packt

Mastering Microsoft Entra ID

Design, implement, secure, and govern modern identity solutions across hybrid enterprises



Pramiti Bhatnagar

Foreword by: Merill Fernando, Principal Product Manager at Microsoft

Mastering Microsoft Entra ID

Design, implement, secure, and govern modern identity solutions across hybrid enterprises

Pramiti Bhatnagar

‹packt›

Mastering Microsoft Entra ID

Copyright © 2026 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

Portfolio Director: Kartikey Pandey
Relationship Lead: Reshma Raman
Project Manager: Sonam Pandey
Content Engineer: Arun Nadar
Technical Editor: Simran Ali
Copy Editor: Arun Nadar
Indexer: Pratik Shirodkar
Production Designer: Ajay Patule

First published: June 2026

Production reference: 1260526

Published by Packt Publishing Ltd.
Grosvenor House
11 St Paul's Square
Birmingham
B3 1RB, UK.

ISBN 978-1-80611-601-0
www.packtpub.com

Foreword

Identity used to be a predictable, bounded problem.

For years, identity management meant keeping the basics ticking along: provisioning users, managing standard groups, and handling the core Joiner-Mover-Leaver (JML) lifecycle. You built your directory, mapped out your standard access patterns, and tried not to change things unless you absolutely had to.

Then, the cloud completely shattered those boundaries.

First came the operational complexity of rapid mergers and acquisitions, forcing identity teams to stitch completely different environments together, inherit mounds of tenant technical debt, and manage complex external collaborations overnight. Right alongside this corporate sprawl came a wave of sophisticated cloud threats. Attackers realized they didn't need to exploit firewall vulnerabilities when they could just steal a session token, abuse a misconfigured app registration, or target a stale guest account.

To fight back, our identity infrastructure had to evolve fast. What used to be a simple sign-on process ballooned into a massive ecosystem of multi-tenant architectures, strict governance workflows, and complex webs of Conditional Access policies.

And just as we started getting a handle on that, the landscape shifted again.

We entered the era of AI and autonomous systems. Today, identity isn't just about human users or traditional software workloads. The moment an AI agent can call an API, read corporate data, or take actions in a business system, it becomes a brand-new identity surface. Managing and governing these Agent IDs, tracking who owns them, what they can access, and preventing "*agent sprawl*", is the newest, highest-stakes frontier for modern identity teams.

This is why identity is now the ultimate control plane for almost everything we do in the cloud. It decides who or what gets access, from what device, to which applications, and under what level of risk.

Keeping all of this in your head is a massive challenge for any admin, architect, or security engineer. That's exactly why we need this book, and why I'm so glad Pramiti wrote it.

Having worked alongside Pramiti at Microsoft, I've seen firsthand her ability to bridge the gap between deep product engineering and messy, real-world customer deployments. She understands the technology inside out, but more importantly, she understands the daily

operational grind: the hybrid technical debt, legacy dependencies, stressful audits, endless admin portals, and the constant barrage of alerts.

This book reflects that practical mindset. It doesn't treat Microsoft Entra ID as a disconnected collection of features; it treats identity as a cohesive system. Pramiti takes you from the foundational building blocks, such as tenants, users, groups, and Conditional Access, right through to the advanced capabilities modern environments demand: Identity Governance, Lifecycle Workflows, Privileged Identity Management (PIM), Workload Identities, Global Secure Access, and now, the critical task of securing AI agent infrastructure.

This end-to-end view is critical because you can't solve identity security with a single feature. You don't "*do Zero Trust*" by flipping a single toggle. You don't protect highly privileged roles by just asking people to be careful. You can't manage joiners, movers, and leavers on a spreadsheet forever. And you certainly can't leave your identity architecture as an afterthought. You need a model. You need patterns. You need to know how the pieces fit together.

That's where this book shines. It is built for the people doing the actual work. Whether you are designing a brand-new architecture, cleaning up a stale tenant, navigating a high-stakes M&A integration, or modernizing away from legacy on-premises Active Directory, this book gives you actionable guidance.

The threat landscape has evolved, and attackers have figured out that identity is the easiest way into an organization. They aren't breaking in; they are logging in. Token theft, consent phishing, over-privileged apps, and stale guest accounts are no longer edge cases, they are everyday realities.

Microsoft Entra ID gives us an incredibly powerful toolkit to defend against these threats, but knowing how to architect and deploy it effectively is the real challenge.

Whether you are a seasoned identity architect, a security engineer, or an admin who just inherited a messy tenant and is wondering where to start, this book will build your confidence. It will take you from simply knowing a feature exists to knowing how to design and operate it responsibly.

Identity is far too critical to be treated as a pile of random settings. It requires architecture, governance, automation, and continuous learning. Pramiti has distilled years of hands-on experience into a clear, actionable blueprint to help you get it right.

Keep this book on your desk. You're going to need it.

Merill Fernando

Principal Product Manager at Microsoft

Contributors

About the author

Pramiti Bhatnagar is a seasoned technology leader with more than 20 years of deep expertise across Microsoft's security and identity ecosystem, including Microsoft Entra, Microsoft Purview, Microsoft Defender, and Microsoft Security Copilot. She holds an honours degree in Applied Psychology from the University of Delhi and a range of industry-recognized certifications, including CIPM, CISSP, and Microsoft Certified: Cybersecurity Architect Expert. Pramiti currently serves as a Principal Product Manager for Microsoft Entra, where she focuses on the Entra Suite with a particular emphasis on Microsoft Security Copilot and Security for AI. She is a respected public speaker, regularly presenting at industry forums such as the **Australian Information Security Association** (**AISA**) and ISACA. Beyond her product leadership, Pramiti is committed to developing the next generation of security professionals. She actively mentors emerging talent through the **Global Mentorship Initiative** (**GMI**) and the **Australian Women in Security Network** (**AWSN**). She was a finalist for Cybersecurity Leader of the Year at the Women in Digital Awards.

About the reviewer

Abbas Kudrati is the Regional Chief Identity Security and AI Advisor at Silverfort and the former Chief Cybersecurity Advisor at Microsoft Asia. A neurodiverse cybersecurity leader and a dedicated advocate for the ADHD community, Abbas brings a unique cognitive perspective to his deep expertise in AI Security, Identity Security, Zero Trust Architecture, **Governance, Risk, and Compliance** (**GRC**), and Cloud Security. He provides strategic and technical guidance to a number of startups, including SquareX, Aona.ai, and PriviEzi, as well as leading institutions such as EC-Council and Vinnies Victoria, while actively mentoring the cybersecurity community.

A bestselling author and renowned keynote speaker, Abbas has authored industry-recognized books such as Threat Hunting in the Cloud, Zero Trust Journey Across the Digital Estate, Cloud Container Security and Managing Risks in Digital Transformation. He also serves as a Professor of Practice at La Trobe University and is a Fellow of the **Australian Information Security Association** (**AISA**).

Table of Contents

Preface **xxix**

Free benefits with your book **xxxv**

Part 1: Foundations of Microsoft Entra **1**

Chapter 1: Introduction to Microsoft Entra **3**

Identity fundamentals **4**

Identification • 4

Authentication • 4

Authorization • 5

Accountability • 5

Identity provider (IdP) • 5

Identity and access management **6**

Authentication and authorization standards • 7

OAuth • 7

Security Assertion Markup Language (SAML) • 8

OpenID Connect (OIDC) • 8

JSON Web Tokens (JWTs) • 8

System for Cross-Domain Identity Management (SCIM) • 8

Web Services Federation (WS-Fed) • 9

Microsoft Identity platform **9**

Microsoft Entra **10**

Microsoft Entra ID • 10

Licensing • 11

Microsoft Entra Domain Services • 12

Pricing • 12

Microsoft Entra ID Governance • 13

Identity and access lifecycle • 14
Privileged access lifecycle • 15
Licensing • 15
Microsoft Entra Identity Protection • 16
Licensing • 16
Microsoft Entra Verified ID • 16
Licensing • 17
Microsoft Entra Workload ID • 17
Licensing • 18
Microsoft Entra External ID • 18
Pricing • 20
Global Secure Access • 20
Microsoft Entra Internet Access • 21
Microsoft Entra Internet Access for Microsoft Services • 22
Microsoft Entra Private Access • 22
Licensing • 22
Summary 22
Exercises 23
Answers 23
Additional resources 23

Chapter 2: Fundamentals of Microsoft Entra ID 25

Microsoft Entra roles 26
Built-in roles • 27
Custom roles • 28
Assigning roles • 29
Assigning directly to users • 30
Using role-assignable groups • 30
Using PIM • 34
Single sign-on 35
Administrative roles • 36
Certificates • 36

Communication • 36
Licensing • 36
Shared accounts • 36
SSO deployment options • 37
Multi-factor authentication 38
Configuring prompts and session lifetime • 39
Configuring system-preferred MFA • 41
Configuring external MFA provider • 42
Configuring MFA rollout • 43
Authentication methods 45
Temporary Access Pass • 45
Passwordless authentication • 49
Windows Hello for Business • 49
Platform Credential for macOS • 51
Platform SSO on macOS with SmartCard • 51
Microsoft Authenticator • 51
Passkey (FIDO2) authentication • 53
Certificate-based authentication • 56
Microsoft Authenticator in Push mode • 57
OATH software token • 62
OATH hardware token • 62
QR code • 64
Conditional Access 66
Protected actions 68
Summary 70
Exercises 70
Answers 71
Additional resources 71

Chapter 3: Implementing Microsoft Entra ID 73

Determining the identity model 73
Setting up Microsoft Entra ID tenant 74

Cloud-only identity 78
Creating users • 79
Creating groups • 80
Hybrid identity 80
Microsoft Entra Cloud Sync • 81
Deployment scenarios • 81
Key components • 82
Installing Microsoft Entra Cloud Sync • 82
Verifying the installation • 84
Microsoft Entra Connect • 84
Installation requirements • 85
Installation steps • 88
Object filtering • 88
Microsoft Entra Connect Health • 89
Authentication methods 89
Password hash sync • 90
Selective password hash synchronization • 92
Setting up password hash synchronization • 92
Pass-through authentication • 93
Configuration prerequisites • 94
Enabling pass-through authentication • 94
Testing pass-through authentication • 95
Federated authentication • 95
Choosing the right method • 96
Administrative units 97
Restricted management administrative units • 97
Creating an administrative unit • 99
Adding members to an administrative unit • 100
Dynamically add members to an administrative unit • 101
Assigning administrative roles to an administrative unit • 103
End-user self-service 107
Self-service password reset • 107

Self-service group management • 109
Self-service application assignment • 111
Fundamental security settings 113
Summary 114
Exercises 114
Answers 115
Additional resources 115

Chapter 4: Microsoft Entra Domain Services 117

Cloud-based directory services 117
Self-managed domain • 118
Overview of Microsoft Entra Domain Services • 118
Microsoft Entra Domain Services managed domain 120
Basic concepts • 121
Replica sets • 121
Forests and trusts • 121
Synchronization • 122
Domain management • 122
User account creation • 124
Password policy • 124
Licensing • 124
Creating a managed domain 125
Enabling applications to use the managed domain • 128
Enabling user accounts for Domain Services • 128
Configuring virtual networking for managed domains • 129
Virtual network subnet in the same virtual network • 129
Virtual network subnet in a separate Azure virtual network • 130
Creating a replica set • 132
Creating a forest trust • 134
Administering a managed domain 136
Creating an administrator VM • 136
Creating an OU • 137

Administering GPOs • 138
Managing DNS • 138
Checking health status • 139
Securing Domain Services 141
Securing managed domain • 141
Configuring Kerberos constrained delegation • 142
Enabling security audit events • 144
Summary 146
Exercises 146
Answers 147
Additional resources 147

Chapter 5: AI in Microsoft Entra 149

Microsoft Security Copilot 149
Security Copilot experiences • 151
Standalone experience • 152
Embedded experience • 152
Privacy and data security • 153
Data storage locations • 154
Data retention • 154
Prompt evaluation locations • 154
Getting started with Security Copilot • 154
Prerequisites • 155
Provisioning capacity • 155
Understanding authentication • 157
Security Copilot in Microsoft Entra 158
Supported scenarios • 160
Tenants • 160
Users • 160
Groups • 160
Devices • 161
Roles and administrators • 161

Domain Services • 161
Conditional Access • 161
Authentication • 162
Sign-in logs • 162
Audit logs • 163
Recommendations • 163
Health monitoring alerts • 164
Service level agreement • 164
Risky users • 164
Application risk • 164
Entitlement Management • 165
Access reviews • 165
Privileged Identity Management • 166
Lifecycle workflows • 166
License usage • 167
Global Secure Access • 167
Security Copilot agents in Microsoft Entra 167
Conditional Access optimization agent • 169
Prerequisites • 170
Limitations • 171
Onboarding the agent • 171
Adjusting settings • 172
Review suggestions • 174
Microsoft Entra Agent ID 177
Summary 180
Exercises 181
Answers 181
Additional resources 182

Part 2: The Entra Governance Stack 183

Chapter 6: Microsoft Entra Entitlement Management 185

Microsoft Entra ID Governance 186
Principle of least privilege 188
Entitlement management 189
Understanding catalogs • 190
Understanding access packages • 190
Connected organizations • 191
Adding a connected organization • 191
Roles in entitlement management • 193
Licensing requirements • 194
Getting started with entitlement management • 194
Delegating to catalog creator • 195
Allowing access to Microsoft Entra portal • 195
Creating a catalog • 196
Adding additional roles • 196
Adding resources to the catalog • 197
Adding resource attributes to the catalog • 198
Creating an access package • 199
Requesting access • 204
Approving access • 205
Validating that it worked • 206
Assigning an access package manually • 206
Auto-assigning users to an access package • 208
Understanding access reviews 209
Multi-stage reviews • 211
Guest user reviews • 213
Access reviews for groups and applications • 214
Creating an access review • 215
Reviewing access • 218

Access reviews for access packages • 219

Creating an access review • 219

Reviewing access • 220

Access reviews for Microsoft Entra and Azure resource roles • 220

Creating an access review • 220

Reviewing access • 222

Reporting • 222

License requirements • 223

Summary 223

Exercises 223

Answers 224

Additional resources 224

Chapter 7: Microsoft Entra Lifecycle Workflows 227

Introduction to Microsoft Entra Lifecycle Workflows 228

LCW as a Zero Trust control 230

Joiner phase • 231

Mover phase • 231

Leaver phase • 232

Components of lifecycle workflows 233

Tasks • 233

Triggers • 235

Scope • 238

Role requirements 239

Licensing requirements 239

Limits 239

Getting started with lifecycle workflows 239

Prerequisites • 240

Inbound provisioning • 240

Attribute synchronization • 240

Creating a lifecycle workflow • 240

Running workflow on demand • 243

Scheduling the workflow • 244
Managing lifecycle workflows 245
Manage workflow properties • 245
Versioning • 247
Email customization • 249
Reprocessing workflows • 251
Workflow history reports • 252
Managing inactive users • 252
Custom task extensions 254
Workflow insights 257
Summary 258
Exercises 258
Answers 259
Additional resources 259

Chapter 8: Microsoft Entra Privileged Identity Management 261

Introduction to privileged identities 262
Overview of Microsoft Entra Privileged Identity Management 263
Role requirements • 264
Terminology • 264
Emergency access accounts • 265
Role assignment overview • 266
Licensing requirements • 267
PIM vs direct role assignment • 268
Plan PIM deployment 269
Microsoft Entra and Azure roles • 270
Groups • 270
Start using PIM 271
Microsoft Entra roles • 271
Preparing a role for PIM • 271
Assigning a role • 275
Activating a role • 279

