Microsoft

Microsoft Security, Compliance, and Identity Fundamentals

SECOND EDITION

Exam Ref SC-900

Yuri Diogenes
Nicholas DiCola
Mark Morowczynski
Kevin McKinnerney

Microsoft

Exam Ref SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Second Edition

Yuri Diogenes
Nicholas DiCola
Mark Morowczynski
Kevin McKinnerney

Exam Ref SC-900 Microsoft Security, Compliance, and Identity Fundamentals, Second Edition

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

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: 978-0-13-836373-4
ISBN-10: 0-13-836373-0

Library of Congress Control Number: 2024932891

$PrintCode

TRADEMARKS

Microsoft and the trademarks listed at *http://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 author, 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 from the use of the 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.

CREDITS

EDITOR-IN-CHIEF
Brett Bartow

EXECUTIVE EDITOR
Loretta Yates

ASSOCIATE EDITOR
Shourav Bose

DEVELOPMENT EDITOR
Rick Kughen

MANAGING EDITOR
Sandra Schroeder

PROJECT EDITOR
Tracey Croom

COPY EDITOR
Rick Kughen

INDEXER
Timothy Wright

PROOFREADER
Charlotte Kughen

TECHNICAL EDITOR
Mike Martin

EDITORIAL ASSISTANT
Cindy Teeters

INTERIOR DESIGNER
codeMantra

COVER DESIGNER
Twist Creative, Seattle

COMPOSITOR
codeMantra

GRAPHICS
codeMantra

Contents at a glance

Contents

Acknowledgments

The authors would like to thank Loretta Yates and the entire Microsoft Press/Pearson team for their support in this project and Mark Simos for reviewing the book.

Yuri: I would also like to thank my wife and daughters for their endless support; my great God for giving me strength and guiding my path on each step of the way; my great friends and coauthors Nicholas DiCola, Kevin McKinnerney, and Mark Morowczynski for this amazing partnership. My manager, Rebecca, for always encouraging me to achieve more and stretch myself to the next level. Thanks to the support from our learning team, especially Cecilia Perez-Benitoa for her contribution to this project. Last but not least, thanks to my parents for working hard to give me an education, which is the foundation I use every day to keep moving forward in my career.

Nicholas: I would like to thank my wife and three children for supporting me while working on this book and my coauthors and friends, Yuri, Kevin, and Mark, for their hard work on this book. I would also like to thank our engineering teams and technical reviewers for their support during the production of this book.

Kevin: I would like to thank my wife and daughter for always being with me and supporting me in everything I do; my parents for their love and support throughout my life and showing me that I can accomplish anything I set my mind to; and my coauthors Yuri, Nick, and Mark for inviting me along on this journey. I would also like to thank all my information protection CXE teammates for their knowledge and mentorship throughout the years. I would not be here today without the help you have provided me.

Mark: I would like to thank my parents for being the most loving parents anyone could have asked for. I would not be where I am today without them. I'd also like to thank my grandma, who I've been extremely lucky to have in my life for too many reasons to name. Thanks to my brother, who is always in my corner and the best fantasy baseball comanager. Thanks to my girlfriend, who listened to me complain through the entire writing process and was way more supportive than I would have been. Thanks to all my coworkers over the years who have spent the time to help me improve in my career. I can never thank you all enough, and I hope this book will help our readers, if even by a fraction of the amount that you all have helped me.

About the authors

YURI DIOGENES, MSC

Yuri has a Master of Science in cybersecurity intelligence and forensics investigation from UTICA College and is currently working on his PhD in Cybersecurity Leadership from Capitol Technology University. Yuri has been working at Microsoft since 2006; currently, he is a Principal PM Manager for the Customer Experience Engineering Defender for Cloud Team, where he manages a global team of product managers focusing on cloud security posture management and workload protection. Yuri has published more than 30 books, mostly about information security and Microsoft technologies. Yuri is also a professor at EC-Council University, teaching in the Bachelor in Cybersecurity Program. Yuri has an MBA and many IT/security industry certifications, such as CISSP, MITRE ATT&CK® Cyber Threat Intelligence Certified, E|CND, E|CEH, E|CTI, E|CSA, E|CHFI, CompTIA Security+, CySA+, Network+, CASP, and CyberSec First Responder. You can follow Yuri on Twitter at @yuridiogenes.

NICHOLAS DICOLA

Nicholas is a Security Jedi and the VP of Customers at Zero Networks, where he leads a global team responsible for all things customer related. He has a Master of Business Administration with a concentration in information systems and various industry certifications such as CISSP and CEH. You can follow Nicholas on Twitter at @mastersecjedi.

KEVIN MCKINNERNEY

Kevin is a senior program manager on the Microsoft Purview Data Governance Customer Experience Engineering (CxE) Team, where he provides best practices and deployment guidance to help customers quickly onboard the Microsoft Purview Data Governance solution. Kevin has been working at Microsoft since 2011 in various roles, including senior support escalation engineer on the Microsoft CSS Security team and senior premier field engineer, focusing on Microsoft security and information protection. Kevin has authored dozens of blog posts and videos related to information protection and Purview data governance and has spoken at many technical conferences, including RSAC, Microsoft Ignite, Microsoft MVP Summits, and the Microsoft Security Engineering Advisory Council. Prior to starting at Microsoft, he worked for IBM as a Microsoft support manager and spent eight years as an information systems technician while on active duty in the United States Navy. Kevin received a Bachelor of Science in business management from the University of Phoenix and holds many certifications, including CISSP and GCIH. You can follow Kevin on Twitter @KemckinnMSFT and on GitHub (*github.com/kemckinnmsft*).

MARK MOROWCZYNSKI

Mark Morowczynski is a principal product manager on the Security Customer Experience Engineering (CxE) team at Microsoft. He spends most of his time working with customers on their deployments in the Identity and Access Management (IAM) and information security space. He's spoken at various industry events such as Black Hat, Defcon Blue Team Village, Blue Team Con, Microsoft Ignite, and several BSides and SANS Security Summits, to name a few. He has a BS in Computer Science and a MS in Computer Information and Network Security as well as an MBA from DePaul University. He also has an MS in Information Security Engineering from the SANS Technology Institute. He can be found online on Mastodon @markmorow@infosec.exchange or on his website at *https://markmorow.com*.

Introduction

The SC-900 exam is targeted at those looking to familiarize themselves with the fundamentals of security, compliance, and identity (SCI) across cloud-based and related Microsoft services. This exam is targeted at a broad audience that includes business stakeholders, new or existing IT professionals, or students interested in Microsoft security, compliance, and identity solutions. This exam covers topics such as Microsoft Azure and Microsoft 365 and requires you to understand how Microsoft security, compliance, and identity solutions can span across these areas to provide a holistic and end-to-end solution.

This book covers every major topic area on the exam but does not cover every exam question. Only the Microsoft exam team has access to the exam questions, 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 “Need more review?” links you’ll find in the text to find more information. Be sure to research and study these topics. Great information is available on docs.microsoft.com, MS Learn, and in blogs and forums.

