



Managing Office 365 Identities and Requirements

SECOND EDITION

Exam Ref

70-346

Orin Thomas

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



Managing Office 365 Identities and Requirements Second Edition

Orin Thomas

Exam Ref 70-346 Managing Office 365 Identities and Requirements, Second Edition

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

Copyright © 2018 by Orin Thomas

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

ISBN-13: 978-1-5093-0479-0

ISBN-10: 1-5093-0479-7

Library of Congress Control Number: 2017949563

First Printing August 2017

Trademarks

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

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The authors, the publisher, and Microsoft Corporation shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or programs accompanying it.

Special Sales

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

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Editor-in-Chief	Greg Wiegand
Senior Acquisitions Editor	Laura Norman
Development Editor	Troy Mott
Managing Editor	Sandra Schroeder
Senior Project Editor	Tracey Croom
Editorial Production	Backstop Media
Copy Editor	Christina Rudloff
Indexer	Julie Grady
Proofreader	Christina Rudloff
Technical Editor	Tim Warner
Cover Designer	Twist Creative, Seattle

Contents at a glance

	<i>Introduction</i>	<i>xi</i>
	<i>Preparing for the exam</i>	<i>xv</i>
CHAPTER 1	Provision Office 365	1
CHAPTER 2	Plan and implement networking and security in Office 365	29
CHAPTER 3	Manage cloud identities	63
CHAPTER 4	Implement and manage identities by using Azure AD Connect	97
CHAPTER 5	Implement and manage federated identities single sign on	137
CHAPTER 6	Monitor and troubleshoot Office 365 availability and usage	193
	<i>Index</i>	<i>235</i>

This page intentionally left blank

Contents

Introduction	xi
Organization of this book	.xi
Microsoft certifications	xii
Acknowledgments	xii
Free ebooks from Microsoft Press	xii
Microsoft Virtual Academy	.xiii
Quick access to online references	.xiii
Errata, updates, & book support	.xiii
We want to hear from you	.xiv
Stay in touch	.xiv
<i>Preparing for the exam</i>	xv

Chapter 1 Provision Office 365	1
Skill 1.1: Provision tenants	1
Configure the tenant name	2
Tenant region	2
Administrator roles	3
Manage tenant subscriptions and licenses	5
Configure tenant for new features and updates	8
Skill 1.2: Add and configure custom domains	9
Specify domain name	9
Confirm ownership	10
Specify domain purpose	12

Move ownership of DNS to Office 365	15
Update and verify domain settings	16
Skill 1.3: Plan a pilot	16
Designate pilot users	17
Identify workloads that don't require migration	18
Run the Office 365 Health, Readiness, and Connectivity checks	18
The IdFix tool	20
Create a test plan or use case	21
Connect existing email accounts for pilot users	21
Service descriptions	23
FastTrack for Office 365	25
Thought experiment	25
Thought experiment answers	26
Chapter summary	26

Chapter 2 Plan and Implement Networking and Security in Office 365 **29**

Skill 2.1: Configure DNS records for services	29
Exchange DNS records	30
Skype for Business Online DNS records	34
SharePoint Online DNS records	38
Update and verify DNS records for Office 365 settings	38
Skill 2.2: Enable client connectivity to Office 365	39
Proxy server configuration	39
Outbound firewall ports	40
Recommend bandwidth	41
Internet connectivity for clients	41
Deploy desktop setup for previous versions of Office clients	42
Skill 2.3: Administer Microsoft Azure Rights Management	42
Azure Information Protection	43
Activate Azure Rights Management and Azure Information Protection	43
Office integration with Rights Management	46

Assign roles for Microsoft Azure Active Directory RM	48
Enable recovery of protected document	49
Configure rights management email templates	49
Managing Azure Rights Management using PowerShell	53
Skill 2.4: Manage administrator roles in Office 365	54
Global administrator	54
Billing administrator	55
User management administrator	55
Service administrator	56
Password administrator	56
Delegated administrator	56
Exchange Online administrator	57
Skype for Business administrator	57
SharePoint Online administrator	58
Manage role membership	58
Thought experiment	60
Thought experiment answers	61
Chapter summary	61

Chapter 3 Manage cloud identities 63

Skill 3.1: Configure password management	63
Working with cloud identities	64
Configuring password policies	64
Following password complexity policies	65
Resetting passwords	66
Skill 3.2: Manage user and security groups	71
Using the bulk import process	71
Using soft delete	73
Enabling multi-factor authentication	75
Skill 3.3: Manage cloud identities with Windows PowerShell	79
Managing user passwords with Windows PowerShell	80
Hard deleting users	82
Performing bulk account operations	83
Using Azure Active Directory cmdlets	85

Thought experiment.	92
Thought experiment answers	93
Chapter summary	94

Chapter 4 Implement and manage identities by using Azure AD Connect 97

Skill 4.1: Prepare on-premises Active Directory for Azure AD Connect	97
Cleaning up existing Active Directory objects	99
Using UPN suffixes and non-routable domains	102
Planning for filtering Active Directory	105
Supporting multiple forests	108
Azure AD Connect Sign-on options	109
Skill 4.2: Set up Azure AD Connect	110
Meeting the Azure AD Connect installation requirements	111
Installing Azure AD Connect	116
Identifying synchronized attributes	125
Syncing Passwords	127
Skill 4.3: Manage Active Directory users and groups with Azure AD Connect in place	128
Create users and groups	128
Modifying users and groups	129
Deleting users and groups	129
Managing synchronization	130
Forcing synchronization	131
Thought experiment.	134
Thought experiment answers	135
Chapter summary	135

Chapter 5 Implement and manage federated identities single sign on 137

Skill 5.1: Plan requirements for Active Directory Federation Services.	137
Deploying AD FS topologies	138
Using certificates	139
Using namespaces	149

Meeting network requirements	150
Configuring multi-factor authentication	150
Accessing filtering using claims rules	151
Skill 5.2: Install and manage AD FS Servers	152
Creating AD FS service accounts	153
Configuring farm or stand-alone settings	155
Installing and configuring AD FS	156
Adding additional servers	166
Converting from standard to federated domain	177
Managing certificate life cycle	178
Skill 5.3: Install and manage AD FS Proxy Servers.	179
Setting up perimeter network name resolution	180
Setting up certificates	180
Installing required Windows roles and features	181
Configuring AD FS Web Application Proxy	184
Setting custom proxy forms login page	189
Password synchronization as fallback	190
Thought experiment	190
Thought experiment answers	191
Chapter summary	191

Chapter 6 Monitor and troubleshoot Office 365 availability and usage 193

Skill 6.1: Analyze reports	193
Office 365 reports	194
Exchange reports	197
OneDrive	200
Skype for Business	202
SharePoint	204
Security and compliance reports	206
Skill 6.2: Monitor service health	208
Service Health dashboard	208
Office 365 Management Pack	211
Windows PowerShell cmdlets	222

Skill 6.3: Isolate service interruption	223
Microsoft Remote Connectivity Analyzer	224
Microsoft Connectivity Analyzer	228
Transport Reliability IP Probe	229
Hybrid Free Busy Troubleshooter	230
Support and Recovery Assistant for Office 365	231
Thought experiment.	233
Thought experiment answers	233
Chapter summary	234
<i>Index</i>	235

Introduction

The 70-346 exam deals with advanced topics that require candidates to have an excellent working knowledge of both Office 365 and Windows Server. Some of the exam comprises topics that even experienced Office 365 and Windows Server administrators may rarely encounter unless they are consultants who deploy new Office 365 tenancies on a regular basis. To be successful in taking this exam, candidates not only need to understand how to deploy and manage Office 365, they need to understand how to integrate Office 365 with an on-premises Active Directory environment. They also need to keep up to date with new developments with Office 365, including new features and changes to the interface.

Candidates for this exam are Information Technology (IT) Professionals who want to validate their advanced Office 365 and Windows Server management skills, configuration skills, and knowledge. To pass this exam, candidates require a strong understanding of how to provision Office 365, plan and implement networking and security in Office 365, manage cloud identities, configure and manage identity synchronization between on-premises and cloud Active Directory instances, implement and manage federated identities as well as have the ability to monitor and troubleshoot Office 365 availability and usage. To pass, candidates require a thorough theoretical understanding as well as meaningful practical experience implementing the technologies involved.