Approving assignments • 281
Extending assignment • 281
Azure resource roles • 282
Selecting Azure resources • 282
Preparing a role for PIM • 284
Assigning a role • 284
Groups • 287
Bringing groups into PIM • 287
Preparing the group for PIM • 289
Assigning eligibility • 290
Alerts 291
Microsoft Entra roles • 291
Azure roles • 293
Auditing PIM 294
Discovery and insights 295
Best practices 297
Best practices for PIM 297
Summary 298
Exercises 299
Answers 299
Additional resources 299

Part 3: Identity Assurance and Protection 301

Chapter 9: Microsoft Entra ID Protection 303

Introduction to Microsoft Entra ID Protection 304
Role requirements • 305
License requirements • 306
Microsoft Entra ID Protection dashboard 307
Understanding risk detections 309
Risk types • 310
Risk levels • 310

Detection types • 311
Risks detected by Microsoft Entra ID Protection • 312
Risk-based access policies ... 316
Prerequisites • 317
Sign-in risk policy • 317
User risk policy • 318
MFA registration policy • 319
Test risk policies • 320
Impact analysis workbook • 321
Continuous Access Evaluation ... 325
Scenarios • 325
Critical event evaluation • 325
Conditional Access policy evaluation • 326
Client capabilities • 326
Securing workload identities ... 326
Configure notifications ... 328
Users at risk detected email • 328
Weekly digest email • 330
Investigate and remediate risks ... 330
Risky users • 331
Risky sign-ins • 333
Risky workload identities • 334
Risk detections • 334
Simulate risk detections ... 335
Anonymous IP address • 335
Unfamiliar sign-in properties • 335
Atypical travel • 336
Leaked credentials for workload identities • 336
Export risk data ... 336
Provide feedback to Microsoft ... 337
Summary ... 337
Exercises ... 338

Answers **338**
Additional resources **338**

Chapter 10: Microsoft Entra Verified ID **341**

Introduction to decentralized identities **342**
Introduction to verifiable credentials **343**
Understanding Microsoft Entra Verified ID **345**
Licensing • 347
Get started with Microsoft Entra Verified ID **347**
Using quick setup • 347
End user experience • 351
Using advanced setup • 353
Creating a key vault • 353
Setting up Verified ID • 354
Registering an application • 355
Registering a DID • 356
Verifying domain ownership • 356
Custom credentials • 357
Issuing custom credentials • 357
Verifying credentials • 361
Setting up Verified ID • 361
Creating the verifier app • 362
Verified ID Face Check **363**
Enabling Face Check • 363
Licensing • 365
Verified ID with entitlement management **365**
Licensing • 369
Account recovery **369**
Revoking credentials **371**
Opting out of Verified ID service **374**
Summary **374**
Exercises **374**

Answers **375**
Additional resources **375**

Chapter 11: Microsoft Entra Workload ID **377**

Applications in Microsoft Entra **377**
Managed identities for Azure resources **379**
Introduction to workload identities **380**
Applications and service principals • 380
Application object • 380
Service principal object • 381
Workload identity federation **383**
Configuring federated identity credentials • 385
Securing workload identities **386**
Conditional Access for workload identities **387**
Continuous Access Evaluation for workload identities **391**
Best practices **391**
Licensing **392**
Summary **392**
Exercises **392**
Answers **393**
Additional resources **393**

Part 4: Extending Identity and Access beyond the Organization **395**

Chapter 12: External Identities in Workforce Tenants **397**

Introduction to Microsoft Entra External ID **398**
External ID in the workforce tenant **402**
Inviting a guest user • 404
Identity providers **409**
External collaboration settings **410**
Cross-tenant access settings **413**
Default settings • 413

Trust settings • 415
Redemption order • 415
Organization-specific settings • 417
Automatic redemption • 418
Cross-tenant sync • 419
Tenant restrictions • 419
Microsoft cloud settings • 423
B2B direct connect • 428
Governance for B2B users 429
ID Protection for B2B users 430
Leaving an organization 430
Best practices 431
Pricing 432
Summary 432
Exercises 432
Answers 433
Additional resources 433

Chapter 13: External Identities in External Tenants 435

External ID in external tenants 436
Creating an external tenant 437
Using the get started guide 440
User profile attributes 442
Configuring identity providers 445
Email and password • 445
Email and OTP • 446
Username or alias • 446
Social identities • 448
Custom OIDC identity provider • 450
Custom SAML/WS-Fed • 452
Registering applications in Entra External ID 455
Registering an OIDC application • 455

Registering a SAML application • 457
Adding an enterprise application • 458
Creating a user flow 459
Customization 462
Customizing neutral branding • 462
Configuring branding themes • 467
Customizing tokens • 468
Configuring optional claims • 469
Adding custom URL domains • 470
Custom authentication extensions • 475
Enabling self-service password reset 477
Securing external tenants 478
Native authentication 479
Migrating to Entra External ID 480
Monitoring External ID 481
Summary 481
Exercises 482
Answers 482
Additional resources 482

Chapter 14: Microsoft Entra Internet Access 485

Overview of Global Secure Access 486
GSA client • 488
Remote networks • 488
Traffic forwarding profiles • 490
Access controls • 492
Universal Conditional Access • 492
Compliant network check • 492
Source IP restoration • 494
Understanding Microsoft Entra Internet Access 494
Internet Access profile • 495
Security profiles • 496

Prerequisites • 499
Configuring web content filtering • 499
Configuring Transport Layer Security inspection • 505
Configuring threat intelligence • 508
Configuring cloud firewall • 510
Network content filtering • 512
Configuring the AI Gateway prompt injection protection • 514
Configuring Secure Web and AI Gateway for Microsoft Copilot Studio agents • 516
Microsoft Entra Internet Access for Microsoft Services 517
Microsoft traffic profile • 517
Licensing 518
Summary 518
Exercises 519
Answers 519
Additional resources 520

Chapter 15: Microsoft Entra Private Access 521

Understanding Microsoft Entra Private Access 522
Quick Access • 523
Creating a private network connector group • 523
Configuring Quick Access • 526
Applying Conditional Access policies • 527
Per-app access • 528
Creating a Global Secure Access app • 528
Application discovery • 529
Intelligent local access • 531
Securing access to private apps with Privileged Identity Management • 532
Kerberos for Single Sign-On • 533
Source IP anchoring • 535
Private Access for Domain Controllers 536
Prerequisites • 536
Creating an application • 537

Installing the Private Access Sensor • 537
Creating Conditional Access policy • 538
Inclusions and exclusions • 538
Break glass mode • 539
Application usage analytics 539
Logs and monitoring 540
GSA Dashboard • 540
Traffic logs • 540
Audit logs • 541
Remote network health logs • 541
Deployment logs • 541
Alerts • 542
Licensing 542
Summary 542
Exercises 542
Answers 543
Additional resources 543

Part 5: Optimizing, Modernizing, and Growing with Microsoft Entra 545

Chapter 16: Microsoft Entra Health, Threats, and Trust 547

Introduction 548
Microsoft Entra activity logs 548
Audit logs • 548
Sign-in logs • 549
Provisioning logs • 551
Diagnostic settings • 551
Usage and insights reports 552
Microsoft Entra recommendations 555
Microsoft Entra workbooks 557
Microsoft Entra threat landscape 558

Types of threats facing Microsoft Entra • 559
Protecting Microsoft Entra from threats • 560
Built-in security features in Microsoft Entra • 560
Advanced protection mechanisms • 561
Example scenarios • 561
Continuous monitoring and improvement • 562
Responding to security incidents • 562
Recoverability 562
Soft deletion • 563
Microsoft Entra Backup and Recovery • 565
Prerequisites • 565
Getting started • 565
Difference report • 566
Recovery • 569
Microsoft Entra and Zero Trust 571
Identity as the new security perimeter • 572
Conditional Access in Microsoft Entra • 572
Multi-Factor Authentication • 572
Least privilege and role-based access control in Microsoft Entra • 572
Continuous monitoring and risk-based access • 573
Device compliance and health integration • 573
Real-time analytics and threat intelligence in Microsoft Entra • 573
Automated threat detection and response • 573
Integration with Microsoft security solutions • 574
Practical scenarios: Microsoft Entra enforcing Zero Trust • 574
Best practices for achieving Zero Trust with Microsoft Entra • 575
Microsoft Entra and Mesh architecture 575
Technical integration points • 576
Identity management integration • 576
Security and compliance in Mesh with Microsoft Entra • 577
Implementation best practices • 577
Real-world use cases • 578

Summary **579**
Exercises **579**
Answers **580**
Additional resources **580**

Chapter 17: Migrating to Microsoft Entra ID **581**

Understanding the migration landscape **582**
States of transformation **583**
Cloud-attached • 584
Hybrid • 584
Cloud-first • 584
Active Directory minimized • 584
Cloud-only • 584
Migration strategies **585**
Phased migration • 585
Hybrid coexistence • 585
Lift-and-Shift migration • 586
Greenfield (Cloud-Native) approach • 586
Journey to the cloud **586**
Prerequisites and planning • 587
Organizational readiness • 587
Technical prerequisites • 587
Licensing requirements • 588
Assessing the current Active Directory environment • 588
Inventory and discovery • 588
Dependency mapping • 588
Identity synchronization • 589
Migrating authentication • 589
Migrating applications • 589
Application discovery and classification • 590
Migration approaches by application type • 590
Conditional Access policies • 590

Device migration and management • 591
Security considerations • 592
Zero Trust alignment • 592
Privileged Access Management • 593
Identity protection • 593
On-premises decommissioning 593
Confirm no service depends on on-premises domain controllers • 594
Validate Entra ID is the authoritative source • 594
Remove hybrid identity components • 595
Clean up the domain • 595
Decommission domain controllers • 595
Summary 595
Exercises 596
Answers 597
Additional resources 597

Chapter 18: Career Opportunities with Microsoft Entra Skills 599

The Entra leverage 600
Job roles for identity professionals 601
Identity administrator / identity operations (identity ops) • 601
Identity engineer (Microsoft Entra / IAM engineer) • 601
Security engineer (identity and access) • 602
Identity governance specialist (access lifecycle and entitlement management) • 603
Access governance analyst • 604
Privileged access engineer (PAM / admin security) • 605
Identity architect / cloud security architect (identity) • 605
Consultant / delivery engineer • 606
Identity product manager • 607
Identity platform owner / technical product owner • 608
Key skills and certifications by career level 608
Career progression paths in identity management 610
Technical architecture track • 610

Operations and platform leadership track • 611
Security and strategy track • 611
Consulting and advisory track • 611
Identity meets AI governance • 611
Decentralized identity and verifiable credentials • 612
Your place in the identity revolution 612
Summary 612
Additional resources 613

Chapter 19: Unlock Your Exclusive Benefits 615

Unlock this Book's Free Benefits in three Easy Steps 616

Other Books You May Enjoy 621

Index 625

Preface

Identity used to be simple. Users signed in, opened applications, and anything inside the network was assumed to be trustworthy. That model worked when systems were centralized and the pace of change was slow. Today, the landscape is very different. Workloads run across clouds, users work from anywhere, and access extends far beyond employees. Partners, customers, applications, and automated workloads all require controlled access, often at massive scale. The perimeter has dissolved, and identity has become the primary control plane.

With that shift, every access decision matters more. It is no longer enough to confirm who is requesting access; you must also understand context, risk, and intent. Zero Trust emerges here not as a slogan, but as a practical necessity. At the same time, operational demands have grown. Managing identity lifecycles, governing access, controlling privileged roles, and responding to identity-driven threats all require a level of rigor that many organizations are still developing.

Microsoft Entra is built for this new reality, but realizing its value takes more than enabling features. It requires a mindset, a way of thinking about identity architecturally, as a strategic layer rather than a background service. This book is written with that perspective. It walks through the core building blocks, the decisions that shape real-world deployments, and the patterns that consistently hold up under pressure.

By the end, you should see identity not just as something to administer, but as something you can intentionally design to strengthen security, reduce friction, and support how your organization truly operates.

Who this book is for

This book is for identity administrators, system administrators, security engineers, cloud architects, and IT professionals responsible for securing and governing enterprise access. If you manage hybrid environments, enforce Zero Trust, automate lifecycle processes, or protect against identity-based threats, this guide is for you. A foundational understanding of networking, IAM, and cloud concepts will help you get the most from this book.

What this book covers

Chapter 1, Introduction to Microsoft Entra, establishes the foundational concepts of identity by introducing the Identity, Authentication, Authorization, Accountability (IAAA) model and

explaining how these principles shape modern access control. It covers the basics of identity and access management and positions the Microsoft identity platform as the core engine behind authentication and authorization across Microsoft services. The chapter concludes with an overview of the Microsoft Entra product family, providing a clear map of the capabilities that will be explored in depth throughout the book.

Chapter 2, Fundamentals of Microsoft Entra ID, introduces the essential building blocks of modern access management, such as Single Sign-On (SSO) and Multi-Factor Authentication (MFA). It explains how Microsoft Entra RBAC provides structured, least-privilege access control and explores the authentication methods that underpin secure sign-ins. The chapter also covers Conditional Access and protected actions, showing how policy-driven enforcement strengthens security while adapting to user context and risk.

Chapter 3, Implementing Microsoft Entra ID, guides you through selecting and implementing the right identity model for your organization. It covers core operational tasks such as user and group management, the use of Administrative Units for delegated administration, and the essential security settings every Entra tenant should configure. The chapter concludes with an overview of end-user self-service capabilities, highlighting how thoughtful design can reduce operational overhead while improving user experience.

Chapter 4, Microsoft Entra Domain Services, explains how Microsoft Entra provides managed domain capabilities for applications that rely on traditional directory protocols. It outlines when and why to use Domain Services, how it integrates into your environment, without needing to maintain on-premises domain controllers.

Chapter 5, AI in Microsoft Entra, introduces AI capabilities in Microsoft Entra. It discusses Security Copilot and explores how AI-driven reasoning enhances identity security, incident response, and operational efficiency. It also explains Microsoft Entra Agent ID, the identity foundation for autonomous and semi-autonomous agents accessing resources across cloud services.

Chapter 6, Microsoft Entra Entitlement Management, explores Entitlement Management as the foundation for governing access at scale through access packages, catalogs, and access reviews. It explains how to streamline user access and enforce approval and review processes. The focus is on building predictable, auditable access patterns that reduce manual effort while strengthening overall governance.

Chapter 7, Microsoft Entra Lifecycle Workflows, explains how Lifecycle Workflows automate the joiner-mover-leaver process. It covers how to design event-driven workflows that provision, update, and retire access with consistency and minimal manual effort.

Chapter 8, Microsoft Entra Privileged Identity Management, covers how Microsoft Entra enables just-in-time, least-privilege access for sensitive roles and resources. It explains role activation, approval workflows, and the controls that reduce standing privilege access.

Chapter 9, Microsoft Entra ID Protection, explores how Microsoft Entra detects and responds to identity-based risks using real-time signals and machine learning. It explains user risk, sign-in risk, and risk policies, along with the automated remediation options that strengthen your security posture.

Chapter 10, Microsoft Entra Verified ID, introduces decentralized and verifiable credentials and explains how they enable secure, privacy-preserving identity verification. It covers the core concepts of issuers, holders, and verifiers, along with practical scenarios where organizations can streamline onboarding, compliance, and proof-of-identity processes.

Chapter 11, Microsoft Entra Workload ID, explains how applications, services, and automated processes authenticate securely without relying on shared secrets. It covers service principals, managed identities, and the controls that govern how workloads access resources across cloud environments.

