



Microsoft

# Microsoft Security, Compliance, and Identity Fundamentals



Exam Ref **SC-900**

Yuri Diogenes  
Nicholas DiCola  
Kevin McKinnerney  
Mark Morowczynski

FREE SAMPLE CHAPTER



# Exam Ref SC-900

# Microsoft Security,

# Compliance, and Identity

# Fundamentals

Yuri Diogenes  
Nicholas DiCola  
Kevin McKinnerney  
Mark Morowczynski

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

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

Copyright © 2022 by Pearson Education, Inc.

All rights reserved. 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.pearson.com/permissions](http://www.pearson.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: 978-0-13-756810-9

ISBN-10: 0-13-756810-X

Library of Congress Control Number: 2021946889

ScoutAutomatedPrintCode

## **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](mailto:corpsales@pearsoned.com) or (800) 382-3419.

For government sales inquiries, please contact [governmentsales@pearsoned.com](mailto:governmentsales@pearsoned.com).

For questions about sales outside the U.S., please contact [intlcs@pearson.com](mailto:intlcs@pearson.com).

## **CREDITS**

EDITOR-IN-CHIEF

Brett Bartow

EXECUTIVE EDITOR

Loretta Yates

DEVELOPMENT EDITOR

Rick Kughen

SPONSORING EDITOR

Charvi Arora

MANAGING EDITOR

Sandra Schroeder

SENIOR PROJECT EDITOR

Tracey Croom

COPY EDITOR

Rick Kughen

INDEXER

Ken Johnson

PROOFREADER

Abigail Manheim

TECHNICAL EDITOR

Mark Simos

EDITORIAL ASSISTANT

Cindy Teeters

COVER DESIGNER

Twist Creative, Seattle

COMPOSITOR

codeMantra

# Pearson's Commitment to Diversity, Equity, and Inclusion

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

Our ambition is to purposefully contribute to a world where:

- Everyone has an equitable and lifelong opportunity to succeed through learning.
- Our educational products and services are inclusive and represent the rich diversity of learners.
- Our educational content accurately reflects the histories and experiences of the learners we serve.
- Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview).

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

- Please contact us with concerns about any potential bias at <https://www.pearson.com/report-bias.html>.

# Contents at a glance

<i>Acknowledgments</i>	<i>xi</i>	
<i>About the authors</i>	<i>xiii</i>	
<i>Introduction</i>	<i>xv</i>	
<b>CHAPTER 1</b>	<b>Describe the concepts of security, compliance, and identity</b>	<b>1</b>
<b>CHAPTER 2</b>	<b>Microsoft Identity and Access Management Solutions</b>	<b>25</b>
<b>CHAPTER 3</b>	<b>Capabilities of Microsoft security solutions</b>	<b>73</b>
<b>CHAPTER 4</b>	<b>Describe the capabilities of Microsoft compliance solutions</b>	<b>143</b>
<i>Index</i>	<i>187</i>	

# Contents

<b>Introduction</b>	<b>xv</b>
<i>Organization of this book</i>	xv
<i>Preparing for the exam</i>	xv
<i>Microsoft certification</i>	xvi
<i>Errata, updates &amp; book support</i>	xvi
<i>Stay in touch</i>	xvii
<b>Chapter 1    Describe the concepts of security, compliance, and identity</b>	<b>1</b>
Skill 1-1: Security and compliance concepts and methodologies .....	1
Zero-trust methodology	1
Shared responsibility model	5
Defense-in-depth	7
Common threats	9
Encryption	10
Cloud Adoption Framework	12
Skill 1-2: Identity concepts.....	12
Identity as the primary security perimeter	13
What is authentication?	13
What is authorization	15
What is Active Directory?	17
What are federation services and identity providers?	18
Common identity attacks	20
Thought experiment.....	21
Thought experiment answers .....	22
Chapter summary .....	22
<b>Chapter 2    Microsoft Identity and Access Management Solutions</b>	<b>25</b>
Skill 2-1: Define the basic identity services and identity types of Azure AD .....	25
Describe what Azure Active Directory is	25

Describe what hybrid identity is	28
Describe Azure AD identities (users, devices, groups, and service principals/applications)	33
Describe the different external identity types (guest users)	39
Skill 2-2: Describe the authentication capabilities of Azure AD.....	41
Describe the different authentication methods	41
Describe password protection and management capabilities	42
Describe self-service password reset	44
Describe multifactor authentication	48
Describe Windows Hello for Business and passwordless credentials	50
Skill 2-3: Describe the access management capabilities of Azure AD .....	54
Describe what conditional access is	54
Describe uses and benefits of conditional access	55
Describe the benefits of Azure AD roles	58
Skill 2-4: Describe the identity protection and governance capabilities of Azure AD .....	63
Describe what identity governance is	63
Describe what entitlement management and access reviews are	64
Describe the capabilities of PIM	67
Describe Azure AD Identity Protection	68
Thought experiment.....	70
Thought experiment answers .....	71
Chapter summary .....	71

<b>Chapter 3 Capabilities of Microsoft security solutions</b>	<b>73</b>
Skill 3-1: Basic security capabilities in Azure .....	73
Azure network security groups	74
Azure DDoS protection	77
Azure Firewall	78
Azure Bastion	80
Web Application Firewall	81
Data encryption in Azure	83

Skill 3-2: Security Management capabilities in Azure .....	84
Microsoft Defender for Cloud	85
Azure Secure Score	87
Cloud workload protection with Defender for Cloud Plans	88
Cloud security posture management capabilities	91
Security baselines for Azure	93
Skill 3-3: Security capabilities in Microsoft Sentinel .....	94
What is Security Information and Event Management (SIEM)?	95
What is security orchestration, automation, and response (SOAR)?	98
What is extended detection and response (XDR)?	99
Microsoft Sentinel	99
Skill 3-4: Threat protection with Microsoft 365 Defender .....	115
Describe Microsoft 365 Defender services	115
Describe Microsoft Defender for Identity	116
Describe Microsoft Defender for Office 365	117
Describe Microsoft Defender for Endpoint	119
Describe Microsoft Cloud App Security	123
Skill 3-5: Security management capabilities of Microsoft 365.....	124
Describe the Microsoft 365 Security Center	125
Describe how to use Microsoft Secure Score	126
Explore security reports and dashboards	128
Describe incidents and incident management capabilities	129
Skill 3-6: Endpoint security with Microsoft Intune.....	134
What is Intune?	134
Endpoint security with Intune and Microsoft Endpoint Manager admin center	136
Thought experiment.....	138
Thought experiment answers .....	139
Chapter summary .....	140

<b>Chapter 4</b>	<b>Describe the capabilities of Microsoft compliance solutions</b>	<b>143</b>
Skill 4-1:	Common compliance needs .....	143
	Microsoft Compliance Center	144
	Microsoft Compliance Manager	148
	Compliance Score	151
Skill 4-2:	Information protection and governance .....	153
	Data classification capabilities	153
	Content Explorer and Activity Explorer	155
	Sensitivity labels	156
	Retention policies and labels	158
	Records management	159
	Data loss prevention	160
Skill 4-3:	Insider risk.....	162
	Insider risk management	163
	Communication compliance	164
	Information barriers	166
	Privileged access management	167
	Customer Lockbox	167
Skill 4-4:	eDiscovery .....	168
	Microsoft 365 eDiscovery	169
	Content Search	169
	Core eDiscovery Workflow	170
	Advanced eDiscovery workflow	173
Skill 4-5:	Auditing.....	174
	Microsoft 365 audit capabilities	174
	Advanced Audit	176
Skill 4-6:	Resource governance .....	177
	Azure resource locks	178
	Azure Blueprints	178
	Azure Policy	179
	Cloud Adoption Framework	180