This edition of this book covers Office 365 and the 70-346 exam objectives circa mid-2017. As Office 365 evolves, so do the Office 365 exam objectives, so you should check carefully if any changes have occurred since this edition of the book was authored and study accordingly.

This book covers every exam objective as of mid-2017, but it does not cover every exam question. Only the Microsoft exam team has access to the exam questions themselves and Microsoft regularly adds new questions to the exam, making it impossible to cover specific questions. You should consider this book a supplement to your relevant real-world experience and other study materials. If you encounter a topic in this book that you do not feel completely comfortable with, use the links you'll find in text to find more information and take the time to research and study the topic. Great information is available on TechNet, through MVA courses, and in blogs and forums.

Microsoft certifications

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

MORE INFO ALL MICROSOFT CERTIFICATIONS

For information about Microsoft certifications, including a full list of available certifications, go to <http://www.microsoft.com/learning/en/us/certification/cert-default.aspx>.

Free ebooks from Microsoft Press

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

<https://aka.ms/mspressfree>

Check back often to see what is new!

Errata, updates, & book support

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

<https://aka.ms/examref3462E/errata>

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

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

To download a list of all URLs mentioned in this book go to: <https://aka.ms/examref3462E/downloads>

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

We want to hear from you

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

<https://aka.ms/tellpress>

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

Stay in touch

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

This page intentionally left blank

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

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

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

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

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

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

This page intentionally left blank

Implement and manage identities by using Azure AD Connect

A substantial number of organizations integrate their on-premises Active Directory Domain Services deployment with the Azure Active Directory instance that supports their Office 365 tenancy. Unlike a cloud-only deployment, where all of the user, group, and contact accounts are stored and managed in Azure Active Directory, integration allows users, groups, and contacts created on-premises to synchronize up to Office 365. Integration can occur through synchronization, which is the subject of this chapter, or through federation, the subject of Chapter 5, “Implement and manage federated identities.”

Skills in this chapter

- Skill 4.1: Prepare on-premises Active Directory for Azure AD Connect

Skill 4.1: Prepare on-premises Active Directory for Azure AD Connect

This skill deals with preparing your on-premises Active Directory environment for synchronization of user accounts, group accounts, and mail-enabled contacts to the Azure Active Directory instance that supports the Office 365 tenancy. To master this skill, you'll need to understand the different Active Directory synchronization tools, the steps needed to prepare an on-premises Active Directory instance for Azure AD Connect, what to do if your on-premises Active Directory uses a non-routable domain name, what to think about when it comes to planning filtering of user account objects for synchronization, and what to do if you have a multiple forest environment.

This section covers the following topics:

- Active Directory synchronization tools
- Cleaning up existing Active Directory objects
- UPN suffixes and non-routable domain names
- Plan for filtering Active Directory
- Support for multiple forests

Azure Active Directory Connect

Azure Active Directory Connect is Microsoft's replacement for DirSync and Azure Active Directory Sync tools. Azure AD Connect is designed to streamline the process of configuring connections between on-premises deployment. Rather than perform some of the complex tasks outlined in this chapter and the next, the Azure Active Directory Connect tool is designed to make the process of configuring synchronization between an on-premises Active Directory deployment and Azure Active Directory as frictionless as possible.

Azure Active Directory Connect can automatically configure and install simple password synchronization or Federation / Single Sign-on, depending on your organizational needs. When you choose the Federation with AD FS option, Active Directory Federation Services is installed and configured, as well as a Web Application Proxy server to facilitate communication between the on-premises AD FS deployment and Microsoft Azure Active Directory.

The Azure Active Directory Connect tool supports the following optional features, as shown in Figure 4-1:

- **Exchange hybrid deployment** This option is suitable for organizations that have an Office 365 deployment where there are mailboxes hosted both on-premises and in the cloud.
- **Exchange mail public folders** This feature allows organizations to synchronize mail-enabled public folder objects from an on-premises Active Directory environment to Office 365.
- **Azure AD app and attribute filtering** Selecting this option gives you the ability to be more selective about which attributes are synchronized between the on-premises environment and Azure AD.
- **Password synchronization** Synchronizes a hash of the user's on-premises password Azure AD. When the user authenticates to Azure AD, the submitted password is hashed using the same process and if the hashes match, the user is authenticated. Each time the user updates their password on-premises, the updated password hash synchronizes to Azure AD.
- **Password writeback** Password writeback allows users to change their passwords in the cloud and have the changed password written back to the on-premises Active Directory instance.

- **Group writeback** Changes made to groups in Azure AD are written back to the on-premises AD instance.
- **Device writeback** Information about devices registered by the user in Azure AD is written back to the on-premises AD instance.
- **Directory extension attribute sync** Allows you to extend Azure AD schema based on extensions made to your organization's on-premises Active Directory instance.

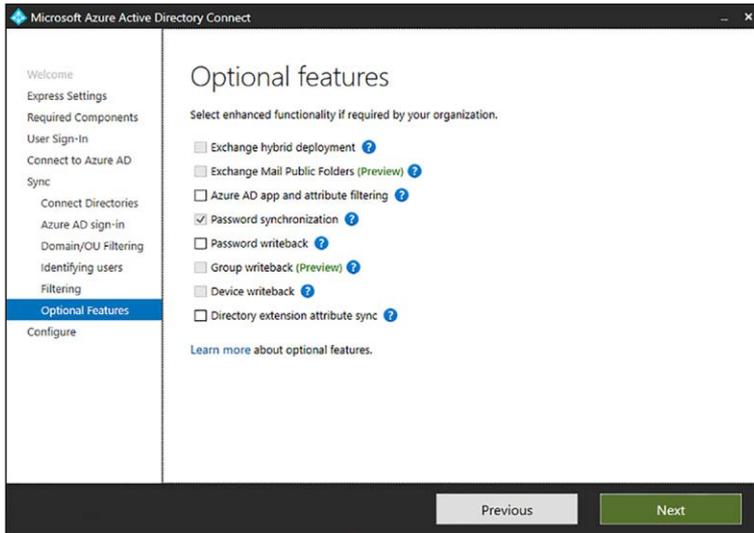


FIGURE 4-1 Azure Active Directory Connect optional features

MORE INFO AZURE ACTIVE DIRECTORY CONNECT

You can learn more about Azure Active Directory Connect at <https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect>.

Cleaning up existing Active Directory objects

Before you deploy Azure AD Connect, it is prudent to ensure that your on-premises Active Directory environment is healthy. You should also have an excellent understanding of the current state of the Active Directory environment. This should include performing an audit to determine the following:

- Do any Active Directory objects use invalid characters?
- Do any Active Directory objects have incorrect Universal Principal Names (UPNs)?
- What are the current domain and forest functional levels?
- Are any schema extensions or custom attributes in use?

Prior to deploying Azure AD Connect, you should ensure that you have performed the following tasks:

- Remove any duplicate proxyAddress attributes
- Remove any duplicate userPrincipalName attributes
- Ensure that blank or invalid userPrincipalName attribute settings have been altered so that the setting contains only a valid UPN
- Ensure that for user accounts that the cn and samAccountName attributes have been assigned values
- Ensure that for group accounts, the member, alias, and displayName (for groups with a valid mail or proxyAddress attribute) are populated
- Ensure that the following attributes do not contain invalid characters:
 - givenName
 - sn
 - samAccountName
 - givenName
 - displayName
 - mail
 - proxyAddress
 - mailNickName

UPNs that are used with Office 365 can only contain the following characters:

- Letters
- Numbers
- Periods
- Dashes
- Underscores

Rather than having to perform this operation manually, Microsoft provides some tools that allow you to automatically remediate problems that might exist with attributes prior to deploying Azure AD Connect.