Organization of this book

This book is organized by the “Skills Measured” list published for the exam. The “Skills measured” list is available for each exam on the Microsoft Learn website: *learn.microsoft.com/en-us/training/*. Each chapter in this book corresponds to a major topic area in the list, and the technical tasks in each topic area determine that chapter’s organization. For example, if an exam covers six major topic areas, the book will contain six chapters.

Preparing for the exam

Microsoft certification exams are a great way to build your resume and let the world know about your level of expertise. Certification exams validate your on-the-job experience and product knowledge. Although there is no substitute for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam. This book is not designed to teach you new skills.

We recommend augmenting your exam preparation plan by using a combination of available study materials and courses. For example, you might use the Exam Ref and another study guide for your “at-home” preparation and take a Microsoft Official Curriculum course for the classroom experience. Choose the combination that you think works best for you. Learn more about available classroom training and find free online courses and live events at *microsoft.com/learn*. Microsoft official practice tests are available for many exams at *aka.ms/practicetests*.

Note that this *Exam Ref* is based on publicly available information about the exam and the authors' experience. To safeguard the integrity of the exam, authors do not have access to the live exam.

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 *microsoft.com/learn*.

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:

MicrosoftPressStore.com/ERSC9002e/errata

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

For additional book support and information, please visit *MicrosoftPressStore.com/Support*.

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 *support.microsoft.com*.

Stay in touch

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

CHAPTER 2

Microsoft identity and access management solutions

Identity and access management is a core foundational piece for security and compliance. Everything today starts with identity. Users have identities to access resources such as applications, and they can do that from anywhere on the planet. Applications themselves have identities to define their permission scopes. Computer objects have identities and can be used as a factor to make access decisions. Understanding identity concepts and capabilities is a requirement for properly achieving security and compliance in your organization.

Skills in this chapter:

- Skill 2.1: Define the function and identity types of Microsoft Entra ID
- Skill 2.2: Describe the authentication capabilities of Microsoft Entra ID
- Skill 2.3: Describe access management capabilities of Microsoft Entra ID
- Skill 2.4: Describe the identity protection and governance capabilities of Microsoft Entra

Skill 2.1: Define the function and identity types of Microsoft Entra ID

This objective deals with the fundamental concepts of Microsoft Entra ID. In this section, you'll learn what Microsoft Entra ID is and its key enterprise features. You'll also learn about internal and external identities, hybrid identity, and the different ways to authenticate to Microsoft Entra ID.

This skill covers:

- Microsoft Entra for unified identity and network access
- Microsoft Entra's key features
- Hybrid identity setups
- Microsoft Entra identities, including users, devices, groups, and workloads

Describe what Microsoft Entra is

Microsoft Entra is a product suite focusing on unified identity and network access for businesses. This new suite was announced in May 2022 and consists of the following identity and network components across three key areas:

Identity and access management

- Microsoft Entra ID is formerly known as Azure Active Directory and is the key focus of this chapter. This core IAM (Identity and Access Management) product allows you to manage and protect users, apps, workload identities, and devices.
- Microsoft Entra ID Governance is discussed in Skill 2.4 and allows businesses to automatically ensure that the right people have the right access to the right apps and services at the right time.
- Microsoft Entra External ID provides functionality to allow business partners and customers secure access to resources and applications.

New identity categories

- Microsoft Entra Verified ID issues and verifies credentials based on open standards to quickly onboard employees, partners, and customers and uses the credentials anywhere that supports those open standards.
- Microsoft Entra Permissions Management is discussed in Skill 2.4 and allows you to manage your identity permissions across your multicloud (Azure, AWS, and GCP) infrastructure.
- Microsoft Entra Workload ID helps apps and services (nonhuman identities) securely access cloud resources.

Network access

- Microsoft Entra Internet Access allows secure access to the Internet and Software as a Service (SaaS) and Microsoft 365 applications.
- Microsoft Entra Private Access allows a secure connection to private apps that would usually require a VPN or other legacy protocols like NTLM or Kerberos to access them.

Describe what Microsoft Entra ID is

Microsoft Entra ID is Microsoft’s cloud-based Identity-as-a-Service (IDaaS) offering. It is an IAM product with 400 million monthly active users and tens of billions of authentications processed daily! Many of the IAM features are covered throughout this chapter, but let’s take a high-level view of some of the key features to help give you an idea of what makes up Microsoft Entra ID.

NOTE **AZURE AD AND MICROSOFT ENTRA ID**

In July 2023, Azure AD was renamed to Microsoft Entra ID to better align with the Microsoft Entra suite of products such as Microsoft Entra Permissions Management, Microsoft Entra Verified ID, and others. Many existing content refers to Azure AD, so just know Azure AD is now Microsoft Entra ID.

Applications

Microsoft Entra ID is the Identity Provider (IdP) for Microsoft applications such as Office365 and Azure. It also leverages modern protocols such as WS-Federation, SAML, OAuth, and OpenID Connect to integrate with non-Microsoft applications. The Microsoft Entra Application Gallery has thousands of pre-integrated applications, making authentication to these apps easy to set up. Also, the Application Gallery uses the SCIM (System for Cross-domain Identity Management) protocol for provisioning users to and de-provisioning users from these applications. If the application is not in the gallery, you can still integrate it with Microsoft Entra ID yourself, or you can request that it should be added to the gallery. You can also build your own applications that call the Microsoft Graph or other Microsoft APIs, your own APIs, and get tokens. The Microsoft Authentication Library (MSAL) is available to help accelerate your developer teams with these tasks.

MORE INFO **ADDING APPLICATIONS TO THE MICROSOFT ENTRA APPLICATION GALLERY**

You can request applications to be added to the Application Gallery at *https://aka.ms/SC900_AddToME-IDAppGallery*.

Application proxy

Application proxy is used to provide remote access to on-premises web applications. This allows any conditional access policies to apply when accessing these on-premises applications without making any changes to the application itself. This is an excellent way to leverage your cloud-based identity security to protect your existing on-premises applications. All connectivity is outbound to Microsoft Entra ID. These applications will appear to the user as any other application. There is no difference to the user if the application is on-premises or in the cloud. They access it in the same way.

Authentication

Skill 2.2 is focused on the authentication aspects of Microsoft Entra ID, such as password hash sync (PHS), pass-through authentication (PTA), federation, multifactor authentication (MFA), passwordless methods such as Windows Hello for Business, Certificate-based, FIDO2, and Microsoft Entra Password Protection.

Access management

Skill 2.3 is focused on the access management aspects of Microsoft Entra ID, specifically the conditional access feature. At a high level, you can define which users or groups must meet a specific criterion, such as completing MFA or having a specific device or platform type, before they can access a resource, such as a specific application or the applications in your tenant. Many different Microsoft Entra roles can be assigned to administrators to follow the principle of least-privilege while also granting them the necessary access to perform necessary tasks. You will also see the concept of least-privilege later in Microsoft Entra Permissions Management.