Chapter 12, External Identities in Workforce Tenants, explains how External Identities enable organizations to collaborate securely with partners, vendors, and contractors inside workforce tenants. It covers the core models for inviting, managing, and governing external users, along with the policies that control their access and lifecycle.

Chapter 13, External Identities in External Tenants, focuses on using External ID in standalone external tenants to support customer, citizen, and large-scale public-facing identity scenarios. It explains how to design user journeys, manage custom attributes, and integrate applications using modern authentication standards.

Chapter 14, Microsoft Entra Internet Access, explains how Microsoft Entra provides secure, identity-aware access control for outbound internet traffic. It covers how policies enforce Zero Trust principles at the network edge, protecting users from malicious sites and risky content.

Chapter 15, Microsoft Entra Private Access, explains how Microsoft Entra provides secure, identity-aware access to private applications and resources without relying on traditional VPNs. It covers how policies, device posture, and identity signals work together to enforce Zero Trust access to internal networks.

Chapter 16, Microsoft Entra Health, Threats, and Trust, focuses on how to monitor the health, performance, and security posture of your Microsoft Entra ID environment. It covers the built-in dashboards, alerts, audit logs, and sign-in analytics that help detect issues and maintain operational readiness.

Chapter 17, Migrating to Microsoft Entra ID, outlines the key approaches for moving from traditional on-premises Active Directory to Microsoft Entra ID. It covers identity synchronization, application modernization, and strategies for reducing domain controller dependencies over time and shifting toward a cloud-first identity model.

Chapter 18, Career Opportunities with Microsoft Entra Skills, highlights the growing career paths shaped by Microsoft Entra across identity, security, governance, and Zero Trust architecture. It outlines roles ranging from identity engineers and cloud security architects to governance specialists. The focus is on how Entra skills translate into high-demand, future-proof opportunities in organizations modernizing their identity and access strategy.

To get the most out of this book

To follow along with the examples in this book, you'll need a working Microsoft 365 environment.

Before you begin, make sure you have the following:

- **Microsoft 365 subscription**: If you don't have one, you can sign up for a 30-day free trial for M365 E3 at `https://www.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-plans-and-pricing`.
- **Microsoft Entra Suite license**: A Microsoft 365 E3 subscription is required to get an Entra Suite license. You can sign up for a 30-day free trial at `https://www.microsoft.com/en-us/security/business/microsoft-entra-suite`
- **Microsoft Entra Workload ID Premium** license. You can sign up for a free trial from within the Microsoft 365 admin center.
- **An Azure subscription** linked to your Microsoft 365 subscription. If you don't have an Azure subscription sign up for a free trial at `https://azure.microsoft.com/en-us/pricing/purchase-options/azure-account`

The exercises in this book are designed to be followed along in your own tenant. You will get the best value if you set up your own environment and follow the instructions in the book. Remember that there are a lot more options for each capability than can be described in the book, so don't hesitate to explore all settings in your own tenants.

Download the color images

We also provide a PDF file that has color images of the screenshots/diagrams used in this book. You can download it here: `https://packt.link/gbp/9781806116010`.

Conventions used

There are a number of text conventions used throughout this book.

`CodeInText`: Indicates code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles. For example: "Ensure that the accounts in Microsoft Entra ID have the `employeeHireDate` and `employeeLeaveDateTime` attributes populated either manually or via HR provisioning."

A block of code is set as follows:

```
POST https://verifiedid.did.msidentity.com/v1.0/verifiableCredentials/
createPresentationRequest
```

Any command-line input or output is written as follows:

```
Set-ADSyncAADCompanyFeature -ForcePasswordChangeOnLogOn $true
```

Bold: Indicates a new term, an important word, or words that you see on the screen. For instance, words in menus or dialog boxes appear in the text like this. For example: "Navigate to **Entra ID | Domain services**. In the right pane, click on the managed domain name."

> **Note**
>
> Warnings or important notes appear like this.

> **Tip**
>
> Tips and tricks appear like this.

Get in touch

Feedback from our readers is always welcome.

General feedback: If you have questions about any aspect of this book or have any general feedback, please email us at `customercare@packt.com` and mention the book's title in the subject of your message.

Errata: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you reported this to us. Please visit `https://www.packt.com/submit-errata`, click **Submit Errata**, and fill in the form.

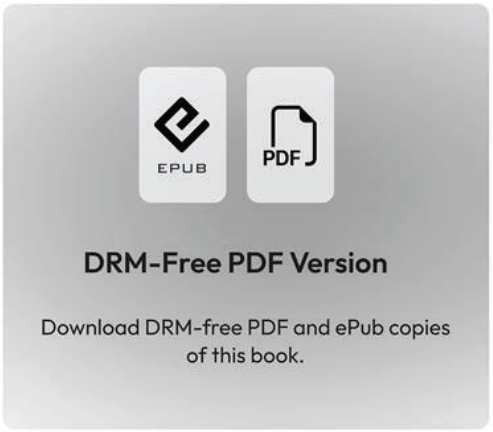
Piracy: If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at `copyright@packt.com` with a link to the material.

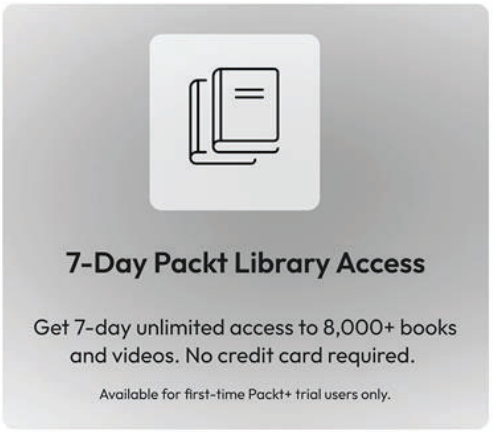
If you are interested in becoming an author: If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, please visit `https://authors.packt.com/`.

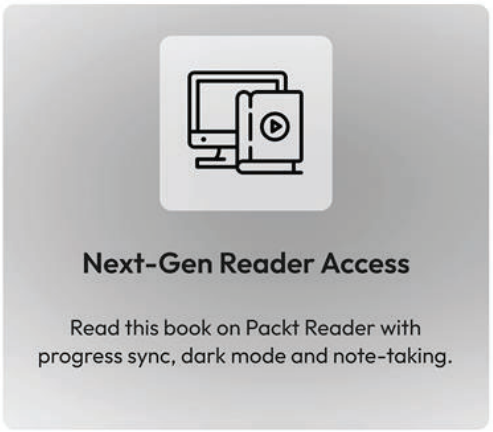
Free benefits with your book

This book comes with free benefits to support your learning. Activate them now for instant access (see the "*How to Unlock*" section for instructions).

Here's a quick overview of what you can instantly unlock with your purchase:







How to Unlock

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.





Note: Keep your invoice handy. Purchases made directly from Packt don't require one

Stay Sharp in Cloud and DevOps — Join 44,000+ Subscribers of CloudPro

CloudPro is a weekly newsletter for cloud professionals who want to stay current on the fast-evolving world of cloud computing, DevOps, and infrastructure engineering.

Every issue delivers focused, high-signal content on topics like:

- AWS, GCP & multi-cloud architecture
- Containers, Kubernetes & orchestration
- Infrastructure as Code (IaC) with Terraform, Pulumi, etc.
- Platform engineering & automation workflows
- Observability, performance tuning, and reliability best practices

Whether you're a cloud engineer, SRE, DevOps practitioner, or platform lead, CloudPro helps you stay on top of what matters, without the noise.

Scan the QR code to join for free and get weekly insights straight to your inbox:



Share your thoughts

Once you've read *Mastering Microsoft Entra ID, First Edition*, we'd love to hear your thoughts! Scan the QR code below to go straight to the Amazon review page for this book and share your feedback.



https://packt.link/r/1-806-11601-4

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

Part 1

Foundations of Microsoft Entra

Part 1 introduces the foundational identity services that power the Microsoft Entra ecosystem. It begins with Microsoft Entra ID, the cloud directory and access platform at the heart of modern identity. It then expands into core concepts such as implementation patterns, and operational best practices. This section also explores Microsoft Entra Domain Services and its role in supporting legacy workloads, as well as the emerging intelligence layer provided by Microsoft Security Copilot and Microsoft Entra Agent ID. Together, these chapters establish the technical and architectural baseline required to understand governance, protection, external identities, and secure access in the later parts of the book.

This part of the book includes the following chapters:

- *Chapter 1*, *Introduction to Microsoft Entra*
- *Chapter 2*, *Fundamentals of Microsoft Entra ID*
- *Chapter 3*, *Implementing Microsoft Entra ID*
- *Chapter 4*, *Microsoft Entra Domain Services*
- *Chapter 5*, *AI in Microsoft Entra*

1

Introduction to Microsoft Entra

Microsoft Entra is Microsoft's cloud-native **Identity and Access Management (IAM)** solution. It is a comprehensive suite designed to unify identity and access management across digital ecosystems. It ensures seamless and secure interactions between people, devices, applications, and services, empowering organizations to streamline their operations while safeguarding sensitive data. Rooted in the principles of zero-trust, Microsoft Entra integrates cutting-edge tools and technologies to address the evolving challenges of digital security. Its offerings include identity governance, access control, and secure network access, all aimed at fortifying organizational resilience against cyber threats.

Microsoft Entra embraces dynamic identity solutions for both human and non-human entities. Through its innovative frameworks, it supports hybrid environments, enabling organizations to transition smoothly between on-premises infrastructure and cloud-based systems. With its robust capabilities, Microsoft Entra positions itself as a cornerstone for modern enterprises striving to lead in a secure, interconnected world.

This chapter will cover:

- Identity fundamentals
- Identity and access management
- Microsoft identity platform
- Microsoft Entra
- **Your purchase includes a free PDF copy + exclusive extras**

Note

Your purchase includes a DRM-free PDF copy of this book, 7-day trial to the Packt+ library (no credit card required), and additional exclusive extras. See the *Free benefits*

> *with your book* section in the *Preface* to unlock them instantly and maximize your learning.

Identity fundamentals

A digital identity is a foundational concept in the realm of digital security and system architecture. Each entity that interacts with a computer system has an identity. This includes not only human but also non-human identities like devices and applications. A digital identity comprises a collection of unique identifiers or attributes that distinguish an individual, software component, or machine. Examples of such identifiers include email addresses, usernames, MAC addresses, and IP addresses. Digital identities serve a critical role in authenticating users and authorizing access to various resources. The fundamentals of computer identity focus on the principles of identification, authentication, authorization, and accountability, all of which are necessary for enabling secure and seamless interactions in virtual environments.

Identification

Identification is the initial step in establishing an identity. It involves recognizing and distinguishing entities within a digital ecosystem. This is usually done using identifiers like usernames, email addresses, or unique device IDs that serve as the primary markers to differentiate one entity from another. These identifiers are critical for tracking and managing digital identities, ensuring that each entity is uniquely identifiable within the system. Identification refers to the process by which a subject asserts an identity. To initiate authentication, authorization, and auditing procedures, the subject must present their identity to the system. This may involve entering a username, swiping a smartcard, or presenting biometric data such as facial features, a hand, or a fingerprint to a scanning device. A core principle is that all subjects must have a unique identity.

Authentication

Authentication is the process of confirming that an entity presenting an identity is genuinely who or what it claims to be by checking one or more credentials against a database of authorized identities, such as user accounts. The credentials used for authentication are confidential and must be properly secured at all times. This involves the use of credentials, such as passwords, biometric data, security tokens, or digital certificates. Authentication is sometimes shortened as *AuthN*. Single-factor authentication relies on one method of verification, while **multi-factor authentication (MFA)** adds layers of security by requiring

two or more proofs of identity. MFA is a security measure that requires users to provide more than one piece of evidence to prove their identities. These are:

- Something you know, like a password
- Something you have, like a security token
- Something you are, like a biometric

MFA must be a combination of two or more of the above. For example, a PIN and password cannot be called MFA because both fall under something you know. A PIN and a biometric is MFA because they are a combination of something you know and something you are.

Single Sign-On (SSO) allows users to authenticate once and later seamlessly authenticate to resources that rely on the same identity.

Identification and authentication normally occur as a single two-step process.

Authorization

Just because an entity is authenticated, it does not mean that it has the authorization to access resources. Authorization is the process of determining what actions or permissions the entity has within the system. It ensures that only entities with the appropriate roles, attributes, or permissions can access specific resources or perform certain functions. For example, administrators can grant access to files based on user's role. Authorization is sometimes shortened as *AuthZ*.

Accountability

Accountability is the process of holding users accountable for the actions they take. Accountability ties the identity to actions and behaviors within a digital system. By maintaining logs and tracking activity, organizations can monitor how identities interact with resources, detect anomalies, and enforce security policies. For instance, auditing can document instances when a user accesses, modifies, or deletes a file. This helps ensure accountability within the system. Accountability not only aids in addressing security incidents but also supports regulatory compliance and auditing efforts.

Together, authentication, authorization, and accountability provide for **nonrepudiation**. Nonrepudiation ensures that a user who performed an action cannot deny performing it or that it occurred.

Identity provider (IdP)

An identity provider is a system that creates, manages, and maintains identity information and offers authentication, authorization, and auditing services. With modern authentication all services are provided by a centralized identity provider. By utilizing a central identity provider,

organizations are able to implement robust authentication and authorization policies, monitor user activity, detect suspicious behaviors, and mitigate the risk of malicious attacks.

Microsoft Entra is Microsoft's cloud-based identity provider. Other examples include Okta, Ping identity, and many more.

Identity and access management

Identity and access management (IAM) is the backbone of modern organizational security, ensuring that the right individuals have access to the right resources at the right times and for the right reasons. At its core, IAM empowers businesses to manage digital identities and control access to critical systems and data efficiently. By implementing IAM, organizations can streamline authentication processes, reduce risks of unauthorized access, and ensure regulatory compliance.

IAM systems provide the following functionality:

- **Identity management**: This is the process of creating, storing, and managing identity information.
- **Identity federation**: Using identity federation, organizations can allow users to use credentials from another system (for example, social identities like Google, Facebook, or Apple) to gain access to their applications.
- **Provisioning and deprovisioning**: This process involves creating user accounts, controlling resource access, and assigning permissions.
- **Authentication**: IAM systems authenticate users, applications, and device identities by confirming that they are who they claim to be. MFA and SSO can be applied at this level.
- **Authorization**: This ensures that users are granted the right access to the resources that they need to access.
- **Access control**: This process involves establishing user roles and permissions, as well as implementing robust authentication and authorization protocols. Access controls are employed to manage and restrict data access appropriately.
- **Reporting and monitoring**: IAM systems can generate reports on sign-in times, system accessed, types of authentication methods used to ensure compliance, and highlight security risks.

