Managing Office 365 Identities and Requirements

SECOND EDITION

Exam Ref 70-346

Orin Thomas

Microsoft

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.

ISBN-13: 978-1-5093-0479-0
ISBN-10: 1-5093-0479-7

Library of Congress Control Number: 2017949563

First Printing August 2017

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

This page intentionally left blank

Contents

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

CHAPTER 4

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.

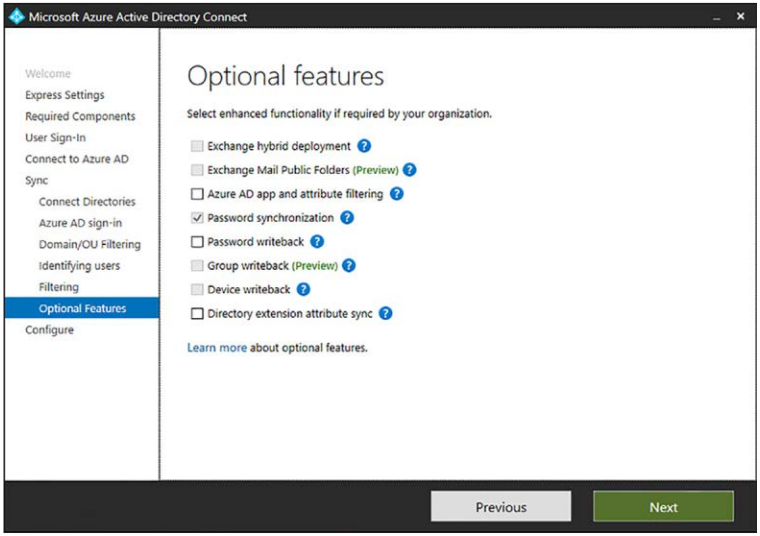

FIGURE 4-1 Azure Active Directory Connect optional features

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.

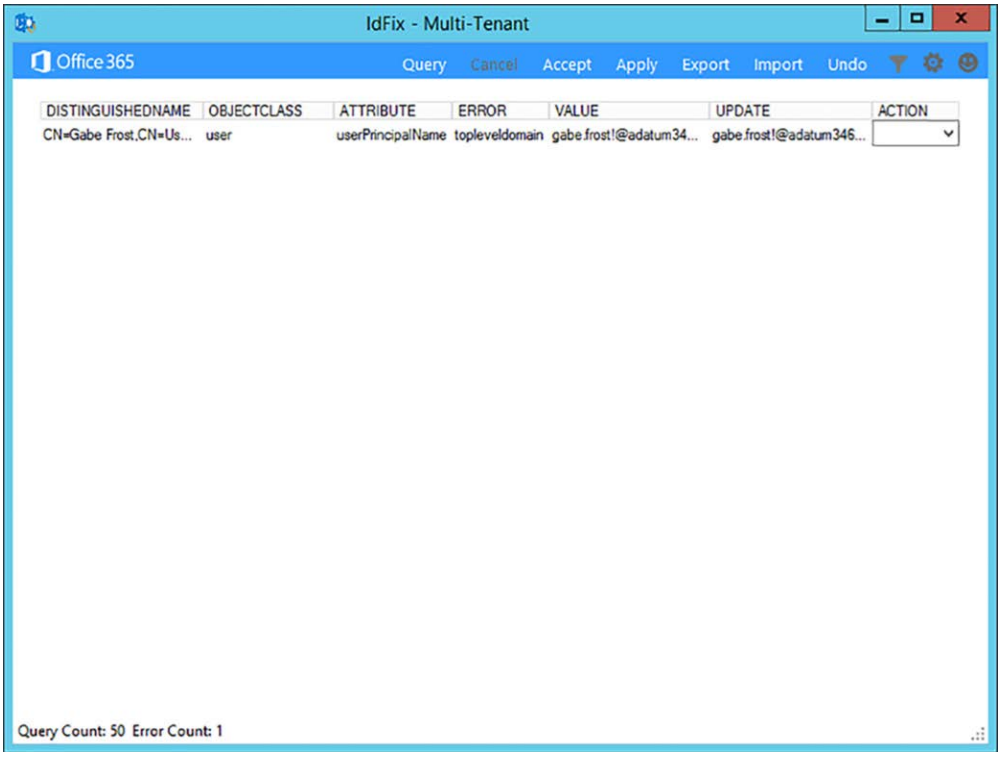

FIGURE 4-2 IdFix finds user with a problematic UPN.