Devices

Microsoft Intune is the primary device management platform for cloud-based devices, but there are device objects in Microsoft Entra ID that are Microsoft Entra–registered, Microsoft Entra hybrid–joined, or Microsoft Entra–joined. We'll cover Microsoft Entra hybrid–joined devices in more detail in the next section, but these devices can be used as a control in conditional access that must be met before accessing the resource. Just be aware that devices do exist in Microsoft Entra ID, but the traditional management you think of with group policy Objects (GPOs) is performed from Microsoft Intune. However, there is a tight relationship between Microsoft Entra ID and Microsoft Intune.

Domain services

Microsoft Entra Domain Services lets you join your Azure virtual machines to a traditional Active Directory domain. This is separate from your on-premises Active Directory domain but is populated from your Microsoft Entra tenant. You can think of this as a resource forest for legacy protocols like NTLM, Kerberos, and LDAP for applications that have been lifted and shifted into Azure.

External identities

Microsoft Entra enables easy collaboration with other companies using Microsoft Entra Business-to-Business (B2B) that share resources like documents or access applications. You would use Azure AD Business-to-Consumer (B2C) if you are creating customer-facing apps that are fully featured Customer Identity and Access Management (CIAM) solutions. Azure Active Directory B2C is a totally separate Microsoft Entra tenant. Both Microsoft Entra B2B and Azure AD B2C support conditional access.

Governance

Skill 2.4 is focused on the governance aspects of Microsoft Entra ID. These features include Lifecycle Workflows, Access Reviews, and several aspects of Entitlement Management, from automatic assignment and using Microsoft Entra Verified ID to improve onboarding. The primary focus of governance is determining which users should access which resources. The governance process must also be auditable to verify that it is working.

Reporting

Various log sources are available, from directory changes in audit logs to sign-in logs for interactive and noninteractive events. Microsoft Entra also includes logs for applications and managed-service identities—a specific type of application identity. You can also see Microsoft Graph API activity from these apps, such as if the application is enumerating the directory or the privileges these applications use. These can all be accessed in the Microsoft Entra portal or exported to Log Analytics, Microsoft Sentinel, or any other SIEM.

EXAM TIP

Remember the different features used for Microsoft Entra ID and which problems they solve for a company.

Licensing

Microsoft Entra ID has four core levels of licensing:

- **Microsoft Entra ID Free** Microsoft Entra ID Free provides user and group management and directory sync. This is included when you sign up for Office 365 or Microsoft 365 resources.
- **Microsoft Entra ID P1** This level includes most of the features discussed in this chapter. This includes conditional access, self-service password reset with writeback, dynamic groups, and much more.
- **Microsoft Entra ID P2** This level includes some governance capabilities, such as basic access reviews, basic entitlement management, and privilege identity management. It also includes identity protection and advanced security features.
- **Microsoft Entra ID Governance** This level includes advanced governance capabilities that can be extended onto the existing governance capabilities in P1 or P2, such as using entitlement management with customer extensions (Logic Apps) or Lifecycle Workflows (LCW).

MORE INFO **MICROFT ENTRA ID FEATURES BY LICENSE**

For a detailed breakdown of what features are included in each license level, see *https://aka.ms/SC900_ME-IDLicensing*.

EXAM TIP

Remember which features are part of Microsoft Entra ID P2 and Microsoft Entra ID Governance. The rest are included in Microsoft Entra ID P1.

Describe what hybrid identity is

Very few customers are starting with a completely greenfield environment (a from-scratch and totally new environment) with only Microsoft Entra ID accounts accessing only cloud resources. Most customers are in a hybrid identity state with their Microsoft Entra tenant(s) connected to an on-premises AD. This is where user accounts must exist in the on-premises Active Directory and in Microsoft Entra ID. The user might access a local file server and then access their email in Office365. They need to be able to do this with one seamless account. Hybrid identity makes this possible. You must use a hybrid identity to leverage your existing Active Directory environment and take advantage of Microsoft Entra ID.

There are two distinct components to a hybrid identity setup:

- Syncing of the users and their attributes from Active Directory to Microsoft Entra ID.
- Authenticating to Microsoft Entra ID using credentials from on-premises Active Directory. This can be accomplished via password hash sync (PHS), pass-through authentication (PTA), or federation.

Microsoft Entra Connect

Microsoft Entra Connect is one of the tools used to create users, groups, and other objects in Microsoft Entra ID. The information is sourced from your on-premises Active Directory, which is the usual scenario for most customers using a hybrid identity. Changes in your on-premises directory to those objects are automatically synced to Microsoft Entra ID. The source of authority (SOA) for these objects is the on-premises Active Directory, meaning the sync is one-way from Active Directory to Microsoft Entra ID.

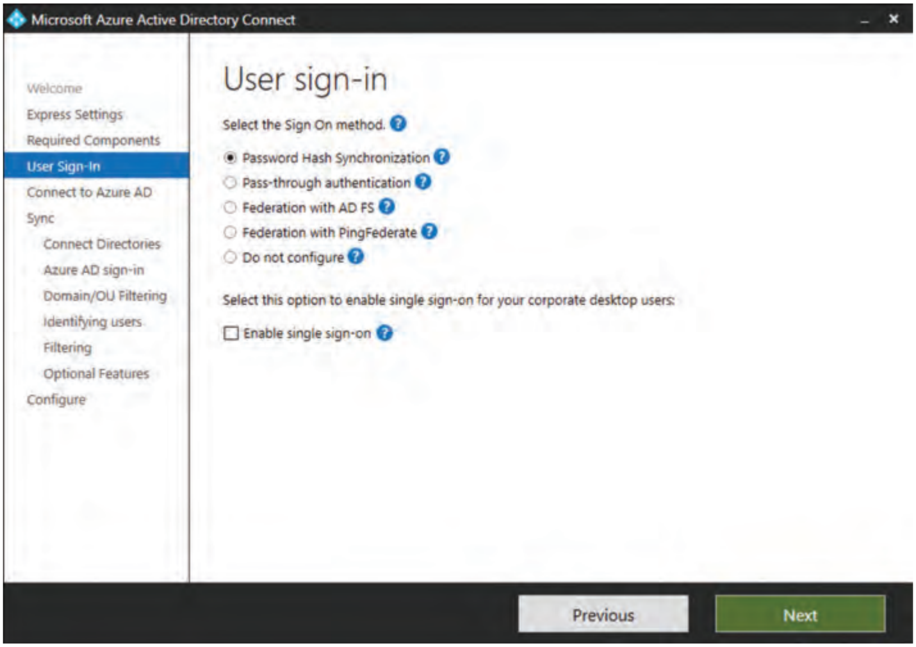
Microsoft Entra Connect has a very robust setup wizard to help you with this process. You use the express setup to choose the default options for you, or you can do a custom installation to get extremely granular with your choices. You can select which objects will be synced to Microsoft Entra ID (and which attributes of those objects, if needed).

Another part of the setup wizard helps you pick which authentication method your users will use to authenticate to Microsoft Entra ID, as shown in Figure 2-1.

Microsoft Entra Connect is a key piece of hybrid infrastructure and must be protected like you would protect a domain controller in Active Directory. If an attacker were to access a Microsoft Entra Connect server, this would be the security equivalent of getting access to a domain controller.