The following figure shows how a typical IAM system works:

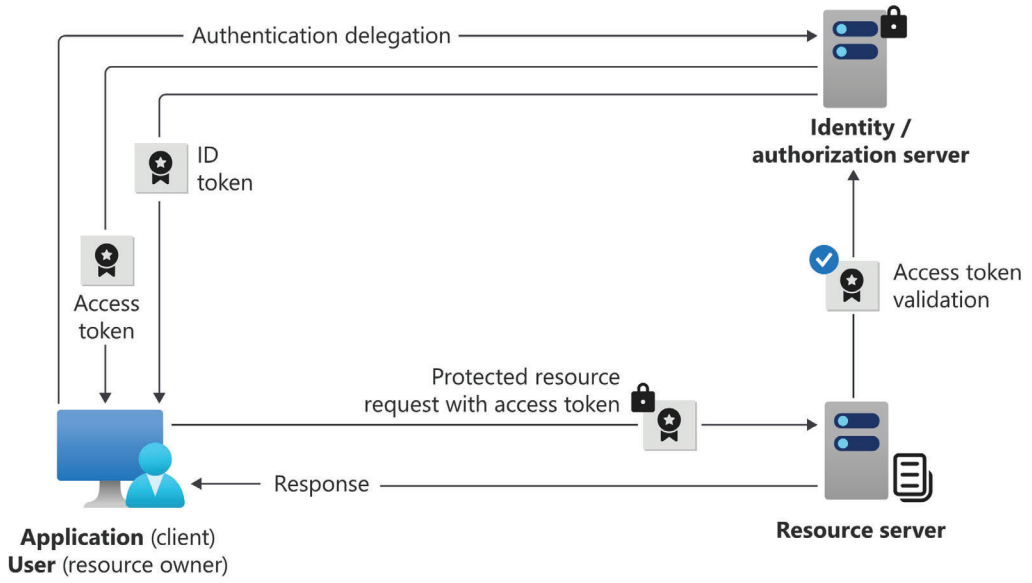


Figure 1.1: Authentication and authorization process

The user initiates an authentication request from the client application with the IdP. If the credentials are valid, the IdP sends an ID token to the client application. The ID token contains information about the user. The IdP obtains end-user consent and authorizes the client application to access protected resources. Authorization is issued in the form of an access token, which is subsequently transmitted to the client application. The access token is then included with all future requests to the protected resource initiated by the client application. Upon receiving a request, the resource server validates the access token; if validation succeeds, the requested resources are made available, and a response is returned to the client application.

Authentication and authorization standards

Before moving forward, it is important to understand some of the commonly used authentication and authorization standards.

OAuth

OAuth (**Open Authorization**) is a standard that allows users to authorize one app or service to sign on to another without revealing the password. It uses access tokens to prove a user's identity and allows it to interact with another service on the user's behalf. A typical example is websites showing messages like "**Login with Facebook**". OAuth was originally designed for websites and is not widely used today.

OAuth 2.0 is the latest release of OAuth and is designed for both apps and websites. It completely replaced OAuth and is now the industry standard for online authorization. It provides consented access and restricts the actions that a client app can perform on a user's behalf without sharing the user's credentials.

Security Assertion Markup Language (SAML)

SAML is an XML-based open standard for securely exchanging authentication and authorization data between an IdP and an application. It facilitates SSO, enabling users to access multiple applications with a single set of credentials. SAML ensures secure communication through assertions, which carry information about user identity, authentication, and permissions.

OpenID Connect (OIDC)

OIDC is an identity layer built on top of the OAuth 2.0 protocol, designed to simplify authentication processes. It uses ID tokens to allow client applications to verify a user's identity and obtain identity claims. It provides authentication while OAuth 2.0 provides authorization. After the release of OpenID Connect that uses public-key encryption, OpenID became a popular choice for the authentication layer for OAuth 2.0. It enables client applications to authenticate users and retrieve their identity information without requiring direct access to sensitive credentials. Like SAML, OIDC is used for SSO but instead of XML, it uses **Representational State Transfer (REST)** and **JavaScript Object Notation (JSON)**. It is designed to work with both native and mobile applications. It uses **JSON Web Tokens (JWTs)** for securely sharing identity assertions, allowing seamless integration across web apps, APIs, and mobile platforms.

JSON Web Tokens (JWTs)

JWTs are open standard, compact, and URL-safe tokens used for securely transmitting information between parties. JWTs are digitally signed and can be encrypted and authenticated making them verifiable and trustworthy. They pass the identity of authenticated users between the IdP and the service. They consist of three parts: a header, payload, and signature. The header specifies the token type and signing algorithm, while the payload contains claims about the user or application. The signature ensures the integrity and authenticity of the token.

System for Cross-Domain Identity Management (SCIM)

SCIM is an open standard that simplifies identity management by automating user provisioning and deprovisioning across systems. It is particularly useful for ensuring consistency in large-scale environments where multiple applications require user data synchronization. SCIM uses RESTful APIs and JSON, making it efficient for exchanging information like user profiles and group memberships.

Web Services Federation (WS-Fed)

WS-Fed is a Microsoft-developed protocol widely used in its applications to transport security tokens for identity and authorization exchange. It facilitates the sharing of authentication and authorization data between trusted domains, allowing users to access multiple applications without repeatedly signing in. WS-Fed employs XML-based messaging to ensure interoperability across platforms, supporting enterprise-level integration for web services. By enabling SSO and identity delegation, WS-Fed enhances security and user convenience.

Microsoft Identity platform

The Microsoft identity platform is a comprehensive cloud-based identity service enabling developers to create applications that support user authentication through Microsoft identities or various social accounts. It facilitates secure access to an organization's proprietary APIs as well as Microsoft APIs, such as Microsoft Graph. Using this, developers can build single-tenant line-of-business applications or multitenant **Software-as-a-Service** (**SaaS**) applications.

There are several components that make up the Microsoft identity platform. They are described as follows:

- **Authentication service**: OAuth 2.0 and OpenID Connect standard-compliant authentication service enables developers to authenticate various identity types like Microsoft Entra ID accounts, personal Microsoft accounts, and social or local accounts using Microsoft Entra External ID.
- **Open-source libraries**: The Microsoft identity platform supports the **Microsoft Authentication Library (MSAL)** and other standards-compliant libraries. Microsoft recommends using MSAL as they provide support for Conditional Access scenarios, SSO, token caching, and more.
- **Microsoft identity platform endpoint**: The Microsoft identity platform endpoint is OIDC certified. It works with MSAL and implements human readable scopes in accordance with industry standards.
- **Application management portal**: This is the Microsoft Entra admin center that provides the configuration experience and other application management capabilities.
- **Application configuration API and PowerShell**: The Microsoft identity platform offers programmatic configuration capabilities of application using Microsoft Graph API and PowerShell enabling organizations to automate DevOps tasks.
- **Developer content**: This includes technical documentation, tutorials, API reference, and code samples.

The following graphic shows the Microsoft identity platform at a high level. It shows the app registration experience, endpoints, **Software Development Kits (SDKs)**, and supported identities.

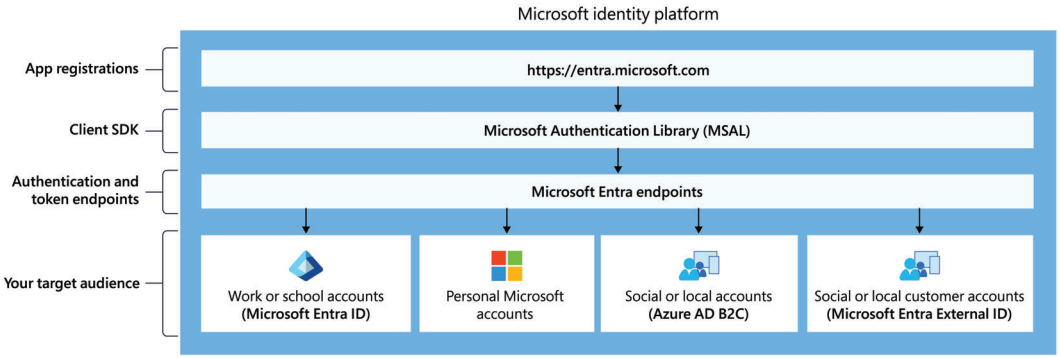


Figure 1.2: Microsoft identity platform

Microsoft Entra

Microsoft Entra is a comprehensive suite of identity and network access products designed to help organizations implement zero-trust architecture. It ensures secure interactions by verifying identities, validating access permissions and conditions, encrypting communication channels, and monitoring for anomalies. Microsoft Entra creates a trust fabric that supports Conditional Access and seamless SSO functionalities. It empowers organizations with tools like programmatic configuration APIs, PowerShell capabilities, and advanced application management through the Microsoft Entra admin center.

The following products are part of the Microsoft Entra family.

Microsoft Entra ID

Microsoft Entra ID, formerly known as Azure Active Directory, is Microsoft's cloud-based identity and access management solution. It provides basic identity, authentication, authorization, and auditing for employees, business guests, devices, and applications. Using Microsoft Entra ID employees can access cloud-based resources like Microsoft 365, Azure, and thousands of other SaaS applications. They can also access internal resources like on-premises applications and file servers running on the corporate network.

IT administrators can use Entra ID to create and manage user accounts including employees and business guests. They can control access to resources by implementing features such as MFA and Conditional Access policies. Entra ID also allows integration with applications to provide SSO capabilities to users. With these powerful tools, administrators can protect user identities and meet access governance requirements.

Application developers can use Microsoft Entra ID as a standards-based authentication provider that helps them provide SSO access to their applications. They can use Microsoft Entra APIs to build pixel-perfect, personalized user experiences.

Microsoft cloud services like Microsoft 365, Azure, and Dynamics use Microsoft Entra ID as their identity provider.

Licensing

To use the services provided by Microsoft Entra ID, organizations must be adequately licensed. It is licensed on a per user per month basis. Each user benefiting from the service must be assigned an appropriate license. The following license types are available:

- **Microsoft Entra ID Free**: All organizations using Microsoft 365, Azure, or Dynamics CRM already use Microsoft Entra ID. By default, they have the Microsoft Entra ID Free license that provides basic user and group management, on-premises directory synchronization, basic reports, self-service password reset for cloud users, SSO, and more.
- **Microsoft Entra ID P1**: This has all the features provided by Microsoft Entra ID Free. In addition, it supports advanced administration capabilities like dynamic groups, self-service group management, and security capabilities like Conditional Access policies. It can be purchased as standalone or as a part of Microsoft 365 E3 and Microsoft 365 Business Premium.
- **Microsoft Entra ID P2**: In addition to all features included in Free and P1, P2 also includes **Microsoft Entra ID Protection**, **Privileged Identity Management**, and basic identity governance capabilities. It can be purchased as standalone or as a part of Microsoft 365 E5.
- **Microsoft Entra Suite**: Microsoft Entra Suite combines network access, identity protection, identity governance, and identity verification solutions. It is available to subscribers of Microsoft Entra ID P1 and P2. It includes Microsoft Entra ID Protection, **Microsoft Entra ID Governance**, **Microsoft Entra Verified ID**, **Microsoft Entra Internet Access** and **Microsoft Entra Private Access**.

Microsoft Entra ID is administered from the **Microsoft Entra admin center** at `https://entra.microsoft.com`. The following figure shows a snapshot of the Microsoft Entra admin center homepage. The homepage is organized by products, which are available in the left navigation menu.

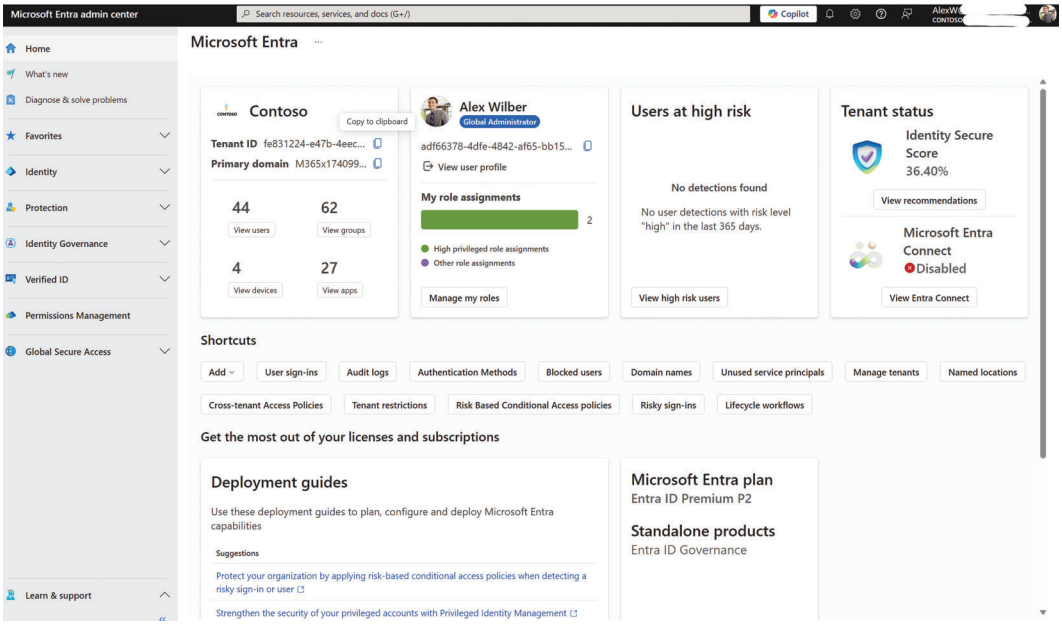


Figure 1.3: Microsoft Entra admin center

Microsoft Entra Domain Services

Microsoft Entra Domain Services provides services like Group Policy, **Lightweight Directory Access Protocol** (**LDAP**), and Kerberos/NTLM authentication. A managed domain in Domain Services helps organizations run legacy applications that cannot use modern authentication without needing to manage an on-premises Active Directory (AD) infrastructure.

Domain Services seamlessly integrates with Microsoft Entra allowing users to sign in to connected services and applications using their existing credentials. Existing groups and user accounts can be used to secure access to resources. This allows a smooth lift-and-shift of on-premises resources to the cloud.

Pricing

Microsoft Entra Domain Services is available in three plans and usage is charged per hour depending on the plan selected. The following table explains the three plans:

Feature	Standard	Enterprise	Premium
Transactions (per hour)	0 - 3000	3000 - 10000	10000 - 70000

Feature	Standard	Enterprise	Premium
Object count	0 – 25000	25000 - 100000	100000 – 500000
Back up frequency	Every 5 days	Every 3 days	Daily
Replicas	Not available	Available	Available
Custom attributes	Not available	Available	Available
Cloud-only sync	Not available	Available	Available
Trusts	Not available	Available	Available

Table 1.1: Microsoft Entra Domain Services plans

Note

Transactions per hour and object count are guidelines and not product limitations. These are provided to enable selection of the appropriate plan.

Microsoft Entra Domain Services will be covered in detail in *Chapter 4, Microsoft Entra Domain Services*.

Microsoft Entra ID Governance

Microsoft Entra ID Governance is an identity governance solution that helps organizations improve productivity, strengthen security, and meet regulatory requirements. Using this, administrators can ensure that the right users have access to the right resources. It helps organizations mitigate identity and access risks by protecting, monitoring, and auditing access to resources.

Microsoft Entra ID Governance helps organizations remain compliant by:

- Ensuring that the right users have access to the right resources
- Understanding how the users are using that access
- Ensure that there are controls in place to manage access
- Facilitate auditing to ensure that the controls are working effectively

Using Microsoft Entra ID Governance, organizations can govern the identity and access lifecycle of employees and business guests and ensure secure privileged access for administrators.