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.

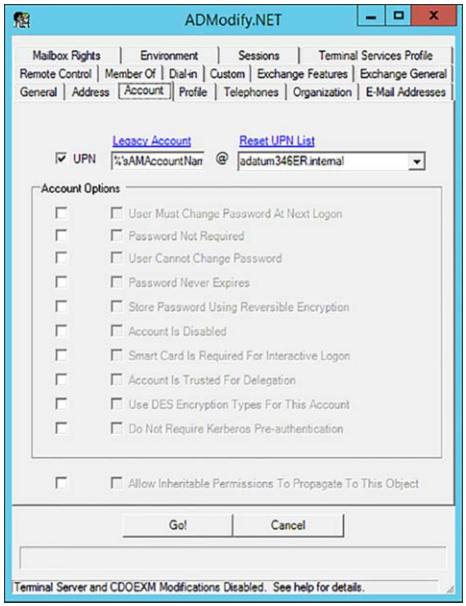

FIGURE 4-3 ADModify.NET

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*.**

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.

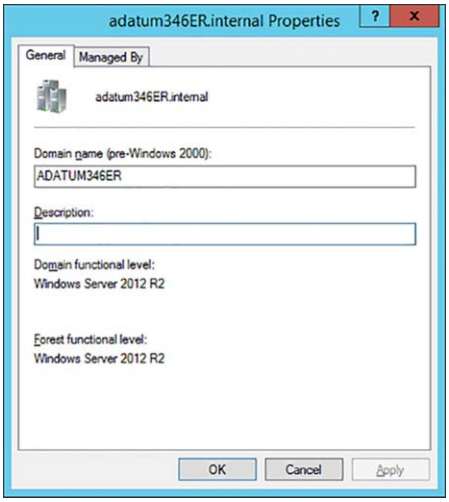

FIGURE 4-4 Non routable domain

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.

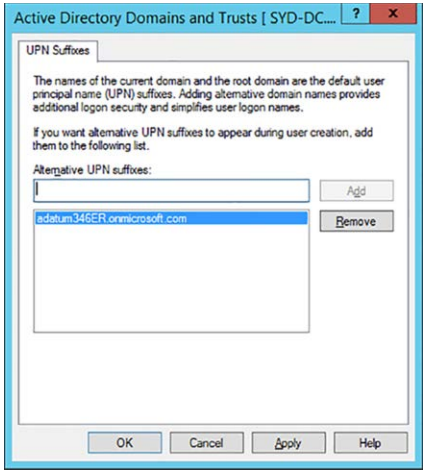

FIGURE 4-5 Non routable domain

4. 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.

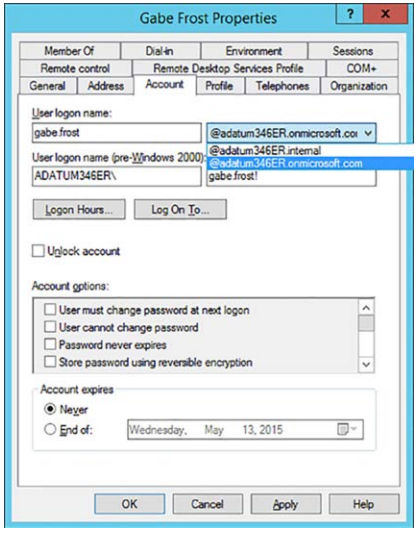

FIGURE 4-6 Configure UPN

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

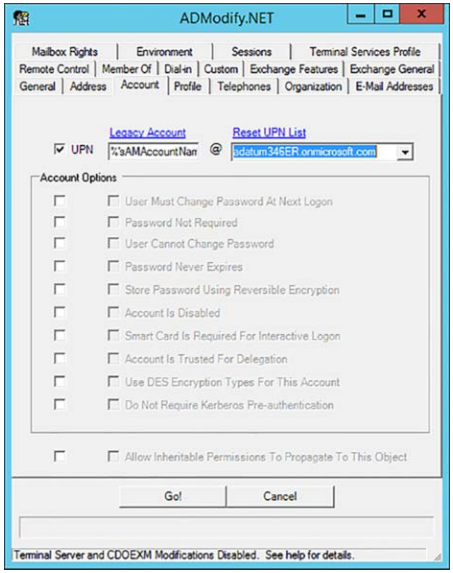

FIGURE 4-7 ADModify.NET

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.