MORE INFO **MICROSOFT ENTRA CONNECT**

You can read more about customizing the Microsoft Entra Connect Sync at *https://aka.ms/SC900_EntraConnectCustomize*.



User sign-in

Select the Sign On method.

● Password Hash Synchronization
○ Pass-through authentication
○ Federation with AD FS
○ Federation with PingFederate
○ Do not configure

Select this option to enable single sign-on for your corporate desktop users:

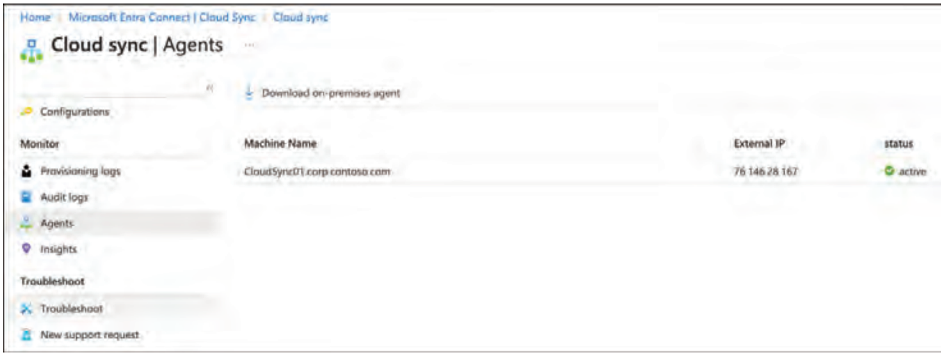
□ Enable single sign-on

FIGURE 2-1 User sign-in options

Microsoft Entra cloud sync

Microsoft Entra Cloud sync is the latest tool used to create users, groups, and contacts in Microsoft Entra ID. It is similar to Microsoft Entra Connect. The primary difference is that a lightweight agent is used, as shown in Figure 2-2, and the cloud sync configuration is entirely managed in the cloud.

This sync agent setup works well for Active Directory multi-forest setups that are disconnected from each other. For example, during a merger and acquisition scenario, the on-prem Active Directory forests would typically not have any network connectivity to each other. Multiple Entra Cloud Sync agents can provide a high-availability sync and run side by side with Microsoft Entra Connect.



Machine Name	External IP	status
CloudSync01.corp.contoso.com	76.146.28.167	✓ active

FIGURE 2-2 Cloud Sync agents

Not all functionality in Microsoft Entra Connect is available yet in Microsoft Entra Cloud sync. At the time of this writing, support for device object syncing is unavailable and neither is syncing groups with more than 250,000 members. However, new functionality continues to be added to Microsoft Entra Cloud Sync. If you can use this over Microsoft Entra Connect, it can simplify your hybrid setup.

MORE INFO **MICROSOFT ENTRA CHOOSE THE RIGHT SYNC CLIENT**

You can read more about the functionality supported in Microsoft Entra cloud sync versus the same in Microsoft Entra Connect at *https://aka.ms/SC900_ChooseSyncClient*.

Password hash synchronization

The current credentials in on-premises Active Directory are synced to Microsoft Entra ID through Microsoft Entra Connect or Microsoft Entra Cloud Sync. The on-premises password itself is never sent to Microsoft Entra ID, but a password hash is. The hashes stored in Microsoft Entra ID differ completely from those in on-premises Active Directory. Active Directory password hashes are MD4, and Microsoft Entra ID password hashes are SHA256. The user authenticates to Microsoft Entra ID, entering the same password they use on-premises. See the next More Info item for the detailed cryptographic specifics on how this process works.

MORE INFO **MICROSOFT ENTRA CONNECT PASSWORD HASH SYNC DETAILS**

You can read more about the Microsoft Entra Connect Sync Password Hash Sync at *http://aka.ms/SC900_HowPHSWorks*.

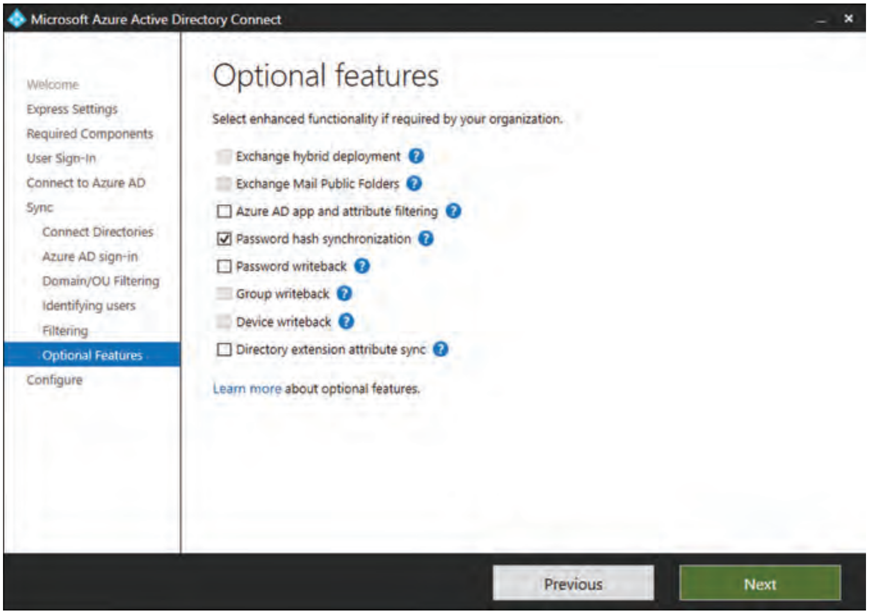
You can also select password hash sync as an optional feature in Microsoft Entra Connect if you use pass-through authentication (PTA) or federation as your primary authentication method, as shown in Figure 2-3. This gives you two benefits:

- Microsoft Entra can alert you when the username and password are discovered online. There will be a leaked credential alert for that user.
- If something catastrophic happens to the on-premises Active Directory, an admin can flip the authentication method to password hash sync. This would allow users to access cloud resources when the full disaster recovery plan is executed.

Password hash synchronization should be used as the default authentication choice unless there are specific requirements not to do so.

Pass-through authentication

Pass-through authentication (PTA) allows the user's password to be validated against the on-premises Active Directory using PTA agents. When a user goes to authentication to Microsoft Entra, the username and password are encrypted and put into a queue. The on-premises PTA agent reaches outbound to Microsoft Entra ID, picks up the request, decrypts the username and password, and then validates it against Active Directory. It then returns to Microsoft Entra ID if the authentication is successful. This allows for on-premises policies such as sign-in-hour restrictions to be evaluated during authentication to cloud services. The password hash doesn't need to be present in Microsoft Entra ID in any form for PTA authentication to work. However, PHS can be enabled as an optional feature.