Identity and access lifecycle

Each identity goes through a lifecycle from the time an employee joins the organization to the time they leave. During this time, they may hold different positions and move across the organization. This is known as the *joiner-mover-leaver* scenario as shown in the following figure:

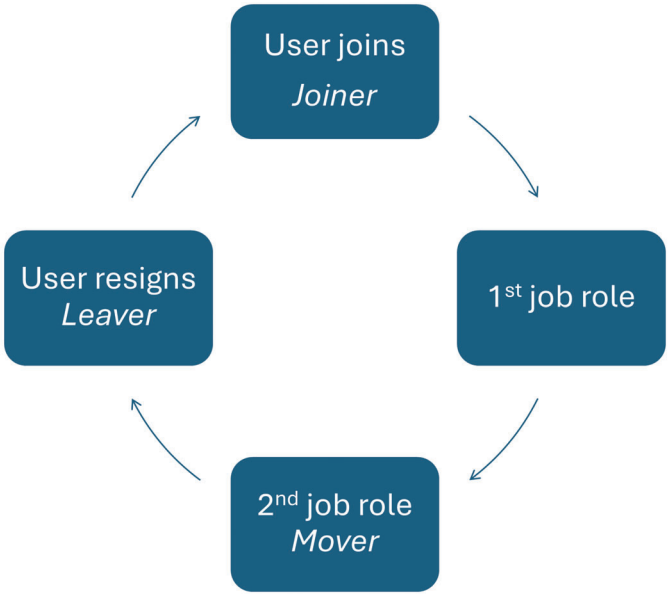


Figure 1.4: Identity and access lifecycle

In most organizations when a user joins, their identity is created in the **Human Capital Management (HCM)** system. Organizations should be able to automate onboarding of users from HCM to the identity system so that they can be productive on day 1. Microsoft Entra ID Governance has the following capabilities that can help organizations automate the identity and access management lifecycle:

- **Inbound provisioning from HCM systems**: Microsoft Entra offers out-of-the-box capabilities to retrieve identities from Workday and SuccessFactors and automatically create those identities in Microsoft Entra ID and Active Directory.
- **Lifecycle workflows**: They are used to automate mundane tasks at different stages in the identity lifecycle. These workflows can be triggered based on certain events like date of joining, change in department, or change in employee leave date. For example, a workflow could be triggered to enable the user's account on the day of joining, send a welcome email, and add the user to required groups and Teams. Lifecycle workflows will be covered in *Chapter 7, Microsoft Entra Lifecycle Workflows*.

- **Entitlement management access packages**: Using this, organizations can provide birthright access to users so that they get access to all the resources they need to do their job. Based on user attributes like department or location, users can be given access to SharePoint sites, applications, or groups. Entitlement management access packages will be covered in *Chapter 6, Microsoft Entra Entitlement Management.*
- **Entitlement management access reviews**: Using access reviews, organizations can periodically recertify access requirements to ensure that users still need access to resources they were given. Entitlement management access reviews will be covered in *Chapter 6, Microsoft Entra Entitlement Management.*

Privileged access lifecycle

Organizations also need to govern privileged accounts to prevent misuse and ensure that administrators have the right permissions to perform the tasks that they need to complete. Microsoft **Entra Privileged Identity Management (PIM)** helps provide just-in-time access to administrators. Just-in-time access is an approach that ensures administrators receive the precise permissions they need for a specific task for a limited duration. This minimizes risks by reducing the exposure of sensitive systems to over-permissioned accounts. PIM helps implement this model by enabling temporary access to high-level permissions. By requiring approval workflows, monitoring, and expiration of elevated rights, organizations can prevent misuse and enhance security.

Licensing

Microsoft Entra ID Governance offers advanced identity governance capabilities to Microsoft Entra ID P1 and P2 customers. They are available as two products – **Microsoft Entra ID Governance** and **Microsoft Entra ID Governance Step up for Microsoft Entra ID P2**.

These two products have the basic identity governance features that are part of Microsoft Entra ID P2. Additionally, they have more advanced identity governance features. The identity governance features are the same in both products. The only difference is that they have different prerequisites.

To purchase an Entra ID Governance license, the tenant needs an active subscription to AAD Premium or AAD Premium P2. This requirement is met if you have Microsoft Entra ID P1, Microsoft 365 E3/E5, EMS E3/E5, or Microsoft 365 F1/F3.

To purchase Microsoft Entra ID Governance step up for Microsoft Entra ID P2, the tenant needs AAD Premium P2. This requirement is met if you have Microsoft Entra ID P2, Microsoft 365 E5, EMS E5, M365 E5/F5 Security, or M365 F5 Security + Compliance.

Microsoft Entra Privileged Identity Management will be covered in detail in *Chapter 8, Microsoft Entra Privileged Identity Management.*

Microsoft Entra Identity Protection

Microsoft Entra Identity Protection helps organizations detect, investigate, and respond to identity-based risks. These risks can be used to enforce risk-based Conditional Access policies or be sent to a **Security Information and Event Management (SIEM)** tool for investigation.

Microsoft receives trillions of risk signals every day from sources like Microsoft Accounts, Microsoft 365, Xbox, and more. These signals help detect risky behavior like atypical travel, anonymous IP addresses, password spray attacks, leaked credentials, and more. Each time a user attempts to sign in, ID protection checks in real time if the user or the sign-in attempt is risky and assigns a risk level. Based on the risk level, appropriate policies can be applied to protect the user and the organization. The detected risks are recorded and tracked, and the reports are available for administrators to investigate and take action.

Licensing

Full feature set of Microsoft Entra Identity Protection is available in Microsoft Entra P2 and Microsoft Entra Suite.

Microsoft Entra Identity Protection is covered in detail in *Chapter 9, Microsoft Entra Identity Protection*.

Microsoft Entra Verified ID

Decentralized Identities (DIDs) represent a transformative approach to identity management. Unlike traditional systems that rely on centralized entities, DIDs allow individuals to manage their own identity information securely. By leveraging blockchain or distributed ledger technologies, DIDs ensure that users retain control over their personal data, reducing reliance on third-party providers. This innovation empowers users with greater privacy and autonomy, fostering trust in digital interactions.

Based on open DID standards, Microsoft Entra Verified ID enables organizations to issue verifiable credentials to users that can be stored on their personal devices. They can then present these digital credentials to any organization when they want to prove their identity. For example, Sally works for Contoso. Contoso has issued Verified ID to their employees which Sally has stored in a wallet on her phone. When she applies for a home loan, the bank offers discounted interest rates to Contoso employees. Sally uses the Verified ID stored on her phone to prove that she is an employee of Contoso. The wallet application records the transaction to show where Sally used her proof of employment.

Licensing

Microsoft Entra Verified ID offers high-assurance identity verification and is included with any Microsoft Entra ID subscription:

- **Microsoft Entra Verified ID Baseline protection**: Offers up to 50,000 transactions per month for free. Any issuance, verification or revocation of a credential is a transaction. To perform more than 50,000 transactions per month customers must have Entra ID P1 or P2 licenses.
- **Face check with Microsoft Entra Verified ID**: Offers high-assurance verification with a privacy-respecting face check feature. Face check can be added as standalone where the customer is charged for every face check. If the customer has Entra Suite, they can perform 8 face check verifications per user per month.

Microsoft Entra Verified ID will be discussed in detail in *Chapter 10, Microsoft Entra Verified ID*.

Microsoft Entra Workload ID

Each entity that requires authentication has an identity. At a high level, there are two types of identities: human and machine/non-human. Human identities are assigned to individual users, while machine or non-human identities are used by devices, applications, and services. The following image shows this in detail:

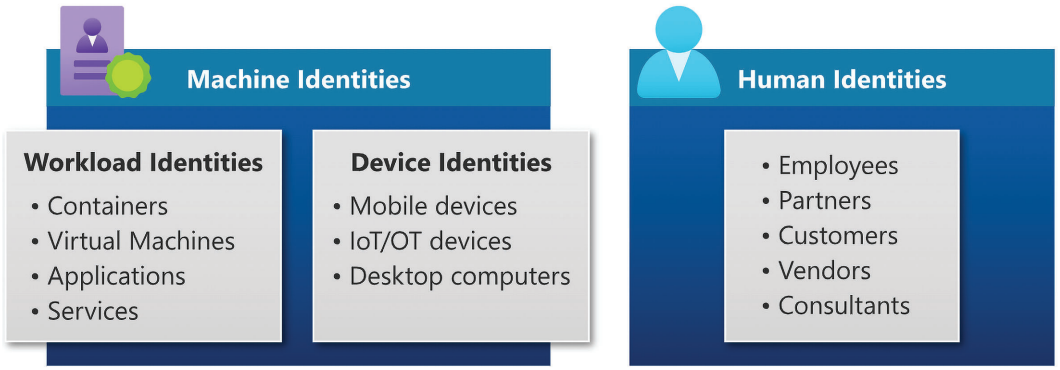


Figure 1.5: Machine and human identities

In Microsoft Entra, identities used by applications, service principals, and managed identities are called workload identities. Microsoft Entra Workload ID is the identity and access management solution for workload identities.

Licensing

The following licensing options are available:

- **Free**: The free version is available with subscription of services like Azure and Power Platform and offers features like creating and managing workload identities, access resources by authenticating workload identities, auditing sign-in activity, workload identity federation, and application management policies.
- **Microsoft Entra Workload ID premium**: It is available as standalone and offers advanced lifecycle management features in addition to the features offered by the Free plan. These include access reviews, app health recommendations, Conditional Access policies, and ID protection.

Microsoft Entra Workload ID will be covered in detail in *Chapter 11, Microsoft Entra Workload ID*.

Microsoft Entra External ID

Microsoft Entra External ID offers a secure way of collaborating with external identities, such as business partners and vendors, on internal applications and resources. In addition, it also helps manage **Customer Identity and Access Management (CIAM)** for customer-facing applications. Users can bring their own identities, ranging from corporate-issued to social accounts like Google, Facebook, or Apple.

The following figure shows the Microsoft Entra External ID ecosystem:

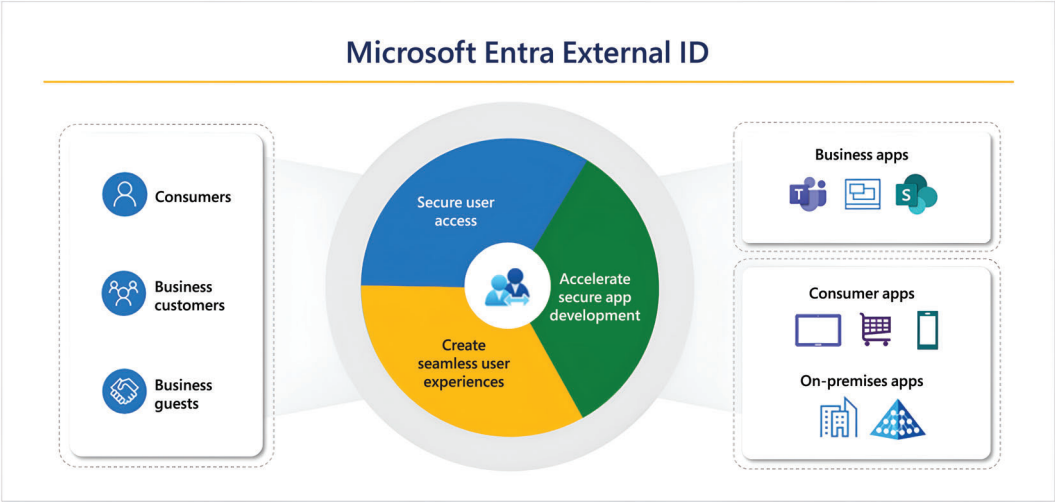


Figure 1.6: Microsoft Entra External ID

External ID scenarios fall under **Business to Business (B2B)** or **Business to Consumer (B2C)**. Let's consider some examples:

- **B2B**: When organizations want their employees to collaborate with business partners and vendors on internal applications, they can use External ID for B2B collaboration. This allows organizations to securely invite business partners and vendors as guests to their *workforce* tenant. They can determine the level of access the guests have and govern their identity lifecycle using the Entra ID Governance capabilities. For example, if your organization is partnering with another organization on a project and needs to collaborate with the external organization on Teams, you can invite the employees from the external organization as business guests for easy collaboration.
- **B2C**: When an organization wants to give access to end consumers to commercial applications they can use Entra External ID in the *external* tenant. Organizations can register their applications, customize branding, and create customized user journeys. Typical examples include booking movie tickets, ordering groceries online, and booking airline tickets.

Before we move on, let's understand the difference between workforce and external tenants.

In Microsoft Entra, a *tenant* is a dedicated instance of Microsoft Entra ID that contains an organization's resources like user accounts, devices, and applications. There are two ways to configure a tenant depending on how the organization intends to use it:

- A **workforce** tenant is a regular Microsoft Entra tenant that contains employees, internal business applications, and other organizational resources. In a workforce tenant, employees are **members** and external users are **guests**. Employees and business guests can collaborate using B2B collaboration.
- An **external** tenant is used exclusively for consumers. This is a separate tenant from the workforce tenant. It follows the standard Entra tenant model but is designed exclusively for consumer and consumer-facing applications.

The following table compares the scenarios for each:

	External ID in workforce tenant	**External ID in external tenant**
Primary scenario	Employees to collaborate with business guests on internal applications.	Publish apps to external consumers.
User management	Business guest identities are managed in the same tenant as the employees	Apps and consumer identities are managed in a separate tenant outside of the workforce tenant.
SSO	SSO to all Microsoft Entra ID connected apps.	SSO to apps registered in external tenant
Branding	Branding has the Microsoft look and feel.	Completely customizable and does not include Microsoft look and feel.

Table 1.2: Workforce tenant vs external tenant

Pricing

Entra External ID billing is based on **Monthly Active Users (MAU)**. The first 50,000 MAU are free. Each user who authenticates to the tenant once a month contributes to the MAU.

Entra External ID is discussed in detail in *Chapters 12 and 13*.

Global Secure Access

The way of working has changed. The days when people worked in traditional offices are long gone. Today, people work from anywhere. As applications and data move to cloud, security threats increase. The modern way of working demands more than perimeter security. An identity-aware cloud-delivered security solution is the need of the hour. This new security category is called **Secure Services Edge (SSE)**.

Microsoft's SSE solution is called **Global Secure Access (GSA)**. This is a unifying term used for **Microsoft Entra Internet Access** and **Microsoft Entra Private Access**. GSA is built on core zero trust principles. The following picture shows these components:

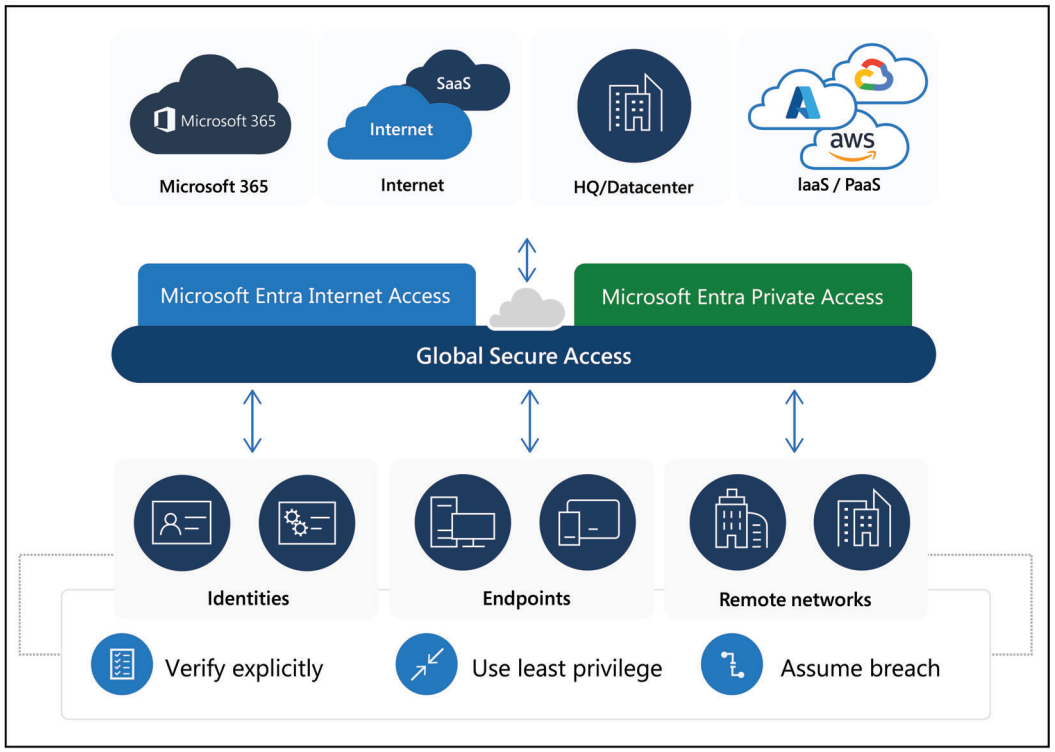


Figure 1.7: Global Secure Access

Microsoft Entra Internet Access and Microsoft Entra Private Access, together with **Microsoft Defender for Cloud Apps** (Microsoft's cloud-focused Cloud Access Security Broker), converge network, identity, and endpoint access controls to help organizations protect any application or resource from anywhere. Microsoft Entra ID simplifies policy management and enables secure employee access to any cloud or on-premises workloads.