Thought experiment .....	183
Thought experiment answers .....	184
Chapter summary .....	184

*Index*

187



# 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** 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 co-authors 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** would like to thank: My wife and three children for supporting me while working on this book and my co-authors 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** 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 co-authors 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** would like to thank: My parents for being the most loving parents that 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 co-manager. 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 am hopeful that 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 (Utica College) and is the principal program manager of Microsoft’s CxE Defender for Cloud, where he primarily helps customers onboard and deploy Microsoft Defender for Cloud as part of their security operations/incident response. Yuri has been working for Microsoft since 2006 in different positions, including five years as senior support escalation engineer for the CSS Forefront Edge team, and from 2011 to 2017 for the content development team, where he also helped create the Azure Security Center content experience since its GA launch in 2016. Yuri has published a total of 26 books, mostly about information security and Microsoft technologies. Yuri also holds an MBA and many IT/Security industry certifications, such as CISSP, E|CND, E|CEH, E|CSA, E|CHFI, CompTIA Security+, CySA+, Cloud Essentials Certified, Mobility+, Network+, CASP, CyberSec First Responder, MCSE, and MCTS. You can follow Yuri on Twitter at @yuridiogenes.

## **NICHOLAS DICOLA**

Nicholas is a partner director at Microsoft on the Cloud Security Customer Experience Engineering (CxE) team, where he leads this global team helping customers with deployments of Azure Security products. 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 and technical lead on the Microsoft Information Protection Customer Experience Engineering (CxE) Team, where he provides best practices and deployment guidance to help customers quickly onboard Microsoft information protection products and Azure Purview. Kevin has been working at Microsoft since 2011 in various roles, including senior support escalation engineer on the Microsoft CSS Security team and as a senior premier field engineer, focusing on Microsoft security and information protection. Kevin has authored dozens of blogs and videos related to information protection 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 GitHub (<https://github.com/kemckinnmsft>).

### **MARK MOROWCZYNSKI**

Mark Morowczynski (@markmorow) is a principal program manager on the customer success team in the Microsoft Identity division. He spends most of his time working with customers on their deployments of Azure Active Directory. Previously, he was a premier field engineer supporting Active Directory, Active Directory Federation Services, and Windows Client performance. He was also one of the founders of the AskPFEPlat blog. He's spoken at various industry events such as Black Hat 2019, Defcon Blue Team Village, GrayHat, several BSides, Microsoft Ignite, Microsoft Inspire, Microsoft MVP Summits, The Experts Conference (TEC), The Cloud Identity Summit, SANs Security Summits, and TechMentor. He can be frequently found on Twitter as @markmorow, where he argues about baseball and sometimes makes funny gifs.

# Introduction

---

The SC-900 exam is targeted to 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 for a broad audience that includes business stakeholders, new or existing IT professionals, or students who have an interest in Microsoft security, compliance, and identity solutions. This exam covers topics such 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 found on the exam, but it 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](http://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 Learning website: <http://aka.ms/examlist>. 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. If an exam covers six major topic areas, for example, 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 that you augment 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 <http://microsoft.com/learn>. Microsoft official practice tests are available for many exams at <http://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 certification

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/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/ExamRefSC900/errata](http://MicrosoftPressStore.com/ExamRefSC900/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](http://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 <http://support.microsoft.com>.

## **Stay in touch**

---

Let's keep the conversation going! We're on Twitter: <http://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:

- Define the basic identity services and identity types of Azure AD
- Describe the authentication capabilities of Azure AD
- Describe access management capabilities of Azure AD
- Describe the identity protection and governance capabilities of Azure AD

## **Skill 2-1: Define the basic identity services and identity types of Azure AD**

---

This objective deals with the fundamental concepts of Azure Active Directory. In this section, you'll learn what Azure Active Directory is and its key enterprise features. You'll also learn about internal and external identities, and you'll also learn about hybrid identity and the different ways to authenticate to Azure Active Directory. This skill provides the building blocks of Azure Active Directory.

### **Describe what Azure Active Directory is**

Azure Active Directory is Microsoft's cloud-based Identity-as-a-Service (IDaaS) offering. It is an Identity and Access Management (IAM) product with 200,000 customers (corporations/business entities), 425 million monthly active users, and 30 billion authentications processed each day! 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 Azure Active Directory.

## Applications

Azure Active Directory 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 Azure AD Application Gallery has thousands of pre-integrated applications to make 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 Azure Active Directory yourself, or you can request that it be added to the gallery.

### **MORE INFO ADDING APPLICATIONS TO THE AZURE ACTIVE DIRECTORY APPLICATION GALLERY**

You can request applications to be added to the Application Gallery here: [https://aka.ms/SC900\\_AddToAAADAppGallery](https://aka.ms/SC900_AddToAAADAppGallery).

## 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 Azure AD. 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 the same way.

## Authentication

Skill 2-2 is focused on the authentication aspects of Azure Active Directory, such as password hash sync (PHS), pass-through authentication (PTA), federation, self-service password reset (SSPR), multifactor authentication (MFA), Windows Hello for Business, and Azure AD Password Protection.

## Access management

Skill 2-3 is focused on the access management aspects of Azure Active Directory, 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. There are also many different Azure Active Directory roles that can be assigned to administrators to follow the principle of least privilege while also granting the necessary access to perform the tasks they need to perform.

## Devices

Intune is the primary device management platform for cloud-based devices, but there are device objects in Azure Active Directory that are Azure AD-registered, hybrid Azure

AD-joined, or Azure AD-joined. We'll cover hybrid Azure AD-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 Azure AD, but the traditional management you think of with group policy Objects (GPOs) is performed from Intune. However, there is a tight relationship between Azure Active Directory and Intune.

## Domain services

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

## External identities

Azure Active Directory enables easy collaboration with other companies using Azure AD Business-to-Business (B2B) that are sharing resources like documents or accessing 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 Azure Active directory. Both Azure AD B2B and Azure AD B2C support conditional access.

## Governance

Skill 2-4 is focused on the governance aspects of Azure Active Directory. These features include Access Reviews and Entitlement Management. The primary focus of governance is to determine which users should have access to which resources. The governance process also needs to be auditable to verify that it is working.

## Reporting

Various log sources are available, including directory changes in audit logs to sign-in logs for both interactive and non-interactive events. Azure AD also includes logs for applications and managed-service identities, which are a specific type of application identity. These can all be accessed in the Azure Active Directory portal or exported to Log Analytics, Microsoft Sentinel, or any other SIEM.



### EXAM TIP

Remember what the different features are used for Azure AD and which problems they solve for a company.

## Licensing

Azure Active Directory has three levels of licensing:

- **Azure AD Free** Azure AD Free provides user and group management, as well as directory sync. This is included when you sign up for Office 365 or Microsoft 365 resources.
- **Azure Active Directory Premium 1** This level is where most of the features discussed in this chapter are included. This includes conditional access, self-service password reset with writeback, dynamic groups, and much more.
- **Azure Active Directory Premium 2** This level includes governance capabilities, such as access reviews, entitlement management, and privilege identity management. It also includes identity protection advanced security features.

### MORE INFO AZURE ACTIVE DIRECTORY FEATURES BY LICENSE

For a detailed breakdown of what features are included in each license level, see [https://aka.ms/SC900\\_AADLicensing](https://aka.ms/SC900_AADLicensing).