Optional features

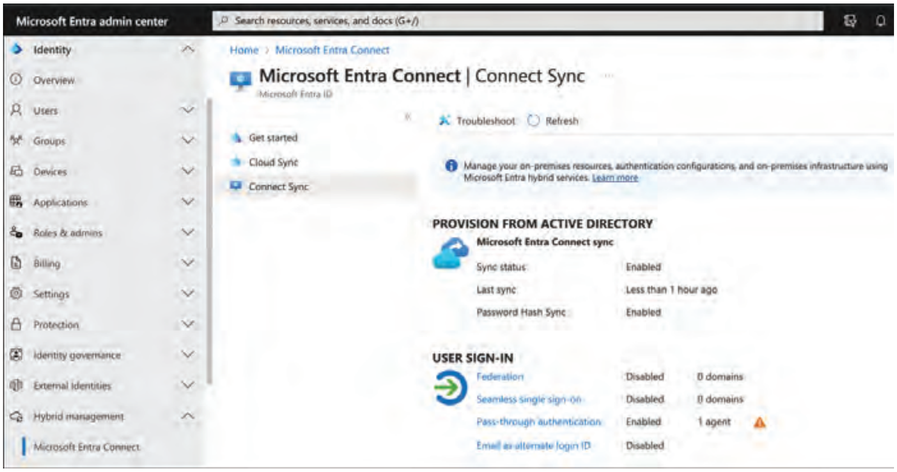
Select enhanced functionality if required by your organization.

- □ Exchange hybrid deployment
- □ Exchange Mail Public Folders
- □ Azure AD app and attribute filtering
- ☑ Password hash synchronization
- □ Password writeback
- □ Group writeback
- □ Device writeback
- □ Directory extension attribute sync

Learn more about optional features.

FIGURE 2-3 Password hash synchronization

The first PTA agent is usually installed on the Microsoft Entra Connect server. In a disconnected forest scenario, Microsoft Entra Cloud Sync does not support PTA authentication. It's recommended that you have a minimum of three PTA agents for redundancy. You can see the total number of PTA agents installed at the Microsoft Entra Connect page in the Microsoft Entra ID Portal, which is shown in Figure 2-4.



Microsoft Entra Connect | Connect Sync

Microsoft Entra ID

Manage your on-premises resources, authentication configurations, and on-premises infrastructure using Microsoft Entra hybrid services. Learn more

PROVISION FROM ACTIVE DIRECTORY

Microsoft Entra Connect sync

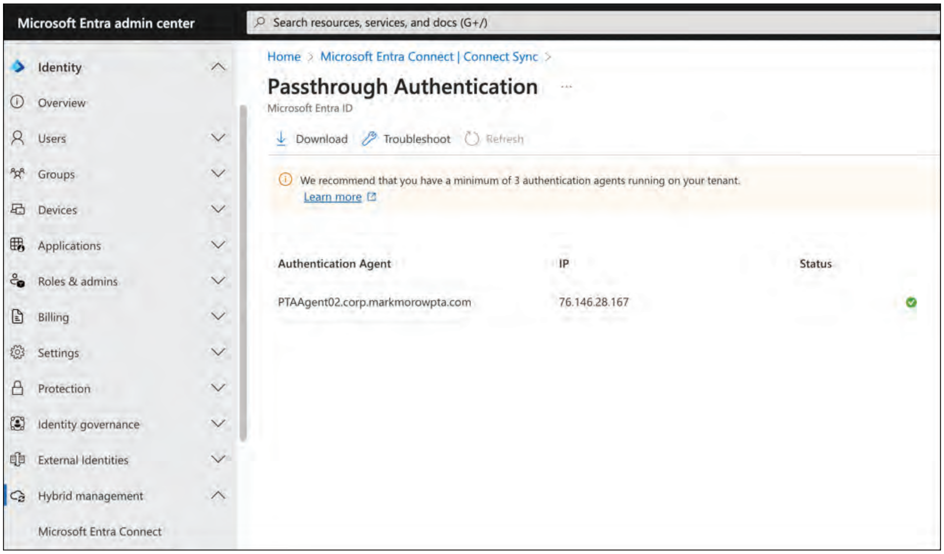
Sync status	Enabled
Last sync	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN-IN

Federation	Disabled	0 domains
Seamless single sign-on	Disabled	0 domains
Pass-through authentication	Enabled	1 agent ⚠
Email as alternate login ID	Disabled	

FIGURE 2-4 Pass-through authentication agent installed

To see the specific IPs of the PTA agents, click **Pass-Through Authentication**, as shown in Figure 2-5. The maximum number of PTA agents per tenant is 40. The servers running PTA agents should also be treated and protected the same as you would protect a domain controller.



Passthrough Authentication

Microsoft Entra ID

We recommend that you have a minimum of 3 authentication agents running on your tenant. Learn more

Authentication Agent	IP	Status
PTAAgent02.corp.markmorowpta.com	76.146.28.167	✓

FIGURE 2-5 Pass-through authentication agent details

PTA should be used as an authentication choice if password hash sync cannot be used or if sign-in hour restrictions are required. Also, PTA is useful for a company trying to move away from federated authentication that doesn't want to move to password hash sync yet.

MORE INFO **PASS-THROUGH AUTHENTICATION**

You can learn more about the details of how PTA works at *https://aka.ms/SC900_PTADeepDive*.

Federation

This allows users to authenticate to Microsoft Entra ID resources using credentials provided by another identity provider (IdP). Active Directory Federation Services is installed and configured in the Microsoft Entra Connect setup when you choose the **Federation With AD FS** option. Also, a Web Application Proxy (WAP) server is installed to facilitate communication between the on-premises AD FS deployment and the Internet. The WAP should be located in the DMZ. The AD FS server should never be exposed to the Internet directly.

Federation is the most complicated identity authentication configuration. There are a few reasons why federated authentication to Microsoft Entra ID would be needed, and doing so should be the last choice when evaluating PHS, PTA, and federation.

Finally, AD FS servers should be protected and treated the same way as domain controllers. If an attacker could access the AD FS server, they could sign claims impersonating any user in the directory.

MORE INFO **CHOOSING THE RIGHT AUTHORIZATION METHOD FOR YOUR HYBRID IDENTITY**

If you are unsure which method is best for you, follow the decision tree located at *https://aka.ms/SC900_ChooseTheRightAuthN*.

EXAM TIP

Make sure to understand what a hybrid identity is and the associated components used in a hybrid identity configuration.

Describe Microsoft Entra identities (users, devices, groups, and workload identities)

Microsoft Entra identities comprise four main categories of identities: users, devices, groups, and workload identities, which can thought of as an application identity. All of these will be present in your Microsoft Entra tenant.

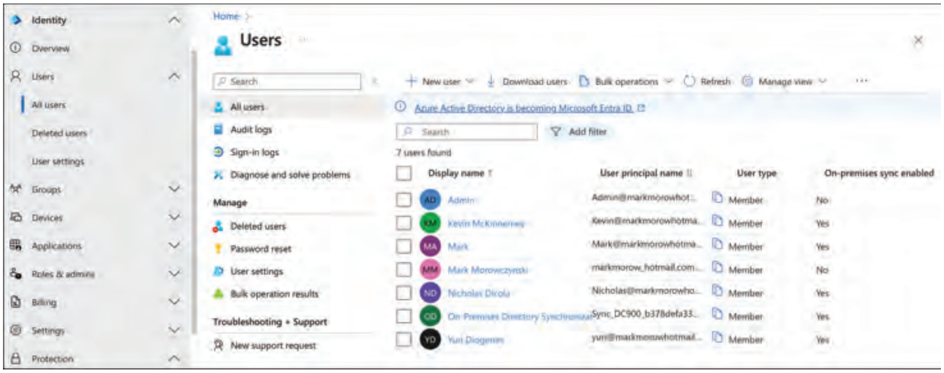
Users

User identities are typically connected to a person. You traditionally think of these identities when users authenticate to a resource. When someone starts working at a company, they are given a user identity to identify the user across various applications and services, such as O365 or external SaaS applications. User identities can be added to groups or distribution lists and hold administrative roles. Authorization decisions are made against user identities. User identities can be members of your organization or outside of your organization.