GSA streamlines the roll-out and management of access control capabilities using Microsoft's network spanning 70 regions and more than 190 network edge locations.

Microsoft Entra Internet Access

Microsoft Entra Internet Access provides secure access to internet and SaaS applications with an identity-based **Secure Web Gateway (SWG)**. It can acquire network traffic either from the user's desktop or from a remote location like a branch office. It is context aware, and uses information like user, device, location, and risk to apply Conditional Access policies. It enables web-content filtering based on web content categories or **Fully Qualified Domain Names (FQDN)**.

Microsoft Entra Internet Access for Microsoft Services

This service provides direct connectivity to Microsoft Services, improving security and performance. Using this service, organizations can connect to Microsoft services directly from a desktop or branch location. **Universal Tenant Restrictions** can be applied to reduce the risk of data exfiltration to unauthorized accounts or tenants. It offers improved threat detection with source IP restoration for Entra ID sign-in logs.

Microsoft Entra Internet Access will be covered in *Chapter 14, Microsoft Entra Internet Access*.

Microsoft Entra Private Access

Using Microsoft Entra Private Access, organizations can provide users secure access to private, corporate resources without a **Virtual Private Network (VPN)**. It builds on Microsoft Entra application proxy and offers per-app adaptive access using Conditional Access policies that provide more granular security than a VPN. Microsoft Entra Private Access provides zero-trust access to a range of IP addresses or FQDNs using a feature called **Quick Access**. Organizations can modernize authentication to legacy applications using its integration with Conditional Access and provide a seamless experience to end users by acquiring network traffic from desktops. It can work side-by-side with existing non-Microsoft SSE solutions.

Microsoft Entra Private Access will be covered in *Chapter 15, Microsoft Entra Private Access*.

Licensing

Both Microsoft Entra Internet Access and Microsoft Entra Private Access can be bought as standalone products or as a part of Entra Suite. Organizations that choose to buy these products as standalone must have at least Microsoft Entra ID P1 licenses.

Microsoft Entra Internet Access for Microsoft services capabilities are included in Microsoft Entra ID P1 or P2 licenses.

Summary

In this chapter, we learned the basics of identity and identity and access management. We also discussed the common authentication and authorization standards. Additionally, we learned about the Microsoft identity platform and how it supports application developers. Lastly, this chapter introduced the Microsoft Entra suite of products, their basic features, and licensing. The rest of the chapters in this book will build upon the content of this chapter. In the next chapter, we will learn the fundamentals of Microsoft Entra ID such as SSO, MFA, authentication methods, and Conditional Access.

Exercises

1. Which of the following is NOT a part of the Microsoft Entra Suite?
    a. Microsoft Entra ID Governance
    b. Microsoft Entra Private Access
    c. Microsoft Entra Identity Protection
    d. Microsoft Entra Workload ID
2. Which of the following is NOT an example of multifactor authentication (MFA)?
    a. Password and security token
    b. Password and PIN
    c. Password and biometric
    d. Password and SMS OTP
3. Which of the following statements best describes a key difference between OAuth 2.0 and SAML?
    a. OAuth 2.0 is designed for Single Sign-On (SSO), whereas SAML is used for authorization between services
    b. OAuth 2.0 uses JSON-based messages, while SAML relies on JSON-based tokens
    c. OAuth 2.0 primarily facilitates delegated authorization, while SAML is more focused on authentication and SSO
    d. OAuth 2.0 and SAML are both token-based protocols that only support mobile application workflows

Answers

1. d
2. b
3. c

Additional resources

- Microsoft Entra: `https://learn.microsoft.com/en-us/entra/fundamentals/what-is-entra`
- Microsoft identity platform: `https://learn.microsoft.com/en-us/entra/identity-platform/v2-overview`

- What is OAuth: `https://www.microsoft.com/en-us/security/business/security-101/what-is-oauth?msockid=23427ecd38c8604e1d566b1d39d861e9`
- What is OIDC: `https://www.microsoft.com/en-us/security/business/security-101/what-is-openid-connect-oidc?msockid=23427ecd38c8604e1d566b1d39d861e9`
- JWTs: `https://learn.microsoft.com/en-us/entra/identity-platform/v2-protocols#tokens`
- SAML: `https://learn.microsoft.com/en-us/entra/identity-platform/saml-protocol-reference`
- SCIM: `https://learn.microsoft.com/en-us/entra/identity/app-provisioning/use-scim-to-provision-users-and-groups`
- WS-Fed: `https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-adfsod/204de335-ea34-4f9b-ae73-8b7d4c8152d1`

Get this book's PDF version and more

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.





Note: Keep your invoice handy. Purchases made directly from Packt don't require an invoice.

2

Fundamentals of Microsoft Entra ID

Microsoft Entra ID is an identity and access management solution intended for enterprise environments. Its main purpose is to provide secure and streamlined access to resources, applications, and services, whether on-premises or in the cloud. Organizations can use Entra ID to authenticate users, manage permissions, and enforce policies aimed at protecting sensitive data from unauthorized access. Conditional Access enables administrators to implement access controls based on user identity, device status, or location. Multifactor authentication is available as an additional security measure, requiring more than just passwords for access. The platform also offers SSO capabilities, allowing users to access different applications and services efficiently.

This chapter will cover:

- Microsoft Entra roles
- Single Sign-On (SSO) and Multi-Factor Authentication (MFA)
- Authentication methods
- Conditional access
- Protected actions

These topics are essential to understanding the more complex topics that the rest of the book will cover.

Microsoft Entra roles

Microsoft Entra follows the **role-based access control (RBAC)** model. RBAC assigns permissions based on specific roles, ensuring users have access only to the resources required for their duties. This minimizes security risks by restricting unauthorized access. Microsoft Entra roles control access to Microsoft Entra resources like users, groups, devices, and applications using the Microsoft Graph API.

It is important to understand how Microsoft Entra ID determines if a user has access to a resource. This information will be useful when troubleshooting access issues. The following are the high-level steps:

1. A user acquires a token for the Microsoft Graph endpoint
2. The user makes an API call to Microsoft Entra ID via Microsoft Graph using the issued token
3. Microsoft Entra ID either evaluates the user's role memberships based on the claims in the user's access token or retrieves all role assignments that apply to the user directly or through group memberships to the resource on which the action is being taken
4. Microsoft Entra ID determines if the action in the API call is allowed in the roles that this user has on the resource. If it is allowed, the access is granted; otherwise, it is denied.

Microsoft Entra offers the following types of roles.

Built-in roles

Built-in roles are out-of-the-box roles with a predefined set of permissions. These roles cannot be modified. There are several built-in roles in Microsoft Entra and new ones are regularly added by Microsoft. Built-in roles are available with the Microsoft Entra ID Free plan. To view the built-in roles in Microsoft Entra, follow these steps:

1. Log in to `https://entra.microsoft.com` and in the left navigation menu navigate to **Entra ID | Roles & admins | All roles**.
2. The right pane will show the list of built-in roles as shown in the following screenshot:

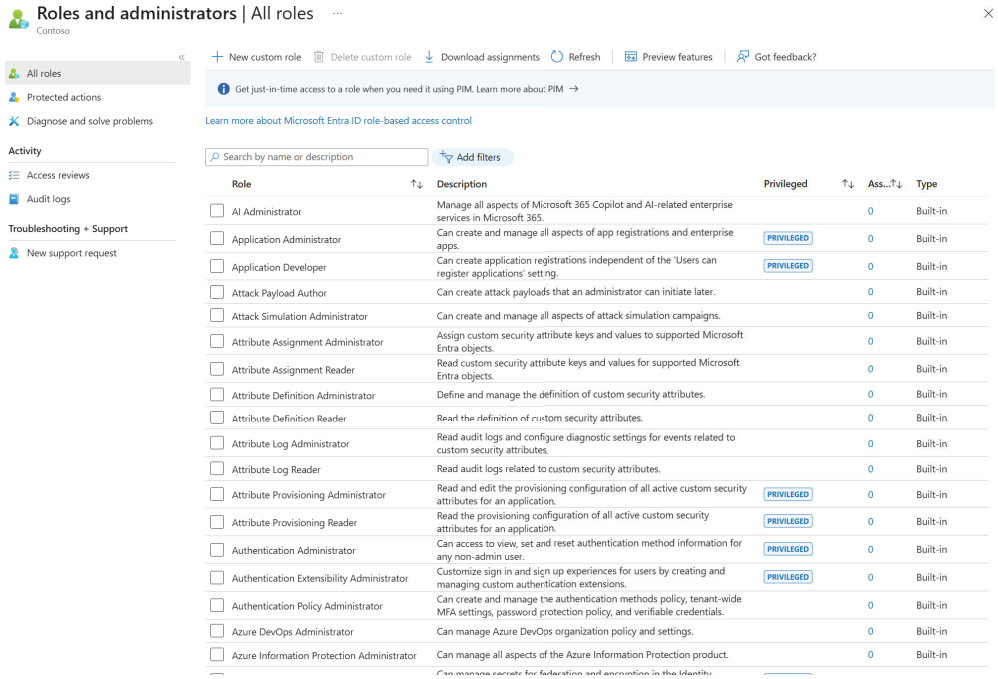


Figure 2.1: Built-in Entra roles

3. Click on any role to see the **Assignments**, **Description**, and **Role settings**. The following screenshot shows the **Description** of the **Global Administrator** role:

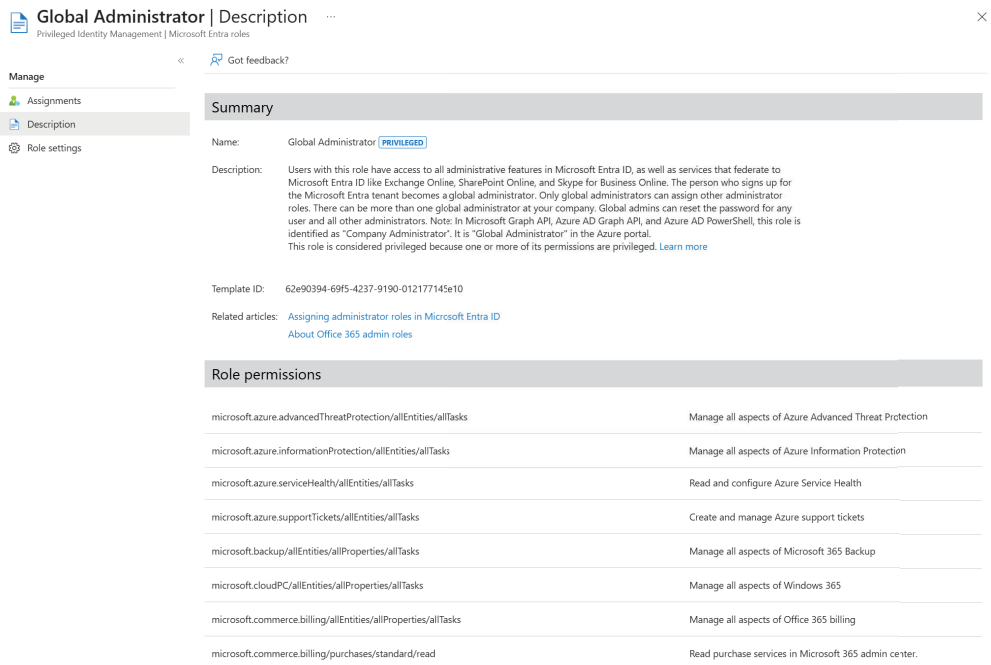


Figure 2.2: Global Administrator role description

Review the permissions for the role to understand its assigned privileges. If you would like to create roles with granular permissions, create custom roles as described in the next section.

Custom roles

For most organizations, the built-in roles meet their requirements. Organizations that have more granular or sophisticated requirements can create custom roles. A custom role is a collection of permissions selected from a predefined list. These are the same permissions used in built-in roles. To create custom roles in Microsoft Entra, you must have an Entra ID P1 or P2 license. The following steps explain how to create a custom role:

1. Log in to `https://entra.microsoft.com` as a **Privileged Role Administrator**. In the left navigation menu click on **Entra ID | Roles & admins | All roles**.
2. In the right pane, click on **New custom role**.
3. On the **Basics** tab, enter a name and description for the role. You can clone baseline permissions for this role from another custom role as shown in the following figure. You cannot clone permissions from a built-in role. Click **Next**:

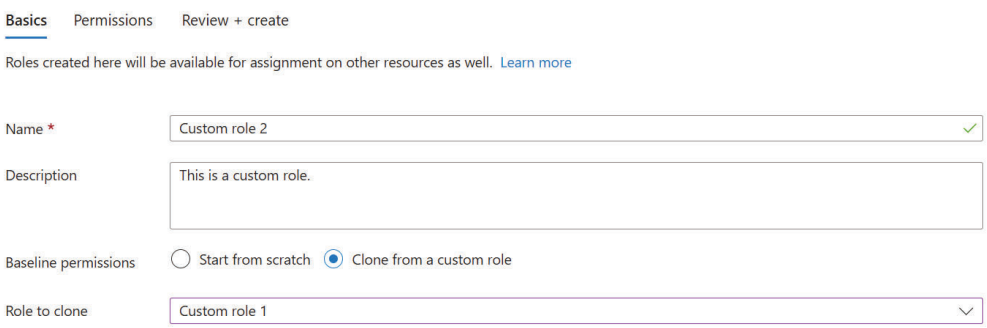


Figure 2.3: Creating a custom role

4. If you cloned from a custom role, the permissions from that role will be preselected on the **Permissions** page. You can add or remove permissions on this screen. If you started from scratch you will need to select all the permissions that this role will have. Refer to *Figure 2.4*. Once done, click **Next**:

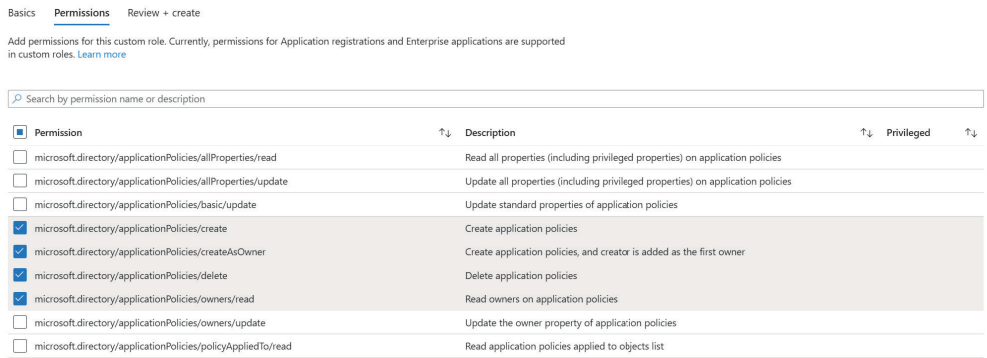


Figure 2.4: Select permissions for custom role

5. On the **Review + create** page, click **Create** to create the role.

Once roles have been created, they need to be assigned to users so that they are able to perform tasks in the Microsoft Entra admin center.