IdFix

The IdFix tool, which you can download from Microsoft's website, allows you to scan an Active Directory instance to determine if any user accounts, group accounts, or contacts have problems that will cause them not to synchronize between the on-premises instance of Active Directory and the Office 365 instance of Azure Active Directory. IdFix can also perform repairs on objects that would otherwise be unable to sync. IdFix runs with the security context of the currently signed on user. This means that if you want to use IdFix to repair objects in the forest that have problems, the security account you use to run IdFix must have permissions

to modify those objects. The IdFix tool is shown in Figure 4-2 displaying an account detected with an incorrectly configured userPrincipalName.

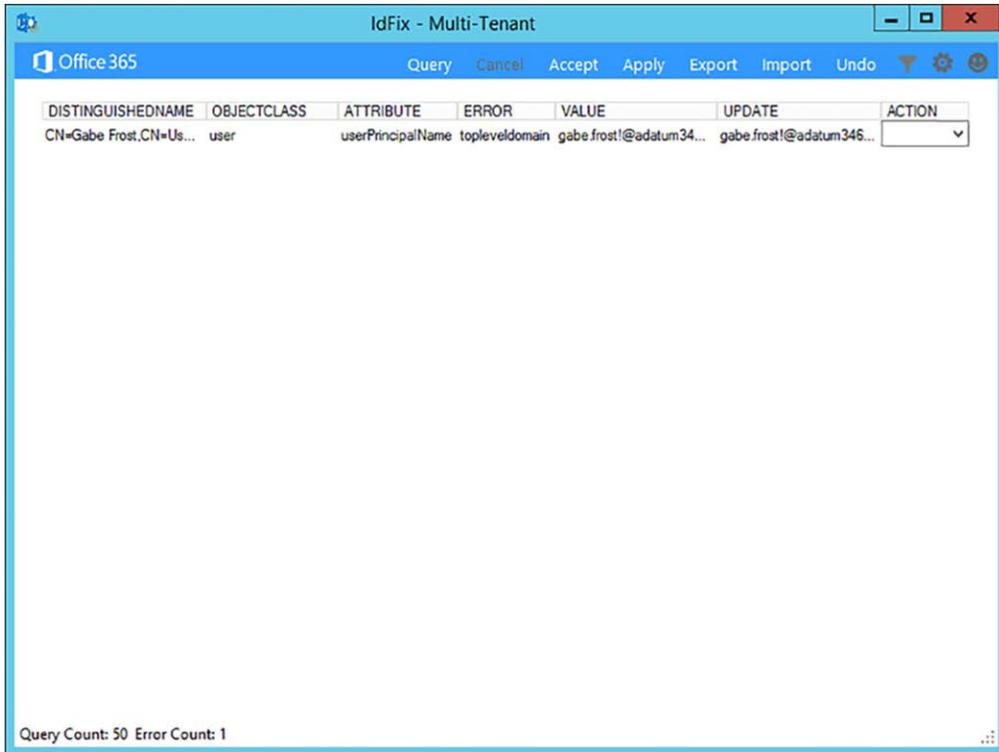


FIGURE 4-2 IdFix finds user with a problematic UPN.

MORE INFO IDFIX

You can download IdFix at the following address <http://www.microsoft.com/en-us/download/details.aspx?id=36832>.

ADModify.NET

ADmodify.NET is a tool that allows you to make changes to specific attributes for multiple objects. If you are using ADSIEdit or the Advanced mode of the Active Directory Users and Computers console, you are only able to modify the attribute of one object at a time. For example, Figure 4-3 shows ADModify.NET used to modify the format of the userPrincipalName attribute for a number of user accounts so that it conforms to a specific format.

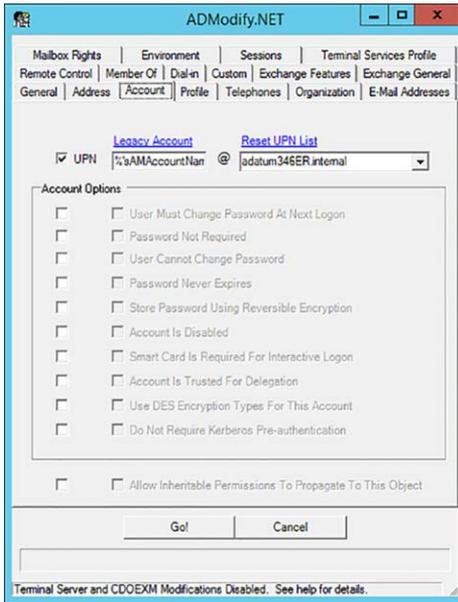


FIGURE 4-3 ADModify.NET

You can also use ADModify.NET to perform other systems administration tasks, such as configuring a large number of accounts, so that the users have to change their password at next logon or to disable multiple accounts.

MORE INFO ADMODIFY.NET

You can learn more about ADModify.NET at [https://technet.microsoft.com/en-us/library/aa996216\(v=EXCHG.65\).aspx](https://technet.microsoft.com/en-us/library/aa996216(v=EXCHG.65).aspx).

Using UPN suffixes and non-routable domains

Prior to performing synchronization between an on-premises Active Directory environment and an Azure Active Directory instance used to support an Office 365 tenancy, you must ensure that all user account objects in the on-premises Active Directory environment are configured with a value for the UPN suffix that is able to function for both the on-premises environment and Office 365.

This is not a problem when an organization's internal Active Directory domain suffix is a publicly routable domain. For example, a domain name, such as contoso.com or adatum.com that is resolvable by public DNS servers will suffice. Things become more complicated when the organization's internal active directory domain suffix is not publicly routable. For example, Figure 4-4 shows the adatum346ER.internal non-routable domain.

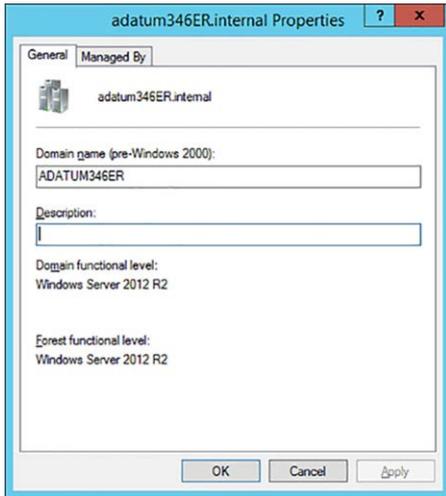


FIGURE 4-4 Non routable domain

If a domain is non-routable, the default routing domain—for example, `adatum346ER.onmicrosoft.com`—should be used for the Office 365 UPN suffix. This requires modifying the UPN suffix of accounts stored in the on-premises Active Directory instance. Modification of UPN after initial synchronization has occurred is not supported. This means that you need to ensure that on-premises Active Directory UPNs are properly configured prior to performing initial synchronization using Azure AD Connect.

To add a UPN suffix to the on-premises Active Directory in the event that the Active Directory domain uses a non-routable namespace, perform the following steps:

1. Open the Active Directory Domains And Trust console and select Active Directory Domains And Trusts.
2. On the Action menu, click Properties.
3. On the UPN Suffixes tab, enter the UPN suffix to be used with Office 365. Figure 4-5 shows the UPN suffix of `adatum346ER.onmicrosoft.com`.

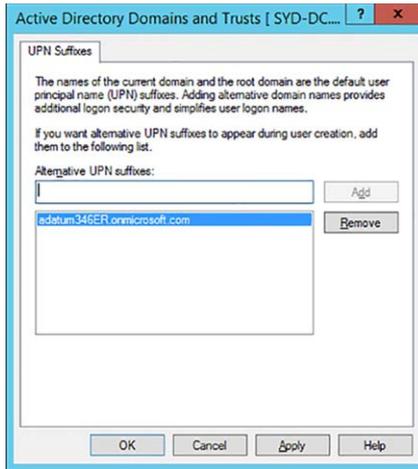


FIGURE 4-5 Non routable domain

- Once the UPN suffix has been added in Active Directory Domains And Trusts, you can assign the UPN suffix to user accounts. You can do this manually as shown in Figure 4-6 by using the Account tab of the user’s properties dialog box in Active Directory Users And Computers.