### EXAM TIP

Remember which features are part of Azure AD P2. The rest are included in Azure AD 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 Azure Active Directory accounts accessing only cloud resources. Most customers are in a hybrid-identity state with their Azure AD tenant(s) connected to an on-premises AD. This is where user accounts need to exist in both the on-premises Active Directory and in Azure Active Directory. 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. If you want to leverage your existing Active Directory environment and take advantage of Azure Active Directory, you'll need to use a hybrid identity.

There are two distinct components to a hybrid identity setup:

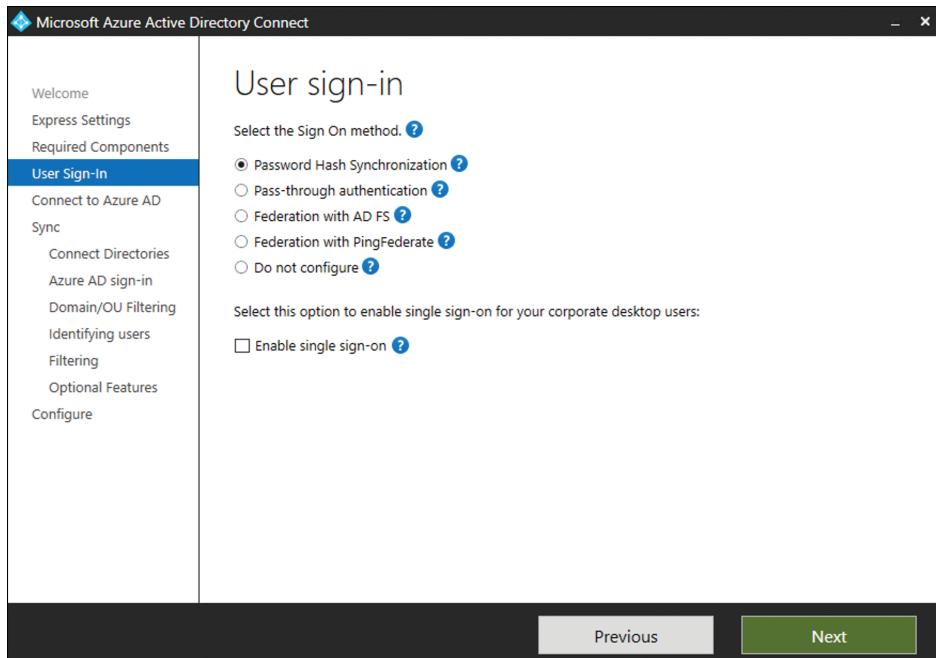
- Syncing of the users and their attributes from Active Directory to Azure Active Directory.
- Authenticating to Azure Active Directory using credentials from on-premises Active Directory. This can be accomplished via PHS, PTA, or federation.

### AZURE ACTIVE DIRECTORY CONNECT

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

Azure AD Connect has a very robust setup wizard to help you with this process. You use the express setup, which will 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 Azure Active Directory (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 Azure Active Directory, as shown in Figure 2.1.



**FIGURE 2-1** User sign-in options

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

#### MORE INFO AZURE ACTIVE DIRECTORY CONNECT

You can read more about customizing the Azure AD Connect Sync at [https://aka.ms/SC900\\_AADConnectCustomize](https://aka.ms/SC900_AADConnectCustomize).

#### PASSWORD HASH SYNCHRONIZATION

The current credentials in on-premises Active Directory are synced to Azure AD through Azure AD Connect. The on-premises password itself is never sent to Azure Active Directory but the password hash. The hashes stored in Azure Active Directory are completely different than the hashes in on-premises Active Directory. Active Directory password hashes are MD4, and Azure

Active Directory password hashes are SHA256. The user authenticates to Azure Active Directory by entering the same password they use on-premises. For the detailed cryptographic specifics on how this process works, see the More Info item below.

#### MORE INFO AZURE ACTIVE DIRECTORY CONNECT PASSWORD HASH SYNC DETAILS

You can read more about the Azure AD Connect Sync Password Hash Sync at <http://aka.ms/aadphs>.

You can also select password hash sync as an optional feature in Azure AD Connect if you are using PTA or federation as your primary authentication method, as seen in Figure 2.2. This gives you two benefits:

- Azure Active Directory 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 still access cloud resources when the full disaster recovery plan is being executed.

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

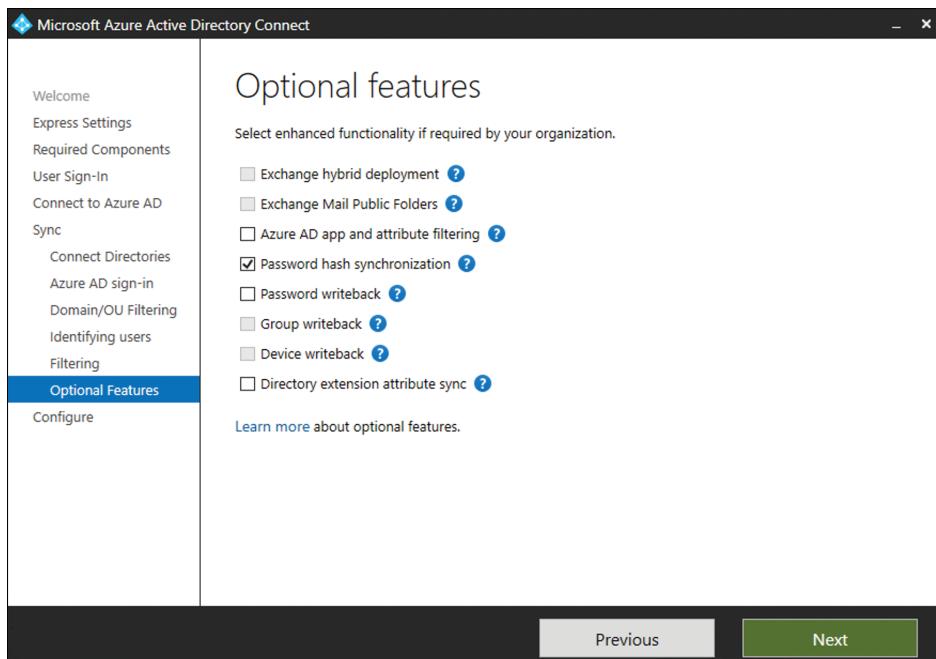


FIGURE 2-2 Password hash synchronization

## PASS-THROUGH AUTHENTICATION

With pass-through authentication, the user's password is validated against the on-premises Active Directory using PTA agents. When a user goes to authentication to Azure AD, the username and password are encrypted and put into a queue. The on-premises PTA agent reaches outbound to Azure AD, picks up the request, decrypts the username and password, and then validates it against Active Directory. It then returns to Azure AD if the authentication was 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 Azure Active Directory in any form for PTA authentication to work. However, PHS can be enabled as an optional feature.

The first PTA agent is usually installed on the Azure AD Connect server. 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 Azure AD Connect page in the Azure AD Portal shown in Figure 2-3.

The screenshot shows the Azure AD Connect interface for the 'Default Directory'. On the left, there's a navigation menu with items like 'Users', 'Groups', 'External Identities', etc., and 'Azure AD Connect' which is currently selected. The main content area has two sections: 'PROVISION FROM ACTIVE DIRECTORY' and 'USER SIGN-IN'. Under 'PROVISION FROM ACTIVE DIRECTORY', there's a section for 'Azure AD cloud sync' with a description and a link to 'Manage Azure AD cloud sync'. Below that is 'Azure AD Connect sync' with status information: Sync Status (Enabled), Last Sync (Less than 1 hour ago), and Password Hash Sync (Enabled). Under 'USER SIGN-IN', there are three options: 'Federation' (Disabled, 0 domains), 'Seamless single sign-on' (Disabled, 0 domains), and 'Pass-through authentication' (Enabled, 1 agent).

