **OK**.
 17. Double-click autodiscover.**labXXXXX.o365ready.com**.
 18. In the **Alias (CNAME)** tab, in the **Fully qualified domain name (FQDN) for target host**, replace the current value with **autodiscover.outlook.com**, and then click **OK**.
 19. Right-click the **labXXXXX.o365ready.com** zone (where XXXXX is your unique o365ready.com number), and click **New Alias (CNAME)**.
 20. In the Alias (CNAME) tab, in **Alias name**, enter **msoid**.
 21. In the **Fully qualified domain name (FQDN) for target host** field, type **clientconfig.microsoftonline-p.net** and then click **b**.
 22. Right-click **labXXXXX.o365ready.com** and click **Other New Records**.
 23. In the **Resource Record Type** dialog box, scroll down and select **Text (TXT)**, then click **Create Record**.
 24. In the **Text field**, enter the value specified in the **TXT VALUE** column in the **Office 365 add these dns records for labXXXXX.o365ready.com at your dns hosting provider** page (typically this value is **v=spf1 include:spf.protection.outlook.com -all**, but it may be different in your location), then click **OK**.
 25. **Important:** Check that when you create this DNS record, you do not include any trailing or leading spaces and that it is an **en-dash (–)**, not an **em-dash (—)**, otherwise the DNS check will fail.
 26. In the **Resource Record Type** dialog box, click **Done**.
 27. Switch back to **LUC-CL1**.
 28. In the **Office 365 admin console**, click **Okay, I've added the records**.
 29. If the check does not complete, wait 15 minutes and then check again.
 30. You should see a message saying **You're done! labXXXXX.o365ready.com is ready to work with the Office 365 services you selected**.
 31. Click **Finish**.
 32. Switch to your personal email account and send a message to **cemond@labXXXXX.o365ready.com**.
 33. On **LUC-CL1**, switch to Coralie's Office 365 login. Confirm that the email appears in Office 365.
 34. You have now set up Exchange Online to work with a custom domain.
- **Task 2: Check Lync Online functionality**
1. Click **Office 365** and then click **Outlook**.
 2. In **Outlook**, note that there is a grey patch between Coralie's name and Admin.
 3. Click on **Coralie Emond** and in the drop-down box, click **Sign in to IM**.
 4. Repeat step 3 and note the message saying **"There's a problem with IM"**.
 5. Confirm that the grey patch does not go green.

Why is IM not working for this account?

Because the user account has been changed to **username@labXXXXX.o365ready.com**, and this domain has not yet been set up for Lync Online.

► **Task 3: Configure DNS Settings for Lync Online**

1. Click **Admin**, then click **Office 365**.
2. On the left-hand column, click **Domains**.
3. In the list of domains, click **labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number), then click **Manage DNS** in the right pane, and then click **Change domain purpose**.
4. Click the **Lync for instant messaging and online meetings** check box, and then click **Next**.
5. Keep the **Add following DNS records for labXXXXX.o365ready.com at your DNS hosting provider** page open.
6. Switch to the **LUC-DC1** virtual machine in the Lucerne Publishing data center.
7. Right-click the **labXXXXX.o365ready.com** zone and select **Other New Records**.
8. In the **Resource Record Type** dialog box, scroll down the list and click **Service Location**, and then click **Create Record**.
9. In the **Service Location (SRV)** tab, enter the following information and then click **OK**:
 - a. Service: **_sip**
 - b. Protocol: **_tls**
 - c. Priority: **100**
 - d. Weight: **1**
 - e. Port number: **443**
 - f. Host offering this service: **sipdir.online.lync.com**
 - g. Time to live: 1 hour (default)
10. In the **Resource Record Type** dialog box, click **Create Record**.
11. In the **Service Location (SRV)** tab, enter the following information and then click **OK**:
 - a. Service: **_sipfederationtls**
 - b. Protocol: **_tcp**
 - c. Priority: **100**
 - d. Weight: **1**
 - e. Port number: **5061**
 - f. Host offering this service: **sipfed.online.lync.com**
 - g. Time to live: 1 hour (default)
12. In the **Resource Record Type** dialog box, scroll back up the list and click **Alias (CNAME)**, and then click **Create Record**.
13. In the **Alias (CNAME)** tab, enter the following information, and then click **OK**:
 - a. Alias name: **sip**

- b. Fully qualified domain name: **sip.labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number)
 - c. Fully qualified domain name (FQDN) for target host: **sipdir.online.lync.com**
 - d. Time to live: **1 hour (default)**
14. In the **Resource Record Type** dialog box, click **Create Record**.
15. In the **Alias (CNAME)** tab, enter the following information, and then click **OK**:
 - a. Alias name: **lyncover**
 - b. Fully qualified domain name: **lyncover.labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number)
 - c. Fully qualified domain name (FQDN) for target host: **webdir.online.lync.com**
 - d. Time to live: **1 hour (default)**
16. In the **Resource Record Type** dialog box, click **Done**.
17. Switch back to **LUC-CL1**, then in the **Office 365 admin console**, click **Okay, I've added the records**.

Note: Lync can sometimes take more than 15 minutes to register.
18. You should now see the message: **You're records are correct and labXXXXX.o365ready.com is all set up**. Click **Finish**.
19. In the **Office 365 admin** console, click **Outlook**, then click **Coralie Emond**.
20. The options for IM should appear and the status patch should turn green.
21. In **LUC-CL1**, on the Task Bar, right-click Internet Explorer and click **Start InPrivate Browsing**.
22. In Internet Explorer, navigate to **login.microsoftonline.com** and log on with a **User name** of **Hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number) and a **Password** of **Pa\$\$w0rd**.
23. Click **Outlook**, and then click the **New** button in the upper left corner.
24. In the **To:** field, enter **Coralie Emond**.
25. When the name resolves, note her IM status. It may take a couple of minutes for her status to update.
26. Click **Coralie Emond** in the **To** field.
27. In the pop-up box, click the **IM** icon on the right.
28. In the IM pop-up window, type a message and press Enter.
29. Switch to the **Coralie Emond** Internet Explorer window. If your session has timed out, log in again.
30. In the **IM request** dialog box, click **Accept**.
31. Reply to the IM. Note that you can now send IMs between the two users.
32. Close Coralie's Office 365 session

Results: Lucerne Publishing has configured the DNS records for Exchange Online, SharePoint Online, and Lync Online.

Lab Discussion Questions

What is the key user action that needs to take place prior to a cutover migration?

Users must reduce the size of their mailboxes by deleting unnecessary email messages. They can back up these email messages to .PST files if necessary.

When setting up DNS on your own server to work with Office 365, what PowerShell cmdlet could you use to verify that a server on IP address 10.176.89.42 is working and authoritative for the lucernepublishing.com zone?

Test-DnsServer -IPAddress "10.176.89.42" -zonename "lucernepublishing.com"

- What is the key user action that needs to take place prior to a cutover migration?
- When setting up DNS on your own server to work with Office 365, what PowerShell cmdlet could you use to verify that a server on IP address 10.176.89.42 is working and authoritative for the lucernepublishing.com zone?

Module Review and Takeaways

Having completed this module, you should now be able to:

- Recommend a mailbox migration strategy for moving to Exchange Online.
- Plan for implementing Exchange Online within your organization.



Best Practice: Best practices when planning Exchange Online and migration include:

- Ensure you have considered all the factors when selecting the migration path to Exchange Online.
- Analyze the risks to consider all possible “what-if” scenarios and identify mitigation plans to deal with each risk.
- Ensure you apply a structured change management methodology to the migration plan and adoption process.
- Keep your project sponsor, management team, administrators, and users informed about what is going on, particularly in the lead-up to any switchover.
- Make sure that everyone involved in the project has had sufficient training and is competent to carry out their tasks.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Timing of DNS updates	
MX records	

Module 7

Administering Exchange Online

Contents:

Module Overview	7-1
Lesson 1: Configure Personal Archive Policies	7-2
Lesson 2: Manage Anti-malware and Anti-spam Policies	7-17
Lesson 3: Configure Additional Email Addresses for Users	7-29
Lesson 4: Create and Manage External Contacts, Resources, and Groups	7-35
Lab: Administering Exchange Online	7-50
Module Review and Takeaways	7-68

Module Overview

In this module, you learn how to configure Exchange Online settings that you planned in the previous module, including archive policies, anti-malware and anti-spam settings, additional email addresses and external contacts and resources. These are actions that you would typically carry out during the Deploy phase of the Office 365™ FastTrack deployment or as part of the normal management operations of Exchange Online.

You typically carry out these actions through the Office 365 portal, although you can also use the Windows Azure™ Active Directory® PowerShell® console to access additional features.

Objectives

After completing this module, you should be able to:

- Configure Messaging Records Management (MRM) for Exchange Online.
- Manage Anti-malware and Anti-spam Policies.
- Configure additional email addresses for users.
- Create and manage external contacts, resources, and groups in Exchange Online.

Lesson 1

Configure Personal Archive Policies

In this lesson, you will learn how to enable personal archive for mailboxes, create custom retention policies, create retention tags, apply retention policy, and review and modify the default retention policy. These actions enable you to control how information is retained and also how users can ensure that important information is protected.

Lesson Objectives

After completing this lesson, you should be able to:

- Explain what MRM is and how it can help protect messaging data.
- Enable an in-place archive for a mailbox.
- Describe how retention tags and retention policies work.
- Describe the difference between mandatory and personal retention tags.
- Explain the process for configuring retention tags.
- Explain the process for configuring retention policies.
- Explain the operation of the Managed Folder Assistant.
- Apply retention policies to mailboxes.
- Configure in-place eDiscovery.
- Enable in-place litigation hold.

Introduction to Messaging Records Management

MRM is a key feature in Office 365 that applies to data stored on the platform to help organizations meet business, legal, and regulatory requirements. For example, a bank may be required to maintain records about specific transaction types, yet it will not want to implement a blanket “store everything” policy that could overwhelm even the generous storage limits in Exchange Online. Alternatively, a health provider may not want staff inadvertently sending out email messages that contain patients’ insurance policy numbers. Finally, organizations that work in regulated environments may have to provide strict tracking and auditing of all communications within the company.

MRM consists of the following elements:

- Personal archives
- Retention tags
- Retention policies
- eDiscovery and litigation hold
- Journaling

- Messaging Records Management is a key feature of Exchange Online
- MRM protects data by ensuring that records are kept of email messages
- MRM also controls mailbox sizes through automatic archiving and deletion
- MRM consists of:
 - Personal archives
 - Retention tags
 - Retention policies
 - eDiscovery and litigation hold
 - Journaling
 - Data loss prevention
 - Auditing

- Data loss prevention
- Auditing



Note: Journaling and Auditing are outside the scope of this course.

Configuring In-Place Archives

In Module 6, you were introduced to the concept of personal or in-place archives and the licensing arrangements that have to be in place to enable users to access this feature. In this topic, you will look at how to configure these archives and how to use them.

To make in-place archives available to users, they must satisfy the following criteria:

- Be assigned a suitable licensing level within Office 365 (typically Office 365 E3/E4 or equivalent, Exchange Online Plan 2, or as an add-on with other plans).
- Have the feature enabled by using Office 365 admin center or PowerShell.
- Be using a supported mail client (either Outlook® 2013, Outlook 2010, Outlook Web App and certain versions of Outlook 2007).

- Requires:
 - Assigned suitable Office 365 licence
 - Archive-enabled mailbox
 - Supported messaging client
- Enable by using EAC or PowerShell
- Disable by using EAC or PowerShell
- Reconnect by using PowerShell only
- Users can move messages to the archive:
 - Manually
 - Through Inbox rules
 - AutoArchive
 - Personal retention policies



For more information on the supported mail clients for in-place archiving, see the following article:

<http://go.microsoft.com/fwlink/?LinkId=391716>

Enabling In-Place Archive

To enable an in-place archive for a user mailbox in Exchange admin center (EAC), perform the following steps:

1. In Exchange admin center (EAC), navigate to **recipients** and view **mailboxes**.
2. Click to select a mailbox.
3. In the **details** pane, under **In-Place Archive**, click **Enable**.
4. In the warning message box, click **yes**. Unlike Exchange 2013, you do not need to select a mailbox database to host the archive mailbox.
5. Under In-Place Archive, you can now click View details. However, until the user logs on and opens his or her in-place archive, this link will give a warning message. Click **OK** and click cancel to close the Archive Mailbox dialog box.

You can also bulk-enable archives by selecting multiple mailboxes, using the Shift or Ctrl keys. After selecting multiple mailboxes, in the details pane, click **More options**. Then, under **Archive** click **Enable**.

To enable an in-place archive by using PowerShell, type the following command and press Enter.

Enable-Mailbox "User Name" -Archive

To check which mailboxes are enabled for archiving, enter the following command:

Get-Mailbox -Archive -ResultSize Unlimited

Disabling In-Place Archive

To disable an in-place archive, carry out the following steps:

1. In EAC, navigate to **recipients** and view **mailboxes**.
2. Click to select a mailbox.
3. In the **details** pane, under **In-Place Archive**, click **Enable**.
4. In the warning message box, click **yes**.

To disable an in-place archive using PowerShell, enter the following command:

Disable-Mailbox -Identity "User Name" -Archive

This command does not disable the mailbox itself.

To connect a disabled archive to a mailbox user, you have to use PowerShell and establish the GUID of the disconnected archive by using the following command:

Get-MailboxDatabase | Get-MailboxStatistics -Filter 'DisconnectDate -ne \$null'

You then use the following command, replacing the GUID shown with the one resulting from the previous command:

Connect-Mailbox -Identity "8734c04e-981e-4ccf-a547-1c1ac7ebf3e2" -Archive -User "User Name"

After you have enabled an in-place archive mailbox, the user has several ways of moving messages into the archive mailbox. Options include:

- Manually transferring messages by drag-and-drop or the Move command.
- Setting up Inbox rules to transfer messages.
- Configuring AutoArchive.
- Moving messages through applying personal retention policies.



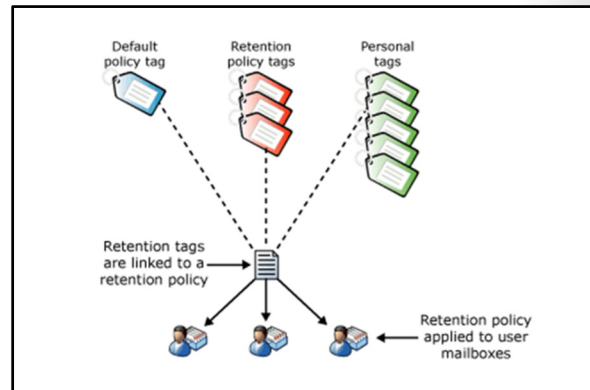
In hybrid Exchange environments, you can also configure online archives that provide storage for on-premises mailboxes. You can also use the stand-alone Exchange Online Archiving service to hold and manage this data. See the following link for more information:

<http://go.microsoft.com/fwlink/?LinkId=391718>

Retention Tags

A retention tag is the main component of MRM. The following are the three types of retention tags that apply at different levels:

- *Default Policy Tags (DPTs)*. Apply automatically to messages in an entire mailbox where no other policy tag applies.
- *Retention Policy Tags (RPTs)*. Apply automatically to the default folders, such as Inbox, Calendar, and so on.
- *Personal tags*. Are set manually through user assignment to messages and folders.



These retention tag types include some or all of the following elements:

- A unique name
- A default folder (RPTs)
- A retention action. Available retention actions are:
 - Delete and allow recovery
 - Permanently delete (do not allow user recovery)
 - Move to archive (for archiving tags – not for RPTs)
- A retention period, measured in days (with the option of Never for personal tags)

These retention tags are then all linked in to a retention policy, and that policy applied to mailboxes, folders, and/or messages.

Office 365 includes the following predefined retention tags:

- DPT: 2 year move to Archive
- RPT: Deleted Items folder – delete after 30 days
- RPT: Junk Email folder – delete after 30 days
- Personal: Never move to archive
- Personal: 5 years move to archive
- Personal: 1 year move to archive
- Personal: Never delete
- Personal: 5 year delete
- Personal: 1 year delete
- Personal: 6 month delete
- Personal: 1 month delete
- Personal: 1 week delete

If necessary, you can then create further retention tags to meet your organization's requirements and either add those tags to the default retention policy or create a new retention policy to hold them.

In their own mailbox settings, a user can select which personal retention tags to apply from all defined retention policies.

The following graphic shows the relationship between retention tags and policies:

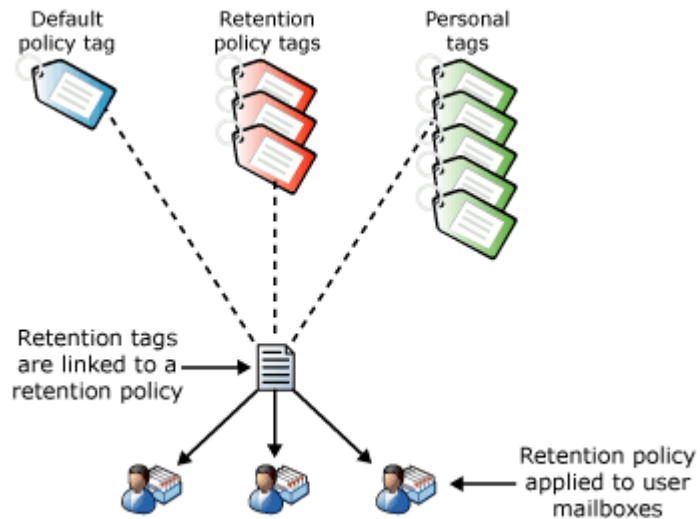



FIGURE 7.1: DIFFERENT TYPES OF RETENTION TAGS CAN BE COMBINED INTO RETENTION POLICIES, WHICH THEN APPLY TO USER MAILBOXES.

Retention Policies

A retention policy is a collection of retention tags that can consist of one or two DPTs, along with a maximum number of RPTs and unlimited personal tags. The organization can then apply the retention policy to user mailboxes and users can also select which personal tags to apply to folders and messages in their mailboxes.

 **Note:** Users cannot see the actual retention policy names – they only see the retention tags within those policies. However, a mailbox can only have one mailbox policy applied to it.

- A retention policy is a group of retention tags that apply to a mailbox
- A mailbox can have only one retention policy applied to it
- When a mailbox is created, a default retention policy is applied
- In Exchange Online, the default retention policy applied to new mailboxes is **Default MRM Policy**
- New policies may be required to deal with differing retention needs

A retention policy can have two DPTs, each with a different retention action, along with one RPT for each default folder, combined with any number of personal tags.

There is a default MRM policy that contains the following retention tags:

- Default 2 year move to archive
- Never Delete
- 5 Year Delete
- 1 Year Delete

- 6 Month Delete
- 1 Month Delete
- 1 Week Delete
- Deleted Items
- Junk Email
- Recoverable Items 14 days move to archive
- Personal 1 year move to archive
- Personal 5 year move to archive
- Personal 5 year move to archive
- Personal never move to archive

If these retention tags meet your organization’s requirements for retaining and deleting messages, then you do not have to define any more retention tags or policies. Alternatively, you can create additional retention tags and add those to the default MRM policy.

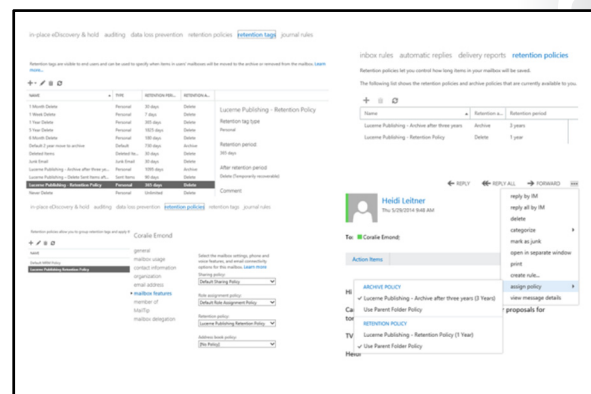
If your organization’s requirements are not well aligned with what is provided in the default MRM policy, then define the retention tags you need, and create a new retention policy that includes those tags, together with any of the existing retention tags.

Alternatively, you may have the situation where, for legal or regulatory reasons, individual employees or entire departments can have different retention needs. You can then create a new retention policy for those employees, link the appropriate retention tags, and then apply the policy to those mailboxes.

To manage retention tags and policies globally across an organization, use Windows PowerShell to connect to Exchange Online.

Distinguishing Tags and Policies

It is important to understand how tags and policies are represented in the Exchange admin console and in the Outlook user interface. This requirement is because the terms “tags” and “policies” are used interchangeably and what the user sees is not what the administrator sees.



Administrator

As an administrator, you will use EAC or PowerShell to create one or more retention tags. Each tag may have archive or retention actions. You then create a retention policy and add the tags you create to that policy (or edit the default policy). Finally, you then assign that policy to one or more users. Optionally, you can then use PowerShell to update users’ mailboxes.

User

As a user, you then add those tags to your account. However, what is confusing here is that what were retention tags in Exchange admin center become retention policies in OWA. To make matters more confusing, when you apply those policies in Outlook, they are separated out into archive policies and

retention policies, depending on whether the original retention tag had a retention action or an archive action.

Managed Folder Assistant

The Managed Folder Assistant is an automatic process that runs on a schedule in the Office 365 data centers and processes the retention settings that apply to each mailbox. The Managed Folder Assistant applies any DTPs and RPTs that exist within the retention policy and makes personal retention tags available in Outlook or Outlook Web App for users to apply. The Managed Folder Assistant also processes item retention, based on factors such as tag type, retention age, and the specified retention actions.

The Managed Folder Assistant does not run to a specific schedule but operates on a seven-day work cycle. The work cycle ensures that retention policy processing for all mailboxes in an organization should take place within that seven-day period.

You can run the Managed Folder Assistant manually by using the **Start-ManagedFolderAssistant** cmdlet in Windows PowerShell. For example, to run the Managed Folder Assistant against Heidi Leitner's mailbox, enter the following string at a PowerShell prompt while connected to Exchange Online:

Start-ManagedFolderAssistant -Identity "Heidi Leitner"

You can also use PowerShell to put a mailbox on retention hold; this action suspends the retention policy that applies to that mailbox and the Managed Folder Assistant will not process any retention settings or execute any retention actions on tagged messages.

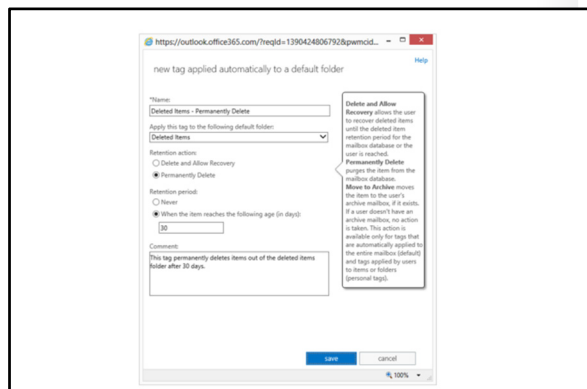
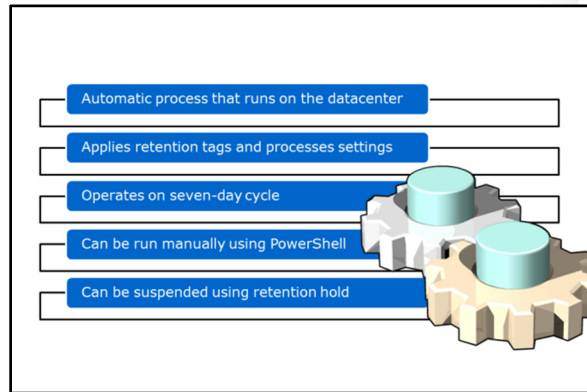
To put a mailbox on retention hold, run the **Set-Mailbox** command with the **-RetentionHoldEnabled** command. For example, to put Remi Desforges' mailbox on retention hold, you would run the following command at the PowerShell prompt:

Set-Mailbox "Remi Desforges" -RetentionHoldEnabled \$true

Configuring Retention Tags

Configuring a retention tag can be done either through the Exchange Online admin center or by using Windows PowerShell commands when connected to Exchange Online.

1. In Exchange admin center, click **Compliance management** and then click **Retention tags**.
2. In Retention tags, click the + (new) button and select one of the following:
 - a. **Applied automatically to an entire mailbox (default)**
 - b. **Applied automatically to a default folder**



c. Applied by users to items or folders

3. The user interface you then see will vary, according to the option you selected.
4. You set a name, configure the retention action, and a retention period, then click **Save** to add the retention tag to the list of default tags.

To create a retention tag using PowerShell, open a PowerShell connection to Exchange Online using the **Connect-MsolService** cmdlet and administrative credentials. Then in the PowerShell window, type the following command and press Enter:

New-RetentionPolicyTag "Tag name" -Type <tagtype> -AgeLimitForRetention <days> -RetentionAction <specify retention action>

The new retention tag will be visible in Exchange admin center and can now be added to retention policies.

The following graphic displays the new retention tag user interface:

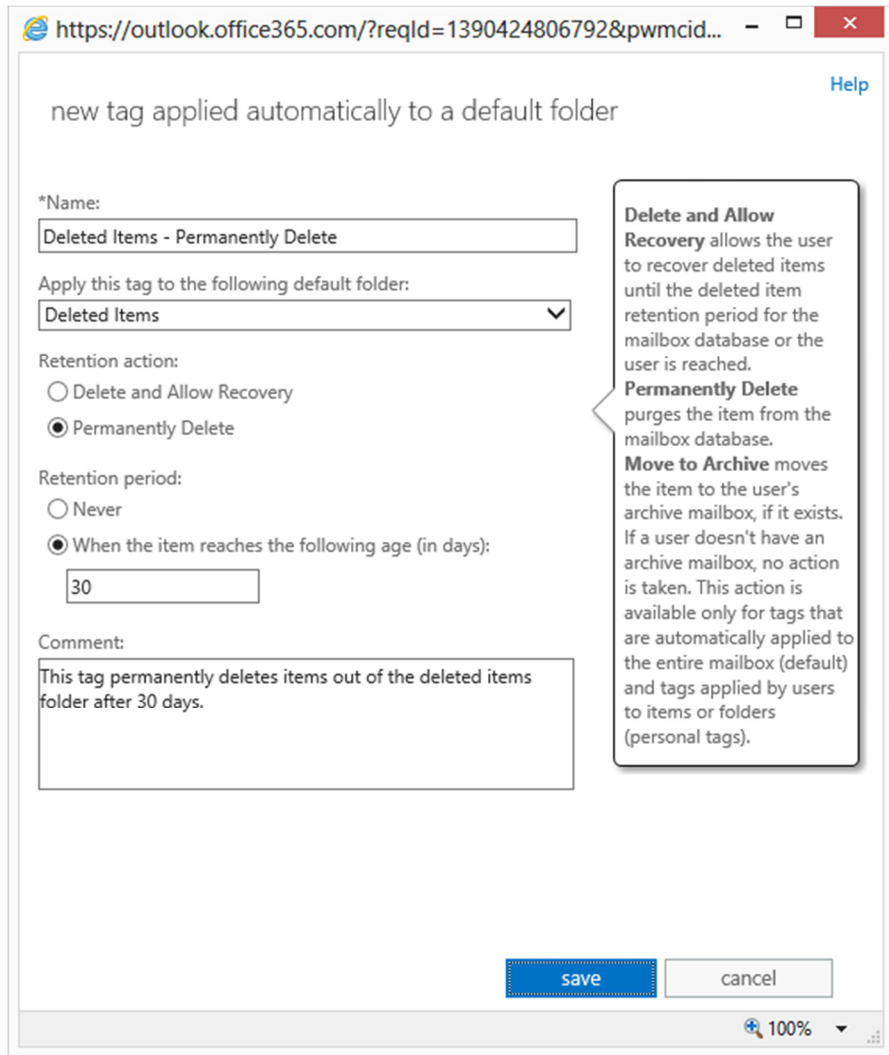


FIGURE 7.2: THE USER INTERFACE FOR THE DEFAULT FOLDER TYPE OF RETENTION TAG

Configuring Retention Policies

Configuring retention policies is simply a matter of creating a new policy and then adding the tags you want to that policy. Again, this process can be carried out using Exchange admin center or PowerShell.

1. In Exchange admin center, click **Compliance management** and then click **Retention policies**.
2. In retention tags, click the + (new) button.
3. Enter a name for the new policy.
4. Click the + button and then select policy tags from those listed.
5. Click **Save**.

The new retention policy interface appears as follows:

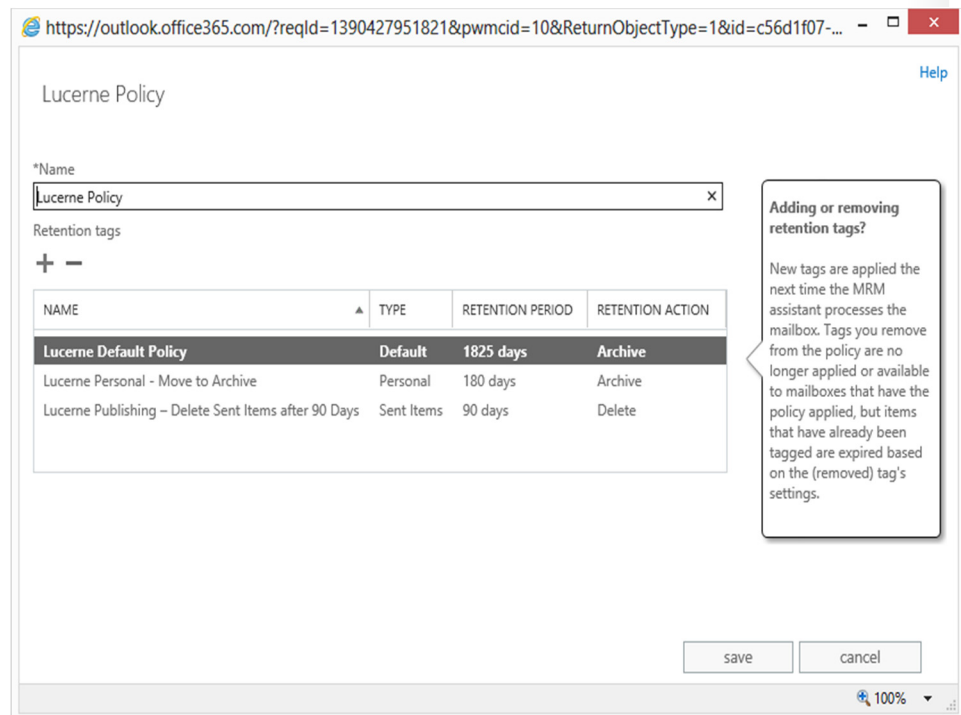


FIGURE 7.3: THE RETENTION POLICY USER INTERFACE

The equivalent PowerShell cmdlet is **New-RetentionPolicy**, which contains the following syntax:

New-RetentionPolicy <name> -RetentionPolicyTagLinks <list of retention tags>

Applying Retention Policies to Mailboxes

To apply a retention policy to a single mailbox or to multiple mailboxes, you can use either EAC or PowerShell.

In EAC, perform the following procedure:

1. Click **Recipients**.
2. In the list view, select the mailbox to which you want to apply the retention policy, and then click the edit icon.
3. In the "User Name" page, click **Mailbox features**.
4. Under **Retention policy**, select the policy you want to apply to the mailbox, and then click **Save**.

- Apply policy to a mailbox using EAC or PowerShell
- With EAC, slightly different steps for single or multiple mailboxes
- With PowerShell, easy to set retention policies for one or multiple mailboxes
- Use the **Get-Mailbox "Mailbox Name" | Select RetentionPolicy** to find what policy applies to a particular mailbox

For multiple recipients, the process is slightly different:

1. In the list view, use the Shift or Ctrl keys to select multiple mailboxes.
2. In the **Details** pane, click **More options**.
3. Under **Retention Policy**, click **Update**.
4. In **Bulk assign retention policy**, select the retention policy you want to apply to the mailboxes, and then click **Save**.

With PowerShell, use the following command to change the policy for one mailbox:

Set-Mailbox "Mailbox Name" -RetentionPolicy "RetentionPolicyName"

To change policy for all mailboxes, use the following command:

Get-Mailbox -ResultSize unlimited | Set-Mailbox -RetentionPolicy "RetentionPolicyName"

To change an old retention policy to a new one, enter the following command:

**\$OldPolicy={Get-RetentionPolicy "Old-Retention-Policy"}.distinguishedName
Get-Mailbox -Filter {RetentionPolicy -eq \$OldPolicy} -Resultsize Unlimited | Set-Mailbox -RetentionPolicy "New-Retention-Policy"**

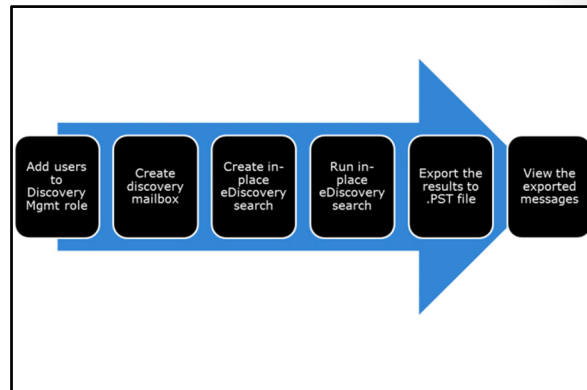
To test whether a mailbox policy has been applied, use the following command:

Get-Mailbox "Mailbox Name" | Select RetentionPolicy

Configuring eDiscovery

Many organizations need to be able to search mailboxes for specific content when they are performing compliance audits. As part of a data loss prevention strategy, you need a way to identify data in users' mailboxes that might violate the organization's compliance policy.

Exchange Online provides a way to search through users' mailboxes called In-Place eDiscovery. Authorized personnel can use In-Place eDiscovery to search one or more mailboxes in the Exchange organization and to see mailbox items resulting from the search query.



To configure eDiscovery, perform the following process:

1. Add users to the Discovery Management role group.
2. Create a discovery mailbox.
3. Create an in-place eDiscovery search.
4. Run the in-place eDiscovery search.
5. Export the results of the eDiscovery search to a .PST file.
6. View the exported messages.

To add users to the Discovery Management Role group, perform the following steps:

1. In EAC, navigate to **Permissions**, then view **Admin roles**.
2. In the list view, select **Discovery Management**, and then click the Edit Icon.
3. In **Role Group**, under **Members**, click Add Icon.
4. In Select Members, select one or more users, click Add, and then click **OK**.
5. In Role Group, click **Save**.

Create a Discovery Mailbox

Exchange Online creates a discovery mailbox by default. You must use the Exchange Shell if you need to create additional discovery mailboxes. To create a discovery mailbox, connect to Exchange Online using Windows Azure Active Directory PowerShell and run the following command:

```
new-mailbox SearchResults -Discovery -PrimarySmtpAddress Searchresults@contoso.com
```

To list the discovery mailboxes in an organization, run the following command:

```
Get-Mailbox -Resultsize unlimited -Filter {RecipientTypeDetails -eq "DiscoveryMailbox"}
```

Create an In-Place eDiscovery Search

To create an in-place eDiscovery search, log on as a user who is a member of the Discovery Management role and carry out the following steps:

1. In EAC, go to **Compliance management** and click **In-place eDiscovery & hold**.
2. Click the + icon.
3. In **New in-place eDiscovery & hold**, on the **Name and description** page, type a name for the search, add an optional description, and then click **Next**.

4. On the **Mailboxes** page, select the mailboxes to search. You can search across all mailboxes or select specific ones to search.



Note: You cannot use the **Search all mailboxes** option to place all mailboxes in Exchange Online on hold. To create an In-Place Hold, you must select **Specify mailboxes to search**.

5. On the **Search query** page, complete the following fields:
 - a. **Include all user mailbox content.** Select this option to place all content in the selected mailboxes on hold.
 - b. **Filter based on criteria.** Select this option to specify search criteria, including keywords, start and end dates, sender and recipient addresses, and message types.



Note: When placing mailboxes or items on In-Place Hold for legal purposes, it is generally recommended to hold items indefinitely and remove the hold when the case or investigation is completed.

6. Set the In-Place Hold settings – these are covered in the next topic.
7. Click **Finish** to save the search, then click **Close** when the search finishes.

Run the In-Place eDiscovery Search

There are three phases to running an in-place eDiscovery search:

1. Estimate the size of the search results.
2. Preview the search results.
3. Run the search.

Although you can go straight to running the search, you are recommended to preview the results to ensure that they are the size that you are expecting. For example, if your preview returns no results, the search criteria may be set too narrowly; in this case, try widening the criteria and run the search again.

To run these three phases, perform the following steps:

1. In EAC, go to **Compliance management**.
2. In **In-place eDiscovery and hold**, click the eDiscovery search that you created earlier.
3. In the icon row, click the magnifying glass symbol, and then click **Estimate search results**.
4. In the **Warning** message box, click **OK**.
5. In the right-hand pane, note the number of items the search has returned.
6. In the icon row, click the magnifying glass symbol, and then click **Preview search results**. A new tab opens with the results.
7. In the **eDiscovery search preview: search name** preview pane, note the number of items the search has returned.
8. If the number of search items is as expected, in the icon row, click the magnifying glass symbol, and then click **Copy search results**.
9. In the **Search name** dialog box, select the options you want, such as including unsearchable items, enabling de-duplication (recommended for large searches), enabling full logging and sending

yourself an email message when the copy operation completes (bearing in mind this can take several hours with a large mailbox when searching all items).

10. Select the discovery mailbox to which you want the search items copied. Note that any additional discovery mailboxes you have created will appear here.
11. In the **Warning** message box, click **OK**.

Export the results of the eDiscovery search

When the search completes, perform the following steps:

1. In **In-place eDiscovery and hold**, click the eDiscovery search that you created earlier.
2. In the icon row, click the download icon.
3. In the **Application Run – Security Warning** dialog box, click **Run**.
4. In the **eDiscovery PST Export Tool** dialog box, click Browse to select the location where you want to save the search results as a PST file, then click **OK**.
5. In the **Windows Security** dialog box, enter the credentials for the user with the Discovery Management role in the form username@office365domain.
6. When the export completes, click **Close**.

View the exported messages

You can now open the exported data files in Outlook 2010 or 2013.

1. In Outlook, click **File**.
2. Click **Open & Export**.
3. Click **Open Outlook Data File**.
4. Browse to the location where you saved the PST file, click it, then click **OK**.
5. In Outlook, browse the folder structure on the left of the application to find the “Name Search – Mailbox name-date-time” folder.
6. Expand the folders and click **Primary Mailbox**. In this folder are all the folders included in the search, such as Inbox, Sent Items, and so on. You can then click and view any item.

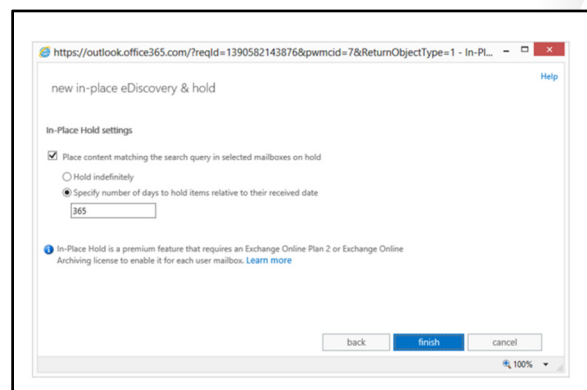


See the following link for more information about in-place eDiscovery:

<http://go.microsoft.com/fwlink/?LinkId=391719>

Configuring In-Place Hold

If an organization has a reasonable expectation that a legal case may arise, then that organization is required to preserve all electronic records, such as email, web pages, and IM messages. As a result, organizations that have a reasonable expectation of being involved in litigation can take steps to preserve electronic records. In-place hold is an add-on to eDiscovery which enables you to place individual mailboxes on hold and preserve messages in that mailbox, preventing both accidental and deliberate deletion.



In-place hold is configured as part of setting up an eDiscovery search. If you have the right licensing level (Exchange Online Plan 2 or Exchange Online Archiving License), then the option for In-Place Hold is available.

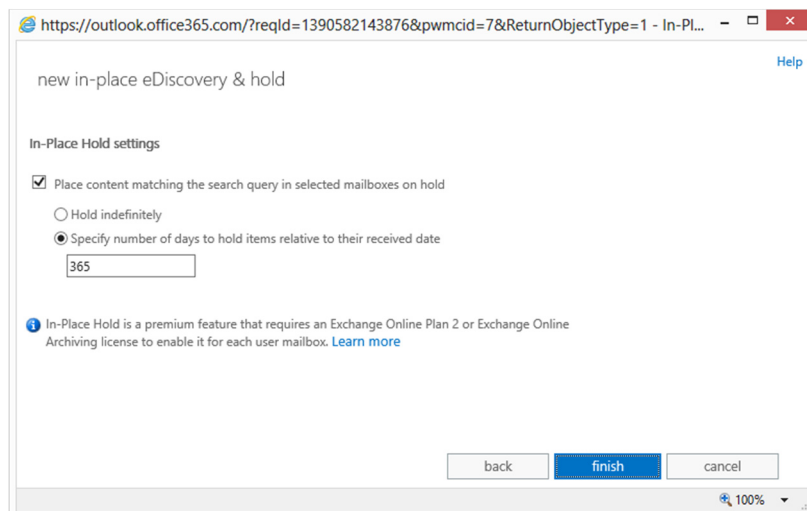
When you run the in-place eDiscovery & hold wizard, you amend the steps as follows:

1. In EAC, go to **Compliance management** and click **In-place eDiscovery & hold**.
2. Click the + icon.
3. In **New in-place eDiscovery & hold**, on the **Name and description** page, type a name for the search, add an optional description, and then click **Next**.
4. On the **Mailboxes** page, click Specify mailboxes to search, and then select those mailboxes.
5. On the **Search query** page, complete the following fields:
 - a. **Include all user mailbox content**. Select this option to place all content in the selected mailboxes on hold.
 - b. **Filter based on criteria**. Select this option to specify search criteria, including keywords, start and end dates, sender and recipient addresses, and message types.
6. On the **In-place hold settings** page, select the **Place content matching the search query in selected mailboxes on hold** check box, and then select one of the following options to place items on In-Place Hold:
 - a. **Hold indefinitely**. Select this option to place the returned items on an indefinite hold. Items on hold will be preserved until you remove the mailbox from the search or remove the search.
 - b. **Specify number of days to hold items relative to their received date**. Use this option to hold items for a specific period. For example, you can use this option if your organization requires that all messages be retained for at least seven years. You can use a time-based In-Place Hold, along with a retention policy, to make sure items are deleted in seven years.
7. Click **Finish** to save the search, then click **Close** when the search finishes.

To use PowerShell to create an in-place hold, use the following command:

New-MailboxSearch "Search Name" -SourceMailboxes "jburns@lucernepublishing.com" -InPlaceHoldEnabled \$true

The following screenshot shows the in-place discover and hold feature user interface:





For more information on in-place hold, see the following link:

<http://go.microsoft.com/fwlink/?LinkId=392268>

Lesson 2

Manage Anti-malware and Anti-spam Policies

AVTest, the independent IT security institute, has registered more malicious software programs in January 2014 than in the whole of 2013. Malware types and variants continue to grow exponentially, with more than 180,000 unique detections in 2013 and the possibility of five times that number in 2014. Kaspersky Labs Spam Statistics Report for Q2 2013 recorded an average of 70.7 per cent of global email traffic as spam, indicating that only three in ten email messages are of value.

These figures show that anti-malware and anti-spam defenses are a critical part of any modern messaging system. Office 365 provides highly effective tools for minimizing the amount of unwanted messages that reach user mailboxes, while providing strong defenses against malicious software. In this lesson, you will review the anti-malware and anti-spam protection that Office 365 provides and learn how to configure administrative policies and settings to provide protection for your users.

Office 365 provides the following defenses against malware and spam:

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

These five features all connect to the multi-engine online virus scanning service in Exchange Online Protection (EOP), coupled with multiple anti-spam technologies. Exchange Online uses Spam confidence levels to classify and manage the response to spam messages.

This lesson concentrates on Office 365's anti-spam and anti-malware features. In the lab, you will configure those features and use test files to trigger the defenses.

Lesson Objectives

After completing this lesson, you should be able to:

- Configure malware filters.
- Explain message headers and spam confidence levels in Exchange Online.
- Customize the connection filter.
- Configure content filters.
- Customize outbound spam settings.
- Manage spam quarantine.
- Configure transport rules.

Configuring Malware Filters

Exchange Online uses the malware protection EOP to protect user mailboxes against infected messages. EOP uses multiple industry-leading malware detection engines to scan incoming and outgoing mail, with these engines being updated as new virus definitions appear.

In the EAC, you configure protection against malware in Office 365 by a malware filter. A malware filter is a combination of two elements:

- A malware policy that defines what happens when malware is detected.
- A malware rule that defines who the policy applies to.

- Malware protection is provided by Exchange Online Protection
- Malware filters control what happens when malware is detected
- Malware filters consist of a malware policy and a malware rule
 - In EAC, you configure the policy and rule together
 - In PowerShell, you configure the policy first and then apply policy with a rule
- The default filter applies to everyone and just deletes the message with no notifications

You configure malware filters through the protection settings in Exchange Online. You can also configure rules and policies separately by using PowerShell.

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

To configure a new malware detection rule and policy, perform the following procedure:

1. Log on to Office 365 as a Global Admin, click **Admin**, then click **Exchange**, and in the left-hand pane, click **Protection**.
2. Under **Malware filter**, click the + (new) icon.
3. In the **Name** field, enter a distinctive name for the new policy.
4. Under Malware detection response, select one of the following options:
 - a. **Delete the entire message** (which does not send any notification).
 - b. **Delete all attachments and use default alert text**.
 - c. **Delete all attachments and use custom alert text**. If you select this option, you can specify the alert text to be sent in response to a malware detection in the **Custom alert text** box.
5. Under Notifications, you can select the following options:
 - a. **Notify internal senders** (notifies users within the organization that their message had a virus).
 - b. **Notify external senders** (notifies users outside the organization that their message had a virus).
6. Under Administrator Notifications, check the options to have the administrator notified of infected messages:
 - a. Select **Notify administrator about undelivered messages from internal senders** and enter the email address of the administrator (this email could be that of a managing partner).
 - b. Select **Notify administrator about undelivered messages from external senders** and enter the email address of the administrator (this can be different to the previous email address).
7. Under **Customize Notifications**, select the option for Use customized notification text, enter a **From** name, **Address**, message **Subject** and content of the **Message** in the relevant fields. Note that you

can set up different notifications in reply to infected messages from internal users, compared to those from external users.

8. Under **Applied To**, you can now specify to whom this policy applies. Options that you can select are:
 - a. The recipient is <select name or names>
 - b. The recipient domain is <enter a registered Office 365 domain>
 - c. The recipient is a member of <select group>



Note: Under the **Applied to** option, you can combine criteria and also set up exclusions, such as selecting everyone from a group and then excluding one person from that group.

9. Click **Save** to store the new policy.

Policies are applied in order from the highest priority down to the lowest. When you have saved the new policy and any additional policies, you can change each policy's priority, which controls the order in which the policy is applied. The default policy is always the lowest priority and provides a final backstop that simply deletes the offending messages.



Note: You cannot disable the default malware filter.



For more information on configuring malware filters, see the following link:

<http://go.microsoft.com/fwlink/?LinkId=391773>

To configure a malware policy with PowerShell, use the **New-MalwareFilterPolicy** command. To configure a malware rule that applies a policy to users, groups, or domains, use the **New-MalwareFilterRule** command.

For example, to create a rule that:

- Blocks messages with malware.
- Does not notify the sender.
- Notifies the administrator at Contoso.

You would enter the following command:

```
New-MalwareFilterPolicy -Name "Contoso Malware Filter Policy" -  
EnableInternalSenderAdminNotifications $true -InternalSenderAdminAddress  
admin@contoso.com
```

To apply that rule to all recipients in the Contoso domain, enter the following command:

```
New-MalwareFilterPolicy -Name "Contoso Malware Filter Policy" -  
EnableInternalSenderAdminNotifications $true -InternalSenderAdminAddress  
admin@contoso.com
```

Message Headers and Spam Confidence Levels

Exchange Online uses a number of anti-spam technologies to minimize incoming spam messages. The primary anti-spam features include anti-spam message headers and spam confidence levels.

Anti-Spam Message Headers

When Microsoft Exchange Online Protection scans an incoming message, it inserts an X-Forefront-Antispam-Report header (X-header) into the message. Fields in this header enable you to gather information about the message and how it was processed.

- Anti-Spam message headers
 - Inserts header into message
 - Includes information about message and how it was processed
- Spam Confidence Levels
 - Rates the likelihood that a message is spam
 - Exchange online uses following levels:
 - -1 – Safe sender, recipient or domain
 - 0, 1 – scanned and found safe
 - 5 – Probable spam
 - 9 – High confidence spam
 - Actions depend on SCL rating



Best Practice: Use the Message Header Analyzer in Microsoft Remote Connectivity Analyzer to view the headers in the message.

The message fields are as follows:

- **CTRY.** The country from which the message connected to the service. This is determined by the connecting IP address, which may not be the same as the originating sending IP address.
- **LANG.** The language in which the message was written, as specified by the country code (for example, ru_RU for Russian).
- **SCL.** The Spam Confidence Level (SCL) value of the message.
- **SRV:BULK.** The message was identified as a bulk email message. If the Block all bulk email messages advanced spam filtering option is enabled, it will be marked as spam. If it is not enabled, it will only be marked as spam if the rest of the filtering rules determine that the message is spam.
- **SFE.** Filtering was skipped and the message was let through because it originated from a safe sender. For more information about safe senders, see Safe Sender and Blocked Sender Lists FAQ.
- **BLK.** Filtering was skipped and the message was blocked because it originated from a blocked sender.
- **SPM.** The message was marked as spam by the content filter.
- **SKS.** The message was marked as spam prior to being processed by the content filter. This includes messages where the message matched a Transport rule to automatically mark it as spam and bypass all additional filtering.
- **NSPM.** The message was marked as non-spam and was sent to the intended recipients.

Spam Confidence Levels

As incoming messages go through spam filtering, they are assigned a spam score. This score maps to an SCL, as recorded in the X-header.

SCL Rating	Interpretation	Default Action
-1	Message comes from safe sender, safe recipient or safe IP address	Deliver to Inbox
0, 1	Message scanned and found to be clean	Deliver to Inbox

SCL Rating	Interpretation	Default Action
5, 6	Spam	Send to Junk Email
9	High confidence spam	Send to Junk Email

Exchange Online Protection does not use SCL levels 2, 3, 4, 7, and 8.

You can use content filtering policies to specify what happens with high confidence spam; for example, deleting the message and not sending it to junk mail. You can also set SCL conditions in transport rules.

Customizing the Connection Filter

Exchange Online provides a connection filter that enables you to configure filtering based on IP addresses, with separate allow and block lists. Unlike malware filters, there is only one default connection filter, but you can customize the settings.

Allow lists are typically addresses or ranges that you trust, whereas block lists are for addresses or even subnets of known spammers from which you do not want to receive messages. You also have the option to enable a safe list. This option enables acceptance of messages that are from known senders. Microsoft uses third-party sources to supply the list of safe senders.

Settings that you can change are:

- Allowed IP addresses
- Blocked IP addresses
- Enable safe list

With both allow and block lists, you can specify individual addresses or network ranges using Classless Inter-Domain Routing (CIDR).

Typically, the allow setting overrides the block setting. So if you add an address to both lists, mail is allowed from that IP address.

To configure the connection filter, perform the following steps:

1. In EAC, click **Protection** and then click **Connection filter**.
2. Double-click the Default filter. Note that you cannot add any more filters.
3. Under **IP allow list**, click the + (add) button.
4. In the **Add allowed IP address** page, type in the IP address or range that you want to allow, then click **OK**.
5. Under **IP deny list**, click the + (add) button.
6. In the **Add blocked IP address** page, type in the IP address or range that you want to deny, then click **OK**.
7. If required, check the **Enable safe list** option, then click **Save**.

- Connection filters enable setting up of allow and block lists for spam based on IP addresses and ranges
- Allow lists and block lists accept CIDR ranges
- CIDR ranges outside /32 to /24 require setting up of Exchange transport rule
- Addresses in both allow and block lists are allowed



Note: Transport rules in Exchange Online provide additional granularity for configuring domain and sender safe and block lists. If you use a CIDR that is outside the range of /32 to /24, you also need to configure an Exchange Transport rule.

Configuring Content Filters

Content Filters are the main component of your armory against the raging tide of spam that threatens to engulf your organization with invitations to assist with repatriating large amounts of money using your bank account. Content filters provide a range of basic and advanced filtering options and automatically add spam processing headers and assign a spam confidence level to the messages before delivery to user mailboxes.

Configuration settings for spam content filters fall into the following categories:

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

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

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

This policy applies to all messages and all mailboxes. You can then add additional content filters that apply different settings to separate groups and prioritize the application order of those policies.



Note: In **Advanced options**, you can set **On**, **Off**, or **Test**. If you select **Test**, then **Test Mode Options** specifies what happens when a message matches the spam rule settings.

To create a new content filter, perform the following procedure:

1. In EAC, navigate to protection and click content filter.
2. Click the + (new) icon.
3. Specify a policy **Name** and optional **Description**. You can use the description field to summarize the settings to assist other administrators.
4. Under **Actions**, set what you want to happen to spam and high confidence spam. Depending on which option you set, you may have to configure additional fields. Options are:
 - **Move message to Junk Email folder (default).**

- Options are:
 - General (name, description)
 - Actions
 - International spam
 - Advanced options
 - Applied to
- Default content filter has the following settings:
 - Spam: move message to Junk Email folder
 - High confidence spam: move message to Junk Email folder
 - International spam: no settings configured
 - Advanced options: all off except for Block all bulk email messages
- Create additional content filters and prioritize them to match your planning requirements

- **Add X-header** (and set the X-header text).
 - **Prepend subject line with text** (and add the prepended subject line text).
 - **Redirect message to email address** (and add the redirect email address).
 - **Delete message.**
 - **Quarantine message** (and set the number of days that you want to keep quarantined messages for up to the maximum of 15).
5. Under international spam, you can filter for messages in specific languages and from individual countries. Check the boxes for **Filter email messages written in the following languages** or **Filter email messages sent from the following countries or regions**, then under each option, click the + icon. Click the language or country to filter, click **Add**, and then click **OK**.
6. In **Advanced options** in the **Increase Spam Score** section, select which of the following message characteristics you want to indicate that a message is more likely to be junk:
- **Image links to remote sites:** any message with image links to remote websites will receive an increased spam score.
 - **Numeric IP address in URL:** any message that has numeric-based URLs (most often in the form of an IP address) will receive an increased spam score.
 - **URL redirect to other port:** any message that contains a hyperlink that redirects the user to ports other than port 80 (regular HTTP protocol port), 8080 (HTTP alternate port), or 443 (HTTPS port) will receive an increased spam score.
 - **URL to .biz or .info websites:** When this setting is enabled, any message that contains a .biz or .info extension in the body of a message will receive an increased spam score.
7. In the mark as spam section, set the following options to match your spam policy planning:
- **Empty messages:** any message in which the body and subject line are both empty, and which also has no attachment, will be marked as spam.
 - **JavaScript or VBScript in HTML:** any message that uses JavaScript or Visual Basic Script Edition in HTML will be marked as spam.
 - **Frame or IFrame tags in HTML:** any message that contains the "Frame" or "IFrame" HTML tag will be marked as spam. These tags are used on websites or in HTML messages to format the page for displaying text or graphics.
 - **Object tags in HTML:** any message that contains the "Object" HTML tag will be marked as spam. This HTML tag allows plug-ins or applications to run in an HTML window.
 - **Embed tags in HTML:** any message that contains the "Embed" HTML tag will be marked as spam. This HTML tag allows varying data types to be embedded into an HTML document. Examples include sounds, movies, or pictures.
 - **Form tags in HTML:** any message that contains the "Form" HTML tag will be marked as spam. This HTML tag is used to create website forms. Email advertisements often include this tag to solicit information from the recipient.
 - **Web bugs in HTML:** any message that contains a Web bug will be marked as spam. A Web bug is a graphic designed to determine whether a Web page or email message has been read.
 - **Apply sensitive word list:** any message that contains a word that's included in the sensitive word list will be marked as spam.
 - **SPF record: hard fail:** messages that hard fail an SPF check will be marked as spam (SPF filtering is always performed). Turning this setting on is recommended for organizations who are

- concerned about receiving phishing messages. (In order to avoid false positives for messages sent from your company, make sure that the SPF record is correctly configured for your domains.)
- **Conditional Sender ID filtering: hard fail:** any message that hard fails a conditional Sender ID check is marked as spam. Turning this setting on is recommended for organizations who are concerned about phishing, especially if their own users are being spoofed. This option combines an SPF check with a Sender ID check to help protect against message headers that contain forged senders.
 - **NDR backscatter:** any message that matches the non-delivery report (NDR) bounce characteristics will be marked as spam. It is not necessary to enable this setting if your organization uses Exchange Online Protection to send outbound mail.
 - **Block all bulk email messages:** any message that is identified as bulk mail, such as advertisements and marketing emails, will be marked as spam.
8. In **Test Mode Options**, you can configure what happens when a match is made to a test-enabled advanced option above. Select one of the following choices:
- **None:** The message is marked as spam but nothing else happens.
 - **Add the default test X-header text:** Select this check box to insert the following text as part of the incoming message header: **X-CustomSpam: This message was filtered by the custom spam filter option.**
 - **Send a Bcc message to this address:** Specify an email address or addresses to send copies of the messages that are filtered in test mode. Separate multiple addresses with a semicolon.
9. Under **Applied To**, select conditions such as the recipient is, the recipient is a member of a group, or the recipient is a member of a domain as discussed in the earlier topic on Configuring Malware.
10. Click **Save**.

When you have created all your content filtering rules, you can change their priority levels and edit them in EAC.

Customizing Outbound Spam Settings

Outbound spam control in Office 365 is at the organization level, similar to connection filters. As a result, there is only one default outbound spam preference entry; this filter applies to all mailboxes.

This filter has the following two settings:

- **Send a copy of all suspicious outbound email messages to the following email address or addresses.** This option enables you to specify the email address or addresses of administrators who will receive copies of all suspicious outbound messages. If sending to multiple addresses, separate the addresses with a semicolon.
- **Send a notification to the following email address or addresses when a sender is blocked for sending outbound spam.** This option enables you to specify the administrator email address or addresses to notify when outbound messages identified as spam are blocked. Again, use a semicolon to separate multiple addresses.

- Organization-level filter acts on all outgoing messages
- No further filters can be added
- Cannot be disabled
- Can be customized:
 - Send a copy of all suspicious outbound email messages to the following email address or addresses
 - Send a notification to the following email address or addresses when a sender is blocked for sending outbound spam

Managing Spam Quarantine

If you set your content policy to direct spam messages into quarantine and your organization then receives a message that is classified as spam, that message will end up in the quarantine area. Messages from transport rule matches can also end up in quarantine.

You can then inspect the messages before choosing to release them on to their original addressees or mark them as false positives and release to the addressees. Alternatively, you can simply leave the messages in quarantine until they expire.

With either option, you can release the message to all recipients or just too selected recipients. However, if you release the message just to one recipient and then subsequently release it to all recipients, the first will not receive the message a second time.

By default, quarantined messages are listed from newest to oldest, based on the value in the **RECEIVED** field. **SENDER**, **SUBJECT**, and **EXPIRES** values are also shown for each message.

To assist with managing quarantined messages, there is also an advanced search function that enables you to filter, based on the following criteria:

- Message ID
- Sender email address
- Recipient email address
- Received (by day)
- Expires (by day)
- Message type (spam or content rule filtering)



Note: A maximum of 500 messages can be displayed in the quarantine interface.