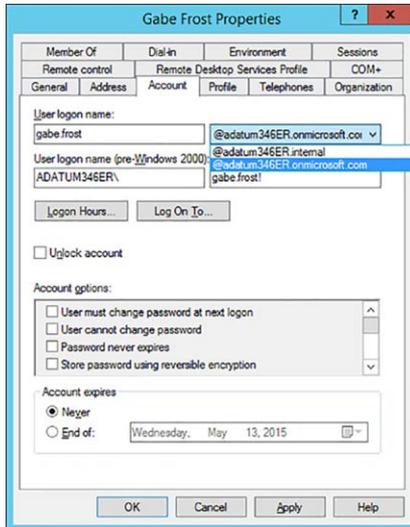


FIGURE 4-6 Configure UPN

- You can use tools like ADModify.NET to reset the UPNs of multiple accounts as shown in Figure 4-7.

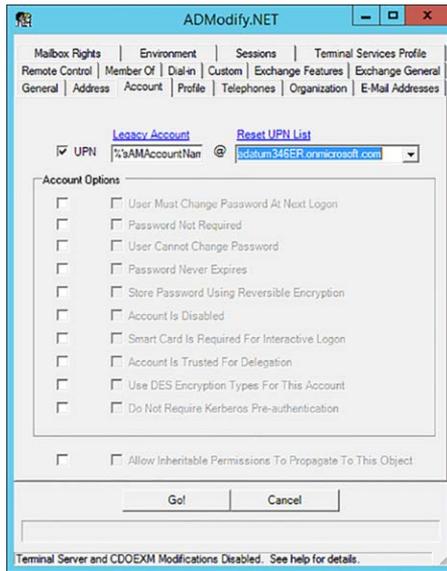


FIGURE 4-7 ADModify.NET

6. You can also use Microsoft PowerShell scripts to reset the UPNs of multiple user accounts. For example, the following script resets UPN suffixes of all user accounts in the adatum346ER.internal domain to adatum346ER.onmicrosoft.com.

```
Get-ADUser -Filter {UserPrincipalName -like "*@adatum346ER.internal"} -SearchBase
"DC=adatum346ER,DC=internal" |
ForEach-Object {
$UPN =
$_.UserPrincipalName.Replace("adatum346.internal", "adatum346ER.onmicrosoft.com")
Set-ADUser $_ -UserPrincipalName $UPN
}
```

Planning for filtering Active Directory

When you use Azure AD Connect to synchronize on-premises Active Directory to an Azure Active Directory instance, the default setting is to have all user accounts, group accounts, and mail-enabled contact objects synchronized up to the cloud. For some organizations, synchronizing everything is exactly what they want. Other organizations want to be more selective about which objects are synchronized from the on-premises Active Directory environment to the Azure Active Directory instance that supports the Office 365 tenancy.

With Azure AD Connect, you can choose to filter based on the following options as shown in Figure 4-8:

- **Domain based** In a forest with multiple domains, you can configure filtering so that only objects from some domains, and not others, are filtered.

- **Organizational unit (OU) based** With this filtering type, you choose which objects are filtered based on their location within specific organizational units.

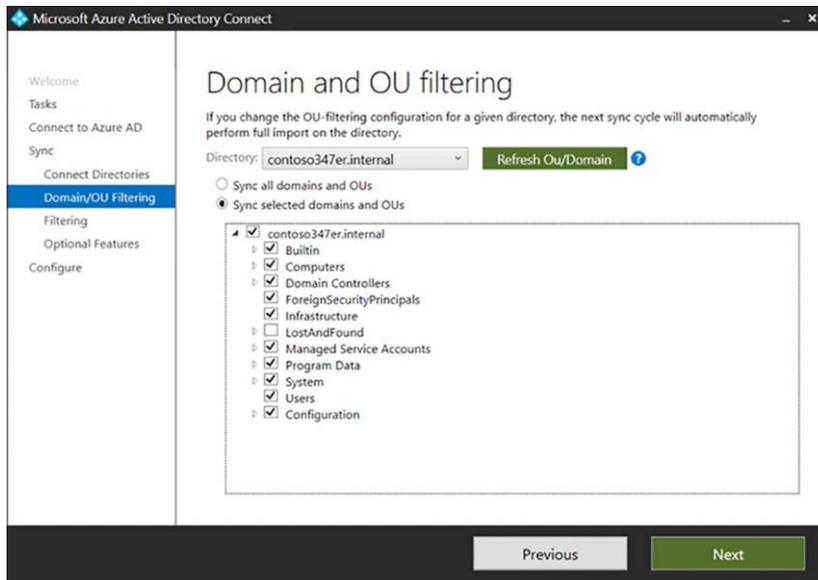


FIGURE 4-8 Domain and OU filtering

You can also configure filtering on the basis of group membership, as shown in Figure 4-9. You can configure separate group based filters for each forest or domain synchronized using Azure AD Connect.

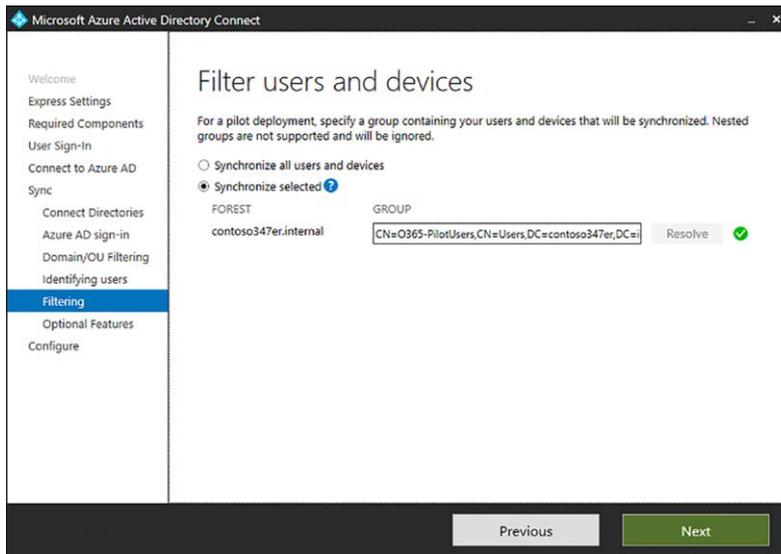


FIGURE 4-9 Filter Users And Devices

MORE INFO FILTERING

You can learn more about Azure AD Sync filtering at <https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnectsync-configure-filtering>.

While Azure AD Connect will address most organization's synchronization requirements, the most comprehensive tool that you can use to filter synchronization is the Synchronization Rules Editor, shown in Figure 4-10. You can use this tool to modify existing synchronization rules, but also to create new rules. Rather than configuring synchronization on a per-domain or per-OU basis, you can tailor rules for individual objects and specific Active Directory attributes.