As covered in the “Describe what hybrid identity is” section, user identities are most typically synced from on-premises Active Directory via Microsoft Entra Cloud Sync or Microsoft Entra Connect. The user’s attributes, such as name, department, and office phone, can all be synced in Microsoft Entra Cloud Sync or Microsoft Entra Connect.

User identities can also be created directly in Microsoft Entra ID. An on-premises Active Directory is not needed. The population of additional user data, such as department, is still needed. Another system usually provides this as part of user onboarding. Both user identity types are shown in Figure 2-6.

NOTE **When the term *identity* is used, it most likely refers to a user identity.**



7 users found

Display name	User principal name	User type	On-premises sync enabled
Admin	Admin@markmorowhot...	Member	No
Kevin McKinnerney	Kevin@markmorowhotma...	Member	Yes
Mark	Mark@markmorowhotma...	Member	Yes
Mark Morowczynski	markmorow_hotmail.com...	Member	No
Nicholas Dicola	Nicholas@markmorowho...	Member	Yes
On-Premises Directory Synchronizat	Sync_DC900_b378defa33...	Member	Yes
Yuri Diogenes	yuri@markmorowhotmail...	Member	Yes

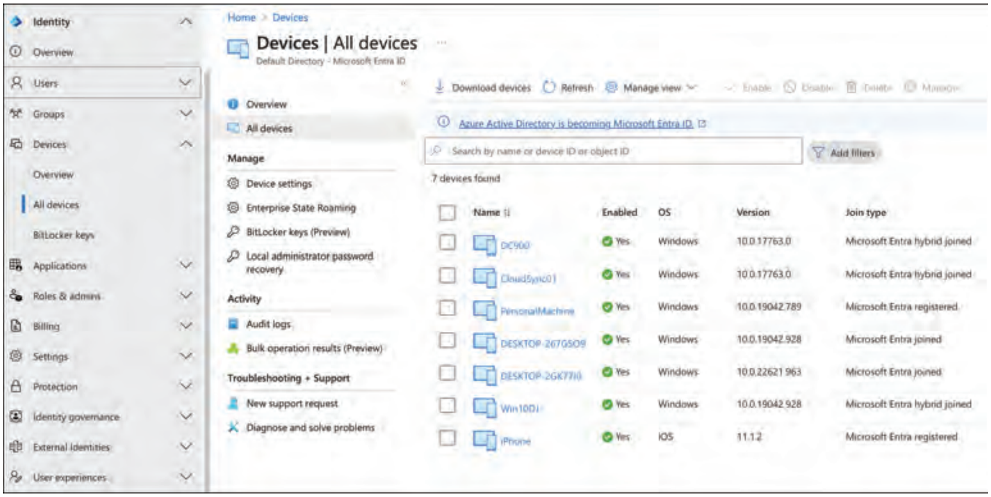
FIGURE 2-6 All users in Microsft Entra, including synced and cloud-only users

Devices

Devices also have an identity in Microsoft Entra. There are three types of device identities in Microsoft Entra ID, but we also included a fourth identity type, an on-premises device identity, so you have a complete picture of all device states you will encounter.

- **Domain–joined computer** First, we have a traditional domain-joined computer. This is usually a corporate-owned device joined to the on-premises Active Directory. The on-premises Active Directory account is used to sign-in. This is probably the device identity type you are the most familiar with because it has been used since Active Directory first arrived in Windows 2000.
- **Microsoft Entra Hybrid–joined device** Next, there is the Microsoft Entra Hybrid–joined device, which is where the device is domain-joined to Active Directory but also has an identity in Microsoft Entra. Typically, this identity is created through the Microsoft Entra Connect sync process when syncing computer accounts to Microsoft Entra ID. The account used to log in to the device is still an on-premises Active Directory account. However, because this device has an identity in Microsoft Entra ID, this can be used as part of the conditional access controls. It also gives users a better user experience by reducing prompts for Microsoft Entra ID–backed applications.
- **Microsoft Entra–joined** Microsoft Entra–joined devices are directly joined to Microsoft Entra ID. Instead of being domain-joined to on-premises Active Directory, it's joined directly to Microsoft Entra ID. Microsoft Intune applies policy and manages the Microsoft Entra–joined device. With a Microsoft Entra–joined device, the Microsoft Entra account is used to log in. A device cannot be domain joined to both Active Directory and Entra ID at the same time.
- **Microsoft Entra–registered** Typically, this is a personal device, such as a mobile phone or a personally owned computer. This is mostly used for BYOD scenarios where some corporate resources are needed, but a device is not provided. Microsoft Intune is used to provide some light management capabilities. A local account, perhaps a

Microsoft account, is used to log in rather than a corporate Active Directory or Microsoft Entra account. Microsoft Entra–joined, Microsoft Entra hybrid–joined, and Microsoft Entra–registered can all be seen in the **Devices** section of the Microsoft Entra admin center, as shown in Figure 2-7.



7 devices found

□	Name	Enabled	OS	Version	Join type
□	DC900	Yes	Windows	10.0.17763.0	Microsoft Entra hybrid joined
□	CloudSync01	Yes	Windows	10.0.17763.0	Microsoft Entra hybrid joined
□	PersonalMachine	Yes	Windows	10.0.19042.789	Microsoft Entra registered
□	DESKTOP-267GSO9	Yes	Windows	10.0.19042.928	Microsoft Entra joined
□	DESKTOP-2GK77I0	Yes	Windows	10.0.22621.963	Microsoft Entra joined
□	Win10DJ	Yes	Windows	10.0.19042.928	Microsoft Entra hybrid joined
□	iPhone	Yes	iOS	11.1.2	Microsoft Entra registered