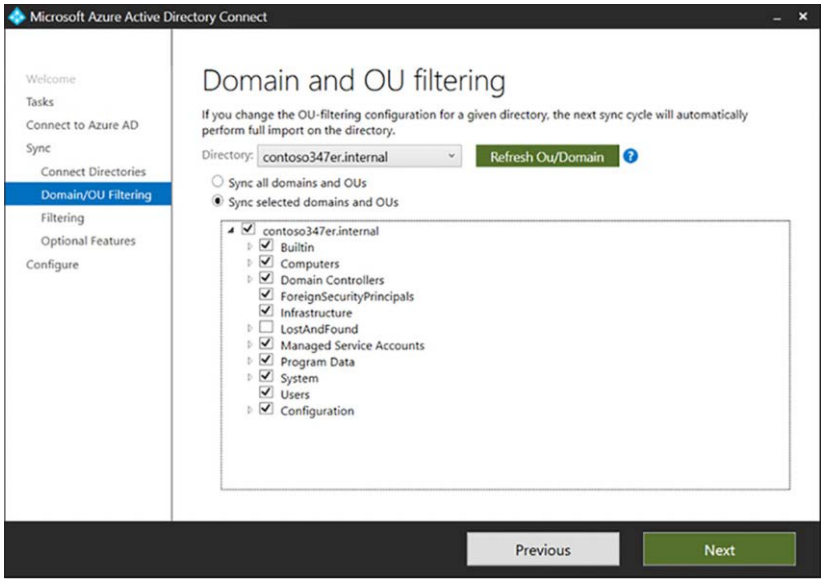

FIGURE 4-8 Domain and OU filtering

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.

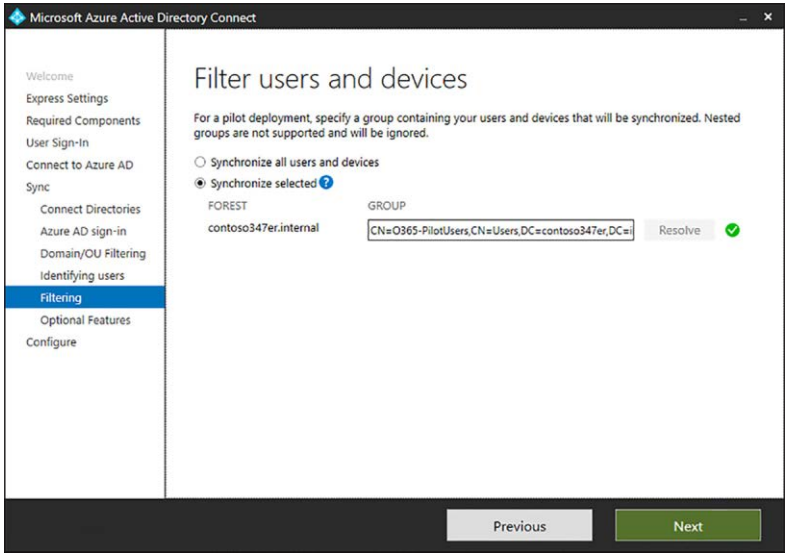

FIGURE 4-9 Filter Users And Devices

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.