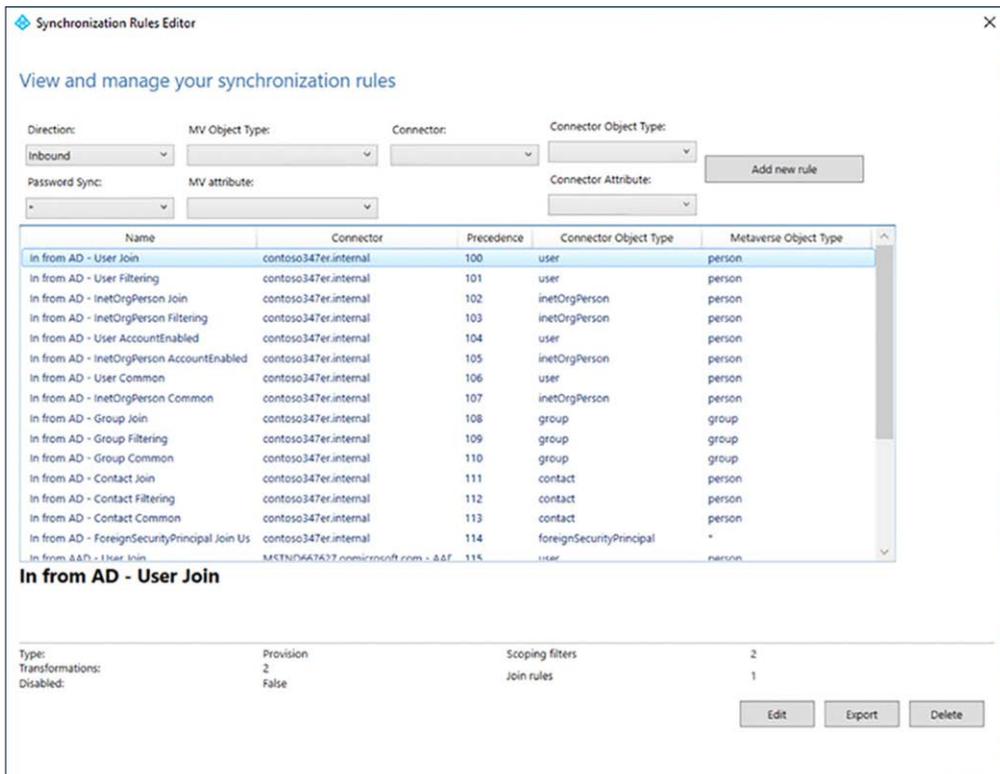


FIGURE 4-10 Synchronization Rules Editor

MORE INFO SYNCHRONIZATION RULES EDITOR

You can learn more about the Synchronization Rules Editor at: <https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnectsync-change-the-configuration>.

Supporting multiple forests

The Azure Active Directory Connect tool also supports synchronization from multiple on-premises Active Directory forests to a single Azure Active Directory instance. Multiple forest synchronization to a single Azure AD instance is supported only when a single Azure AD Connect server is in use. Microsoft does not support multiple Azure AD Connect servers synchronizing with a single Azure AD instance, whether there is one or multiple forests being synchronized.

By default, Azure AD Connect will assume that:

- A user has a single enabled account. Also, the forest where this account is located must host the directory that is used to authenticate the user. This assumption is used in both password sync and federation scenarios. On the basis of this assumption, the UserPrincipalName and sourceAnchor/immutableID are drawn from this forest.
- Each user has a single mailbox, and the forest that host that mailbox is the best source of attributes visible in the Exchange Global Address List (GAL). In the event that a user doesn't have an associated mailbox, any configured forest can function as the source for these attribute values.
- If a user account has a linked mailbox, there will be an account in an alternate forest used for the sign-in process.
- The key to synchronizing user accounts from multiple forests is that only one user account from all synchronized forests should represent the user. This means that the synchronization engine should have a way to determine when accounts in separate forests represent the same user. You can configure how the Azure AD Connect sync engine identifies users on the Uniquely Identifying Your Users page, shown in Figure 4-11 using one of the following options:

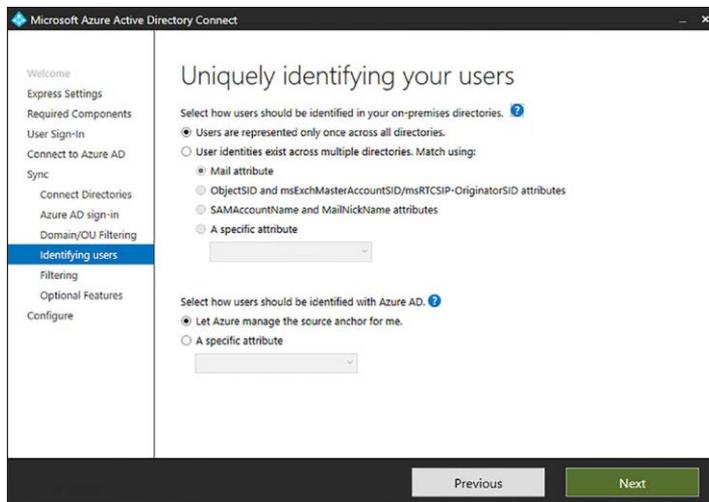


FIGURE 4-11 Uniquely identify users

- Match users using the mail attribute
- Match user using ObjectSID and msExchangeMasterAccountSID/msRTCIP-Originator-SID attributes
- Match user using SAMAccountName and MailNickName attributes
- Specify a custom attribute upon which to match names

MORE INFO MULTI-FOREST SYNCHRONIZATION

You can learn more about multi-forest synchronization at the following address:

<https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-topologies>.

Azure AD Connect Sign-on options

Azure AD Connect supports a variety of sign in options. You configure which one you want to use when setting up Azure AD Connect as shown in Figure 4-12. The default method, Password Synchronization, is appropriate for the majority of organizations who will use Azure AD Connect to synchronize identities to the cloud.

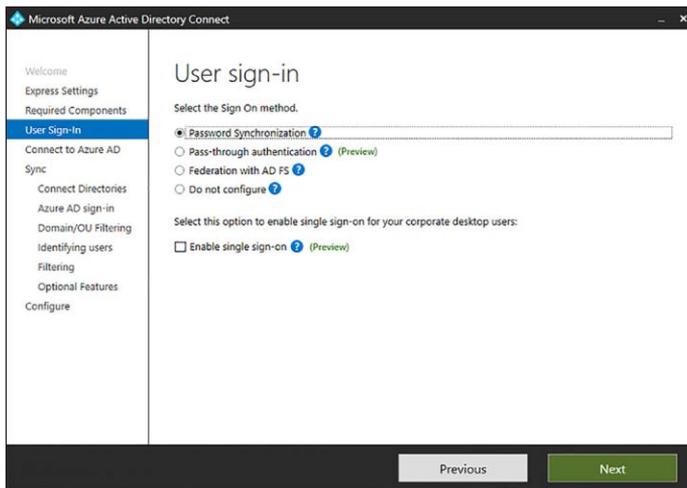


FIGURE 4-12 User sign-in

Password synchronization

Hashes of on-premises Active Directory user passwords synchronize to Azure AD and changed password synchronize to Azure AD immediately. Actual passwords are never sent to Azure AD and are not stored in Azure AD. Allows for single sign-on for users of computers that are joined to an Active Directory domain that synchronizes to Azure AD. Password synchronization also allows you to enable password write-back for self-service password reset functionality through Azure AD.

Pass-through authentication

When authenticating to Azure AD, the user's password is validated against an on-premises Active Directory domain controller. Passwords and password hashes are not present in Azure AD. Pass-through authentication allows for on-premises password policies to apply. Pass-through authentication requires that Azure AD Connect have an agent on a computer joined to the domain that hosts the Active Directory instance that contains the relevant user accounts. Pass-through authentication also allows single sign-on for users of domain joined machines.

With pass-through authentication, the user's password is validated against the on-premises Active Directory controller. The password doesn't need to be present in Azure AD in any form. This allows for on-premises policies, such as sign-in hour restrictions, to be evaluated during authentication to cloud services.

Pass-through authentication uses a simple agent on a Windows Server 2012 R2 domain-joined machine in the on-premises environment. This agent listens for password validation requests. It doesn't require any inbound ports to be open to the Internet.

In addition, you can also enable single sign-on for users on domain-joined machines that are on the corporate network. With single sign-on, enabled users only need to enter a username to help them securely access cloud resources.

Active Directory Federation

This allows users to authenticate to Azure AD resources using on-premises credentials. It also requires the deployment of an Active Directory Federation Services infrastructure. You will learn more about this in Chapter 5, "Implement and manage federated identities for single sign on."

MORE INFO SIGN-IN OPTIONS

You can learn more about sign-in options, consult the following article: <https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-user-signin>.