FIGURE 2-3 Pass-through authentication agent installed

To see the specific IPs of the PTA agents, click **Pass-Through Authentication**, as shown in Figure 2-4. 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.

## Pass-through authentication

Azure Active Directory

 [Download](#)
 [Troubleshoot](#)
 [Refresh](#)

Authentication Agent	IP	Status	Warnings
✓Default group for Pass-through Authentica...			
DC900.corp.contoso.com	73.35.191.191	Active	

**FIGURE 2-4** Pass-through authentication agent installed 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 that is trying to move away from federated authentication but 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](https://aka.ms/SC900_PTADeepDive).

## FEDERATION

This allows users to authenticate to Azure AD resources using credentials provided by another identity provider (IDP). In the Azure AD Connect set up, when you choose the **Federation With AD FS** option, Active Directory Federation Services is installed and configured. 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 few reasons why federated authentication to Azure AD would be needed, and doing so should be the last choice when evaluating PHS, PTA, and federation.

At the time of this writing, Smart Card authentication is not supported in Azure AD. If that is a core requirement, then you will need to use federation. If a custom MFA provider is needed that is not available in Azure AD, you will need to use federation for authentication.

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

### MORE INFO CHOOSING THE RIGHT AUTH 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](https://aka.ms/SC900_ChooseTheRightAuthN).



#### EXAM TIP

Make sure to understand what a hybrid identity is, as well as the associated components that are used in a hybrid identity configuration.

## Describe Azure AD identities (users, devices, groups, and service principals/applications)

Azure AD identities are made up of four main categories of identities: users, devices, groups, and applications. All of these will be present in your Azure AD tenant.

### USERS

User identities are typically connected to a person. These are the identities that you traditionally think of when users authenticate to a resource. When someone starts working at a company, they are given a user identity that is used 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 they can hold administrative roles. Authorization decisions are made against user identities. User identities can be members of your organization or outside of your organization, as will be discussed later in this skill.

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

User identities can also be created in Azure AD directly. An on-premises Active Directory is not needed. Population of additional user data, such as department, is still needed. This is usually provided by some other system as part of user onboarding. Both user identity types can be seen in Figure 2-5.

When the term identity is used, its most likely referring to a user identity.

The screenshot shows the 'All users (Preview)' page in the Azure Active Directory portal. The left sidebar includes links for 'All users (Preview)', 'Deleted users (Preview)', 'Password reset', 'User settings', 'Diagnose and solve problems', 'Activity' (with 'Sign-ins', 'Audit logs', and 'Bulk operation results'), 'Troubleshooting + Support' (with 'New support request'), and a 'Help' link. The main area displays a table of users with the following data:

Name	User principal name	User type	Directory synced
AD Admin	Admin@markmorowhot...	Member	No
KM Kevin McKinney	Kevin@markmorowhot...	Member	Yes
MA Mark	Mark@markmorowhot...	Member	Yes
MM Mark Morowczynski	markmorow_hotmail.c...	Member	No
ND Nicholas Dicola	Nicholas@markmoro...	Member	Yes
OD On-Premises Directory S...	Sync_DC900_b378defa...	Member	Yes
YD Yuri Diogenes	yuri@markmorowhot...	Member	Yes

FIGURE 2-5 All users in Azure AD, including synced and cloud-only users

## DEVICES

Devices also have an identity in Azure AD. There are three types of device identities in Azure AD, but we're including an on-premises device identity, so there is a complete picture for all device states that you will encounter.

- **Domain-joined computer** First, we have a traditional domain-joined computer. This is usually a corporate-owned device that is 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 and has been used since Active Directory first arrived in Windows 2000.
- **Hybrid Azure AD-joined device** Next, there is the hybrid Azure AD-joined device, which is where the device is domain-joined to Active Directory but also has an identity in Azure AD. Typically, this identity is created through the Azure AD Connect sync process when syncing computer accounts to Azure AD. The account that is used to log in to the device is still an on-premises Active Directory account. However, because this device has an identity in Azure AD, this can be used as part of the conditional access controls. It also gives users a better user experience by reducing prompts for Azure AD-backed applications.
- **Azure AD-joined** Azure AD-joined devices are directly joined to Azure AD. Instead of being domain-joined to on-premises Active Directory, it's joined directly to Azure AD. Intune is used to apply policy and manage the Azure AD-joined device. With an Azure AD-joined device, the Azure AD account is used to log in. A device cannot be domain joined to both Active Directory and Azure Active Directory at the same time.
- **Azure AD-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. Intune is used to provide some light management capabilities. A local account, perhaps a Microsoft account, is used to log in, not a corporate Active Directory or Azure Active Directory Account. Azure AD-joined, hybrid Azure AD-joined, and Azure AD-registered can all be seen in the **Devices** section of the Azure AD portal as shown in Figure 2-6.

Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant
PersonalMachine	Yes	Windows	10.0.19042.789	Azure AD registered	Mark	None	N/A
DESKTOP-267G...	Yes	Windows	10.0.19042.789	Azure AD joined	Mark	None	N/A
Win10DJ	Yes	Windows	10.0.19042.928	Hybrid Azure AD join...	N/A	None	N/A

FIGURE 2-6 All devices in Azure AD

## 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, and 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 to use as a security group.
- You can also create an Azure AD security group where the membership is assigned directly to the group.
- The group can also be made to be of a dynamic membership based on attributes on the user or the device.

The different group types and membership types are shown in Figure 2-7.

The screenshot shows the 'New Group' creation interface. At the top, there's a breadcrumb navigation: Home > Default Directory > Groups >. Below that is the title 'New Group' followed by a three-dot ellipsis. The form fields are as follows:

- Group type \***: A dropdown menu showing 'Security'.
- Group name \***: An input field with placeholder text 'Enter the name of the group'.
- Group description**: An input field with placeholder text 'Enter a description for the group'.
- Azure AD roles can be assigned to the group (Preview)**: A toggle switch with options 'Yes' and 'No', currently set to 'No'.
- Membership type \***: A dropdown menu showing 'Dynamic User'.
- Owners**: A section indicating 'No owners selected'.
- Dynamic user members \***: A section with a link 'Edit dynamic query'.

**FIGURE 2-7** New Group creation

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 2-8). These dynamic groups are constantly reevaluating and adding and removing members. The automation that can be built around dynamic groups is tremendous.

## Dynamic membership rules

X

[Save](#) [Discard](#) | [Got feedback?](#)[Configure Rules](#) [Validate Rules \(Preview\)](#)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	

[+ Add expression](#) [+ Get custom extension properties](#)**Rule syntax**[Edit](#)

(user.department -eq "Sales")

**FIGURE 2-8** Dynamic Membership Rules

Microsoft 365 groups—sometimes referred to as *unified groups*—is a newer group type and represents 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.