Assigning roles

Users need to be assigned roles for them to be able to perform tasks on Microsoft Entra resources. This is done by creating a role assignment. A role assignment ties a *role definition* to a *security principal* at a *scope* level. These terms are explained as follows:

- **Security principal**: The identity that gets the permissions defined in the role. This could be a user, group, or a service principal.

- **Role definition**: A role is also called a role definition. It is either a built-in or custom role.
- **Scope**: A group of Microsoft Entra resources on which the role definition provides permissions. For example, the entire tenant, an Administrative Unit, or a specific Microsoft Entra resource such as a group or application.

For example, a role assignment could grant a user the App Registration Administrator role only for specific applications.

There are multiple options to assign roles in Microsoft Entra as described next.

Assigning directly to users

This is the default way of assigning roles. Both built-in and custom roles can be assigned directly to users.

Using role-assignable groups

Using this method you create role-assignable groups and assign roles to the groups. Assigning roles to groups makes administration easier than assigning roles to individual users.

To add roles to a group, create a new security or Microsoft 365 group with the `isAssignableToRole` property set to `true`. A role-assignable group has the following restrictions:

- The `isAssignableToRole` property cannot be changed once the group is created.
- You cannot make an already existing group a role-assignable group.
- A role-assignable group cannot have dynamic membership. The members must be manually assigned.
- Another group cannot be added as a member of a role-assignable group.
- A maximum of 500 role-assignable groups can be created in a single tenant.

A Microsoft Entra P1 license is required to create and use role-assignable groups.

Creating role-assignable groups

The following steps explain how to create a role-assignable group:

1. Log in to `https://entra.microsoft.com` as a **Privileged Role Administrator**. In the left menu navigate to **Groups | All groups**.
2. In the right pane, click on **New group**.
3. On the New Group page, enter the group type, name, and description.
4. Set the **Microsoft Entra roles can be assigned to the group** to **Yes** as shown in the following figure:

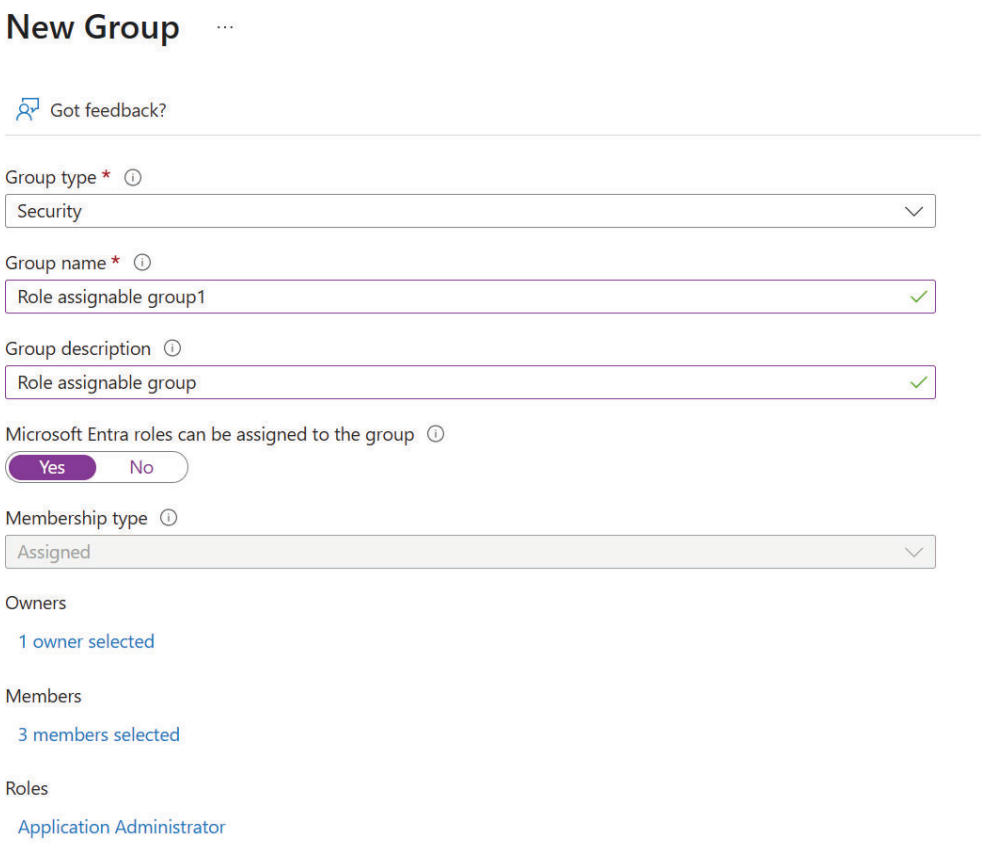


Figure 2.5: Role-assignable group

5. Select the members and owners for the group and optionally, assign roles to the group.

Click **Create**. You will see a message warning that creating a group to which roles can be assigned is a setting that cannot be changed later. Click **Yes** to create the group.

Assigning roles to users or groups

The following are the steps to assign roles to users or role-assignable groups:

1. Log in to `https://entra.microsoft.com` as a **Privileged Role Administrator**. In the left navigation menu, navigate to **Entra ID | Roles & admins | All roles**.
2. In the right pane, click on the role that you want to assign.
3. In the next page, click on **Add assignments**:

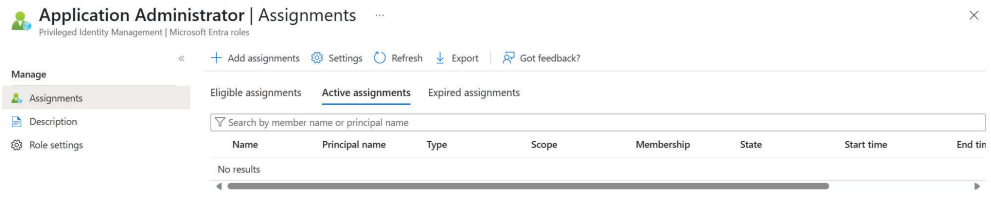


Figure 2.6: Adding assignments

4. On the Add assignments page, select the scope as **Directory**, **Application**, or Service principal. If you choose Application or Service principal, select the application or service principal by clicking on No scope selected. Refer to *Figure 2.7*:

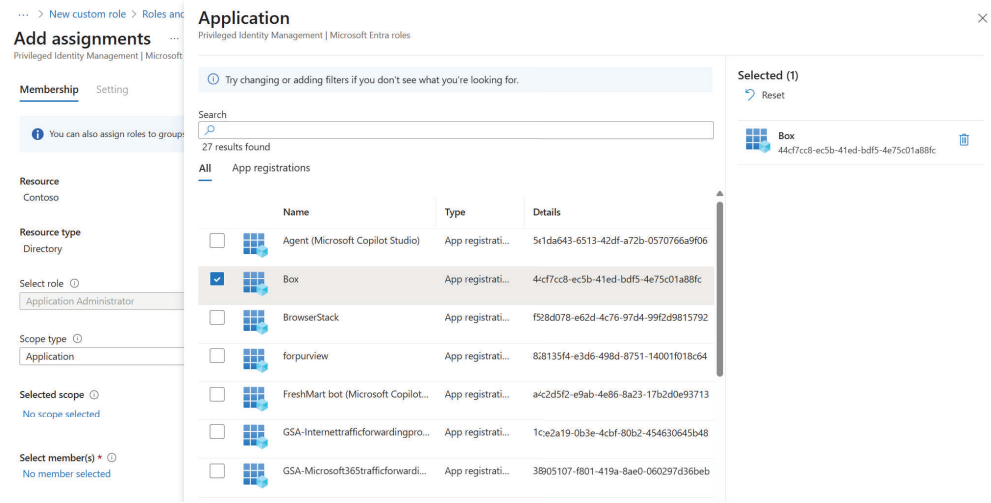


Figure 2.7: Define scope

5. Click **No member selected** to assign the role. Select the user or group to which you want to assign the role and click on **Select**. Refer to *Figure 2.8*. Click **Next** to continue:

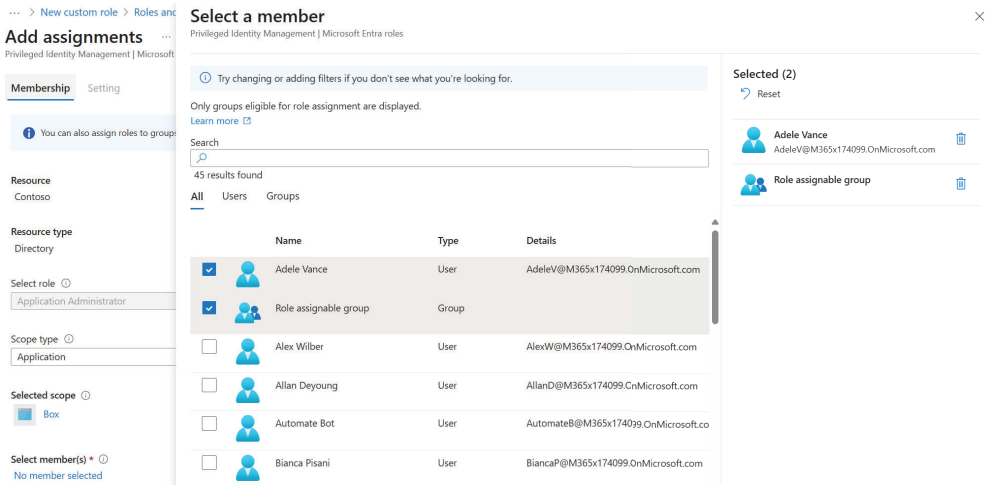


Figure 2.8: Select members

6. On the **Settings** tab, select **Assignment type** as **Active** and provide a justification. Click **Assign** to create the role assignment:

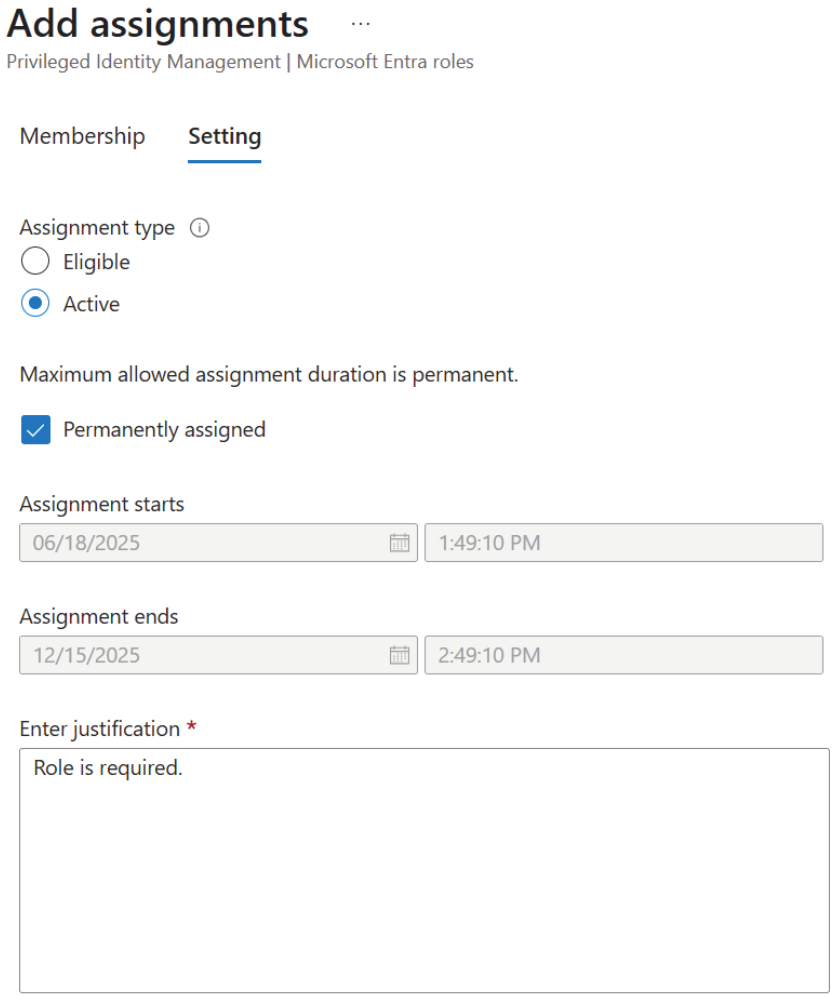


Figure 2.9: Create the assignment

Using role-assignable groups to assign roles eases the administrative overhead of assigning to individual users. You can perform access reviews on role-assignable groups to ensure that the members of the group still require the role.

Using PIM

This allows assigning just-in-time access to roles. A Microsoft Entra ID P2 license is required to use PIM. PIM is discussed in detail in *Chapter 8, Microsoft Entra Privileged Identity Management.*

Single sign-on

Companies create and host web applications and make them available to users to be accessed as a service. Users access these applications using a browser. **Single Sign-On** (**SSO**) makes it possible for users to navigate between these applications without having to enter credentials multiple times. Instead of remembering and entering separate usernames and passwords for each application, users log in once and gain entry to all interconnected systems without further prompts. This approach streamlines user experience by reducing password fatigue and enhances productivity and security.

Microsoft Entra ID application gallery has several applications that can be configured for SSO. There are several SSO options to choose from depending on the needs of the organization. They are listed as follows:

- **Federation**: When SSO is set up to work between multiple **identity providers** (**IdPs**), it is called federation. Federation improves security, reliability, and end-user experience. With federated SSO, users use their Microsoft Entra account to authenticate. Federation is supported for SAML 2.0, WS-Fed, and OIDC applications. It is the richest method of SSO and is recommended over other SSO methods like password-based SSO.
- **Password**: This method is primarily used for on-premises applications that are configured to use **Microsoft Entra Application Proxy**. In this method, the user signs into the application using their password for the first time. For subsequent login attempts, Entra ID provides the user credentials to the application. This enables secure password storage and replay using a web browser extension or mobile application.
- **Linked**: This method provides a consistent user experience for organizations that are in the process of migrating applications to Entra ID. In this method, once the user authenticates with a linked application, a user account needs to be created before SSO can be provided. This account can be created either manually or automatically. The user can see links for all linked applications in their MyApps portal. Conditional Access policies or MFA cannot be used as the linked application does not provide SSO through Entra ID.
- **Integrated Windows Authentication** (**IWA**): Microsoft Application Proxy can be used to provide SSO for applications that use Integrated Windows Authentication. These applications require a Kerberos ticket.
- **Header-based**: Microsoft Entra application proxy supports SSO for applications that use headers for authentication. Header values are configured in Microsoft Entra ID based on application requirements. These values are then sent to the application via

application proxy. This helps organizations to replace VPNs and remove dependencies on on-premises infrastructure.

How SSO is implemented depends on where the application is hosted. This matters because hosting affects the way traffic is routed to access the application. For example, users don't need internet access to access an on-premises application but need it to access an application hosted on the cloud.

As you plan your SSO deployment, consider the following points.

Administrative roles

Adhering to the zero-trust principle, it is advisable to assign roles with the minimum necessary permissions for each task. Carefully assess the available Microsoft Entra roles and select the most appropriate one for each application persona. Certain roles may only be needed on a temporary basis.