A

- AADRM module 53
- Active Directory. *See* Azure Active Directory
- Active Directory Domains and Trusts console 112
- Active Directory Domain Services (AD DS)
 - deployment 97
- Active Directory Federation Services (AD FS) 98, 110, 137–192
 - claim rules 151–152
 - configuration 155–166
 - deploying topologies 138–139
 - installing 156–166
 - network requirements 150
 - proxy servers 179–190
 - certificates for 180–181
 - configuration 184–189
 - custom proxy forms login page 189
 - installing required Windows roles and features 181–184
 - setting up perimeter network name resolution 180
 - requirements for 137–152
 - server farm 152–179
 - adding additional servers to 166–177
 - configuration 155–156
 - service accounts 153–155, 176–177
 - stand-alone configuration 155–156
 - using certificates with 139–149, 178–179
 - using namespaces 149–150
 - versions of 138
- Active Directory objects
 - cleaning up 99–102
- Active Incidents 220
- Active Users report 195–196
- Add-MsolAdministrativeUnitMember cmdlet 91
- Add-MsolForeignGroupToRole cmdlet 90
- Add-MsolGroupMember cmdlet 86
- Add-MsolRoleMember cmdlet 59, 86
- Add-MsolScopedRoleMember cmdlet 91
- AD FS Configuration Wizard 155, 160–165
- administrative unit management cmdlets 91
- administrator roles 3–5
 - assigning 58
 - billing administrator 55
 - delegated administrator 56–57
 - Exchange Online administrator 57
 - global administrator 54–55
 - management of, in Office 365 54–60
 - password administrator 56
 - service administrator 56
 - SharePoint Online administrator 58
 - Skype for Business administrator 57–58
 - user management administrator 55
- ADModify.NET 101–102, 104–105
- ADSIEdit 101
- AIP. *See* Azure Information Protection
- alerts 220
- aliases
 - column xii
- APIPA addresses 41–42
- app passwords 77–79
- attribute filtering 98
- auditing reports 206–207
- authentication
 - multi-factor 75–79, 113, 150
 - pass-through 110
- Autodiscover CNAME records 31, 32
- Azure
 - rights management 42–53
- Azure Active Directory 97
 - Azure AD Connect requirements 111–112
 - cloud identities in 63, 64
 - cmdlets 85–91
 - filtering 105–107
 - forest account 120

Azure Active Directory Roles

- objects 99–102
- preparing for Azure AD Connect 97–110
- Recycle Bin 82, 130
- sign-in configuration 121
- user and group management 128–134
- Azure Active Directory Roles 48–49
- Azure Active Directory Sync tools 98
- Azure AD Connect 97–136
 - about 98–99
 - AD filtering 105–107, 123
 - AD objects and 99–102
 - features 98–99
 - identifying synchronized attributes 125–127
 - installation requirements 111–116
 - account requirements 115–116
 - connectivity requirements 114
 - hardware requirements 114–115
 - Office 365 requirements 111
 - on-premises AD environment requirements 111–112
 - server requirements 113
 - SQL Server requirements 115
 - installing 116–124
 - multiple forest support 108–109
 - non-routable domains and 102–105
 - password synchronization 190
 - preparing on-premises AD for 97–110
 - setting up 110–128
 - sign-on options 109–110
 - UPN suffixes and 102–105
 - user and group management 128–134
- Azure AD reports 207
- Azure Information Protection (AIP) 43
 - activation of 43–46
 - configure rights management email templates 49–52
 - Office integration with 46–48
- Azure Multi-Factor Authentication Server 150–151
- Azure Rights Management
 - activation of 43–46
 - assign roles for 48–49
 - enable recovery of protected document 49
 - managing using PowerShell 53
 - Office integration with 46–48
 - super users 48–49

B

- bandwidth recommendations 41
- billing administrator 3, 55

- bulk account operations 83–84
- bulk import process 71–73
- bulk license users 84

C

- CATCH block. *See also* TRY-CATCH construct
- Certificate Import Wizard 166–171
- certificates
 - exporting 146–149
 - for proxy servers 180–181
 - importing 166–171
 - life cycle management 178–179
 - requesting 140–145
 - Service Communications Certificates 139–149, 166–171, 178–181
 - using 139–149
 - Web Application Proxy requirements 149
- claim rules 151–152
- client connectivity
 - bandwidth recommendations 41
 - Internet 41–42
 - outbound firewall ports 40–41
 - proxy servers 39–40
 - to Office 365 39–42
- cloud identities 63–96
 - managing with PowerShell 79–91
 - password management 63–71
 - user and security group management 71–79
 - working with 64
- CLR. *See* Common Language Runtime (CLR)
- CNAME records 31, 32, 149–150
 - Exchange federation 34
 - Skype for Business Online 37–38
- company information and service management
 - cmdlets 90
- configuration
 - AD FS 155–166
 - app passwords 77–79
 - Azure AD Connect 110–128
 - custom domains 9–16
 - DNS records 29–39
 - federation with Office 365 137–152
 - firewalls 42
 - multi-factor authentication 150–151
 - Office 365 Management Pack 215–218
 - online services 13

- password expiration 81
- password management 63–71
- password policies 64–65
- proxy servers 39–40
- rights management email templates 49–52
- single sign on 137
- tenant name 2
- UPN 104–105
- Web Application Proxy server 184–189
- Confirm-MsolDomain cmdlet 88
- Connect-MsolService cmdlet 90, 177
- Convert-MsolDomainToFederated cmdlet 89
- Convert-MsolDomainToStandard cmdlet 88–89
- Convert-MsolFederatedUser cmdlet 85
- CTEs. *See* common table expressions (CTEs)
- custom domains
 - add and configure 9–16
 - confirming ownership of 10–12
 - DNS records configuration 29–39
 - moving ownership to Office 365 15–16
 - specifying names 9–10
 - specifying purpose of 12–15
 - update and verify settings for 16
- custom proxy forms 189

D

- data
 - querying. *See* queries
- Data Loss Prevention (DLP) reports 207
- default gateway addresses 42
- delegated administrator 56–57
- deleting
 - groups 129–130
 - objects 130
 - user accounts 73–75, 82–83, 129–130
- device writeback 99
- diagnostic tools 18–20
- DirSync 98
- Disable-AadrmSuperUserFeature cmdlet 49
- DLP policy matches by severity for mail report 207
- DLP policy matches, overrides, and false positives for mail report 207
- DNS records
 - Autodiscover CNAME records 31, 32
 - configuration of 29–39
 - Exchange 30–34

- Exchange federation CNAME records 34
- Exchange federation TXT records 33–34
- MX records 31–32
- SharePoint Online 38
- Skype for Business 34–38
- SPF records 33
 - update and verify for Office 365 settings 38–39
- DNS settings 14, 15, 16
- Domain Administrator credentials 173–174
- domain controller role 156
- domain management cmdlets 88
- domain names
 - confirming ownership of 10–12
 - custom 2
 - specifying 9–10
- Domain Name Server (DNS) Connectivity test 227
- domains
 - adding 10
 - buying 10
 - confirming ownership of 10–12
 - converting from standard to federated 177–178
 - custom 9–16
 - filtering 105
 - non-routable 102–105
 - publicly routable 102–105
 - specifying purpose of 12–15
 - update and verify settings for 16

E

- email accounts
 - for pilot users 21–23
- Email Activity report 198
- Email App Usage report 199
- email templates
 - rights management 49–52
- email tests 224, 226
- Enable-AadrmSuperUserFeature cmdlet 49
- Exchange ActiveSync connectivity tests 224, 225
- Exchange Client Network Bandwidth Calculator 41
- Exchange hybrid deployment 98
- Exchange Online 23
- Exchange Online administrator 57
- Exchange Online Archiving 23
- Exchange Online Protection 23
- Exchange reports 197–199
- Exchange Web Services connectivity tests 224, 225–226

F

farms. *See* server farms

FastTrack for Office 365 25

federation. *See also* Directory Federation Services (AD FS)