## APPLICATIONS

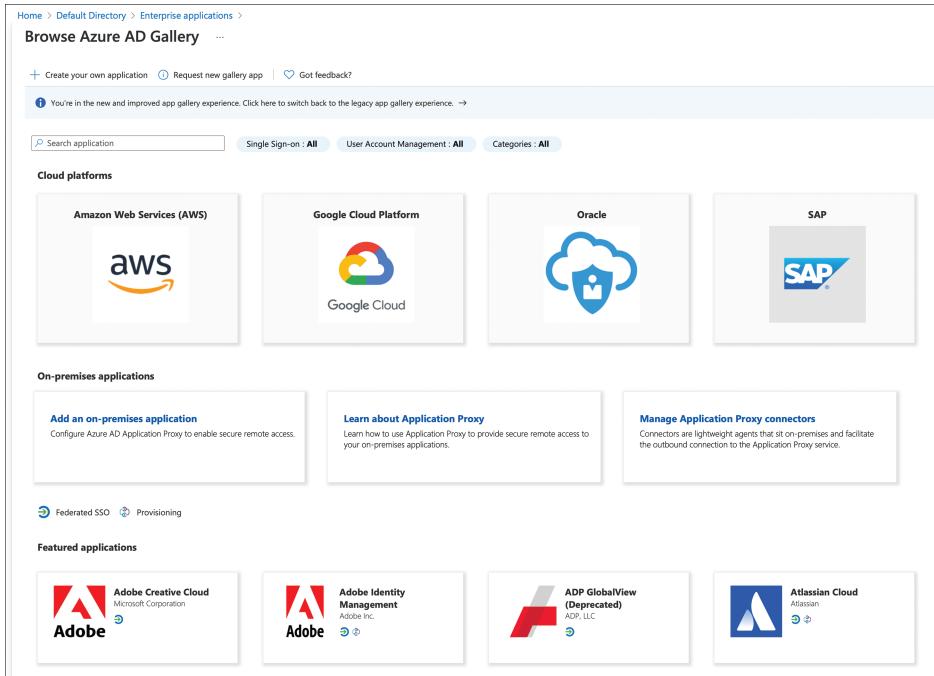
Nobody logs into anything for the fun of it. Users log in to do something important to them, such as send an email, check their paystub, or access a line-of-business application. Applications are the day-to-day drivers for users, and there are lots of applications in Azure AD.

As described earlier, Azure AD supports open standards such as SAML, OAuth, and OpenID Connect. Any applications that support these protocols can be integrated into Azure AD. Azure AD 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 2-9. Azure AD also can work with your on-premises web applications using Azure AD Application Proxy, as described earlier.

Line-of-business applications can also be updated to use Azure AD authentication. Because Azure AD supports open standards, any language that has a library for SAML, OAuth, or OpenID Connect can integrate with Azure Active Directory. Microsoft also has the MSAL library to simplify the authentication process 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](https://aka.ms/SC900_MSAL).



**FIGURE 2-9** Azure AD application gallery

Application identities can be seen in the Enterprise Apps section of the Azure AD portal, as shown in Figure 2-10. 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 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.

Name	Homepage URL	Object ID	Application ID
ContosoO365App		a85fd013-e90c-4a11-b9f4-cbd68b12d5f7	5978996_SaJe-462a-bf6d-e6a3dc516eb8
Office 365 Exchange Online	http://office.microsoft.com/outlook/	5446413c-e653-4553-b065-d63264b028b8	00000002-0000-0ff1-ce00-000000000000
Office 365 Management APIs		eb71157b-ddf1-46e6-8952-1ea91e3b03e7	c5393580-f805-4401-95e8-94b7afef2fc2
Office 365 SharePoint Online	http://office.microsoft.com/sharepoint/	30615b33-de3a-48b7-9634-fa7009819e90	00000003-0000-0ff1-ce00-000000000000
Outlook Groups		352debae-f31c-4ff1-aeca-e5ec9f03cd3b	925eb0d0-da50-4604-a19f-bd8de9147958
Skyline for Business Online		3e7c507f-1c78-4365-af71-8eec3e6901b2	00000004-0000-0ff1-ce00-000000000000

**FIGURE 2-10** Azure AD 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 Azure Active Directory authentication. The idea is that there 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 AZURE AD 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 Azure AD identities for authentication (in your tenant or by other people's Azure AD tenants if you choose to allow that) and results in an application object being created in Azure AD. Things like the application uniform resource identifier (URI) and permissions of the application 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 2-11).

The screenshot shows the Azure Active Directory portal with the 'App registrations' section selected. On the left, a sidebar lists various management categories like Overview, Preview features, and Diagnose and solve problems. The main area displays a table of registered applications. A single row is visible for 'ContosoDBApp', which has the following details:

Display name	Application (client) ID	Created on	Certificates & secrets
ContosoDBApp	5978996-5a3e-462a-b8ed-e6a3dc516eb8	5/6/2021	Current

FIGURE 2-11 Azure AD 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. There will *not* be an application registration for those applications. The application registration would be in the Microsoft tenant, not in 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 Azure AD 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 AZURE AD APPLICATIONS AND SERVICE PRINCIPALS**

To learn more about Azure AD applications and service principals, see [https://aka.ms/SC900\\_AADAppObjects](https://aka.ms/SC900_AADAppObjects).

## **Describe the different external identity types (guest users)**

Most companies' business models require them to work with external identities. This can be in the shape of business partners, distributors, suppliers, or vendors. Previously in this type of scenario, an external Active Directory forest would be used, and the business partner would be given a separate account in that forest. This presented a couple of challenges. First, because these identities were not the business partners' main corporate identities, they would frequently forget their passwords, which would increase help desk calls. Second, when this business partner would leave their company, they would still have an account in the external Active Directory forest unless a separate notification process had been set up (which is rare). The business partner would still be able to log in and access resources, even if they shouldn't be able to. Azure AD business-to-business (B2B) solves both issues.

Azure AD B2B focuses on enabling collaboration between companies. For example, let's consider an airline that designs and sources parts from many different companies. These business partners frequently need to work on a document or access other resources hosted by the airline. Azure AD B2B facilitates this collaboration and solves the two problems above by inviting their corporate identity into your tenant as a guest user, as shown in Figure 2-12. The only thing needed for this to work is the corporate entity's email. Access to resources in your tenant would be controlled just like it would for other users, including the ability to apply conditional access policies to these guest accounts. All authentication for the guest user takes place in their home directory. The airline would invite its supplier into their tenant to work on a document. Before the supplier company user could access the document, they would authenticate in their home tenant. If the authentication is successful and passed the Conditional Access requirements, the supplier would have access to whatever was granted to them in the airline company's tenant, which in this case, is the document.

This solves the first password problem because the supplier is using their current corporate credentials, not an additional account they must remember when they use it. Any password resets would need to take place in their home directory for their main corporate account, just like they would do today if they forgot their password. It also solves the second problem because if the partner left their company, their corporate account would be terminated. They would not be able to successfully authenticate and access any of your organization's resources.

## New user

Default Directory

[Got feedback?](#)

### Create user

Create a new user in your organization. This user will have a user name like alice@markmorowhotmail.onmicrosoft.com.  
[I want to create users in bulk](#)

### Invite user

Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.  
[I want to invite guest users in bulk](#)

[Help me decide](#)

#### Identity

Name (1)

Nicholas DiCola

Email address (\*) (1)

Nicholas@company.com

First name

Nicholas

Last name

DiCola

#### Personal message

Nicholas,

Super excited to work on this project with you. You should have access to the SharePoint site with all the documents to get started. Let's catch up next week once you are settled in.

-Mark

#### Groups and roles

Groups

0 groups selected

Roles

User

#### Settings

[Invite](#)**FIGURE 2-12** Azure AD B2B invite**MORE INFO B2B INVITE AND REDEMPTION**

To learn the different ways B2B users can redeem invitations, see [https://aka.ms/SC900\\_B2BRedemption](https://aka.ms/SC900_B2BRedemption).