To manage messages in the quarantine area, perform the following process:

1. In EAC, click **Protection** and then click **Quarantine**.
2. Review the messages currently in quarantine.
3. To search for a message, click the **Advanced search** icon.
4. In **Advanced search**, select the search criteria and add any additional information about the selected criteria in the relevant box.
5. Click **OK**.
6. Double-click a message that you want to release.
7. If you want to release the message but not report it as a false positive, click **Release to**.
 - a. In the release message dialog box, either select **Release message to all recipients** or **Release message to specified recipients**.

- Quarantine holds messages picked up by content filters or transport rules
- Messages remain in quarantine for up to 15 days
- Advanced filtering enables sorting on:
 - Message ID
 - Sender email address
 - Recipient email address
 - Received (by day)
 - Expires (by day)
 - Message type (spam or content rule filtering)
- Messages can be released to recipients
- Messages can be marked as false positives to Microsoft

- b. If you select **Release message to specified recipients**, then click the names of the recipients and click **Add**.
 - c. Click **Release**.
8. If you want to release the message and report that it was not spam, click **Release message and report it as a false positive**.
 9. In the **Report false positive** page, click **Report false positive**.

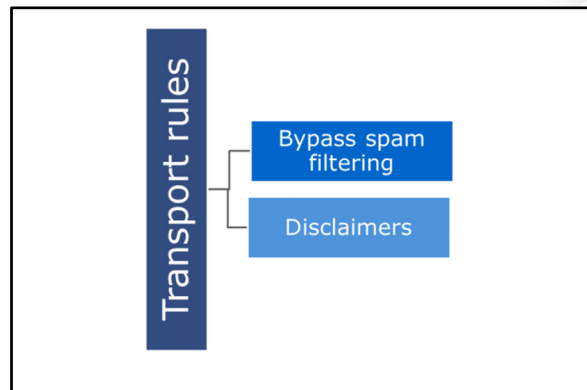


Note: False positive reports will not be processed if the message was quarantined because of an advanced spam filter option, or if it was quarantined due to a transport rule match.

Configuring Transport Rules

Transport rules are another mechanism that can be used to improve defenses against spam and to carry out other functions. Specifically, transport rules can:

- Prevent inappropriate content from entering or leaving the organization.
- Filter confidential organization information.
- Track or archive copying messages that are sent to or received from specific individuals.
- Redirect inbound and outbound messages for inspection prior to delivery.
- Append disclaimers to messages as they pass through the organization.



Each transport rule consists of:

- *Conditions*. Message characteristics to which you can apply a transport rule action.
- *Exceptions*. Further conditions that can exclude messages from the transport rule action.
- *Actions*. Apply to messages that match the conditions and exceptions.

This topic specifically concentrates on two applications of transport rules: Bypass spam filtering and Add disclaimers.

Bypass Spam Filtering

Bypass spam filtering enables you to allow list domains and ensure that messages from those domains are always accepted. However, you should be aware that SMTP address spoofing can lead to messages being accepted that do not originate from the specified domain.

To bypass spam filtering and allow list a domain, carry out the following procedure:

1. In EAC, click **Mail flow**.
2. In **Mail flow**, under **Rules**, click the + sign and click **Bypass spam filtering**.
3. In the **Name** field, enter a descriptive name, such as "Allow list all partner domains".
4. Under **Apply this rule if**, drop down the box, then **The sender**, then click **Domain is**.
5. In the **Specify domain** box, enter the domains that you want to allow list and click the + sign.

6. Click **OK** when you have finished adding domains.
7. Under **Do the following**, the action should already be set to **Set the spam confidence level (SCL) to** and the value set to **Bypass spam filtering**.
8. Under **Except if**, click add exception and include any of the options for excluding people within those domains.
9. Select the option for **Audit this rule** and select an auditing level if you want to have the bypass spam filtering action audited.
10. Under **Choose a mode for this rule**, ensure that **Enforce** is selected, unless you only want to test the effect, in which case select **Test without Policy Tips**.
11. Under **Match sender address in message**, ensure that **Header** is selected, then click **Save**.

All the domains that you specified are now allow listed and messages sent from those domains will go directly to the recipients without having spam filtering applied.

Add Disclaimers

Disclaimers provide a mechanism for organizations to attach standard text to the bottom of an email, such as explaining what to do if the recipient is sent the message in error or disclaiming responsibility for any actions the recipient may carry out as a result of the contents of the email. Typically, legal disclaimers try to address five main areas:

- *Breach of confidentiality, whether accidental or deliberate.* For example, do not forward this message to people outside the company.
- *Transmission of viruses.* For example, we cannot guarantee this message is virus-free.
- *Entering into contracts.* For example, this email does not form a contract.
- *Negligent misstatement.* For example, this email does not consist of advice and should not be used as such.
- *Employer's liability.* For example, do not send offensive emails and company email systems are subject to monitoring.

The main problem with disclaimers are that courts may take a very different view of the legal position of the content of the message as compared to the information set out in the disclaimer. However, they can indicate that the sender's organization has attempted to prevent, for example, a virus outbreak at a client site by warning the recipient to have the incoming email scanned.

Disclaimers can also be added for marketing reasons, although these are more like footnotes or email signatures.

Setting up disclaimers is similar to bypass spam filtering:

1. In EAC, click **Mail flow**.
2. In **Mail flow**, under **Rules**, click the + sign and click **Apply disclaimers**.
3. In the **Name** field, enter a descriptive name, such as "Corporate Disclaimer".
4. Under **Apply this rule if**, drop down the box, then click **The recipient is located**.
5. In the **Select recipient location** box, click **Outside the organization**.
6. Under **Do the following**, the action should already be set to **Append the disclaimer**.
7. Click **Enter text**, and in the **Specify disclaimer text** box, enter the text of the disclaimer, then click **OK**.

8. After **Fall back to action**, click **Select one**, then in the **Specify fallback action** box, select **Wrap**, **Ignore**, or **Reject**.
9. Under **Except if**, click **Add exception** and include any of the options for excluding senders, recipients, or messages.
10. Select the option for **Audit this rule** and select an auditing level if you want to have the bypass spam filtering action audited.
11. Under **Choose a mode for this rule**, ensure that **Enforce** is selected, unless you only want to test the effect, in which case select **Test without Policy Tips**.
12. Click **More options** to specify additional information, such as times when this rule will be activated or deactivated, then click **Save**.

Lesson 3

Configure Additional Email Addresses for Users

Configuring additional email addresses in Exchange Online is a somewhat different process than with on-premises versions of Exchange Server. The key difference is that Exchange Online does not provide an email policy, like Exchange Server. As a result, you have to use alternative approaches for configuring these additional email addresses.

In this lesson, you will examine how to create these additional email addresses, including using tools such as the EAC, PowerShell, and ADSI Edit.

Lesson Objectives

After completing this lesson, you should be able to:


- Explain the process for assigning email addresses in Office 365.
- Configure additional email addresses with EAC and PowerShell.
- Describe SIP addressing issues with Lync Online.
- Manage email addresses with Directory Synchronization.

Email Address Assignment in Exchange Online

When you create a new tenant account in Office 365, you are automatically issued with a default domain name in the form *companyname.onmicrosoft.com*. The administrator account logon details are set to *administratorname@companyname.onmicrosoft.com*, as is the primary email address for the account.

When you add a new user account to a simple Office 365 account (that is, one that does not have any external domains configured), then the mailbox for that user is automatically assigned an SMTP email address that uses this default domain. This email address is of the form *SMTP:username@domainname*. Lync Online also generates a Session Initiation Protocol (SIP) address in the same form.

For example, assume the default domain is *lucernepublishing.onmicrosoft.com*, in which case the default email address policy will assign user Remi Desforges an email address with a *@lucernepublishing.onmicrosoft.com* address, such as *rdesforges@lucernepublishing.onmicrosoft.com*. Typically, this email address will match his user logon to Office 365.

 **Note:** The primary (or reply-to) SMTP address for a mailbox always has the acronym **SMTP:** in capitals. Secondary and subsequent addresses have **smtp** in lower case. For example: *SMTP:user@domain.microsoftonline.com* – this is the PRIMARY address. *smtp:user@domain.com* – this is the SECONDARY address.

If you then register an external domain with Office 365, you can create email addresses that use that domain. New users will get a primary address of *@companyname.onmicrosoft.com* and a secondary email

- Office 365 does not use email policies like Exchange on-premises
- Default email addresses for new Office 365 account are *@companyname.onmicrosoft.com*
- Additional domains can be registered, allowing you to create email addresses for those domains
- Email addresses can be created or marked as primary (reply-to) in EAC or with PowerShell

address of @externaldomain. You can then allocate the second address at the primary or reply-to address for a user, either manually through EAC or in bulk by using PowerShell. The primary address is always shown in bold in the EAC user interface.

Similarly, you can add further email addresses, but only where the email domain matches the DNS domains registered with Office 365. For example, take the Lucerne Publishing illustration above. In addition to the default lucernepublishing.onmicrosoft.com domain, the tenant administrator has registered the following external DNS domains:

- Lucernepublishing.com
- Lucernepublishing.org
- Content.lucernepublishing.com

Remi Desforges can therefore have the following email addresses:

- SMTP:rdesforges@lucernepublishing.onmicrosoft.com (primary)
- smtp:rdesforges@lucernepublishing.com (secondary)
- smtp:remidesforges@lucernepublishing.com
- smtp:remid@content.lucernepublishing.com

In this case, the administrator will probably want to set the @lucernepublishing.com address to primary.



Note: You will receive an error message if you attempt to add an email address for an unregistered domain.

In a cloud-only environment, you manage email addresses through EAC or PowerShell. However, if you are using DirSync to synchronize your on-premises environment with Office 365 or you are using hybrid Exchange, then you manage email addresses on-premises.

Configuring Additional Email Addresses

To configure additional email addresses, perform the following procedure:

1. In EAC, click **Recipients**.
2. Under **Mailbox**, click the mailbox you want to change and click the edit symbol.
3. In the user's page, click **Email address**.
4. Under **Email address**, click the + sign.
5. Under email address type, ensure **SMTP** is selected and then in **Email address**, enter the address using a registered domain name.
6. Optionally, click the **Make this the reply address** to make this address the primary.
7. Click **OK**.

Messages now sent to this new address will be delivered to this mailbox. If you selected **Make this the primary address**, then this is the address that reply messages are sent to.

- Configure additional email addresses individually through EAC or in bulk using PowerShell

- PowerShell command must evaluate all users and then change the email address. For example:

```
$users = Get-Mailbox
foreach ($a in $users)
{$a.emailaddresses.Add("smtp:$($a.alias@thenewdomainname")}
$users | %{$Set-Mailbox $_.Identity -EmailAddresses
$_EmailAddresses}
```

- Must connect to Exchange Online Service first

To configure additional proxy addresses with PowerShell in the form `alias@content.lucernepublishing.com`, connect to Exchange Online and use the following commands. To perform this update, you have to list all the mailboxes into a variable and then run the command on each of the items in the variable:

```
$users = Get-Mailbox
```

```
foreach ($a in $users) {$a.emailaddresses.Add("smtp:$(($a.alias)@thenewdomainname")}
```

```
$users | %{Set-Mailbox $_.Identity -EmailAddresses $_.EmailAddresses}
```

An alternate approach is to use a comma-separated variable (CSV) file. The CSV file should contain two columns, one for Mailbox, the other for NewEmailAddress. You then run the following command:

```
Import-CSV "C:\Users\Administrator\Desktop\AddEmailAddress.csv" | ForEach {Set-Mailbox $_.Mailbox -EmailAddresses @{add=$_.NewEmailAddress}}
```



Note: You must connect to the Exchange Online service before running these commands.

SIP Addressing

Office 365 not only generates an SMTP address for each user, it also generates a SIP address for use with Lync Online. This sign-in address is kept automatically synchronized with the user's logon identity in Office 365.

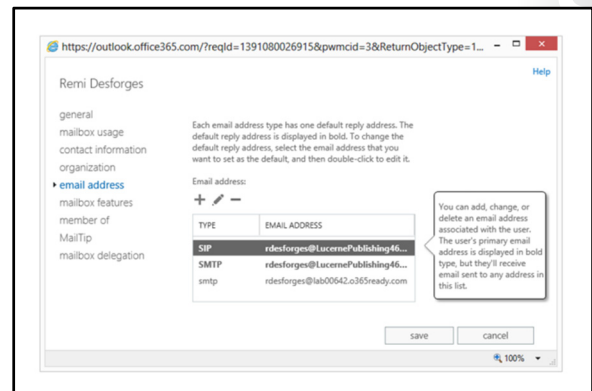
As a result, when you change the sign-in address for a user – for example, from `user@lucernepublishing.onmicrosoft.com` to `user@lucernepublishing.com` – Office 365 generates a new SIP address for the user. This change requires the user to carry out the following actions:

- *Reschedule any future and recurring Lync Online meetings.* If the name part of the address has changed (that is, from `rdesforges@domainname` to `remi.desforges@domainname`, then the user has to update his or her Lync Online meetings by resending the invitation. This requirement is because the Lync meeting link changes. If users do not update their meetings, then users joining the meeting will see an error message.
- *Communicate changes to external contacts in Lync Online contact lists.* External contacts, such as other federated Lync organizations, Windows Live users, and MSN users must be notified about the change to the user's SIP address. If external contacts do not make this change, the contact card for the affected user will simply remain as either **Presence Unknown** or **Offline**.

Some organizations may want to use separate sign-on and SIP addresses, which is a supported configuration. However, you should be aware that this arrangement is potentially confusing for users, as they may have to log on to the Lync client with different user names and SIP addresses.

User Lync settings can be configured by modifying the Office Communicator registry settings in **HKEY_CURRENT_USER\Software\Microsoft\Shared\UcClient** as follows:

- Set **ServerSipUri** to a string value of the user's SIP proxy address
- Set **ConfigurationMode** to a dword value of 0



- Delete the **ServerAddressInternal** string
- Delete the **ServerAddressExternal** string
- Delete the **ServerUserName** string

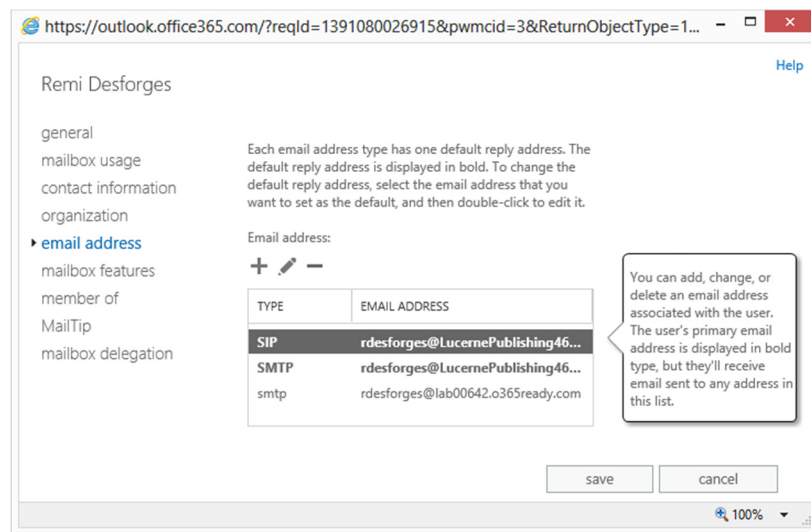
If your organization is using Directory Synchronization (DirSync) or is configuring Lync Online in a hybrid environment, then you can update the SIP address independently by changing the **msRTCSIP-PrimaryUserAddress** value by using ADSIEdit.



The following link deals with issues of possible duplication of SIP addresses:

<http://go.microsoft.com/fwlink/?LinkId=391774>

The interface for configuring SIP addresses is part of Exchange Online. Here is an example of user Remi Desforges, who has a primary SMTP account matching his SIP address of `rdesforges@lucernepublishing460.onmicrosoft.com`.



Managing Email Addresses with DirSync

When you have configured DirSync to synchronize on-premises Active Directory accounts with Office 365, then there is a flow of information from Active Directory to Office 365. This information includes fields such as SMTP addresses and UPNs.

It is important to note that there must be a match between the UPNs and the verified domain names in Office 365. For the sake of this discussion, let us assume that you are trying to synchronize the LUCERNE on-premises domain with Office 365. In this scenario, the best approach is to have a UPN suffix of `lucernepublishing.com` set up in Active Directory Domains and Trusts, and ensure that all users have that UPN suffix applied. The users then have primary on-premises SMTP addresses that match their UPNs. In Office 365, you register the `lucernepublishing.com` domain to Office 365 and set it up for use with Exchange Online.

- With DirSync, email addresses in Office 365 can be populated using attributes in Active Directory
- DirSync synchronization then pushes these addresses to Office 365 mailboxes
- Proxy email addresses can be edited in ADSI Edit or Active Directory Users and Computers
- Primary email addresses start with **SMTP:**
- Secondary email addresses start with **smtp:**
- You can still add email addresses to Exchange Online for registered domains through EAC or PowerShell

When you run the first DirSync synchronization, Office 365 creates the mailboxes in Office 365 and assigns a primary SMTP address of user@lucernepublishing.com. It will also create a secondary address of user@lucernepublishing.onmicrosoft.com. Users can now log on to Office 365 and access their mailboxes.


If you then set up either password synchronization with Dirsync or implement SSO, typically using Active Directory Federation Services (AD FS), then users can log on to Office 365 using the same credentials that they use for on-premises logins. In the case of password sync, there are still two separate accounts, one online and one in the cloud, but they have the same user name (user@lucernepublishing.com) and the password is synchronized between the two environments.

With SSO, there is a federation trust relationship between Office 365 and the on-premises AD FS, so the user logs on as user@lucernepublishing.com and that logon request is redirected to AD FS. AD FS constructs a token and passes that token to Office 365. Office 365 then grants the user access to his or her mailbox based on the fact that they were successfully authenticated by the on-premises Active Directory Directory Service.

In the case of DirSync, Dirsync with password Sync, or AD FS (which is implemented with DirSync), there are additional ways to create email addresses and have those addresses replicate into Office 365. To perform this procedure, complete the following steps:

1. In the on-premises environment, log onto a Domain Controller, then in **Server Manager**, click **Tools** and click **ADSI Edit**.
2. In ADSI Edit, connect to your default naming context.
3. Browse down the tree to the OU in which you want to make the change.
4. Right-click the user account that you want to change, and select **Properties**.
5. In the Properties dialog box, scroll down until you get to the **ProxyAddresses** value. Click the **Edit** button.
6. In **Value to add**, enter an SMTP address for a domain that is registered with Office 365 (otherwise Office 365 won't display it) in the form SMTP:username@domain or smtp:username@domain.
7. The entry SMTP:username@domain will be the primary address, so there should only be one entry of that type. All other entries are secondary addresses.
8. Click **OK** and click **OK**, then close ADSI edit.
9. Either wait for the next synchronization cycle or run the **Start-OnlineCoexistenceSync** command.
10. The new addresses should appear as mailbox attributes in Office 365.

You can also carry out the same process in Active Directory Users and Computers by selecting **Advanced Features** from the **View** menu and then using the **Attribute** tab.

 **Note:** If you do not have an SMTP (upper case) entry in the on-premises directory service for a user, then the username@domain.onmicrosoft.com address will be marked as primary. Having the mail or user principal name attributes set in ADSI Edit also creates a primary SMTP address that matches that value.

Discussion: How should Lucerne Publishing be managing email addresses?

How should Lucerne Publishing be managing email addresses?

- Which option would provide the best way for Lucerne Publishing to manage additional email addresses:
 - EAC
 - PowerShell
 - DirSync

Lesson 4

Create and Manage External Contacts, Resources, and Groups

Up to this point, we have specifically been working with mailbox-enabled users in Office 365. However, this platform provides a range of other mailbox types that enable organizations to work more effectively and maintain contact details in one place for easy access through Outlook or the Outlook Web App.

These features include:

- Contacts, which can be one of two types:
 - Mail contacts
 - Mail users
- Resources, which can also be of two types:
 - Rooms
 - Equipment
- Shared mailboxes
- Groups for external contacts

Each account type has specific characteristics and requirements.

Lesson Objectives

After completing this lesson, you should be able to:

- Configure mail contacts in Exchange Online.
- Import contacts in bulk.
- Hide external contacts from the address book.
- Configure mail users in Exchange Online.
- Configure shared mailboxes.
- Configure resources mailboxes for rooms and equipment.
- Change mailboxes from one type to another.
- Configure distribution and security groups in Exchange Online.

Configuring Mail Contacts

Mail contacts are the simplest concept to understand. These are just like contacts in Active Directory, and when you create them, they consist of just some name fields, an alias, and an external email address.

Mail contacts do not have a user account in Office 365, and therefore, they cannot log on. However, they do appear in the global address list (GAL) throughout the organization and can be added to mail-enabled security groups, distribution groups or dynamic distribution groups (but not security groups). As a result, you can use contacts as you might use entries in your contacts folder in Outlook, with the difference that Office 365 contacts are managed centrally.

You can also use contacts within your own hierarchy and assign them a manager. This approach is useful if your organization engages outside contractors or associates.

After you have created a contact, you can add some optional fields, such as contact information, phone numbers, notes, title, department, company, manager and direct reports. Finally, you can configure a MailTip that appears when someone sends a message to that person.

To create a contact, perform the following procedure:

1. In Office 365, click **Admin** and then click **Exchange**.
2. In Exchange admin center, click **Recipients** and then click **Contacts**.
3. Click the + (new) icon and click **Mail contact**.
4. In the **New mail contact** page, enter a First name, Initials, and Last name.
5. The **Display name** is autogenerated based on those first three fields in the form of First name, middle initial, Last name, but you can change that format.
6. In **Alias**, enter a unique value.
7. In **External email address**, enter the address to which you want mail for that user to be sent.
8. Click **Save**.



Note: Typically, it can take a minute or two for the item to be updated in Office 365. As a result, you may get an error message stating that the object does not exist the first time you attempt to edit the new contact.

The new mail contact now shows up in the GAL.

When you have created the new mail contact, you can then edit the details to add or change further information in the following tabs:

- *General*. Name fields, alias, and external SMTP address.
- *Contact information*. Add street, Zip/post code, city and so on if required.
- *Organization*. Add manager and department information.

- Mail contacts in Office 365 are the equivalent of contacts in Active Directory
- Mail contacts enable external contact details to be added to the GAL
- Mail contacts can be created through EAC or by using PowerShell
- Mail contacts require an alias and an external email address
- Further fields are available after you have created the contact

- *MailTip*. Create MailTip to provide additional information that users can see when they select this address in an email.

Deleting a contact is as simple as selecting the contact and clicking the Delete icon. You can also export contact information to a CSV file and display additional columns in EAC.

Forwarding an email to an external contact is as simple as forwarding a message to an internal mailbox. You simply click the Forward button and add the contact as a new addressee. However, if a message or attachment has Information Rights Management protection applied, you may not be able to forward the message to an external recipient.

If you are using Directory Synchronization and your Active Directory contacts are appearing in the Exchange Online GAL, then you manage those contacts in Active Directory and let DirSync take care of the synchronization process.

Bulk Importing Contacts

Adding contacts individually is a somewhat laborious process, so if you have a large number of contacts to import, it is best to do this in bulk by using PowerShell. Here, the **Import-CSV file** command comes in handy.

To bulk import contacts, perform the following process:

1. Create a CSV file containing the necessary information.
2. Use PowerShell to create the contacts.
3. Customize the newly created contacts using PowerShell.

- Bulk Import process
 - Create a CSV file containing the necessary information
 - Use PowerShell to create the contacts
 - Customize the newly created contacts using PowerShell
- Import file must provide:
 - FirstName
 - LastName
 - Name
 - ExternalEmailAddress
- Use the Import-CSV command to create contacts with mandatory fields
- Rerun Import-CSV command to populate additional variables

The starting point is the CSV file. The Office 365 community site provides a sample file that can help.

 **The sample CSV file is available from the following link:**

<http://go.microsoft.com/fwlink/?LinkId=391775>

In the CSV file, do not delete any of the header row, but you can delete the sample data. You can then populate the spreadsheet with your own information.

At a minimum, you must provide values for the following fields:

- FirstName
- LastName
- Name
- ExternalEmailAddress

You then connect to Exchange Online using PowerShell and run the following command to create the contacts:

```
Import-Csv .\ExternalContacts.csv|{%{New-MailContact -Name $_.Name -DisplayName $_.Name -ExternalEmailAddress $_.ExternalEmailAddress -FirstName $_.FirstName -LastName $_.LastName}}
```

The contacts will now appear in the GAL.

Finally, you can add further information about each contact by running the **import-CSV** command again. This time, it is a two-stage process.

```
$Contacts = Import-CSV .\externalcontacts.csv
```

This command imports all the entries in the CSV file into a variable called `$Contacts`.

```
$contacts | ForEach {Set-Contact $_.Name -StreetAddress $_.StreetAddress -City $_.City -
StateorProvince $_.StateorProvince -PostalCode $_.PostalCode -Phone $_.Phone -MobilePhone
$_.MobilePhone -Pager $_.Pager -HomePhone $_.HomePhone -Company $_.Company -Title
$_.Title -OtherTelephone $_.OtherTelephone -Department $_.Department -Fax $_.Fax -Initials
$_.Initials -Notes $_.Notes -Office $_.Office -Manager $_.Manager}
```

This second command then replaces each value in the contact record with the new value in the CSV file.



Note: If you are not adding the Manager variable for the contacts, then delete the `$_Office -Manager $_.Manager` element from the command.

Hiding External Contacts

There may be times when you want to hide external contacts from the GAL. For example, you may only want external contacts to be part of distribution groups. The mechanism for hiding external contacts depends on whether they are in the cloud or on-premises contacts that are being synchronized to Exchange Online using DirSync.

To hide a single cloud-based contact, connect to Exchange Online and run the following PowerShell command:

```
Set-MailContact <contact name> -
HiddenFromAddressListsEnabled $true
```

For example, to hide Remi Desforges, enter:

```
Set-MailContact <Remi Desforges> -HiddenFromAddressListsEnabled $true
```

To hide all external contacts at once, run the following command:

```
Get-Contact -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'MailContact')}} | Set-
MailContact -HiddenFromAddressListsEnabled $true
```

If you are using DirSync and your on-premises Active Directory contacts are being synchronized with Office 365, then you may still want to hide those contacts from the GAL. In this case, you set the **msExchHideFromAddressLists** property in the Active Directory schema to True for the account or accounts that you want to hide.

- Hide one contact
 - Set-MailContact <contact name> - HiddenFromAddressListsEnabled \$true
- Hide all contacts
 - Get-Contact -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'MailContact')}} | Set-MailContact - HiddenFromAddressListsEnabled \$true
- Hide with DirSync
 - Change msExchHideFromAddressList to TRUE
- Check if a user is hidden
 - Get-MailUser -Identity <alias> |fl *HiddenFromAddressListsEnabled*



Note: If you do not have Exchange Server installed in your on-premises environment, the **msExchHideFromAddressLists** property will not be present in Active Directory. In that case, you should update the Active Directory schema with the Exchanger Server extensions.

To check from Office 365 that a mailbox has been hidden from the GAL, connect to Exchange Online and run the following command:

Get-MailUser -Identity <alias> |fl *HiddenFromAddressListsEnabled*

Configuring Mail Users

A mail user combines some of the attributes of a full mailbox user along with the characteristics of a contact. Mail users provide a useful “half-way house” that enables administrators to provide logon facilities to Office 365 while continuing to provide an external email address. Organizations that use associates often use mail user accounts to provide logon facilities to these personnel while forwarding their emails to their external email address. The mail user accounts can be assigned to a manager and department for administrative purposes.

- Mail users can log onto Office 365
- Mail users have an external address rather than a mailbox
- Create in EAC or with PowerShell
- Unlike contacts, mail users can be added to shared mailboxes



Note: Mail users are used extensively in hybrid Exchange environments, where users with on-premises mailboxes are made mail users in Office 365, with their email address configured as their on-premises mailbox. These users then show up in the online GAL as contacts.

The characteristics of a mail user include:

- They can log onto Office 365 and access resources such as OneDrive for Business or SharePoint Online.
- They have an email address that is external to Office 365, registered against the **ExternalEmailAddress** attribute.
- They can have a secondary email address for the default companyname.onmicrosoft.com domain.

To create a new mail user, perform the following procedure:

1. In Office 365, click **Admin** and then click **Exchange**.
2. In Exchange admin center, click **Recipients** and then click **Contacts**.
3. Click the + (new) icon and click **Mail user**.
4. In the **New mail user** page, enter a First name, Initials, and Last name.
5. The **Display name** is autogenerated based on those first three fields in the form of First name, middle initial, Last name, but you can change that format.
6. In **Alias**, enter a unique value.
7. In **External email address**, enter the address to which you want mail for that user to be sent.

8. In **User ID**, enter the logon information for that user and from the drop-down box, select his or her domain from the list of registered domains.
9. In **New password** and **Confirm password**, enter the user's logon password.
10. Click **Save**.

When you have created the new mail user, you can then edit the details to add or change further information in the following tabs:

- *General*. Hide from the address list, add custom attributes.
- *Contact information*. Add street, Zip/post code, city and so on if required.
- *Organization*. Add manager and department information.
- *Email address*. Add further email addresses if required.
- *Mail flow settings*. Restrict who can and can't send email to this account.
- *Member of*. Add to distribution groups.
- *MailTip*. Create MailTip to provide additional information that users can see when they select this address in an email.

To use PowerShell to create a new mail user, run the following command:

```
New-MailUser -Name <name> -WindowsLiveID <Microsoft ID> -Password (ConvertTo-SecureString -String '<password>' -AsPlainText -Force)
```

You can then use the **Set-MailUser** command to change attributes, such as this example that changes the external email address:

```
Set-MailUser johnsmith -ExternalEmailAddress johnsmith@contoso.com
```

Configuring Shared Mailboxes

Shared mailboxes are special types of mailboxes that multiple different users can access in order to send and receive email messages. Shared mailboxes can also be used for setting up shared calendars to enable employees to schedule vacation time or plan shifts.

Shared mailboxes provide:

- A generic email address, such as `marketing@lucernepublishing.com` or `sales@lucernepublishing.com` to field customer enquiries.
- A way for departments that provide centralized services to respond to requests from employees or customers, like the helpdesk, HR, or printing.
- Support for multiple users to monitor and reply to external or internal email addresses.

When a user replies to a message sent to a shared mailbox, the reply appears to come from the shared mailbox address. Also, all users who have access to that shared mailbox can see the messages that have been sent to that account.

- Shared mailboxes provide generic email addresses that multiple user accounts can access
- Can have three permission levels:
 - Full Access: can act as mailbox owner
 - Send As: can send mail as if from the mailbox
 - Send on Behalf Of: can send mail on behalf of the mailbox
- Mailbox users and mail users can access shared mailboxes, not contacts
- Automapping feature automatically opens all Full Access mailboxes but can be disabled

Shared mailboxes can have the following delegate permissions:

- *Full Access*. Users with full access permission can log on and carry out actions consistent with a mailbox owner. However, to send mail, users with Full Access permission must also have Send As or Send on Behalf of permission. You can configure Full Access permission through EAC or through PowerShell.
- *Send As*. Users with Send As permission can impersonate the mailbox when sending mail. Messages received are “from” the mailbox, so appear to come directly from, say, marketing@lucernepublishing.com. You can configure Send As permission through EAC or through PowerShell.
- *Send on Behalf of*. Send on Behalf of permission grants the right to send messages, but those messages are stamped as from “Remi Desforges on behalf of Marketing”. Send on Behalf of permission is only configurable through PowerShell.



Note: Typically, you use shared mailboxes with security groups, creating a security group, adding users to that group then granting the security group Full Access and Send As control on the mail. To change access rights, you then simply add or remove users from the security group.

Shared mailboxes do not on their own require user licenses, so you can grant both mailbox users and mail users Send-As and Full Access permission. However, you should be aware that with mail users, you could potentially be granting someone outside the organization the right to send mail on behalf of the organization.

To use a shared mailbox with in-place archive, you have to assign an Exchange Online Plan 1 or Plan 2 license. The mailbox size will then increase to 50 GB. To put a shared mailbox on in-place hold requires you to assign an Exchange Online Plan 2 license.

Shared mailboxes have lower storage limits of 10 GB (up from 5 GB). This compares to 50 GB (up from 25 GB) for a user mailbox and 2 GB (up from 1 GB) for a kiosk user.

To create a shared mailbox in EAC, perform the following procedure:

1. In EAC, click **Recipients**, and then click **Shared**.
2. Under shared, click the + (add) icon.
3. In the **Display Name** field, enter the name for the mailbox that you want recipients to see. For example, “Marketing” if the shared mailbox is to send out mailings from the Marketing Department.
4. Under **Email address**, enter the shared mailbox’s email address and select the domain from the list of registered domain names, for example, marketing@lucernepublishing.com.
5. Under **Send As**, add the names of people that you want to have the right to send mail as marketing@lucernepublishing.com.
6. Click the + button and from the list of names, select the Send As users, click **Add**, then click **Save**.
7. Click **Save** to save the new mailbox.

Users set up with the Send As permission can now enter that address in the **From** field when they send e-mails. The reply comes back to the Marketing mailbox.

When you have created the shared mailbox, you can then edit the details to add or change further information in the following tabs:

- *General*. Hide from the address list, add custom attributes.
- *Mailbox delegation*. Configure Full Access and Send As permissions.

- *Mailbox usage.* View current size of the mailbox.
- *Contact information.* Add street, Zip/post code, city and so on if required.
- *Organization.* Add manager and department information.
- *Email address.* Add further email addresses if required.
- *Mailbox features.* Apply policies, enable and disable protocols, apply litigation hold, set up archiving, control message delivery, and set message sizes.
- *Member of.* Add to distribution groups.
- *MailTip.* Create MailTip to provide additional information that users can see when they select this address in an email.

To create a shared mailbox in Office 365 by using PowerShell, run the **New-Mailbox** command:

New-Mailbox -Name "Corporate Printing Services" -Alias corpprint -Shared

To edit the mailbox, use the **Set-Mailbox** command, just as with a user mailbox.

Set-Mailbox corpprint -ProhibitSendReceiveQuota 5GB -ProhibitSendQuota 4.75GB -IssueWarningQuota 4.5GB

Automapping is an issue with shared mailboxes. Automapping works with Outlook 2007 and 2010 to open any mailboxes to which a user has Full Access permission automatically, along with their main profile account. This approach works fine with one or two mailboxes but can significantly increase startup time for Outlook if the user has ten or more mailboxes to which he or she has Full Access permission.

To fix this issue, remove the Full Access right for that user using the following command:

Remove-MailboxPermission -Identity <Mailbox ID1> -User <Mailbox ID2> -AccessRights FullAccess

You now replace the Full Access rights but include the **-AutoMapping:\$false** setting:

Add-MailboxPermission -Identity <Mailbox ID1> -User <Mailbox ID2> -AccessRights FullAccess -AutoMapping:\$false

The following example shows this command:

Add-MailboxPermission -Identity JeroenC -User 'Mark Steele' -AccessRight FullAccess -InheritanceType All -Automapping \$false


Configuring Resource Mailboxes

Resource mailboxes in Office 365 provide a facility that enables you to assign a mailbox to a room or an item of equipment and then book that item by sending it a meeting request. These mailboxes are like those in on-premises Exchange Server and come in two different flavors, which are:

1. *Equipment mailboxes.* These mailboxes are for communal-use, discrete items of equipment that aren't nailed down, such as portable projectors, computer monitors, laptops, and so on. Typically, if it moves and doesn't belong to a nominated person, then an equipment mailbox is a good way to manage it.
2. *Room mailboxes.* These mailboxes are for booking immovable objects, such as conference rooms, meeting rooms, cinemas, sports halls, swimming pools – in fact, any physical space can be created as a room and then booked through Exchange Online. If a room has fixed equipment, such as a ceiling-mounted projector, then that equipment can be considered part of that room.

- Resource mailboxes can be for rooms or equipment
- Their main purpose is to accept or reject booking requests
- Booking requests can be automatically or manually accepted
- Users can log on to the resource mailbox through delegated access rights
- Ensure that labelling of the resource is carried out logically and consistently

However, a movable room (such as a portable cabin or a caravan) is probably better set up as a room mailbox.

 **Note:** You are recommended to have a structured and consistent way to label room or equipment mailboxes so that it is immediately apparent where a room is located or what piece of equipment is which.

Creating a New Room Mailbox

To create a new room mailbox in EAC, perform the following procedure:

1. In EAC, click **Recipients**, and then click **Resources**.
2. Under **Resources**, click the + (add) icon, then select **Room mailbox**.
3. In the **Room Name** field, enter a descriptive name for the room. For example, type "Conference Room 11/306" if the room is in building 11 and identified on the door as room 306.
4. Under **Email address**, enter the room's email address and select the domain from the list of registered domain names. Again, make the email address consistent and easy to identify, such as conf-room-11-306@lucernepublishing.com.
5. Add a **Location** for the room, such as Building 11, Third Floor.
6. If there is a phone in the room, such as a conference phone, enter that number in the **Phone** field.
7. Enter a **Capacity** for the room, such as 25.
8. Under Booking requests, either choose the option for **Accept or decline booking requests automatically**, where the room mailbox will accept booking requests automatically and inform users if there is booking conflict, or **Select delegates who can accept or decline booking requests**, in which case the booking request is forwarded to the selected delegate for approval.
9. If using the second option, click the + sign under **Delegates**, select the delegates, click **Add** and then click **Save**.
10. Click **Save** to save the new room mailbox.

After creating the room mailbox, you can configure the following settings:

- *General.* Specify Name, capacity, hide from address lists, department, company, address book policy, and custom attributes.
- *Booking delegates.* Accept booking requests automatically, select delegates or customize acceptance policy for this mailbox.
- *Booking options.* Allow repeated meetings, only schedule during working hours, maximum booking lead time, maximum meeting duration, and a customized reply to the meeting organizer.
- *Contact information.* Add street, Zip/post code, city and so on if required.
- *Email address.* Add further email addresses if required.
- *MailTip.* Create MailTip to provide additional information that users can see when they select this address in an email.
- *Mailbox delegation.* Configure Send As, Send on Behalf Of and Full Access permission for this mailbox, as with shared mailboxes.

To create the mailbox by using PowerShell, run the following command:

New-Mailbox -Name "Second Floor Conference Room" -Room

To configure the room mailbox to process booking requests automatically, run this command:

Set-CalendarProcessing <Identity> -AutomateProcessing AutoAccept

Creating a New Equipment Mailbox

To create a new equipment mailbox in EAC, perform the following procedure:

1. In EAC, click **Recipients**, and then click **Resources**.
2. Under **Resources**, click the + (add) icon, then select **Equipment mailbox**.
3. In the **Equipment Name** field, enter a descriptive name for the equipment. For example, type "Portable Projector S/N 32011044" if the equipment is a projector with that serial number. Alternatively, provide a tag number if there is one.
4. Under **Email address**, enter the equipment's email address and select the domain from the list of registered domain names. Again, make the email address consistent and easy to identify, such as projector-32011044@lucernepublishing.com.
5. Under Booking requests, either choose the option for **Accept or decline booking requests automatically**, where the equipment mailbox will accept booking requests automatically and inform users if there is booking conflict, or **Select delegates who can accept or decline booking requests**, in which case the booking request is forwarded on to the selected delegate for approval.
6. If using the second option, click the + sign under **Delegates**, select the delegates, click **Add** and then click **Save**.
7. Click **Save** to save the new equipment mailbox.

After creating the room mailbox, you can configure the following settings:

- *General.* Specify Name, capacity, hide from address lists, department, company, address book policy and custom attributes.
- *Booking delegates.* Accept booking requests automatically, select delegates or customize acceptance policy for this mailbox.

- *Booking options.* Allow repeated meetings, only schedule during working hours, maximum booking lead time, maximum meeting duration, and a customized reply to the meeting organizer.
- *Contact information.* Add street, Zip/post code, city and so on if required.
- *Email address.* Add further email addresses if required.
- *MailTip.* Create MailTip to provide additional information that users can see when they select this address in an email.
- *Mailbox delegation.* Configure Send As, Send on Behalf Of and Full Access permission for this mailbox, as with shared mailboxes.

To create the mailbox by using PowerShell, run the following command:

New-Mailbox -Name "Demonstration Laptop – Tag 305911" –Equipment

To configure the equipment mailbox to process booking requests automatically, run this command:

Set-CalendarProcessing <Identity> -AutomateProcessing AutoAccept

Changing Mailbox Types

You can change the different types of mailbox into each other by using PowerShell commands, with one exception. Direct changes you can make are:

- User mailbox to resource mailbox
- Resource mailbox to user mailbox
- Shared mailbox to resource mailbox
- Resource mailbox to shared mailbox
- Shared mailbox to user mailbox

To make these changes, use the **Set-Mailbox** command. There is no EAC option to make this change. For example, to convert the marketing department to a user mailbox:

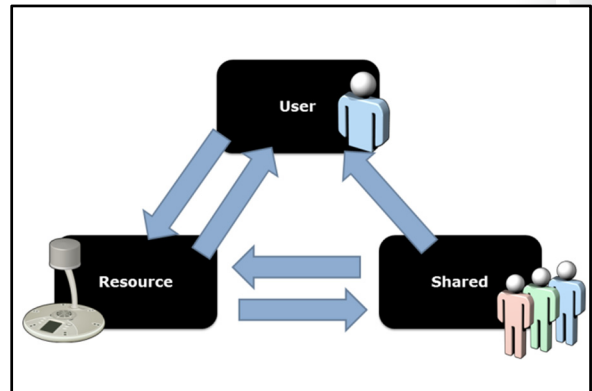
Set-Mailbox <mailboxname> -Type Regular

You can use the following values for the **-Type** parameter in this command:

- Regular
- Shared
- Room
- Equipment

To check that this process worked, run the following command:

Get-Mailbox -Identity <mailboxname> | Format-List RecipientTypeDetails



Configuring Distribution and Security Groups


In the Office 365 admin center, you can create security groups and add users to those security groups. You can then assign permissions to that security group, such as, in SharePoint Online. If you have synchronized your Office 365 account with your on-premises Active Directory, security groups created in Active Directory are also synchronized across to Office 365. Module 3 covers creating security groups, and synchronizing on-premises security groups is covered in Module 10.

	Office 365 Security Group	Exchange Online Security Group	Exchange Online Distribution Group	Exchange Online Dynamic Distribution Group
Visible in Office 365 Users and Groups	Yes	Yes	No	No
Visible in Exchange Online Groups	No	Yes	Yes	Yes
Can set permissions	Yes	Yes	No	No
Has email address	No	Yes	Yes	Yes
Has dynamic membership	No	No	No	Yes
Supports Self-enrol	No	No	Yes	No

Exchange Online provides additional group features, which enable the creation of the following group types:

- Mail-enabled security groups
- Mail-enabled distribution groups
- Mail-enabled dynamic distribution groups

The main difference between security and distribution groups is that security groups can specify permissions in Office 365, whereas distribution groups cannot. With dynamic distribution lists, the membership of the group is query-based and depends on how many users meet the selected criteria, rather than a static membership as in distribution groups.

 **Note:** If you create a mail-enabled security group in Exchange Online, it appears in Office 365 admin console under security groups. However, Office 365 security groups do not appear in Exchange Online.

Mail-enabled Security Groups

A mail-enabled security group enables you to distribute messages and grant access permissions in Windows Azure Active Directory. To create a mail-enabled security group, perform the following procedure:

1. In EAC, click **Recipients** and click **Groups**.
2. In groups, click the + icon and click **Security group**.
3. In **Display Name**, enter the name of the group that you want to appear in the Address Book.
4. In **Alias**, enter a unique alias for the group. This value auto-populates the first part of the **Email address** field.
5. Select the domain for the email address from the drop-down list.
6. Give the group a **Description** so that other administrators know what the purpose of the group is.
7. Under **Owners**, note that by default, the group creator is an owner. However, you can remove yourself as an owner and assign ownership to someone else, including to security groups.
8. To add an owner, click the + icon, then select users or security groups and click **Add**, then click **Save**.
9. Under Members, note that by default, the group owner is a member. However, you can deselect the **Add group owners as members** box and add other members to the group. Alternatively, you can let the group owner select members.

10. To add a Member, click the + icon, then select users or security groups and click **Add**, then click **Save**.
11. Check the option for **Owner approval is required** if you want the group owners to receive requests to join the group. If you do select this option, only group owners can remove members (not the administrator).
12. Click **Save** to save the new group.

When you have created the mail-enabled security group, you can change the following settings:

- *General.* Change the display name, alias, email address, description and hide the group from address lists.
- *Ownership.* Modify the owners of the group.
- *Membership.* Modify the group membership.
- *Membership approval.* Specify whether owner approval is required.
- *Delivery management.* Specify whether external addressees can email this group or only internal users and further.
- *Message approval.* Here you can configure moderation, both specifying who can moderate the group and who can send messages to the group without moderation.
- *Email options.* Add further email addresses for the group.
- *MailTip.* Add a MailTip to specify what is displayed when users send messages to the group.
- *Group delegation.* Specify **Send As** and **Send on Behalf Of** permission for users or groups.

To create a mail-enabled security group in PowerShell called IT Administrators, run the following command:

New-DistributionGroup -Name "File Server Managers" -Alias fsadmin -Type security

To show information about this new security group, run the following command:

Get-DistributionGroup <Name> | FL Name,RecipientTypeDetails,PrimarySmtppAddress

Mail-enabled Distribution Groups

A mail-enabled Distribution group enables you to distribute messages and grant access permissions in Windows Azure Active Directory. To create a mail-enabled Distribution group, perform the following procedure:

1. In EAC, click **Recipients** and click **Groups**.
2. In groups, click the + icon and click **Distribution group**.
3. In **Display Name**, enter the name of the group that you want to appear in the Address Book.
4. In **Alias**, enter a unique alias for the group. This value auto-populates the first part of the **Email address** field.
5. Select the domain for the email address from the drop-down list.
6. Give the group a **Description** so that other administrators know what the purpose of the group is.
7. Under **Owners**, note that by default, the group creator is an owner. However, you can remove yourself as an owner and assign ownership to someone else, including to Distribution groups.
8. To add an owner, click the + icon, then select users or Distribution groups and click **Add**, then click **Save**.

9. Under **Members**, note that by default, the group owner is a member. However, you can deselect the **Add group owners as members** box and add other members to the group. Alternatively, you can let the group owner select members.
10. To add a Member, click the + icon, then select users or Distribution groups and click **Add**, then click **Save**.
11. Under **Choose whether owner approval is required to join the group**, you now have the following options:
 - a. **Open**: Anyone can join this group without being approved by the group owners.
 - b. **Closed**: Members can be added only by the group owners. All requests to join will be rejected automatically.
 - c. **Owner approval**: All requests are approved or rejected by the group owners.
12. In addition, under **Choose whether the group is open to leave**, you can specify the following options for leaving the group:
 - a. **Open**: Anyone can leave this group without being approved by the group owners.
 - b. **Closed**: Members can be removed only by the group owners. All requests to leave will be rejected automatically.
13. Click **Save** to save the new group.

When you have created the mail-enabled distribution group, you can change the following settings:

- *General*. Change the display name, alias, email address, description and hide the group from address lists.
- *Ownership*. Modify the owners of the group.
- *Membership*. Modify the group membership.
- *Membership approval*. Specify the options for joining or leaving the group.
- *Delivery management*. Specify whether external addressees can email this group or only internal users and further.
- *Message approval*. Here you can configure moderation, both specifying who can moderate the group and who can send messages to the group without moderation.
- *Email options*. Add further email addresses for the group.
- *MailTip*. Add a MailTip to specify what is displayed when users send messages to the group.
- *Group delegation*. Specify **Send As** and **Send on Behalf Of** permission for users or groups.

To create a mail-enabled Distribution group in PowerShell called IT Administrators, run the following command:

New-DistributionGroup -Name "IT Administrators" -Alias itadmin -MemberJoinRestriction open

Dynamic Distribution Groups

Dynamic distribution groups change their membership depending on a query against account types and additional criteria. Because dynamic distribution lists can be quite large, it is important to correctly design them.


Creating dynamic distribution lists in EAC is similar to a distribution list, except for setting up the criteria. When selecting Members, you can select one, some or all of the following options:

- Users with Exchange mailboxes

- Mail users with external email addresses
- Resource mailboxes
- Mail contacts with external email addresses
- Mail-enabled groups

You can then add further criteria to refine the number of accounts that will appear in the results. The additional options include:

Variable	Condition
State or province	A match on the recipient's State or province property.
Company	A match on the recipient's Company property.
Department	A match on the recipient's Department property.
Custom attribute N (where N is a number from 1 to 15)	A match on the recipient's CustomAttributeN property.

 **Note:** Filtering on Organizational Unit or domain is not available in Exchange Online.

You can create a dynamic distribution group by using PowerShell with the following command:

```
New-DynamicDistributionGroup -IncludedRecipients MailboxUsers -Name "Sales Users Dynamic Group" -Department Sales
```

To view information about a dynamic distribution list, enter the following command:

```
Get-DynamicDistributionGroup -Identity "Marketing" | Format-List
```

Lab: Administering Exchange Online

Scenario

With Exchange Online now implemented as part of the Deploy Phase, Lucerne Publishing is administering its user accounts both in the cloud and on-premises. Heidi has moved on to manage protection policies, which are very important for the company. She is implementing personal archives, together with anti-spam and anti-malware settings. To assist in communicating with different associates and contacts, she is also setting up mail contacts and mail users in Exchange Online.

Objectives

By the end of this lab, you should be able to:

- Configure personal archive policies, customize retention tags, and apply retention policies.
- Set anti-malware and anti-spam policies in line with company requirements.
- Add external user email addresses as both mail contacts and mail users.
- Create and schedule events with resource mailboxes.

Lab Setup

Estimated Time: 90 minutes

Virtual machine: 20346C-LUC-CL1

Username: **Student1**

Password: **Pa\$\$w0rd**

Where you see references in the steps to `lucernepublishingXXXX.onmicrosoft.com`, you should replace XXXX with the unique Lucerne Publishing number that you are assigned when you set up your Office 365 accounts in Module 1, Lab 1B, Exercise 2, Task 3, Step 5.

Where you see references to `labXXXXX.o365ready.com`, you should replace XXXXX with the unique O365ready.com number you are assigned when you registered your IP address at `www.o365ready.com` in Module 2, Lab 2B, Exercise 1, Task 2, Step 6.

Exercise 1: Configure Personal Archive Policies

Scenario

Lucerne Publishing is a company that does a lot of emailing with increasingly large attachments. The organization also needs to retain content for a considerable length of time without clogging up mailboxes. Hence, the archiving feature in Exchange Online was particularly appealing. The plan is to enable archive mailboxes for users and then configure additional retention policies so that folders such as Sent Items are regularly cleared out to the users' online archives.

The main tasks for this exercise are as follows:

1. Enable Personal Archive for Mailboxes
2. Use Personal Archives
3. Create a Retention Tag in Exchange Admin Center
4. Create a Custom Retention Tag in PowerShell and Add Tags to a Policy
5. Apply Policies to Folders and Messages

► **Task 1: Enable Personal Archive for Mailboxes**

1. On your host computer, switch to the **20346C-LUC-CL1** virtual machine.
2. Ensure you are logged on as **Student1** with a password of **Pa\$\$word**.
3. On **LUC-CL1**, on the Task Bar, click Internet Explorer, and navigate to **login.microsoftonline.com**.
4. In **User name** and **Password**, enter **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number) and **Pa\$\$w0rd**, respectively.
5. On the Task Bar, right-click **Internet Explorer** and select **Start InPrivate Browsing**.
6. Navigate to **login.microsoftonline.com**.
7. In **User name** and **Password**, enter **cemond@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number) and **Pa\$\$w0rd**, respectively.
8. Click **Outlook**.
9. Note that there is only an Inbox with some folders there.
10. Note that you may have a message about an account error.
11. Click the configuration cog and click **Options**.
12. In **Options**, click **Connected accounts**.
13. Click **cemond@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number), and then click the **Delete** icon.
Note: You may need to refresh your browser at this point.
14. In the warning message, click **Yes**.
15. Click the **Option** button to go back to the Outlook page.
16. Switch to Heidi Leitner's session, under **Admin**, click **Exchange**.
17. In **Recipients**, click **Coralie Emond**, and in the right-hand pane, under **In-Place Archive**, click **Enable**.
18. In the warning message, click **Yes**.
19. In the right-hand pane, under **In-Place Archive**, click **View details**.
20. Note the warning. Click **OK**.
21. View the information in **Archive mailbox**.
22. Click **Cancel**.
23. Switch to the **InPrivate session** of Internet Explorer.
24. Click **Coralie Emond** and click **Sign Out**.
25. Close Internet Explorer.

► **Task 2: Use Personal Archives**

1. Open an **InPrivate session** of Internet Explorer and navigate to **login.microsoftonline.com**.
2. In **User name** and **Password**, enter **cemond@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number) and **Pa\$\$w0rd**, respectively.
3. Click **Outlook**.
4. Click **More to show**.

5. If you click on the **In-Place Archive – Coralie Emond** folder, you may get a message saying **Your archive appears to be unavailable. Please try again later.** Click **OK**.
6. Switch back to Heidi Leitner's session and with Coralie Emond's name selected, under **In-Place Archive**, click **View details**.
7. Notice that the error message may still appear. This is a timing issue.
8. Switch back to **Coralie Emond's** Inbox.
9. Click the **In-Place Archive – Coralie Emond** folder and confirm you can access it successfully.
Note: You may have to log off, close Internet Explorer and log back on again as Coralie Emond to access the In-Place Archive folder.
10. Click **Inbox** and click a message.
11. Drag the message from the Inbox into the **In-Place Archive - Coralie Emond** folder.
12. Click the **In-Place Archive - Coralie Emond** folder and view the message.
13. Right-click the message in the **In-Place Archive - Coralie Emond** folder and click **Move**, then click **More**.
14. In the **Move 1 conversation** dialog box, click **Inbox** and click **Move**.
15. The message now moves back to Coralie's Inbox.

► **Task 3: Create a Retention Tag in Exchange Admin Center**

1. Switch back to Heidi Leitner's account, then click **Admin** and click **Exchange**.
2. On the left-hand column, click **Compliance management**.
3. On the right-hand side, click **Retention tags**.
4. Click the + sign and click **Applied by users to items and folders (personal)**.
5. In new tag applied by users to items and folders (personal), under **Name**, enter **Lucerne Publishing – Archive after three years**.
6. Under **Retention Action**, click **Move to Archive**.
7. Under **Retention period**, click **When the item reaches the following age (in days)**, and enter **1095**.
8. Click **Save**.

Note: Your screen may freeze or you may receive an error message at this point. If so, check to see if the new tag has been created and if not, start the task again.

► **Task 4: Create a Custom Retention Tag in PowerShell and Add Tags to a Policy**

1. On **LUC-CL1**, press the Windows key, then on the **Start** page, click **Windows Azure Active Directory**.
2. Click on **Run as administrator**.
3. Type the following commands, pressing Enter after every line:

```
Set-ExecutionPolicy unrestricted
Import-Module MSOnline
$O365Cred = Get-Credential
```

4. In the **Windows PowerShell Credential** box, in **User name**, enter **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number).

5. In **Password**, enter **Pa\$\$w0rd**. Click **OK**.
6. Type the following commands, pressing Enter after every line:

```
$0365Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
https://ps.outlook.com/powershell -Credential $0365Cred -Authentication Basic -
AllowRedirection
Import-PSSession $0365Session -AllowClobber
Connect-MsolService -Credential $0365Cred
```

7. In the Windows Azure Active Directory Module for Windows PowerShell window, enter the following command and press Enter:

```
New-RetentionPolicyTag "Lucerne Publishing - Delete Sent Items after 90 Days" -Type
SentItems -AgeLimitForRetention 90 -RetentionAction DeleteAndAllowRecovery
```

8. In the Windows Azure Active Directory Module for Windows PowerShell window, enter the following command and press Enter:

```
Get-RetentionPolicy
```

9. Note the retention policies currently in place. There should be a **Default MRM** policy and an **ArbitrationMailbox** policy.
10. Switch back to Internet Explorer running Heidi's logon.
11. In the **Exchange admin center**, click **Retention policies**.
12. In **Retention policies**, click the + sign.
13. In **New retention policy**, under **Name**, enter **Lucerne Publishing Retention Policy**.
14. Under **Retention tags**, click the + sign.
15. Click the two policies starting with **Lucerne**, click **Add**, and then click **OK**.
16. In the **New Retention Policy** page, click b.
17. Switch to Coralie's account and click **Outlook**.
18. Click the cog to the right of Coralie's name and click **Options**.
19. Click **Email**.
20. Click **Retention policies**.
21. Note that there are none of the Lucerne Publishing retention tags that you defined earlier listed.
22. Click the **plus (+) sign** and note that the Lucerne Publishing retention tags are also not visible.
23. Switch back to Heidi's account and click **Recipients**.
24. Click **Coralie's mailbox** and click the **edit** symbol.
25. In the **Coralie Emond** page, click **Mailbox features**.
26. Under **Retention policy**, click **Lucerne Publishing Retention Policy**.
27. Click **Save**.
28. Switch to the Windows Azure Active Directory prompt.
29. Enter the following command and press Enter:

```
Start-ManagedFolderAssistant -identity "Coralie Emond"
```

30. Switch back to Coralie's account on the **Retention policies** page, click the + sign. Now you can see the Lucerne Publishing – Archive tag.
31. In the interface, select the **Lucerne Publishing-Archive after three years** policy and click **Add**, then click **Save**.

► Task 5: Apply Policies to Folders and Messages

1. In Coralie's account, click **Outlook**.
2. In **Outlook Web Access**, right click the **Inbox** folder and click **Assign policy**.
3. Note the Archive Policies and Retention Policies that apply to this mailbox.
4. Switch to Heidi's Office 365 session, and in Exchange admin center, click **Recipients**.
5. In Recipients, double-click Coralie Emond.
6. In Coralie Emond, click Mailbox features.
7. Under Retention policy, select Lucerne Publishing Retention Policy and click Save.

Note: Remember that what is shown as a policy in the user's interface is what Heidi defined in the Exchange admin center as a tag. The user doesn't actually see the policy that Heidi created at all, only the individual tags.

8. Switch back to the Windows Azure Active Directory prompt.
9. Enter the following command and press Enter:

```
Start-ManagedFolderAssistant -identity "Coralie Emond"
```

This action applies the selected retention policy to Coralie's mailbox.

10. Switch back to Coralie Emond's account and click **Outlook**.
11. Click the cog to the right of Coralie's name and click **Options**.
12. Click **Email**.
13. Click **Retention policies**.
14. Note the retention policies that are listed.
15. Click **Outlook**, and right-click the **Inbox** folder.
16. Click **Assign policy**, and under **Archive Policy**, click **Lucerne Publishing – Archive after three years**.

This action sets the new Lucerne Publishing three-year archive policy as the default policy on this folder.

17. Right-click an email in the **Inbox** folder, and click **Assign policy**.
18. Under **Archive Policy**, click **Lucerne Publishing – Archive after three years**.
This action applies the Lucerne Publishing archive policy to an individual item within the inbox folder.
19. In the message preview window on the right, click the ellipsis (...) button, and then click **Assign policy**.
20. Note that under ARCHIVE POLICY, the **Lucerne Publishing – Archive after three years** policy is checked.

Results: Lucerne Publishing has now enabled personal archive for mailboxes, created custom retention policies, created retention tags, applied retention policy, and modified the default retention policy.

Exercise 2: Manage Anti-malware and Anti-spam Policies

Scenario

To protect its intellectual property, Lucerne Publishing requires effective anti-spam and anti-malware defenses. Following discussions between Remi, Justin, and Heidi, it was decided to add further anti-spam and anti-malware policies and then apply those policies throughout the organization. Management has requested a demonstration of the effectiveness of these defenses, using test malware and spam messages to verify that spam and messages with a malicious payloads were being diverted properly.