- converting from standard to federated domain 177–178
- requirements for 137–152
- server certificate requirements 139–149

federation servers

- adding additional 166–177

filtering

- accessing, using claim rules 151–152

firewalls

- configuration 42
- outbound ports 40–41
- testing 230

First Release 8

forests

- functional levels 112
- multiple 108–109

G

GAL. *See* Global Address List

Get-AadrmSuperUser cmdlet 49

Get-AdminAuditLogConfig cmdlet 222

Get-ADSyncScheduler cmdlet 130, 131

Get-MailboxAuditBypassAssociation cmdlet 223

Get-MessageTrackingReport cmdlet 223

Get-MsolAccountSku cmdlet 89

Get-MsolAdministrativeUnit cmdlet 91

Get-MsolAdministrativeUnitMember cmdlet 91

Get-MsolCompanyInformation cmdlet 90

Get-MsolContact cmdlet 90

Get-MsolDomain cmdlet 88, 178

Get-MsolDomainFederationSettings cmdlet 89

Get-MsolDomainVerificationDns cmdlet 88

Get-MsolFederationProperty cmdlet 89

Get-MsolGroup cmdlet 86

Get-MsolGroupMember cmdlet 86

Get-MsolPartnerContract cmdlet 90

Get-MsolPartnerInformation cmdlet 90

Get-MsolPasswordPolicy cmdlet 88

Get-MsolRole cmdlet 59, 86

Get-MsolRoleMember cmdlet 59, 86

Get-MsolScopedRoleMember cmdlet 91

Get-MsolServicePrincipal cmdlet 87

Get-MsolServicePrincipalCredential cmdlet 87

Get-MsolSubscription cmdlet 89

Get-MsolUser cmdlet 84, 85

Get-MsolUserRole cmdlet 86

Global Address List (GAL) 108

global administrator 3–5, 54–55

GoDaddy 10

group and role management cmdlets 86–87

group-based filters 106

group managed service accounts 155, 162

groups

- creating 128–129
- deleting 129–130
- managing 128–134
- modifying 129

group writeback 99

H

hard delete

- user accounts 82–83

History 209

HOST records 150

hybrid deployments 18

Hybrid Free Busy Troubleshooter 230–231

I

IdFix tool 20, 100–101

Internet connectivity

- for clients 41–42

K

Kerberos 150

L

licenses

- assigning 6–7
- assigning to accounts 129
- bulk 84
- conflict resolution 7
- tenant 5–7

Log On As A Batch Job 154, 170
 Log On As A Service Job 171

M

Mailbox access by non-owners report 206
 Mailbox content search and hold report 206
 Mailbox litigation holds report 207
 mailbox usage report 198–199
 mail public folders 98
 maintenance
 planned 210
 Malware detections report 207
 message auditing cmdlets 222–223
 Message Center 221–222
 message tracking cmdlets 223
 Microsoft Azure. *See* Azure
 Microsoft Connectivity Analyzer 228–229
 Microsoft Dynamics CRM Online 24
 Microsoft Remote Connectivity Analyzer 224–228
 Monitoring Dashboard 218–222
 multi-factor authentication 75–79
 configuration of 150–151
 multi factor authentication (MFA) 113
 multi-forest synchronization 108–109
 MX records 11, 31–32

N

names
 domain 2
 specifying domain 9–10
 tenant 2
 name servers 15–16
 namespaces
 using 149–150
 network requirements
 for AD FS 150
 New-AdminAuditLogSearch cmdlet 222
 New-MailboxAuditLogSearch cmdlet 223
 New-MsolAdministrativeUnit cmdlet 91
 New-MsolDomain cmdlet 88
 New-MsolFederatedDomain cmdlet 88
 New-MsolGroup cmdlet 87
 New-MsolLicenseOptions cmdlet 89
 New-MsolServicePrincipalAddress cmdlet 87
 New-MsolServicePrincipal cmdlet 87
 New-MsolServicePrincipalCredential cmdlet 87

New-MsolUser cmdlet 85
 non-routable domains 102–105

O

objects
 AD 99–102
 deleting 130
 modifying 101–102
 repairing 100–101
 Office 365
 administrator roles 54–60
 billing administrator 55
 delegated administrator 56–57
 Exchange Online administrator 57
 global administrator 54–55
 password administrator 56
 service administrator 56
 SharePoint Online administrator 58
 Skype for Business administrator 57–58
 user management administrator 55
 Azure AD Connect and 111
 bandwidth recommendations 41
 blocking access to 151–152
 client connectivity to 39–42
 desktop setup for previous versions of 42
 FastTrack for 25
 moving DNS ownership to 15–16
 password management 63–71
 pilot project 16–25
 connect existing email accounts 21–23
 designate pilot users 17–18
 identify workloads not requiring migration 18
 ldFix tool 20
 run diagnostic checks 18–20
 service descriptions 23–24
 test plan or use case 21
 rights management 42–53
 single sign on for 137
 user accounts. *See* cloud identities
 user and security group management 71–79
 Office 365 Health, Readiness, and Connectivity Checks
 tool 18–20
 Office 365 Management Pack 211–222
 configuration 215–218
 installing 211–214
 Monitoring Dashboard 218–222
 Office 365 platform service 23
 Office 365 reports 193–208
 Activation report 195

- Active Users report 195–196
- auditing reports 206–207
- Data Loss Prevention (DLP) reports 207
- Email Activity report 198
- Email App Usage report 199
- Exchange reports 197–199
- Groups Activity report 196–197
- mailbox usage report 198–199
- monitoring 193–223
- OneDrive reports 200–202
- planned maintenance 210
- protection reports 207
- rules reports 207
- security and compliance reports 206–208
- service health monitoring 208–223
- service interruptions 223–232
- SharePoint reports 204–206
- Skype for Business reports 202–204
- Office 365 tenancy
 - administrator roles 3–5
 - configuration for new features and updates 8–9
 - custom domains 9–16
 - provision 1–28
 - tenant regions 2–3
 - tenant subscriptions and licenses 5–7
- Office 2003 42
- Office 2007 42
- Office Activation report 195
- Office Applications 24
- Office Online 24
- OneDrive activity report 200–201
- OneDrive for Business 24
- OneDrive for Business Activity report 200–201
- OneDrive for Business Synchronization Calculator 41
- OneDrive for Business usage report 201–202
- OneDrive reports 200–202
- OneDrive usage report 201–202
- one-time passwords 75
- online services
 - configuration of 13
- organization unit (OU) filtering 106
- outbound firewall ports 40–41
- Outlook 2007 42
- Outlook 2010 42
- Outlook 2013 42
- Outlook connectivity tests 224, 226

P

- pass-through authentication 110
- password administrator 3, 56
- password management 63–71
 - expiration configuration 81
 - password complexity policy 65–66, 82
 - password policies 64–65
 - with PowerShell 80–82
- passwords
 - app 77–79
 - changing 80
 - complexity 82
 - one-time 75
 - pass-through authentication 110
 - resetting 66–71
 - administrator reset 66–68
 - self-service reset 69–71
 - service accounts 153
 - synchronization of 98, 109, 127
- Password Sync 127
- password synchronization 190
- password writeback 98, 112
- Personal Certificates store 149
- pilot project 16–25
 - connect existing email accounts 21–23
 - designate pilot users 17–18
 - identify workloads not requiring migration 18
- IdFix tool 20
 - run diagnostic checks 18–20
 - service descriptions 23–24
 - test plan or use case 21
- planned maintenance 210
- Power BI for Office 365 24
- PowerShell
 - administator role management using 59
 - administrative unit management cmdlets 91
 - Azure Active Directory cmdlets 85–91
 - Azure Rights Management using 53
 - bulk account operations 83–84
 - cloud identity management using 79–91
 - compant information and service management cmd-lets 90
 - converting from standard to federated domain using 177–178
 - customizing proxy forms login page with 189

- domain management cmdlets 88
- group and role management cmdlets 86–87
- message auditing cmdlets 222–223
- message tracking cmdlets 223
- password management with 80–82
- service principal management cmdlets 87
- single sign-on management cmdlets 88–89
- subscription and license management cmdlets 89
- synchronization management in 130–131
- user management cmdlets 85–86
- private keys
 - exporting 146–149
 - protection 168
- Project Online 24
- Project Pro for Office 365 24
- protected documents
 - recovery of 49
- protection reports 207
- Protect-RMSFile cmdlet 49
- provision tenants 1–9
- proxy servers
 - AD FS 179–190
 - authentication 42
 - certificates for 180–181
 - configuration 39–40, 184–189
 - custom proxy forms login page 189
 - installing required Windows roles and features 181–184
 - setting up perimeter network name resolution 180
- publicly routable domains 102–105