# Index

## A

- access
  - ACL, 15
  - Azure AD, 26
  - conditional access policies, 54–58, 135, 138
  - privileged access management, 167
  - RBAC, 86
  - reviews, 65–67
- accounts (service), authorization, 16
- ACL (Access Control Lists), 15
- Activity Explorer, Microsoft Compliance Manager, 155–156
- AD (Active Directories), Azure
  - access
    - management, 26, 54–58
    - reviews, 65–67
  - applications (apps), 26
    - identities, 36–39
    - proxies, 26
  - authentication, 26, 41
    - MFA, 42
      - passwordless, 42
  - authorization, 16–17, 18
  - Azure Active Directory Connect, 28–29
  - Azure AD Free, 28
  - Azure AD Password Protection, 42
    - Azure AD integration, 44
    - Azure AD Premium 1, 28
    - Azure AD Premium 2, 28
    - custom banned lists, 43
    - scoring passwords, 44
  - B2B, 39–40, 41
  - B2C, 41
  - defined, 17–18, 25
  - devices
    - identities, 34
    - management, 26–27
  - domain services, 27
- entitlement management, 64–65
- FS, 32
- governance, 27
- hash synchronization, 29–30
- identity
  - device identities, 34
  - external identities, 27, 39–41
  - governance, 63–64
  - group identities, 35–36
  - hybrid identities, 28–33
  - Identity Protection, 68–70
  - managed identities, 38
  - user identities, 33
- Intune, 26–27
- licensing, 28
- MFA, 48–50
- PTA, 31–32
- reporting (logs), 27
- roles, 58–62
- SSPR, 44–48
- ADE (Azure Data Encryption), 83
- administrative roles, authentication, 15
- advanced auditing, Microsoft 365 Compliance Center, 176–177
- Advanced eDiscovery workflows, 173
- aggregating data/logs, SIEM, 95–96
- AIR (Automated Investigation and Remediation), 122
- alerts, insider risk management, 164
- allowed/blocked actions, records management, 159
- analytics
  - Analytics Rules, Azure Sentinel, 102–105
  - forensic analysis 97
  - SIEM, 96
  - UEBA, 108–109
- App Service, 84
- applications (apps)
  - Azure AD, 26

## **applications (apps)**

identities, 36–39  
Logic Apps, 113  
MCAS, 123–124  
Microsoft Intune, endpoint security, 134–136  
proxies, Azure AD, 26  
zero-trust methodology, 3, 5  
assessments, Microsoft Compliance Manager, 150  
attacks  
    botnets, 10  
    common identity attacks, 20–21  
    credential reuse, 20  
    data breaches, 10  
    DDoS attacks, 9–10, 78  
    DoS attacks, 9–10  
    eavesdropping attacks, 9  
    malware, 9  
    Microsoft Threat Intelligence, 80  
    MITM attacks, 10  
    MSDE, 119–122  
    MSDO, 115  
        policies, 118  
        threat tracking, 118–119  
    password sprays, 20–21  
    phishing attacks, 9, 21  
    port scanning attacks, 9  
    ransomware, 10  
auditing, Microsoft 365 Compliance Center  
    advanced auditing, 176–177  
    capabilities, 174–176  
    unified audit logs, 174  
authentication  
    ACL, 15  
    administrative roles, 15  
    Azure AD, 26, 41  
        MFA, 42  
        passwordless authentication, 42  
    common authentication methods, 14  
    defined, 13  
    factors of, 14  
    FIDO 2, 54  
    MFA, 42, 48–50  
    passwordless authentication, 42, 50–54  
    passwords, 44–47  
authorization, 16  
    Azure AD roles, 16–17, 18  
    defined, 15  
    least-privilege, 16–17  
    RBAC, 15–16  
    service accounts, 16

automation, Azure Sentinel, 111–113  
availability (CIA pillars), defense-in-depth, 7  
Azure Active Directory Connect, 28–29  
Azure AD  
    access  
        management, 26, 54–58  
        reviews, 65–67  
    applications (apps), 26  
        identities, 36–39  
        proxies, 26  
        authentication, 26, 41  
            MFA, 42  
            passwordless, 42  
        authorization, 16–17, 18  
        Azure Active Directory Connect, 28–29  
        Azure AD Free, 28  
        Azure AD Password Protection, 42  
            Azure AD integration, 44  
        Azure AD Premium 1, 28  
        Azure AD Premium 2, 28  
        custom banned lists, 43  
        scoring passwords, 44  
        B2B, 39–40, 41  
        B2C, 41  
        defined, 17–18, 25  
        devices  
            identities, 34  
            management, 26–27  
        domain services, 27  
        entitlement management, 64–65  
        FS, 32  
        governance, 27  
        hash synchronization, 29–30  
        identity  
            device identities, 34  
            external identities, 27, 39–41  
            governance, 63–64  
            group identities, 35–36  
            hybrid identities, 28–33  
            Identity Protection, 68–70  
            managed identities, 38  
            user identities, 33  
        Intune, 26–27  
        licensing, 28  
        MFA, 48–50  
        PTA, 31–32  
        reporting (logs), 27  
        roles, 58–62  
        SSPR, 44–48

Azure Bastion, 80–81  
 Azure Blueprints, 178–179  
 Azure Defender, 87–90  
 Azure Firewall, 78–80  
 Azure Key Vault, 83, 84  
 Azure Policy, 179–180  
 Azure Secure Score, 87–88  
 Azure Security Benchmark, 93–94  
 Azure Security Center, 85–87  
 Azure Sentinel, 94  
   Analytics Rules, 102–105  
   automation, 111–113  
   collect, 99–102  
   data connectors, 99–102  
   detection, 102–105  
   Entity Behavior, 108–109  
   Hunting, 109–111  
   Incidents, 105–106  
   investigate, 105–111  
   Investigation Graphs, 107  
   playbooks, 113  
   respond, 111–113  
   SIEM, 95–97  
   SOAR, 98  
   UEBA, 108–109  
   visualize, 114–115  
 Workbooks, 114–115  
 XDR, 99

## B

B2B (Business-to-Business) identities, 39–40, 41  
 B2C (Business-to-Consumers) identities, 41  
 banned password lists  
   Azure AD Password Protection, 44  
   custom, 43  
   global, 43  
 barriers, information, 166–167  
 baselines, Azure Security Benchmark, 93–94  
 basic DDoS protection, 77–78  
 Bastion, Azure, 80–81  
 benchmarks, Azure Security, 93–94  
 blocked/allowed actions, records management, 159  
 Blueprints, Azure, 178–179  
 botnets, 10  
 breaches, data, 10  
 Business, Windows Hello for, 50–54

## C

CEF (Common Event Format), 95–96  
 CIA pillars, defense-in-depth, 7  
 claims, defined, 19  
 classifying data  
   Microsoft Compliance Manager, 153–154  
   trainable classifiers, 154  
 Cloud Adoption Framework, 12, 180–183  
 cloud security  
   Azure Defender, 87–90  
   CSPM, 70, 91–93  
   CWPP, 87–90  
   MCAS, 123–124  
 common authentication methods, 14  
 common identity attacks, 20  
   credential reuse, 20  
   password sprays, 20–21  
   phishing attacks, 21  
 common threats, 9  
   botnets, 10  
   data breaches, 10  
   DDoS attacks, 9–10, 78  
   DoS attacks, 9–10  
   eavesdropping attacks, 9  
   malware, 9  
   MITM attacks, 10  
   phishing attacks, 9  
   port scanning attacks, 9  
   ransomware, 10  
 communication compliance, 164–166  
 compliance, 143  
   assessments, 150  
   communication compliance, 164–166  
   Microsoft 365 Compliance Center  
     Microsoft Compliance Manager, 148–153  
     navigating, 144–146  
     permissions, 146–148  
     rule groups, 148  
   Microsoft Compliance Manager, 148–149  
     Activity Explorer, 155–156  
     assessments, 150  
     compliance scores, 151–153  
     Content Explorer, 155  
     controls, 149–150  
     Data Classification page, 153–154  
     Improvement Actions, 150–151  
     label activities, 156  
     Overview page, 149