FIGURE 2-7 All devices in Microsoft Entra ID

Groups

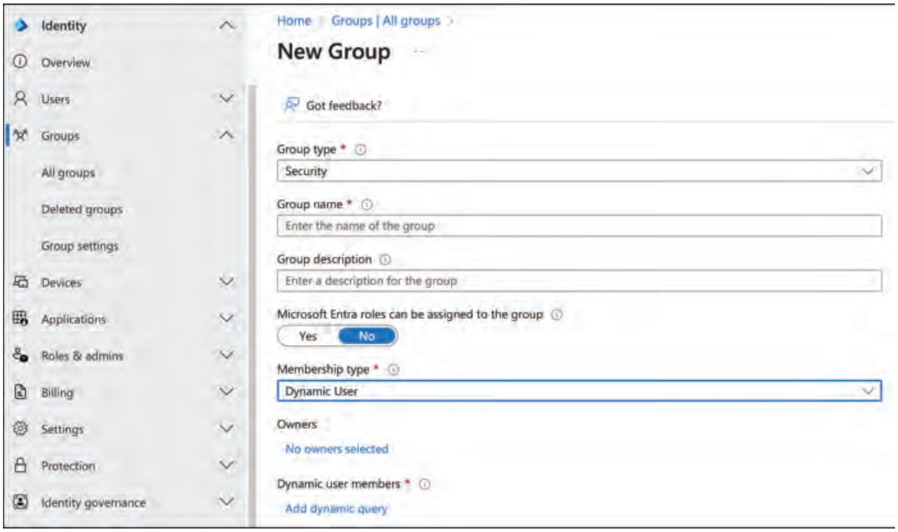
Groups are a collection of users or devices. They are used to specify an action or apply a policy on many of these objects at once instead of doing it individually. For example, if we want to grant everyone in the sales department access to a sales application, we can assign the sales group instead of assigning each member individually. We can also apply licenses to the group; all members will receive the license assignment. This allows the admin to take actions at a greater scale.

There are several types of groups that you can use in Azure AD:

- You can sync your on-premises groups from Active Directory for use as a security group.
- You can also create a Microsoft Entra security group where the membership is assigned directly to the group.
- The group can also be made to be of a dynamic membership. This means membership will be automatically populated based on the user's attributes or the device you want in the group.

The different group types and membership types are shown in Figure 2-8.

Using the previous sales team example, a dynamic group could be made where when the `department` equals `Sales`, which means they are automatically in the group (see Figure 2-9). These dynamic groups are constantly reevaluating and adding and removing members. The automation that can be built around dynamic groups is tremendous.



New Group

Group type * : Security

Group name * : Enter the name of the group

Group description : Enter a description for the group

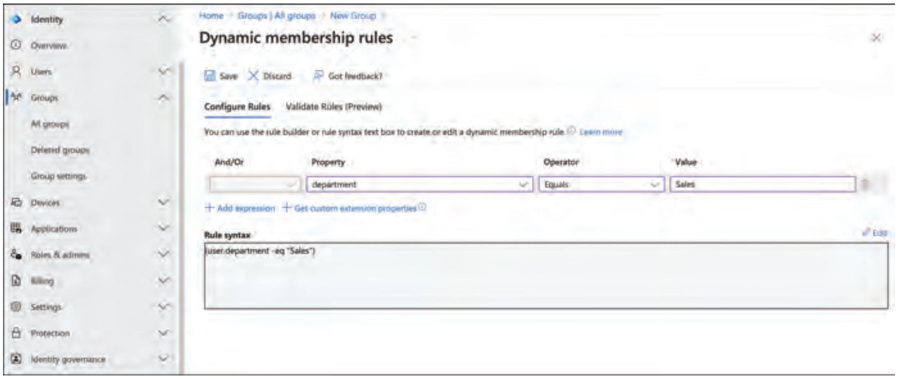
Microsoft Entra roles can be assigned to the group : Yes [✓ No]

Membership type * : Dynamic User

Owners : No owners selected

Dynamic user members * : Add dynamic query

FIGURE 2-8 New Group creation



Dynamic membership rules

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. Learn more

And/Or	Property	Operator	Value
	department	Equals	Sales

Rule syntax

```
(user.department -eq "Sales")
```

FIGURE 2-9 Dynamic Membership Rules

Microsoft 365 groups—sometimes called unified groups—are newer group types representing the future direction for resource permissions in Microsoft 365, such as Teams, SharePoint, and Exchange Online. One group can be used to ensure consistent access with minor administrative effort across the Microsoft 365 suite of applications.

Workload identities

Nobody logs into anything for the fun of it. Users log in to do something important to them, such as send an email, check their paystub, or access a line-of-business application. Applications are the day-to-day drivers for users, and many applications exist in Microsoft Entra ID. These will sometimes be referred to as a *workload identity*. There is no industry standard for this term; depending on the context, they can discuss a few different things. This can refer to an application, a service principal, a specific instance of an application, or a managed identity, a special type of service principal. All three of these will be covered in this section.

As described earlier, Microsoft Entra ID supports open standards such as SAML, OAuth, and OpenID Connect. Any applications that support these protocols can be integrated into Microsoft Entra ID. Microsoft Entra ID also has an Application Gallery where Microsoft has worked with these different application providers to make the setup as easy as possible. The Application Gallery can be seen in Figure 2-10. Microsoft Entra ID can also work with your on-premises web applications using Microsoft Entra Application Proxy, as described in the "Describe what Microsoft Entra ID is" section later in this chapter.

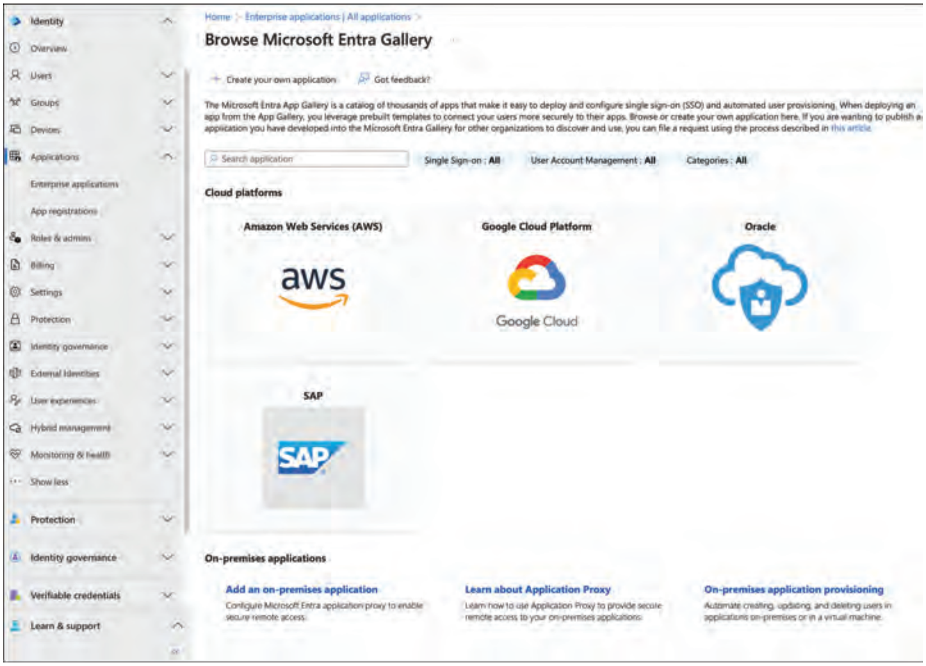
MORE INFO **MODERN AUTHENTICATION**

To learn more about modern authentication, watch the Bailey, Bercik, and Mark Morowczynski session at Defcon Blue Team Village Modern Authorization for the Security Admin at *https://aka.ms/SC900_ModernAuthBTV*.