R

- Recycle Bin 82, 130
- Redo-MsolProvisionContact cmdlet 90
- Redo-MsolProvisionGroup cmdlet 87
- Redo-MsolProvisionUser cmdlet 86
- Remote Access role 181–184
- remote connectivity troubleshooting 224–228
- Remove-MsolAdministrativeUnit cmdlet 91
- Remove-MsolAdministrativeUnitMember cmdlet 91
- Remove-MsolContact cmdlet 90, 130
- Remove-MsolDomain cmdlet 88
- Remove-MsolFederatedDomain cmdlet 89
- Remove-MsolGroup cmdlet 87, 130
- Remove-MsolGroupMember cmdlet 87
- Remove-MsolRoleMember cmdlet 59, 87
- Remove-MsolScopedRoleMember cmdlet 91
- Remove-MsolServicePrincipalCredential cmdlet 87
- Remove-MsolUser cmdlet 74, 82–83, 86, 130
- reports. *See* Office 365 reports
- resetting passwords 66–71
- Resolved Incidents 221
- Restore-MsolUser cmdlet 86
- rights management
 - email templates, configuration 49–52
 - Microsoft Azure 42–53
- Role group changes report 206
- RSS feed 211
- Rule matches for mail report 207
- rules reports 207

S

- Search-AdminAuditLog cmdlet 222
- Search-MailboxAuditLog cmdlet 223
- Search-MessageTrackingReport cmdlet 223
- Secure Sockets Layer (SSL) certificates 139–149, 161, 178–179
- security and compliance reports 206–208
- security groups
 - management of 71–79
- self-service password reset 69–71
- Sender Protection Framework (SPF) records 33
- Skype for Business Online 35–36
- Sent and received mail report 207
- server authentication certificates 139–149, 161, 178–179
- server farms 138
 - adding additional servers to 166–177
 - AD FS 152–179
 - configuration 155–156
- Server Manager console 159
- servers
 - federation 166–177
 - proxy 179–190
- service accounts 153–155
 - group managed 155, 162
 - specifying 176–177
- service administrator 3, 56
- Service Communications Certificates 139–149, 166–171, 178–181
- service descriptions 23–24

Service Health dashboard

- Service Health dashboard 208–211
- service health monitoring 208–223
- service interruptions 223–232
- service principal management cmdlets 87
- Service Principal Names (SPNs) 155
- Service Status 218–220
- Set-AdfsGlobalWebContent cmdlet 189
- Set-AdfsWebTheme cmdlet 189
- Set-ADSyncScheduler cmdlet 131
- Set-MailboxAuditBypassAssociation cmdlet 223
- Set-MsolADFSContext cmdlet 89, 177
- Set-MsolAdministrativeUnit cmdlet 91
- Set-MsolCompanyContactInformation cmdlet 90
- Set-MsolCompanySecurityComplianceContactInformation cmdlet 90
- Set-MsolCompanySettings cmdlet 90
- Set-MsolDirSyncEnabled cmdlet 90
- Set-MsolDomainAuthentication cmdlet 88
- Set-MsolDomain cmdlet 88
- Set-MsolDomainFederationSettings cmdlet 89
- Set-MsolGroup cmdlet 87
- Set-MsolPartnerInformation cmdlet 90
- Set-MsolPasswordPolicy cmdlet 65, 88
- Set-MsolServicePrincipal cmdlet 87
- Set-MsolUser cmdlet 65, 81, 82, 84, 86
- Set-MsolUserLicense cmdlet 89
- Set-MsolUserPassword cmdlet 80–81, 86
- Set-MsolUserPrincipalName cmdlet 86
- SharePoint Activity report 204–205
- SharePoint Online 23
 - DNS records 38
- SharePoint Online administrator 58
- SharePoint reports 204–206
- SharePoint Site Usage report 205–206
- single sign on. *See also* federation
 - AD FS deployment for 138–139
 - configuration of 137
 - password synchronization and 190
- single sign-on management cmdlets 88–89
- single-use passwords 75
- SKU ID information 83
- Skype for Business
 - DNS records 34–38
- Skype for Business activity report 202
- Skype for Business administrator 57–58
- Skype for Business Client Used report 204
- Skype for Business Conference Organizer Activity report 203
- Skype for Business Conference Participant Activity report 203–204
- Skype for Business Device Usage report 204
- Skype for Business Online 24
 - CNAME records 37–38
 - Sender Protection Framework (SPF) records 35–36
- Skype for Business Online Bandwidth Calculator 41
- Skype for Business Online Peer-To-Peer Activity report 202–203
- Skype for Business reports 202–204
- soft delete
 - user accounts 73–75
- Spam detections report 207
- SPNs. *See* Service Principal Names
- SQL instance 115
- SQL Server Express 114, 115
- SQL Server instance 114, 166
- SRV records 14–15
- SSL certificates 139–149, 161, 178–179
- Standard Release 8
- StrongPasswordRequired parameter 82
- subscription and license management cmdlets 89
- Subscription Health 218
- subscriptions
 - tenant 5–7
- Support and Recovery Assistant for Office 365 231–232
- synchronization. *See also* Azure AD Connect
 - Active Directory 97–110
 - attributes 125–127
 - filtering 105–107
 - forcing 131–134
 - managing 130–131
 - multi-forest 108–109
 - password 98, 109, 127
 - UPN suffixes and 102–105
- Synchronization Rules Editor 107
- Synchronization Service Manager 131–134

T

- TCP/IP connectivity 150
- TCP port 443 114
- TCP port 1433 114
- temporary passwords 66
- tenant regions 2–3
- tenants
 - configuration for new features and updates 8–9
 - name configuration 2
 - provision 1–9

- subscriptions and licenses 5–7
- Top DLP policy matches for mail report 207
- Top DLP rule matches for mail report 207
- Top malware for mail report 207
- Top rule matches for mail report 207
- Top senders and recipients report 207
- Transport Layer Security (TLS) certificate 139
- Transport Reliability IP Probe (TRIPP) 229–230
- troubleshooting
 - Hybrid Free Busy Troubleshooter 230–231
 - Microsoft Connectivity Analyzer 228–229
 - Microsoft Remote Connectivity Analyzer 224–228
 - service interruptions 223–232
 - Support and Recovery Assistant for Office 365 231–232
 - Transport Reliability IP Probe 229–230
- TXT records 11–12, 15
 - federation 33–34

U

- UDFs. *See* user-defined functions (UDFs)
- Unprotect-RMSFile cmdlet 49
- Update-MsolFederatedDomain cmdlet 89
- UPN suffixes 102–105
- user accounts
 - assigning UPN suffix to 104
 - bulk import process 71–73
 - bulk operations on 83–84
 - cloud identities 63–96
 - creating 128–129
 - deleting 129–130
 - hard delete of 82–83
 - licenses for 129
 - managing with PowerShell 79–91
 - password management 63–71, 80–82
 - soft delete of 73–75
 - synchronization across multiple forests 108–109
- user groups
 - management of 71–79
- user management administrator 3, 55
- user management cmdlets 85–86
- User Principal Names (UPNs)
 - configuration 104–105
 - suffixes 102–105
- users
 - bulk licensing 84
 - bulk update properties 84
 - creating 128–129
 - deleting 7, 129–130
 - filtering 123
 - importing 83–84
 - managing 128–134
 - modifying 129
 - multi-factor authentication for 75–79
 - pilot 17–18
 - uniquely identifying 108, 122

V

- VoIP quality 230

W

- Web Application Proxy server 98, 138
 - certificate requirements 149
 - certificates for 180–181
 - configuration 184–189
 - installing required Windows roles and features 181–184
 - setting up perimeter network name resolution 180
- Web Application Server 179–190
- web server certificates 139
- Windows PowerShell. *See* PowerShell
- Windows Server 2003 112, 113
- Windows Server 2008 112
- Windows Server 2012 R2 138, 139, 155
- Windows Server 2016 139, 155
- Write-AdminAuditLog cmdlet 222

Y

- Yammer 24