## compliance

scores, 151–153  
templates, 150  
trainable classifiers, 154  
conditional access policies, 54–58, 135, 138  
confidentiality (CIA pillars), defense-in-depth, 7  
configuring  
    DDoS, 78  
    NSG, 77  
connectors (data), Azure Sentinel, 99–102  
Content Explorer, Microsoft Compliance Manager, 155  
Content Search tool, Microsoft 365, 169–170  
controls, Microsoft Compliance Manager, 149–150  
Core eDiscovery workflows, 170–173  
correlation, SIEM, 96  
credentials, reusing, 20  
cryptography, public key cryptography, 19  
CSPM (Cloud Security Posture Management), 70, 91–93  
custom banned password lists, 43  
Customer Lockbox, 167–168  
CWPP (Cloud Workload Protection Platform), 87–90

## D

data, zero-trust methodology, 3, 5  
data aggregation, SIEM, 95–96  
data breaches, 10  
Data Classification page, Microsoft Compliance Manager, 153–154  
data connectors, Azure Sentinel, 99–102  
data encryption  
    ADE, 83  
    App Service, 84  
data locations, encryption, 10–11  
data retention, SIEM, 97  
data visualization, SIEM, 96–97  
DDoS (Distributed Denial of Service)  
    attacks, 78  
    basic protection, 77–78  
    configuring, 78  
    Standard tier, 77–78  
DDoS (Distributed Denial of Service) attacks, 9–10  
Defender, Azure, 87–90  
Defender, Microsoft  
    MSDE, 119–122  
    MSDO, 115  
        features, 117  
        policies, 118  
    services, 115–116

    threat tracking, 118–119  
defense-in-depth, 7  
    Azure networks, 8–9  
    CIA pillars, 7  
    traditional, 7–8  
devices  
    Azure AD  
        device management, 26–27  
        identities, 34  
        security with Microsoft Intune, 134–136  
digests (hashing text), 12  
digital signatures, 12  
DLP (Data Loss Prevention), 160–162  
domain services, Azure AD, 27  
DoS (Denial of Service) attacks, 9–10

## E

eavesdropping attacks, 9  
eDiscovery, 169  
    advanced workflows, 173  
    core workflows, 170–173  
encryption  
    ADE, 83  
    App Service, 84  
    data locations, 10–11  
    digital signatures, 12  
    hashing text (digests), 12  
    keys, 12  
    TPM, 83  
endpoints  
    DLP, 160–162  
    MDE, 136–137  
    MSDE, 119–122  
    security with Microsoft Intune, 134–137  
    zero-trust methodology, 3, 5  
entitlement management, Azure AD, 64–65  
Entity Behavior, Azure Sentinel, 108–109  
event management  
    CEF, 95–96  
    SIEM, 95–97  
external identities, Azure AD, 27, 39–41

## F

federation  
    AD FS, 32

- services, 18
    - IdP, 19
    - trusts, 19
  - FIDO 2 authentication, 54
  - firewalls
    - Azure Firewall, 78–80
    - WAF, 81–82
  - forensic analysis, SIEM, 97
- 
- ## G
- global banned password lists, 43
  - governance, Azure AD, 27
  - groups
    - identities, 35–36
    - NSG, 74–77
    - rule groups, Microsoft 365 Compliance Center, 148
- 
- ## H
- hash synchronization, passwords, 29–30
  - hashing text (digests), 12
  - Hello for Business, Windows, 50–54
  - Hunting, Azure Sentinel, 109–111
  - hybrid identities, 28
    - AD FS, 32
    - Azure Active Directory Connect, 28–29
    - password hash synchronization, 29–30
    - PTA, 31–32
    - SSPR, 47
- 
- ## I
- identity
    - application (app) identities, Azure AD, 36–39
    - attacks, common, 20–21
    - Azure Active Directory Connect, 28–29
    - Azure AD identities
      - application (app) identities, 36–39
      - Azure AD Identity Protection, 68–70
      - device identities, 34
      - external identities, 27, 39–41
      - group identities, 35–36
      - managed identities, 38
      - user identities, 33
    - credential reuse, 20
  - device identities, Azure AD, 34
  - external identities, Azure AD, 27, 39–41
  - governance, Azure AD, 63–64
  - group identities, Azure AD, 35–36
  - hash synchronization, 29–30
  - hybrid identities, 28
    - AD FS, 32
    - Azure Active Directory Connect, 28–29
    - password hash synchronization, 29–30
    - PTA, 31–32
    - SSPR, 47
  - managed identities, Azure AD, 38
  - MSDO, 116–117
  - password sprays, 20–21
  - phishing attacks, 21
  - PIM, 67–68
  - as primary security perimeter, 13
  - PTA, 31–32
  - user identities, Azure AD, 33
  - zero-trust methodology, 3, 5

- IdP (Identity Providers), 19
- Improvement Actions, Microsoft Compliance Manager, 150–151
- incident management, 129–133
- Incidents, Azure Sentinel, 105–106
- information barriers, 166–167
- information protection/guidance, 153
  - Microsoft 365
    - auditing, 174–177
    - communication compliance, 164–166
    - Compliance Center, 174–177
    - Content Search tool, 169–170
    - Customer Lockbox, 167–168
    - DLP policies, 160–162
    - eDiscovery, 169
    - eDiscovery, advanced workflows, 173
    - eDiscovery, core workflows, 170–173
    - information barriers, 166–167
    - insider risk management, 162–164
    - privileged access management, 167
    - records management, 159
    - retention labels, 158
  - Microsoft Compliance Manager
    - Activity Explorer, 155–156
    - Content Explorer, 155
    - Data Classification page, 153–154
    - trainable classifiers, 154
- infrastructures, zero-trust methodology, 3, 5
- insider risk management, 162–164

## **integrity, CIA pillars, defense-in-depth**

integrity, CIA pillars, defense-in-depth, 7  
Intune, Microsoft, 26–27  
    conditional access policies, 135, 138  
    device security, 134–136  
    endpoint security, 134–137  
    MAM, 134–136  
    MDM, 134–136  
Investigation Graphs, Azure Sentinel, 107

## **J - K**

keys  
    Azure Key Vault, 83, 84  
    encryption, 12

## **L**

label activities, 156  
labels  
    retention labels, 158  
    sensitivity labels, 156–158  
least-privilege, authorization, 16–17  
licensing, Azure AD, 28  
lists, banned passwords  
    custom, 43  
    global, 43  
locations of data, encryption, 10–11  
lock screen, Windows 10, SSPR integration, 48  
Lockbox, Customer, 167–168  
locks, resource, 177–178  
Logic Apps, 113  
logs  
    aggregation, SIEM, 95–96  
    reporting, Azure AD, 27  
    unified audit logs, 174

## **M**

malware, 9  
MAM (Mobile Application Management), Microsoft Intune endpoint security, 134–136  
managing  
    access  
        Azure AD, 26, 54–58  
        conditional access policies, 54–58

applications (apps), Microsoft Intune, endpoint security, 134–136  
devices, Azure AD, 26–27  
entitlement management, Azure AD, 64–65  
events, SIEM, 95–97  
identity  
    Azure AD, 38  
    PIM, 67–68  
incidents, 129–133  
insider risk, 162–164  
privileged access, 167  
records, 159  
MCAS (Microsoft Cloud App Security), 123–124  
MDM (Mobile Device Management), Microsoft Intune, endpoint security, 134–136  
methodologies, 1  
    defense-in-depth, 7  
    Azure networks, 8–9  
    CIA pillars, 7  
    traditional, 7–8  
shared responsibility model, 5–7  
zero-trust methodology, 1–5  
MFA (Multifactor Authentication), 42, 48–50  
Microsoft 365  
    communication compliance, 164–166  
    Compliance Center  
        advanced auditing, 176–177  
        auditing, 174–177  
        Microsoft Compliance Manager, 148–153  
        navigating, 144–146  
        permissions, 146–148  
        rule groups, 148  
        unified audit logs, 174  
    Content Search tool, 169–170  
    Customer Lockbox, 167–168  
    DLP policies, 160–162  
    eDiscovery, 169  
        advanced workflows, 173  
        core workflows, 170–173  
    information barriers, 166–167  
    insider risk management, 162–164  
    privileged access management, 167  
    records management, 159  
    retention labels, 158  
Microsoft 365 Security Center, 124–125  
    incident management, 129–133  
    Microsoft Secure Score, 126–127  
    Security Reports, 128–129  
Microsoft 365 Security Reports, 128–129