Line-of-business applications can also be updated to use Microsoft Entra authentication. Because Microsoft Entra ID supports open standards, any language that has a library for SAML, OAuth, or OpenID Connect can integrate with Microsoft Entra ID. Microsoft also has the MSAL library to simplify authentication for many common languages, such as .NET, ASP.NET, Node.js, Java, Python, iOS, macOS, Android, and Xamarin.

MORE INFO **MSAL LIBRARIES**

To learn more about the MSAL libraries available, see *https://aka.ms/SC900_MSAL*.



Browse Microsoft Entra Gallery

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates to connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish a application you have developed into the Microsoft Entra Gallery for other organizations to discover and use, you can file a request using the process described in this article.

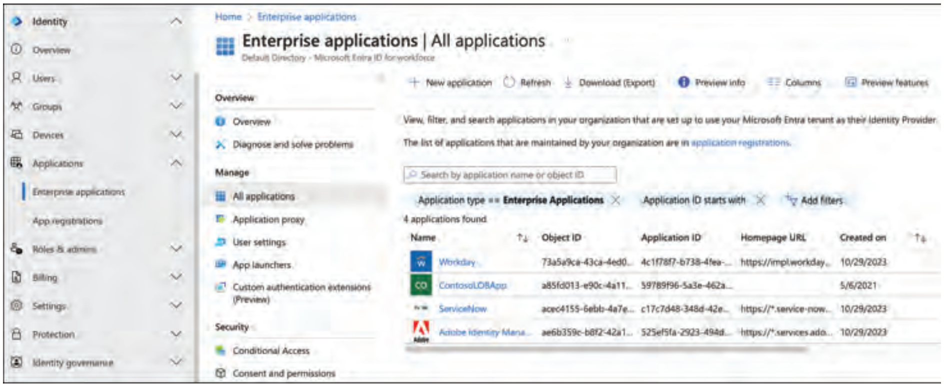
Add an on-premises application
Configure Microsoft Entra application proxy to enable secure remote access.

Learn about Application Proxy
Learn how to use Application Proxy to provide secure remote access to your on-premises applications.

On-premises application provisioning
Automate creating, updating, and deleting users in applications on-premises or in a virtual machine.

FIGURE 2-10 Microsoft Entra application gallery

Application identities can be seen in the Enterprise Apps section of the Microsoft Entra admin center, as shown in Figure 2-11. These are called *service principals*. These define the access policy and permissions for the application insofar as what it can do in the tenant. There is a lot of developer detail beyond the scope of this exam, but here is a real-world example: When applying a conditional access policy, such as requiring users to complete MFA before accessing an application, you apply a conditional access policy to a service principal. These are automatically added to the tenant when you integrate an application from the Application Gallery, consent to an application, or add an app proxy application.



View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

The list of applications that are maintained by your organization are in application registrations.

4 applications found

Name	Object ID	Application ID	Homepage URL	Created on
Workday	73a5a9ca-43ca-4ed0...	4c1f78f7-b738-4fea-...	https://impl.workday...	10/29/2023
ContosoLOBApp	a85fd013-e90c-4a11...	59789f96-5a3e-462a...		5/6/2021
ServiceNow	acec4155-6ebb-4a7e...	c17c7d48-348d-42e...	https://*.service-now...	10/29/2023
Adobe Identity Mana...	ae6b359c-b8f2-42a1...	525ef5fa-2923-494d...	https://*.services.ado...	10/29/2023

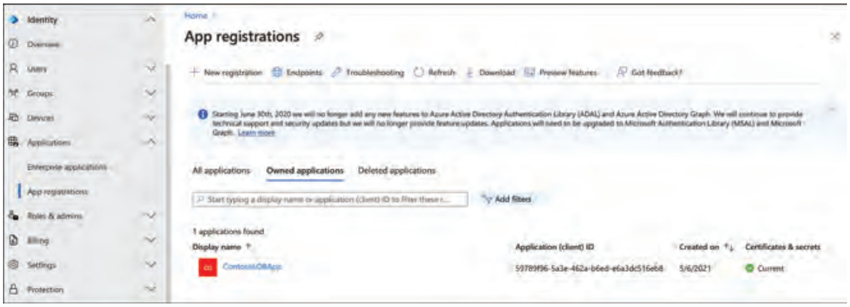
FIGURE 2-11 Microsoft Entra Enterprise Applications

A second type of service principal is called a *managed identity*. This is typically for developers, but it can really be used by anyone managing Azure resources that access Microsoft Entra authentication. The idea is that no credential management needs to be done for the application. Without managed identities, a developer would need to rotate either a shared secret (a password for an application) or a certificate at regular intervals. These credentials need to be protected as well. With a managed identity, the service handles the storage and rotation.

MORE INFO **MICROSOFT ENTRA MANAGED IDENTITIES**

To learn more about Managed Identities, see *https://aka.ms/ManagedIdentities*.

The final type of application identity is the application object created by application registration. This configures the application to use Microsoft Entra identities for authentication (in your tenant or by other people's Microsoft Entra tenants if you choose to allow that) and results in an application object being created in Microsoft Entra ID. Things like the application uniform resource identifier (URI) and application permissions are defined in this object. Every application object (created through the Azure portal or by using the Microsoft Graph APIs or the Azure AD PS Module) also creates a corresponding service principal object that inherits certain properties from that application object. This is located in a tenant, but it would not be in your tenant unless it were an application your company was developing (see Figure 2-12).



Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

1 applications found

Display name	Application (client) ID	Created on	Certificates & secrets
CO ContosoLOBApp	59789f96-5a3e-462a-b6ed-e6a3dc516eb8	5/6/2021	Current

FIGURE 2-12 Microsoft Entra Application Registration

Putting it all together with a few examples should clarify what administrators see in the portal. Contoso is using Office 365. There will be a service principal for Office 365 Exchange online, Office 365 SharePoint online, and so on in their Enterprise Apps. No application registration for those applications occurs. The application registration will happen in the Microsoft tenant, not the Contoso tenant. The only thing Contoso would see is the service principal in Enterprise Applications. This applies to any application added from the gallery or that is manually added. Contoso is moving its line-of-business application to leverage Microsoft Entra authentication. In this scenario, there would be an object for this line-of-business application in the Application Registrations section and a service principal object in the Enterprise Applications section.

MORE INFO **MICROSOFT ENTRA APPLICATIONS AND SERVICE PRINCIPALS**

To learn more about Microsoft Entra applications and service principals, see *https://aka.ms/SC900_ME-IDAppObjects*

Skill 2.2: Describe the authentication capabilities of Microsoft Entra ID

This objective deals with the authentication capabilities of Microsoft Entra ID. You will learn how you can prevent users from using weak passwords in your Microsoft Entra ID and Active Directory. Then, we'll focus on multifactor authentication—what it means, and what methods are available for users. Finally, we'll discuss passwordless and phishing-resistant authentication methods such as Hello for Business, certificate-based authentication, FIDO2, and the authenticator app, which significantly increase both security and the user experience.

This skill covers:

- Authentication methods, including passwords MFA
- Learn about password protection and management
- Multifactor authentication methods
- Learn about passwordless credentials, which provide the best balance between user experience and security

Index