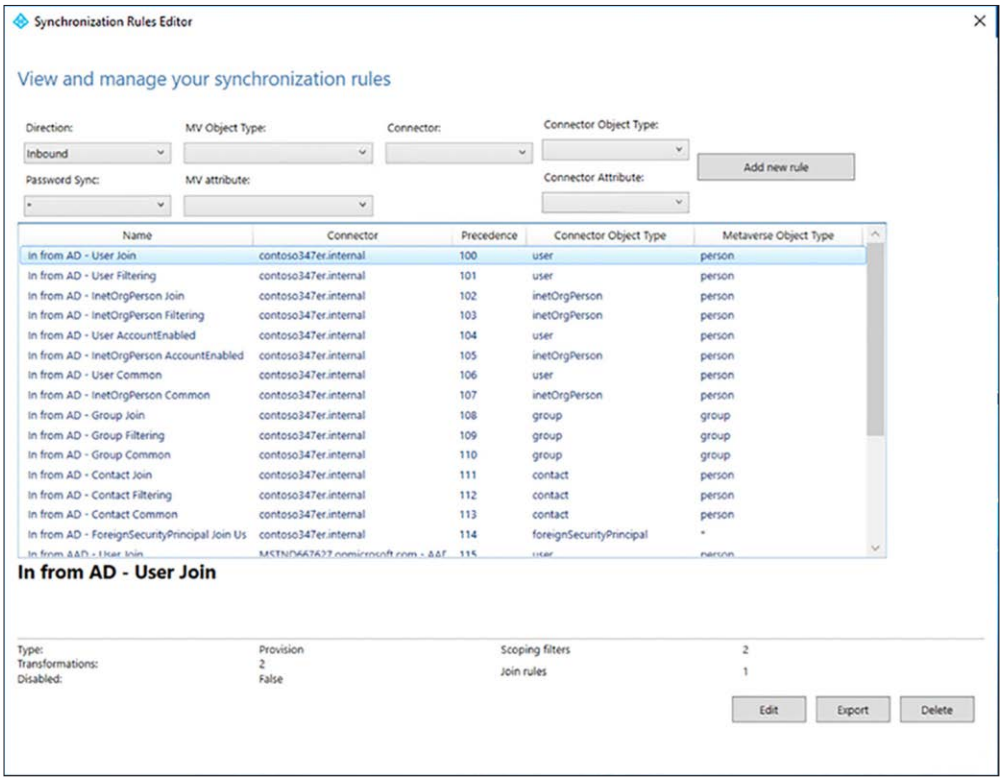

FIGURE 4-10 Synchronization Rules Editor

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:

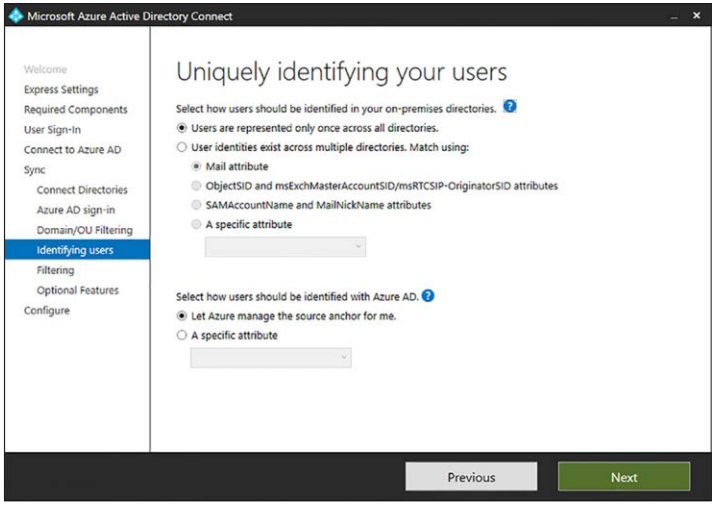

FIGURE 4-11 Uniquely identify users

- Match users using the mail attribute
- Match user using ObjectSID and msExchangeMasterAccountSID/msRTCIP-Orgiginator-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.

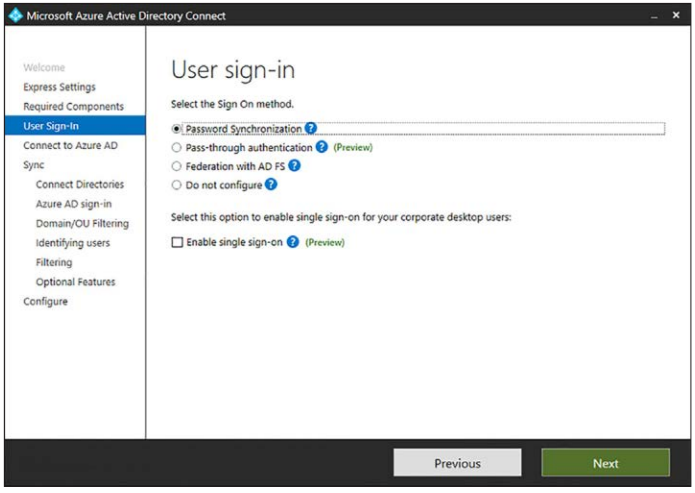

FIGURE 4-12 User sign-in

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-though 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*.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Y