Heidi sets up this demonstration, working with Luc Cartier and Coralie Emond to show how the anti-malware and anti-spam policies work.

The main tasks for this exercise are as follows:

1. Configure a New Malware Policy
2. Create a Test Malware File
3. Send Malware to Recipients
4. Configure an Anti-Spam Policy
5. Configure End-User Spam Notifications and Manage Spam Messages

► Task 1: Configure a New Malware Policy

1. Switch to Heidi Leitner's session on Internet Explorer.
2. Click **Admin** and then click **Exchange**.
3. In the left-hand column, click **Protection**.
4. Under **Malware filter**, click the + sign.
5. In **Name**, type **Lucerne Publishing - High Security**.
6. In **Malware Detection Response**, select **Delete the entire message**.
7. Do not select any notifications.
8. In **Applied to**, under **If**, click **The recipient is**.
9. In the selection box, click **Heidi Leitner**, and click **Add**.
10. Click **OK**.
11. In the **New anti-malware policy** page, click **Save**.
12. Review the new policy in the malware filter list. Note the priority assigned to the policy.
13. Switch to the Windows Azure Active Directory Module for Windows PowerShell window.
14. Type the following command on one line and press Enter:

```
New-MalwareFilterPolicy -Name "Internal User Policy" -action  
DeleteAttachmentAndUseDefaultAlertText -EnableInternalSenderNotifications $true -  
EnableInternalSenderAdminNotifications $true -InternalSenderAdminAddress  
hleitner@labXXXXX.o365ready.com (where XXXXX is your unique 0365ready.com number)
```

15. If you are prompted for credentials, in the **Windows PowerShell Credential Required** box, in **User name**, enter **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number) and in **Password**, enter **Pa\$\$w0rd**.
16. Type the following command on one line and press Enter:

```
New-MalwareFilterRule -Name "Lucerne Publishing - Medium Security" -
MalwareFilterPolicy "Internal User Policy" -RecipientDomainIs LabXXXXX.o365ready.com
(where XXXXX is your unique O365ready.com number)
```

17. Switch to Heidi's session in Internet Explorer, and in **Exchange admin center**, under **Malware filter**, click the refresh button.
18. Double-click **Lucerne Publishing – Medium Security**.
19. Click **Settings**.
20. Scroll down and confirm the following settings:
 - a. Delete all attachments and use default alert text.
 - b. Notify internal senders.
 - c. Notify administrator about undelivered messages from internal senders.
 - d. Administrator email address is **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number).
21. Click **Applied to**.
22. Confirm that the recipient domain is **labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number).
23. Click **Cancel**.

► Task 2: Create a Test Malware File

1. Click **Start**, type **services**, click **Settings**, and then click **View local services**.
2. In the **Services** console, scroll down and double-click on **Windows Defender Service**.
3. Next to **Startup type**, select **Disabled**.
4. Click **Stop** and then click **OK** to close the **Windows Defender Services Properties (Local Computer)** dialog box. Minimize the Services console.
5. Click **Start**, type **Note** and click **Notepad**.
6. In Notepad, copy and paste this exact text:


```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```
7. Click **File** and click **Save**.
8. Save the file on your desktop as **Eicar.txt**. The file size should be exactly 68 bytes.

Note: If you are performing this exercise on your own computer and you are running desktop anti-virus software, you may not be able to save the file. If this is the case, disable your anti-virus software from scanning the Desktop folder for this exercise.

► Task 3: Send Malware to Recipients

1. Switch to Coralie's session in Internet Explorer.
2. In **Outlook**, click **New**.
3. In the **To** box, enter **Luc Cartier** and add a subject.

4. Click **INSERT** and then click **Attachments or OneDrive files**.
5. Click **Eicar.txt** and then click **Upload and share with OneDrive/Send as attachment**.
6. Click **SEND**.
7. Press the Windows key, and then on the Start page click **Internet Explorer**.
8. Browse to **outlook.office365.com**.
9. Log on as **LCartier@labXXXXX.o365ready.com** with a password of **Pa\$\$w0rd** (where XXXXX is your unique O365ready.com number).
10. Double-click on the message from Coralie.
11. Double-click on the attachment and click **Open**. The attachment opens in Notepad on the Desktop.
12. What does the attachment body now say?
13. In Heidi's Internet Explorer session, click **Outlook** and review the messages in her Inbox.
14. Does Heidi receive an alert message? If not, why not?
15. In Heidi's account, click **Admin** and then click **Exchange**.
16. In the **Exchange admin center**, click **Protection**.
17. In **Protection**, under **Malware filter**, click **Lucerne Publishing – Medium Security**, click **Edit**, and then click **Settings**.
18. In **Settings**, under **Malware Detection Response**, click **Delete the entire message**.
19. Click **Save**.
20. Switch to Coralie Emond's session, and in **Outlook**, click **New**.
21. In the **To** field, enter **LCartier** and add a subject.
22. Click **INSERT** and then click **Attachments or OneDrive files**.
23. Attach the **eicar.txt** file from Step 5.
24. Click **SEND**.
25. Note the non-deliverable message in Coralie's account.
26. In Heidi's account, click **Outlook**.
27. Note the non-deliverable message there as well.
28. Press Start and click **Internet Explorer**.
29. Note that Luc does not receive any message.
30. Switch back to the **Services** console.
31. In the Services console, scroll down and double-click on **Windows Defender Service**.
32. Next to **Startup type**, select **Automatic** and click **Apply**.
33. Click **Start** and then click **OK** to close the **Windows Defender Services Properties (Local Computer)** dialog box. Close the Services console.
34. Note that the eicar.txt file may disappear from the desktop after a few seconds if Windows Defender detects this file immediately. However, in some cases the file will remain on the desktop until a full scan is done on the machine.

► Task 4: Configure an Anti-Spam Policy

1. In Internet Explorer, logged on as **Heidi Leitner**, click **Admin** and then click **Exchange**.
2. On the left-hand side, click **Protection** and then click **Content filter**.
3. Click the + sign to add a new policy.
4. In **Name**, enter **Lucerne Publishing Anti-Spam Filter**.
5. Under **Actions**, under **Spam**, select **Prepend subject line with text**.
6. Under **High-confidence spam**, select **Quarantine message**.
7. Under **Prepend subject line with this text**, enter **SPAM, SPAM, SPAM, SPAM, SPAM:**.
8. Under **International spam**, click **Filter email messages written in the following languages**.
9. Click the + sign.
10. Scroll down the list, click **Latin**, click **Add**, and then click **OK**.
11. Click **Filter email messages sent from the following countries or regions**.
12. Click the + sign.
13. Scroll down the list, click **South Georgia and the South Sandwich Islands**, click **Add** and then click **OK**.
14. Under **Advanced options**, under **Increase Spam Score**, select **On** for the following settings:
 - a. Image links to remote sites
 - b. Numeric IP address in URL
 - c. URL redirect to other port
15. Under **Mark as Spam**, select **On** for the following settings:
 - a. Empty messages
 - b. Apply sensitive word list
16. Under **Applied To**, under **If**, click **The recipient domain is**, select **labXXXXX.o365ready.com**, (where XXXXX is your unique O365ready.com number) and click **Add** then click **OK**.
17. Click **Save**.
18. Review the new policy in the **Exchange admin center**.
19. Switch to your external email client and create a new message.
20. In the **To** field, enter **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number).
21. Enter a subject of **Offers**.
22. In the body of the message, enter **http://131.107.30.10/offers**.
23. Click **Send**.
24. Switch to Heidi Leitner's account and click **Outlook**.
25. Double-click the new message. Note that it may appear in the Inbox or the Junk Mail folder.
26. You should now see the item with the IP address URL appended with the phrase **SPAM, SPAM, SPAM, SPAM, SPAM**.
27. In your external email client, navigate to the **Junk Mail** folder.

28. Find an obvious junk message and click **Forward**.
29. In the **To** field, enter **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number) and click **Send**.
30. Switch to Heidi Leitner's account.
31. Check the **Junk Mail** folder in her mailbox.
32. You should now see the forwarded junk mail item.
33. From your external email account, create a new message to **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number) with the subject **More Spam**:
34. In the body of the message, add the following plain text:
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
35. Send the message.
36. Check Heidi's Outlook account to see if the **More Spam**: message arrives. Note that the message may either be in the Inbox or the Junk Mail folders.

► **Task 5: Configure End-User Spam Notifications and Manage Spam Messages**

1. In Internet Explorer, logged on as **Heidi Leitner**, click **Admin** and then click **Exchange**.
2. On the left-hand side, click **Protection** and then click **Content filter**.
3. Click **Lucerne Publishing Anti-Spam Filter**.
4. On the right-hand side, scroll down and then click **Configure end-user spam notifications**.
5. Click **Enable end-user spam notifications**.
6. Click **Save**.
7. In the **Exchange admin center**, click **Quarantine**.
8. Double-click one of the quarantined messages.
9. Click **Release to**. Do NOT report as a false positive.
10. In the **Release message** window, click **Release message to specified recipients**, select **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number), click **Add** and then click **Release**.
11. Click **Close**.
12. In Internet Explorer, click **Outlook**, and in Heidi Leitner's mailbox, check the **Inbox** and **Junk Mail** folders for the message.

Results: Lucerne Publishing has created and applied anti-spam and anti-malware polices that are protecting the organization.

Exercise 3: Configure Additional Email Addresses for Users

Scenario

Because Lucerne Publishing has several DNS domains and subdomains registered with Office 365, and users may have email accounts associated with those domains, it is necessary to create additional email addresses for specific users and ensure that each user's email accounts are associated with the user's

mailbox. Heidi is working with Coralie's account to ensure that these records are added correctly, both by using EAC and PowerShell.

The main tasks for this exercise are as follows:

1. Create an Additional Email Address
2. Configure the DNS Information for the New Domain
3. Create Additional Proxy Email Addresses for Multiple Users

► Task 1: Create an Additional Email Address

1. Switch to your **private email account** and send a message to **coralieemond@content.labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number).
2. What happens to the message?
3. On Heidi Leitner's account, click **Admin** and then click **Exchange**.
4. In **Recipients**, double-click **Coralie Emond**.
5. Click **Email address**.
6. Under **Email address**, click the + sign.
7. In **New email address**, select **SMTP** and enter **coralieemond@content.labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number).
8. Click **OK**.
9. Click **Save**.
10. Switch to your **private email account** and send a message to **coralieemond@content.labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number).
11. What happens to the message this time?

► Task 2: Configure the DNS Information for the New Domain

1. In **Heidi Leitner's** account, click **Admin** and click **Office 365**.
2. Click **Domains** and next to **content.labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number), click **Complete setup**.
3. Click **Next**.
4. Click **Next**.
5. In **How do you want to use content.labXXXXX.o365ready.com with office 365?** (where XXXXX is your unique O365ready.com number), select **Outlook for email, calendar, and contacts**, and then click **Next**.
6. Remain on the **Add these DNS records for content.labXXXXX.o365ready.com at your DNS hosting provider** page (where XXXXX is your unique O365ready.com number).
7. In **E:\RDP_files**, double-click **LUC-DC1.rdp**.
8. Log on as **LUCERNE\LucAdmin** with a password of **Pa\$\$w0rd**.
9. In **Server Manager**, click **Tools**, and then click **DNS**.
10. In the DNS console, expand **Forward Lookup Zones**, right-click **labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number) and click **New Domain**.

11. In the **New DNS Domain** dialog box, enter **content**, and click **OK**.
12. Right-click **content** and click **New Mail Exchanger (MX)**.
13. In the **Mail Exchanger (MX)** tab, check that **Host or child domain** is blank and that **Fully qualified domain name** is **content.labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number).
14. In **Fully qualified domain name (FQDN) of mail server**, enter the POINTS TO ADDRESS value from the **DNS records** page in Office 365, in the form **content-labXXXXX-o365ready-com.mail.protection.outlook.com** (where XXXXX is your unique O365ready.com number), and then click **OK**.
15. Right-click **Content** and point to **New Alias (CNAME)**.
16. In **Alias name**, type **autodiscover**.
17. In **Fully qualified domain name (FQDN) for target host**, type **autodiscover.outlook.com**, and click **OK**.
18. Right-click **Content** and point to **New Alias (CNAME)**.
19. In **Alias name**, type **msoid**.
20. In **Fully qualified domain name (FQDN) for target host**, type **clientconfig.microsoftonline-p.net**, and click **OK**.
21. Right-click **Content** and click **Other New Record**.
22. In the **Resource Record Type** dialog box, scroll down and select **Text (TXT)**, then click **Create Record**.
23. In the **Text Field**, enter the **TXT VALUE** from the **DNS records** page in Office 365, then click **OK**.
24. In the **Resource Record Type** dialog box, click **Done**.
25. On the **Add the following DNS records for content.labXXXXX.o365ready.com** page (where XXXXX is your unique O365ready.com number), click **Okay, I've added the records**.
26. On the **Your records are correct and content.labXXXXX.o365ready.com is all set up** page, click **Finish**.
27. Switch to your **private email account** and send a message to **coralieemond@content.labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number).
28. What happens to the message this time?

► Task 3: Create Additional Proxy Email Addresses for Multiple Users

1. Switch to Windows Azure Active Directory Module for Windows PowerShell.
2. If the session has timed out, log on again as **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number) with a password of **Pa\$\$w0rd**.
3. Enter the following three commands and press Enter after each line:

```
$users = Get-Mailbox
foreach ($a in $users)
{$a.emailaddresses.Add("smtp:$($a.alias)@content.labXXXXX.o365ready.com")}
$users | %{Set-Mailbox $_.Identity -EmailAddresses $_.EmailAddresses}
```

(where XXXXX is your unique O365ready.com number).

4. Use your external email account to send a message to **cemond@content.labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number).
5. Switch to Internet Explorer for Coralie's account.
6. Check that the message is received.
7. At the top right-hand corner, click **Coralie Emond** and click **Sign out**.
8. Close the Internet Explorer window.

Results: Lucerne Publishing has configured secondary email addresses for additional domains in Office 365.

Exercise 4: Create and Manage External Contacts, Resources, and Groups

Scenario

Because Lucerne Publishing engages many associates for content creation, it is important the company can stay in contact with and position these individuals within the company management structure. In addition, some of these users need to be given access to resources within Office 365 while maintaining email addresses outside the organization. As a result, Lucerne Publishing needs to use both mail contacts and mail users within Office 365 to manage these accounts.

The company also wants to set up shared mailboxes for departments to use and resource mailboxes to enable management of resources such as conference rooms, projectors, and other locations and pieces of equipment. Again, Heidi has been tasked to set up these resources.

The main tasks for this exercise are as follows:

1. Create Mail User Accounts
2. Manage Mail Users and Contacts
3. Create a Shared Mailbox and Grant Send As Permissions
4. Send Mail from a Shared Mailbox
5. Connect to a Shared Mailbox
6. Create and Manage Resource Mailboxes

► Task 1: Create Mail User Accounts

1. Logged on as **Heidi Leitner**, click **Admin** and then click **Exchange**.
2. In the **Exchange admin center**, in **Recipients**, click **Contacts**.
3. In **Contacts**, click the + sign and click **mail contact**.
4. In **New mail contact**, enter the following information:
 - a. First name: **Alain**
 - b. Last name: **Richer**
 - c. Display name: **Alain Richer (External)**
 - d. Alias: **Aricher**
 - e. External email address: **aricher@contoso.com**
5. Click **Save**.

6. Note that the information on the right-hand pane may not display correctly.
7. Click the refresh button.
8. Confirm that the information you entered has been added.
9. Double-click on Alain Richer's account.
10. Click **MailTip**.
11. In the warning message box, enter **This is an external email address**.
12. Click **Save**.
13. Under **Recipients**, click the + sign and click **Mail user**.
14. Complete the fields with your information.
15. In **Alias**, enter your first initial and last name.
16. In **External email address**, enter your external email address.
17. In **User ID**, enter the same information for your alias.
18. Ensure that **labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number) is selected as the domain.
19. In the **New password** and **Confirm password** fields, enter **Pa\$\$w0rd**.
20. Click **Save**.
21. Click the refresh button until the new account appears.

► Task 2: Manage Mail Users and Contacts

1. Switch to Windows Azure Active Directory Module for Windows PowerShell.
2. At the prompt, type the following on one line and then press Enter:

```
New-DistributionGroup -Name "External Users" -Alias ExternalUsers -Members YourAlias, aricher -PrimarySmtpAddress externalusers@labXXXXX.o365ready.com -Type Distribution
```

(replace **YourAlias** with your alias that you entered in Step 15 in the previous task and XXXXX with your unique O365ready.com number).

3. Switch to Internet Explorer and logged on as **Heidi Leitner**, under **Recipients**, click **Groups**.
4. If the group does not appear, click the refresh button.
5. Double-click **External Users**.
6. In the **General** tab, confirm that the email address is **externalusers@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number).
7. Click Membership.
8. Confirm that your account and Alain Richer's are members of this group.
9. Click **Cancel**.
10. Switch back to Heidi's account and click **Outlook**.
11. Click **New**, and in the **To** field, enter **aricher**.
12. Note that the mail account resolves to Alain Richer.
13. Click **Alain Richer**. Note the external email account under **Send mail**.
14. Enter a subject and some text in the body.

15. Note the MailTip reminding you that Alain is external to the organization.
16. Click **DISCARD** and click **DISCARD in discard MESSAGE**.
17. Click **New**.
18. In the **To** box, enter **External users**.
19. Add a subject and some text to the body of the message.
20. Click **SEND**.

Note that the mailtip does not appear.

21. Check your **external email account** for the received message.

► Task 3: Create a Shared Mailbox and Grant Send As Permissions

1. In **Heidi Leitner's** account, click **Admin** and then click **Exchange**.
2. Click **Recipients**.
3. In **Recipients**, click **Shared**.
4. Click the + sign.
5. In the **New shared** mailbox, in **Display name**, enter **Marketing Department**.
6. In **Email**, enter **Marketing**, and after the @ sign, select **labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number).
7. Under **Users**, click the + sign, then select **Coralie Emond**.
8. Click **Add**, then click **OK**.
9. Click **Save**.
10. Switch to Windows Azure Active Directory Module for Windows PowerShell.
11. At the prompt, type the following on one line and then press Enter:

```
Add-RecipientPermission marketing@labXXXXX.o365ready.com -AccessRights SendAs -
Trustee lmartin@labXXXXX.o365ready.com
```

(where XXXXX is your unique O365ready.com number).

12. At the **Confirm** message, press Enter.
13. At the prompt, type the following on one line and then press Enter:

```
Get-RecipientPermission -Identity marketing@labXXXXX.o365ready.com
```

(where XXXXX is your unique O365ready.com number).

14. You should have **SendAs** entries for **NT AUTHORITY\SELF**, **Cemond**, and **LMartin**.

► Task 4: Send Mail from a Shared Mailbox

1. On the Task Bar, right-click **Internet Explorer** and click **InPrivate Browsing**.
2. Browse to **login.microsoftonline.com**.
3. Log on as **lmartin@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number) with a password of **Pa\$\$w0rd**.
4. Click **Outlook**.

5. In **Language**, click ensure **English (United States)** is selected and under **Time zone**, select **(UTC + 01:00) Amsterdam etc**, then click **Save**.
6. Click **New**.
7. In the **New mail** pane, click the **New window** icon on the right.
8. Click the ellipsis (...) icon and click **Show from**.
9. In the **From** field, delete **Imartin@labXXXXX.o365ready.com**, (where XXXXX is your unique O365ready.com number), and enter **Marketing**.
10. In the **To** field, enter your external email account.
11. Give the email a subject and some body text, then click **SEND**.
12. When you receive the message on your external email, check the reply-to address and then reply to the mail.

► **Task 5: Connect to a Shared Mailbox**

1. Switch to Heidi's logon, click **Admin** and then click **Exchange**.
2. In the **Exchange admin center**, under **Recipients**, click **Shared**.
3. Double-click the **Marketing Department** group.
4. In **Marketing Department**, click **Mailbox delegation**.
5. Under **Full Access**, click the + sign.
6. Click **Liane Martin**, click **Add**, then click **OK**.
7. Click **Save**.
8. Switch back to Liane's session and click **Outlook**.
9. At the top right-hand corner of the page, click **Liane Martin**, and click **Open another mailbox**.
10. In **Open another mailbox**, enter **Marketing**, and click **Open**.
11. Under **Language**, select **English (United States)** and in **Time zone**, select **Amsterdam**.
12. Click **Save**.
13. Note the message you replied to in Step 12 of the previous task in the Inbox.
14. Click **New** and send a new email message to **Heidi Leitner**.
15. Switch to Heidi Leitner's account and see the message appear in her Inbox. Note that it comes from Marketing.
16. Switch back to Liane's session, click **Liane Martin**, and click **Sign out**. Close the Internet Explorer window.

► **Task 6: Create and Manage Resource Mailboxes**

1. In Heidi Leitner's account, click **Admin** and click **Exchange**.
2. In Recipients, click Resources.
3. Click the + sign and click **Room mailbox**.
4. Enter the following information:
 - a. Room name: **Main Conference Room**
 - b. Email address: **MainConferenceRoom@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number)

- c. Location: **2nd Floor**
 - d. Capacity: **25**
5. Click **Save**.
Note that by default, resource mailboxes automatically accept booking requests.
 6. Switch to Windows Azure Active Directory Module for Windows PowerShell.
 7. Type the following command on one line and press Enter:

```
new-mailbox -PrimarySmtpAddress confroomprojector@labXXXXX.o365ready.com -alias confroomprojector -Name "Main Conference Room Projector" -equipment
```

(where XXXXX is your unique O365ready.com number).

8. Switch to **Heidi Leitner's** account.
9. In **Resources**, click the **Refresh** button.
10. Double-click **Main Conference Room Projector**.
11. Click **Booking options** and in the **If you want the meeting organizer to receive a reply, enter the text below** box, type **Ensure that you have a spare bulb for the projector**.
12. Click **Save**.
13. In Heidi Leitner's Outlook account, click **Calendar**.
14. Click **New event**.
15. In **Event**, enter **Office 365 Meeting**.
16. Next to **Location**, click **Add room**.
17. Select **Main Conference Room**.
18. In **Attendees**, type **Main Conference Room Projector**. Also type **Elisabeth Labrecque** and **Luc Cartier**.
19. Enter **08:00** in the **Start time** and set the **Date** to **tomorrow**. Set the **Duration** to **1 hour**.
20. Click **SEND**.
21. On the Task Bar, right-click Internet Explorer, click **Start InPrivate Browsing** and browse to **login.microsoftonline.com**.
22. Log on as **kgruber@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number) with a password of **Pa\$\$w0rd**.
23. Under **Language**, select **English (United States)** and in **Time zone**, select **Amsterdam**.
24. Click **Calendar** and click **New event**.
25. In **Event**, enter **Marketing GroupThink**.
26. Next to **Location**, click **Add room**.
27. Select **Main Conference Room**.
28. In **Attendees**, type **Main Conference Room Projector**, **Coralie Emond** and **Justin Muller**.
29. Enter **08:30** in the **Start time** and set the **Date** to **tomorrow**. Set the **Duration** to **1 hour**.
30. Click **SEND**.
31. Click **Outlook**, and then look in Karen Gruber's Inbox. What message has appeared?

Results: Lucerne Publishing has created external mail contacts and mail users and set up shared and resource mailboxes.

Lab Discussion Questions

How would you typically configure ownership and Send As permissions for a shared mailbox where you wanted to separate out who could perform each function?

By creating two security groups, one for Full Access and the other for Send As. You then add users to the groups as required.

What is a primary cause of failure to book a resource through a resource mailbox for global companies?

Failure to use the correct time zone for booking the resource, often caused by not changing the time zone on the client computer to match the location.


- How would you typically configure ownership and Send As permissions for a shared mailbox where you wanted to separate out who could perform each function?
- What is a primary cause of failure to book a resource through a resource mailbox for global companies?

Module Review and Takeaways

In this module, you have covered the following topics:

- Configuring Messaging Records Management (MRM) for Exchange Online.
- Managing Anti-malware and Anti-spam Policies.
- Configuring additional email addresses for users.
- Creating and managing external contacts, resources, and groups in Exchange Online.

You have also had practical experience of these activities in the labs:

-  **Best Practice:** Design your Exchange Online policies to reflect business need before implementing them.
- Ensure that you train users on how to apply retention tags and use archive mailboxes.
- Implement a process for managing spam quarantine and designate responsibility for attending to spam items.
- Identify who needs to be a mail user and who needs to be a mail contact.
- Decide whether mail contacts will be visible in the GAL.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Junk mail is not being moved to the junk mail folder.	
Spam is not being correctly flagged.	

Module 8

Configuring SharePoint Online

Contents:

Module Overview	8-1
Lesson 1: Manage SharePoint Site Collections	8-2
Lesson 2: Configure External User Sharing	8-12
Lesson 3: Plan a Collaboration Solution	8-21
Lab: Configuring SharePoint Online	8-28
Module Review and Takeaways	8-37

Module Overview

In this module, students learn how to plan a SharePoint® Online implementation that reflects the customer's needs, and then create site collections that reflect those requirements. This module covers the process of external user sharing with SharePoint Online and describes how this arrangement helps organizations share information more effectively.

Objectives

After completing this module, you should be able to:

- Manage SharePoint site collections by using the SharePoint Online admin center and Windows PowerShell®.
- Configure external user sharing by using the Office 365™ admin center.
- Plan a collaboration solution.

Lesson 1

Manage SharePoint Site Collections

In this lesson, students learn how to set the SharePoint Online site collection administrator, set resource quotas and warning levels, set storage quota for site collections, and configure the name and URL of site collection.

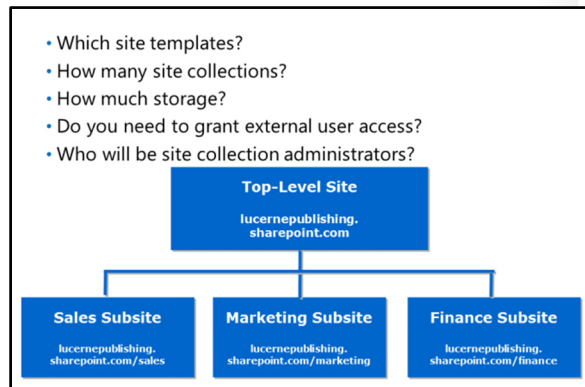
Lesson Objectives

After completing this lesson, you should be able to:

- Plan site collections.
- Create site collections with the Office 365 admin center.
- Configure site collections with the Office 365 admin center.
- Configure site collections with the Office 365 admin center.
- Manage site collections with Windows PowerShell.
- Describe common errors and best practices for managing SharePoint site collections.

Plan Site Collections

A SharePoint Online site collection is a hierarchical group of sites that you, as an administrator of SharePoint Online, can manage on an individual basis or as a whole. The sites in a site collection share items such as administration settings, owner, and collection-wide permissions. Each site collection contains one top-level site that is created automatically when you create the site collection, and a number of subsites that are below it in the site hierarchy. Subsites can inherit permissions and navigation from the parent site, or these components can be configured and managed separately.



Plan the Site Collections You Need to Create

Having a hierarchy of top-level sites and subsites means that you can maintain different control levels over the features and settings for each site. This enables you to have a primary site for an entire organization or team, as well as individual and shared sites for sub-teams, divisions, or other projects. You can also create separate site collections for external websites.

How you organize your site collections depends mainly on the organization's size and the needs of the business. If you know some key factors, such as what a site collection might be used for, who will require access to it, and who will manage it, this will make it easier for you to make key planning decisions about which site templates to use, how many sites and site collections you will need to create, and how much storage you will need. You should consider the following factors when planning your site collections:

- *What site templates should be used?* You can create a site collection from a site template. These templates already contain items such as document libraries, lists, pages, and several other common site components that provide various features for your organization. Any sites that you create from a

template will inherit the template's properties. It is common to use several different site templates when building your site collection.

- *How many site collections are required?* This number is typically dependent on your organization's storage limits and its business needs. Some types of sites, such as the Enterprise Search Center and the My Site Host, exist as stand-alone site collections and may be automatically created for you when you sign up for Office 365. You will likely need to create further site collections to fulfill the specific requirements of your organization.
- *How much storage is required for each site collection?* When you purchase the SharePoint Online service as part of your Office 365 plan, you are allocated a storage pool based on the number of user licenses and the type of Office 365 plan you purchase. You then need to determine how much storage should be allocated to each of your site collections, with the minimum allocation being 100 MB. When assigning storage to your site collections, you can see the total amount of storage allocated to your organization and how much of that remains to allocate to other site collections. These storage levels can be modified at a later date and can be increased or decreased as needed within your storage allocation limit.
- *Is multi-language support required?* The Multilingual User Interface (MUI) feature allows your users to display sites and web pages in other languages. This feature is not a translation tool; rather, it modifies the display language for specific default interface components. MUI modifies the user interface on a per-user basis and does not affect how other users view the site or page. This MUI feature only modifies the viewable on-screen components; it does not modify content, such as documents, held within the site. The MUI feature is enabled in SharePoint by default, but if you want to use it on a site collection, then you, or another site collection administrator, also need to enable it on that site collection.
- *Do you need to grant access to external users?* Some of your users may need to collaborate with users external to the organization. In this case you will need to consider sharing content with those external users; this will require a little thought and planning.
- *Who will manage your site collections?* The following roles can administer the SharePoint Online service:
 - *Global administrator.* This is the main administrative role for the Office 365 admin center and can perform all administrative tasks, including managing service licenses, users and groups, domains, subscribed services, and define site collection administrators.



Note: Office 365 global administrators are also automatically SharePoint Online administrators.

- *SharePoint Online administrator.* This is the global administrator whose primary role is to administer SharePoint Online using the SharePoint admin center. This role can create and manage site collections, define site collection administrators, define tenant settings, and configure most other administrative elements, such as Business Connectivity Services, Secure Store, InfoPath Forms Services, Records Management, Search, and User Profiles.
- *Site collection administrator.* This role is granted the administrative permissions to manage a site collection. Although a site collection can have several administrators, there can only be one primary site collection administrator. The SharePoint Online administrator defines the primary site collection administrator when they create a new site collection. They can add further people to the list of site collection administrators after the site collection has been created. Site collection administrators can add or delete sites, specify a secondary site collection administrator, and modify site settings for any site in the site collection.



Best Practice: A recommended best practice is to define more than one site collection administrator, where the additional administrators act as backups to the primary site collection administrator.

Create Site Collections

As the SharePoint Online administrator for your Office 365 environment, you will be responsible for creating and deleting site collections. You can create multiple private site collections that can be used internally by your organizations' users.

Create Site Collections

SharePoint Online administrators can create private organization-wide site collections and assign primary site collection administrators to each site collection by using the SharePoint Online admin center.

- Create site collections
 - Site name, domain name, URL path
 - Template
 - Site collections administrators
 - Storage and resource quotas
- Delete site collections
 - Retained in Recycle Bin for 30 days
- Restore site collections
 - Within 30 days to restore yourself
 - Within a further 14 days for Microsoft to restore

To create a site collection:

1. Sign in to Office 365 as a global administrator or SharePoint Online administrator.
2. In the Office 365 admin center choose **Admin**, and then **SharePoint**.
3. In the left-hand side, choose **Site collections**.
4. In the ribbon, choose **New**, and then **Private Site Collection**.
5. In the new site collection dialog box, specify the following:
 - A name for the site collection.
 - A domain name and URL path for the site collection. You can choose either **/sites** or **/teams** as part of the path and then supply a further path extension to be the path to the site in the empty text box.
 - A language for the site collection.



Note: You must ensure you select the correct language for your site collection here, because it cannot be changed afterwards.

- A template that matches the purpose of the site collection. For example, if your site collection is going to be used for a specific project, you would choose the Project Site from the list.



Note: There are three categories of template to choose from: Collaboration, Enterprise, and Publishing, or you can pick the Custom template which enables you to select a template at a later time.

- An appropriate time zone.
- A site collection administrator. You can use either the Check Names or Browse buttons to help find a user's name.


- A Storage Quota to allocate to this site collection. This must not exceed the total storage available that is displayed next to the box.
 - A Server Resource Quota to allocate to this site collection.
6. Choose **OK**.
- The site collection will then be created and eventually appear in the URL list. You will know it has finished when the URL for the site collection is highlighted in blue as a hyperlink. At this point, the assigned site collection administrator can begin creating and managing sites in the site collection.

Delete Site Collections

There may be situations where you will be required to delete a site collection. This might occur for any number of reasons, including:

- You have a team site collection and that team has been disbanded.
- Teams have been reorganized.
- You commonly use project-based sites and the projects are short term and are not required once the project is complete.

When you delete a site collection, it stays in the Recycle Bin for 30 days before it is permanently deleted; this gives you a 30-day window of opportunity to restore the site collection if it was deleted in error or your situation has changed and you wish to retain it.

 **Note:** When you delete a site collection, you also delete all the sites and site components and content in the site hierarchy, including documents and document libraries, lists and list items, events, site configuration settings, and security information for all sites and their subsites.

As other people will likely be affected by the removal of the site collection, ensure that all interested parties, such as site owners and site contributors, are aware of the impending deletion and are given time to move their content or data to another place if necessary.

To delete a site collection:

1. Sign in to Office 365 as a global administrator or SharePoint Online administrator.
2. In the Office 365 admin center, choose **Admin**, and then **SharePoint**.
3. In the left-hand side, choose **Site collections**.
4. Select the check box for the site collection/s you want to delete.
5. In the ribbon, choose **Delete**.
6. On the delete site collections page, read the warning and choose **Delete**.

Restore Deleted Site Collections

If you have deleted a site collection in error you can see it listed in the Recycle Bin and restore it from there. This list also shows you how many days are left before the site collection is permanently deleted.

To restore a deleted site collection:

1. Sign in to Office 365 as a global administrator or SharePoint Online administrator.
2. In the Office 365 admin center choose **Admin**, and then **SharePoint**.
3. In the left-hand side, choose **Site collections**.

4. In the ribbon, choose **Recycle Bin**.
5. Select the check box for the site collection/s you want to restore.
6. In the ribbon, choose **Restore Deleted Items**.
7. On the restore site collections page, choose **Restore**.

The site collection will take some time to restore, and once restoration is complete, the site collection will be listed under Site Collections again.



Note: If a site collection has been permanently deleted from the Recycle Bin, you have a further 14 days from the time of deletion in which to contact Microsoft Online Services through a service request and have them restore it for you.

Configure Site Collections

There are several site collection elements and properties you can configure as a SharePoint Online administrator, including site collection properties, owners, sharing, and storage and resource quotas.

View Site Collection Properties

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

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

- View site collection properties
- Define site collection owners
 - Primary and standard site collection administrators
- Share a site collection
- Set site collection quotas
 - Storage
 - Server Resources
- Upgrade site collection settings
 - If version is not most recent

Add or Remove Site Collection Administrators

You can modify the current primary site collection administrator and add or remove other site collection administrators.

To change the primary site collection administrator:

1. In the Office 365 admin center, choose **Admin**, and then **SharePoint**.
2. In the left-hand side, choose **Site collections**.
3. Select the check box next to the appropriate site collection.
4. On the ribbon, in the **Manage** section, choose **Owners**, and then **Manage Administrators**.
5. In the manage administrators dialog box, under **Primary Site Collection Administrator**, change the user name for the primary site collection administrator.
6. Use the **Check Names** button to verify that the user names are valid.
7. Choose **OK**.

To add or remove site collection administrators:

1. In the Office 365 admin center, choose **Admin**, and then **SharePoint**.
2. In the left-hand side, choose **Site collections**.
3. Select the check box next to the appropriate site collection.
4. On the ribbon, in the **Manage** section, choose **Owners**, and then **Manage Administrators**.
5. In the manage administrators dialog box, under **Site Collection Administrators**, add people to, or remove them from, the list.
6. Use the **Check Names** button to verify that the user names are valid.
7. Choose **OK**.

Sharing Site Collections

The Sharing option on the ribbon enables you to share your site collections with users outside your organization. This can be done through invitations or anonymous guest links.



Note: External user sharing is covered in greater detail later in this module.

Manage Storage Quotas for Site Collections

A storage quota is the maximum amount of storage space (in MB) allocated for a site collection – you will need to specify the storage quota for each site collection that you manage. You can modify the quota level by increasing or decreasing it as needed, but the minimum quota you can specify per site collection is 100 MB. You also set the storage quota warning level and can specify that a notification alert should be sent to you by email message when you near the storage limit for the site collection.

To modify the storage quota for a site collection:

1. Sign in to Office 365 as a global administrator or SharePoint Online administrator.
2. In the Office 365 admin center, choose **Admin**, and then **SharePoint**.
3. In the left-hand side, choose **Site collections**.
4. Select the check box for the site collection you want to specify a storage quota for.
5. In the ribbon, in the Manage section, choose **Storage Quota**.
6. In the set storage quota dialog box, enter the maximum value in megabytes (MB) you want to allocate to the selected site collection. The default is 100 MB.
7. Ensure the **Send e-mail to site collection administrators when a site collection reaches**: check box is selected. This will send an email alert when you are getting close to the storage quota limit.
8. Enter a percentage value to set the warning level for the alert email to be triggered. Note that while the default value is 0, the recommended value is 85%.
9. Save your settings.

If your storage is running low, you have three options:

- Decrease the overall amount of content in your site collections by removing any unnecessary, out of date, or superfluous content.
- Delete some unnecessary or out of date site collections.
- Buy more storage from Microsoft Online Services.

Manage the Server Resource Quota for a Site Collection

The server resource quota is a value generated by SharePoint Online for each site collection. Having these resource quotas helps reduce the risk that custom code running in sandboxed solutions will adversely affect the performance of other site collections by depleting available server resources.

As a SharePoint Online administrator you can specify a quota for server resource usage for each site collection which SharePoint Online will monitor, to ensure they do not go above the specified level. SharePoint will also send an alert email to notify the site collection owner when the server resource quota is near its limit, again based on a warning level set by you. The monitoring that SharePoint carries out is based on performance data collected for key resources such as processor and memory usage. If a site collection reaches its server resource quota limit, SharePoint will turn off the sandbox for the site collection so that custom code can no longer be run.

To change the server resource quota for a site collection:

1. Sign in to Office 365 as a global or SharePoint Online administrator.
2. In the Office 365 admin center, choose **Admin**, and then **SharePoint**.
3. In the left-hand side, choose **Site collections**.
4. Select the check box for the site collection you want to specify a storage quota for.
5. In the ribbon, in the Manage section, choose **Server Resource Quota**.
6. In the set server resource quota dialog box, enter a maximum number of resources to allocate to the selected site collection out of the available displayed total. The default number of resources is 300.
7. Ensure the **Send e-mail when each selected site collection resource usage reaches warning level at:** check box is selected. This will send an email alert notification when you are getting close to the server resource quota limit.
8. Enter a percentage value to set the warning level for the alert email to be triggered. The default is 85%.
9. Save your settings.

Upgrading Site Collections from a Previous Version

In the SharePoint admin center, under site collections, there is an option on the Manage section of the ribbon to upgrade the links and settings for your site collections. This setting enables you to:

- Specify site collection upgrade settings.
- Send an email notification about site collection upgrades to the site collection administrator.




Note: If your site collection is the most current, when you select either of the above two options, you will see a message displayed in the dialog box confirming that you have the most current version and therefore do not need to upgrade.

Managing Site Collections with PowerShell

You can use the SharePoint Online Management Shell to simplify the management of your site collections in SharePoint Online. This can be very useful if you are creating and configuring a lot of site collections and want to speed up the process rather than manually creating and configuring them in the SharePoint Online admin center.

As with other Microsoft services, you run Windows PowerShell command-line operations by using cmdlets. You can view a full list of all the available cmdlets by running the **Get-Command** cmdlet, and access help on how to use each cmdlet by using the **Get-Help** cmdlet.

- Set up the SharePoint Online Management Shell
 - Install Windows PowerShell 3.0
 - Download and install the SharePoint Online Management Shell
- Connect to the SharePoint Online service
 - Connect-SPOService
- Create and configure site collections
 - New-SPOSite
 - Set-SPOSite
 - Remove-SPOSite
 - Restore-SPODeletedSite

 **Note:** In order to use these cmdlets a SharePoint Online site administrator must be a global administrator in Office 365.

Before you can run cmdlets, you have to set up the SharePoint Online Management Shell environment and connect to the service.

Set up the SharePoint Online Management Shell

The SharePoint Online Management Shell is used by SharePoint Online global administrators to remotely manage site collections.

To set up the SharePoint Online Management Shell:

- Ensure that you have installed Windows PowerShell 3.0 from Windows Management Framework 3.0.
- Install the SharePoint Online Management Shell from the Microsoft Download Center, at <http://go.microsoft.com/fwlink/?LinkId=401133>.
- Open the SharePoint Online Management Shell.

Connect to the SharePoint Online Service

Having set up the SharePoint Online Management Shell, you need to connect to the SharePoint Online service before you can use PowerShell to manage your site collections.

To connect to the SharePoint Online service:

- Open the Windows PowerShell.
- At the prompt, type the following command and press Enter:

```
Connect-SPOService -Url https://contoso-admin.sharepoint.com -credential
admin@contoso.com
```

Using Windows PowerShell to Manage Site Collections

There are several useful cmdlets in the SharePoint Online Management Shell that can create and configure site collections.

You can use the **Get-SPOSite** cmdlet to view all site collections or view specific properties of site collections.

To view a list of all your current site collections:

- At the prompt, type the following command and press Enter:

```
Get-SPOSite
```

To view the details of a specific site collection:

- At the prompt, type the following command and press Enter:

```
Get-SPOSite -Identity urlofsitecollection
```

When you create a site collection, you can specify a site collection template to use. You can use the **Get-SPOWebTemplate** cmdlet to view all the available site collection templates or all those that match the given identity.

To view a list of all site collection templates:

- At the prompt, type the following command and press Enter:

```
Get-SPOWebTemplate
```

You can use the **New-SPOSite** cmdlet to create new site collections in SharePoint Online. This cmdlet has several parameters that can be used with it to specify configuration settings such as site collection owner, storage and resource quota, name, and template.

To create a new site collection:

- At the prompt, type the following command and press Enter:

```
New-SPOSite -Url urlofnewsitecollection -Owner upnofsitecollectionowner -StorageQuota number -Title "nameofsitecollection"
```

- Example:

```
New-SPOSite -Url http://contoso.sharepoint.com/sites/sales -Owner user@contoso.com -StorageQuota 400 -Title "Sales Site"
```

You can use the **Set-SPOSite** cmdlet to configure or update settings on existing site collections in SharePoint Online. As with the New-SPOSite cmdlet above, this cmdlet has several parameters that can be used with it to specify configuration settings such as site collection owner, storage and resource quota, and name.

To set the storage quota and quota warning level for an existing site collection:

- At the prompt, type the following command and press Enter:

```
Set-SPOSite -Identity https://contoso.sharepoint.com/sites/sales -StorageQuota 1000 -StorageQuotaWarningLevel 750
```

You can use the **Remove-SPOSite** cmdlet to delete a site collection. This does not permanently delete it from the site collections list, but instead, moves it to the SharePoint Online Recycle Bin. If necessary, deleted site collections stored in the SharePoint Online Recycle Bin can still be restored by using the **Restore-SPODeletedSite** cmdlet.

If you want to permanently delete a site collection, after moving it to the SharePoint Online Recycle Bin using the **Remove-SPOSite** cmdlet above, use the **Remove-SPODeletedSite** cmdlet.

To delete a site collection:

- At the prompt, type the following command and press Enter:

```
Remove-SP0Site -Identity https://contoso.sharepoint.com/sites/sales -NoWait
```

To restore a deleted site collection:

- At the prompt, type the following command and press Enter:

```
Restore-SP0DeletedSite -Identity https://contoso.sharepoint.com/sites/sales -NoWait
```



For more information on all the available cmdlets for administering site collections in SharePoint Online, go to:

<http://go.microsoft.com/fwlink/?LinkId=390900>

Common Errors and Best Practice Guidelines

When managing site collections in SharePoint Online, there are some common errors that you should avoid, and some best practices you should follow.

These common errors include:

- Granting too many permissions or not granting enough permissions.
- Setting quotas too high or too low.
- Poor planning of site collections, domain names and URLs.

- Common errors
 - Granting too many or not enough permissions
 - Setting quotas too high or too low
 - Poor planning of site collections, domains, and URLs
- Best practices
 - Follow the KISS principle
 - Centralize your management of SharePoint Online
 - Maintain your site to keep it fresh and up to date
 - Plan your permission structure carefully
 - Keep thorough and up-to-date documentation
 - Work with SharePoint developer or partner

To ensure that you manage SharePoint Online site collections correctly, you are recommended to follow these best practices:

- Follow the Keep It Simple Stupid (KISS) principle.
- Centralize your management of SharePoint Online.
- Maintain your site to keep it fresh and up-to-date.
- Plan your permission structure carefully.
- Keep thorough and up-to-date documentation of site configuration.

Lesson 2

Configure External User Sharing

In this lesson, students learn how to configure a site so that it can be accessed by users who are external to the organization. They cover how to enable these settings globally, per site collection, then share content with external users and remove external user access.

Lesson Objectives

After completing this lesson, you should be able to:

- Plan external user sharing.
- Enable external user sharing.
- Share content with external users.
- Remove external user sharing.
- Describe common errors and best practices for external user sharing.

Plan External User Sharing

If users in your organization sometimes work on projects that require them to share documents with and/or collaborate with, their clients or vendors, then it is likely that you will want to host a site in SharePoint Online to share content with users who are external to your organization. These are referred to as "external users" and would include any person who you want to give permission to access your site, but who does not have a license for your organization's Office 365 tenancy. External users would typically be non-employees such as contractors, or onsite agents or yours or your affiliates. Although you might invite external users to contribute as members of a long-term project and allow them to perform a range of tasks on a project site, they typically will not have the same capabilities and rights as full-time, licensed users in your organization.

Planning for sharing content with these external users is an important part of your overall permission strategy for SharePoint Online in Office 365.

There are three methods for sharing site content with external users as follows:

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

- Users sometimes need to share documents with, or collaborate with, external users
 - Share a whole site with external users by inviting them to sign in to your site
 - Share individual documents with external users by inviting them to sign in to your site
 - Share individual documents with external users by sending them an anonymous guest link
- Plan how and what to share
- Understand what external users can and cannot do when external user sharing is enabled

Planning How and What to Share

You should consider the following when planning your content sharing strategy, including how to share your site content with external users and what to share with them:

- Who needs access to content on your site and any subsites?
- Do they need access to an entire site or just a subsite?
- Do they only need access to a few specific documents?
- Do they only need to view the shared content, or do they need to make changes to it too?
- Which users in your organization need to be able to share content with external users?
- Which content on your site should never be shared with users external to your organization?

What External Users Can and Cannot Do When You Enable Sharing

After you enable external user sharing, those external users can perform several tasks and will inherit some rights and capabilities, but there are also some tasks they cannot perform and rights and capabilities they will not receive. The table below summarizes what external users can and cannot do:

External users can.....	External users cannot.....
Use Office Web Apps to view and edit documents.	Create personal sites and therefore will not have their own OneDrive for Business library. Also, they cannot install the desktop version of Office on their computers.
Inherit the use rights of the Office 365 tenant who has invited them to collaborate on a site collection. For example, if an organization subscribes to an E3 Enterprise plan, and creates a site that utilizes enterprise features, the external user will be given rights to view and use any enterprise features within the site collection where they have been invited.	View the organizational newsfeed. They also cannot edit their profile, change their picture, or view aggregated tasks.
Perform site-based tasks that map to the permission level that they have been assigned. For example, if an external user is added to the Members group, they will possess Edit permissions. Therefore, they could add, edit and delete lists, and could also view, add, update and delete list items and documents.	Be an administrator for a site collection.
View other types of content on subsites within a site collection they have been invited to, as well as view newsfeeds on those sites.	Access the Search Center and cannot execute searches against "everything" by default.

MCT USE ONLY STUDENT USE PROHIBITED

Enable External User Sharing

You can enable or disable external user sharing at two levels within the SharePoint admin center:

- *At the global level for your entire SharePoint Online tenant.* If you enable external sharing, you can also configure whether to allow sharing only with authenticated users, or allow sharing with both authenticated users and anonymous users through guest links.
- *At the individual site collection level.* This enables you to secure content on specific site collections when you do not want all your content to be shared. As above, you can also configure whether or not to allow sharing with authenticated users, or sharing with both authenticated users and anonymous users on a site collection.

- Enable or disable external user sharing at two levels:
 - Tenant
 - Site-collection
- Do not allow sharing outside your organization
- Allow external users who accept sharing invitations and sign in as authenticated users
- Allow both external users who accept sharing invitations and anonymous guest links

By default, external user sharing is enabled for the whole tenant and all the site collections it contains. It is common practice to disable it globally first and then start planning how, and where, to use it.

Configure External Sharing for a SharePoint Online Tenant or Site Collection

You must be a SharePoint Online administrator in order to configure external sharing for a tenant or a site collection.

To configure external sharing for a tenant:

1. In the Office 365 admin center, choose **Admin**, and then **SharePoint**.
2. In the left-hand side, choose **Settings**.
3. Under **External sharing**, choose one of the following:
 - **Don't allow sharing outside your organization.** This prevents users from sharing sites or content with any external users.
 - **Allow external users who accept sharing invitations and sign in as authenticated users.** This requires that any external user who has received an invitation to access shared content must log in with a Microsoft account before being allowed to access the content.
 - **Allow both external users who accept sharing invitations and anonymous guest links.** This allows external users who have received an invitation and signed in with a Microsoft account to access shared content, and also allows users to share documents directly with external users through anonymous guest links.
4. Choose **OK**.



Note: If you disallow external user sharing at the tenant level, then you cannot enable external user sharing at any site collection level. If you try to do this, you will receive the following message: "Sharing is disabled in Tenant Settings". Similarly, if you enable only sharing with invitations for authenticated users, and if you try to allow sharing through anonymous guest links, you will receive the following message: "Sharing links is disabled in Tenant Settings".

To configure external sharing for a site collection:

1. In the Office 365 admin center, choose **Admin**, and then **SharePoint**.

2. In the left-hand side, choose **Site collections**.
3. Select the check box for the site collection you want to configure external sharing for.
4. In the **Manage** section of the ribbon, choose **Sharing**.
5. Choose one of the following:
 - **Don't allow sharing outside your organization.** This will prevent users from sharing sites or content with any external users.
 - **Allow external users who accept sharing invitations and sign in as authenticated users.** This will require that any external user who has received an invitation to access shared content must log in with a Microsoft account before being allowed to access the content.
 - **Allow both external users who accept sharing invitations and anonymous guest links.** This will allow external users who have received an invitation and signed in with a Microsoft account to access shared content, but will also allow users to share documents directly with external users through anonymous guest links.
6. Choose **Save**.



Note: Anonymous guest links could potentially be shared with, or forwarded to, other people; this means that content could be viewed by people other than your intended target.



For more information on configuring external user sharing for a tenant or site collection, see the following link:

<http://go.microsoft.com/fwlink/?LinkId=390903>

You can easily view the current external user sharing settings for multiple site collections by selecting those site collections on the site collections page and then choosing **Sharing**, which will display all the current settings. Each site collection will display one of the following three sharing settings:

- Not allowed
- Share invitations
- Share links and invitations

Share Content with External Users

Remember that once external user sharing has been enabled for the tenant or a site collection, depending on the sharing setting, you can then share either a whole site or individual documents.

Share Sites using Invitations

To share an entire site with an external user, you need to send them an invitation to the site, which they will use to log in to your site and access the content. The invitation is sent to external users through an email message with a link to the site and an optional message you may have provided

- Share Sites
 - Invitations (users need to sign in)
 - Read, Edit, or Full Control
- Share Documents
 - Invitations (users need to sign in)
 - Anonymous Guest Links (share by email message, chat, social media)
 - View Only or Edit
- View Who Sites and Documents are Shared With

in the invitation. When the external user receives the email invitation they click the link and are then required to sign in with either a Microsoft account or an Office 365 ID to access the site and its content.



Note: Invitations to view content can be redeemed only once. After an invitation has been accepted, it cannot be shared or used by others to gain access.

When you send the invitation, you have the option of deciding what kind of permission that external user will receive when they access your site. The available permission options are:

- *Full Control*. This is chosen by selecting the **Sitename Owners [Full Control]** option.
- *Edit*. This is chosen by selecting the **Sitename Members [Edit]** option.
- *Read*. This is chosen by selecting the **Sitename Visitors [Read]** option.



Note: You need to be a site owner or have at least Full Control permission on a site to be able to share it with external users.

It is recommended that you be very cautious when sharing your sites; by sharing your site and its contents, you are allowing people outside your organization to access and perhaps edit your site content. It is a best practice to create a site dedicated to sharing non-sensitive content with external users and setting specific unique access permissions for that site only.



Note: When granting external user access to your site content, you should always apply the principle of *least privilege*, so that those external users only receive the minimum permission required to perform their tasks, and no more. You should only grant Full Control in extremely rare cases.

To share a site with an external user for read-only access:

1. Navigate to the site you wish to share with an external user.
2. Choose **SHARE**.
3. In the **Share sitename** dialog box, enter the email address of the external user you want to invite to share your document (If you wanted to share with an internal user, you would just enter their name instead).
4. Enter a message that will be included as part of your invitation.
5. Choose **SHOW OPTIONS**.
6. Under **Select a group or permission level**, in the drop-down list, select **Sitename Visitors [Read]**.
7. Choose **Share**.
8. When the external user receives the emailed invitation, they will see your message and will need to click to **Go To sitename** link and then sign in with either a Microsoft account or an Office 365 ID.



Note: By default, invitations expire after seven days, so if the external user has not accepted the invitation within that time, you will need to send a new one.

Share Individual Documents using Invitations or Anonymous Guest Links

To share an individual document with an external user, you can either send an invitation in the same way as you do for a site – but only for the individual document – or you can send an anonymous guest link to the document, if this setting has been enabled for our tenant and the site collection.

Anonymous guest links only enable external users to open the document in the relevant Office Web App, such as Excel Web App; they cannot open it in the full desktop version of the application. If you later decide to disable external user sharing at the tenant level, any anonymous guest links will stop working; when you enable it again, those anonymous guest links will start working again.

To share a document that requires the external user to sign in:

1. Navigate to the site containing the document you wish to share with an external user.
2. Click the ellipses (...) next to the document to open its callout window and then choose **SHARE**.
3. Ensure that, in the left-hand pane, **Invite people** is selected.
4. Enter the email address of the person you want to share the document with.
5. In the drop-down list, select either **Can edit**, or **Can view**.
6. Optionally, enter a message to include in your invitation.
7. Select the **Require sign-in** check box.
8. Choose **Share**.

To share a document using an anonymous guest link:

1. Navigate to the site that contains the document you wish to share with an external user.
2. Click the ellipses (...) next to the document to open its callout window and then choose **SHARE**.
3. In the left-hand pane, choose **Get a link** is selected.
4. Select one of the following:
5. Under **View Only**, choose **CREATE LINK** to grant read-only permission to the document.
6. Under **Edit**, choose **CREATE LINK** to grant edit permission to the document.
7. After the anonymous guest link URL is created, copy it to a location where it can be easily retrieved, such as Notepad.
8. Close the dialog box.
9. You can then copy the anonymous guest link URL and paste into a location of your choice, such as an email message, a chat window, or a social media page.



Note: Files in a library that has been IRM-protected cannot be shared with external users.

Auditing Shared Access to Sites and Documents

You can also quickly see users with whom a site or document has been shared, which can be useful for auditing and reporting purposes.

To see a list of users with whom a site has been shared:

1. On the site home page, click **SHARE** in the top right of the page.
2. Note the list of users after the words **Shared with**.

To see a list of users with whom a specific document has been shared:

1. Select the document in the library.
2. On the **FILES** tab, in the **Manage** section of the ribbon, choose **Shared With**.
3. The Shared With dialog box lists all the users who this document has been shared with.
4. Choose **Close**.

Remove External User Sharing

There are several ways of stopping external user sharing, which include removing user permissions from a user by taking them out of a group, revoking invitations, disabling anonymous guest links, and disabling external user sharing for the tenant or site collection.

Remove External User Permissions

If an external user has already accepted an invitation, you can stop their access to a site by removing their permissions.

To remove an external user's permissions:

1. On the site's home page click the **Settings** icon (the cog).
2. Choose **Site settings**.
3. Under **Users and Permissions**, choose **People and groups**.
4. In the left-hand side, under **Groups**, select the group from which you want to remove users, for example **Sitename Members**.
5. Select the user or users you want to remove, choose **Actions**, and then choose **Remove Users from Group**.
6. Choose **OK**.

Revoke Invitations

You can withdraw invitations you have sent to external users if you need to, but only if they have not yet been accepted.

To revoke an invitation:

1. On the site's home page click the **Settings** icon (the cog).
2. Choose **Site settings**.
3. Under **Users and Permissions**, choose **Access requests and invitations**.
4. Under **EXTERNAL USER INVITATIONS**, click the ellipsis button (...) for the person you would like to revoke the invitation.
5. Choose **WITHDRAW**.

- Remove External User Permissions
- Revoke Invitations
 - If they have not been accepted
- Disable Anonymous Guest Links
- Turn off External User Sharing
 - For the tenant
 - For the site collection only

Disable Anonymous Guest Links

You can revoke access to a document you have shared individually by disabling the guest link on the document.

To disable an anonymous guest link:

1. Navigate to the library that contains the document you want to disable the anonymous guest link for.
2. Click the ellipsis button (...) for the document, and then click on the words “**a guest link**”.
3. In the dialog box, choose **DISABLE**.
4. In the dialog box, choose **Disable Link**.
5. Close the dialog box.

Turn Off External User Sharing

The other option you have is to disable external user sharing at the tenant or site collection level. Disabling sharing at the tenant level means nothing can be shared with any external users in any site collections. Disabling sharing at the site collection level means that external user sharing is only disabled for that specific site collection.

To disable external user sharing for a tenant:

1. In the Office 365 admin center choose **Admin**, and then **SharePoint**.
2. In the left-hand side choose **Settings**.
3. Under **External sharing** choose **Don't allow sharing outside your organization**.
4. Choose **OK**.

To disable external user sharing for a site collection:

1. In the Office 365 admin center choose **Admin**, and then **SharePoint**.
2. In the left-hand side choose **Site collections**.
3. Select the check box for the site collection you want to disable external user sharing for.
4. In the **Manage** section of the ribbon, choose **Sharing**.
5. Choose **Don't allow sharing outside your organization**.
6. Choose **Save**.
7. Choose **OK**.

Common Errors and Best Practice Guidelines

When configuring external user sharing in SharePoint Online, there are some common errors that you should avoid, and some best practices you should follow.

These common errors include:

- Sharing more content than is necessary by sharing a whole site rather than one or two documents.
- Granting more shared access than is required; for example, by giving an external user edit permission when they only need to read the document.
- Granting access through anonymous guest links temporarily, but then forgetting you have done it.
- Lack of awareness of what external users can and cannot do in SharePoint Online.
- Lack of documentation of SharePoint configuration in relation to external user sharing.

• Common errors

- Sharing more content than is necessary
- Granting more shared access than is required
- Forgetting you've created anonymous guest links

• Best practices:

- Plan what external users can see and access
- Consider creating a site purely for external users
- Use the principle of "least privilege".
- Avoid using anonymous guest links for sensitive content
- Ensure you know the identity of any external users

To ensure that you configure external user sharing successfully in SharePoint Online, you are recommended to follow these best practices:

- Plan what external users can see and access, by segmenting your content by its data sensitivity.
- Consider creating a site purely for the purposes of sharing content with external users.
- Exercise security awareness by using the principle of "least privilege".
- Set appropriate permissions on site collection so users can't share info they shouldn't be sharing.
- Anonymous guest links could potentially be forwarded or shared with other people, who might also be able to view or edit the content without signing in. Avoid using anonymous guest links for sensitive content; instead, share a document by using an invitation that requires sign-in.
- Ensure you know the identity of any external users before you start sharing content with them. Remember that these users will be able to log in to your site and start browsing and accessing content just like other site members. Depending on the access permission you gave them, this may mean that they can share content with other external users.
- If you share Team Site content, consider creating a subsite for the shared content, and then share that subsite with external users so that you can assign unique permissions only to that subsite.

Lesson 3

Plan a Collaboration Solution

In this lesson, students learn how to plan for SharePoint Online as part of the Deploy phase of the FastTrack process. They identify the factors that affect the selection of collaboration features and briefly cover the options for SharePoint adoption. They contrast the requirement for Yammer versus Newsfeeds, look at co-authoring, and identify if there is any requirement to access files across multiple client devices.

Lesson Objectives

After completing this lesson, you should be able to:

- Plan for Yammer integration.
- Plan for co-authoring.
- Plan for OneDrive for Business.

Plan for Yammer Integration

Yammer is an enterprise-class social network that organizations can use to enable their users to collaborate in a secure manner. Yammer helps users to be more productive by allowing them to work with other people within the organization in real time, and across departmental and geographic boundaries.

The Yammer application is provided in two versions:

- *Yammer Basic*. This is the free version that is available to all users, offering fundamental features for co-workers to collaborate within an organization.
- *Yammer Enterprise*. This is the premium version which is provided either as a stand-alone upgrade from the basic version or is provided as part of some SharePoint Online and Office 365 plans. This enterprise version of Yammer provides several extra features and resources to enable an organization to implement a professional enterprise social network.

- Yammer
 - Enterprise-class social network for organization's users to collaborate in a secure manner
 - Basic or Enterprise versions
- Use Yammer with Office 365
 - Replace Newsfeed with Yammer
 - Use Yammer app for SharePoint
- Replace Newsfeed with Yammer
 - Settings > Enterprise Social Collaboration
 - Users can still use Newsfeed

Use Yammer with Office 365

Office 365 provides two enterprise social network services – the Newsfeed feature in SharePoint Online or Yammer. If you decide that Yammer is the best option for your organization, there are two ways in which you can use it:

- *Use Yammer instead of SharePoint Newsfeed*. You can switch to using Yammer instead of Newsfeed by changing the Enterprise Social Collaboration setting in the SharePoint admin center.
- *Use the Yammer app for SharePoint*. You can download the Yammer app for SharePoint from the Office Store, and after you make it available for users, they will be able to add a Yammer feed to their sites in SharePoint Online. Users will then be able to post to the Yammer network from Office 365, the Yammer app, and Yammer mobile apps.



Note: The enterprise version of Yammer is provided with some SharePoint Online and Office 365 plans, but is a completely separate service and therefore has different user rights and privacy and security policies than Office 365. Yammer is not a service that is covered by the Office 365 Trust Center at the time of this writing.

Replace Newsfeed with Yammer

The default social collaboration network in Office 365 is the SharePoint Newsfeed; however, as mentioned previously you can configure Yammer to be the enterprise social collaboration network of choice for SharePoint Online in Office 365. When you make the change, the navigation bar in the Office 365 portal will change to display Yammer instead of Newsfeed.

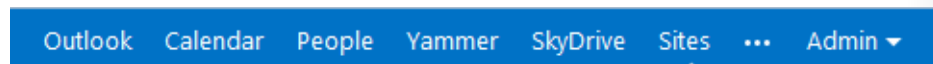


FIGURE 8.1: OFFICE 365 ADMIN CENTER NAVIGATION BAR

Although the navigation bar will change, SharePoint Newsfeed functionality is not lost; users will still be able to use the SharePoint Newsfeed feature, as it will still be listed in the left-hand navigation on site pages. The main difference is that users will no longer be able to post to Everyone.

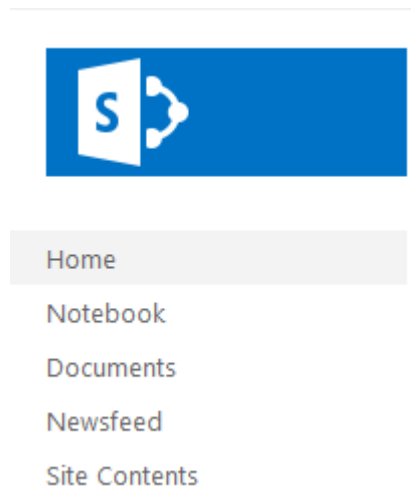



FIGURE 8.2: OFFICE 365 ADMIN CENTER LEFT NAVIGATION MENU.



Note: Making this switch is a major change to your users' working environment, so ensure you inform them of the change prior to it occurring, and provide some training on how to use Yammer if required.

To replace the Newsfeed link on the Office 365 portal with a link to Yammer:

1. In the Office 365 admin center, choose **Admin**, then **SharePoint**.
2. In the SharePoint admin center, choose **Settings**.
3. Under **Enterprise Social Collaboration**, choose **Use Yammer.com service**.
4. Choose **OK**.

 **Note:** Making the change from Newsfeed to Yammer can take up to 30 minutes to complete, depending on the number of users you have in your tenancy.

Once the change has been made, when a user clicks Yammer in the navigation bar, they will be redirected automatically to Yammer.com.

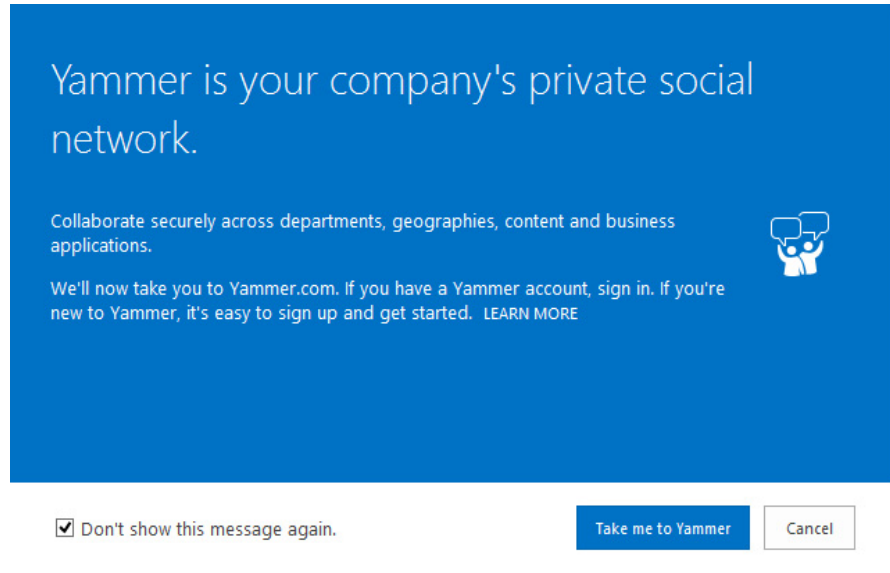



FIGURE 8.3: REDIRECT TO YAMMER WEBSITE.

 **For more information on choosing whether to use Yammer or Newsfeed as your enterprise social network, see the following link:**

<http://go.microsoft.com/fwlink/?LinkId=331308>

Plan for Co-Authoring

In the past, document collaboration has meant users passing documents to each other by email messages, working on the document, and sending changes back by return email. This rather archaic system is prone to errors and can cause major problems with tracking changes to documents and maintaining a proper version history of documents.

SharePoint provided some solutions to these issues by providing version control and tracking functionality. However, the issue of multiple users wanting to work on the same document at the same time is not really solved by these features – this is where co-authoring functionality comes in.

- Co-authoring in SharePoint Online
 - Enables multiple users to work on the same document without affecting each other
- Planning for co-authoring in SharePoint Online
 - Permissions
 - Versioning level
 - Number of versions
 - Require check out
 - Content approval
- Co-authoring support for SharePoint Online
- Co-authoring in mixed Office environments

Co-authoring Functionality in SharePoint Online

An organization's users can use the co-authoring capabilities of SharePoint Online to simplify collaboration between co-workers working on common documents and projects. Co-authoring is built into SharePoint Online and is already enabled, so there is no need to configure any settings.

Co-authoring allows a user to work on the same document as another user without either user impacting the other's changes to the document. Office 2013 applications, such as Word 2013 and PowerPoint 2013, offer co-authoring functionality, but if you are using Office 365 and SharePoint Online, you can use the co-authoring functionality provided by Office Web Apps, such as Word Web App, Excel Web App, and PowerPoint Web App.

Co-authoring functionality in SharePoint Online addresses many of the issues faced by users wanting to work on documents at the same time as their co-workers. This functionality helps to solve and simplify many typical document-collaboration scenarios, such as:

- Two or more authors are working on different sections of a document simultaneously. Each author wants to work on his or her section of the document while other authors work on their sections – and that each wants to do this without affecting the other authors.
- Several authors are working on a PowerPoint slide show, where each author wants to add slides to the presentation and make changes to them, rather than working on separate PowerPoint presentations and attempting to merge them together to make them look consistent at the end.
- A document is sent out for review to several technical editors and copy editors, each of whom will add their own edits and comments, but the final reviewed document needs to contain all the edits and comments in one centralized and controlled version.

Planning Considerations for Co-authoring in SharePoint Online

When you plan to implement co-authoring in SharePoint Online, there are several things you need to consider first:

- *Permissions.* If you want multiple users to work on the same document you will need to grant them edit permissions on the document library that stores the documents they will work on.
- *Versioning level.* SharePoint Online uses the **Version History** feature to keep track of changes to a document and store multiple versions of it. However, you need to enable this feature as it is disabled by default in SharePoint Online. You can either use major versioning, which keeps versions such as 1.0, 2.0, 3.0, and so on, or you can use minor versioning, which keeps versions such as 1.1, 1.2, 1.3, 2.0, 2.1, and so on. This setting is configured at the document library level in **Library Settings**, then **Versioning settings**.
- *Number of versions.* You can limit the number of versions that are stored in the version history for a document if you need to control the amount of storage space being used by having multiple versions of your documents. This setting is configured at the document library level in **Library Settings**, then **Versioning settings**.
- *Check out.* If a user wants to edit a document, you can configure the versioning settings for the document library to require that the user checks out the document first. This locks the document so that other users cannot edit it at the same time. This provides you with more control but also prevents co-authoring, so you need to think about how you want your users to collaborate on documents in your document libraries. This setting is disabled by default in SharePoint Online. The **Require Check Out** setting is configured at the document library level in **Library Settings**, then **Versioning settings**.
- *Content approval.* This setting specifies whether submissions to changes on existing documents or the submission of new documents are required to remain in a pending state until an approver approves

them. This can be useful in document libraries that contain sensitive information such as marketing materials or human resources documentation and helps to apply a consistent level of accuracy, quality, and security to your content. The **Content Approval** setting is configured at the document library level in **Library Settings**, then **Versioning settings**.

Co-Authoring Support in SharePoint Online

The following Office application versions are supported for co-authoring with SharePoint Online:

- Excel Web App
- OneNote 2013
- OneNote Web App
- OneNote 2010
- PowerPoint 2013
- PowerPoint Web App
- PowerPoint 2010
- Visio 2013
- Word 2013
- Word Web App
- Word 2010

Co-Authoring in Mixed Office Environments

There may be situations where an organization has users who collaborate on documents but use a mixture of Office versions. In these scenarios co-authoring is supported by SharePoint Online in different ways:

- *Co-authoring in Office 2007 environments.* In this scenario users who have Word 2007 and PowerPoint 2007 are able to share and edit documents stored in a document library in SharePoint Online, but they cannot use co-authoring functionality to work on these documents at the same time. If a user of Word 2007 or PowerPoint 2007 opens a document currently being edited by another user, they will see a message stating that the document is being used and they will not be able to edit it. If a Word 2007 or PowerPoint 2007 user opens a document to edit it, then the document becomes locked and other users will not be able to edit it. This includes Office 2013 users attempting to open it using co-authoring functionality.
- *Co-authoring in Office 2010 environments.* In this scenario, users who have Word 2010 and PowerPoint 2010 can use co-authoring functionality to work on documents alongside Office 2013 users. However, although co-authoring is supported between these Office versions, users of Office 2013 applications get an improved co-authoring experience compared to users of older Office versions.
- *Co-authoring in Excel.* This scenario is very different to Word and PowerPoint because Excel 2013 does not support co-authoring workbooks in SharePoint Online at all. However, co-authoring of workbooks in SharePoint Online is supported by the Excel Web App, which is included with Office Web Apps, as long as everyone collaborating is using the Excel Web App. In fact, if another user opens a workbook in Excel 2010 or Excel 2013, co-authoring in Excel Web App will become disabled for that workbook while it is open in the application.
- *Co-authoring in mixed OneNote environments.* OneNote 2010 and OneNote 2013 are both backward compatible with OneNote 2007 and therefore support co-authoring with OneNote 2007 users.

However OneNote notebooks must be saved in the OneNote 2007 file format in order for OneNote 2007, OneNote 2010, and OneNote 2013 users to collaborate on it. If users upgrade to the OneNote 2013 file format, they gain some key benefits, including OneNote Web App compatibility, which enables users who do not have a local copy of OneNote installed to edit and co-author OneNote notebooks.



For information on improvements to the co-authoring experience in Office 2013, see the following link:

<http://go.microsoft.com/fwlink/?LinkId=390904>

Plan for OneDrive for Business

OneDrive for Business is a private library for the storage, organization, and sharing of users' work documents. It is an integral component of a user's Office 365 online environment, and is provided to each of your organization's users through its subscription to SharePoint Online in Office 365. If you get OneDrive for Business through your organization's subscription to Office 365, then you get 25 GB of personal storage space by default; however, if your OneDrive for Business library is hosted on an on-premises SharePoint server, then your storage space is allocated and controlled by your SharePoint administrators.

- OneDrive for Business
 - Private library for the storage, organization, and sharing of users' work documents
 - Share with "Everyone" or specific users
 - Provided with some Office 365 plans
 - Not the same as consumer OneDrive but called "OneDrive" in UI
- Sync OneDrive for Business to local computer
 - SYNC>Sync now
 - Resyncs automatically when back online
- Set storage quotas on OneDrive for Business folders
 - 25GB, 50GB, 100GB, 250GB, 500GB or 1000GB

Your files stored in OneDrive for Business are initially only visible to you, but you can share them with your co-workers if you need to. You can either share a file with everyone in the organization by simply locating it in the **Shared with Everyone** folder, or you can share a file with specific co-workers by using the **SHARE** option when you click the ellipsis (...) menu for a file, and then entering their names to send a sharing invitation to them.



Note: OneDrive for Business is not the same thing as OneDrive, which is a cloud-based service intended for personal storage and is provided with Microsoft accounts and Outlook.com accounts. This can be confusing because, in the Office 365 portal, the OneDrive for Business feature is actually displayed as "OneDrive" in the navigation bar.

Sync OneDrive for Business to Your Computer

You can use the OneDrive for Business feature to synchronize files in your library to a storage medium on your local computer. This enables you to take files offline to work on and then synchronize them back to your OneDrive for Business library once you are back online.

To synchronize OneDrive for Business with your local computer:

1. In the Office 365 admin center or in a SharePoint Online site page, choose **OneDrive** from the navigation bar.
2. In the top-right menu, choose **SYNC**.
3. Choose **Sync now**.
4. If prompted for an application to launch, choose **Microsoft OneDrive for Business**, then choose **OK**.

5. Sign in to your account if required.
6. On the **Ready to sync your OneDrive for Business documents?** page, click **Sync Now**.
7. Choose **Show my files...**
8. You will find your synchronized files in a **OneDrive for Business** subfolder under your username.
9. You can then work on the files locally, and any changes will be synchronized automatically with your OneDrive for Business library when you go back online.

Manage the Storage Quota for OneDrive for Business Libraries

In SharePoint Online, each user is allocated 25 GB of storage space on OneDrive for Business by default. This storage is on top of the storage pool allocated to the tenant. If users start to outgrow their default allocated storage on OneDrive for Business, perhaps because they store numerous large video files, you can increase their storage allocation in OneDrive for Business. However, you are limited to specifying the 25 GB standard, or increasing it to 50 GB, or increasing it to a maximum of 100 GB – this extra storage will be taken from the tenant’s main storage pool.

When users are close to reaching their allocated OneDrive for Business limit, they will receive an alert email message informing them of that fact. The email notification gives the user information about their own storage usage and provides recommendations on how to reduce it. Additionally, if a user reaches the OneDrive for Business limit they will receive another email message informing them. At this point, the user would need to contact a SharePoint Online administrator to request more storage.

To modify OneDrive for Business storage limits:

1. In the Office 365 admin center, choose **Admin**, and then **SharePoint**.
2. In the left-hand side, choose **OneDrive for Business**.
3. Enter and select the names and/or email addresses for the users whose OneDrive for Business storage quotas you want to change. You can select a maximum of 25 users.
4. As you verify each user, it displays their current individual usage in a table.
5. In the **Change storage limit to:** dropdown list, select either **25 GB**, **50 GB**, or **100 GB** as the storage value to allocate to each selected user.
6. Save your settings.

 **For more information on OneDrive for Business, see the following link:**

<http://go.microsoft.com/fwlink/?LinkId=390905>

 **For more information on managing the limits on OneDrive for Business libraries, see the following link related to software boundaries and limits for SharePoint Online:**

<http://go.microsoft.com/fwlink/?LinkId=524350>

Lab: Configuring SharePoint Online

Scenario

With the deployment of Office 365 now in full swing and the excitement of the Exchange Online cutover migration behind them, the management team at Lucerne Publishing is looking to implement the other services in the Office 365 portfolio. The company definitely wants to adopt some of the features in SharePoint Online, including social media capabilities such as Yammer. Again, Heidi is heading up this effort to configure site collections, Yammer, and OneDrive for Business. She begins by creating site collections, both through the SharePoint Online user interface and PowerShell.

Objectives

To provide the students with the experience of planning, setting up, and configuring SharePoint Online.

Lab Setup

Estimated Time: 70 minutes

Virtual machine: 20346C-LUC-CL1

Username: **Student1**

Password: **Pa\$\$w0rd**

Where you see references in the steps to `lucernepublishingXXXX.onmicrosoft.com`, you should replace XXXX with the unique Lucerne Publishing number that you are assigned when you set up your Office 365 accounts in Module 1, Lab 1B, Exercise 2, Task 3, Step 5.

Where you see references to `labXXXXX.o365ready.com`, you should replace XXXXX with the unique O365ready.com number you are assigned when you registered your IP address at `www.o365ready.com` in Module 2, Lab 2B, Exercise 1, Task 2, Step 6.

Exercise 1: Create SharePoint Site Collections

Scenario

After the excitement of the successful Exchange Online cutover migration, Heidi is settling down to review the deployment of SharePoint Online. The company does not plan to replace its existing on-premises document management environment, but wants to use SharePoint Online to connect more easily with associates, partners, and suppliers. Consequently, Heidi starts off by creating site collections, both with SharePoint admin center and with PowerShell. She works with Rick Torres to validate access rights to these sites.

The main tasks for this exercise are as follows:

1. Create Site Collections in the SharePoint Online Admin Center
2. Create a Site Collection with PowerShell
3. Verify and Use Site Collections
4. Upload Documents to a Site Collection

► Task 1: Create Site Collections in the SharePoint Online Admin Center

1. On your host computer, ensure you are logged into the **20346C-LUC-CL1** virtual machine as **Student1** with a password of **Pa\$\$word**.
2. In **LUC-CL1**, click **Desktop**, in the Task bar, click Internet Explorer and browse to **<https://login.microsoftonline.com>**.

3. Sign in as **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number) with a password of **Pa\$\$w0rd**.
4. In the **Office 365 Admin** console, click **Admin**, then click **SharePoint**.
5. On the left-hand side, click **Site collections**.
6. In the ribbon, in the **Contribute** section, click **New**, and then **Private Site Collection**.
7. In the **Title** box, type **Publishing Sales**.
8. In **Web Site Address** box, leave the first address as **https://lucernepublishingXXXX.sharepoint.com**, where XXXX is your unique Lucerne Publishing number).
9. Leave the second box as **/sites/**.
10. In the third box, type in **PubSales**.
11. Under **Select a template**, select **Team Site**.
12. In the **Administrator** box, type **Justin**, and then click the **Check names** button.
13. In the **Storage Quota** box, type **500**.
14. Click **OK**.
15. Wait for the site collection to be created, which may take about 10 minutes.
16. In the ribbon, in the **Contribute** section, click **New**, and then **Private Site Collection**.
17. In the **Title** box, type **External User Share**.
18. In the final **Web Site Address** box, type **ExtShare**.
19. Under **Select a template**, select the **Enterprise** tab, then select **Document Center**.
20. In the **Administrator** box, type **Justin**, and then click the **Check names** button.
21. In the **Storage Quota** box, type **1000**.
22. Click **OK**.
23. Wait for the site collection to be created, which may take about 10 minutes.
24. In the top-right corner, click **Heidi Leitner**, then **Sign Out**.
25. Close Internet Explorer.

► Task 2: Create a Site Collection with PowerShell

1. The **SharePoint Online Management Shell** is a tool that contains a Windows PowerShell Module to manage your SharePoint Online subscription in Office 365.

To install the SharePoint Online Management Shell, you must first download it from the **Microsoft Download Center**. To do so, open a new Internet Explorer tab and browse to **<http://www.microsoft.com/en-us/download/details.aspx?id=35588>**.

2. On the **SharePoint Online Management Shell** download page, in the **Select Language** drop-down box, select your appropriate language, and then click **Download**.
3. On the **Choose the download you want** page, select the check box for the **64 bit version**; the file name is **sharepointonlinemanagementshell_3716-1200_x64_en-us.msi**. Click **Next**.
4. If a message about pop-ups appears, click **Allow once**.

5. In the Internet Explorer dialog box asking whether you want to run or save the file, click **Run**.
6. In the **SharePoint Online Management Shell Setup** page, select the **I accept the terms in the License Agreement** checkbox, and click **Install**.
7. If a **User Account Control** dialog box appears, click **Yes**.
8. When the installation completes, click **Finish**.
9. Click **Start**, type **sharep**, right-click **SharePoint Online Management Shell** and then click **Run as administrator**.
10. In the **User Account Control** dialog box, click **Yes**.
11. At the prompt, type the following command and press Enter (where XXXX is your unique Lucerne Publishing number and XXXXX is your unique O365ready.com number):

```
Connect-SPOService -Url https://lucernepublishingXXXX-admin.sharepoint.com -
credential hleitner@labXXXXX.o365ready.com
```

12. In the **Enter your credentials** dialog box, in the **Password** box, type **Pa\$\$w0rd**.
13. Click **OK**.
14. At the prompt, type the following command and press Enter (where XXXX is your unique Lucerne Publishing number and XXXXX is your unique O365ready.com number):

```
New-SPOSite -Url https://lucernepublishingXXXX.sharepoint.com/sites/AcctsProj -Owner
jmuller@labXXXXX.o365ready.com -StorageQuota 500 -NoWait -Template PROJECTSITE#0 -
Title "Accounts Project"
```

15. At the prompt, type the following command and press Enter:

```
Exit
```

► Task 3: Verify and Use Site Collections

1. In **LUC-CL1**, on the Desktop, right-click **Internet Explorer** on the Task Bar and click **Start InPrivate Browsing**.
2. Browse to **https://login.microsoftonline.com**.
3. Sign in as **rtorres@labXXXXX.o365ready.com**, (where XXXXX is your unique O365ready.com number) and a password of **Pa\$\$w0rd**.
4. In the same **InPrivate session** of Internet Explorer, press Ctrl+T to open a new tab and browse to **https://lucernepublishingXXXX.sharepoint.com/sites/PubSales**, (where XXXX is your unique Lucerne Publishing number).
5. Note the **You need permission to access this site** message, and that you need to send an access request for permission to view the site.
6. Click **Start**, then on the **Start** page, click **Internet Explorer** to start a modern browser session.
7. Navigate to **https://login.microsoftonline.com**.
8. Sign in as **jmuller@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number), with a password of **Pa\$\$w0rd**.
9. If prompted for your **Language**, click **English (United States)** and select **(UTC) Coordinated Universal Time** as the time zone, then click **Save**.

10. In the **modern browser**, press **Ctrl+T** to open a new tab and browse to **https://lucernepublishingXXXX.sharepoint.com/sites/PubSales**, (where XXXX is your unique Lucerne Publishing number).
11. In the top-right corner, click the **Settings** icon (the cog), and then click **Site settings**.
12. Under **User and Permissions**, click **Site permissions**.
13. Click **Publishing Sales Members**.
14. Click **New**, then click **Add Users**.
15. In the text box at the top, type **rick** and then click **Rick Torres**.
16. Click **Share**.
17. In the **modern browser** tab, browse to **https://lucernepublishingXXXX.sharepoint.com/sites/ExtShare**, (where XXXX is your unique Lucerne Publishing number).
18. In the top-right corner, click the **Settings** icon (the cog), and then click **Site settings**.
19. Under **User and Permissions**, click **Site permissions**.
20. Click **External User Share Owners**.
21. Click **New**, then click **Add Users**.
22. In the text box at the top, type **elisabeth** and then click **Elisabeth Labrecque**.
23. Click **Share**.
24. Press **Ctrl-F4** to close this tab only.
25. Press the Windows key and click **Desktop**.
26. Switch to Rick Torres' Office 365 logon.
27. In Internet Explorer, open a new tab and browse to **https://lucernepublishingXXXX.sharepoint.com/sites/PubSales**, (where XXXX is your unique Lucerne Publishing number).
28. Verify that you can access the site.
29. Close the current tab.
30. In the Task Bar, right-click the **Internet Explorer** icon and click **Internet Explorer**.
31. In the desktop session, browse to **https://login.microsoftonline.com**.
32. Sign in as **elabrecque@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number), with a password of **Pa\$\$w0rd**.
33. Press **Ctrl-T** to open a new tab and browse to **https://lucernepublishingXXXX.sharepoint.com/sites/ExtShare**, (where XXXX is your unique Lucerne Publishing number).
34. Verify that you can access the site.

► **Task 4: Upload Documents to a Site Collection**

1. Click **Upload a Document**.
2. Click **Browse**.
3. Navigate to **E:\Labfiles\Lab08** and select the first of these documents:

- **Company Profile.docx**
 - **Sales Fact Sheet.docx**
 - **Sales Proposal.docx**
4. Click **Open**.
 5. Click **OK**.
 6. In the **Documents** dialog box, click **Check In**.
 7. Repeat steps 1 to 6 for the remaining documents in the list above.
 8. Refresh the **External User Share** page.
 9. In the left navigation click **Documents**.
 10. Verify that there are three documents listed.
 11. In the top-right corner, click **Elisabeth Labrecque**, then **Sign Out**.
 12. Close the desktop instance of Internet Explorer.

Results: Lucerne Publishing has created site collections and configured external access.

Exercise 2: Configure External User Sharing

Scenario

Because partners and associates need to access some of the Lucerne Publishing sites, Heidi must configure external access to the site collections so that associates and partners can connect. She uses her personal external email address to test access rights and connectivity to the share.

The main tasks for this exercise are as follows:

1. Configure a Site Collection for External User Sharing
2. Verify External User Sharing

► Task 1: Configure a Site Collection for External User Sharing

1. Press the Windows key and in the Start page, click **Internet Explorer**.
2. If you are not logged in as **Heidi Leitner**, sign out and sign in as **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number) with a password of **Pa\$\$w0rd**
3. In the **Office 365 Admin** console, click **Admin**, and then click **SharePoint**.
4. On the left-hand side, click **Site Collections**.
5. Select the check box for the **https://lucernepublishingXXXX.sharepoint.com/sites/ExtShare** site collection, (where XXX is your unique Lucerne Publishing number).
6. In the ribbon, in the **Manage** section, click **Sharing**.
7. In the **Sharing** dialog box, click **Allow both external users who accept sharing invitations and anonymous guest links**.
8. Click **Save**.
9. Wait for the operation to complete, which may take about 10 minutes.

10. Click on Heidi Leitner's profile picture icon in the top right screen and then **Sign-Out**.
11. In Internet Explorer, press **Ctrl+T** to open a new tab and browse to **https://lucernepublishingXXXX.sharepoint.com/sites/ExtShare**, (where XXX is your unique Lucerne Publishing number).
12. Sign in as **jmuller@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number) with a password of **Pa\$\$w0rd**.
13. In the top-right corner, click **SHARE**.
14. In the **Share 'External User Share'** dialog box, type in the email address of the Microsoft Live account you used to set up Office 365 in Lab 1.
15. In the message box, type **You can now access this shared site on Lucerne Publishing**.
16. Click **SHOW OPTIONS**.
17. Under **Select a group or permission level**, in the drop-down list, select **External User Share Members [Contribute]**.
18. Click **Share**.
19. In the left navigation click **Documents**.
20. In the document list, click the ellipsis button (...) next to the document you want to share, then click **SHARE**.
21. Click **Get a link**, then under **View Only**, click **CREATE LINK**.
22. Select the link, then right-click it and choose **Copy**.
23. Click **Close**.
24. In **SharePoint Online**, click **Outlook**.
25. If prompted, select your language and time zone, and then click **Save**.
26. Click **New**.
27. In the **To** box, type the email address for your personal external email account or your Microsoft Live account.
28. In the **Subject** box, type **Shared Document**.
29. In the message box, right-click and choose **Paste**.
30. Click **SEND**.
31. In **Outlook Web App**, in the top-right corner, click **Justin Muller**, then **Sign out**.
32. Press **Alt-F4** to close the modern browser.

► **Task 2: Verify External User Sharing**

1. On the Start page, click **Internet Explorer** to open a **modern browser** session.
2. Browse to **mail.live.com**.
3. In **Microsoft account**, and **Password**, enter the email address and password you used to set up the Office 365 subscription in Lab 1.
4. Open the invitation email message from the **Microsoft Online Services Team**.
5. Click the **Go to External User Share** link.
6. Click **Microsoft account**.

7. Verify that you can access the shared site collection.
8. Click **Upload a document**.
9. In the **Add a document** dialog box, click **Browse**.
10. Click **Go up** and click **Go up** again.
11. Click **Computer**, click **Allfiles (E:)**, then click **Labfiles** and click **Lab08**.
12. Click **Sales Proposal** and click **Open**.
13. Click **OK**.
14. In the **Add a document** dialog box, in the **Name** field, enter **Sales Proposal V2**, and then click **Check In**.
15. Refresh the page and verify that your uploaded document is listed.
16. In the top-right corner, click your name, and click **Sign Out**.
17. Press **Ctrl-F4** to close the browser tab.
18. Access your personal email account and open the email message from **Justin Muller** with the subject of **Shared Document**.
19. Copy the URL in the email message into a new browser tab and press Enter.
20. Verify that the document opens in **Word Web App**, and that it is in view-only mode, and that you cannot edit it.
21. Close the browser tab.
22. Press **Alt-F4** to close the modern browser session.

Results: Heidi has configured external user access to external SharePoint sites in Office 365.

Exercise 3: Configure Social and Collaboration Features

Scenario

Lucerne Publishing is now ready to implement internal social networking tools. This initiative is being implemented at the request of Jesse Wagner, the COO, who is anxious to connect employees and associates together and improve collaboration on time-sensitive projects. By having Yammer open, employees and associates can keep track of what's developing within a project without having to send email messages or reply to instant messages. Here Heidi sets up Yammer, configures version control, and sets quotas on OneDrive.

The main tasks for this exercise are as follows:

1. Configure Yammer in SharePoint Online
2. Configure Versioning Settings for Co-authoring
3. Configure OneDrive for Business

► Task 1: Configure Yammer in SharePoint Online

1. On the **Start** page, click Internet Explorer and browse to **https://login.microsoftonline.com**.
2. Sign in as **hleitner@labXXXXX.o365ready.com**, (where XXXXX is your unique O365ready.com number) with a password of **Pa\$\$w0rd**.

3. In the **Office 365 admin center**, click **Admin**, and then click **SharePoint**.
4. In the **SharePoint admin center**, click **Settings**.
5. Under **Enterprise Social Collaboration**, select **Use Yammer.com service**.
6. Click **OK**.
7. It will take some time for the change to take effect.
8. In the **Office 365 admin center**, click **Admin** and click **Office 365**.
9. Verify that the blue Office 365 navigation menu bar at the top of the page now displays **Yammer** instead of Newsfeed.

Note: If the menu bar has not yet updated to display Yammer, try refreshing the page or navigating to another page and then back to the Sites page again. Alternatively, if it is taking longer than expected, continue with the rest of the lab exercises and come back to verify this step later in the lab.

10. Click the **Get information on Yammer** link.
11. A new Internet Explorer page appears, displaying the **Yammer Sign-up** page.
12. Close the new Internet Explorer page.

► Task 2: Configure Versioning Settings for Co-authoring

1. Press the Windows key and click **Desktop**.
2. Switch to **Elisabeth Labrecque's** session in Internet Explorer.
3. In Internet Explorer, press Ctrl-T to open a new tab and browse to **https://lucernepublishingXXXX.sharepoint.com/sites/ExtShare**, (where XXXX is your unique Lucerne Publishing number).
4. On the **External User Share** page, click **Documents**.
5. Click the **LIBRARY** tab.
6. In the **Settings** section, click **Library Settings**.
7. Under **General Settings**, click **Versioning settings**.
8. Under **Document Version History**, click **Create major versions**.
9. Select the **Keep the following number of major versions** check box, and in the text box, type **5**.
10. Under **Require Check Out**, click **Yes**.
11. Click **OK**.
12. In the top-right corner, click **Elisabeth Labrecque** and then click **Sign Out**.
13. Press **Alt-F4** to close Internet Explorer.

► Task 3: Configure OneDrive for Business

1. Press the Windows key and click **Internet Explorer** to go to **Heidi Leitner's** session.
2. In the **Office 365 admin center**, click **OneDrive**.
3. On the **Welcome to OneDrive for Business** page, click **Next**.
4. In the menu bar, click **Sync**.

5. Click **Sync now**.
6. On the **Did you mean to switch apps?** banner, click **Yes**.
7. On the **Sign in** dialog box, enter **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number), and click **Next**.
8. Enter a password of **Pa\$\$w0rd**, and click **Sign in**.
9. On the **Ready to sync your OneDrive for Business documents?** page, click **Sync Now**.
10. Click **Show my files...**
11. Verify your synchronized files are in a **OneDrive for Business** subfolder under your username.
12. Close the OneDrive for Business folder.

Results: Heidi has successfully configured Yammer, OneDrive for Business, and version control.

Lab Discussion Questions

Is it mandatory to choose a template when creating a new site collection?

No, you could use the Custom tab to create an empty site collection and select a site template later.

What is the default versioning setting for a site collection in SharePoint Online?

The default versioning setting is to maintain no versions other than the original document.

- Is it mandatory to choose a template when creating a new site collection?
- What is the default versioning setting for a site collection in SharePoint Online?

Module Review and Takeaways

Now that you have completed this module you can manage SharePoint site collections, configure external user sharing, and plan a collaboration solution in Office 365.

MCT USE ONLY. STUDENT USE PROHIBITED

Module 9

Configuring Lync Online

Contents:

Module Overview	9-1
Lesson 1: Plan for Lync Online	9-2
Lesson 2: Configure Lync Online Settings	9-9
Lab: Configuring Lync Online	9-14
Module Review and Takeaways	9-21

Module Overview

In this module, students learn how to identify factors in the customer's environment that need to be reflected in the Lync® Online deployment plan, then configure Lync Online to reflect the customer's business requirements, both at the end-user level and the organization level.

Objectives

After completing this module, you should be able to:

- Plan for Lync Online.
- Configure Lync Online settings.

Lesson 1

Plan for Lync Online

In this lesson, students learn how to identify the business factors for customers wanting to use a cloud-based presence monitoring, instant messaging, and telephony solution. This information is then used to create a plan for implementing Lync Online. Planning information includes global external communications settings, enabling external access, managing Session Initiation Protocol (SIP) domains and public IM connectivity, customizing meeting invitations, and configuring push notifications.

Lesson Objectives

After completing this lesson, you should be able to:

- Describe Lync Online.
- Plan for domain federation in Lync Online.
- Plan for public IM connectivity in Lync Online.
- Plan for Lync coexistence in Lync Online.
- Plan Lync Online conferencing.

Overview of Lync Online

Lync Online helps connect your organization's users to each other from multiple devices and offers a consistent experience for presence, instant messaging, as well as voice and video conferencing. Lync Online is available as an Office 365™ stand-alone service or as a part of the Office enterprise suite.

Lync Online provides the following key features:

- *Real-time presence.* Users get availability and location information to make it easier for them to choose the best method of communication with their co-workers.
- *Instant messaging (IM).* Users can use standard text-based IM to communicate in real time with multiple users, and can also transfer files to those users.
- *Voice calls.* Users can make Lync calls to other Lync users inside and outside the organization and, if enabled, can also have calls with Skype users.
- *Planned and on-the-fly conferencing.* Users can create scheduled or spontaneous audio and video conference calls online with internal and external users.
- *Enhanced presentations.* Users can enhance their online presentations by using the screen-sharing, application-sharing, and virtual whiteboard features of Lync Online.
- *Lync domain federation.* Users can communicate and collaborate with co-workers and customers who use Lync or Skype in external domains.

- Real-time presence
- Instant messaging (IM)
- Voice calls
- Planned and on-the-fly conferencing
- Enhanced presentations
- Lync domain federation
- Multiple Lync Online clients available

Clients for Lync Online

The following Lync Online clients can be used with Office 365:

- *Lync 2013 for Office 365 client.* This most recent client provides full access to Lync presence, instant messaging, and conferencing capabilities. It includes enhanced features not available with Lync 2013 Basic, such as multiparty video (gallery view), OneNote® meeting notes, recording, and calendar delegation.
- *Lync 2013 Basic.* This is a locally-installed client that provides a scaled-down set of Lync presence, instant messaging, and conferencing features based on the capabilities provided in the subscription plan. However, Lync Basic does not provide the same enhanced features as the full Lync 2013 client described above. The Office 365 administration portal contains information about how to download the current version of Lync Basic.
- *Lync 2010 for Office 365 client.* The Lync 2010 client is still supported for Lync Online but the version acquired as part of an Office 365 subscription must be upgraded to the Lync 2013 Basic client by April 8, 2014. Lync 2010 clients acquired as part of Office Professional Plus 2010 do not have this same upgrade requirement.
- *Lync Windows Store App.* This is a Lync app, optimized for touch, that has been designed specifically for Windows® 8 and Windows RT. Users can download this app through the Windows Store.
- *Lync Web App.* The web-based Lync Web App client offers users IM in meetings, enhanced application and desktop-sharing, whiteboard, and presenter access controls. In addition, Lync Web App now includes PC-based audio and video. Lync Web App is designed mainly for external users who are invited to Lync Meetings and employees not using their usual computer during a meeting. Lync Web App supports Windows and Macintosh operating systems but other operating systems are not supported.
- *Lync mobile clients.* Lync apps for mobile clients extend Lync features to users' mobile devices. Lync apps provide voice and video over wireless connections, rich presence, instant messaging, conferencing, and calling features from a single interface. Lync 2013 apps are available for Windows Phone and iOS (iPhone/iPad). A Lync 2010 app is available for Android.
- *Lync for Mac 2011.* This client provides users of the Mac platform with integrated presence, IM, conferencing, and audio/video capabilities as well as desktop, application, and file sharing. It works with both Lync Server 2013 and Lync Online.
- *Lync for iPad.* This latest app brings Lync presence, IM, joining a conference and viewing shared meeting content, and voice and video capabilities to the Apple iPad.

- Lync 2013 for Office 365 client
- Lync 2013 Basic
- Lync 2010 for Office 365 client
- Lync Windows Store App
- Lync Web App
- Lync mobile clients
- Lync for Mac 2011
- Lync for iPad



For more information on the available Lync features for different clients go to:

<http://go.microsoft.com/fwlink/?LinkId=391776>



For more information on the available Lync features for different mobile device platforms go to:


<http://go.microsoft.com/fwlink/?LinkId=391777>

Lync Online and On-Premises Comparison

Lync Online and Lync 2013 on-premises offer broadly the same features but with certain minor differences. You need to understand these differences so that you are able to evaluate whether Lync Online is right for your company. However, rather than list all the features, this topic simply highlights the differences between Lync Server 2013 and Lync Online Plan 2/Office 365 E3.

Feature	Lync 2013	Lync Online
My Picture: URL Photo Experience	Yes	No
Persistent Chat	Yes	No
Media path optimization	Yes	No
Network QoS - DSCP	Yes	No
XMPP	Yes	No
AOL and Yahoo! Federation	Yes	No
Dial-in PSTN Conferencing via Certified ACP	No	Yes
Create public meetings with static IDs from Outlook	Yes	No
IM and File Filtering	Yes	No
Application Sharing, and Desktop Sharing Archiving	Yes	No
UM interoperability with Exchange Server	Yes	No
UM interoperability with Exchange Online	Yes	No
Archiving interoperability with Exchange Server	Yes	No
Skill Search with SharePoint Server	Yes	No
Admin through Office 365 Portal	No	Yes

Feature	Lync Server 2013	Lync Online
My Picture: URL Photo Experience	Yes	No
Persistent Chat	Yes	No
Media path optimization	Yes	No
Network Quality of Service (QoS) – Differentiated Services Code Point (DSCP)	Yes	No
XMPP (used by Google Talk, for example) and Sametime federation	Yes	No
AOL and Yahoo! federation	Yes	No
Dial-in PSTN Conferencing via Certified Audio Conferencing Provider (ACP)	No	Yes
Create public meetings with static meeting IDs from Outlook	Yes	No
IM and File Filtering	Yes	No
Application Sharing, and Desktop Sharing Archiving	Yes	No
Unified Messaging interoperability with Exchange Server	Yes	No
Unified Messaging interoperability with Exchange Online	Yes	No (but available with Lync Plan 3/Office 365 E4 level)
Archiving interoperability with Exchange Server	Yes	No
Skill Search with SharePoint Server	Yes	No
Admin through Office 365 Portal	No	Yes

 **Note:** The Lync Online Plan 3 includes Enterprise Voice, which can be used to replace PBX systems with Lync Server 2013 on-premises.

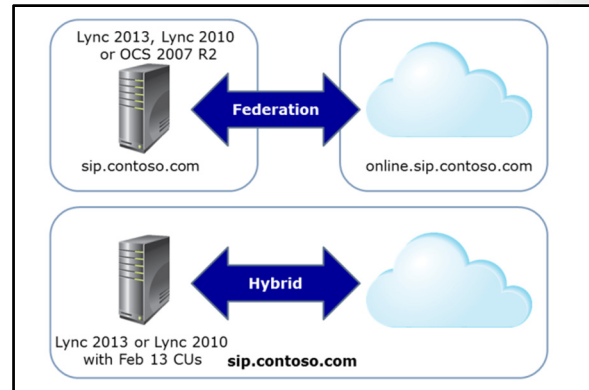
 **For a complete feature list, see the following link:**

<http://go.microsoft.com/fwlink/?LinkId=400792>

Lync Federation and Co-Existence

Lync Online can work in different ways with a Lync on-premises implementation. The two options are federation and hybrid co-existence.

With Federation, Lync Online and the on-premises environment have different SIP domains. For example, the on-premises SIP domain might be sip.contoso.com and the Lync Online SIP domain, online.sip.contoso.com. You would then configure a Lync federation relationship between sip.contoso.com and online.sip.contoso.com. This federation relationship is described in the next topic and is a simple process.



With hybrid co-existence, the Lync on-premises environment and Lync Online share the same SIP domain, so user addresses for both online and on-premises Lync implementations will end in sip.contoso.com.

Hybrid Lync requires the following infrastructure additions:

- Directory synchronization (DirSync).
- Single sign-on through Active Directory Federation Services (AD FS).
- A Lync Server 2013 or Lync Server 2010 with Feb 13 cumulative updates.
- The latest Office 365 tenant release running Lync Online 2013.
- Lync Server 2013 administrative tools.

 **For more information on planning hybrid Lync implementations, see the following link:**

<http://go.microsoft.com/fwlink/?LinkId=400791>

Plan for Domain Federation

Domain federation in Lync Online enables your users to communicate with Lync users in other organizations. You can enable domain federation with other external domains; you can set up domain federation with your on-premises domain. To set up domain federation between Lync Online with your own on-premises implementation of Lync, the two environments must use separate SIP domains.

Domain federation is disabled by default, but when you do enable it, you can choose either of the following options:

- Enable domain federation for all domains except those that you explicitly add to the blocked domains list.
- Enable domain federation only for the domains you explicitly add to the allowed domains list.

Once federation has been enabled between domains, users in those domains can participate in IM chat sessions and audio and video calls; users will be able to see presence information about each other.



Note: Lync domain federation should not be confused with Lync coexistence, which is something that Microsoft Online Services is working to make available in the future to Office 365 users. Coexistence will enable domains to share the same SIP domain. It will also provide greater functionality than is available through domain federation, such as split features between on-premises and online Lync environments, and the use of an integrated global searchable address book.

- Enables users to communicate with external users or with on-premises Lync implementations
 - Requires separate SIP domains
- Disabled by default:
 - Enable for all but listed blocked domains
 OR
 - Enable for only listed allowed domains
- Not the same as Lync coexistence

Plan for Public IM Connectivity

If you want to enable your organization's users to communicate with users in external organizations by using Lync, or even Skype, you need to enable public IM connectivity. Public IM connectivity is disabled by default in Lync Online, but you can either enable or disable public it for the whole company using the **organization** setting in Lync Online. With the users setting, you can also enable or disable it for an individual user.



Note: Public IM connectivity in Lync Online only supports public IM connectivity with Lync or Skype users; it does not support other public IM networks such as AOL Instant Messenger or Yahoo Messenger.


- Enables users to communicate using IM with other public IM networks
 - Lync
 - Skype
- Disabled by default
 - Enable or disable for entire organization – **organization** settings
 - Enable or disable for individual users – **users** setting
- Does not support AOL/Yahoo

Plan for Lync Coexistence

Currently Lync does not support coexistence between an on-premises Lync Server and Lync Online with a single SIP domain. This means that you cannot deploy some users in Lync Online, and some users on-premises, and then split different Lync features between them.

You need to deploy Lync Server in your on-premises environment if you want to deploy Lync to both Office 365 users and on-premises users. You will then need to decide which users will be homed to your Lync Online implementation and which to your on-premises Lync Server, based on the features required by individual users.

- Coexistence not yet supported between Lync Online and Lync Server in same SIP domain
 - Cannot split users and features
- Deploy Lync Server on-premises
 - Decide which users are homed to on-premises environment and which to online environment
- Upgrade OCS 2007 to Lync Server in readiness for coexistence features in future Lync offerings

 **Note:** Coexistence between Lync Server on-premises and Lync Online is not supported at the time of this writing. If you are planning to take advantage of Lync coexistence capabilities when they do become available, and your current on-premises implementation uses Office Communications Server (OCS) 2007, you should consider upgrading your on-premises implementation to Lync Server 2010 or Lync Server 2013 as Office Communications Server implementations will not be supported for Lync coexistence scenarios.

Plan for Conferencing

To prepare your environment for Lync conferencing there are some key network optimization configurations you can perform:

- Enable the required firewall ports to access the Lync Online conferencing servers.
- Disable authentication for Lync Online audio and video traffic when an authenticating HTTP proxy is used.
- Configure the network to allow User Datagram Protocol (UDP) traffic for better audio and video performance.
- Modify internal routers and optimize internal network paths for audio and video traffic.
- Filter traffic if required by the service provider's service level agreement (SLA).

- Key network optimization configurations:
 - Enable the required firewall ports
 - Disable authentication for Lync Online audio and video traffic when an authenticating HTTP proxy is used
 - Configure the network to allow UDP traffic
 - Modify routers and optimize internal network paths
 - Filter traffic if required by service provider's SLA
- Ports
 - TCP port 443/TCP port 5223 (mobile push notifications)
- Assess required network bandwidth for Lync Online conferencing features

Network Port Configuration

Lync 2010 clients normally use TCP port 5061 for network communications in an on-premises environment. However, when clients are configured for Lync Online, they use TCP port 443, which is a more commonly available port on customer firewalls, routers, and proxies. Lync Online also uses TCP port 5223 for Lync mobile push notifications.

 **For detailed information on the protocols and ports used by Lync Online in Office 365, go to:**

<http://go.microsoft.com/fwlink/?LinkId=391778>

Bandwidth Requirements for Office 365

You should carry out a comprehensive assessment of the required network bandwidth for Lync Online and its conferencing features, as these services may necessitate an increase in the required bandwidth.



For information on the required bandwidth for Lync conferencing, go to:

<http://go.microsoft.com/fwlink/p/?LinkID=243579>



For general information on Internet bandwidth usage for Office 365 services, go to:

<http://go.microsoft.com/fwlink/?LinkId=391779>

Lesson 2

Configure Lync Online Settings


In this lesson, you will learn how to configure Lync Online settings for end users, including turning off non-archived features for compliance, configuring presence, configuring the availability of Lync features, configuring per-user external communication, and configuring dial-in conferencing settings. You will also learn how to configure Lync Online organizational settings, including presence privacy mode, mobile phone notifications, domain federation, and public IM connectivity.

Lesson Objectives

After completing this lesson, you should be able to:

- Configure Lync Online user settings by using the Lync Online admin center.
- Configure Lync Online organizational settings by using the Lync Online admin center.
- Configure Lync Online settings by using Windows PowerShell®.

Configuring Lync Online User Settings

You can configure several settings for individual or multiple users by using the Lync admin center. Under **users**, you select the user or users in the list and then click the  (Edit) button. From here, you can change several Lync user options.

Configuring Lync User General Settings

The following settings can be configured in the **General** section:

- *Audio and video*. This enables you to select one of four options for audio and video capabilities:
 - None
 - Audio only
 - Audio and video
 - Audio and HD video
- *Record conversations and meetings*. This setting defines whether or not a user is allowed to use the record option to record meetings.
- *Allow anonymous attendees to dial out*. This enables an unauthenticated meeting attendee to be called by the conferencing service instead of having to dial in directly to the service.
- *For compliance, turn off non-archived features*. This setting turns off the features that are not archived when your organization implements the in-place hold feature of Exchange. You should use this option if your organization is legally bound to archive electronically-stored data.
- Configuring Lync User External Communications Settings

- General settings
 - Audio and video
 - Record meetings
 - Compliance features
- External communications settings
 - Lync users
 - Skype users
- Dial-in conferencing settings
 - Provider, Toll numbers, Passcode

External communications are typically configured at the organizational level to enable users to communicate with users outside the organization who either also use Lync Online or the Skype public IM service. However, Lync Online does enable you to configure this setting on a per-user basis.

The following settings can be configured in the **External communications** section:

- Choose people outside your organization that the user can communicate with:
 - Lync users
 - People on public IM networks

Configuring Lync User Dial-In Conferencing Settings

The following settings can be configured in the **Dial-in conferencing** section:

- *Provider name.* This enables you to choose your audio conferencing provider from the list. At the time of this writing, the available providers include:
 - *Intercall*
 - *BT Conferencing*
 - *PGi*
- *Toll number and toll-free number.* These are the phone numbers supplied to you by the audio conferencing provider. The numbers you enter here appear in the same format in Lync Meeting requests. The toll number is a required setting, but the toll-free number is optional.
- *Passcode.* This is the code that meeting participants enter when they join meetings scheduled by this particular user.



Note: When editing user settings and selecting more than one user in the user list, the **Dial-in conferencing** option is not available; it is only displayed when you edit an individual user.

Configure Lync Online Organizational Settings

There are several settings that can be configured for Lync Online at the organizational level. These are configured under the **organization** section in Lync admin center.

Configure General Organizational Settings

The following organizational settings can be configured in the **General** section:

- *Presence privacy mode.* This defines whether or not your users' presence information is shown to everyone who they communicate with, or just to their own contacts. The options include:
 - Automatically display presence information (default)
 - Display presence information only to a user's contacts

- General settings
 - Presence privacy
 - Mobile phone notifications
- Meeting invitations
 - Customize for your organization (logo, help, legal)
- External communications
 - External access
 - All but blocked domains
 - Only allowed domains
 - Public IM connectivity
 - Skype only

- *Mobile phone notifications.* This setting enables alerts for items such as incoming IMs, voicemails, and missed calls and IMs through push notifications from one or both of the following services:
 - Microsoft PUSH Notification Service
 - Apple Push Notification Service

Configure Meeting Invitations

In the **Meeting invitation** section you can configure customized Lync meeting invitations for your organization using the following:

- *Logo URL.* The logo that the URL points to must be a JPG or GIF image which is a maximum of 188 pixels wide by 30 pixels high.
- *Help URL.* This would point to your organization's support website.
- *Legal URL.* This would point to a website containing the organization's legal disclaimers.
- *Footer text.* This allows you to enter free text, such as legal disclaimer information, directly into the meeting invitation.

Configure External Communications Organizational Settings

There are two organizational settings configurable in the **External communications** section: external access and public IM connectivity.

Configure External Access

This setting enables you to control whether or not your users can communicate with other domains by federation. There are essentially three ways of configuring the setting:

- *Off completely.* This allows no federation with any external domains.
- *On except for blocked domains.* This allows federation with all domains except those that you add to the blocked domains list. When you choose this setting and click the + (Add) button, you are then asked to supply the name of a domain that uses Lync, that will be blocked from communicating with your users.
- *On only for allowed domains.* This allows federation only with the domains you add to the allowed list, and blocks federation with all other domains. When you choose this setting and click the + (Add) button, you are then asked to supply the name of a domain using Lync that will be allowed to communicate with your users.



Note: In order for the federation to work, the other domain that your users want to communicate with must also enable domain federation with your domain.

Lync communications between the users in the federated domains are restricted to Lync Online features that both organizations support. Therefore, if your organization supports video conversations but the other domain does not, your users will not be able to start video conversations with users in that federated domain.

Configure Public IM Connectivity

This setting controls whether or not your users are able to communicate using IMs and audio and video calls with users who are using public IM service providers; specifically Skype, at the time of this writing.

You must enable some form of domain federation if you want to support communication with Skype contacts through public IM connectivity.

Skype Connectivity

At the time of this writing, the following functionality is supported for Skype users who sign in with a Microsoft Account:

- *Available.*
 - Presence
 - Person-to-person instant messaging
 - Person-to-person audio calls
 - Find and add Lync contacts in Skype
 - Add Skype contacts in Lync
- *Not available in Skype.*
 - Video conversations
 - Multi-party instant messaging
 - Audio and video conversations with more than two people
 - Desktop and program sharing



For more information on current and future support for Lync and Skype connectivity, go to:

<http://go.microsoft.com/fwlink/?LinkId=392269>

Configure Lync Online with Windows PowerShell

With the version of Lync Online released in June 2013, Office 365 administrators can now manage their Lync Online implementation and user accounts using Windows PowerShell. Everything you can do to administer and configure Lync Online using the Lync admin center, you can do by using Windows PowerShell.

As a result, whether you decide to use the Lync admin center or Windows PowerShell to manage Lync Online is your personal preference. That being said, Windows PowerShell does offer some advantages over the Lync admin center:

- Some tasks can only be performed by using Windows PowerShell.
- More experienced users can use Windows PowerShell to organize multiple Windows PowerShell commands into scripts and then use these scripts to automate and speed up repetitive tasks.

In order to manage Lync Online with Windows PowerShell, the computer you are using must have the following installed:

- *Windows PowerShell 3.0.* This is already pre-installed on the Windows Server 2012, Windows Server 2012 R2, Windows 8, and Windows 8.1 operating systems.
- *Microsoft Online Services Sign-In Assistant.* This provides sign-in and authentication functionality for Office 365 applications, including Lync Online. This can be downloaded from the Microsoft Download Center at <http://go.microsoft.com/fwlink/?LinkId=401134>.

- Required for Lync Online Management
 - Windows PowerShell 3.0
 - Microsoft Online Services Sign-In Assistant
 - Windows PowerShell Module for Lync Online
- Windows PowerShell Cmdlets for Managing Lync Online
 - Perform common and repetitive tasks
 - Get-CsTenant
 - Set-CsTenantFederationConfiguration
 - Set-CsMeetingConfiguration
 - Get-CSOnlineUser

- *Windows PowerShell Module for Lync Online.* This installs the Lync Online Connector module and the **New-CsOnlineSession** cmdlet to your local computer.

Windows PowerShell Cmdlets for Managing Lync Online

These are some of the more common management tasks that you might perform by using the Windows PowerShell Module for Lync Online:

- To enable or disable push notifications from either Apple iPhones or Windows Phones, you can use the **Set-CsPushNotificationConfiguration** cmdlet, which uses the **EnableApplePushNotificationService** and **EnableMicrosoftPushNotificationService** parameters.
- To return information about your Lync Online users, you can use the **Get-CsOnlineUser** cmdlet. This has several additional parameters associated with it.
- To assign an audio conferencing provider to a user, you can use the **Set-CSUserAcp** cmdlet, which uses parameters such as **-TollNumber**, **-TollFreeNumbers**, and **-ParticipantPassCode**.
- To get information about your Lync Online tenant, you can use the **Get-CsTenant** cmdlet.
- To enable or disable the ability to record online conferences, you can use the **Set-CsMeetingConfiguration** cmdlet with the **-AllowConferenceRecording** parameter. This cmdlet has many parameters associated with it to enable you to perform fine-tune configuration of your online scheduled meetings.
- To enable or disable federation with public IM providers, you can use the **Set-CsTenantFederationConfiguration** cmdlet with the **-AllowPublicUsers** parameter.
- To allow federation with all domains, you can use a variable with the **New-CsEdgeAllowAllKnownDomains** cmdlet, and then use the **Set-CsTenantFederationConfiguration** cmdlet with the **-AllowedDomains** parameter and the variable used earlier.
- To view a list of blocked domains, you can use the **Get-CsTenantFederationConfiguration** cmdlet, with the **| Select-Object -ExpandProperty BlockedDomains** parameters.
- To add a domain to the blocked domains list, you can use a variable with the **New-CsEdgeDomainPattern** cmdlet, and then use the **Set-CsTenantFederationConfiguration** cmdlet with the **-BlockedDomains** parameter and the **Add** method with the variable used earlier.

 **For more information on using Windows PowerShell to perform common administrative tasks in Lync Online go to:**

<http://go.microsoft.com/fwlink/?LinkId=391780>

 **For more information on the specific Windows PowerShell cmdlets used to administer and configure Lync Online go to:**

<http://go.microsoft.com/fwlink/?LinkId=391781>

Lab: Configuring Lync Online

Scenario

A key business goal for Lucerne Publishing is to improve collaboration between its full-time employees and its associate pool. Lync Online is a key factor in the provisioning of these facilities. As the company completes the Deploy phase of the FastTrack process, Remi, Justin, and Heidi are deciding which facilities the company requires, and they have brought in Odessa Brunner as the company's Lync expert. After much consultation, they decide that at this point in the project Lync federation will only be allowed with the litware.com domain.

Objectives

To provide students with the experience of configuring Lync Online.

Lab Setup

Estimated Time: 60 minutes

Virtual machine: 20346C-LUC-CL1

Username: **Student1**

Password: **Pa\$\$w0rd**

In all tasks, where you see references to lucernepublishingXXXX.onmicrosoft.com, replace the XXXX with the unique Lucerne Publishing number that you were assigned when you set up your Office 365 account in Module 1, Lab 1B, Exercise 2, Task 3, Step 5

Where you see references to labXXXXX.o365ready.com, replace the XXXXX with the unique o365ready.com number you were assigned when you registered your IP address at www.o365ready.com in Module 2, Lab 2B, Exercise 1, Task 2, Step 6.

Exercise 1: Configure Lync End-User Communication Settings

Scenario

Lucerne Publishing wants to investigate the effects of applying policies that restrict users from accessing various features in Lync Online. Odessa Brunner is working with Luc Cartier, Rick Torres, and Mario Ledford to demonstrate the effect of enabling and disabling Lync features.

The main tasks for this exercise are as follows:

1. Attempt to IM Someone Who Is Out
2. Verify Lync Communications
3. Configure User Settings

► Task 1: Attempt to IM Someone Who Is Out

1. In Internet Explorer, on the **Office 365 sign in** page, login as **mledford@labXXXXX.o365ready.com**, (where XXXXX is your unique o365ready.com number). Use MLedford's temporary password from Lab 2.
2. When prompted, change his password to **Pa\$\$w0rd** and click **Save**.
3. When prompted again, re-enter the new password and click **Sign in**.
4. In the **Office 365 Admin** console, click **Outlook**.
5. In **Outlook Web App**, specify your language and time zone, and click **Save**.


6. In the menu bar at the top of the page, note the grey box to the left of **Mario Ledford**, then click it.
7. **Note:** If the box shows green, continue with the steps.
8. Verify that, under his name, there is a message stating: **“There’s a problem with IM. Please try again later.”**
9. Click **Sign in to IM**.
10. Verify that nothing happens.
11. In the top-right corner, click **Mario Ledford**, and then click **Sign out**.
12. In Internet Explorer, click **Use another account**.
13. Sign in as **rschmid@labXXXXX.o365ready.com**, (where XXXXX is your unique o365ready.com number) with a password of **Pa\$\$w0rd**.
14. In the **Office 365 Admin** console, click **Outlook**.
15. In **Outlook Web App**, specify your language and time zone, and click **Save**.
16. In the menu bar at the top of the page, note the green box to the left of **Robert Schmid**, then click it.
17. Verify that there is presence information showing.
18. In the menu bar, click **People**.
19. In the **Search people** text box, type **justin** and press ENTER.
20. In the right-hand pane, under **Justin Muller**, note that he is offline, then click the **Send an instant message** button.
21. In the Internet Explorer pop-up blocker window, click **Options for this site**, and then click **Always allow**.
22. In the chat box that opens, in the bottom window, type, **Hi Justin, can you IM me when you return please**, and press ENTER.
23. Note the message stating **Your instant message couldn’t be delivered**.
24. Close the chat window.




► Task 2: Verify Lync Communications

1. In the taskbar, right-click the **Internet Explorer** icon and click **Start InPrivate Browsing**.
2. In the new Internet Explorer window, browse to **https://login.microsoftonline.com**.
3. Sign in as **jmuller@labXXXXX.o365ready.com**, (where XXXXX is your unique o365ready.com number) with a password of **Pa\$\$w0rd**.
4. In the **Office 365 Admin** console, click **Outlook**.
5. In **Outlook Web App**, in the menu bar at the top of the page, note the green box to the left of **Justin Muller**, then click it.
6. Verify that there is presence information showing.
7. Switch back to the other Internet Explorer window where **Robert Schmid** is logged in.
8. In **Outlook Web App**, refresh the page.
9. In the **Search People** text box, type **justin** and press ENTER.
10. In the right-hand pane, under **Justin Muller**, click the **Send an instant message** button.

11. In the chat box that opens, in the bottom window, type, **Hi Justin, can you IM me when you return please**, and press ENTER.
12. Switch back to the other Internet Explorer **InPrivate Browsing** window where **Justin Muller** is logged in.
13. In the **IM REQUEST** window, click **Accept**.
14. Verify that the chat box opens displaying the instant message from Robert Schmid.
15. In the bottom window of the chat box, type **I am back now if you want to come and see me**, and press ENTER.
16. Switch back to the open chat window for **Robert Schmid**, and verify that the response has come back from Justin Muller.
17. Close any open chat windows.
18. In the top-right corner, click **Robert Schmid**, and then click **Sign out**.
19. Switch back to the other Internet Explorer b window.
20. Close any open chat windows.
21. In the top-right corner, click **Justin Muller**, and then click **Sign out**.
22. Close Internet Explorer.

► Task 3: Configure User Settings

1. On your host computer, ensure you are logged into the **20346C-LUC-CL1** virtual machine as **Student1** with a password of **Pa\$\$word**.
2. On **LUC-CL1**, click the Task Bar and click **Internet Explorer**.
3. Browse to **https://login.microsoftonline.com**.
4. Sign in as **obrunner@labXXXXXX.o365ready.com**, (where XXXXX is your unique o365ready.com number) with a password of **Pa\$\$w0rd**.
5. If the **Don't lose access to your account** page appears, then enter the following information:
 - a. In **Country or Region**, select **Switzerland**.
 - b. In **Mobile phone number**, enter **5553000**.
 - c. In **Alternate user name**, enter **user@alt.none**.
 - d. Click **Save and continue**.
6. In the **Office 365 admin center**, click **Admin**, then click **Office 365**.
7. On the left-hand side, click **Users**, and then click **Active users**.
8. Select the check box for **Mario Ledford**.
9. Click the  (Edit) button.
10. In the left-hand menu, click **Licenses**.
11. Clear the **Lync Online (Plan 2)** check box.
12. Click **Save**.
13. In the **Office 365 admin center**, click **Admin**, then click **Lync**.
14. On the left-hand side, click **Users**.

15. Select the check box for **Luc Cartier**.
16. Click the  (Edit) button.
17. In the **General** section, under **Audio and video**, click the drop-down list and then click **Audio only**.
18. In the left-hand menu click **External communications**.
19. Clear the **People on public IM networks** check box.
20. Click **Save**.
21. Select the check box for **Robert Schmid**.
22. Click the  (Edit) button.
23. In the **General** section, under **Audio and video**, click the drop-down list and then click **None**.
24. Click **Save**.
25. On the left-hand side, click **Users**.
26. Select the check box for **Rick Torres**.
27. Click the  (Edit) button.
28. In the left-hand menu click **Dial-in conferencing**.
29. In the **Provider name** drop-down list, click **Intercall**.
30. In the **Toll number** box, type **555-1234**.
31. In the **Passcode** box, type **123456**.
32. Click **Save**.
33. Click **Dial-in conferencing**.
34. Click **Dial-in users**.
35. Note that Rick Torres's number and passcode shows up on the list.
36. In the left-hand side, click **Users**.
37. Verify that **Mario Ledford** is not listed as a Lync user.
38. In the top-right corner, click **Odessa Brunner**, and then click **Sign out**.
39. If necessary, close Internet Explorer to complete the logout process.

Results: Lucerne Publishing now has a Lync Online deployment correctly configured to meet the organization's business needs.

Exercise 2: Configure Lync Organizational Settings

Scenario

Odessa Brunner is anxious to try out PowerShell as a mechanism for controlling settings in Lync Online. He downloads and installs the PowerShell Module for Lync Online and then configures several settings. Odessa finishes off by changing the federation setting so that Lucerne Publishing only allows federated Lync conversations with Litware.com. He then reviews this setting in the Lync admin center.

The main tasks for this exercise are as follows:

1. Download and install Windows PowerShell Module for Lync Online

2. Configure Lync Online Organizational Settings with Windows PowerShell

▶ **Task 1: Download and install Windows PowerShell Module for Lync Online**

1. Open Internet Explorer and browse to **https://login.microsoftonline.com**.
2. Sign in as **obrunner@labXXXXXX.o365ready.com**, (where XXXXX is your unique o365ready.com number) with a password of **Pa\$\$w0rd**.
3. In **Outlook Web App**, specify your language and time zone, and click **Save**.
4. Press CTRL+T to open a new Internet Explorer tab and browse to **http://go.microsoft.com/fwlink/?LinkId=294688**.
5. On the **Windows PowerShell Module for Lync Online** page, click **Download**.
6. Click **Run**.
7. Select the **I agree to the license terms and conditions** check box.
8. Click **Install**.
9. If a **User Account Control** dialog box appears, click **Yes**.
10. When the install completes, click **Close**.
11. Close the Download Center Internet Explorer tab.

▶ **Task 2: Configure Lync Online Organizational Settings with Windows PowerShell**

1. On the desktop, right-click **Windows Azure Active Directory Module for Windows PowerShell**, and then click **Run as administrator**.
2. In the **User Account Control** dialog box, click **Yes**.
3. At the prompt, type the following command and press Enter:

```
Import-Module LyncOnlineConnector
```

4. At the **Start WinRM Service** message, press Enter.
5. At the prompt, type the following command and press Enter:

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

6. In the **Enter your credentials** dialog box, in the **User name** box, type **obrunner@labXXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number), and in the **Password** box, type **Pa\$\$w0rd**.

7. Click **OK**.
8. At the prompt, type the following command and press Enter:

```
$session = New-CsOnlineSession -Credential $credential
```

9. At the prompt, type the following command and press Enter:

```
Import-PSSession $session
```

10. At the prompt, type the following command and press Enter:

```
Set-CSPrivacyConfiguration -EnablePrivacyMode $True
```


Note the warning you receive about enabling client version checking.

11. At the prompt, type the following command and press Enter:

```
Set-CSPushNotificationConfiguration -EnableApplePushNotification $False
```

12. At the prompt, type the following command and press Enter:

```
Get-CSPrivacyConfiguration
```

You should see the following output:

- Identity: Global
- EnablePrivacyMode: True
- AutoInitiateContacts: True
- PublishLocationDataDefault: True
- DisplayPublishedPhotoDefault: True

13. At the prompt, type the following command and press Enter:

```
Get-CSPushNotificationConfiguration
```

14. At the prompt, type the following command and press Enter:

```
Set-CsTenantFederationConfiguration -AllowPublicUsers $True
```

15. At the prompt, type the following command and press Enter:

```
Set-CsTenantFederationConfiguration -AllowFederatedUsers $True
```

16. At the prompt, type the following command and press Enter:

```
$x = New-CsEdgeDomainPattern -Domain "litware.com"
```

17. At the prompt, type the following command and press Enter:

```
$newAllowList = New-CsEdgeAllowList -AllowedDomain $x
```

18. At the prompt, type the following command and press Enter:

```
Set-CsTenantFederationConfiguration -AllowedDomains $newAllowList
```

19. At the prompt, type the following command and press Enter:

```
Get-CsTenantFederationConfiguration
```

20. At the prompt, type the following command and press Enter:

```
Remove-PSSession $session
```

21. At the prompt, type the following command and press Enter:

```
Exit
```

22. In the **Office 365 Admin** console, click **Admin**, then click **Lync**.

23. On the left-hand side, click **Organization**.

24. In the **General** section, under **Presence privacy mode**, verify that the setting is configured as **Display presence information only to a user's contacts**.
25. Under **Mobile phone notifications**, verify that push notifications are turned off.
26. Click **External communications**.
27. Under **External access**, verify that **On only for allowed domains** is set.
28. Verify that under **Blocked or allowed domains**, litware.com is listed.

Results: Lucerne Publishing now has a Lync Online deployment correctly configured to meet the organization's business needs.

Lab Discussion Questions

What is the default general setting under Audio and video for Lync Online users?

The default general setting under Audio and video in Lync Online is Audio and HD video.

Can you manage and configure Lync Online using just Windows PowerShell?

No. You must also install the Windows PowerShell Module for Lync Online which contains the Lync Online Connector module and cmdlets specific to Lync Online management.

- What is the default general setting under Audio and video for Lync Online users?
- Can you manage and configure Lync Online using just Windows PowerShell?

Module Review and Takeaways

Now that you have completed this module, you can plan for Lync Online, configure Lync Online user settings, and configure Lync Online organizational settings using the Office 365 admin center and Windows PowerShell.

MCT USE ONLY. STUDENT USE PROHIBITED

Module 10

Implementing Directory Synchronization

Contents:

Module Overview	10-1
Lesson 1: Prepare On-premises Active Directory for DirSync	10-2
Lesson 2: Set up DirSync	10-14
Lesson 3: Manage Active Directory Users and Groups with DirSync In Place	10-23
Lab: Implementing Directory Synchronization	10-28
Module Review and Takeaways	10-46

Module Overview

In this module, students learn how to plan, prepare, and implement DirSync as a methodology for user and group management in an Office 365™ deployment. The module covers the preparation of an on-premises environment, the installation and configuration of DirSync, and how to manage Active Directory® users after DirSync has been enabled.

Objectives

After completing this module, you should be able to:

- Prepare an on-premises environment ready for directory synchronization.
- Install and configure DirSync.
- Manage Active Directory users in a DirSync-enabled scenario.

Lesson 1

Prepare On-premises Active Directory for DirSync

In this lesson, you will learn about directory synchronization with DirSync. Included in this lesson is a review of the installation requirements, planning for non-routable domain names such as .LOCAL, cleaning up existing objects in Active Directory, and enabling directory synchronization.

Lesson Objectives

After completing this lesson, you should be able to:

- Describe the function and features of DirSync.
- List the prerequisites for installing DirSync.
- Describe Active Directory cleanup issues, and list tools that can be used for remediation.
- Describe potential UPN suffix issues, and solutions.
- Describe the role of the Office 365 OnRamp Tool, and list its main services.
- List the key DirSync planning considerations and best practices.
- Describe how to enable Active Directory synchronization.

DirSync Overview

Windows Azure™ Active Directory Synchronization, also known as DirSync, synchronizes on-premises Active Directory objects (users, contacts, and groups) with Windows Azure Active Directory-based services, such as Office 365. DirSync replicates all additions, deletions, and modifications of users, groups, and contacts from on-premises to Office 365. DirSync is designed to operate as a software-based set-and-forget “appliance”. For Office 365, the purpose of DirSync is to enable coexistence between an on-premises Active Directory/Exchange environment and Office 365 in the cloud.

- DirSync enables coexistence
- Source of authority: one-way sync by default
- Email address matching
- Simple and hybrid scenarios

When running DirSync:

- New user, group, and contact objects in on-premises Active Directory are added to Office 365; however, Office 365 licenses are not automatically assigned to these objects.
- Attributes of existing user, group, or contact objects that are modified in on-premises Active Directory are modified in Office 365; however, not all on-premises Active Directory attributes are synchronized to Office 365.
- Existing user, group, and contact objects that are deleted from on-premises Active Directory are deleted from Office 365.
- Existing user objects that are disabled on-premises are disabled in Office 365; however, licenses are not automatically unassigned.

In a cloud-only Office 365 deployment, all Windows Azure Active Directory directory objects are originally created (mastered) in the cloud, and must be edited using cloud-based tools (either using the Office 365 portal or admin center, or by using PowerShell cmdlets). In this scenario, Windows Azure Active Directory is referred to as the source of authority for all Active Directory objects.

Windows Azure Active Directory requires there to be a single source of authority for every object. It is important to understand, therefore, that in a DirSync scenario, when you are running Active Directory synchronization, you are mastering objects from within your on-premises Active Directory, using tools such as Active Directory Users and Computers or PowerShell – the source of authority is the on-premises Active Directory. After the first synchronization cycle has completed, the source of authority is transferred from the cloud to the on-premises Active Directory. All subsequent changes to cloud objects (except for licensing) are mastered from the on-premises Active Directory tools. The corresponding cloud objects are read-only, and Office 365 administrators cannot edit cloud objects if the source of authority is on-premises.

Email address matching is used to identify the on-premises Active Directory user object that relates to an Office 365 user.

- If a user exists in the on-premises Active Directory and no matching user yet exists in Office 365, DirSync will create a new Office 365 with the same email address as the on-premises account.
- If a user already exists in both the on-premises Active Directory and in Office 365 and these objects have the same email address, then during the first synchronization these objects will become linked.

More information on attributes and matching is provided later in this module.

By synchronizing user, contact, and group objects, DirSync provides a unified Global Address List (GAL) experience between an on-premises Active Directory/Exchange environment, and Office 365. Using the filtering features in DirSync, objects hidden from the GAL on-premises are also hidden from the GAL in Office 365. Filtering and scoping are covered later in this module.

DirSync supports the following simple scenarios:

- Where Office 365 replaces on-premises Exchange.
- Where there are both on-premises and Exchange Online mailboxes in a hybrid deployment scenario.

In hybrid scenarios, DirSync enables mail routing between on-premises and Office 365 with a shared domain namespace. This scenario enables on-premises/cloud coexistence for both Exchange and Lync.



Note: DirSync is not designed to be used as a single-use bulk upload tool for Office 365, and does not automatically assign licenses to the Office 365 accounts.

Some Office 365 deployment models set up ADFS and Single Sign-On (SSO) before DirSync, and then use DirSync to ensure that there are Office 365 accounts for all on-premises users after federation has been enabled. However, this course follows the Office 365 FastTrack methodology, where DirSync is used as an enabler for SSO through ADFS.

DirSync Prerequisites

DirSync uses a version of the Microsoft Forefront Identity Manager (FIM) 2010 R2 synchronization service manager, pre-configured for synchronizing user, group, and contact objects from on-premises Active Directory to Office 365. This pre-configuration is why DirSync is referred to as a "software appliance" (set and forget); DirSync is 64-bit only, earlier 32-bit appliances are now unsupported.

- Domain and forest
- Hardware
- Operating System and supporting software
- DirSync quota limit
- Network ports
- Permissions and accounts
- Database
- Schema Extensions

Domain and Forest Requirements

DirSync requires an Active Directory forest, which is at Windows Server 2003 forest functional mode or higher. The DirSync appliance supports a single forest. Multi-forest scenarios always require a full deployment of a licensed copy of FIM 2010 R2 due to requirements for unique object attributes across the forest (these attributes are described later in this module). Multiple Exchange organizations are not currently supported.



Note: Using FIM for DirSync, using DirSync with a non-Microsoft directory service, and installing DirSync on a non-Windows computer are all out of scope for this course.

To work with DirSync, domain controllers must be running one of the following operating systems:

- 32-bit or 64-bit versions of Windows Server 2003 Standard Edition or Enterprise Edition with Service Pack 1 (SP1).
- 32-bit or 64-bit versions of Windows Server 2008 Standard or Enterprise.
- Windows Server 2008 R2 Standard or Enterprise, Windows Server 2008 Datacenter, or Windows Server 2008 R2 Datacenter (all are 64-bit only).
- Windows Server 2012 Standard or Datacenter (both are 64-bit only).

The DirSync computer must be a member of a domain, and for standard single forest scenarios, this computer must be joined to a domain within the same forest that will be synchronized. DirSync now supports installations on domain controllers; previous versions did not. However, for production scenarios, it is recommended to use a separate server for DirSync.



Note: For complex multi-forest scenarios, it is important to be able to manually select a unique Active Directory attribute to use as a **SourceAnchor** (the link between on-premises Active Directory and Windows Azure Active Directory). This must be an immutable attribute, such as Employee ID, as the default SourceAnchor (GUID) is unique to one forest, and if an object is moved across forests, the object will appear to DirSync to be a new object. For this reason, multi-forest scenarios always require a full deployment of a licensed copy of FIM 2010 R2.

Hardware Requirements

Deployments with more than 50,000 objects in Active Directory require a significant increase in memory requirements (from 4 GB RAM to 16 GB); therefore, it is important to implement adequate hardware resources when transitioning from the pilot to production phase.

Number of objects in Active Directory	CPU	Memory	Hard disk size
Fewer than 10,000	1.6 GHz	4 GB	70 GB
10,000–50,000	1.6 GHz	4 GB	70 GB
50,000–100,000	1.6 GHz	16 GB	100 GB
100,000–300,000	1.6 GHz	32 GB	300 GB
300,000–600,000	1.6 GHz	32 GB	450 GB
More than 600,000	1.6 GHz	32 GB	500 GB

DirSync Server OS and Supporting Software Requirements

DirSync requires the following Windows Server versions:

- 64-bit edition of Windows Server 2008 R2 SP1 Standard or Enterprise (or later), or Windows Server 2008 Datacenter or Windows Server 2008 R2 Datacenter or later.
- 64-bit edition of Windows Server 2012 Standard or Datacenter or later.

In addition, DirSync requires the following software prerequisites:

- Microsoft .NET Framework 3.5 SP1 and the Microsoft .NET Framework 4.0. The .NET Framework 4.0 will already be installed if installing on Windows Server 2012; Microsoft .NET Framework 3.5 SP1 will need to be enabled.
- Windows Azure AD Module for Windows PowerShell (64-bit version).

DirSync Quota Limit

The current release of Office 365 has a default object limit of 50,000 objects (users, mail-enabled contacts, and groups). This object limit is automatically increased to 300,000 after the first domain is verified. If a synchronization results in the existing quota being exceeded, the tenant administrator will receive an email message, such as:

```
The Directory Synchronization batch run was
completed on Tuesday, 03 December 2013 23:45:22 GMT for tenant <name>
The following errors occurred during synchronization:
Synchronization has been stopped. The company has exceeded the number of objects that can be
synchronized. Contact Technical
Support and ask for an increase in your company's quota.
```

If there is a verified domain and a requirement to synchronize more than 300,000 objects, or there are no verified domains and a requirement to synchronize more than 50,000 objects, you will need to contact Microsoft Technical Support to request an increase to the object quota limit. It is therefore important to plan for any likely DirSync quota increase; otherwise, if left to the last minute, this could become a deployment blocker.

 **More information on identifying and resolving the problem can be found here:**

<http://go.microsoft.com/fwlink/?LinkId=390907>

Network Ports

Synchronization with the Windows Azure Active Directory used by Office 365 occurs over SSL; this synchronization is outbound (as it is initiated by DirSync) and uses port 443. Internal network

communication uses standard Active Directory-related ports; for successful synchronization, the DirSync server must be able to contact all DCs in the Forest.

Service	Protocol	Port
LDAP	TCP/UDP	389
Kerberos	TCP/UDP	88
DNS	TCP/UDP	53
Kerberos Change Password	TCP/UDP	464
RPC	TCP	135
RPC randomly allocated high TCP ports	TCP	1024 - 65535 49152 - 65535
SMB	TCP	445
SSL	TCP	443
SQL	TCP	1433

Permissions and Accounts

Installing and configuring DirSync requires the following accounts:

- An Office 365 account with Administrator permission in the Office 365 tenant.
- An on-premises account with Enterprise Administrator permissions in the on-premises Active Directory.

DirSync uses the Office 365 tenant administrator account to provision and update objects when the DirSync configuration wizard is run. If a dedicated service account is created in Office 365 to use for DirSync in place of the standard Office 365 tenant administrator account, it is important to disable the default 90-day password expiration; otherwise, the synchronization service will stop working when the password expires, which will require reconfiguration of DirSync.

To disable service account password expiration by using the Windows Azure Active Directory Module for Windows PowerShell, type the following command, and press Enter:

```
Set-MsolUser -UserPrincipalName <service account>@<domain>.onmicrosoft.com - PasswordNeverExpires $true
```

On-premises, the account used to install and configure DirSync must have the following permissions:

- *Enterprise Administrator permissions in Active Directory.* Required to create the synchronization user account in Active Directory.
- *Local machine administrator permissions.* Required to install the DirSync software.

The account used to configure DirSync and run the configuration wizard must reside in the local machine's **FIMSyncAdmins** group; by default, the account used to install DirSync (the Enterprise Administrator) is automatically added to this group.

The Enterprise Administrator account is only required when installing and configuring DirSync, and the Enterprise Administrator credential is not stored or saved by the configuration wizard. Therefore, it is good practice to create a special "DirSync Administrator" account for installing and configuring DirSync,

and to only assign this account to the Enterprise Administrators group when DirSync is being set up. This DirSync Administrator account should be removed from the Enterprise Administrators group after DirSync setup is complete. It is also good practice to ensure that the password for this account is set to never expire.


The Enterprise Administrator account is required to:

- Create the MSOL_<id> domain account in the CN=Users container of the root domain.
- Delegate the following permissions to MSOL_<id> on each domain partition in the forest
 - Replicating Directory Changes
 - Replicating Directory Changes all
 - Replication Synchronization

In hybrid coexistence scenarios where “Rich Coexistence” is selected during DirSync configuration, the Enterprise Administrator account also automatically creates an MSOL_Active Directory_Sync_RichCoexistence group in the **CN=Users** container of the root domain. In such scenarios, the Enterprise Administrator account is used to delegate write permissions for six attributes that are written back from Office 365 to on-premises Active Directory. These Rich Coexistence attributes are covered later in this module.

The following accounts are created in Active Directory during DirSync configuration:


- *MSOL_<id>*. This account is created during DirSync installation, and is configured to synchronize to the Office 365 tenant. The account has directory replication permissions in the local Active Directory and write permission on certain attributes to enable Hybrid Deployment.
- *AAD_<id>*. This is the service account for the Synchronization Engine, and is created with a randomly generated complex password automatically configured to never expire. When the directory synchronization service runs, it uses the service account credentials to read from the local Active Directory and then to write the contents of the synchronization database to Office 365 using the tenant administrator credentials entered during the DirSync wizard.

 **Note:** Do not change this service account after installing DirSync, as DirSync will always attempt to run using the account created during setup. If the account is changed, DirSync will stop running and scheduled synchronizations will no longer occur.

Database Requirements

SQL Server Express is installed by default as part of the DirSync installation; this option has a 10 GB database limit (approximately 50,000 objects). For large deployments (where it is anticipated that there will be more than 50,000 objects in Active Directory), DirSync must be installed to use a full SQL Server database.

If using full SQL Server, SQL Server rights are also required to create the DirSync database, and to set up the SQL service account with the role of db_owner. This can be achieved by ensuring that the Enterprise Administrator account used to install DirSync has “sysadmin” rights on the SQL database, and that the service account used to run DirSync has “public” permissions on the DirSync database.

 **Note:** Full SQL Server configuration requires that DirSync be deployed using the command line.

Schema Extensions

If your environment is running Active Directory but not Exchange Server, then you need to install the Exchange Server 2013 Schema extensions prior to installing and running DirSync.

 **For information on installing the Schema extensions for Exchange Server, see the following link:**

<http://go.microsoft.com/fwlink/?LinkId=400790>

Active Directory Cleanup

Before deploying DirSync, it is essential that the on-premises Active Directory and related technologies are checked for potential issues, and any issues discovered are remediated. Such checks should include:

- Analyzing the on-premises environment for invalid characters in Active Directory object attributes and for incorrect UPNs.
- Performing domain email discovery and user counts.
- Identifying domain functional levels and schema extensions, and identify custom attributes in use.
- Identifying Exchange proxies.
- Identifying Lync SIP domains.
- Identifying SharePoint domains.
- Evaluating client for SSO readiness.
- Recording network port use, and DNS records related to Office 365.

- Manual checks to perform
- Tools to check and remediate Active Directory:
 - IdFix
 - ADModify.Net

After the checks have been carried out, key remediation tasks include:

- Removing duplicate proxyAddress and userPrincipalName attributes.
- Updating blank and invalid userPrincipalName attributes, and replacing with valid userPrincipalName attributes.
- Removing invalid characters in the following attributes: givenName, surname (sn), sAMAccountName, displayName, mail, proxyAddresses, mailNickname, and userPrincipalName.

UPNs that are used for SSO can contain letters, numbers, periods, dashes, and underscores; no other character types are allowed. If the Office 365 deployment includes plans for SSO, it is important to ensure that UPN names meet this requirement before SSO is rolled out.

After Windows Azure Active Directory Sync has been configured, an email that lists any errors that still need to be corrected is sent to the Office 365 tenant administrator account specified during the DirSync wizard.

 **List of attributes that are synced by the Windows Azure Active Directory Sync tool.**

<http://go.microsoft.com/fwlink/?LinkId=390908>

 **List of attributes that may need cleaning up.**

<http://go.microsoft.com/fwlink/?LinkId=390909>


Active Directory Health Check Tools

The following Active Directory health check tools can be used to identify and remediate issues.

IdFix

The Microsoft Office 365 IdFix tool enables you to identify and remediate the majority of object synchronization errors in Active Directory, including common issues such as duplicate or malformed proxyAddresses and userPrincipalName. IdFix is designed to run on Windows 7 and Windows Server 2008 R2; however, it does also run on Windows Server 2012.

You can select the OUs for IdFix to check, and common errors can be fixed within the tool itself. Common errors include such things as invalid characters that may have been introduced during scripted user imports to attributes such as proxyAddresses and mailNickname.

 **Note:** For distinguished names that contain format and duplicate errors, IdFix may not be able to suggest an automatic remediation for the error. Such errors can either be fixed outside IdFix, or be manually remediated within IdFix.

 **For more information, and to download IdFix, go to the IdFix DirSync Error Remediation Tool page on the Microsoft Download Center.**

<http://go.microsoft.com/fwlink/?LinkId=390910>

ADModify.NET

For errors such as format issues, you can make changes to specific attributes object by object, using either ADSIEdit or Advanced Mode in Active Directory Users and Computers. However, to make attribute changes to multiple objects, ADModify.NET is a better tool; the batch mode operation provided by ADModify.NET is particularly useful for making changes to attributes such as UPNs across OUs or domains.

 **Introduction to Active DirectoryModify.net.**

<http://go.microsoft.com/fwlink/?LinkId=390911>

 **Download link for Active DirectoryModify.NET on CodePlex.**

<http://go.microsoft.com/fwlink/?LinkId=390912>

UPN Suffixes

Before deploying DirSync, it is important to verify that on-premises user objects have a non-null value for UPN suffix, and that this is correct for both the domain and Office 365. The UPN suffix is the part of a UPN to the right of the @ character. If a verified public routable domain is being used in Office 365, then this domain should be the UPN suffix, so that the users' principal names are of the form <user>@<verified domain>. If the on-premises UPN suffix does not contain a public routable DNS domain (such as contoso.local), the default routing domain (for example, contoso.onmicrosoft.com) is used for Office 365 UPN suffix.

- UPN must not be null
- UPN must match any verified public routable domain
- Default routing domains

If the UPN suffix must be changed, it is important to check for any applications that may be dependent on a specific UPN. If planning SSO, you need know your Active Directory UPN to register the domain for SSO (for federated or non-fed ids).

After sync is in place, modifying the user's UPN suffix is not supported. If you need to modify the UPN after sync is in place, you have to sync first and then manually change the UPN; therefore, it is important that you plan the UPN suffix correctly right from the start.

To add a UPN suffix to the on-premises Active Directory:

1. In **Active Directory Domains and Trusts**, log on to one of the organization's Active Directory domain controllers.
2. In the console tree, right-click **Active Directory Domains and Trusts**, and then click **Properties**.
3. Select the **UPN Suffixes** tab, type an alternative UPN suffix for the forest, and then click **Add**.
4. Repeat step 3 to add additional alternative UPN suffixes.

If Active Directory synchronization has already been set up, the user's UPN for Office 365 may not match the user's on-premises UPN defined in Active Directory; this can occur if the user was assigned an Office 365 license before the domain was verified. To fix this issue, Windows PowerShell can be used to update users' UPNs to ensure that their Office 365 UPN matches their corporate user name and domain.

Office 365 OnRamp Tool

The Office 365 OnRamp tool is used to run automatic checks against a current on-premises environment and to assess readiness to deploy Office 365. These checks are read-only, and do not make permanent changes to the on-premises Active Directory. After the checks have completed, the Office 365 OnRamp tool lists the configuration steps that will be needed to complete a deployment.

Depending on the type of Office 365 deployment required, the OnRamp Tool checks include:

OnRamp checks include:

- Credentials
- Network
- Domains
- Users and groups
- Mail
- Sites
- Lync
- User software

- *Credentials.* Determines whether there are valid credentials available in the local environment, including necessary admin rights in Exchange if migrating from Exchange on-premises, and tenant admin credentials for any existing trial account with Office 365.
- *Network.* Determines whether there is network connectivity to Office 365, and checks for availability of required ports.
- *Domains.* Determines the on-premises domain suffixes, and identifies whether any domains are already verified with Office 365. Appropriate DNS records are also checked.
- *Users and groups.* Determines whether the on-premises Active Directory is ready for directory synchronization and SSO. User and group objects are also checked to ensure that they meet the requirements for successful synchronization with Office 365.
- *Mail.* Evaluates messaging integration with the on-premises environment, and for readiness for email migration if required.
- *Sites.* Determines whether the on-premises Active Directory environment is able to support the deployment of SharePoint Online.
- *Lync.* Identifies any current integration with Lync or Office Communications Server.
- *User software.* Determines whether domain-joined computers meet the service and identity requirements for the required Office 365 deployment.

The computer used to run the Office 365 OnRamp tool must meet the following system requirements:

- Windows Server 2008 R2 or Windows 7
- Internet Explorer 9.0
- PowerShell v2.0
- WinRM 2.0



Note: An Office 365 trial account is needed in order to complete all the tests. Some tests involve similar steps as in the initial Office 365 configuration, but they are not permanent changes.



For more information, see the OnRamp site at Office 365.

<http://go.microsoft.com/fwlink/?LinkId=390913>

Planning Considerations and Best Practices

When planning for directory synchronization, the following issues must be considered:

- Identifying directory preparation tasks. For example, including any attribute updates, and whether an Active Directory upgrade is required in order to meet minimum version requirements for forest functional level.
- Identifying any requirements for auditing once synchronization has been enabled.
- Identifying any domain controller placement issues that may affect synchronization performance and reliability.
- Determining the required accounts and permissions to use during DirSync deployment, configuration, and operation.
- Planning for multiforest/directory scenarios, and identifying options for integrating multiple forests.
- Performing capacity planning, such as preparation for large scale deployments requiring SQL Server databases, and Windows Azure Active Directory quota extensions. Note that there is no "highly available" DirSync option, other than to ensure that the DirSync server and database are protected, such as by hosting the database on a separate, clustered SQL Server, instead of the DirSync server's SQL Express, and to back up the DirSync management agent to file after configuring filtering.
- Planning for two-way synchronization, in rich coexistence/hybrid scenarios.
- Planning for non-routable domain names, such as .LOCAL, by using additional UPN suffixes.
- Planning for Active Directory filtering, so that only those parts of Active Directory that are required to be synchronized to Office 365 are included in the synchronization.

DirSync best practices include:

- Having a proper project plan
- If using filtering, setting it up before synchronizing any objects
- Working with a cloud services partner
- Performing thorough capacity planning
- Remediating the Active Directory before building DirSync infrastructure
- Adding all SMTP domains as verified domains before synchronizing

Best practices for deploying DirSync, include:

- Having a proper project plan.
- If using filtering, setting it up before synchronizing any objects.
- Working with a cloud services partner.
- Performing thorough capacity planning.
- Remediating the Active Directory before building the DirSync infrastructure.
- Adding all Simple Mail Transfer Protocol (SMTP) domains as verified domains before synchronizing; domains cannot be removed until all synchronized objects are no longer using the domain as a proxy address or UPN.

Enabling Active Directory Synchronization

Active Directory Synchronization must first be enabled in Office 365, before DirSync can be used to initiate a synchronization. This process can take up to 24 hours to complete, so it is important to plan for this requirement ahead of DirSync deployment. Active Directory Synchronization can be enabled in the Office 365 tenant through the Office 365 portal or admin center, or by using PowerShell.

To enable DirSync by using the Office 365 portal or admin center:

1. In the left navigation, click **Users**.
2. To the right of Active Directory synchronization, click **Set up**.
3. Under Activate Active Directory synchronization, click **Activate**.
4. At the prompt, click **Activate**.

To enable DirSync by using the Windows Azure Active Directory Module for Windows PowerShell, type the following command, and press Enter:

```
Set-MsoDirSyncEnabled -EnableDirSync $true -Force
```

DirSync can be enabled using:

- Office 365 portal
- PowerShell
- May take up to 24 hours to complete

Discussion: Planning DirSync for Lucerne Publishing

Discuss as a class whether Lucerne Publishing should implement DirSync or continue with its current user management arrangements.

- Discuss as a class whether Lucerne Publishing should implement DirSync or continue with its current user management arrangements

Lesson 2

Set up DirSync

In this lesson, you examine how to set up and configure DirSync, including filtering Active Directory, identifying synchronized attributes, scheduling synchronization and forcing synchronization through PowerShell and the DirSync console, and implementing password synchronization.

Lesson Objectives

After completing this lesson, you should be able to:

- Describe the DirSync installation and configuration process.
- Describe hybrid mode, and how this affects directory synchronization.
- Explain how to perform filtering and scoping of directory synchronization.
- List the methods used to initiate directory synchronization.
- Describe how to verify directory synchronization.
- Describe the password synchronization feature of DirSync.

DirSync Installation and Configuration

The DirSync tool should always be installed from the download link in the Office 365 admin center – this ensures that the current version is always installed.

To install DirSync:

1. In the Office 365 portal or admin center, in the left navigation, click **Users**.
2. To the right of **Active Directory synchronization**, click **Manage** (or if Active Directory synchronization has not yet completed, click **Set up**).
3. Under **Install and configure the Directory Sync tool**, click **Download**.
4. Then click **Run** to initiate immediate installation, or **Save** to save the DirSync executable to local storage.

- DirSync installation source should be the Office 365 portal
- DirSync configuration wizard options:
 - Exchange hybrid deployment
 - Synchronization post-configuration
- Limited management agent customization

The **Windows Azure Active Directory Sync tool Configuration Wizard** will launch automatically at the end of the installation, unless the **Start Configuration Wizard now** check box is cleared.

After DirSync has been installed, you must log off and log on again before starting the Configuration Wizard to add the user account to the Synchronization Engine FIMSyncAdmins group.

DirSync Configuration

DirSync is configured using the Windows Azure Active Directory Sync tool Configuration Wizard, or by using the DirSync installation shell. During configuration, DirSync creates the **AAD_<id>** account (where <id> is a 12 alphanumeric installation-specific string) in the **Users** OU of the root domain in the Active Directory forest. DirSync then uses this service account to read and synchronize local Active Directory

objects to Windows Azure Active Directory. The DirSync Configuration Wizard sets up recurring synchronizations to occur every three hours.

After DirSync has been configured and synchronized for a cloud tenant organization, it cannot be configured to populate other cloud tenants. In order to synchronize with another Windows Azure Active Directory tenant organization, a new instance of DirSync must be installed.

To configure directory synchronization using the Windows Azure Active Directory Sync tool Configuration Wizard, perform the following steps:

1. If setting up directory synchronization for the first time, on the last page of the **Windows Azure Active Directory (Windows Azure Active Directory) Sync Setup** wizard, select the **Start Configuration Wizard** now check box, and then click **Finish**.
2. If updating the configuration of directory synchronization, or the **Start Configuration Wizard** now check box was cleared at the end of the installation, click the **Directory Sync Configuration** shortcut.
3. On the **Windows Azure Active Directory (Windows Azure Active Directory) Credentials** page, type the cloud credentials to use (such as the tenant administrator or dedicated service account), and then click **Next**.
4. On the **Active Directory Credentials** page, type the Active Directory Enterprise Admin Credentials to use (such as the dedicated DirSync admin account), and then click **Next**.
5. On the **Exchange hybrid deployment** page, activate the Exchange hybrid deployment features if required, provided there is Exchange Server 2010 SP1 or Exchange Server 2013 is installed. If the Exchange hybrid deployment features are activated, DirSync will write attribute data back into the on-premises Active Directory. More information on hybrid deployments is provided in the next topic in this lesson.
6. To immediately begin the first synchronization, leave the **Synchronize your directories now** check box selected on the **Finished** page of the wizard.

Management Agents

In the current version of the Directory Sync tool, the name of the Active Directory Domain Service management agent is **Active Directory Connector**; in previous versions, this management agent was called **Source Active Directory**. The Active Directory Connector uses Active Directory GUID as the SourceAnchor (link between Active Directory and Office365 Object); this is automatically set, and in DirSync this link cannot be changed (unlike in full FIM 2010 R2).

DirSync has a second management agent, **Windows Azure Active Directory Connector**; that is responsible for exporting information from DirSync to Windows Azure Active Directory.



Note: If a new domain is added to the Active Directory forest, the Windows Azure Active Directory Sync tool Configuration Wizard must be rerun in order to add the new domain to the list of domains to be synchronized.

Hybrid Mode

There are two levels of coexistence between on-premises Active Directory and Exchange, and Office 365 – simple coexistence and hybrid coexistence (also known as rich coexistence). In simple coexistence, some users are provisioned in Office 365, while the remaining users are provisioned in the on-premises environment. Both sets of users see the same objects in the GAL, and DirSync is used for GAL synchronization.

Coexistence enables mail routing between on-premises and Office 365 using a shared DNS namespace, and email messages are routed

between Office 365 users and on-premises users, with the MX record pointing to either the on-premises environment or to Office 365. Simple coexistence does not require an on-premises Hybrid Exchange server.

- Simple coexistence
- Hybrid or Rich Coexistence
- Attribute write back

Hybrid (rich coexistence) Office 365 deployments provide additional shared features over simple coexistence, including:

- Cross-premises Free/Busy and calendar sharing.
- Cross-premises Out of Office support, mail tips, messaging tracking, and mailbox search.
- A single OWA URL for both on-premises and cloud.
- Single tool to manage cross-premises Exchange functions (including migrations).
- Mailbox moves support both onboarding and offboarding.
- No Outlook reconfiguration or OST resynchronization are required after a mailbox migration.
- Authorization headers are preserved, to ensure internal email is not marked as spam, and that messages resolve against the GAL.
- Centralized mail flow, to ensure that all email routes (inbound and outbound) are through the on-premises Exchange servers.
- Support for cloud-based Exchange archiving.

Hybrid mode requires an on-premises Hybrid Exchange server deployment. In hybrid mode, there is two-way synchronization of certain attributes from the Office 365 directory infrastructure back to the on-premises Active Directory environment (in non-hybrid, all synchronization is one way, from on-premises to Office 365). The following table identifies the six attributes that are written *back* from Office 365 to on-premises Active Directory.

Attribute	Scope
MSExchArchiveStatus	User
MSExchBlockedSendersHash	User
MSExchSafeRecipientsHas	User
MSExchSafeSendersHash	User
MSExchUCVoiceMailSettings	User

Attribute	Scope
ProxyAddresses	User, Contact, Group

For example, if a user has an Archive folder in Office 365, **MSEchArchiveStatus** is written back to the on-premises Active Directory; therefore, when the user is running Outlook, this will use the cloud for its archive folder.

Filtering and Scoping


By default, after running the Windows Azure Active Directory Sync tool Configuration Wizard, the entire Active Directory forest is scoped for synchronization, including all user objects, all group objects, and all mail-enabled contact objects. Passwords will not be synchronized unless the **Enable Password Sync** check box is selected; password synchronization is covered later in this lesson.

Active Directory synchronization filtering can be configured at any time; if filtering must be enabled immediately after DirSync is deployed, the

Synchronize your directories now check box must be cleared on the **Finished** page of the wizard, and filtering set up before the first synchronization. If the first synchronization has already been run and then filtering enabled, the objects that are filtered out are no longer synchronized to the cloud, and any previously synchronized objects in the cloud that were then filtered out of the synchronization are deleted by the directory synchronization process. In a single forest, scopes/filters apply across a forest.

DirSync filter configuration types:


- Organizational unit (OU)-based
- Domain-based
- User attribute-based

 **Note:** If using filtering, it should be set up before synchronization; otherwise, there is a risk of orphaning Office 365 objects if they are subsequently affected by a filter. If objects were inadvertently deleted because of a filtering error, these can be re-created in the cloud by removing the filtering configuration, and then resyncing the directories.

The following three filtering configuration types can be applied to the Directory Synchronization tool:

- *Organizational unit (OU)-based.* Selects which OUs are permitted to synchronize to the cloud. It is important to note that moving users between OUs in Active Directory can orphan them in Office 365 if they are moved out of scope, due an operational filter.
- *Domain-based.* Selects the domains that are permitted to synchronize to the cloud.
- *User attribute-based.* Specifies attribute-based filters for user objects, and controls which should not be synchronized to the cloud. Filtering can use any user object attribute.

In some scenarios, a combination of OU and attribute filtering provides the best filtering solution.

 **Note:** A full implementation of FIM 2010 R2 offers more filtering options, but is beyond the scope of this course.

Filters specify objects that will *not* be synchronized. Multiple filter rules within a single condition are treated as OR statements, and the filter will be applied if *any one* of the rules are true; multiple conditions within the same rule are treated as AND statements, and the filter will be applied if *all* the conditions are true. Group memberships cannot be used as the basis for filtering; they can only be used on attributes that every object has.

Domain credentials requirement

When configuring the Active Directory Connector management agent for filtering, the MSOL_<id> account will be displayed in the credentials dialog box. This account uses a randomly generated password; therefore, administrators will not know the password. As a result, Enterprise Admin credentials should be used when configuring filtering; for example, you should use an account that can view the entire forest and perform the filtering within any domain within the forest.

To configure filtering – first steps:

1. Log on to the DirSync computer using an account that is a member of the FIMSyncAdmins local security group.
2. Start **Identity Manager**, from the following location: Program Files\Windows Azure Active Directory Sync\SYNCBUS\Synchronization Service\UIShell\miisclient.exe.
3. In Identity Manager, click **Management Agents**, and then double-click **Active Directory Connector**.

To set up OU-based filtering:

1. In **Active Directory Connector**, click **Configure Directory Partitions**, and then click **Containers**.
2. When prompted, enter enterprise admin credentials.
3. In the **Select Containers** dialog box, clear the OUs that should not be synchronized with Office 365, and then click **OK**.
4. Click **OK** on the Active Directory Connector Properties page.
5. Perform a full sync: on the **Management Agent** tab, right-click **Active Directory Connector**, click **Run**, click **Full Import Full Sync**, and then click **OK**.

To set up domain-based filtering:

1. In **Active Directory Connector**, click **Configure Directory Partitions**, and then select the domains that should not be synchronized with Office 365, by clearing the domain's check box.
2. Click **OK** on the Active Directory Connector Properties page.
3. Click **Configure Run Profiles**, and then check each Profile and remove any steps where the Partition is shown as a GUID, rather than an LDAP path, leaving one run step for each domain.
4. Perform a full sync: on the **Management Agent** tab, right-click **Active Directory Connector**, click **Run**, click **Full Import Full Sync**, and then click **OK**.

To set up user attribute-based filtering:

First identify the attribute to filter on; some attributes may already be present. For example, to configure DirSync so that Exchange 2013 Health Mailboxes are not synchronized to Office 365, use a filter for **sAMAccountName** that Starts With "SM_".

For other attributes, the attribute may first need to be configured in Active Directory before the filter can be activated. For example, using Active Directory Users and Computers in Advanced mode, or ADSIEdit, the string "NoSync" could be added to the **extensionAttribute15** user attribute for each user in the on-premises organization that must not be synchronized to Office 365.

The following steps describe how to configure user filtering using the “NoSync” string on **extensionAttribute15**:

1. In **Active Directory Connector**, click **Configure Connector Filter**, and then do the following:
2. Select **User** in the **Data Source Object Type** grid, and then click **New**.
3. In **Filter for user**, on the **Data Source** attribute, select **extensionAttribute15**; for **Operator**, select **Equals**, and then type **NoSync** in the **Value** field.
4. Click **Add Condition**, and then click **OK**.
5. Click **OK** on the Active Directory Connector Properties page.
6. Perform a full sync: on the **Management Agent** tab, right-click **Active Directory Connector**, click **Run**, click **Full Import Full Sync**, and then click **OK**.

If a filtering configuration does not produce the desired results, deleting the Windows Azure Active Directory Connector and the Active Directory Connector and re-running the DirSync configuration will recreate these agents with their default settings.



Note: Contacts and groups use complex filtering rules that are out of scope for this course.

Initiating Synchronization

The first Active Directory synchronization must be planned for and scheduled, as this takes time and bandwidth, especially if filtering has not been enabled and large numbers of objects need to be synchronized. DirSync can synchronize approximately 5,000 objects every 45 to 60 minutes. Subsequent synchronization cycles are deltas only and, therefore, much faster. It is important that you plan ahead if synchronizing thousands of objects.

To perform the first full synchronization immediately after running the Windows Azure Active Directory Sync tool Configuration Wizard, leave the **Synchronize your directories now** check box selected on the **Finished** page of the wizard.

To perform the first full synchronization after configuring filtering, in **Identity Manager**, on the **Management Agent** tab, right-click **Active Directory Connector**, click **Run**, click **Full Import Full Sync**, and then click **OK**.

You can also initiate synchronization using PowerShell:

1. On the DirSync server’s desktop, right-click the **Windows PowerShell** shortcut and click **Run as administrator**
2. Type the following command and press Enter:

```
Set-ExecutionPolicy Unrestricted
```

3. Press Enter again to confirm the operation.
4. At the prompt, type the following command and press Enter:

Initiating synchronization:

- Windows Azure Active Directory Sync tool Configuration Wizard
- PowerShell
- Scheduled synchronization

Import-Module DirSync

- At the prompt, type the following command and press Enter:

Start-OnlineCoexistenceSync

Scheduled synchronization occurs every three hours; therefore, you can use the **Start-OnlineCoexistenceSync** cmdlet to force a sync outside of the regular synchronization schedule, or use Identity Manager to initiate synchronizations. For example, immediate synchronization may be required after an employee's employment is terminated to ensure that this person does not retain access to either on-premises or Office 365 resources.

It is also possible to change the default synchronization interval from three hours by modifying the **Microsoft.Online.DirSync.Scheduler.exe.config** configuration file, in %programfiles%\Windows Azure Active Directory Sync. After making changes to this file, restart the synchronization service on the DirSync computer. Editing **Microsoft.Online.DirSync.Scheduler.exe.config** is not supported by Microsoft, and the best practice is to leave the synchronization interval set at three hours.

Verifying Synchronization

To verify that DirSync is working, it is important to test both manual and automatic synchronization, bearing in mind that initial synchronization may take several hours to complete, depending on the number of objects in the synchronization scope.

To verify synchronization:

- *Check Office 365 for synced Active Directory accounts.* Office 365 Portal accounts should be replicated within a few minutes and will appear in the Office 365 Portal with a status of "Synced with Active Directory".
- *View synchronization results in Identity Manager.* Details of the results of all management agent operations are shown on the Operations tab.
- *View synchronization entries in Event Viewer.* DirSync writes Directory Synchronization entries to the DirSync computer's event log. These entries indicate the start and end of a directory synchronization session:
 - Event ID 1 provides information on started imports.
 - Event ID 2 provides information on completed imports.
 - Event ID 4 provides information on completed synchronizations.

- Check Office 365 for synced Active Directory accounts
- View synchronization results in Identity Manager
- View synchronization entries in Event Viewer
- Last synced time:
 - Office 365 Portal
 - PowerShell

If directory synchronization errors occur, they are reported in the event log and an email message is sent to the Office 365 tenant administrator account specified during the DirSync wizard.

To view the last synchronization time, using the Office365 Portal on the Admin page, in the left pane, click **Users**, and note **the Last Synced** status next to **Active Directory® synchronization**. Last synchronization time can also be obtained using the Windows Azure Active Directory module for Windows PowerShell by using the following command:

```
Get-MsolCompanyInformation | fl LastDirSyncTime
```


Password Synchronization

The DirSync Password Sync feature synchronizes user passwords from on-premises Active Directory to Windows Azure Active Directory. This enables users to log into Office 365 using the same password they use to log into the on-premises network. Password Sync does not provide SSO, as password sharing does not include the token sharing/exchange steps performed by solutions such as ADFS (see next module); password sync is not, therefore, used for federated domains.

Password Sync is only supported by DirSync v6382.0000 or greater; the latest version of the Directory Sync tool can be downloaded from the Admin Portal.

In Active Directory, passwords are stored as a hash of the actual user password. This password hash cannot be used as the password itself, and cannot be reverse engineered to obtain the user's plain text password. To synchronize a password, DirSync extracts the user password hash from the on-premises Active Directory, and the plain text version of a user's password is never exposed to the password sync tool or to Azure Active Directory or any of the associated services. When a user presents his or her synced password to Office 365, it is checked against the synchronized hash, so there is never a requirement to synchronize the password itself.

Passwords are synchronized more frequently than other attributes (generally in chronological order). When a user's password is synchronized from the on-premises Active Directory to the cloud, the existing cloud password will be overwritten.

When Password Sync is first enabled, DirSync performs an initial synchronization of the passwords of all in-scope users from on-premises Active Directory to Office 365; it is not possible to define the set of users that will have their passwords synchronized to the cloud. Subsequently, when an on-premises user changes his or her password, the Password Sync feature will detect and synchronize the changed password, usually within a few minutes. Failed user password syncs are automatically retried, with any errors logged in Event Viewer.

Password Complexity

After Password Sync is enabled, the password complexity policies configured in the on-premises Active Directory override any complexity policies that may be defined in the cloud for synchronized users. This means any password that is valid in the customer's on-premises Active Directory environment can be used for accessing Azure Active Directory services. Passwords for users that are created directly in the cloud are still subject to password policies as defined there.

Password Expiration

For users with synced passwords, their cloud account passwords are set to "Never Expire", so it is possible for a user's password to expire in the on-premises environment, but they can continue to log into cloud services using this expired password. The cloud password will then be updated the next time the user changes the password in the on-premises environment.

Enabling Password Sync

Password Sync is enabled by running the Windows Azure Active Directory Sync tool Configuration Wizard; this wizard can be run against an existing synchronization and will not overwrite the management agent settings and filters. In the Wizard, select the **Enable Password Synchronization** check box; this process will trigger a full synchronization. Password Sync is disabled in the same way, by running the Windows

- Password Complexity
- Password Expiration
- Enabling Password Sync
- Disabling user accounts

Azure Active Directory Sync tool Configuration Wizard and clearing the **Enable Password Synchronization** check box.

Initiating a Full Sync using Identity Manager or the DirSync shell cmdlets does *not* initiate a full password sync. To force a full password sync, run the following command at the DirSync shell prompt:

```
Set-FullPasswordSync
```

Then, in the Services.msc console, restart the **Forefront Identity Manager Synchronization Service** service.

To determine which users have successfully had their passwords synchronized, open Event Viewer and review Event IDs 656 (processed password change requests), and 657 (request results).

Disabling User Accounts

If you have enabled password sync and you disable a user's account in Active Directory (for example, after an employee's contract has been terminated) then this disable message is replicated to Office 365 as part of the password sync update process and completes in a couple of minutes. However, if you do not have password sync enabled, the user's account is not disabled until the next scheduled directory synchronization, which could take up to three hours. Hence, if a user account is disabled without password sync in place, you need to force a directory synchronization cycle.

Lesson 3

Manage Active Directory Users and Groups with DirSync In Place

In this lesson, you learn how to delete, create and modify users in an environment with DirSync configured and operating successfully to synchronize on-premises accounts with Office 365. In a DirSync-enabled environment, Active Directory is the source of all accounts, so it is important that the on-premises environment is properly managed, and to understand how on-premises and Office 365 accounts are matched.

Lesson Objectives

After completing this lesson, you should be able to:

- List the main user and group management issues.
- Explain how and when SMTP matching is used during directory synchronization.
- Describe the key DirSync monitoring and management tasks, and list issues for DirSync upgrades.


Managing Users and Groups

After DirSync has been successfully deployed and scheduled synchronization has been enabled, there are several management tasks that may need to be regularly performed.

Managing Primary SMTP addresses

One of the key user maintenance tasks is to manage user mailbox attributes, in particular primary SMTP addresses. For an on-premises user account to get the correct primary SMTP address, it needs to be mailbox-enabled, either by using the Exchange 2010 or Exchange 2013 management console, or by setting this mail attribute manually to mail-enable the user.

- Managing Primary SMTP addresses
- Recovery from Accidental Deletes
- Recovery from Unsynchronized Deletes
- Bulk Activation of New Accounts

 **Note:** If a primary SMTP address is not set for a user account, Office 365 will use an @<domain>.onmicrosoft.com as the user's default SMTP address.

If it is not possible to ensure that all synced users will have a valid primary SMTP address prior to synchronization, user attribute filtering could be used to ensure that all accounts without a valid UPN are out of synchronization scope.

Recovery from Accidental Deletes

Windows Azure Active Directory now supports soft delete. After a user is deleted in Office 365, either following a synchronization or if an unsynchronized user is manually removed in Office 365, the user's data is deleted and the user's licenses can be reassigned; however, accounts remain recoverable for 30 days. After the cloud recycle bin is purged (hard delete), it is no longer possible to restore deleted accounts.

Recovery from Unsynchronized Deletes

Another important maintenance task is dealing with an on-premises delete that does not synchronize to Office 365, so that the linked object is not removed from Windows Azure Active Directory. Such a situation may occur if directory synchronization has not yet completed, or if directory synchronization failed to delete a specific cloud object, both of which results in an orphaned Windows Azure Active Directory object.

To fix this issue, follow these steps:

1. Manually run a directory synchronization update.
2. Force directory synchronization.
3. Check that directory synchronization occurred correctly.
4. Verify directory synchronization.

If the above steps verify that synchronization is working correctly but the Active Directory object deletion has still not propagated to Windows Azure Active Directory, the orphaned object can be manually removed using one of the following Windows Azure Active Directory Module for Windows PowerShell cmdlets:

```
Remove-MsolContact
Remove-MsolGroup
Remove-MsolUser
```

For example, to manually remove an orphaned user originally created using directory synchronization, run the following cmdlet:

```
Remove-MsolUser -UserPrincipalName <username>@<Office 365 domain>
```

Accidental Account Deletion

If you accidentally delete a user account and a synchronization cycle runs, this action deletes the user in Office 365. However, if you have the recycle bin feature enabled in Active Directory, you can recover the account from the recycle bin and the link between accounts is re-established. If you do not have the recycle bin enabled, you have to create another account with a new GUID.

Bulk Activation of New Accounts

User accounts that are created in Office 365 through DirSync are not automatically activated for Office 365. It is recommended that you use scripting to manage this requirement. A simple approach makes use of Windows Azure Active Directory Module for Windows PowerShell cmdlets. For example:

```
Get-MsolAccountSku (to report the Office365 SKUs that, such as EXCHANGESTANDARD)
Get-MsolUser -UnlicensedUsersOnly | Set-MsolUser -UsageLocation <location>, such as "US"
Get-MsolUser -UnlicensedUsersOnly | Set-MsolUserLicense -AddLicenses SKU
```

The user attribute **isLicensed** indicates whether a user has a license assigned (**True**) or not (**False**). PowerShell can, therefore, be used to report on licensed Office 365 user accounts. To show all users licensed in Office 365, enter the following command at the Windows Azure Active Directory Module for Windows PowerShell prompt:

```
Get-MsolUser | Where-Object {$_.isLicensed -eq "True"}
```

To export a list of licensed Office 365 users to CSV, use the following command:

```
Get-MsolUser | Where-Object { $_.isLicensed -eq "True" } | Export-Csv
C:\Labfiles\LicensedUsers.csv
```



For more information, see Getting all Licensed Office 365 users with PowerShell at the following link:

<http://go.microsoft.com/fwlink/?LinkId=390914>

For information on a set of scripts that can automatically assign the correct SKU to users, see How to Use PowerShell to Automatically Assign Licenses to Your Office 365 Users at the following link:

<http://go.microsoft.com/fwlink/?LinkId=390915>

SMTP Matching

There are situations where the source of authority for a user account may need to be transferred from Office 365 to Active Directory if an account was originally created in Office 365 prior to directory synchronization being enabled – for example, with pilot user accounts. By transferring the source of authority, the account can then be managed in the on-premises Active Directory. Such a transfer is achieved in DirSync by using "SMTP matching," where the primary SMTP address is used to match a newly-created on-premises user account to an existing Office 365 user account.

SMTP matching is only applicable if the following conditions are met:

- The user account has an Office 365/Microsoft Exchange Online email address
- SMTP matching has not previously been used on that account
- The user account was originally authored by using Office 365 management tools

SMTP matching is only applicable if the following conditions are met:

- The user account has an Office 365/Microsoft Exchange Online email address.
- SMTP matching has not previously been used on that account, as it can only be used during one synchronization run.
- The user account was originally authored by using Office 365 management tools.

After SMTP matching has been used, the Office 365 user account is linked to the on-premises user account by an immutable identity value, not a primary SMTP address.



See the following link for information on how to use SMTP matching to match on-premises user accounts to Office 365 user accounts for directory synchronization:

<http://go.microsoft.com/fwlink/?LinkId=390916>

Monitoring and Managing DirSync

Key monitoring and management tasks for DirSync include analyzing logs for errors, and remediating sync errors with the tool itself. Typical issues that can lead to problems including:

- Installation errors, such as using incorrect on-premises or Office 365 credentials.
- Inadvertently deactivating DirSync in the portal or through PowerShell.
- Unexpected changes in Active Directory that affect OU scoping or attribute filtering.
- Corrupted Active Directory, requiring directory recovery.

- Common issues:
 - Installation errors
 - Inadvertently deactivating DirSync
 - Unexpected changes in Active Directory
 - Corrupt Active Directory
 - Deactivating, then reactivating synchronization
- Use System Center Operations Manager to monitor for problems
- Upgrading DirSync
 - Always use the latest version

As a best practice, it is recommended that you use System Center Operations Manager for monitoring the DirSync server and services such as Active Directory to ensure that problems are detected and communicated effectively to all responsible administrators. You should also make use of Windows PowerShell cmdlets and scripts to help manage Windows Azure Active Directory, report synchronization state, and so on.



For more information, see Manage Windows Azure Active Directory using Windows PowerShell at the following link:

<http://go.microsoft.com/fwlink/?LinkId=390917>

Another area that can lead to issues unless clearly understood is when you deactivate and then reactivate synchronization. When directory synchronization is deactivated, the source of authority is transferred from the on-premises Active Directory to Office 365. Deactivation is needed when on-premises Active Directory/Exchange is no longer being used to create and manage users, groups, contacts, and mailboxes, such as after a staged Exchange migration to the cloud, where the organization no longer wishes to manage objects from on-premises.

Problems can subsequently arise if directory synchronization is then reactivated, with the source of authority transferred back from Office 365 to the on-premises Active Directory.

For example, assume an organization activated directory synchronization in January, and then created new users on-premises, which were synced to Office 365. In this case, the source of authority is the on-premises Active Directory. In July, the organization deactivated directory synchronization, resulting in transfer of the source of authority to Office 365; from this point on, objects were edited in Office 365. In September, the company decided to deploy ADFS and SSO. To meet this requirement, directory synchronization was reactivated, transferring the source of authority back to the on-premises Active Directory. In this example, when directory synchronization is reactivated and run, any changes that have been made to the Office 365 objects from July through to September would be overwritten and lost.



For more information on issues to be aware of when transferring the source of authority during synchronization deactivation and reactivation, such as when federation is implemented, see the “Changing the source of authority” section in the following TechNet page:

<http://go.microsoft.com/fwlink/?LinkID=390918>

Upgrading DirSync

It is important to be on the latest version of DirSync, since the link from the Office 365 portal or admin center is always to the current release. When upgrading to a new version of DirSync, all existing filters and other management agent customizations will not be automatically imported into the new installation. If you are upgrading to a newer version of directory synchronization, you must always manually re-apply filtering configurations after you upgrade, but before you run the first synchronization cycle.

Lab: Implementing Directory Synchronization

Scenario

Lucerne Publishing is beginning to realize that cloud-based user and group management in Office 365 is failing to meet the organization's needs. Users are forgetting passwords, and helpdesk calls are up 68 percent. As a result, the company is anxious to investigate DirSync and password synchronization for user and group management.

Objectives

To provide the students with practical experience of planning and deploying DirSync.

Lab Setup

Estimated Time: 120 minutes

Virtual machine: 20346C-LUC-CL1

Username: **Student1**

Password: **Pa\$\$w0rd**

In all tasks, where you see references to lucernepublishingXXXX.onmicrosoft.com, replace the XXXX with the unique Lucerne Publishing number that you were assigned when you set up your Office 365 account in Module 1, Lab 1B, Exercise 2, Task 3, Step 5.

Where you see references to labXXXXX.o365ready.com, replace the XXXXX with the unique o365ready.com number you were assigned when you registered your IP address at www.o365ready.com in Module 2, Lab 2B, Exercise 1, Task 2, Step 6.

Exercise 1: Prepare on-premises Active Directory for DirSync

Scenario

Over the last few weeks, it has been particularly obvious that, as predicted by Alain Richer, cloud-based user and group management simply isn't working. The company needs to move to a different model for organizing users and groups between its on-premises and cloud-based environments. As a result, the deployment team has been analyzing DirSync functionality and the option of Password Sync. Before this deployment can proceed, there are several checks that the team needs to run; these include looking for duplicate accounts, filtering the directory, and correcting UPNs.

The main tasks for this exercise are as follows:

1. Prepare Problem User Accounts
2. Remediate AD Errors with IDFix
3. Remediate AD Errors with ADModify
4. Activate Directory Synchronization
5. Create an Enterprise Administrator Account for Use in DirSync Setup

► Task 1: Prepare Problem User Accounts

1. On your host computer, switch to the **20346C-LUC-CL1** virtual machine.
2. Ensure you are logged on as **Student1** with a password of **Pa\$\$word**.
3. On the **LUC-CL1** computer, on the Desktop, on the Taskbar, click **File Explorer**.
4. Navigate to **E:\RDP_files**.

5. Double-click **LUC-EX1.rdp**, and connect as **LUCERNE\LucAdmin**, password: **Pa\$\$w0rd**.
6. On the Start screen, type **PowerShell**.
7. Right-click **Windows PowerShell**, and then click **Run as administrator**.
8. At the Windows PowerShell prompt, type the following command, and press Enter:

```
CD C:\Temp
```

9. At the Windows PowerShell prompt, type the following command, and press Enter:

```
Set-ExecutionPolicy Unrestricted
```

10. Press Enter to confirm the execution policy change.
11. At the Windows PowerShell prompt, type the following command, and press Enter:

```
.\CreateProblemUsers.ps1
```

Important: Wait until the script has completed before proceeding to the next step.

12. In **LUC-CL1**, double-click on **E:\RDPFiles\LUC-DC1.rdp** and log on as **LUCERNE\LucAdmin**, password: **Pa\$\$w0rd**.
13. In **Server Manager**, click **Tools**, and then click **ADSI Edit**.
14. In **ADSI Edit**, in the navigation pane, right-click **ADSI Edit**, and click **Connect to**.
15. In the **Connection Settings** dialog box, click **OK**.
16. In the navigation pane, expand **Default naming context**, then expand **DC=lucernepublishing,DC=local**, and then click **OU=Engineering**.
17. In the **Results** pane, right-click **dshivers**, and then click **Properties**.
18. In the **Properties** dialog box, in the **Attributes** list, select **userPrincipalName**, and then click **Edit**.
19. In the **String Attribute Editor**, add a "|" character in front of "lucerne", and click **OK**.
20. Click **OK**, to close the Properties dialog box.
21. In the **Results** pane, right-click **kfredrickson**, and then click **Properties**.
22. In the **Properties** dialog box, in the **Attributes** list, select **mailnickname**, and then click **Edit**.
23. In the **String Attribute Editor**, replace the existing string with "duplicate", and click **OK**.
24. Click **OK**, to close the Properties dialog box.
25. In the **Results** pane, right-click **bhowerton**, and then click **Properties**.
26. In the **Properties** dialog box, in the **Attributes** list, select **mailnickname**, and then click **Edit**.
27. In the **String Attribute Editor**, replace the existing string with "duplicate", and click **OK**.
28. Click **OK**, to close the Properties dialog box.
29. In the **Results** pane, right-click **gdonato**, and then click **Properties**.
30. In the **Properties** dialog box, in the **Attributes** list, select **mailnickname**, and then click **Edit**.
31. In the **String Attribute Editor**, add quote marks around the existing string, and click **OK**.
32. Click **OK**, to close the Properties dialog box.
33. In the **Results** pane, right-click **bbeach**, and then click **Properties**.

34. In the **Properties** dialog box, in the **Attributes** list, select **mailnickname**, and then click **Edit**.
35. In the **String Attribute Editor**, replace the existing string with a single space, and click **OK**.
36. Click **OK**, to close the Properties dialog box.

► **Task 2: Remediate AD Errors with IdFix**

1. Switch to the **LUC-CL1** virtual machine session.
2. On the Desktop, on the Taskbar, click **File Explorer**.
3. Navigate to **E:\RDP_files**.
4. Double-click **LUC-CL2.rdp**, and connect as **LUCERNE\LucAdmin**, password: **Pa\$\$w0rd**.
5. On the Start screen, click **Computer**.
6. Navigate to **\\LUC-DC1\C\$\Labfiles\Lab10**, and double-click **IdFix**.

Note: When connecting to **LUC-DC1**, Microsoft's testing has, on rare occasions, received a message asking if you want to install updates. Do NOT install updates if such a message appears.

7. If an **Open File – Security Warning** dialog box appears, click **Run**.
8. In the **WinZip Self-Extractor** dialog box, click **Unzip**, click **OK**, and then click **Close**.
9. In File Explorer, navigate to **C:\Deployment Tools\IdFix**, then right-click **IdFix**, and click **Run as administrator**.
10. In the **IdFix Privacy Statement** message box, click **OK**.
11. Click **Query**. You should see a number of errors, which may vary per student.
12. Click the **ERROR** column to bring the character errors to the top.

Note: Ignore **topleveldomain** errors, which cannot be fixed by the IdFix tool.

13. For each distinguished name that includes a character error, in the **ACTION** column, select **EDIT**; there should be three objects to select.
14. On the toolbar, click **Apply**.
15. In the **Apply Pending** dialog box, click **Yes**; note the **COMPLETE** status in the **ACTION** column indicating successful writes.
16. Switch to **File Explorer**, and in the **C:\Deployment Tools\IdFix** folder, double-click **Verbose <date> <time>.txt**, to view the updated transactions in the transaction log.
17. Switch back to **IdFix**.
18. On the toolbar, click **Query**.
19. Note that one of your fixes has introduced a new error (the **mailnickname** now has brackets).
20. Click in the **UPDATE** column for the **Beverley Beach** error, and replace the string with **bbeach**, to meet the requirements for this string (initial+surname), and then in the **ACTION** column, select **EDIT**.
21. Click in the **UPDATE** column for the **Kelly Fredrickson** error, and replace the string with **kfredrickson**, to meet the requirements for this string (initial+surname), and then in the **ACTION** column, select **EDIT**.

22. Click in the **UPDATE** column for the **Bobby Howerton** error, and replace the string with **bhowerton**, to meet the requirements for this string (initial+surname), and then in the **ACTION** column, select **EDIT**.
23. On the toolbar, click **Apply**.
24. In the **Apply Pending** box, click **Yes**.
25. On the toolbar, click **Query**; the only remaining errors apply to multiple users, and IdFix cannot suggest a fix.
26. Note the results:
 - dshivers = | in userPrincipalName generates character error, idfix can fix this.
 - gdonato = "mailnickname" generates character error, idfix can fix this.
 - bbeach = space for mailnickname generates character error, idfix can fix this.
 - All users = format error on proxyAddresses and userPrincipalName contains @local.

Note: Where there are format and duplicate errors for distinguished names, the UPDATE column either contains the same string as the VALUE column, or the UPDATE column entry is blank; in either case, this means that IdFix cannot suggest a remediation for the error.

You can either fix these errors outside IdFix, or manually remediate them within IdFix. You will fix specific individual errors in IdFix, but use another tool, ADModify, to fix errors that apply to multiple users.

► Task 3: Remediate AD Errors with ADModify

1. Press the Windows key to go to the Start screen.
2. On the Windows Start screen, right-click **Windows PowerShell**, and then click **Run as administrator**.
3. If you get a **User Account Control** dialog box, click **Yes**.
4. At the **Windows PowerShell** prompt, type the following command, and press Enter:

```
Set-ExecutionPolicy Unrestricted
```

5. Press Enter to confirm the execution policy change.
6. At the Windows PowerShell prompt, type the following command, and press Enter:

```
Add-WindowsFeature NET-Framework-Core -Source C:\Windows\WinSxS
```

7. Wait for the installation to complete, which may take about 10 minutes.
8. On **LUC-CL2**, on the Task Bar, click **File Explorer**.
9. Navigate to **\\LUC-DC1\C\$\Labfiles\Lab10**, and right-click **ADModify_2.1**, and then click **Extract All**.
10. In the **Extract Compressed (Zipped) Folders** dialog box, click **Browse**, and navigate to **C:\Users\LucAdmin\My Documents**.
11. Click **OK**.
12. In the **Extract Compressed (Zipped) Folders** dialog box, click **Extract**.
13. In **My Documents**, right-click **ADModify**, and click **Run as administrator**.

14. In **ADModify.NET**, click **Modify Attributes**.
15. Click in the **Domain List**, and select **DC=lucernepublishing,DC=local**.
16. Click in the **Domain Controller List**, and select **LUC-DC1.lucernepublishing.local**, and then click the right arrow.
17. In the **Domain Tree List**, click **lucernepublishing**, then click **+**, then select **Engineering**, and then click **Add To List**.
18. In the **Results** pane, select all the objects, and then click **Next**.
19. In the **ADModify.NET** dialog box, click the **Account** tab.
20. Select the **UPN** check box, then click **Legacy Account**, and then in the UPN list, select your lab UPN in the form **labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number).
21. Click the **E-Mail Addresses** tab.
22. Select the **Add SMTP Address** check box.
23. In the text box, replace the existing string with **'userPrincipalName'%**.
24. Select the **Set as Primary** check box.
25. Select the **Remove E-Mail Address** check box.
26. In the text box, replace the existing string with **smtp:*@*lucernepublishing.local**.
27. Click **Go**.
28. In the dialog box, note the name of the results XML file, and then click **OK**.
29. In **File Explorer**, double-click the results XML file you noted above, to view the results in Internet Explorer.
30. Close Internet Explorer.
31. On **LUC-CL2**, switch to **IdFix**.
32. On the toolbar, click **Query**; the accounts that you fixed should no longer appear.
Note: There will be other account errors for system accounts that are unconnected with this lab.
33. Close IdFix.

► Task 4: Activate Directory Synchronization

1. Switch to the **LUC-CL1** virtual machine session.
2. Press the Windows key to go to the Start screen.
3. On the Windows Start screen, right-click Windows Azure Active Directory Module for Windows PowerShell, and then click Run as administrator.
4. In the **User Account Control** dialog box, click **Yes**.
5. At the **Windows Azure Active Directory Module for Windows PowerShell** prompt, type the following command, and press Enter:

```
Set-ExecutionPolicy Unrestricted
```

6. Press Enter to confirm the execution policy change.
7. At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
$msolcred = Get-Credential
```

8. In the **Windows PowerShell Credential** dialog box, enter **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number) in the **User name** box, enter **Pa\$\$w0rd** in the **Password** box, and then click **OK**.
9. At the **Windows Azure Active Directory Module for Windows PowerShell** prompt, type the following command, and press Enter:

```
Connect-MsolService -Credential $msolcred
```

10. At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Set-MsolDirSyncEnabled -EnabledDirSync $true -Force
```

Note: The *-Force* switch disables the confirmation dialog box.

11. Although you may have to wait up to 24 hours for activation to complete, you should be able to continue.
12. At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
(Get-MsolCompanyInformation).DirectorySynchronizationEnabled
```

13. The output returns **"True"** if sync is enabled.

Note: It may take a few minutes to return "True". Re-run the command until you see "True" showing.

14. Switch to Internet Explorer, and in the address box, type **http://portal.microsoftonline.com**, and press Enter.
15. On the **Sign** page, in the **Name** box, type **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number). In the **Password** box, type **Pa\$\$w0rd**, and then click **Sign in**.
16. In the **Office 365 admin center**, in the left navigation, click **Users**, and then click **Active users**.
17. To the right of **Active Directory synchronization**, verify that there is a **Deactivate** link (if activation was not yet completed, this link would say "Activate").

► Task 5: Create an Enterprise Administrator Account for Use in DirSync Setup

1. Switch to the **LUC-CL1** virtual machine session.
2. On the Desktop, on the Taskbar, click **File Explorer**.
3. Navigate to **E:\RDP_files**.
4. Double-click **LUC-DC1.rdp**, and connect as **LUCERNE\LucAdmin**, password: **Pa\$\$w0rd**.
5. On **LUC-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
6. In the console tree, expand **lucernepublishing.local**, right-click **Users**, point to **New**, and then click **User**.
7. In the **Full name** and **User logon name** boxes, type **dirsync-admin**, and then click **Next**.

8. In the **Password** and **Confirm password** boxes, type **Pa\$\$w0rd**, clear the **User must change password at next logon** check box, select the **Password never expires** check box, and then click **Next**, and then click **Finish**.
9. In **Active Directory Users and Computers**, expand **Users**, and then double-click **dirsync-admin**.
10. In **dirsync-admin Properties**, click the **Member Of** tab, and then click **Add**.
11. In the **Select Groups** dialog box, in the **Enter the object names to select** box, type the following group names: **domain admins; enterprise admins**
12. Click **Check Names**.
13. Click **OK** to close the **Select Groups** dialog box.
14. Click **OK** to close the **dirsync-admin Properties** dialog box.

Results: At the end of this exercise, the implementation of DirSync can now proceed at Lucerne Publishing. Specifically, any accounts in Active Directory that will prevent synchronization have been identified, directory filtering has been applied, UPNs corrected, and the Enterprise Administrator account recreated.

Exercise 2: Set up DirSync

Scenario

With all the problem user accounts identified, Lucerne Publishing is ready to install DirSync and run its first directory synchronization. The company has decided to start with just DirSync, and once the on-premises directory has successfully synchronized, it will then enable password synchronization.

The main tasks for this exercise are as follows:

1. Download and Install DirSync
2. Install Windows Azure Active Directory Module for Windows PowerShell
3. Configure DirSync
4. Perform Initial Synchronization
5. Implement Password Synchronization
6. Verify Password Synchronization

► Task 1: Download and Install DirSync

1. On **LUC-DC1**, in **Server Manager**, in the navigation pane, click **Local Server**.
2. In the Properties for **LUC-DC1**, next to **IE Enhanced Security Configuration**, click **On**.
3. In the **Internet Explorer Enhanced Security Configuration** dialog box, select **Off** for **Administrators**, and then click **OK**.
4. Close Server Manager.
5. On **LUC-DC1**, press the Windows key, to go to the Start screen.
6. On the Windows Start screen, click **Internet Explorer**.
7. If you get a **Windows Internet Explorer 10** dialog box, select **Use recommended security and compatibility settings**, and then click **OK**.

8. In the **Address** box, type **http://portal.microsoftonline.com**, and press Enter.
9. On the **Sign** page, in the **Name** box, type **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number).
10. In the **Password** box, type **Pa\$\$w0rd**, and then click **Sign in**.
11. In the **Office 365 admin center**, in the left navigation, click **Users**, and then click **Active users**.

Note: If you see the **Active Directory synchronization is being activated** warning banner, you can ignore it at this time, but you will not be able to run directory synchronization later in this exercise. You must wait until directory synchronization is activated. However, you can complete the following steps, even if you do see the warning message.

12. To the right of **Active Directory synchronization**, click **Manage** (or if Active Directory synchronization has not yet completed, click **Set up**).
13. Under **Install and configure the Directory Sync tool**, click **Download**.
14. In the Internet Explorer notification bar, click **Save**, click **Save as**, then browse to **C:\Labfiles**, and click **Save**.
15. When the download has completed, in the Internet Explorer notification bar, click **Open folder**.
16. In File Explorer, right-click **dirsysnc.exe**, and then click **Run as administrator**.
17. In the **Windows Azure Active Directory Sync Setup** wizard, on the **Welcome** page, click **Next**.
18. On the **Microsoft Software License terms** page, click **I accept**, and click **Next**.
19. On the **Select Installation Folder** page, click **Next**.

Note: The installation process will take around 10 minutes to complete.

20. When the installation is complete, on the **Installation** page, click **Next**.
21. On the **Finished** page, clear the **Start Configuration Wizard now** check box, and click **Finish**.

IMPORTANT: Do NOT run the configuration wizard at this time. Make sure you clear the **Start Configuration Wizard now** check box. You need to log off and log on again to add your user account to the Synchronization Engine FIMSyncAdmins group; you will do this at the start of the next task.

► Task 2: Install Windows Azure Active Directory Module for Windows PowerShell

1. On **LUC-DC1**, press the Windows key to go to the Start screen.
2. On the Windows Start screen, click **lucadmin**, and then click **Sign out**.
3. On the **LUC-CL1** virtual machine session, on the Desktop, on the Taskbar, click **File Explorer**.
4. Navigate to **E:\RDP_files**.
5. Double-click **LUC-DC1.rdp**, and connect as **LUCERNE\LucAdmin**, password: **Pa\$\$w0rd**.
6. On **LUC-DC1**, press the Windows key, to go to the Start screen, and click **Computer**.
7. In File Explorer, in **C:\Labfiles\Lab10**, double-click **AdministrationConfig-EN**.
8. In the **Windows Azure Active Directory Module for Windows PowerShell Setup** wizard, on the **Welcome** page, click **Next**.
9. On the **License Terms** page, click **I accept the terms in the License Terms**, and click **Next**.
10. On the **Install Location** page, click **Next**.

11. On the **Ready to Install** page, click **Install**.
12. In the **User Account Control** dialog box, click **Yes**.
13. On the **Completing the Windows Azure Active Directory Module for Windows PowerShell Setup** page, click **Finish**.

► **Task 3: Configure DirSync**

1. On the Desktop, double-click **Directory Sync Configuration**.
2. In the **Windows Azure Active Directory Sync tool Configuration Wizard**, on the **Welcome** page, click **Next**.
3. On the **Windows Azure Active Directory Credentials** page, enter the following credentials, and click **Next**:
 - User name: **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number)
 - Password: **Pa\$\$w0rd**
4. On the **Active Directory Credentials** page, enter the following credentials, and then click **Next**:
 - User name: **LUCERNE\LucAdmin**
 - Password: **Pa\$\$w0rd**

Note: This account information is required to set up permissions.

5. On the **Hybrid Deployment** page, ensure that **Enable Hybrid Deployment** is NOT checked, and click **Next**.
6. On the **Password Synchronization** page, ensure that **Enable Password Sync** is NOT checked, and click **Next**.

Note: You will set up password synchronization later in this lab.
7. When the configuration has completed, on the **Configuration** page, click **Next**.
8. On the **Finished** page, clear the **Synchronize your directories now** check box, and click **Finish**.

Note: You clear this check box because you are setting up OU filtering in the next step.
9. On the **Desktop**, on the **Taskbar**, click **File Explorer**.

10. Navigate to **C:\Program Files\Windows Azure Active Directory Sync\SYNCBUS\Synchronization Service\UIShell**.
11. Double-click **miisclient.exe**.
12. In **Synchronization Service Manager**, click the **Management Agents** tab.
13. In the **Management Agents** tab, double-click **Active Directory Connector**.
14. In the **Properties** dialog box, click **Configure Directory Partitions**.
15. Click **Containers**.

Note: The credentials dialog box initially displays the MSOL_<id> account; this account uses a randomly generated password, so administrators will not know it.

16. In the **Credentials** dialog box, enter the following credentials, and click **OK**:
 - User name: **dirsync-admin**
 - Password: **Pa\$\$w0rd**

- Domain: **LUCERNE**

Note: This account is the one used for synchronization.

17. In the **Select Containers** dialog box, clear the **root level** check box, then select only the **Accounts** and **Sales** check boxes, and then click **OK**.
18. In the **Properties** dialog box, click **Configure Connector Filter** and then in the **Data Source Object Type** grid, scroll down and select the **User** object.

Note: All filters defined for the User object will be displayed. Note the FIM accounts that are excluded from sync by default.

19. With **User** selected in the Data Source Object Type grid, click **New**.
20. In the **Filter for user** dialog box, in the **Data Source attribute** list, select **extensionAttribute15**, in the **Operator** list, select **Equals**, and then in the **Value** box, type **NoSync**.
21. Click **Add Condition**, and then click **OK** to close the **Filter for user** dialog box.
22. With **User** selected in the **Data Source Object Type** grid, click **New**.
23. In the **Filter for user** dialog box, in the **Data Source attribute** list, select **sAMAccountName**, in the **Operator** list, select **Starts with**, and then in the **Value** box, type **SM_**.
24. Click **Add Condition**, and then click **OK**, to close the **Filter for user** dialog box.
25. Click **OK** to close the Properties dialog box.

Note: Because you have filtered on Accounts and Sales OUs, the Exchange 2013 Health Mailboxes would not sync anyway as they are in the Users container; however, this is still good practice, as OU filtering might change in the future.

26. In **Synchronization Service Manager**, on the **Management Agents** tab, right-click **Active Directory Connector**, and click **Export Management Agent**.
27. In the **Save As** dialog box, browse to **C:\Labfiles**, and in the **File name** box, type **AD_Connector**, and then click **Save**.

► Task 4: Perform Initial Synchronization

1. In **Synchronization Service Manager**, on the **Management Agents** tab, right-click **Active Directory Connector**, and click **Run**.
2. In the **Run Management Agent** dialog box, click **Full Import Full Sync**, and then click **OK**.
3. Right-click the **Windows Azure Active Directory Connector** and click **Run**.
4. In the **Run Management Agent** dialog box, click **Export**, and then click **OK**.
5. Press the Windows key to go to the Start screen.
6. On the Windows Start screen, double-click **Windows Azure Active Directory Module for Windows PowerShell**.
7. At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Connect-MsolService
```

8. In the **Enter Credentials** dialog box, enter the following credentials, and click **OK**:

- User name: **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number)
 - Password: **Pa\$\$w0rd**
9. At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Get-MsolCompanyInformation | fl LastDirSyncTime
```

10. On **LUC-DC1**, press the Windows key, to go to the Start screen.
11. On the Windows Start screen, click **Internet Explorer**.
12. In the **Address** box, type **http://portal.microsoftonline.com**, and press Enter.
13. On the **Sign** page, in the **Name** box, type **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number).
14. In the **Password** box, type **Pa\$\$w0rd**, and then click **Sign in**.
15. In the **Office 365 admin center**, in the left navigation, click **Users**, and then click **Active users**.
16. Verify that the message **Last synced less than an hour ago** is displayed.
17. In the **Active users** list, note that your on-premises accounts from the Accounts and Sales OUs now have a status of **Synced with Active Directory**.
18. In the **Active users** list, verify that your users from the Engineering OU have not been synced to Office 365.
19. In the **Active users** list, verify that your Office 365 users have a status of **In cloud**. These users should include:
- The mail user account you created for yourself.
 - The Main Conference room.
 - The Main Conference room projector.
 - The Marketing Department group.
20. In **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
21. In **Active Directory Users and Computers**, open the **Users** OU, and verify that the Office 365 users from this OU have not been synchronized from the on-premises Active Directory to Office 365.
22. Open the **Engineering** OU and verify that these users have not been synchronized from the on-premises Active Directory to Office 365.

► Task 5: Implement Password Synchronization

1. On **LUC-DC1**, switch to the **Office 365 admin center** session in Internet Explorer logged in as **Heidi Leitner**.
2. In the **Active users** list, select the check box for **William Douglas**.
3. Under **Quick steps**, click **Reset passwords**.
4. On the **Send results in email** page, click **Reset password**.
5. On the **Results** page, note the temporary password here

.....

6. Click **Finish**.
7. Switch to the **LUC-CL2** RDP session.
8. Press the Windows key to go to the Start screen.
9. On the Start screen, click **LucAdmin**, and then click **Sign out**.
10. On the **LUC-CL1** virtual machine session, on the Taskbar, click **File Explorer**.
11. Navigate to **E:\RDP_files**, double-click **LUC-CL2.rdp**, and connect as **LUCERNE\ wdouglas**, password: **Pa\$\$w0rd**.
12. On the Windows Start screen, click **Internet Explorer**.
13. If you get a **Windows Internet Explorer 10** dialog box, select **Use recommended security and compatibility settings**, and then click **OK**.
14. In the **Address** box, type **http://portal.microsoftonline.com**, and press Enter.
15. On the **Sign** page, in the **Name** box, type **wdouglas@labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number).
16. In the **Password** box, type the temporary password you noted above, and then click **Sign in**.
17. On the **Update password** page, in the **Old password** box, type the temporary password, and in the **New password** and **Confirm new password** boxes, type **N3wPa\$\$w0rd**, and then click **Save**.
18. On the **Office 365** page, in the **Password** box, type **N3wPa\$\$w0rd**, and then click **Sign in**.
19. Verify that you can sign in to Office 365 with your updated password.
20. On the **Getting started with Office 365** page, click **William Douglas**, and then click **Sign Out**.
21. Switch to the **LUC-DC1** session.
22. On **LUC-DC1**, on the **Desktop**, double-click **Directory Sync Configuration**.
23. In the **Windows Azure Active Directory Sync tool Configuration Wizard**, on the **Welcome** page, click **Next**.
24. On the **Windows Azure Active Directory Credentials** page, enter the following credentials, and click **Next**:
 - User name: **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number)
 - Password: **Pa\$\$w0rd**
25. On the **Active Directory Credentials** page, enter the following credentials, and then click **Next**:
 - User name: **lucadmin@lucernepublishing.local**
 - Password: **Pa\$\$w0rd**
26. On the **Hybrid Deployment** page, ensure that **Enable Hybrid Deployment** is NOT checked, and click **Next**.
27. On the **Password Synchronization** page, select the **Enable Password Sync** check box, and click **Next**.
28. When the configuration has completed, on the **Configuration** page, click **Next**.
29. On the **Finished** page, verify that the **Synchronize your directories now** check box is selected; select this check box if it is not checked by default. Click **Finish**.

30. On the **Windows Azure Active Directory Sync tool Configuration Wizard** dialog box, click **OK**.

► **Task 6: Verify Password Synchronization**

1. In **Server Manager**, click **Tools**, and then click **Event Viewer**.
2. In **Event Viewer**, in the console tree, expand **Windows Logs**, and then click **Application**.
3. Select **Directory Synchronization events, Event ID 656**.

Note: This lists all password change requests for synchronized users.

4. Select **Directory Synchronization events, Event ID 657**.

Note: This lists all successful password change requests.

5. Switch to the **LUC-CL2** session.
6. In Internet Explorer, on the **Office 365 Sign** page, in the **Name** box, type **wdouglas@labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number), in the **Password** box, type **N3wPa\$\$w0rd** (the Office 365 password you just set), then click **Sign in**.
7. You will see a **We don't recognize this user ID or password** message. Enter **Pa\$\$w0rd** (the on-premises password), and then click **Sign in**.
8. Verify that you can sign in to Office 365 with the same password as is used for Active Directory on-premises.
9. On the **Getting started with Office 365** page, click **William Douglas**, and then click **Sign Out**.

Results: Lucerne Publishing has configured Directory Synchronization, migrated its users and groups into Office 365, and then enabled password synchronization.

Exercise 3: Manage Active Directory users and groups with DirSync in place

Scenario

Now that DirSync and password sync are in place, Lucerne Publishing needs to modify its user and group management procedures so that all users and groups are created and edited in Active Directory. At that point, all additions, deletions, and updates will be synchronized to Office 365.

The main tasks for this exercise are as follows:

1. Add New Users in AD Using GUI Tools, and then Sync
2. Add New Users in AD Using PowerShell, then Sync and Activate
3. Modify AD Users and then Sync
4. Delete AD Users and then Sync
5. Set a User as NoSync and Verify Office 365 Removal

► **Task 1: Add New Users in AD Using GUI Tools, and then Sync**

1. On **LUC-EX1**, in **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, expand **lucernepublishing.local**, right-click **Sales**, point to **New**, and then click **User**.

3. In the **First name** box, type **Lynette**.
4. In the **Last name** box, type **Kelly**.
5. In the **User logon name** box, type **lkelly**, then select your lab domain UPN (**not** `lucernepublishing.local`), and then click **Next**.
6. In the **Password** and **Confirm password** boxes, type **Pa\$\$w0rd**, clear the **User must change password at next logon** check box, select the **Password never expires** check box, click **Next**, and then click **Finish**.
7. In the **User** list, double-click **Lynette Kelly**.
8. In the **Properties** dialog box, in the **E-mail** box, type **lkelly@<your lab domain UPN>**, and click **OK**.
9. Switch to the **LUC-CL1** virtual machine session.
10. On the Desktop, on the Taskbar, click the **LUC-DC1 RDP** session.
11. On the desktop, right-click the **Windows PowerShell** shortcut and click **Run as administrator**.

Note: This generic Windows PowerShell session is now configured as a **DirSyncConfigShell** session.

12. If a **User Account Control** dialog box appears, click **Yes**.
13. At the prompt, type the following command and press Enter:

```
Set-ExecutionPolicy Unrestricted
```

14. Press Enter again to confirm the operation.
15. At the prompt, type the following command and press Enter:

```
Import-Module DirSync
```

16. At the prompt, type the following command, and press Enter:

```
Start-OnlineCoexistenceSync
```

17. On **LUC-DC1**, switch to the **Office 365 Admin Center** session in Internet Explorer.
18. In the **Office 365 Admin Center**, in the left navigation, click **Users**, and then click **Active users**.
19. In the **Active users** list, verify that **Lynette Kelly** has a status of "**Synced with Active Directory**".
20. In the **Active users** list, select the check box for **Lynette Kelly**.
21. Note that under **Quick Steps** there is an option to **Activate synced users**, as DirSync does not automatically activate synced new accounts in Office 365. Click **Activate synced users**.
22. On the **Assign Licenses** page, select **Switzerland** and then click **Activate**.
23. On the **Results** page, note that the password has not been reset, as password synchronization is now in operation.
24. On the **Results** page, click **Finish**.

► **Task 2: Add New Users in AD Using PowerShell, then Sync and Activate**

1. On **LUC-DC1**, on the Desktop, on the Taskbar, click **File Explorer**.
2. Navigate to **C:\Labfiles\Lab10**.

3. Double-click **SalesUserNames.csv**.
4. In the **How do you want to open this type of file?** dialog box, click **Notepad**.
5. Note the new accounts that you will create, and then close Notepad.
6. Right-click **CreateUsers.ps1**, and click **Edit**.
7. In the **PowerShell ISE**, note the code you will use to create new accounts, especially UPN and email setting.
8. At the **Windows PowerShell** prompt, type the following command, and press Enter:

```
Set-ExecutionPolicy Unrestricted
```

9. At the **Execution Policy Change** dialog box, click **Yes**.
10. In the **PowerShell ISE**, on the toolbar, click **Run Script**.
11. At the first prompt, type **SalesUserNames.csv**, and press Enter.
12. At the second prompt, type **<your lab upn>** in the form **labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number), and press Enter.
13. Switch to the **Windows PowerShell** session used for the DirSync configuration on LUC-DC1.
14. At the **Windows PowerShell** prompt, type the following command, and press Enter:

```
Start-OnlineCoexistenceSync
```

15. Switch to the **Windows Azure Active Directory Module for Windows PowerShell** session.
16. At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Get-MsolAccountSku
```

Note: If the number of **ConsumedUnits** is the same as the number of **ActiveUnits**, you will not be able to do the next step.

17. Note the sku details: for example, **LucernePublishingXXXX:ENTERPRISEPACK** (where XXXX is your unique Lucerne Publishing number).
18. At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Get-MsolUser
```

Note: All Office 365 users are shown.

19. At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Get-MsolUser -Synchronized
```

Note: Only the users that have been synced from on-premises are shown, including William Douglas and Lynette Kelly and these are already enabled for Office 365. (isLicensed = True.)

20. At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Get-MsolUser -UnlicensedUsersOnly
```

Note: William Douglas and Lynette Kelly are not shown, as they are already enabled for Office 365.

- At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Get-MsolUser -Search Wade
```

- Verify that this user is listed.
- At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Get-MsolUser -Search Wade | Set-MsolUser -UsageLocation CH
```

- At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Get-MsolUser -Search Wade | Set-MsolUserLicense -AddLicenses  
LucernePublishingXXXX:ENTERPRISEPACK
```

(where XXXX is your unique Lucerne Publishing number).

Note: This command adds a mailbox for this user.

- At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Get-MsolUser | Where-Object {$_.isLicensed -eq "True"}
```

- Verify that your new user is now licensed in Office 365.

► Task 3: Modify AD Users and then Sync

- At the **Windows Azure Active Directory Module for Windows PowerShell** prompt, type the following command, and press Enter:

```
Get-MsolUser | ft DisplayName, Office, City, Title
```

Note: The current Office, City, and Title for Lynette Kelly should be blank.

- Switch to **Active Directory Users and Computers**.
- In the console tree, expand **lucernepublishing.local**, and click **Sales**.
- In the **User** list, double-click **Lynette Kelly**.
- In the **Properties** dialog box:
 - On the **General** tab, type **Western Europe Sales** in the **Office** field, and then click **Apply**.
 - On the **Address** tab, type **Paris** in the **City** field, and then click **Apply**.
 - On the **Organization** tab, type **Sales Manager** in the **Job Title** field, and then click **OK**.
- Switch to the **Windows PowerShell** session used for the **DirSync configuration on LUC-DC1**.
- At the Windows PowerShell prompt, type the following command, and press Enter:

```
Start-OnlineCoexistenceSync
```

8. Switch to the **Windows Azure Active Directory Module for Windows PowerShell** session.
9. At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Get-MsolUser | ft DisplayName, Office, City, Title
```

10. Verify that the new Office, City, and Title for Lynette Kelly are shown.

► Task 4: Delete AD Users and then Sync

1. At the **Windows Azure Active Directory Module for Windows PowerShell** prompt, type the following command, and press Enter:

```
Get-MsolAccountSku
```

2. Note the number of **ConsumedUnits**.
3. At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Get-MsolUser -Search Lynette
```

4. Verify that the new user is listed.
5. Switch to **Active Directory Users and Computers**.
6. In the console tree, expand **lucernepublishing.local**, and click **Sales**.
7. In the **User** list, right-click **Lynette Kelly**, and then click **Delete**.
8. In the **Active Directory Domain Services** dialog box, click **Yes**.
9. Switch to the **Windows PowerShell** session used for the **DirSync configuration** on **LUC-DC1**.
10. At the Windows PowerShell prompt, type the following command, and press Enter:

```
Start-OnlineCoexistenceSync
```

11. Switch to the **Windows Azure Active Directory Module for Windows PowerShell** session.
12. At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Get-MsolUser -Search Lynette
```

13. Verify that no user is listed.
14. At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Get-MsolAccountSku
```

15. Note the number of **ConsumedUnits** is now one less than before.

► Task 5: Set a User as NoSync and Verify Office 365 Removal

1. At the **Windows Azure Active Directory Module for Windows PowerShell** prompt, type the following command, and press Enter:

```
Get-MsolUser -Search William
```


2. Verify that the user is listed.
3. On **LUC-DC1**, switch to **ADSI Edit**.
4. In **ADSI Edit**, in the navigation pane, expand **Default naming context**, then expand **DC=lucernepublishing,DC=local**, and then click **OU=Accounts**.
5. In the **Results** pane, right-click **William Douglas**, and then click **Properties**.
6. In the **Properties** dialog box, in the **Attributes** list, select **extensionAttribute15**, and then click **Edit**.
7. In the **Attribute Editor**, in the **Value** box, type **NoSync**, and click **OK**, to close the Attribute Editor.
8. Click **OK**, to close the Properties dialog box.
9. Switch to the **Windows PowerShell** session used for the **DirSync configuration** on **LUC-DC1**.
10. At the Windows PowerShell prompt, type the following command, and press Enter:

```
Start-OnlineCoexistenceSync -FullSync
```

Note: This needs to be a full sync.

11. At the **Windows Azure Active Directory Module for Windows PowerShell** prompt, type the following command, and press Enter:

```
Get-MsolUser -Search William
```

12. Verify that no user is listed.
13. At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Get-MsolAccountSku
```

14. Note the number of **ConsumedUnits** is now one less than before.

Lab Review Discussion Questions

How do you configure OU-level filtering when using DirSync?

Miisclient.exe is used to configure details of the synchronization tasks to be performed during directory synchronization operations, including configuration of OU-level filtering.


How can you initiate an immediate directory synchronization, without waiting for the default synchronization interval?

You can use **Miisclient.exe**, or the **Start-OnlineCoexistenceSync** command in Windows PowerShell by importing the DirSync PowerShell module.

- How do you configure OU-level filtering when using DirSync?
- How can you initiate an immediate directory synchronization, without waiting for the default synchronization interval?

Module Review and Takeaways

Having completed this module, you can now prepare an on-premises environment ready for directory synchronization, install and configure DirSync, and manage Active Directory users in a DirSync enabled scenario.

-  **Best Practice:** You must have a proper project plan.
- If using filtering, it should be set up before synchronizing any objects.
- You should work with a cloud services partner.
- You should perform thorough capacity planning.
- You should remediate the Active Directory before building the DirSync infrastructure.
- You should add all SMTP domains as verified domains before synchronizing.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
DirSync filtering is no longer working.	

Module 11

Implementing Active Directory Federation Services

Contents:

Module Overview	11-1
Lesson 1: Planning for AD FS	11-2
Lesson 2: Install and Manage AD FS Servers	11-14
Lesson 3: Install and Manage AD FS Proxy Servers	11-22
Lab: Implementing Active Directory Federation Services	11-26
Module Review and Takeaways	11-43

Module Overview

In this module, you will learn how to plan for single sign-on (SSO) by using Active Directory® Federation Services (AD FS) and then cover the process for setting up an AD FS server farm and an AD FS proxy. This module also covers the management process for certificates and the AD FS servers.

Objectives

After completing this module, you should be able to:

- Plan for an AD FS deployment.
- Install and manage AD FS servers.
- Install and manage AD FS proxies.

Lesson 1

Planning for AD FS

In this lesson, you will learn about the concepts and requirements for AD FS, such as namespaces and certificates. You will examine the process of planning AD FS internal topologies and dependencies and planning AD FS proxy topologies. You will also cover the network requirements, multi-factor authentication and access filtering using claims rules.

Lesson Objectives

After completing this lesson, you should be able to:

- Describe the function and key features of AD FS.
- Explain how AD FS works with Office 365™.
- List AD FS planning considerations.
- Describe AD FS client's requirements and issues.
- Lists requirements for successful AD FS deployment.
- Perform AD FS capacity planning.
- Describe AD FS topologies, and server roles.
- Explain how to ensure high availability for AD FS.
- List best practices for AD FS.

AD FS Overview

AD FS provides the infrastructure that enables a user to authenticate in one network and use a secure service or application in another. In an Office 365 environment, AD FS enables users to authenticate through their on-premises Active Directory, and then use an account in Office 365 without any requirement for further authentication prompts. In this way, AD FS enables SSO, as long as the user is accessing Office 365 or other service using the same account that they used to log on to their workstation. This requirement for matching on-premises and remote service accounts is why an Office 365 SSO solution requires both AD FS and DirSync. When AD FS is implemented, all password management and password polices are performed within the on-premises Active Directory.

- What AD FS is
- How AD FS works
- Authentication
- Attribute stores
- End-user experience
- AD FS versions

How AD FS works

If a user initiates an authentication request through AD FS by using an AD FS "client" such as a supported browser, AD FS first verifies that the user credentials enable successful authentication to Active Directory. After successful Active Directory authentication, the Security Token Service (STS) component of AD FS server then issues a security token which is used to authenticate the user to the other service, such as Office 365. Office 365 implicitly trusts the token issuer, in this case Active Directory.


The security token contains claims about the user, such as user name, group membership, User Principal Name (UPN), email address, manager details, phone number, and other attribute values. It is up to the consuming application, such as Office 365, to decide how to use these claims, and to make appropriate authorization decisions; the application does not make authentication decisions, as these are made by the original service (on-premises Active Directory).

Trust between the parties is managed through certificates. HTTPS communications between the issuer (AD FS) and consuming server (such as Office 365) requires a public key infrastructure (PKI); the certificates used for security token signing and encryption can be self-signed by the AD FS server.

Authentication

The primary AD FS authentication methods are:


- For resources published to be accessed from outside the corporate network, Forms Authentication is selected by default. In addition, you can also enable Certificate Authentication – in other words, smart card-based authentication or user client certificate authentication that works with Active Directory Domain Services (AD DS).
- For intranet resources, Windows® Authentication is selected by default. In addition, you can also enable Forms and/or Certificate Authentication.

 **Note:** Windows authentication is not supported on all browsers. The AD FS authentication mechanism detects the user's browser user agent and uses a configurable setting to determine whether that user agent supports Windows Authentication. The Windows PowerShell® **Set-AdfsProperties -WIASupportedUserAgents** command can be used to specify alternate user agent strings for browsers that support Windows Authentication. If the client's user agent does not support Windows Authentication, the default fallback method is Forms Authentication.

You can also enable device authentication to provide a secondary authentication method, where multifactor authentication (MFA) is required. Device authentication requires that a registered device is used before a user can access a resource.

 **For more information about using devices for second-factor authentication and SSO, see Overview: Join to Workplace from Any Device for SSO and Seamless Second Factor Authentication Across Company Applications at the following link:**

<http://go.microsoft.com/fwlink/?LinkId=390919>

 **Note:** Office 365 has a separate MFA process for administrator accounts that has now been extended to user accounts. This authentication process requires users to acknowledge a phone call, text message or app notification after correctly entering their password. This MFA feature is not the same as AD FS MFA.

Attribute stores

AD FS attribute stores are the directories or databases used to store user accounts and associated attribute values. AD FS supports the following directories or databases as attribute stores:

- Active Directory in Windows Server 2003, Active Directory Domain Services (AD DS) in Windows Server 2008, AD DS in Windows Server 2012.
- All editions of Microsoft SQL Server® 2005 and SQL Server 2008.
- Custom attribute stores, to enable AD FS to operate with non-Microsoft platforms.

End-user experience

When a user accesses a resource through AD FS on the corporate intranet, the user will not be prompted for their credentials a second time, as long as:

- Internal DNS can resolve the AD FS service name to the backend AD FS servers or load-balanced IP for the AD FS service.
- Any Web-proxy configured on the client is configured to bypass proxy, for requests to the AD FS URL. The AD FS URL should, therefore, be added to the IE > Security > Intranet zones > sites.
- Internet Explorer® is configured for **Enable Integrated Windows Authentication**.
- There is a Service Principal Name (SPN) '<AD FS hostname>/<AD FS service account name>' registered for the AD FS service, under the AD FS farm service account, to allow Kerberos authentication.
- The default authentication configuration for the AD FS service in IIS is Integrated Windows Authentication (this is the default setting).

When a user accesses a resource through AD FS from the Internet or other external network, the request is intercepted by the AD FS Proxy in the perimeter network (unless an AD FS Proxy has not been configured), which then displays a webpage form prompting for user credentials. The default configuration on an AD FS proxy is Form-Based Authentication, as this requires just the SSL port 443 to be exposed. By contrast Windows Integrated Authentication has a range of ports and services that should not be exposed to the Internet. Unlike the intranet scenario, when accessing a resource over the Internet, unless the currently logged in credentials are domain credentials, the user will be prompted for a second set of credentials.



You can also customize the AD FS sign in pages as described in the following link:

<http://go.microsoft.com/fwlink/?LinkId=400789>

AD FS versions

There have been several versions of AD FS since the initial release, including:

- AD FS 1.0 was originally released as a Windows component with Windows Server 2003 R2.
- AD FS 1.1 was released with Windows Server 2008 and Windows Server 2008 R2, as an installable server role.
- AD FS 2.0 was released as an installable download for Windows Server 2008 SP2 or above.
- AD FS 2.1 was released with Windows Server 2012 as an installable server role.
- AD FS 3.0 is an installable server role on Windows Server 2012 R2. AD FS 3.0 does not require a separate IIS install and it includes a new AD FS proxy role called the Web Application Proxy.

AD FS 1.x was limited in its standards support, including WS-Federation Passive Requestor Profile (browser), and SAML 1.0 TOKENS. AD FS 2.0 extends standards support for WS-Federation and supports WS-Federation PRP, WS-Federation Active Requestor Profile, SAML 1.1/2.0 TOKENS, SAML 2.0 Operational Modes, and IdP Lite/SP Lite/eGov 1.5.



Note: The labs in this course use AD FS 2.1 on Windows Server 2012.

AD FS and Office 365

The Windows Azure™ Active Directory service used by Office 365 requires an STS infrastructure in order to provide SSO. Currently, Windows Azure AD supports the following STS:

- Active Directory Federation Services (AD FS).
- Shibboleth Identity Provider.
- Other third-party identity providers.

This course covers the use of AD FS as the STS.

How AD FS works with DirSync

AD FS enables SSO for Office 365, as long as the user has an account in both Active Directory and Office 365. The reason for the dual account requirement is that the user is always authenticating to an Office 365 account, even if SSO is not in place. When SSO is implemented, authentication occurs through a security token rather than through a user directly authenticating to Office 365. Therefore, user accounts are created on-premises in Active Directory, which DirSync then synchronizes to Office 365.

By synchronizing users and policy settings to Windows Azure Active Directory, DirSync maintains the object source of authority on the on-premises Active Directory, and ensures that the same objects, attributes, and settings are also available when the federation service accesses these objects from Office 365.



Note: It is important to keep this fundamental point in mind, that SSO with Office 365 is, in effect, a hybrid environment, where users have two separate accounts – a local on-premises Active Directory account and a Windows Azure Active Directory account. Users do not use their local Active Directory account to login to Office 365; rather, their Active Directory credentials provide access to their Office 365 account through the claims within the security token.

DirSync with Password Sync vs. AD FS

As discussed in Module 10, DirSync now supports password synchronization, so that a user's on-premises Active Directory account and Windows Azure Active Directory account have the same password at all times (password resets are synchronized in near real time, unlike other attribute changes which are subject to the default three-hour synchronization schedule). For this reason, organizations may decide not to implement AD FS, and instead opt for the lower overhead of a DirSync-only infrastructure in order to provide a "Same Sign-On" rather than "Single Sign-On" experience for users. The potential disadvantage of using DirSync with password synchronization is that there are two separate password policies (on-premises and cloud), and password updates require successful synchronization. The advantage of using DirSync with password synchronization is that any failure in the on-premises infrastructure will just mean that users cannot change their passwords; whereas in an AD FS-based Single Sign-On environment, any failure in the AD FS infrastructure will prevent users from accessing Office 365. More information on High Availability and AD FS is provided later in this lesson.

- Security token service (STS) infrastructure:
 - AD FS
 - Shibboleth Identity Provider
 - Third-party identity providers
- How AD FS works with DirSync
- DirSync with Password Sync versus AD FS

AD FS Planning Considerations

AD FS is a full featured, potentially complex set of technologies. In order to successfully deploy AD FS, the following planning issues must be considered:

- Preparation for the kind of end devices and browsers to be supported.
- Placement of AD FS servers and proxies.
- Selection of appropriate internal topologies, and network load balancing for federation farms and proxies.
- Remediation of Active Directory for non-supported characters, and invalid data.
- Preparation of DNS host names records.
- Purchase or issuing of certificates.
- Configuration of firewalls for AD FS-related ports.
- Selection of appropriate AD FS database technology.
- Capacity planning to determine required servers, and server specifications.
- Planning for AD FS High Availability.
- Preparation for multifactor authentication.
- Planning for access filtering using claims rules.

- Preparation for end devices and browsers
- Placement of AD FS servers and proxies
- Appropriate internal topologies for farms/proxies
- Check AD for non-supported characters, and invalid data
- Preparation of DNS host names records
- Purchase or issuing of certificates
- Configuration of firewalls for AD FS-related ports
- Selection of appropriate AD FS database technology
- Capacity planning to determine required servers, and server specifications
- Planning for AD FS High Availability
- Preparation for multifactor authentication
- Planning for access filtering using claims rules

These planning considerations are examined in detail throughout the remainder of this module.


AD FS Clients

In order to implement AD FS, users must access resources through appropriate client-side tools. For intranet users on corporate domain-joined computers, this typically means implementing the Microsoft Online Services Sign-In Assistant (MOS SIA). MOS SIA can be installed in a variety of ways, including:

- Installed automatically as part the Office 365 Desktop setup.
- Deployed using System Center Configuration Manager (SCCM) or other electronic software distribution (ESD) system.
- Installed manually.

- Microsoft Online Services Sign-In Assistant
 - Office 365 Desktop setup
 - System Center Configuration Manager
 - Manual install
- Browsers with JScript
 - Internet Explorer
 - Mozilla Firefox
 - Safari

MOS SIA enables authentication support for rich clients, such as Microsoft Outlook® and Lync®, by obtaining the service token from Office 365 and returning it to the application.

 **Note:** MOS SIA is used to facilitate SSO on client PCs, but it is also used for administrative tasks. For example, it is a requirement for the Windows Azure Active Directory Module for Windows PowerShell, and it is used by DirSync, Exchange, and AD FS.

For extranet and Internet users, and for web kiosk scenarios, access is typically through browser-based applications, such as Office Web Apps. Any current Web browser with JScript enabled can work as an AD FS client, although only Internet Explorer, Mozilla Firefox, and Safari on Apple Macintosh have been tested by Microsoft.

Cookies must be enabled, or at least trusted, for the federation servers and Web applications that are being accessed. Cookies prevent users from being continually prompted for logons within the same session. The authentication cookie is signed, but not encrypted, which requires SSL support in AD FS.

AD FS Topologies

AD FS can be deployed as a stand-alone server, or as a server farm. It is recommended that an AD FS server farm always be used, even if the farm consists initially of just one server, as this provides the option to add more AD FS servers later on for load balancing or fault tolerance. However, if AD FS is deployed as a stand-alone federation server, then no additional servers can be added at a later date.

- Stand-alone server versus server farm
- WID versus. SQL Server
- Number of servers
- Using AD FS Proxies
- Server placement

Database

AD FS servers require a database, and can be configured to use either the Windows Internal Database (WID) or full SQL Server. If WID is used, then AD FS servers in a farm are configured as primary or secondary. A primary federation server is initially the first federation server in the farm, and has a read/write copy of the AD FS configuration database. All other federation servers created in the farm (the secondary servers) regularly poll the primary server and synchronize any changes to a read-only copy of the AD FS configuration database stored locally. The poll interval is five minutes by default, but an immediate synchronization can be forced anytime by using Windows PowerShell.

Secondary servers provide fault tolerance for the primary server and, with appropriate server placement, can load-balance access requests across network sites. If the primary federation server is offline, all secondary federation servers continue to process requests as normal. However, no new changes can be made to the AD FS database until the primary federation server has been brought back online, or a secondary server is promoted to the primary role. Primary and secondary role assignment is managed by using the **Set-AdfsSyncProperties** Windows PowerShell cmdlet.

If SQL Server is used to store AD FS information, all servers in the farm are considered "primary", as they all have read/write access to the database.

Number of servers

The number of AD FS servers that should be deployed in an organization depends on the number of users likely to issue authentication requests. The recommended minimum requirements are displayed in the following table:

Number of users	Minimum number of servers
Fewer than 1,000	0 dedicated federation servers (install AD FS role on Domain Controllers) 0 dedicated federation server proxies (install AD FS role on Web servers) 1 dedicated NLB server to load balance the federation server proxies
1,000 to 15,000	2 dedicated federation servers 2 dedicated federation server proxies
15,000 to 60,000	Between 3 and 5 dedicated federation servers At least 2 dedicated federation server proxies

Using AD FS Proxies

AD FS Proxy servers are not mandatory, but are highly recommended. The proxy is used to provide Extranet/Internet users with access to SSO applications and services. AD FS proxies cannot produce security tokens themselves; instead, they are used to route or redirect tokens to clients and, if necessary, back to the AD FS server.

Server placement

The most critical component of an AD FS deployment is the federation server or server farm. Therefore, it is important that server placement strategy is properly considered. AD FS servers must be domain-joined and should be placed behind a firewall on the corporate network to prevent exposure to the Internet. AD FS proxies should not be domain-joined and should be installed in the perimeter network.

AD FS Requirements

Prior to deploying AD FS, a range of requirements must be in place.

Active Directory

Several user attributes must be checked before implementing AD FS. For example, the UPN must be set for every user, and must be known by each user if used as his or her login name. UPNs used for SSO can only contain letters, numbers, periods, dashes, and underscores. If there are invalid characters in UPNs, these must be remediated before AD FS is enabled.

- Active Directory
- DNS and namespaces
- Certificates
- Network
- Database

The UPN domain suffix must be either the domain to be configured for SSO, or a subdomain. If the Active Directory domain name is not a public Internet domain (for example, it ends with a ".local" suffix), the UPN must be changed to include either a publically registered domain, or a subdomain of an Internet domain name. If the domain suffix needs to be changed and DirSync has already been enabled, Office 365 user UPNs may not match the on-premises UPN defined in Active Directory.

To fix these UPNs, Office 365 UPNs can be reset using the **Set-MsolUserPrincipalName** cmdlet in the Windows Azure Active Directory Module for Windows PowerShell.

For example:

```
Set-MsolUserPrincipalName -UserPrincipalName user@domain1.com -NewUserPrincipalName user@domain2.com
```

DNS and namespaces

In DNS, the AD FS service requires a common name. Typically, this name is something like **sts**, **fs**, or **adfs**; for example, sts.contoso.com. This name should be different from the host names for the AD FS servers in the farm. The service name must exist as a common name in the certificates used by the AD FS Proxy and AD FS servers, and must also be registered as an SPN to the AD FS service account to enable Kerberos authentication to succeed.

For AD FS clients on the local intranet to be able to use Windows Integrated Authentication through local federation servers, the corporate DNS must include a host (A) resource record that resolves the fully qualified domain name (FQDN) host name of the federation service to the IP address of either a single AD FS server or AD FS server cluster – such as through Microsoft Network Load Balancing (NLB) providing a single cluster FQDN name and a single cluster IP address for the server farm. DNS resolution of the AD FS service endpoint must be through an A record, and not through a CNAME (alias) record lookup.

For external AD FS clients using forms-based authentication, the publicly accessible DNS must include a host record that resolves the FQDN host name of the federation service proxy to the IP address of either a single AD FS Proxy server or to a proxy array. As the AD FS Proxy is placed in a perimeter network, this service will typically require a Hosts file entry for the AD FS service. This enables the proxy to resolve the name of the AD FS service on the corporate network, unless a split-brain DNS environment is used, where the same DNS provides name resolution for both internal and external zones.


Certificates

HTTPS (SSL) communications require a public certificate through a PKI; the certificates used for security token signing and encryption can be self-signed by the AD FS server. Certificates must use RC4 ciphers and not AES ciphers; this is because Windows XP does not support AES ciphering, and any Windows XP clients will get HTTP 404 errors.

All AD FS servers must use the same HTTPS certificate as the AD FS configuration that gets replicated through WID; or SQL Server database sharing includes the SSL certificate thumbprint. AD FS Proxies do not need to use the same public certificate as used by the internal AD FS servers, as configuration information is not shared between the AD FS proxies, and a different SSL certificate can be used on each AD FS proxy server, as long as the common name (CN) on each certificate matches the service name of the internal AD FS servers. If required, however, all AD FS and AD FS Proxy server can use the same certificates.

Network

AD FS servers must be able to communicate with AD FS Proxies. This means that the corporate firewall server must be configured to allow Secure Hypertext Transfer Protocol (HTTPS) traffic from the federation server proxy to the federation server (port 443). Within the intranet, the AD FS servers must be able to communicate over all the standard Active Directory ports.

 **Note:** DirSync also needs all ports open to Active Directory, port 443 to Office 365 for synchronization traffic, as well as port 80 in order to verify the Office 365 Certificate Revocation List (CRL).

Database

AD FS requires a configuration database to store configuration data. This database can either be a Microsoft SQL Server 2005 or newer database, or the Windows Internal Database (WID) included with Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012.

WID is easy to set up and implement and supports up to five federation servers in a farm, providing load balancing and fault tolerance. WID does not support SAML artifact resolution and SAML/WS-Federation token replay detection, and WID is not supported if there are more than 100 claim trust providers or more than 100 relying party trusts. WID also requires primary (read-write) and secondary (read-only) database roles to be manually configured.

SQL Server is not subject to the limitations of WID, supporting more than five federation servers in a farm; however, it does require more setup and management. SQL Server is also a requirement if there are more than 50,000 accounts in Active Directory. If SQL Server is used, AD FS must be installed using PowerShell. It is possible to migrate an AD FS configuration database from WID to an instance of SQL Server.

 **For information on how to migrate AD FS from WID to SQL Server, see AD FS: Migrate Your AD FS Configuration Database to SQL Server on the TechNet Wiki site at the following link:**

<http://go.microsoft.com/fwlink/?LinkId=390920>

AD FS Capacity Planning

Capacity planning for federation servers helps organizations estimate and prepare for growth in the size of the AD FS configuration database. Capacity planning also helps assess the hardware requirements for each federation server and the number of federation servers to use.

The AD FS Capacity Planning Sizing Spreadsheet includes calculator-like functionality that takes expected usage data about users in the organization, and returns a recommended optimal number of federation servers for an AD FS production environment.

AD FS Capacity Planning Sizing Spreadsheet:

- Number of users sending authentication requests (peak)
- Duration of peak usage period
- Number of users requiring SSO access

The AD FS Capacity Planning Sizing Spreadsheet requires the following inputs:

- A value (40, 60, or 80 percent) that best represents the percentage of total users expected to send authentication requests to AD FS during peak usage periods.
- A value (one minute, 15 minutes, or one hour) that best represents the length of time the peak usage period is expected to last.
- The total number of users that will require single sign-on access to the target claims-aware application, based on whether the users are:
 - Logging into Active Directory from a computer on the corporate network
 - Logging into Active Directory remotely from a computer
 - From another organization or from a SAML 2.0 identity provider


 **The AD FS Capacity Planning Sizing Spreadsheet can be downloaded from the Microsoft Download Center at the following link:**

<http://go.microsoft.com/fwlink/?LinkId=390921>

High Availability for AD FS

If AD FS is deployed in an Office 365 environment but the AD FS service is inaccessible, no users (internal or external) will be able to access Office 365 resources. If the AD FS Proxy server is down or unavailable, external user authentication requests will not be passed to the back-end AD FS servers, and these users will not be able to connect to Office 365. Therefore, it is essential that preparation for AD FS deployment include planning for high availability of both back-end AD FS servers and AD FS Proxy servers.

- Why HA is essential
- Network Load Balancing
- Protecting SQL Server
- Office 365 Adapter for Windows Azure Virtual Machines


 **Note:** AD FS unavailability only affects user authentication and does not affect Office 365 services. Therefore, while email will still be delivered to users' mailboxes, users will not be able to access it.

Network Load Balancing

Network Load Balancing (NLB), or other forms of clustering, should be used to allocate a single IP address for multiple federation server computers. In this way, failure of any single AD FS server will not affect the whole AD FS service. NLB should also be used to provide an AD FS Proxy array in the perimeter network, to ensure that external clients are not affected by failure of any AD FS Proxy computer.

Protecting SQL Server

If WID is used as the AD FS data storage, there will be a copy of the database on each server; however, if SQL Server is used and the AD FS service cannot connect to its database, the AD FS service will not start. For this reason, it is recommended that AD FS use a SQL Server cluster, or a SQL Server failover partner is configured. A SQL failover partner can be configured either during AD FS configuration or afterwards.

 **For information on how to configure the SQL failover partner, see AD FS 2.0 High Availability and High Resiliency Walkthrough at the following link:**


<http://go.microsoft.com/fwlink/?LinkId=390922>

Office 365 Adapter for Windows Azure Virtual Machines

Deploying AD FS imposes significant resource and management overhead on an organization. This is particularly true for small to medium-sized enterprises, where the move to Office 365 has been driven by a desire to move mission-critical IT to the cloud. As a result, the requirement to then have to maintain an on-premises AD FS infrastructure in order to provide access to cloud resources can seem retrograde. For this reason, the option to also migrate the federation service to the cloud should also be considered.

The Office 365 Adapter for Windows Azure Virtual Machines provides the option to deploy some or all of the following functionality in Microsoft Azure:

- Active Directory Domain Services (AD DS)
- Active Directory Federation Services (AD FS)
- Directory synchronization services

 **Note:** The Office 365 Adapter for Windows Azure Virtual Machines does not currently support Exchange in hybrid mode.



For more information on the Office 365 Adapter for Windows Azure Virtual Machines, download the Office 365 Adapter: Deploying Office 365 Single Sign-On using Windows Azure Virtual Machines document, available from the following link:

<http://go.microsoft.com/fwlink/?LinkId=400783>

Best Practices for AD FS

You should consider the following best practices when planning for AD FS deployment:

- Always plan for using an AD FS proxy server; publishing 443 from the Internet directly to the AD FS server is not a good idea, otherwise any external computer could have direct access to your federation servers.
- Avoid having federation servers directly accessible on the Internet; direct Internet access should only be used when setting up a test lab environment, or when the organization does not have a perimeter network. You should isolate your federation servers, so that they can only be accessed by client computers that are authenticated against the corporate network through an AD FS Proxy.
- Prepare DNS to mitigate against incorrect DNS updates, especially with split brain DNS. If DNS is not functioning correctly, client computers may not be able to access AD FS.
- Pay close attention to networking, firewall, and security design, to ensure that client computers can authenticate to the corporate Active Directory.
- Ensure that all certificates are exported to include the private key; this is because both public and private keys are required for certificates to function on the Default Web Site.

- Plan for AD FS proxy servers
- Avoid having federation servers directly accessible on the Internet
- Prepare DNS
- Networking, firewall, and security design
- Ensure certificates export includes private key

Discussion: Design SSO for Lucerne Publishing

With the DirSync deployment working well and password synchronization requiring users only to maintain one set of credentials to access Office 365, users have been relatively happy with the deployment of Office 365 and the number of calls to the helpdesk has decreased considerably.

However, one area that is becoming increasingly problematic is the ability of users to find content across both the on-premises SharePoint implementation and SharePoint Online. Because it has become a pressing business need for Lucerne Publishing users to find documents company-

wide, Justin Muller and Alain Richer have decided to install a hybrid SharePoint environment. During their analysis of the situation, they learn that Hybrid SharePoint with Enterprise Search requires Single Sign-On (SSO), and that AD FS is the most obvious choice for this SSO deployment.

- How many AD FS servers and AD FS proxies are required?
- Where should the AD FS servers be located?
- What type of certificate provider should be used?
- What authentication level should be implemented?
- What level of service access is required?
- What load balancing should be used for AD FS and AD FS proxy?

In this discussion task, you will work as a class to identify planning factors and solutions for deploying SSO at Lucerne Publishing.

Lesson 2

Install and Manage AD FS Servers

In this lesson, you will learn about the process of installing and managing AD FS servers, including creating the AD FS service account, configuring farm or stand-alone servers, incorporating additional servers, converting from a standard to a federated domain, and managing the certificate life cycle.

Lesson Objectives

After completing this lesson, you should be able to:

- Prepare for AD FS server installation.
- Install the AD FS Server Role.
- Use the AD FS Federation Server Configuration Wizard, to configure an AD FS server farm.
- Convert an Office 365 domain from standard to federated.
- Manage AD FS servers.
- Convert an Office 365 domain from federated to standard.
- List best practices for installing and managing AD FS servers.

Preparing for AD FS Installation

In Windows Server 2012, AD FS 2.1 is installed from the Server Manager as a role. The Server Manager Configuration wizard performs validation checks and automatically installs all the services required by AD FS. The AD FS server role includes Windows PowerShell cmdlets that can be used to perform PowerShell-based deployment of AD FS servers and proxies. Before installing AD FS, the following items must be in place:

Service account

An AD FS service account should be created in Active Directory. This account should be set for the password to never expire. The service account requires the following access rights on the AD FS server computer:

- Log on as service
- Log on as batch



Note: When GPOs are used to limit access rights, such policies can potentially remove the "Log on as batch" or "Log on as service" access rights to the AD FS service account. If these rights are removed, in Event Viewer you will see "503 Service unavailable" errors from the AD FS App Pool in IIS.

The SPN of the service account should also be set by using the following Windows PowerShell command:

```
setspn -a host/<FQDN of the federation service> <service account name>
```


To verify the SPN setting, use the following Windows PowerShell command::

```
setspn -l <service account name>
```

Certificates

The certificates to be used in the deployment should have been obtained and installed into the Personal certificate store on the AD FS computer. If multiple servers are being deployed, the certificates should either be multi-name or use wildcards. The common name (CN) on each certificate must match the AD FS service name.

Load balancing

NLB for the AD FS server farm computers should be installed and configured.



The following external link has a walkthrough on configuring NLB for AD FS 2.0.

<http://go.microsoft.com/fwlink/?LinkId=400782>

DNS

DNS host records (not CNAME) for internal and external AD FS should also be configured prior to installing AD FS servers.

Installing AD FS Server Role

To install the AD FS Server Role, use the **Server Manager Add Roles and Features Wizard**, and select the **Active Directory Federation Services** server role. The Add Roles and Features Wizard will automatically select the .NET Framework, Internet Information Services (IIS), and Windows Process Activation Service features. On the Select role services page, select the **Federation Service** check box, to install an AD FS Server.

IIS will be running after the role has been successfully installed. The next task is to assign the public certificate to the default website on the AD FS server, in order to secure the traffic between AD FS and client computers. In **Internet Information Services (IIS) Manager**, edit site bindings, and in the **SSL certificate list**, select the previously imported certificate to use.

- Add Roles and Features Wizard:
 - Active Directory Federation Services server role
 - Federation Service role service
- Assign public certificate to default website in IIS

Using the AD FS Federation Server Configuration Wizard

When the AD FS role has been installed, the **AD FS Federation Server Configuration Wizard** can be run to configure the AD FS server. The steps required vary depending on whether a standalone server or AD FS Server Farm is being deployed. The AD FS Federation Server Configuration Wizard is run from the Server Manager, Tools menu, or by running **C:\Program Files\Active Directory Federation Services 2.0\FsConfigWizard.exe**.

- AD FS Federation Server Configuration Wizard
 - Stand-alone server
 - First server in AD FS Server Farm
 - Second, and subsequent, servers in AD FS Server Farm
- Event Viewer to verify federation server is operational
 - Event ID 100

Standalone server

In the **AD FS Federation Server Configuration Wizard**, select the **Create a new Federation Service** checkbox, and on the **Select Stand-Alone or Farm Deployment** page, select **Stand-alone federation server**. The **Specify the Federation Service Name** page should display the public certificate that was previously imported and bound to the default website; if the correct certificate is not displayed, select the appropriate certificate from the SSL certificate list. The wizard will automatically create a new WID database, unless an existing AD FS database is detected.

When configuring a stand-alone server, the service account is automatically assigned to be the NETWORK SERVICE account. After the configuration wizard has completed, this service account should be changed to the previously created AD FS service account, unless the AD FS server is being used in a test environment; this will help mitigate against possible attack vectors that would otherwise make the federation server vulnerable to malicious attacks.

First server in AD FS Server Farm

For the first server in an AD FS Server Farm, in the **AD FS Federation Server Configuration Wizard**, select the **Create a new Federation Service** check box, and on the **Select Stand-Alone or Farm Deployment** page, select **New federation server farm**. The **Specify the Federation Service Name** page should display the public certificate that was previously imported and bound to the default website; if the correct certificate is not displayed, select the appropriate certificate from the SSL certificate list. The wizard will automatically create a new WID database, unless an existing AD FS database is detected. On the **Specify a Service Account** page, select the previously created AD FS service account and enter its password.

Second, and subsequent, servers in AD FS Server Farm


For additional servers in an AD FS Server Farm, in the **AD FS Federation Server Configuration Wizard**, select the **Add a federation server to an existing Federation Service**; the wizard will automatically create a new WID database, unless an existing AD FS database is detected. On the **Specify the Primary Federation Server and Service Account** page, enter the name of the Primary federation server name, and on the **Specify a Service Account** page, select the previously created AD FS service account, and enter its password. The **Specify the Federation Service Name** page should display the public certificate that was previously imported and bound to the default website; if the correct certificate is not displayed, select the appropriate certificate from the SSL certificate list.

To verify that the federation server is operational, use **Event Viewer**, and check for events with ID 100 in **Applications and Services Logs\AD FS\Admin**. This event verifies that the federation server was able to successfully communicate with the Federation Service.

Converting Domain from Standard to Federated

Converting a domain sets up a federation trust between the identity provider, on-premises Active Directory, and Windows Azure Active Directory used by Office 365. This relying-party trust relationship provides a secure channel for security tokens to be sent between Active Directory and Office 365, using certificates for token signing between the two parties. As the relying-party, Office 365 only sees the specific information that AD FS sends as claims, such as username, UPN, and email address, and Office 365 cannot use the federation trust to query on-premises Active Directory for additional accounts information.


- Conversion overview
- Preparing for conversion
- Adding federated sub-domains
- Converting single domain
- Converting multiple domains

 **Note:** Unlike Windows trusts, which require a constantly connected secure channel between two or more domains to function, federation trusts are only used for the exchange of secure tokens over HTTPS/SSL, and this exchange is always initiated by the client.

After the conversion, every licensed user will become a federated user, using their existing Active Directory corporate credentials (user name and password) to access your cloud services.

Preparing for conversion

To avoid potential conversion problems before initiating the conversion, first verify that the domain to be federated is marked as active in the Office 365 admin center. Group policy should also be updated or configured in the on-premises Active Directory, as policies such as password complexity and password expiry will be set from the local Active Directory, and not Office 365, after the conversion has taken place.

 **Note:** If AD FS Proxies are to be deployed (as recommended), it may be best to delay the conversion until after the proxies are in place; otherwise, external users will not be able to access Office 365.

Adding federated sub-domains

If you are using a subdomain (for example, corp.contoso.com) in addition to a top-level domain (for example, contoso.com), you must add the top-level domain in your cloud service before you add any subdomains. When the top-level domain is set up for single sign-on, all subdomains are automatically set up as well.

Converting single domain

To convert a single domain, use the Windows Azure Active Directory Module for Windows PowerShell. After entering Office 365 administrator account credentials using **Get-Credential**, and connecting to Office 365 using **Connect-MsolService**, run the following command to specify a connection to a particular AD FS server:

```
Set-MsolAdfsContext -Computer <AD FS primary server>
```

where <AD FS primary server> is the internal FQDN name of the primary AD FS server.



Note: If the Windows Azure Active Directory Module is being run on the primary AD FS server, the **Set-MsolAdfscontext** cmdlet is optional.

At the Windows Azure Active Directory Module for Windows PowerShell prompt, run the following command to change the domain from standard authentication to federated:

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

where <domain> is the domain to be converted.

To verify that the conversion has been successful, compare the settings on the AD FS server and in Office 365 by running **Get-MsolFederationProperty -DomainName <domain>**; if the **FederationServiceIdentifier** settings listed under "AD FS Server" and "Microsoft Office 365" do not match, run **Update-MsolFederatedDomain -DomainName <domain>** to synchronize the settings.

The trust can also be verified by opening the **AD FS Management** console, and under **Trust Relationships\Relying Party Trusts, Microsoft Office 365 Identity Platform** should show as **Enabled**.



Note: Domains do not need to be added as standard and then converted; using the **New-MsolFederatedDomain** cmdlet, domains can be added as federated, as long as the domain name has already been verified (see Module 5).

Converting multiple domains

Office 365 supports multiple top level domains for users' UPN suffixes within the same organization. To convert multiple top-level domains, use the **-SupportMultipleDomain** switch with the **Convert-MsolDomainToFederated** cmdlet; for example, to convert both contoso.com and fabrikam.com domains, use:

```
New-MsolFederatedDomain -DomainName contoso.com -SupportMultipleDomain
New-MsolFederatedDomain -DomainName fabrikam.com -SupportMultipleDomain
```

After converting multiple domains, the **FederationServiceIdentifier** settings listed under "AD FS Server" and "Microsoft Office 365" will not match; each Office 365 federated domain will have the **FederationServiceIdentifier** as `http://<domainname>/adfs/services/trust/`, and the AD FS configuration will have the **FederationServiceIdentifier** as `http://<STSname>/adfs/Services/trust`. In a multiple domain scenario, an additional claim rule is automatically created to add the suffix value of the user's UPN to a new claim called **Issuerid**, used in the security token.



For more information on converting name spaces to support multiple domains, and the effect of this conversion on trusts and claims, see SupportMultipleDomain switch when managing SSO to Office 365 in the following link:

<http://go.microsoft.com/fwlink/?LinkId=390924>

Managing AD FS Servers

After AD FS has been deployed, there are several management tasks that may need to be performed.

Managing the certificate life cycle

In order to prevent issues from certificate expiry, the self-signed, self-generated certificates generated by AD FS support automatic roll-over through **AutoCertificateRollover** (ACR), which renews AD FS certificates once a year. ACR generates two new token signing certificates every year; if Office 365 is not updated with the new token-signing certificate, no user will be able to sign into and use Office 365 as these certificates sign all assertions from the federation server. If an internal PKI is used to issue the token signing certificate, AD FS does not provide ACR, and renewal and updating Office 365 must be a manual task.


- Managing the certificate life cycle
 - AutoCertificateRollover
 - Expiry dates
 - AD FS Management console
 - Get-ADFSCertificate cmdlet
 - Microsoft Office 365 Federation Metadata Update Automation Installation Tool
- Changing the primary AD FS server

Certificate expiry dates for the service communications, token-decrypting, and token-signing certificates can be viewed by using the AD FS Management console. In the console tree, expand **Service**, and then click **Certificates**. Windows Azure Active Directory Module for Windows PowerShell can also be used to view certificate details, by using the **Get-ADFSCertificate** cmdlet.

To manage certificate rollover if ACR is used, the downloadable Federation Metadata Update Tool automatically updates the Office 365 service using the **update-msolfederateddomain** cmdlet when the AD FS token signing certificate renews on an annual basis. This tool should be run as a daily scheduled task on the AD FS server; otherwise, token signing certificate renewal on the AD FS server will have to be manually monitored. The update tool script scheduled task should only be run on one AD FS server.

 **To download the Federation Metadata Update Tool, go to the Microsoft Office 365 Federation Metadata Update Automation Installation Tool page on the following link:**

<http://go.microsoft.com/fwlink/?LinkId=390925>

 **Note:** AD FS is likely not to require the use of the Federation Metadata Update Tool. However, no authoritative information was available at the time of publication.

Changing the primary AD FS server

If WID is used as the AD FS data store, the primary and secondary database roles can be changed using Windows PowerShell. The **Get-AdfsSyncProperties** cmdlet displays the current database role setting for the AD FS server. To change roles, first determine which secondary computer will be switched to primary, then at the Windows Azure Active Directory Module for Windows PowerShell prompt from that computer, type the following command and press Enter:

```
Set-AdfsSyncProperties -Role PrimaryComputer
```

Then at the Windows Azure Active Directory Module for Windows PowerShell prompt on the current primary computer, type the following command and press Enter:

```
Set-AdfsSyncProperties -Role SecondaryComputer -PrimaryComputerName <new primary computer name>
```

After this command has run, the primary role will be switched to the old secondary computer.



Note: Switching AD FS server roles does not apply if SQL Server is used as the AD FS data store, as all AD FS servers have read/write access to the database.

Converting Domain from Federated to Standard

In some situations it may be necessary to convert a domain from federated back to a standard managed domain. For example, it may be decided that AD FS is no longer appropriate if server overhead for AD FS HA cannot be justified, or if AD FS has been down for some time and will not be restored for a while. Conversion back to a managed state will enable users to log into Office 365 services.

To change the domain from federated to standard authentication, convert all users to non-federated ones and create a new password for each user and save it in a specified file. To make this change, run the following command at the Windows Azure Active Directory Module for Windows PowerShell prompt:

To make this change, run the following command at the Windows Azure Active Directory Module for Windows PowerShell prompt:

- Requires password reset for Office 365 accounts
- ForceChangePassword flag
- Password synchronization

```
Convert-MSolDomainToStandard -DomainName <domain> -SkipUserConversion $false -PasswordFile <filename and path>
```

where <domain> is the domain to be converted, and filename and path refers to a location to store new passwords for Office 365 users after the changeover.

The command sets the flag "**ForceChangePassword**" on the users to **\$true**, so the users will have to change their own password after the first time they log on with the new one you provided from the file.

If something goes wrong with the conversion of the users when running the conversion command above, such as if a network outage occurs during the operation, you may have to convert the users manually to non-federated ones with the **Convert-MSolFederatedUser -UserPrincipalName** cmdlet.



Note: Users must be fully converted to managed authentication in order for their passwords to synchronize successfully. Therefore, the domain and all users must have been completely converted before initiating a password synchronization using DirSync; otherwise, user passwords will not successfully synchronize to Office 365.



For more information on converting a domain from federated, and a sample script to manually convert all users in a domain, see AAD Sync: How To Switch From Single Sign-On To Password Sync at the following link:

<http://go.microsoft.com/fwlink/?LinkId=390926>

Best Practices for AD FS Servers

Obstacles to a successful AD FS server deployment include Web proxies or other Internet content filtering devices, intercepting AD FS traffic, incorrectly configured firewalls, incorrect DNS records and/or certificate configuration.

Best practices

You should consider the following best practices when installing and managing AD FS servers:

- Use the AD FS capacity planning tool, to help ensure that your AD FS environment can meet your requirements for concurrent logons.
- Design a high availability AD FS infrastructure, and avoid stand-alone AD FS, to ensure that users are always able to authenticate to Active Directory.
- Verify that required ports are open on the firewall, to ensure that AD FS is available to all client computers.
- Do not mix between AD FS and other roles on the same server, to help ensure the availability and security of AD FS.
- Develop test cases for all browsers, and for internal and external clients, to ensure that all users can use Single Sign-On from all supported devices.
- Ensure that all hotfixes and the .NET Framework version are up to date.
- Ensure that certificates are correctly configured, and are exported to include private key.
- Ensure that the parent domain is always federated before any sub-domains.

- Use AD FS capacity planning tool
- Design HA A DFS infrastructure
- Verify required ports on firewall
- Do not mix AD FS and other roles
- Develop test cases for browsers and clients
- Install all hotfixes, and latest .NET Framework version
- Ensure that certificates are correct and exported with private key
- Ensure that parent domain is always federated before sub-domains

Lesson 3

Install and Manage AD FS Proxy Servers

In this lesson, you will learn about installing and managing AD FS proxy servers, including setting up perimeter network name resolution, installing the required Windows roles and features, setting up certificates, configuring AD FS proxy settings, and specifying a custom proxy forms login page.

Lesson Objectives

After completing this lesson, you should be able to:

- Prepare for AD FS Proxy installation.
- Install the AD FS Proxy Role.
- Use the AD FS Federation Services Proxy Configuration Wizard, to configure an AD FS Proxy.
- Configure AD FS Proxy settings.
- List best practices for installing and managing AD FS proxies.

Preparing for AD FS Proxy Installation

In Windows Server 2012, AD FS Proxies are installed from the Server Manager as a role, using the same Server Manager Configuration wizard pages that were used to install AD FS servers. The configuration wizard performs validation checks and automatically installs all the services required by the AD FS Proxy. In a production environment, the AD FS proxy server should be placed in the perimeter network (also known as screened subnet), not in the internal corporate LAN.

- Certificates
- Load balancing
- DNS

Certificates

The certificates to be used in the deployment should have been obtained and installed into the Personal certificate store on the AD FS Proxy computer. The common name (CN) on each certificate must match the AD FS service name. When exporting certificates ready for use on the AD FS Proxy, it is important to ensure that the private key is included in the export. Once imported to a local computer personal store, the certificate is ready for binding in IIS, as soon as IIS and the AD FS Proxy role is installed.

Load balancing

NLB for the AD FS Proxy array should be installed and configured.

DNS

DNS host records (not CNAME), for internal and external AD FS, should also be configured prior to installing AD FS servers. As the AD FS Proxy is typically placed outside the corporate LAN, it is recommended that you:

- Configure the proxy to use external DNS servers for external name resolution.
- Add internal hostnames that the proxy needs to resolve, such as the internal AD FS farm, to the Hosts file on the proxy.

Installing the AD FS Proxy Role

To install the AD FS Proxy Role, use the Server Manager **Add Roles and Features Wizard**, and select the **Active Directory Federation Services** server role. The **Add Roles and Features Wizard** will automatically select the .NET Framework, Internet Information Services (IIS), and Windows Process Activation Service features. On the **Select role services** page, clear the Federation Service check box and select **Federation Service Proxy**.

IIS will be running once the role has been successfully installed. The next task is to assign the public certificate to the default website on the AD FS server, in order to secure the traffic between the AD FS Proxy and client computers, and between the AD FS Proxy and AD FS itself. In IIS Manager, edit site bindings, and in the SSL certificate list, select the previously imported certificate to use.

- Add Roles and Features Wizard:
 - Active Directory Federation Services server role
 - Federation Service Proxy role service
- Assign public certificate to default website in IIS

Using the AD FS Federation Services Proxy Configuration Wizard

When the AD FS Proxy role has been installed, the **AD FS Federation Services Proxy Configuration Wizard** can be run to configure the AD FS Proxy server. The AD FS Federation Services Proxy Configuration Wizard is run from the Tools menu on the Server Manager, or by running **C:\Windows\ADFS\FspConfigWizard.exe**.

In the **AD FS Federation Services Proxy Configuration Wizard**, on the **Specify Federation Service Name** page, verify that the correct federation service name is displayed, click **Test Connection** to verify a connection to the Federation Service, and enter credentials for the AD FS service account; these credentials are necessary to establish a trust between this federation server proxy and the Federation Service. By default, only the service account used by the Federation Service or a member of the local BUILTIN\Administrators group can authorize a federation server proxy.

To verify that the proxy is operational, use Event Viewer and check for events with ID 198. If the federation server proxy is configured properly, there will be a new event in the Application log of Event Viewer with the event ID 198. This event verifies that the federation server proxy service was started successfully and is now online.

- AD FS Federation Services Proxy Configuration Wizard
- Event Viewer to verify federation server is operational
 - Event ID 198

Configuring AD FS Proxy Settings

After an AD FS Proxy has been deployed, there are several configuration tasks that may need to be performed.

Specifying a custom proxy forms login page

The default login page displays the federation service name, boxes for user name and password, and text to describe user name format. This page can be customized; for example, you can include a logo, change example and instruction text, change the page title, remove or change the federation service name display, and add an "Authorized Use" disclaimer or other text at the bottom of the page.

- Custom proxy forms login page
 - Logo
 - Instruction text
 - Page title
 - Service name
- Access control
 - Block all extranet access to Office 365
 - Except for specific devices, group members, browser users

 **For more information on customizing the proxy forms login page, see Customizing the AD FS forms based login page at the following link:**

<http://go.microsoft.com/fwlink/?LinkId=390927>

Configuring access control


AD FS client access policies can be used to limit access to Office 365 services. For example, you can:

- Block all extranet client access to Office 365.
- Block all extranet client access to Office 365, except for devices accessing Exchange Online for Exchange Active Sync.
- Block all extranet client access to Office 365, except for members of specific Active Directory groups.
- Block all extranet client access to Office 365, except for browser-based applications.

To use these access policies, a claim rule must exist in AD FS for each of the following claim types:

- x-ms-forwarded-client-ip
- x-ms-client-application
- x-ms-client-user-agent
- x-ms-proxy
- x-ms-endpoint-absolute-path

If these claim rules are not present, they must be added using the AD FS Management console. Custom claim rules can then be created to block access using the criteria, such as Active Directory group membership or client IP address.

 **For detailed information on configuring access rules, see Limiting Access to Office 365 Services Based on the Location of the Client at the following link:**

<http://go.microsoft.com/fwlink/?LinkId=390928>

Best Practices for AD FS Proxies

You should consider the following best practices when installing and managing AD FS proxies:

- AD FS Proxy should not be domain joined, as this would negate one of the key benefits of the AD FS Proxy in providing a security separation between internal Active Directory and external clients.
- AD FS Proxy should be placed in the perimeter network, not internal LAN, again to help ensure the integrity of the security separation between internal Active Directory and external clients.
- Use the AD FS capacity planning tool, to ensure that your AD FS Proxies are able to support the number of external clients that require authentication against the corporate Active Directory.
- Design a high availability AD FS infrastructure that includes highly available proxies, to ensure that external clients are always able to authenticate against the corporate Active Directory.
- Verify that required ports are open on the firewall.
- Do not mix AD FS Proxy and other roles on the same server, to help ensure the availability and security of AD FS.
- Develop test cases for all browsers, and for internal and external clients, to ensure that all users can use Single Sign-On from all supported devices.
- Ensure that all hotfixes and the .NET Framework version are up to date.
- Ensure that certificates are correctly configured, and are exported to include private key.

- AD FS Proxy should not be domain joined
- Place AD FS Proxy in DMZ, not internal LAN
- Use the AD FS capacity planning tool
- Design a HA AD FS infrastructure, including HA proxies
- Verify required ports on firewall
- Do not mix AD FS Proxy and other roles
- Develop test cases for browsers and clients
- Install all hotfixes, and latest .NET Framework version
- Ensure that certificates are correct and exported with private key

Lab: Implementing Active Directory Federation Services

Scenario

With the DirSync deployment working well and password synchronization requiring users only to maintain one set of credentials to access Office 365, users have been relatively happy with the deployment of Office 365 and the number of calls to the helpdesk has decreased considerably. However, one area that is becoming increasingly problematic is the ability of users to find content across both the on-premises SharePoint implementation and SharePoint Online. Because it has become a pressing business need for Lucerne Publishing users to find documents company-wide, Justin Muller and Alain Richer have decided to install a hybrid SharePoint environment. During their analysis of the situation, they learn that Hybrid SharePoint with Enterprise Search requires Single Sign-On (SSO), and that AD FS is the most obvious choice for this SSO deployment.

Objectives

To provide students with practical experience in the planning, installation and management of Active Directory Federation Services for single sign-on.

Lab Setup

Estimated Time: 105 minutes

Virtual machine: 20346C-LUC-CL1

Username: **Student1**

Password: **Pa\$\$w0rd**

In all tasks, where you see references to `lucernepublishingXXXX.onmicrosoft.com`, replace the `XXXX` with the unique Lucerne Publishing number that you were assigned when you set up your Office 365 account in Module 1, Lab 1B, Exercise 2, Task 3, Step 5.

Where you see references to `labXXXXX.o365ready.com`, replace the `XXXXX` with the unique `O365ready.com` number you were assigned when you registered your IP address at `www.o365ready.com` in Module 2, Lab 2B, Exercise 1, Task 2, Step 6.

Where you see references to your public IP address, replace the your public IP address with the IP address you noted in Module 2, Lab 2B, Exercise 1, Task 2, Step 2.

Exercise 1: Install AD FS Servers and Proxy Servers

Scenario

With the complexity of this deployment, Remi decides that he wants to be involved at a hands-on level. Heidi works with Elizabeth Labrecque to verify whether single-sign on is functioning properly, and then Remi makes the final configuration changes to switch the Office 365 domain across to federated. Finally, Elizabeth sees the different experience with AD FS.

The main tasks for this exercise are as follows:

1. Import 3rd Party Certificate on First AD FS Server
2. Verify UPNs for Accounts and Sales Users
3. Create Host Records for AD FS Services
4. Configure a Service Account for Federation Server Farm
5. Install the First Active Directory Federation Services in the Farm
6. Configure the First Active Directory Federation Services in the Farm

7. Import Third-party Certificate on Second AD FS Server
8. Install the Second Active Directory Federation Services in the Farm
9. Configure the Second Active Directory Federation Services in the Farm
10. Verify the Federation Server is Operational
11. Import Third-party Certificate on AD FS Proxy
12. Install and Configure Active Directory Federation Services Proxy Server
13. Verify the Federation Server Proxy is Operational
14. Verify the Pre-federation User/Client Experience
15. Create a New User Account for Domain Management
16. Convert a Managed Domain to a Federated Domain using Windows PowerShell
17. Verify Identity Federation and Internal Client Connectivity
18. Verify Client Connectivity Using AD FS Proxy

► **Task 1: Import 3rd Party Certificate on First AD FS Server**

1. On your host computer, switch to the **20346C-LUC-CL1** virtual machine.
2. Ensure you are logged on as **Student1** with a password of **Pa\$\$word**.
3. On **LUC-CL1**, on the Desktop, on the Taskbar, click **File Explorer**.
4. Navigate to **E:\RDP_files**.
5. Double-click **LUC-SV1.rdp**, and connect as **LUCERNE\LucAdmin**, password: **Pa\$\$w0rd**.
6. On **LUC-SV1**, on the Taskbar, click **File Explorer**.
7. Right-click **Local Disk (C:)**, click **New**, and then click **Folder**.
8. Type **Certificates**, and then press Enter.
9. Browse to **\\LUC-EX1\C\$\Temp**, right-click **Labcert.pfx**, and click **Copy**.
10. On **LUC-SV1**, in **File Explorer**, browse to the **C:\Certificates** folder that you just created and paste in the **LabCert.pfx** certificate.
11. In **C:\Certificates**, double-click **LabCert.pfx**.
12. In the **Certificate Import Wizard**, on the **Welcome to the Certificate Import Wizard** page, select **Local Machine**, and click **Next**.
13. On the **File to Import** page, click **Next**.
14. On the **Private key protection** page, in the **Password** box, type **Pa\$\$w0rd**, and click **Next**.
15. On the **Certificate Store** page, click **Place all certificates in the following stores**, and click **Browse**.
16. In the **Select Certificate Store** dialog box, click **Personal**, and then click **OK**.
17. On the **Certificate Store** page, click **Next**.
18. On the **Completing the Certificate Import Wizard** page, click **Finish**.
19. If you get a **Security Warning** dialog box, click **Yes**.
20. In the **Certificate Import Wizard** dialog box, click **OK**.

► Task 2: Verify UPNs for Accounts and Sales Users

1. On **LUC-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Domains and Trusts**.
2. In **Active Directory Domains and Trusts**, right-click **Active Directory Domains and Trusts [LUC-DC1.lucernepublishing.local]**, and then click **Properties**.
3. In **Active Directory Domains and Trusts [LUC-DC1.lucernepublishing.local] Properties**, verify that your lab domain, in the form **labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number) is listed as a UPN suffix.
4. On the Taskbar, click **Windows PowerShell**.
5. At the Windows PowerShell prompt, type the following command, and press Enter:

```
Get-ADForest
```

6. Verify that your lab domain is listed as a UPN suffix.

► Task 3: Create Host Records for AD FS Services

1. On **LUC-DC1**, in **Server Manager**, click **Tools**, and then click **DNS**.
2. In **DNS Manager**, on the **View** menu, click **Advanced** to display the TTL value on records.
3. In **DNS Manager**, expand **LUC-DC1**, then expand **Forward Lookup Zones**.
4. Right-click **labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number), and click **New Host (A or AAAA)**.
5. In the **New Host** dialog box, in the **Name** box, type **fs**, in the **IP address** box, type **your public IP address** (where "your public IP address" is the address you noted in Module 1, Lab 1A, Exercise 1), in the **Time to live (TTL)** box, change the value to **0:0:2:0** (two minutes), and then click **Add Host**.

Note: This is the external IP address of the AD FS Proxy server, and will be used by external clients to access the AD FS server through the AD FS Proxy.

Important: We are using a low TTL value for testing only; in a production environment, you would use a longer duration for the TTL.

6. In the **DNS** dialog box, click **OK**.
7. In the **New Host** dialog box, create another host record, name **fs**, with IP address: **10.0.0.6**; in the **Time to live (TTL)** box, ensure that the value is set to **0:0:2:0** (two minutes), and then click **Add Host**.

Note: This is the IP address of the **LUC-SV1** server where AD FS will be installed, and will be used by internal clients to directly access the AD FS server, bypassing the AD FS Proxy.

Important: We are using a low TTL value for testing only; in a production environment, you would use a longer duration for the TTL.

8. In the **DNS** dialog box, click **OK**.
9. In the **New Host** dialog box, click **Done**.

► Task 4: Configure a Service Account for Federation Server Farm

1. On **LUC-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, expand **lucernepublishing.local**, right-click **Users**, point to **New**, and then click **User**.

3. In the **Full name** and **User logon name** boxes, type **adfs-service**, and then click **Next**.
4. In the **Password** and **Confirm password** boxes, type **Pa\$\$w0rd**, clear the **User must change password at next logon** check box, select the **Password never expires** check box, click **Next**, and then click **Finish**.
5. In the **Results** pane, right-click **adfs-service**, and then click **Properties**.
6. In **adfs-service Properties**, click the **Member Of** tab, and then click **Add**.
7. In the **Select Groups** dialog box, in the **Enter the object names to select** box, type **domain admins**, and then click **Check Names**.
8. Click **OK** to close the Select Groups dialog box.
9. Click **OK** to close the adfs-service Properties dialog box.
10. Switch to **Windows PowerShell**, which should still be open from an earlier task.
11. At the Windows PowerShell prompt, type the following command, and press Enter:

```
setspn -a host/fs.LabXXXXX.o365ready.com adfs-service
```

(where XXXXX is your unique O365ready.com number).

12. On **LUC-DC1**, at the Windows PowerShell prompt, type the following command, and press Enter:

```
setspn -l adfs-service
```

► Task 5: Install the First Active Directory Federation Services in the Farm

1. Switch to the **LUC-CL1** virtual machine session.
2. On the Desktop, on the Taskbar, click **File Explorer**.
3. Navigate to **E:\RDP_files**.
4. Double-click **LUC-SV1.rdp**, and connect as **LUCERNE\LucAdmin**, password: **Pa\$\$w0rd**.
5. On **LUC-SV1**, in **Server Manager**, click **Manage**, and then click **Add Roles and Features**.
6. In the **Add Roles and Features Wizard**, on the **Before you begin** page, click **Next**.
7. On the **Select installation type** page, click **Role-based or Feature-based installation**, and click **Next**.
8. On the **Select destination server** page, click **Select a server from the server pool**, verify that the target computer is highlighted, and then click **Next**.
9. On the **Select server roles** page, click **Active Directory Federation Services**.
10. In the **Add Roles and Features Wizard** dialog box, click **Add Features** to install additional .NET Framework, IIS, and Windows Process Activation Service features.
11. On the **Select server roles** page, click **Next**.
12. On the **Select features** page, click **Next**.
13. On the **Active Directory Federation Service (AD FS)** page, click **Next**.
14. On the **Select role services** page, verify the **Federation Service** check box is selected; if it's not, then select it now. Click **Next**.
15. On the **Web Server Role (IIS)** page, click **Next**.
16. On the **Select role services** page, click **Next**.

17. On the **Confirm installation selections** page, click **Install**.
18. When the installation is complete, on the **Installation progress** page, click **Close**.
19. In **Server Manager**, click **Tools**, and click **Internet Information Services (IIS) Manager**.
20. In **Internet Information Services (IIS) Manager**, expand **LUC-SV1**.
21. If you get an **Internet Information Services (IIS) Manager** dialog box, click **No**.
22. Expand **Sites**, and then click **Default Web Site**.
23. In the **Actions** pane, under **Edit Site**, click **Bindings**.
24. In the **Site Bindings** dialog box, click **Add**.
25. In the **Add Site Binding** dialog box, select **https** as **Type**.
26. In the **SSL certificate** list, select **Microsoft Exchange**, and then click **OK**.
27. In the **Site Bindings** dialog box, click **Close**, and then close IIS Manager.

► **Task 6: Configure the First Active Directory Federation Services in the Farm**

1. In **Server Manager**, click **Tools**, and then click **AD FS Management**.
2. In the **AD FS** console, click **AD FS Federation Server Configuration Wizard**.
3. In the **AD FS Federation Server Configuration Wizard**, on the **Welcome** page, verify that **Create a new Federation Service** is selected, and then click **Next**.
4. On the **Select Stand-Alone or Farm Deployment** page, click **New federation server farm**, and then click **Next**.
5. On the **Specify the Federation Service Name** page, verify that the **Microsoft Exchange** SSL certificate is displayed; if this is not the correct certificate, select the appropriate certificate from the SSL certificate list.
6. Click **Next**.
7. On the **Specify a Service Account** page, click **Browse**.
8. In the **Select User** dialog box, in the **Enter the object names to select** box, type **adfs-service**, and then click **Check Names**.
9. In the **Select User** dialog box, click **OK**.
10. On the **Specify a Service Account** page, in the **Password** box, type **Pa\$\$w0rd**, and then click **Next**.
11. On the **Ready to Apply Settings** page, review the details, and then click **Next**.
12. On the **Configuration Results** page, review the results; when all the configuration steps are finished, click **Close** to exit the wizard.
13. On the Start screen, type **PowerShell**.
14. Right-click **Windows PowerShell**, and then click **Run as administrator**.
15. At the Windows PowerShell prompt, type the following command, and press Enter

```
Enable-PSRemoting -force
```

► **Task 7: Import Third-party Certificate on Second AD FS Server**

1. Switch to the **LUC-CL1** virtual machine session.
2. On the Desktop, on the Taskbar, click **File Explorer**.

3. Navigate to **E:\RDP_files**.
4. Double-click **LUC-SV2.rdp**, and connect as **LUCERNE\LucAdmin**, password: **Pa\$\$w0rd**.
5. On **LUC-SV2**, on the Taskbar, click **File Explorer**.
6. Right-click **Local Disk (C:)**, click **New**, and then click **Folder**.
7. Type **Certificates**, and then press Enter.
8. Browse to **\\LUC-EX1\C\$\Temp**, right-click **LabCert.pfx**, and click **Copy**.
9. On **LUC-SV2**, in **File Explorer**, browse to the **C:\Certificates** folder that you just created and paste in the **LabCert.pfx** certificate.
10. In **C:\Certificates**, double-click **LabCert.pfx**.
11. In the **Certificate Import Wizard** page, on the **Welcome to the Certificate Import Wizard** page, select **Local Machine**, and click **Next**.
12. On the **File to Import** page, click **Next**.
13. On the **Private key protection** page, in the **Password** box, type **Pa\$\$w0rd**, and click **Next**.
14. On the **Certificate Store** page, click **Place all certificates in the following stores**, and click **Browse**.
15. In the **Select Certificate Store** dialog box, click **Personal**, and then click **OK**.
16. On the **Certificate Store** page, click **Next**.
17. On the **Completing the Certificate Import Wizard** page, click **Finish**.
18. If you get a **Security Warning** dialog box, click **Yes**.
19. In the **Certificate Import Wizard** dialog box, click **OK**.

► **Task 8: Install the Second Active Directory Federation Services in the Farm**

1. On **LUC-SV2**, in **Server Manager**, click **Manage**, and then click **Add Roles and Features**.
2. In the **Add Roles and Features Wizard**, on the **Before you begin** page, click **Next**.
3. On the **Select installation type** page, click **Role-based or Feature-based installation**, and click **Next**.
4. On the **Select destination server** page, click **Select a server from the server pool**, verify that the target computer is highlighted, and then click **Next**.
5. On the **Select server roles** page, click **Active Directory Federation Services**.
6. In the **Add Roles and Features Wizard** dialog box, click **Add Features** to install additional .NET Framework, IIS, and Windows Process Activation Service features.
7. On the **Select server roles** page, click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **Active Directory Federation Service (AD FS)** page, click **Next**.
10. On the **Select role services** page, verify the **Federation Service** check box is selected; if it's not, then select it now. Click **Next**.
11. On the **Web Server Role (IIS)** page, click **Next**.
12. On the **Select role services** page, click **Next**.
13. On the **Confirm installation selections** page, click **Install**.
14. When the installation is complete, on the **Installation progress** page, click **Close**.

15. On **LUC-SV2**, in **Server Manager**, click **Tools**, and then click **Internet Information Services (IIS) Manager**.
16. In **Internet Information Services (IIS) Manager**, expand **LUC-SV2**.
17. If you get an **Internet Information Services (IIS) Manager** dialog box, click **No**.
18. Expand **Sites**, and then click **Default Web Site**.
19. In the **Actions** pane, under **Edit Site**, click **Bindings**.
20. In the **Site Bindings** dialog box, click **Add**.
21. In the **Add Site Binding** dialog box, select **https** as the **Type**.
22. In the **SSL certificate** list, select **Microsoft Exchange**, and then click **OK**.
23. In the **Site Bindings** dialog box, click **Close**, and then close IIS Manager.
24. If you receive a connection error, close the error and restart these steps from Step 1, overwriting any existing settings.

► **Task 9: Configure the Second Active Directory Federation Services in the Farm**

1. On **LUC-SV2**, in **Server Manager**, click **Tools**, and then click **AD FS Management**.
2. In the **AD FS console**, click **AD FS Federation Server Configuration Wizard**.
3. In the **AD FS Federation Server Configuration Wizard**, on the **Welcome** page, click **Add a federation server to an existing Federation Service**, and then click **Next**.
4. On the **Specify the Primary Federation Server and Service Account** page, under **Primary federation server name**, type **LUC-SV1.lucernepublishing.local**, and then after the **Service account** box, click **Browse**.
5. In the **Select User** dialog box, in the **Enter the object names to select** box, type **adfs-service**, and then click **Check Names**.
6. In the **Select User** dialog box, click **OK**.
7. On the **Specify the Primary Federation Server and Service Account** page, in the **Password** box, type **Pa\$\$w0rd**, and then click **Next**.
8. On the **Specify the Federation Service Name** page, verify that the **Microsoft Exchange** SSL certificate is displayed; if this is not the correct certificate, select the appropriate certificate from the SSL certificate list.
9. Click **Next**.
10. On the **Ready to Apply Settings** page, review the details, and then click **Next**.
11. On the **Configuration Results** page, review the results. Note the information message about any website customizations needing to match on all sites in the farm.

Note: If you get a connection error, you must return to step 1 and re-run all the steps in this task

12. When all the configuration steps are finished, click **Close** to exit the wizard.

► **Task 10: Verify the Federation Server is Operational**

1. On **LUC-SV2**, in **Server Manager**, click **Tools**, and then click **Event Viewer**.
2. In the **Details** pane, expand **Applications and Services Logs**, then expand **AD FS**, and then click **Admin**.

3. In the **Event ID** column, look for event ID **100**.

Note: If the federation server is configured properly, you should see a new event with event ID 100 in the Application log of Event Viewer. This event verifies that the federation server was able to successfully communicate with the Federation Service.

4. Switch to the **LUC-CL1** virtual machine session.
5. On the Desktop, on the Taskbar, click **File Explorer**.
6. Navigate to **E:\RDP_files**.
7. Double-click **LUC-CL2.rdp**, and connect as **LUCERNE\LucAdmin**, password: **Pa\$\$w0rd**.
8. On the Start screen, click **Internet Explorer**.
9. In Internet Explorer, in the address bar type **https://fs.LabXXXXX.O365Ready.com/adfs/fs/federationsservice.asmx** (where XXXXX is your unique O365ready.com number), and then press Enter.
10. If you get a message stating **There is a problem with this website's security certificate**, click **Continue to this website**.

Note: The expected output is a display of XML with the service description document. If this page appears, IIS on the federation server is operational and serving pages successfully.

11. On **LUC-CL2**, press the Windows key to go to the Start screen.
12. On Start screen, click **LucAdmin**, and then click **Sign out**.
13. If a **Remote Desktop Connection** dialog box appears, click **OK**.

► **Task 11: Import Third-party Certificate on AD FS Proxy**

1. Switch to the **LUC-CL1** virtual machine session.
2. On the Desktop, on the Taskbar, click **File Explorer**.
3. Navigate to **E:\RDP_files**.
4. Double-click **LUC-SV3.rdp**, and connect as **LUC-SV3\LocalAdmin**, password: **Pa\$\$w0rd**.
5. On **LUC-SV3**, on the Taskbar, click **File Explorer**.
6. Right-click **Local Disk (C:)**, click **New**, and then click **Folder**.
7. Type **Certificates**, and then press Enter.
8. Browse to **\\10.0.0.5\C\$\Temp**, right-click **LabCert.pfx**, and click **Copy**.
9. On **LUC-SV3**, in **File Explorer**, browse to the **C:\Certificates** folder that you just created and paste in the **LabCert.pfx** certificate.
10. In **C:\Certificates**, double-click **LabCert.pfx**.
11. In the **Certificate Import Wizard**, on the **Welcome to the Certificate Import Wizard** page, select **Local Machine**, and click **Next**.
12. On the **File to Import** page, click **Next**.
13. On the **Private key protection** page, in the **Password** box, type **Pa\$\$w0rd**, and click **Next**.
14. On the **Certificate Store** page, click **Place all certificates in the following stores**, and click **Browse**.
15. In the **Select Certificate Store** dialog box, click **Personal**, and then click **OK**.
16. On the **Certificate Store** page, click **Next**.

17. On the **Completing the Certificate Import Wizard** page, click **Finish**.
 18. If you get a **Security Warning** dialog box, click **Yes**.
 19. In the **Certificate Import Wizard** dialog box, click **OK**.
- **Task 12: Install and Configure Active Directory Federation Services Proxy Server**
1. On **LUC-SV3**, in **Server Manager**, click **Manage**, and then click **Add Roles and Features**.
 2. In the **Add Roles and Features Wizard**, on the **Before you begin** page, click **Next**.
 3. On the **Select installation type** page, click **Role-based or Feature-based installation**, and click **Next**.
 4. On the **Select destination server** page, click **Select a server from the server pool**, verify that the target computer is highlighted, and then click **Next**.
 5. On the **Select server roles** page, click **Active Directory Federation Services**.
 6. In the **Add Roles and Features Wizard** dialog box, click **Add Features**.
 7. On the **Select server roles** page, click **Next**.
 8. On the **Select features** page, click **Next**.
 9. On the **Active Directory Federation Service (AD FS)** page, click **Next**.
 10. On the **Select role services** page, clear the **Federation Service** check box, select the **Federation Service Proxy** check box, and then click **Next**.
 11. On the **Web Server Role (IIS)** page, click **Next**.
 12. On the **Select role services** page, click **Next**.
 13. On the **Confirm installation selections** page, click **Install**.
 14. When the installation is complete, on the **Installation progress** page, click **Close**.
 15. On **LUC-SV3**, in **Server Manager**, click **Tools**, and then click **Internet Information Services (IIS) Manager**.
 16. In **Internet Information Services (IIS) Manager**, expand **LUC-SV3**.
 17. If you get an **Internet Information Services (IIS) Manager** dialog box, click **No**.
 18. Expand **Sites**, and then click **Default Web Site**.
 19. In the **Actions** pane, under **Edit Site**, click **Bindings**.
 20. In the **Site Bindings** dialog box, click **Add**.
 21. In the **Add Site Binding** dialog box, select **https** as the **Type**, in the **SSL certificate** list, select **Microsoft Exchange**, and then click **OK**.
 22. In the **Site Bindings** dialog box, click **Close**, and then close **IIS Manager**.
 23. On **LUC-SV3**, in **Server Manager**, click **Tools**, and then click **AD FS Federation Services Proxy Configuration Wizard**.
 24. In the **AD FS Federation Services Proxy Configuration Wizard**, on the **Welcome** page, click **Next**.
 25. On the **Specify Federation Service Name** page, verify that **fs.LabXXXXX.O365Ready.com** is displayed as the federation service name (where XXXXX is your unique O365ready.com number).
 26. Click **Test Connection**, and verify that you can connect to the Federation Service, and then click **OK**.
 27. On the **Specify Federation Service Name** page, click **Next**.

28. In the **Windows Security** dialog box, enter the following credentials, and click **OK**:

- User name: **LUCERNE\adfs-service**
- Password: **Pa\$\$w0rd**

Note: These credentials are necessary to establish a trust between this federation server proxy and the Federation Service. By default, only the service account used by the Federation Service, or a member of the local BUILTIN\Administrators group, can authorize a federation server proxy.

29. On the **Ready to Apply Settings** page, review the details, and then click **Next**.

30. On the **Configuration Results** page, review the results; when all the configuration steps are finished, click **Close** to exit the wizard.

31. Switch to the **LUC-CL1** virtual machine.

32. Switch to the **Windows Azure Active Directory Module for Windows PowerShell** session.

33. At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
CD E:\Labfiles\Lab11
```

34. At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
.\ResetPortForwarding.ps1
```

► Task 13: Verify the Federation Server Proxy is Operational

1. On **LUC-SV3**, in **Server Manager**, click **Tools**, and then click **Event Viewer**.
2. In the **Details** pane, expand **Applications and Services Logs**, expand **AD FS**, and then click **Admin**.
3. In the **Event ID** column, look for event ID **198**.

Note: If the federation server is configured properly, you should see a new event with event ID 198 in the Application log of Event Viewer. This event verifies that the federation server proxy service was started successfully and is now online.

► Task 14: Verify the Pre-federation User/Client Experience

1. Switch to the **LUC-CL1** virtual machine session.
2. On the **Desktop**, on the Taskbar, click **File Explorer**.
3. Navigate to **E:\RDP_files**.
4. Double-click **LUC-CL2.rdp**, and connect as **elabrecque@LabXXXXX.O365Ready.com** (where XXXXX is your unique O365ready.com number), and password: **Pa\$\$w0rd**.
5. Press the Start key and click **Internet Explorer**.
6. If the **Set up Internet Explorer** dialog box appears, click **Use recommended security and compatibility settings**, and click **OK**.
7. In the **Address** box, type **http://mail.office365.com**, and press Enter.
8. On the **Sign** page, in the **Name** box, type **elabrecque@LabXXXXX.O365Ready.com**, (where XXXXX is your unique O365ready.com number).
9. Click the **Password** box.
10. Review the **Office 365** page for **Elisabeth Labrecque** and then close Internet Explorer.

11. On **LUC-CL2**, press the Windows key to go to the Start screen.
12. On Start screen, click **Elisabeth Labrecque**, and then click **Sign out**.
13. If the **Remote Desktop Connection** dialog box appears, click **OK**.

► **Task 15: Create a New User Account for Domain Management**

1. On **LUC-DC1**, open Internet Explorer and connect to your Office 365 tenant (<https://portal.microsoftonline.com>) as **HLeitner@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number).
2. In the **Office 365 admin center**, in the left navigation, click **Domains**, select domain **labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number), and then click **Manage DNS**.
3. Review the domain type information for the partially delegated domain. It should say:
 - DNS is managed outside Office 365
 - The domain is set up with the following purpose: ExchangeOnline and LyncOnline
 - Domain status: Active
4. Click **Back to Domain Manager**.
5. Click **Users** and then click **Active users**.
6. Click the + (Add) sign.
7. In the **Details** page, in **First name**, enter **Remi**.
8. In **Last name**, enter **Desforges**.
9. In **User name**, enter **rdesforges**.
10. Click **Create** and note the temporary password. Click **Close**.
11. Double-click on **Remi Desforges** and then click **Settings**.
12. In **Settings**, under **Assign role**, click **Yes**, and then select **Global Administrator**.
13. In the **Alternate email address** field, enter **user@alt.none**.
14. Click **Licenses** and ensure **Switzerland** is selected. Click **Save**.
15. Click the **Heidi Leitner** profile icon in the top right corner, and then click **Sign out**.

► **Task 16: Convert a Managed Domain to a Federated Domain using Windows PowerShell**

1. Log on as **rdesforges@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number) with the temporary password.
2. In the **Old password** box, enter the temporary password.
3. In the **New password** and **Confirm password** boxes, enter **Pa\$\$w0rd**.
4. Click **Save**.
5. Re-enter **Pa\$\$w0rd** to sign on.
6. If you get a Don't lose access to your account page, enter **551234** for the **Mobile phone number**, **user@alt.none** for the **Alternate email address**, and then click **Save and continue**.
7. On **LUC-DC1**, press the Windows key, to go to the Start screen.

- On the Windows Start screen, click **Windows Azure Active Directory Module for Windows PowerShell**.
- At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Set-ExecutionPolicy Unrestricted
```

- Press Enter to confirm the execution policy change.
- At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
$msolcred = Get-Credential
```

- In the **Windows PowerShell Credential** dialog box, enter the following credentials, and click **OK**:
 - User name: **rdesforges@lucernepublishingXXXX.onmicrosoft.com** (where XXXX is your unique Lucerne Publishing number)
 - Password: **Pa\$\$w0rd**
- At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Connect-MsolService -Credential $msolcred
```

- At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Get-MsolDomain
```

- Verify that your lab domain, **labXXXXX.o365Ready.com** (where XXXXX is your unique O365ready.com number), is listed as **Verified** and **Managed**.
- At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Set-MsolAdfsContext -Computer LUC-SV1.lucernepublishing.local
```

- At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Convert-MsolDomainToFederated -DomainName LabXXXXX.O365Ready.com
```

(where XXXXX is your unique O365ready.com number).

- Verify that you get a **Successfully updated <your lab domain> domain** message.
- At the Windows Azure Active Directory Module for Windows PowerShell prompt, type the following command, and press Enter:

```
Get-MsolFederationProperty -DomainName LabXXXXX.O365Ready.com
```

(where XXXXX is your unique O365ready.com number).

- This command reports the status of the domain federation, and provides details of URLs and certificates.
- Switch to the **Office 365 admin center**, logged on as **Remi Desforges**.

22. In the **Office 365 admin center**, in the left navigation, click **Domains**, select domain **labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number), and then click **Manage DNS**.
23. Verify that under **DNS management**, the domain is now configured for single sign on.

► **Task 17: Verify Identity Federation and Internal Client Connectivity**

1. Switch to the **LUC-CL1** virtual machine session.
2. On the Desktop, on the Taskbar, click **File Explorer**.
3. Navigate to **E:\RDP_files**.
4. Double-click **LUC-CL2.rdp**, and connect as **elabrecque@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number) with a password of **Pa\$\$w0rd**; you are using this computer to test internal connectivity, as it is domain-joined.
5. Press the Windows key to go to the Start screen, and click **Internet Explorer**.
6. In Internet Explorer, in the upper-right hand corner, click the **cogwheel** icon to open the **Tools** menu, and then click **Internet Options**.
7. In the **Internet Options** dialog box, click the **Security** tab, click **Local intranet**, and then click **Sites**.
8. In the **Local Intranet** dialog box, click **Advanced**.
9. Under **Add this website to the zone**, enter ***.o365Ready.com**, then click **Add**.
10. Click **Close**, then click **OK** and click **OK** again.
11. In the **Address** box, type **http://portal.microsoftonline.com**, and press Enter.
12. On the **Sign** page, in the **Name** box, type **elabrecque@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number).
13. Click the **Password** box.
Note: Notice that clicking in the Password box takes you directly to the Office 365 page, without the need to enter the password again.
14. Review the **Office 365** page for **Elisabeth Labrecque** and then close Internet Explorer.
15. Press the Windows key and in the Start page, type **Outlook**.
16. Click **Outlook 2013**.
17. In the **Welcome to Outlook 2013** page, click **Next**.
18. In the **Add an Email Account** page, click **Next**.
19. In **Auto Account** setup, ensure that **elabrecque@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number) is the **email address** and click **Next**, enter **Pa\$\$w0rd** as the **Password** for **elabrecque**, and then click **Finish**.
20. Verify that Outlook has successfully configured email for **Elisabeth Labrecque**.

► **Task 18: Verify Client Connectivity Using AD FS Proxy**

1. Switch to the **LUC-CL1** virtual machine session.

Note: This computer is not domain-joined, so you are using this to simulate external access through the AD FS Proxy.
2. Press the Windows key to go to the Start screen.
3. Click **Internet Explorer**, and in the **Address** box, type **http://mail.office365.com**, and press Enter.

4. On the **Sign** page, in the **Name** box, type **elabrecque@labXXXXX.o365Ready.com** (where XXXXX is your unique O365ready.com number).
5. Click the **Password** box.
6. On the **ADFS Proxy** page, on the **Sign In at fs.LabXXXXX.o365Ready.com** page (where XXXXX is your unique O365ready.com number), in the **User name** box, type **elabrecque@labXXXXX.o365Ready.com** (where XXXXX is your unique O365ready.com number), in the **Password** box, type **Pa\$\$w0rd**, and click **Sign In**.

Note: This is the out-of-the-box sign-in page; you would customize this page with your company branding and logos.
7. On the **Outlook Web App** page, select your **time zone**, and click **Save**.
8. Review the **Office 365** page for **Elisabeth Labrecque** and then close Internet Explorer.
9. Note the experience from an external public computer, through the AD FS Proxy.

Results: At end of this process, Lucerne Publishing will have an AD FS farm installed and running correctly, with the AD FS proxy connected to AD FS farm, and users authenticating to Office 365 services with their on-premises user name and password.

Exercise 2: Manage AD FS Servers and Proxy Servers

Scenario

Heidi wants to verify that she can perform administrative tasks in AD FS, such as renewing certificates, updating federation metadata, changing the primary AD FS server to the secondary and back again, and viewing the AD FS Proxy configuration through PowerShell.

The main tasks for this exercise are as follows:

1. View Certificate Expiry Dates
2. Install the Microsoft Office 365 Federation Metadata Update Tool
3. Switch the Primary AD FS Server in the Farm
4. Use Windows PowerShell to View AD FS Proxy Configuration

► Task 1: View Certificate Expiry Dates

1. Switch to the **LUC-CL1** virtual machine session.
2. On the Desktop, on the Taskbar, click the **LUC-SV2 RDP** session.
3. On **LUC-SV2**, in **Server Manager**, click **Tools**, and then click **AD FS Management**.
4. Note the message that all configuration must be done from the primary federation server computer.
5. Switch to the **LUC-CL1** virtual machine session.
6. On the Desktop, on the Taskbar, click the **LUC-SV1 RDP** session.
7. In the **AD FS console**, in the console tree, expand **Service**, and then click **Certificates**.
8. Note the expiry dates for service communications, token-decrypting, and token-signing certificates.

► Task 2: Install the Microsoft Office 365 Federation Metadata Update Tool

1. On the Taskbar, click **Windows PowerShell**.
2. At the Windows PowerShell prompt, type the following command, and press Enter:

Set-ExecutionPolicy Unrestricted

3. Press Enter to confirm the execution policy change.
4. At the Windows PowerShell prompt, type the following command, and press Enter:
Add-WindowsFeature NET-Framework-Core -Source C:\Windows\WinSxS
5. Point your mouse to the bottom right hand corner to bring up the **Charms menu**, then click **Settings**, click **Power**, click **Restart** and click **Continue**.
6. Wait a few minutes, and then on **LUC-CL1**, on the **Desktop**, on the **Taskbar**, click **File Explorer**.
7. Navigate to **E:\RDP_files**.
8. Double-click **LUC-SV1.rdp**, and connect as **LUCERNE\LucAdmin**, password: **Pa\$\$w0rd**.
9. On **LUC-SV1**, on the Taskbar, click **File Explorer**, and then navigate to **\\LUC-DC1\C\$\Labfiles\Lab11**.
10. In **\\LUC-DC1\C\$\Labfiles\Lab11**, double-click **msoidcli_64**.
11. In the **Microsoft Online Services Sign-in Assistant Setup** wizard, on the **License Terms** page, click **I accept the terms in the License Agreement and Privacy Statement**, and click **Install**.
12. On the **Completed the Microsoft Online Services Sign-in Assistant Setup Wizard** page, click **Finish**.
13. In **File Explorer**, navigate to **\\LUC-DC1\C\$\Labfiles\Lab11** and double-click **AdministrationConfig-EN.msi**.
WARNING: If you receive an error stating that .NET Framework 3.5 SP1 is not installed, restart LUC-SV1 and try step 10 again.
14. In the **Windows Azure Active Directory Module for Windows PowerShell Setup** wizard, on the **Welcome** page, click **Next**.
15. On the **License Terms** page, click **I accept the terms in the License Terms**, and click **Next**.
16. On the **Install Location** page, click **Next**.
17. On the **Ready to Install** page, click **Install**.
18. On the **Completing the Windows Azure Active Directory Module for Windows PowerShell Setup** page, click **Finish**.
19. On the Taskbar, click **File Explorer**, and then navigate to **\\LUC-DC1\C\$\Labfiles\Lab11**.
20. In **\\LUC-DC1\C\$\Labfiles\Lab11**, right-click **O365-Fed-MetaData-Update-Task-Installation.ps1**, and then click **Copy**.
21. Right-click **C:**, and click **New**, and then click **Folder**.
22. Type **Labfiles**, and then press Enter.
23. Open **C:\Labfiles** and paste the **O365-Fed-MetaData-Update-Task-Installation.ps1** script file.
24. On the Taskbar, click **Windows PowerShell**.
25. At the Windows PowerShell prompt, type the following command, and press Enter:
CD C:\Labfiles
26. At the Windows PowerShell prompt, type the following command, and press Enter:
.\O365-Fed-MetaData-Update-Task-Installation.ps1
27. If you get a security warning, type **R**, and then press Enter.

28. At the **MSOL username** prompt, type **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique o365ready.com number), and press Enter.
29. At the **MSOL password** prompt, type **Pa\$\$w0rd**, and press Enter.
30. At the **LUCERNE\LucAdmin password** prompt, type **Pa\$\$w0rd**, and press Enter.
31. Switch to **File Explorer**, and navigate to **C:\Office365-Scripts**.
32. Verify that there is a new script: **Microsoft-Office365-Update-MSOLFederatedDomain.ps1**.
33. In **Server Manager**, from the **Tools** menu, click **Task Scheduler**.
34. In **Task Scheduler**, under **Active Tasks**, note that **Microsoft-Office365-Update-MSOLFederatedDomain.ps1** is scheduled to run every day at 12:00 AM.

► **Task 3: Switch the Primary AD FS Server in the Farm**

1. Switch back to the **Windows PowerShell** prompt and type the following command, then press Enter:

```
Get-AdfsSyncProperties
```

2. Verify that this server has the **PrimaryComputer** role.
3. On **LUC-SV2**, on the Taskbar, click **Windows PowerShell**.
4. At the Windows PowerShell prompt, type the following command, and press Enter:

```
Get-AdfsSyncProperties
```

5. Verify that this server has the **SecondaryComputer** role, and note the last sync status.
6. At the Windows PowerShell prompt, type the following command, and press Enter:

```
Set-AdfsSyncProperties -Role PrimaryComputer
```

7. Switch to the **LUC-SV1 RDP session**, and at the Windows PowerShell prompt, type the following command, and press Enter:

```
Set-AdfsSyncProperties -Role SecondaryComputer -PrimaryComputerName LUC-SV2
```

8. At the Windows PowerShell prompt, type the following command, and press Enter:

```
Get-AdfsSyncProperties
```

9. Verify that this server now has the **SecondaryComputer** role, and note the last sync status.
10. On **LUC-SV2**, at the Windows PowerShell prompt, type the following command, and press Enter:

```
Get-AdfsSyncProperties
```

11. Verify that this server now has the **PrimaryComputer** role.

► **Task 4: Use Windows PowerShell to View AD FS Proxy Configuration**

1. Switch to the **LUC-CL1** virtual machine session.
2. On the Desktop, on the Taskbar, click the **LUC-SV3 RDP** session.

Note: There is no Microsoft Management Console (MMC) snap-in to use for administering a federation server proxy. To configure and view settings for the federation server proxy you can either use Windows PowerShell cmdlets or rerun the AD FS Federation Services Proxy Configuration Wizard. For the purposes of this lab, we will use Windows PowerShell.

3. On **LUC-SV3**, on the Taskbar, click **Windows PowerShell**.
4. At the Windows PowerShell prompt, type the following command, and press Enter:

```
Get-ADFSPProxyProperties
```

5. Verify the host name and ports used by the AD FS Proxy. The host name should be **fs.labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number) and it should use the standard **https (443)** and **http (80)** ports.

Results: At end of this exercise, Lucerne Publishing has updated its AD FS certificates, and managed the AD FS environment successfully.

Lab Review Discussion Questions

In the lab, why did you create two DNS host records for the AD FS server?

The scenario required an internal record for domain-joined AD FS clients on the corporate network, and an external record for non-domain-joined clients.

What are the key steps in the conversion of a managed domain to a federated domain?


You must configure Office 365 with the name of the AD FS server to use for authentication requests, by using the **Set-MsolAdfsContext -**

Computer <server name> command, and then switch the Office 365 domain to federated, by using the **Convert-MsolDomainToFederated -DomainName <domain>** command.

- In the lab, why did you create two DNS host records for the AD FS server?
- What are the key steps in the conversion of a managed domain to a federated domain?

Module Review and Takeaways

Having completed this module, you can now plan for an AD FS deployment, install and manage AD FS servers, and install and manage AD FS proxies.

-  **Best Practice:** Always plan for using an AD FS proxy server; publishing 443 from the Internet directly to the AD FS server is not a good idea, otherwise any external computer could have direct access to your federation servers.
- Avoid having federation servers directly accessible on the Internet; direct Internet access should only be used when setting up a test lab environment, or when the organization does not have a perimeter network. You should isolate your federation servers, so that they can only be accessed by client computers that are authenticated against the corporate network through an AD FS Proxy.
- Prepare DNS to mitigate against incorrect DNS updates, especially with split brain DNS. If DNS is not functioning correctly, client computers may not be able to access AD FS.
- Pay close attention to networking, firewall, and security design, to ensure that client computers can authenticate to the corporate Active Directory.
- Ensure that all certificates are exported to include the private key; this is because both public and private keys are required for certificates to function on the Default Website.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
AD FS server configuration fails.	

MCT USE ONLY. STUDENT USE PROHIBITED

Module 12

Monitoring Office 365

Contents:

Module Overview	12-1
Lesson 1: Isolate Service Interruption	12-2
Lesson 2: Monitor Service Health	12-12
Lesson 3: Analyze Reports	12-14
Lab: Monitoring Office 365 (Optional)	12-23
Module Review and Takeaways	12-28

Module Overview

In this module, students learn about monitoring user connections to Office 365™ and how to cope with service outages. They look at a range of tools that diagnose service health and review the reports that Office 365 provides.

Objectives

After completing this module, you should be able to:

- Isolate and identify causes of Office 365 service interruption.
- Monitor Office 365 service health.
- Analyze and use Office 365 reports.

Lesson 1

Isolate Service Interruption

In this lesson, students learn about creating a service request, and how to use a range of tools such as the Microsoft® Remote Connectivity Analyzer (RCA), the Transport Reliability IP Probe (TRIPP), the Microsoft Connectivity Analyzer tool, and the hybrid free/busy troubleshooter tool.

Lesson Objectives

After completing this lesson, you should be able to:

- Provide an overview of Office 365 troubleshooting techniques, and describe the use of the Do it yourself troubleshooter.
- Describe service requests in Office 365.
- List the connectivity analysis tools that can be used with Office 365, and explain how these tools are used.
- Explain the purpose of the Transport Reliability IP Probe (TRIPP), and describe how this tool is used.
- Describe how to troubleshoot free/busy notifications in a hybrid Office 365 environment.
- Describe how to use Office 365 message tracking tools.

Office 365 Troubleshooting Overview

There is a range of tools and resources that can be used to identify and isolate service interruptions, and to help troubleshoot issues in Office 365, and in related services such as Microsoft Exchange, Lync® Online, and SharePoint® Online. These tools include Office 365 service requests, connectivity analysis tools, TRIPP, Hybrid free/busy troubleshooter, and message tracking tools.

As a starting point, the Office 365 Troubleshooter can help with initial diagnosis. This troubleshooter is available from the Office 365 admin center, by clicking **tools**, and then clicking **Do it yourself troubleshooter**.

- Office 365 Troubleshooting tools:
 - Office 365 service requests
 - Connectivity analysis tools
 - Transport Reliability IP Probe (TRIPP)
 - Hybrid free/busy trouble-shooter
 - Message tracking tools, such as Message Trace and Delivery Reports
- Office 365 Troubleshooter



The Office 365 Troubleshooter is also available directly from the following link:

<http://go.microsoft.com/fwlink/?LinkId=524373>

To use the Office 365 Troubleshooter:

- Select an Office 365 plan (such as Office 365 Enterprise).
- Select a role (user or administrator).
- Select a service, topic, and a specific area.
- The troubleshooter then provides a list of relevant support resources, such as:
 - Service: Service Management

- Topic: Active Directory synchronization
- Specific area: Creating, editing, or deleting users



For information on which tools should be used for specific Office 365 problem areas, go to:

<http://go.microsoft.com/fwlink/?LinkId=391782>

The remainder of this lesson provides details on the commonly-used tools to help identify and isolate service interruption issues.

Service Requests

Office 365 administrators can request technical assistance from the Office 365 Support team either online, by submitting a service request, or by phone.

To open a new service request:

1. In the Office 365 admin center, in the left pane, click **Support**; you must be an Office 365 administrator.
2. On the Support page, under **Contact support**, click **New service request**.
3. On the New service request page, under **identify the issue**, select the **Issue type** (for example, **Service Interruption**), **Service** (for example, **Exchange Online**), **Service area** (for example, **Mail Flow**), and **Problem area** (for example, **Read receipts and delivery receipts**).
4. Links to possible solutions for the specified problem are provided. These should be read before proceeding with the service request in case the issue is a common one that can be resolved without requesting additional support.

- Service requests:
 - Used to obtain help from Office 365 team
 - Initiate from Office 365 admin center, support page
- Response times:
 - Standard plans
 - Elevated support



Note: If a service is unavailable, the service health dashboard should be checked before opening a new service request (service health is discussed in the next lesson). If a service appears to be unavailable but there are no reports in the service health dashboard, you should call the Office 365 support telephone number for your country or region by selecting the call technical support link on the support page.

5. After entering the problem area information on the **Add a detailed description** page, you then add further information to the service request, including title, description, any error messages, and a contact name and phone number. It is important to be as detailed as possible in service requests to help the support team rapidly diagnose the issue.
6. On the **Add supporting information** page, select the Office 365 domain which is experiencing the problem, and (optionally) any relevant operating system, Microsoft Office version, and browser version information. It is also important to state whether the problem can be reproduced on more than one computer.
7. You can then add up to five screenshots of any errors or other relevant documents to the service request. These files must be no larger than 5 MB each.

8. After you click **Submit** to submit the service request, a reference number for the request is provided, and the new request will be listed in the open service requests list. Service requests are passed directly to a Support representative, who will respond with an email message. The target initial response time for a new service request depends on both the severity level of the issue and the Office 365 subscription type, as highlighted in the table below.

Severity Level	Office 365 for Enterprises	*Elevated Support Options
Response time for Severity A (Example: One or more services aren't accessible or are unusable.)	Within 1 hour, 24 hours a day, seven days a week.	Within 1 hour, anytime. Calls and service requests are handled 24 hours a day, seven days a week.
Response time for Severity B (Example: The service is usable but in an impaired fashion.)	Within 8 hours, 24 hours a day, seven days a week.	Within 2 hours, anytime.
Response time for Severity C (Example: the issue is important but doesn't currently have a significant impact on service or productivity.)	Anytime. Calls and service requests are handled 24 hours a day, seven days a week.	Within 4 hours, anytime.

***Elevated Support** provides additional support options and SLAs over the standard support provided with Office 365 Small Business, Office 365 Midsize Business, and Office 365 Enterprise plans.

After a service request has been submitted, any further actions required by the Support representative, such as requests for additional information, will be shown as "Action required" in the list of open requests on the Service requests page. Notes and files can also be added to an existing service request. When an issue is resolved or assistance is no longer needed, it is important to close the request.

Connectivity Analysis Tools

Microsoft provides several tools that can be used to analyze connectivity issues in Office 365 deployments. The Microsoft Remote Connectivity Analyzer (RCA) is used to run tests directly from the <http://testconnectivity.microsoft.com> website. The Microsoft Connectivity Analyzer tool runs a similar set of tests to RCA, but from a client computer.

Microsoft Remote Connectivity Analyzer (RCA)

The Microsoft RCA website, also known as the Exchange Remote Connectivity Analyzer, provides a set of tools for identifying common connectivity issues for Outlook®, Exchange, Lync®, and Office 365. RCA also hosts the Message Analyzer, which is covered in Lesson 3 of this module.

Two sets of connectivity analysis tools:

- Microsoft Remote Connectivity Analyzer (RCA)
 - Tests run from <http://testconnectivity.microsoft.com>
 - No client requirements
 - Select problem area, then run a test
- Microsoft Connectivity Analyzer tool (MCA)
 - Tests run from client computer
 - Installed in client, requires .NET Framework 4.5
 - Set of test questions

There are several tests available that are accessed from tabs in the RCA tool.

Tab	Tests
Exchange Server	<ul style="list-style-type: none"> • Microsoft Exchange ActiveSync Connectivity Tests: <ul style="list-style-type: none"> ○ Exchange ActiveSync ○ Exchange ActiveSync Autodiscover • Microsoft Exchange Web Services Connectivity Tests: <ul style="list-style-type: none"> ○ Synchronization, Notification, Availability, and Automatic Replies ○ Service Account Access (Developers) • Microsoft Office Outlook Connectivity Tests: <ul style="list-style-type: none"> ○ Outlook Anywhere (RPC over HTTP) ○ Outlook Autodiscover • Internet Email Tests: <ul style="list-style-type: none"> ○ Inbound SMTP Email ○ Outbound SMTP Email ○ POP Email ○ IMAP Email
Lync/OCS Server	<ul style="list-style-type: none"> • Microsoft Lync Tests: <ul style="list-style-type: none"> ○ Lync Server Remote Connectivity Test ○ Lync Autodiscover Web Service Remote Connectivity Test • Microsoft Office Communications Server Tests: <ul style="list-style-type: none"> ○ Office Communications Server Remote Connectivity Test
Office 365	<ul style="list-style-type: none"> ○ Includes all the tests from the Exchange Server tab, plus • Office 365 General Tests: <ul style="list-style-type: none"> ○ Office 365 Exchange Domain Name Server (DNS) Connectivity Test ○ Office 365 Lync Domain Name Server (DNS) Connectivity Test ○ Office 365 Single Sign-On Test • Mail Flow Configuration: <ul style="list-style-type: none"> ○ Verify Service Delivery Test ○ Verify MX Record and Outbound Connector Test • Free/Busy Test: <ul style="list-style-type: none"> ○ Free/Busy

All the RCA tests run from the <http://testconnectivity.microsoft.com> website, and there are no local prerequisites.

After performing a test, RCA provides very detailed log information on the test steps that were passed successfully and on the steps that failed, followed by a suggested resolution. This log information can be saved to the clipboard, or to an .xml or .html file. For most tests, a **Tell me more about this issue and how to resolve it** link is available that provides additional information to help fix the issue.

Microsoft Connectivity Analyzer (MCA)

The MCA tool is a downloadable client program that is used to identify connectivity issues between email clients and Microsoft Exchange Server, and between email clients and Office 365. MCA can be used both by email users to identify common problems, and by administrators to troubleshoot Exchange Server and Office 365 deployments.

MCA is a companion to the RCA website, but where RCA enables administrators to identify connectivity issues by simulating connectivity from outside the customer environment (the RCA website), the MCA enables users and administrators to run similar tests from a client computer within the corporate network. Although MCA provides tests that are similar to RCA, the tests are presented as a set of statements based on possible issues:


- *I can't log on with Office Outlook.* This test helps identify connectivity issues between email clients and Microsoft Exchange Server. The test goes through each step that Outlook must complete in order to connect through Outlook Anywhere (RPC over HTTP), and how Outlook obtains Autodiscover service settings. The **I use single sign-on** check box option enables this test to also validate whether a user can log on to Office 365 by using on-premises credentials, which also validates basic Active Directory Federated Services (AD FS) configuration settings.
- *I can't send or receive email on my mobile device.* This test simulates steps used by mobile devices to obtain settings from the Exchange Autodiscover service, and then to connect to Exchange using Exchange ActiveSync.
- *I can't log on to Lync on my mobile device or the Lync Windows Store app.* This test verifies DNS records for an on-premises domain in order to validate correct configuration for Mobile Lync clients. This test also checks the Autodiscover web service to ensure that authentication, certificates, and web services are properly configured.
- *I can't send or receive email from Outlook (Office 365 Only).* This test validates correct configuration for mail flow by verifying DNS records in an Office 365 domain.
- *I can't view the free/busy information of another user.* This test is for hybrid Exchange environments; it checks whether an Office 365 mailbox can access the free/busy information for an on-premises mailbox and that an on-premises mailbox can access the same information for Office 365. This test includes a range of checks, including that the system time of the Exchange hybrid server is not offset by more than five minutes (which can cause failures through AD FS), and that inbound connectivity to the hybrid server does not require firewall pre-authentication (this can only be checked when the MCA client is run from outside the corporate network). The test also includes links to guidance on using the Hybrid Configuration wizard; if the wizard is incorrectly used, it can lead to potential hybrid deployment misconfiguration.
- *I am experiencing other problems with Outlook (English Only).*
- *I can't set up federation with Office 365, Azure, or other services that use Azure Active Directory.* This test performs the following steps:
 1. Retrieves and validates domain registration and federation status to ensure that provisioned data matches that for the identity provider.
 2. Tests the sign-in flow against the active AD FS endpoint for rich client sign-in scenarios.
 3. Tests the Metadata Exchange Endpoint (MEX) data used by rich clients to determine how to communicate with AD FS.
 4. Tests the sign-in flow with the passive AD FS endpoint for browser-based sign-in scenarios.

The Microsoft Connectivity Analyzer tool is installed from the Microsoft Remote Connectivity Analyzer website, at <http://testconnectivity.microsoft.com>; click the **Client** tab, and then click **Install Now**.

The prerequisites for the MCA tool include:

- Windows 8, Windows 7, Windows Vista, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008.
- Microsoft .NET Framework 4.5.
- Lync diagnostics require the Unified Communications Managed API (UCMA) 4.0 Runtime, and only run on 64-bit operating systems.
- One of the following browsers:
 - Internet Explorer
 - Google Chrome with ClickOnce for Google Chrome
 - Firefox with Microsoft .Net Framework Assistant for Firefox

The MCA is similar to RCA in that it gives a log showing the test steps that were passed successfully and the steps that failed, and then provides a **Tell me more about this issue and how to resolve it** link that makes suggestions to help fix any reported issues. The log can be saved as **MCATestResults.html**.

 **The Microsoft Connectivity Analyzer tool page provides a list of articles with detailed information on the specific error conditions that are identified by MCA, and help on resolving the issue. The MCA tool page can be accessed here:**

<http://go.microsoft.com/fwlink/?LinkId=391783>

Lync Transport Reliability IP Probe

The Lync Online Transport Reliability IP Probe (TRIPP) tool is a Java-based tool that tests the following conditions:

- The transport path between a computer and a Lync Online data center.
- Port availability.
- Routing to the data center.
- Voice over IP (VoIP) simulation.
- Network speed.

- Checks transport between client and Lync Online
- Used in browser, requires Java
- TRIPP performs several tests:
 - Speed
 - Route
 - VoIP
 - Firewall

For example, TRIPP can help troubleshoot issues when connecting to a Microsoft Lync Online conference or when making a peer-to-peer call, where the audio or video quality may be choppy, tinny, or delayed, causing the meeting or call to be unusable.

TRIPP performs several tests:

- *Speed*. This test measures download and upload speeds, quality of data, and TCP efficiency, and uses TCP port 443 for download and upload testing.
- *Route*. This test measures route quality, including packet loss, latency, round trip, and ISP peering points, and uses Internet Control Message Protocol (ICMP).
- *VoIP*. This test estimates expected VoIP quality by measuring UDP loss and jitter, and uses UDP ports 50021 and 50022 to simulate audio streams using the G722 codec at 50pps.

- *Firewall.* This tests whether any network firewall is blocking the ports used by the Microsoft Lync Online Service, and uses outbound connections to TCP port 443 for Client Signaling plus AppShare, TCP port 5061 for Federation Signaling, UDP port 3478 for Media Access, and UDP ports within the 50,000-59,999 range for Audio/Video transport tests.

To obtain and access the TRIPP tool, select the URL that is closest to the user's physical location:

- San Antonio, Texas, USA: <http://trippsn2.online.lync.com/>
- Blue Ridge, Virginia, USA: <http://trippbl2.online.lync.com/>
- Amsterdam, Netherlands, Europe: <http://trippams.online.lync.com/>
- Dublin, Ireland, Europe: <http://trippdb3.online.lync.com/>
- Hong Kong SAR, China, East Asia: <http://trippkh.online.lync.com/>
- Singapore, Singapore, East Asia: <http://trippsg1.online.lync.com/>



Note: TRIPP is run from a browser and requires that Java be installed on the client computer. To get TRIPP to run, you must lower your Java security requirements to medium and add both the lync.com domain and the IP address used for the speed test site to your list of safe sites.

How to Analyze the Tool Output

After TRIPP tests have completed, the following graphs and statistics should be examined:

- *Media Access test.* This test verifies that the client computer can connect to the Lync Online media servers over UDP port 3478. The test may fail if a firewall is blocking UDP port 3478 for both incoming and outgoing connections. If this port is blocked, symptoms may include audio/video calls that do not connect, desktop sharing and other collaboration features that do not connect, and conference join failures.
- *AudioVideo - lowerbound and AudioVideo - upperbound tests.* These tests can fail if the UDP port range 50,000-59,999 is blocked in any network firewall. TRIPP does not check all the ports in the range, and assumes that if both the lowerbound port and upperbound port are open, the ports that are in between these two are also likely to be open.
- *Download and upload speed tests.* These tests identify whether the download or upload speed is less than 1 Mbps, which can lead to audio/video quality degradation, in turn affecting the quality of the audio/video connection or the collaboration features.
- *Voice over IP (VoIP) test.* This test verifies whether the connections have a consistent round-trip response time, and validates the Consistency of Service. If the response rates for each packet vary too much, or if there is too much packet loss, the audio/video connection may be jittery or choppy. Connections that have more than 5ms jitter or more than two percent packet loss may experience degraded quality in audio, video, or application sharing. Switching to a more consistent connection or reducing the number of hops in the route may resolve this issue.



For detailed information on using TRIPP to diagnose audio and video quality issues, go to:

<http://go.microsoft.com/fwlink/?LinkId=391788>

Hybrid Free/Busy Troubleshooter

The Hybrid Environment Free/Busy Troubleshooter is a guided-walk-through tool. It covers the troubleshooting of free/busy issues in a hybrid deployment of Microsoft Exchange Online in Office 365 and an on-premises Microsoft Exchange Server. The troubleshooter is designed to be used by the Tenant Administrator, and elevated access is required for many of the steps.

The Hybrid Environment Free/Busy Troubleshooter also provides an overview of how Free and Busy is designed to work in Hybrid Exchange 2010/2013, Exchange 2007, and Exchange 2003 environments.

The troubleshooter also provides links to other tools that can be used to troubleshoot free/busy issues, including RCA.

 **The Hybrid Environment Free/Busy Troubleshooter tool can be downloaded from the following site:**

<http://go.microsoft.com/fwlink/?LinkId=524406>

- Guided-walk-through, available from <http://aka.ms/hybridfreebusy>
- Provides:
 - Troubleshooting steps
 - Overview of how Free and Busy is designed to work
 - Links to other free/busy troubleshooting tools
- Start points:
 - My Cloud user cannot see Free/busy for an on-premises user
 - My On-premises user cannot see Free/busy for a cloud user

Using the Hybrid Environment Free/Busy Troubleshooter

The Hybrid Environment Free/Busy Troubleshooter provides the following start points:

- My Cloud user cannot see Free/busy for an on-premises user.
- My On-premises user cannot see Free/busy for a cloud user.

After selecting the appropriate start point, the troubleshooter presents a series of items to check or test, along with suggested solutions and relevant links if an item matches the tester's situation.

Message Tracking Tools

There are several message tracking tools that can be used in Office 365 environments to help diagnose email delivery issues.

Message Header Analyzer

Email messages are transmitted between mail servers using Simple Mail Transfer Protocol (SMTP). SMTP message headers contain information that records both the origins of a message and its path through one or more SMTP servers to its destination. The RCA Message Analyzer feature can display the contents of these headers, and help diagnose any email transfer issues. All Message Analyzer processing is done in the browser, and no additional software is required. The Message Analyzer can be used on any SMTP header, whether generated by Exchange, Office 365, or any other RFC standard SMTP server or agent.

- Message Header Analyzer
- Delivery reports
 - Exchange Online message trace tool in the Exchange Admin Center (EAC)
 - Delivery reports in the EAC
 - Personal delivery reports in OWA

After you receive a delivery failure message:

- Note the reason for the failure, such as **NonExistentDomain**, or **550 Requested action not taken: mailbox unavailable**.
- Copy the message headers from a message.
- Go to **<http://testconnectivity.microsoft.com>** and select the **Message Analyzer** tab.
- Paste the message and click **Analyze headers**.
- In the Message Header Analyzer, diagnostic information and the time taken for the message to be rejected will be displayed.

Delivery Reports

Delivery reports provide an alternative method for tracking email delivery, and can be run at the Exchange server/Office 365 level, or within the Outlook Web App (OWA) by users wishing to track their own personal messages.

There are three kinds of delivery reports available to you: the Exchange Online Message Trace tool, server level delivery reports, and personal delivery reports.

The Exchange Online Message Trace Tool in the Exchange admin center (EAC)

To run the Exchange Online message trace tool from the EAC:

1. Select **Mail flow**.
2. Click **Message trace**.
3. In Message trace, next to Sender, click **Add users**, and select the users to trace.
4. Under **Message was sent or received**, select one of the time periods:
 - Last 24 hours
 - Last 48 hours
 - Last 7 days
 - Custom (select start and end date and time)
5. Under **Delivery status**, select one of following statuses:
 - Delivered
 - Failed
 - Pending
 - Expanded
 - Unknown
6. Or leave to search for all statuses.
7. Optionally, click **Message ID** to narrow the search based on a specific Internet message ID (also known as the Client ID). This ID is generated by the sending mail system and can be found in the header of the message with the "Message-ID:" token. Specify the full Message ID of the message. This may include angle brackets (< >).
8. Then click **Search**.
9. Double-click any returned message to view the sender, recipient, message size, message ID, IP address information, and delivery status.

10. The Message trace tool then displays a series of event associated with the message; for example, RECEIVE, SUBMIT, and SEND for a successful message; or RECEIVE, SUBMIT, and FAIL for a message that could not be delivered.

Delivery Reports in the EAC

To run the server level delivery reports from the Exchange admin center (EAC):

1. Select **Mail flow**.
2. Click **Delivery reports**.
3. Next to **Mailbox to search**, click browse to select a mailbox.
4. Then do one of the following:
 - **Search for messages sent to**, and click **Select users**.
 - **Search for messages received from**, and click **Select users**.
5. Optionally, you can type in specific words to search for in the subject line.
6. Click **Search**.

Personal Delivery Reports in OWA

To run Personal delivery reports within OWA:

1. Select the **Settings** menu.
2. Click **Options**.
3. On the Options page, click **Organize email**, and then click **Delivery reports**.
4. Double-click a message to view the delivery report.



Note: Personal delivery reports provide the same options as EAC delivery reports, except that **Select mailbox to search** is not an option (this report only searches the current user's mailbox).

The following is an example of a delivery report for a successful transfer:

```
RE: December Sales Meeting
From: Miriam Pichler
To: rick.torres@contoso.com
Sent: 11/11/2013 20:00
Delivery Report for rick.torres@contoso.com (rick.torres@contoso.com)
Transferred
11/11/2013 20:0
The message was successfully handed off to a different email system. This is as far
as we can track it.
```

Lesson 2

Monitor Service Health

In this lesson, students learn how to monitor service health using tools such as the RSS feed and the Service Health dashboard. This enables students to become aware of issues such as planned maintenance, together with service updates and historical data. Students also learn about the Office 365 Management Pack for System Center Operations Manager.

Lesson Objectives

After completing this lesson, you should be able to:

- Describe service health, planned maintenance, and RSS feeds in Office 365.
- Describe the Office 365 Management Pack for System Center Operations Manager.

Service Health and Planned Maintenance

The Service Health page of the Office 365 admin center provides information on the health of your online services and access to information about any impending maintenance tasks that have been planned by Microsoft.

Service Health

On the main Office 365 **Dashboard** page, in the **Service overview** section, you can see an overview of your service health, which lists the current health state of your online services. However, if you need more detail then view the **Service health** page, which can be accessed in the left menu or by clicking **View details and history** on the **Service overview** page.

• Service health
• Health status
• Current day, last 6 days, 30 day history
• Planned maintenance
• Upcoming and historical maintenance
• Date and time
• RSS feeds
• Subscriptions added to the Common Feed List
• IE and Outlook
• New events and updated events

The table on the **Service health** page displays status information for the current day and the previous six days. This table shows the current status of each of the online service components, and you can click each status icon for more information.

You can also click **View history for past 30 days** to see further historical service health data. On the **30 day history** page you can see specific incidents that have occurred within the last 30 days and the categories they come under, including Office 365 Portal, Identity Service, Lync Online, and Exchange Online.

To see specific incident details, click on the **INCIDENT ID** in the table, which gives you chronological data about the outage or issue and any resolution to the problem. If a post-incident report has been published, you can also download or view the report for more detail.



Note: The **Service health** page only includes information about the health of your online services; it does not cover other items, such as network infrastructure issues.

Planned Maintenance

You can also view information on any upcoming Office 365 maintenance tasks that have been scheduled by clicking **Planned Maintenance** on the **Service health** page. This page displays the date and time of any planned maintenance that will be occurring, and you can click the link in the status column for more information.

RSS Feeds

The **Service health** page also provides a link to an RSS feed for Office 365 service health. Click the **Subscribe to this feed** link to subscribe to the feed. This will add the feed to your Common Feed List, which can be viewed in programs that use the Common Feed List, such as Internet Explorer and Outlook. The feed is updated each time a new incident event is added or an existing incident event is updated.

Office 365 Management Pack for SCOM

You can use System Center Operations Manager (SCOM) to perform some very basic monitoring of Office 365 services, including checking Internet connectivity and some service availability.

There is a basic management pack available which contains the following tests:

- *LoginOffice365*. This tests logging in to the Office 365 portal.
- *InboxOffic365*. This tests accessing an Office 365 mailbox.
- *TeamSiteOffice365*. This tests accessing the Office 365 team site.



For more information on how to obtain and setup this management pack, go to:

<http://go.microsoft.com/fwlink/?LinkId=391789>

- SCOM Management Pack for Office 365
- Performs basic tests
 - Login to Office 365 portal
 - Access Office 365 mailbox
 - Access Office 365 Team Site

Lesson 3

Analyze Reports

In this lesson, students learn to analyze service reports from Office 365, such as mail protection reports, the auditing log, and portal email hygiene reports. Students also learn about some of the Windows PowerShell cmdlets for reporting in Exchange Online.

Lesson Objectives

After completing this lesson, you should be able to:

- Describe the auditing logs in Office 365.
- Describe the portal email hygiene reports in Office 365.
- Describe the mail protection reports in Office 365.
- Describe the Exchange Online protection reports in Office 365.
- Describe Windows PowerShell cmdlets for reporting in Exchange Online.

Auditing Reports

There are several auditing reports available in the **Reports** menu of the Office 365 admin center. These reports can be found in the **Overview** section under **Auditing**.

Mailbox Access by Non-Owners Report

This report returns a list of mailboxes that have been accessed by someone other than the owner of the mailbox. The audit log that the report is generated from logs information such as the person accessing the mailbox, when they accessed it, what actions they performed, and whether their actions were successful or not.

To run the Mailbox Access by Non-owners report:

1. In the Office 365 admin center, in the left menu, click **Reports**.
2. At the bottom of the **Overview** page, under **Auditing**, click **Mailbox access by non-owners**.
3. In the **Start date** boxes, specify a start date for the report.
4. In the **End date** boxes specify an end date for the report.
5. Then do one of the following steps:
 - a. Click Select mailboxes and select which mailboxes to search
or
 - b. Leave the field blank to search all mailboxes.
6. Under **Search for access by**, click the drop-down list and select one of these options:
 - **All non-owners**
 - **External users**

- Office 365 admin center>reports>auditing
 - Mailbox access by non-owners
 - Role group changes
 - Mailbox content search and hold
 - Mailbox litigation holds
- Print reports

- **Administrators and delegated users**
 - **Administrators**
7. Click **Search**.
 8. The results are returned in the **Search results** window.



For information about running a mailbox access by non-owners report in the Exchange admin center, go to:

<http://go.microsoft.com/fwlink/?LinkId=391790>

Role Group Changes Report

This report returns a list of all the changes made to the Office 365 role groups by administrators in your organization. The audit log that this report is generated from logs information about who made the change, when they did it, and what the change was.

To run the Role Group Changes report:

1. In the Office 365 admin center, in the left menu, click **Reports**.
2. At the bottom of the page, under **Auditing**, click **Role group changes**.
3. In the **Start date** boxes, specify a start date for the report.
4. In the **End date** boxes specify an end date for the report.
5. Then do one of the following steps:
 - a. Click Select role groups and select the role groups to search.
or
 - b. Leave the field blank to search all role groups.
6. Click **Search**.
7. The results are returned in the window at the bottom of the page.



For more information about running the role group changes report in the Exchange admin center, go to:

<http://go.microsoft.com/fwlink/?LinkId=391791>

Mailbox Content Search and Hold Report

This report returns a list of all the mailboxes that have been put on, or removed from In-Place Hold or In-Place eDiscovery using the In-Place eDiscovery and Hold feature. The audit log that this report is generated from logs information about who put the mailbox on hold, and when they did it.

To run the Mailbox Content Search and Hold report:

1. In the Office 365 admin center, in the left menu, click **Reports**.
2. At the bottom of the page, under **Auditing**, click **Mailbox content search and hold**.
3. In the **Start date** boxes, specify a start date for the report.
4. In the **End date** boxes specify an end date for the report.
5. Click **Search**.
6. The results are returned in the **Search results** window.



For more information on In-Place Hold, go to:

<http://go.microsoft.com/fwlink/?LinkId=391792>



For more information on In-Place eDiscovery, go to:

<http://go.microsoft.com/fwlink/?LinkId=391793>

Mailbox Litigation Holds Report

This report returns a list of all changes made to per-mailbox litigation holds. The audit log that this report is generated from logs information about who enabled or disabled litigation hold on a mailbox, and when they did it.

To run the Mailbox Litigation Holds report:


1. In the Office 365 admin center, in the left menu, click **Reports**.
2. At the bottom of the page, under **Auditing**, click **Mailbox litigation holds**.
3. In the **Start date** boxes, specify a start date for the report.
4. In the **End date** boxes specify an end date for the report.
5. Then do one of the following steps:
 - a. Click Select users and select which users' mailboxes to search.
or
 - b. Leave the field blank to search all users' mailboxes.
6. Click **Search**.
7. The results are returned in the **Search results** window.



For more information about running the mailbox litigation holds report in the Exchange admin center, go to:

<http://go.microsoft.com/fwlink/?LinkId=391794>



Note: For all of these auditing reports you can click the  (printer) icon to print the resulting reports.

Mail and Protection Reports

The **Reports** menu of the Office 365 admin center provides access to several mail and protection reports.

Mail Reports

There are several mail-related reports available under the **Mail** section of the **Reports** menu in the Office 365 admin center, including:

- *Active and inactive mailboxes*. This report shows the number of active and inactive mailboxes over a period of time. A mailbox is considered inactive if a user has not accessed it for more than 30 days.

- Office 365 admin center>reports>mail
 - Active and inactive mailboxes
 - New and deleted mailboxes/groups
 - Mailbox usage/types of mailbox connections
- Office 365 admin center>reports>protection
 - Received /sent mail
 - Received/sent spam
 - Malware detections
 - Top malware
- Chart or Table views

- *New and deleted mailboxes.* This report shows the number of active, new, and deleted mailboxes.
- *New and deleted groups.* This report shows the number of groups created and deleted.
- *Mailbox usage.* This report shows the total number of mailboxes, inactive mailboxes, mailboxes which have exceeded their storage quota, and mailboxes which are currently using less than a quarter of their storage quota.
- *Types of mailbox connections.* This report shows the number of mailbox connections made over time, which are then grouped by connection type, such as POP3, IMAP, and OWA.

All these reports are displayed as charts and provide a link to view each chart as a table instead. Some of them have clickable links which display the information on a daily, weekly, monthly, or yearly basis.

Protection Reports

There are several protection-related reports available under the **Protection** section of the **Reports** menu in the Office 365 admin center, including:

- *Received mail.* This report shows mail that has been received, grouped by type of traffic, such as good mail, spam, malware, transport rules, and DLP policy. It also displays a list of top mail recipients, showing the recipient's email address and count of emails received.
- *Sent mail.* This report shows mail that has been sent, grouped by type of traffic, such as good mail, spam, malware, transport rules, and DLP policy. It also displays a list of top mail senders, showing the sender's email address and count of emails sent.
- *Received spam.* This report shows what spam has been detected, grouped by spam filtering type, such as SMTP blocked, IP blocked, and Content filtered. It also displays a list of top spam recipients, showing each recipient's email address and count of spam emails received.
- *Malware detection in received mail.* This report shows the number of malware detections in received mail, before the malware action was applied. It also displays a list of top malware recipients, showing each recipient's email address and count of malware received.
- *Malware detection in sent mail.* This report shows the number of malware detections in sent mail, before the malware action was applied.
- *Top malware.* This report shows a list of the most frequently-detected malware.
- *Sent spam.* This report shows sent mail that is suspected of being spam, grouped by filtering type, such as SMTP blocked, and content filtered.

All of these reports are displayed as charts and provide a link to view each chart as a table instead. They also all have clickable links to enable the chart to display the information over seven-day, 14-day, 30-day, or 60-day periods.

Mail Protection Reports for Office 365

On the **Reports** page of the Office 365 admin center, under **Download your reports**, there is a **Mail protection reports (Excel)** link which enables administrators to download mail protection reports for Office 365. The link opens a webpage on the Microsoft Download Center, where you can download the **Microsoft Office 365 Excel Plugin for Exchange Online Reporting**. The download is packaged as an MSI file, and there are 32-bit and 64-bit versions that can be downloaded.

- Office 365 admin center>Reports>Download your reports>Mail protection reports (Excel)
 - Download link to Microsoft Download Center
 - Excel 2013 reporting workbook
 - Install creates desktop shortcut
- Run queries from report workbook tabs
 - Drill down into details tabs
 - Look for trends and anomalies in data

The download installs an Excel 2013 reporting workbook which provides a comprehensive view of the email protection information that is also available in the **Reports** menu of the Office 365 admin center.

To download and install the workbook:

1. Navigate to **<http://go.microsoft.com/fwlink/?LinkId=524407>**.
2. Click **Download**.
3. Select the check box for the version you want to download.
4. Click **Next**.
5. Save the file to a location of your choice.
6. Browse to the location where you saved the MSI file and double-click it.
7. On the **Welcome** page, click **Next**.
8. Select the **I accept the terms in the License Agreement** check box, and click **Next**.
9. Select one of the following:
 - Microsoft Exchange Online
 - Microsoft Exchange Online Protection
10. Click **Next**.
11. On the **Prerequisites** page, click **Next**.
12. Click **Install**.
13. Click **OK**.
14. Click **Finish**.

To use the Mail Protection Reports workbook for Office 365:

1. On the desktop, double-click the **Mail Protection Reports for Office 365** shortcut.
2. On the Microsoft Office Customization Installer page, click **Install**.
3. Select one of the worksheet tabs in the workbook and click the **Query** button in the worksheet.
4. Enter your Office 365 credentials and click **Login**.
5. In the **Query** dialog box, select a time interval and click **OK**.
6. On the **Progress** page, when it completes, click **OK**.

The workbook contains summary graphs for various types of email message filtering and includes information about messages that have been identified as either good mail, spam, or malware. It also displays graphs for messages that were identified by either a transport rule or Data Loss Prevention (DLP) policy.

You can also employ data slicers in Excel 2013 to perform deeper analysis of the data. If you notice specific trends or unusual activities in the data, you can drill down further into the report by running queries on the other detailed tabs in the workbook and viewing more detailed information about the messages themselves.

Exchange Online Protection Reports

Microsoft Exchange Online Protection (EOP) is a cloud-based email filtering service that can help safeguard your company from spam and malware. EOP includes features to protect your company from messaging-policy abuse.

EOP can be used for messaging protection in the following situations:

- *In a stand-alone scenario.* EOP provides cloud-based email protection for your on-premises Microsoft Exchange Server 2013 environment, legacy Exchange Server versions, or for any other on-premises SMTP email solution.
- *As a part of Microsoft Exchange Online.* By default, EOP protects Microsoft Exchange Online cloud-hosted mailboxes.
- *In a hybrid deployment.* EOP can be configured to protect your messaging environment and control mail routing when you have a mix of on-premises and cloud mailboxes.

- EOP auditing reports help organizations meet regulatory, compliance and litigation requirements
- EOP auditing reports are the same as Office 365
- Exchange admin center>Compliance management>Auditing
 - Non-owner mailbox access report
 - Administrator role group report
 - In-Place eDiscovery & Hold report
 - Per-mailbox litigation hold report
- Enable mailbox audit logging

EOP auditing reports can help your organization meet regulatory, compliance, and litigation requirements by determining what changes have been made to the configuration of EOP. Auditing reports can help you troubleshoot issues with configuration and determine the cause of security-related or compliance-related problems.

The four auditing reports available in the Exchange admin center are the same as the four auditing reports discussed earlier in the Office 365 admin center, but with slightly different names in the user interface.

To access the Exchange Online Protection auditing reports:

1. In the Office 365 admin center, click **Admin**, then click **Exchange**.
2. In the left menu, click **Compliance management**.
3. On the Compliance management page, click **Auditing**.
4. Select one of the following reports:
 - **Non-owner mailbox access report**
 - **Administrator role group report**
 - **In-Place eDiscovery and Hold report**

- **Per-mailbox litigation hold report**

From the auditing section you can also export mailbox audit logs, view and export the administrator audit log, and view the datacenter admin log.



For more information on running Exchange Online Protection reports, go to:

<http://go.microsoft.com/fwlink/?LinkId=391795>

Enable Mailbox Audit Logging

You have to enable mailbox audit logging for each mailbox that you want to run a Non-owner Mailbox Access report for. If mailbox audit logging is not enabled for a mailbox, you will not receive any results when you run a report for it or export the mailbox audit log.

To enable mailbox audit logging for a single user's mailbox:

1. Open Windows PowerShell.
2. At the prompt, type the following command and press Enter:

```
Set-Mailbox user@domainname.com -AuditEnabled $true
```

To enable mailbox audit logging for all users' mailboxes:

1. Open Windows PowerShell.
2. At the prompt, type the following command and press Enter:

```
$UserMailboxes = Get-mailbox -Filter {(RecipientTypeDetails -eq 'UserMailbox')}
```

3. At the prompt, type the following command and press Enter:

```
$UserMailboxes | ForEach {Set-Mailbox $_.Identity -AuditEnabled $true}
```

Windows PowerShell Reporting in Exchange Online

There are several Windows PowerShell cmdlets that you can use for reporting purposes in Exchange Online.

Auditing Cmdlets

You can use the following Windows PowerShell cmdlets to configure audit logging, and to view the audit logs:

- Auditing cmdlets
 - Get-AdminAuditLogConfig
 - New-MailboxAuditLogSearch
- Message tracking cmdlets
 - Get-MessageTrackingReport
 - Search-MessageTrackingReport
- General reporting cmdlets
 - Get-LogonStatistics
 - Get-MailboxStatistics

Cmdlet	Purpose
Search-AdminAuditLog	Search the contents of the administrator audit log.
Write-AdminAuditLog	Add comments to the administrator audit log.

Cmdlet	Purpose
Get-AdminAuditLogConfig	View configuration settings for the current administrator audit logging.
New-AdminAuditLogSearch	Search the contents of the administrator audit log and send the results to the recipients you specify.
Get-MailboxAuditBypassAssociation	View the accounts that bypass mailbox audit logging.
Set-MailboxAuditBypassAssociation	Specify accounts that bypass mailbox audit logging. For example, you can specify service accounts that frequently access mailboxes to reduce the noise in mailbox audit logs.
Search-MailboxAuditLog	Search the contents of the mailbox audit log.
New-MailboxAuditLogSearch	Search the contents of the mailbox audit log and send the results to the recipients you specify.

Message Tracking Cmdlets

You can use the following Windows PowerShell cmdlets to track delivery information about messages sent by, or received from, any specific mailbox in your organization:

Cmdlet	Purpose
Get-MessageTrackingReport	Return the data for a specific message tracking report. This cmdlet requires you to specify the ID for the message tracking report you want to view. Therefore, first you need to use the Search-MessageTrackingReport cmdlet to find the message tracking report ID for a specific message. You then pass the message tracking report ID from the output of the Search-MessageTrackingReport cmdlet to the Get-MessageTrackingReport cmdlet.
Search-MessageTrackingReport	Find the unique message tracking report based on the search criteria provided. You can then pass this message tracking report ID to the Get-MessageTrackingReport cmdlet to get full message tracking information.

General Reporting Cmdlets

You can use the following Windows PowerShell cmdlets for general reporting in Exchange Online:

Cmdlet	Purpose
Get-FailedContentIndexDocuments	View the list of documents in a mailbox that couldn't be indexed by Exchange Search.
Get-LogonStatistics	View information about open logon sessions to a specified mailbox, such as user name, logon time, and last access time. A user must sign out to close a logon session; therefore, multiple sessions may appear for users who just close their browser.
Get-MailboxFolderStatistics	View information about the folders in a specified mailbox, including the number and size of items in the folder, the folder name and ID, and other information.

Cmdlet	Purpose
Get-MailboxStatistics	View information about a specified mailbox, such as the size of the mailbox, the number of messages it contains, and the last time that it was accessed.
Get-RecipientStatisticsReport	View information about the total number of recipients in your organization, including the number of mailboxes, active mailboxes, contacts, and distribution groups.

Lab: Monitoring Office 365 (Optional)

Scenario

The deployment of Office 365 at Lucerne Publishing is now complete, and single sign-on is federating the Lucerne Publishing domain with Office 365. As the team enters the final phase of this project, Heidi recruits Elizabeth to assist her in setting up a suitable monitoring environment to keep track of the status of Office 365 and ensure that the helpdesk and IT management can respond to any reported issues.

Objectives

By the end of this lab, you should be able to:

- Identify and fix networking issues that affect Office 365 access.
- Track message delivery in Exchange Online.
- Monitor service health and analyze reports.

Lab Setup

Estimated Time: 30 minutes

Virtual machine: 20346C-LUC-CL1

Username: **Student1**

Password: **Pa\$\$w0rd**

In all tasks, where you see references to `lucernepublishingXXXX.onmicrosoft.com`, replace the `XXXX` with the unique Lucerne Publishing number that you were assigned when you set up your Office 365 account in Module 1, Lab 1B, Exercise 2, Task 3, Step 5.

Where you see references to `labXXXXXX.o365ready.com`, replace the `XXXXXX` with the unique `O365ready.com` number you were assigned when you registered your IP address at `www.o365ready.com` in Module 2, Lab 2B, Exercise 1, Task 2, Step 6.

Exercise 1: Track Message Delivery

Scenario

Heidi is informed that there have been problems with non-delivery of messages to some key customers. Justin has asked her to identify what the problems are and find out why delivery is not happening to those addresses.

The main tasks for this exercise are as follows:

1. Send Mail to a Non-Existent Domain
2. Track Mail Delivery
3. Send Mail to a Non-Existent User
4. Track Mail Delivery
5. Analyze Mail Flow

► Task 1: Send Mail to a Non-Existent Domain

1. On **LUC-CL1**, on the Taskbar, click **Internet Explorer**.
2. Browse to **<http://mail.office365.com/>** and log on as **`hleitner@labXXXXXX.o365ready.com`** (where `XXXXXX` is your unique `O365ready.com` number), then press TAB.

3. In the **Sign In** page, enter a user name of **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number) and a Password of **Pa\$\$w0rd**, then click **Sign In**.
4. Click **Outlook** and click **new mail**.
5. In the **To** field, enter **user@alt.none**.
6. Enter a subject and some body text.
7. Click **SEND**.

► **Task 2: Track Mail Delivery**

1. Wait for the delivery failure message to appear.
2. Note the reason for the failure (**NonExistentDomain**).
3. Select the body text of the message from the phrase "**Generating server**" down to **X-OriginatorOrg: labXXXXX.o365ready.com** and press Ctrl+C to copy it to the clipboard.
4. On Internet Explorer, press **Ctrl+T** to create a new tab.
5. In the new tab, browse to testconnectivity.microsoft.com.
6. In the **Microsoft Remote Connectivity Analyzer** page, click the **Message Analyzer** tab.
7. Under **Message Header Analyzer**, paste in the message and click **Analyze headers**.
8. Note the diagnostic information and the time taken for the message to be rejected (typically around seven seconds).
9. Click **Clear** to reset the Message Header Analyzer.

► **Task 3: Send Mail to a Non-Existent User**

1. In Internet Explorer, click on **Heidi Leitner's** tab.
2. Click **New mail**, and in the **To** field, enter **difflop4890@outlook.com**.
3. Enter a subject and some body text.
4. Click **SEND**.

► **Task 4: Track Mail Delivery**

1. Wait for the delivery failure message to appear.
2. Note the reason for the failure: **550 Requested action not taken: mailbox unavailable**.
3. Select the body text of the message from the phrase "**Generating server**" down to **X-OriginatorOrg: labXXXXX.o365ready.com** and press **Ctrl+C** to copy it to the clipboard.
4. In Internet Explorer, switch to the **Microsoft Remote Connectivity Analyzer** tab.
5. In the **Microsoft Remote Connectivity Analyzer** page, ensure that you are on the **Message Analyzer** tab.
6. Under **Message Header Analyzer**, paste in the message and click **Analyze headers**.
7. Note the diagnostic information and the time taken for the message to be rejected (typically around zero seconds).
8. Press **Ctrl-F4** to close the Message Header Analyzer tab.

► **Task 5: Analyze Mail Flow**

1. In **Heidi Leitner's** tab, click the **Apps** menu, click **Admin**, and then click **Exchange**.

2. Click **Mail flow**.
3. In **Mail flow**, click **Message trace**.
4. In **Message trace**, next to **Sender**, click **Add sender**.
5. In the **Select Members** dialog box, click **Heidi Leitner**, and click **add**, then click **OK**.
6. Under **Date range**, select **Past 24 hours**.
7. Under **Delivery status**, select **Failed**, then click **Search**. Note the two messages.
8. Double-click each message to view the sender, recipient, message size, ID and IP address information.
9. Note the differences between the message processing events (RECEIVE, SUBMIT, RECEIVE, FAIL for the non-existent domain, RECEIVE, RECEIVE, SUBMIT, FAIL for the non-existent user).
10. Close the Message Trace window.

Results: Lucerne Publishing can identify reasons for non-delivery of email by use of mail header analysis.

Exercise 2: Monitor Service Health and Analyze Reports

Scenario

Justin has identified the management reports that he needs to provide to Remi Desforges and Jesse Wagner. Of particular interest to Remi are the number of malware and spam items that are reaching the organization. Again, Justin turns to Heidi to lead this project. She begins by familiarizing herself with the reporting tools in Office 365. Her next task is to produce reports on the numbers of messages that Exchange Online Protection is intercepting.

The main tasks for this exercise are as follows:

1. View Office 365 Service Health
2. View Reports in the Office 365 Admin Center
3. Install Mail Protection Reports for Office 365
4. Use Mail Protection Reports for Office 365

► Task 1: View Office 365 Service Health

1. In the **Office 365 admin center** logged on as **Heidi Leitner**, click the **Apps** menu, click **Admin**, and then click **Office 365**.
2. In the **Office 365 admin center Dashboard** page, in the left menu, click **Service health**.
3. Click **View details and history**.
4. At the top-right of the table, click **View history for past 30 days**.
5. Click any entry in the **INCIDENT ID** column to see further details.
6. Click the back arrow.
7. On the **Service health** page, click **Planned Maintenance**.
8. Note any planned maintenance events (there may be none).

► Task 2: View Reports in the Office 365 Admin Center

1. In the **Office 365 admin center**, on the left-hand side, click **Reports**.

2. In the **Reports** page, in the **Mail** section, click **Mailbox usage**.
Note: There may be little or no data shown since there has not been a lot of mailbox usage in the lab environment.
3. Click the back arrow.
4. In the **Reports** page, in the **Protection** section, click **Sent and received mail**.
5. Click **View table**.
6. Close the table view.
Note: There may be little or no data shown since there has not been a lot of mailbox usage in the lab environment.
7. Close the open window.
8. In the **Reports** page, in the **Protection** section, click **Malware detections**.
Note: You should see malware detections resulting from Lab 7.
9. Close the open window.
10. In the **Reports** page, in the **Protection** section, click **Spam detections**.
Note: You should see spam detections resulting from Lab 7.
11. Close the open window.

► **Task 3: Install Mail Protection Reports for Office 365**

1. In the **Office 365 admin center**, on the **Reports Overview** page, under **Download your reports**, click **Mail protection reports (Excel)**.
2. On the **Microsoft Download Center** page, click **Download**.
3. On the **Choose the download you want** page, select the check box for **MailProtectionReport_v2_en32.msi**, and then click **Next**.
4. In the Internet Explorer notification bar, click **Allow once**.
5. In the Internet Explorer notification bar, click **Run**.
6. In the **Mail Protection Reports for Office 365 Setup** dialog box, on the **Welcome to the Mail Protection Reports for Office 365 Setup Wizard** page, click **Next**.
7. On the **End-User License Agreement** page, select the **I accept the terms in the License Agreement** check box, and click **Next**.
8. On the **Service Selection** page, click **Next**.
9. On the **Prerequisites Required** page, click **Next**.
10. On the **Ready to install Mail Protection Reports for Office 365** page, click **Install**.
11. In the **User Account Control** dialog box, click **Yes**.
12. On the **Completed the Mail Protection Reports for Office 365 Setup Wizard** page, click **Finish**.

► **Task 4: Use Mail Protection Reports for Office 365**

1. Minimize Internet Explorer.
2. On the desktop, double-click **Mail Protection Reports for Office 365**.

3. If you get an error message, click **OK**, and double-click **Mail Protection Reports for Office 365** again.
4. In the **Microsoft Office Customization Installer** dialog box, click **Install**.
5. If you get a **First things first** page, click **Accept**.
6. In the **Email traffic** page, click **Query**.
7. In the **Sign into Office 365** page, enter **hleitner@labXXXXX.o365ready.com** (where XXXXX is your unique O365ready.com number) and a password of **Pa\$\$w0rd**, then click **Login**.
8. In the **Query** dialog box, click **OK**.
9. In the **Progress** dialog box, click **OK**.
10. In **Microsoft Excel**, note the data shown on the **Traffic** worksheet.
11. Click the **Spam** worksheet and note the detail on Spam traffic.
12. Click the **Malware** worksheet and note the detail on Malware traffic.

Results: Lucerne Publishing has used the reporting functions in Office 365 to monitor service health and identify levels of malware and spam in email traffic.

Lab Review Discussion Questions

How would you view all the failed messages for a group of users?

Use the Exchange Online admin center, signed in as an administrator, and then select mail flow, and message trace, and then choose Select Members.

What is the main prerequisite for using Mail Protection Reports for Office 365?

Mail Protection Reports for Office 365 requires Microsoft Excel.

- How would you view all the failed messages for a group of users?
- What is the main prerequisite for using Mail Protection Reports for Office 365?

Module Review and Takeaways

Now that you have completed this module, you can isolate service interruptions, track message delivery, monitor service health, and analyze reports in Office 365.



Best Practice: There is a wide range of tools available to help troubleshoot issues in Office 365; as a starting point, the Office 365 Troubleshooter can help with initial diagnosis.

Course Evaluation

Your evaluation of this course will help Microsoft understand the quality of your learning experience.

Please work with your training provider to access the course evaluation form.

Microsoft will keep your answers to this survey private and confidential and will use your responses to improve your future learning experience. Your open and honest feedback is valuable and appreciated.

MCT USE ONLY. STUDENT USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED

Notes

MCT USE ONLY. STUDENT USE PROHIBITED

Notes