Microsoft Compliance Manager, 148–149  
 Activity Explorer, 155–156  
 assessments, 150  
 compliance scores, 151–153  
 Content Explorer, 155  
 controls, 149–150  
 Data Classification page, 153–154  
 Improvement Actions, 150–151  
 label activities, 156  
 Overview page, 149  
 templates, 150  
 trainable classifiers, 154

Microsoft Intune  
 conditional access policies, 135, 138  
 device security, 134–136  
 endpoint security, 134–137  
 MAM, 134–136  
 MDM, 134–136  
 Microsoft Secure Score, 126–127  
 Microsoft Threat Intelligence, 80  
 MIP (Microsoft Information Protection), sensitivity labels, 156–158  
 MITM (Man-in-the-Middle) attacks, 10  
 MSAL libraries, 36  
 MSDE (Microsoft Defender for Endpoint), 119–122  
 MSDO (Microsoft Defender for Office 365), 115  
 features, 117  
 policies, 118  
 services, 115–116  
 threat tracking, 118–119

## N

NSG (Network Security Groups), 74  
 configuring, 77  
 creating, 77  
 implementations, 74  
 parameters, 77  
 rules, 75–76  
 number matches, passwordless authentication, 52–53

## O

Office 365  
 MSDE, 119–122  
 MSDO  
 features, 117

identity, 116–117  
 policies, 118  
 services, 115–116  
 threat tracking, 118–119  
 organizational password policies, 42  
 Overview page, Microsoft Compliance Manager, 149

## P

passwordless authentication, 42, 50–54  
 passwords  
 Azure AD Password Protection, 42  
 Azure AD integration, 44  
 banned password lists, 44  
 custom banned lists, 43  
 global banned lists, 43  
 scoring passwords, 44  
 hash synchronization, 29–30  
 organizational password policies, 42  
 PIN versus, 50  
 resetting, 44–48  
 scoring, 44  
 sprays, 20–21  
 SSPR, 44  
 authentication methods, 44–47  
 hybrid identities, 47  
 Windows 10 lock screen integration, 48  
 write-backs, 47  
 write-backs, SSPR, 47  
 permissions, Microsoft 365 Compliance Center, 146–148  
 phishing attacks, 9, 21  
 PIM (Privileged Identity Management), 67–68  
 PIN versus passwords, 50  
 playbooks, Azure Sentinel, 113  
 policies  
 Azure Policy, 179–180  
 conditional access policies, 54–58, 135, 138  
 DLP policies, 160–162  
 insider risk policies, 163–164  
 MSDO Policies, 118  
 organizational password policies, 42  
 retention policies, 158  
 port scanning attacks, 9  
 privileged access management, 167  
 PTA (Pass-Through Authentication), 31–32  
 public key cryptography, 19

## **Q - R**

ransomware, 10  
RBAC (Role-Based Access Control), 15–16, 86  
records management, 159  
reporting  
    logs, Azure AD, 27  
    Microsoft 365 Security Reports, 128–129  
resetting passwords, SSPR, 44–48  
resource locks, Azure networks, 177–178  
retaining data, SIEM, 97  
retention policies/labels, 158  
reusing credentials, 20  
reviewing access, 65–67  
risk generation, Azure AD Identity Protection, 70  
risk management, insider, 162–164  
roles, Azure AD, 58–62  
rules  
    groups, Microsoft 365 Compliance Center, 148  
    NSG, 75–76

## **S**

scoring  
    Azure Secure Score, 87–88  
    compliance scores, Microsoft Compliance Manager, 151–153  
    Microsoft Secure Score, 126–127  
    passwords, 44  
searching, Content Search tool, Microsoft 365, 169–170  
Secure Score, Azure, 87–88  
Secure Score, Microsoft, 126–127  
Security Benchmark, Azure, 93–94  
Security Center, Azure, 85–87  
Security Center, Microsoft 365, 124–125  
    Microsoft Secure Score, 126–127  
    Security Reports, 128–129  
Security Reports, Microsoft 365, 128–129  
sensitivity labels, 156–158  
Sentinel, Azure, 94  
    Analytics Rules, 102–105  
    automation, 111–113  
    collect, 99–102  
    data connectors, 99–102  
    detection, 102–105  
    Entity Behavior, 108–109  
    Hunting, 109–111  
    Incidents, 105–106

investigate, 105–111  
Investigation Graphs, 107  
playbooks, 113  
respond, 111–113  
SIEM, 95–97  
SOAR, 98  
UEBA, 108–109  
visualize, 114–115  
Workbooks, 114–115  
XDR, 99  
service accounts, authorization, 16  
services  
    domain services, Azure AD, 27  
    federation services, 18  
        IdP, 19  
        trusts, 19  
    MSDO, 115–116  
shared responsibility model, 5–7  
SIEM (Security Information and Event Management), 94–95  
    analytics, 96  
    correlation, 96  
    data retention, 97  
    data visualization, 96–97  
    data/log aggregation, 95–96  
    forensic analysis, 97  
signatures, digital, 12  
SOAR (Security Orchestration, Automation and Response), 98  
sprays, password, 20–21  
SSPR (Self-Service Password Reset)  
    authentication methods, 44–47  
    hybrid identities, 47  
    Windows 10 lock screen integration, 48  
    write-backs, 47  
Standard tier, DDoS, 77–78  
synchronization, hash, 29–30

## **T**

templates, Microsoft Compliance Manager, 150  
text, hashing (digests), 12  
threat hunting, Azure Sentinel, 109–111  
Threat Intelligence, Microsoft, 80  
threats  
    botnets, 10  
    common identity attacks, 20–21  
    credential reuse, 20

data breaches, 10  
DDoS attacks, 9–10, 78  
DoS attacks, 9–10  
eavesdropping attacks, 9  
malware, 9  
Microsoft Threat Intelligence, 80  
MITM attacks, 10  
MSDE, 119–122  
MSDO, 115  
    policies, 118  
    threat tracking, 118–119  
password sprays, 20–21  
phishing attacks, 9, 21  
port scanning attacks, 9  
    ransomware, 10  
TPM (Trusted Platform Module), 83  
tracking threats, MSDO, 118–119  
trainable classifiers, 154  
trusts, federation, 19

## **U**

UEBA (User and Entity Behavior Analytics), 108–109  
unified audit logs, 174  
user identities, 33

## **V**

visualization, data, 96–97

## **W**

WAF (Web Application Firewall), 81–82  
Windows 10 lock screen, SSPR integration, 48  
Windows Hello for Business, 50–54  
Workbooks, Azure Sentinel, 114–115  
workflows, eDiscovery  
    advanced workflows, 173  
    core workflows, 170–173  
write-backs, SSPR, 47

## **X - Y - Z**

XDR (Extended Detection and Response), 99  
zero-trust methodology, 1–5