Certificates

When SAML applications are federated with Entra ID, a certificate is created that is valid for three years by default. The expiration date can be customized if needed. It is important to document and manage the certificate renewal process to ensure that there are no unforeseen outages due to certificate expiry. Identify the right people who should be involved in managing the certificate lifecycle.

Communication

It is important to set up a proper communication process to proactively inform the relevant stakeholders of any upcoming changes. Identify the relevant stakeholders, including end users of the application, and the process by which they should be informed of upcoming changes and available support options.

Licensing

Typically, the following licenses are required:

- **Microsoft Entra ID**: SSO is free for applications already integrated with Entra ID. Additional licenses may be required if you wish to deploy advanced features.
- **Application licensing**: Some applications require that all users who access the application be assigned appropriate licenses. Check with your application owner to ensure compliance with license requirements.

Shared accounts

Some applications allow the use of shared accounts. From an Entra perspective, there is no difference between applications that use shared accounts and applications that use individual

user accounts. Some additional care may need to be taken while deploying an application that uses shared accounts. The following are some best practices:

- Document the sets of users who should have access to the application and the credentials associated with each set.
- Create and use a security group to manage users in each set.
- Change the password of the shared account. Once the application is deployed, users don't need the password of the shared account. The password is stored in Entra ID and should be long and complex.
- Consider configuring automatic password rollover.

SSO deployment options

There are several ways to configure SSO for applications, depending on the authentication method they use. Cloud applications typically support OIDC, OAuth, SAML, password-based, or linked SSO. On-premises applications, on the other hand, may rely on password-based, Integrated Windows Authentication, header-based, or linked SSO. To enable SSO for on-premises apps, Microsoft Entra Application Proxy must be configured.

Following is a handy flow chart that helps you choose the correct SSO deployment option:

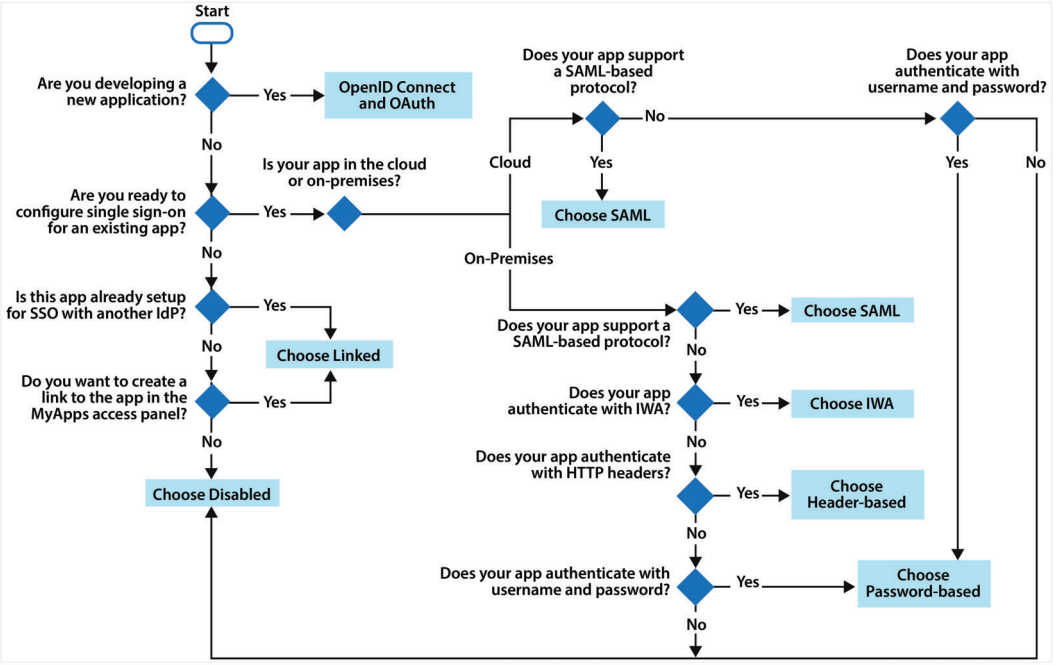


Figure 2.10: Choose the right SSO method

Based on this flowchart, you can determine the most appropriate SSO method for your organization.

Multi-factor authentication

As covered in *Chapter 1, Introduction to Microsoft Entra*, **multi-factor authentication** (**MFA**) is an enhanced security feature that requires the user to present a combination of two or more forms of authentication methods from the following list:

- Something you know, like a PIN or password
- Something you have, like a hardware security token
- Something you are, like a biometric

Administrators can decide the second factor to challenge the user with. There are several verification methods to choose from like Microsoft Authenticator app, Passkeys, hardware, and software tokens, and certificates. Once the administrator enables the second factor authentication, users will be asked to register for it at next logon. On subsequent logons, they will be able to satisfy the MFA conditions to complete login.

Microsoft Entra MFA also provides for secure password reset. When users register for MFA, they can also register for **self-service password reset (SSPR)**.

Microsoft Entra MFA processes and stores personal and organizational information in datacenters in the United States, Europe, and Asia Pacific. Microsoft Entra MFA stores bypassed users, Microsoft Authenticator device token change requests, MFA activity reports, and MFA activation for 90 days. Personal data like usernames, phone numbers, and IP addresses are not stored. Log data is stored for 30 days. Tenant settings like account lockout thresholds, notifications, and phone call settings might also be stored.

Before rolling out MFA, it is important to understand the settings that can affect how often a user will be prompted for MFA. The following sections explain some of these settings.

Configuring prompts and session lifetime

There are several settings that determine how often a user will need to reauthenticate to Microsoft Entra ID. This can involve only the first factor or the second factor as well. The default setting for user sign-in frequency is a rolling 90-day window. Organizations can choose to change this to suit their requirements. The following settings are recommended by Microsoft:

- Organizations with Entra ID P1 or P2 license:
  - Enable SSO across applications
  - Use **Microsoft Entra Conditional Access Sign-in frequency** policy to enable reauthentication
  - Limit sign-in duration for users who sign in from unmanaged devices
- Organizations with Entra ID Free license:
  - Enable SSO across applications
  - Enable the **Stay signed in?** option
- Ensure mobile users have the Microsoft Authenticator app to broker into other Microsoft Entra ID federated apps

Without session lifetime settings, each time a user closes and reopens the browser they are asked to reauthenticate. This is because the browser has no persistent cookie. In Office clients, the default is a 90-day rolling window. If a user is inactive for 90 days, they will be asked for first and second factor authentication. If there are multiple settings defining session lifetime, the most restrictive one applies. For example, if you have both the following settings enabled, the user will need to reauthenticate every 14 days.

- Show option to remain signed in
- Remember MFA for 14 days

To configure the option to remain signed in follow these steps:

1. Sign in to `https://entra.microsoft.com` as a **Global Administrator**.
2. In the left pane, navigate to **Users** | **User settings**.
3. In the right pane, toggle the **Show keep user signed in** to **Yes**.

With this option enabled, users are presented with a **Stay signed in?** prompt at sign in. Refer to *Figure 2.11*. When they select **Yes**, a persistent cookie is set in the browser which remembers both the first and second factors.

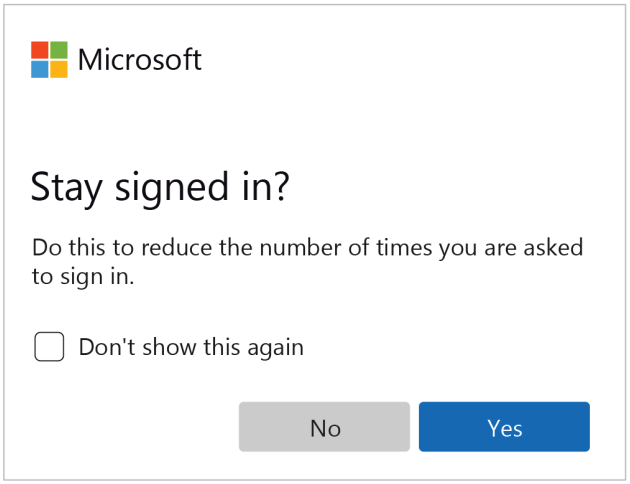


Figure 2.11: Stay signed in box

To configure remember MFA on trusted devices follow these steps:

1. Sign in to `https://entra.microsoft.com` as an **Authentication Policy Administrator**.
2. In the left pane, navigate to **Entra ID | Multifactor authentication**.
3. In the right pane, click on **Additional cloud-based multifactor authentication settings**.
4. On the next page, click on **Service settings** tab.
5. Check the box **Allow users to remember multifactor authentication on devices they trust**.
6. In the **Number of days users can trust devices for** choose number between 1 and 365.
7. Click **Save**.

Once this option is enabled, users are presented with an option to remember MFA as shown in the following figure. When they check the box, a persistent browser cookie is set. This option reduces the number of reauthentication prompts on web applications. However, setting this value to less than 90 days can increase the number of times Office clients request reauthentication. If this setting is used with **Keep me signed in?** or Conditional Access policies, users might experience an increase in the number of authentication requests.

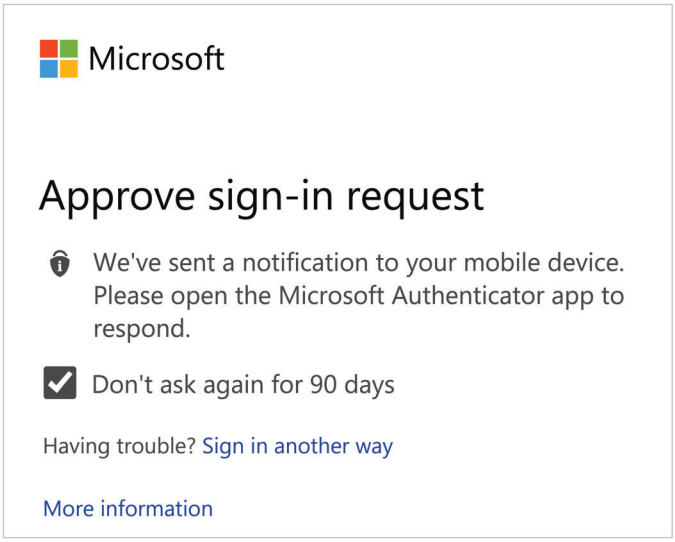


Figure 2.12: Remember MFA prompt

Organizations that have Microsoft Entra P1 and P2 licenses should consider using Conditional Access Sign-in frequency.

Configuring system-preferred MFA

Administrators can use **system-preferred MFA** to prompt users to sign in using the most secure method they are registered for. For example, if users register for both SMS OTP and the Microsoft Authenticator app, they will be prompted to complete MFA using the Authenticator app as it is more secure than a text message. Users can still choose to sign in using SMS OTP, but they are first prompted to try the most secure method.

Use the following steps to manage this setting:

1. Sign in to `https://entra.microsoft.com` as an **Authentication Policy Administrator**.
2. In the left pane, navigate to **Entra ID** | **Authentication methods**. In the right pane click on **Settings**.
3. The default **State** under **System-preferred authentication** is **Microsoft managed**. This means that Microsoft decides the appropriate time to turn this feature on. You can choose to include or exclude groups.
4. You can change the **State** to **Enabled** or **Disabled** by selecting the appropriate option from the drop-down box. Include or exclude groups as appropriate. Refer to *Figure 2.13*:

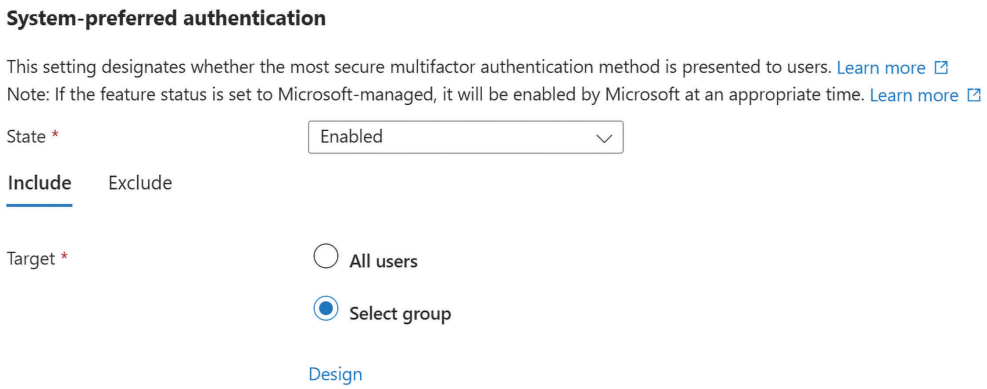


Figure 2.13: System-preferred authentication

5. Click **Save**.

Configuring external MFA provider

Microsoft Entra ID offers the ability to add an external authentication provider as an MFA method. This feature is called **External Multifactor Authentication (external MFA)** and requires at least a Microsoft Entra ID P1 license. External MFA methods are added to the Microsoft Entra ID tenant by the administrator. When external MFA is used, the first-factor authentication is completed by Microsoft Entra ID and the second factor is completed by the external MFA.

External MFA is implemented on top of OIDC and requires an OIDC discovery endpoint, a valid OIDC authentication endpoint and a URL where the public certificates of the EAM provider are published.

The following figure details how sign-in using external MFA works:

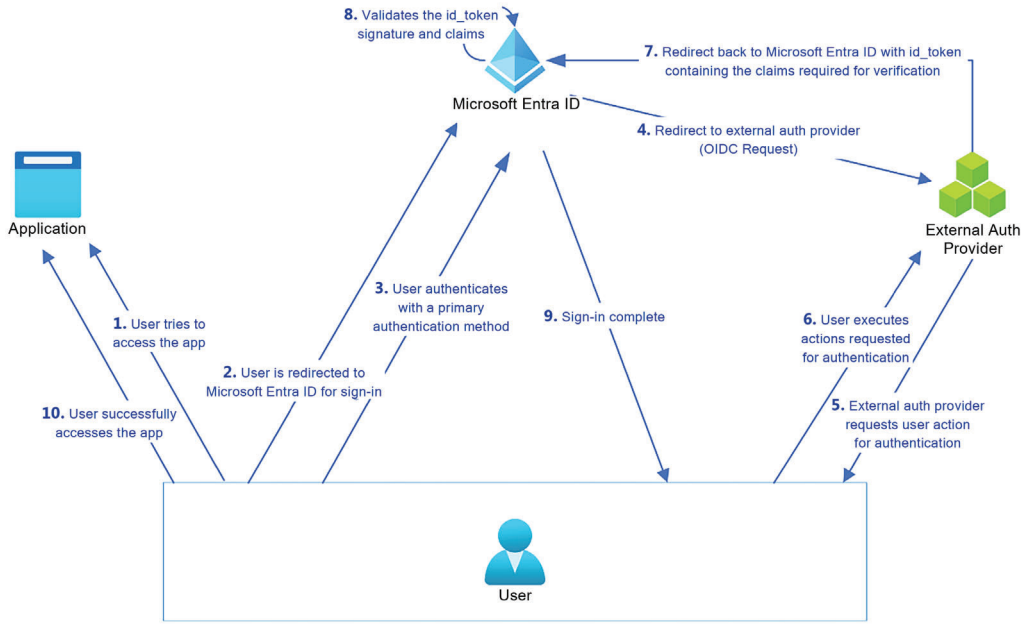


Figure 2.14: External MFA sign-in process

Configuring MFA rollout

To effectively roll out MFA to end users, you can use the **MFA registration policy**, which will force users to register for MFA regardless of the app they are signing into. The following are the steps to configure an MFA registration policy:

1. Log in to `https://entra.microsoft.com` as a **Security Administrator**
2. Navigate to **ID Protection | Dashboard | Multifactor authentication registration policy**
3. In the right-pane, click on **Users** to include users and groups in the policy as follows:

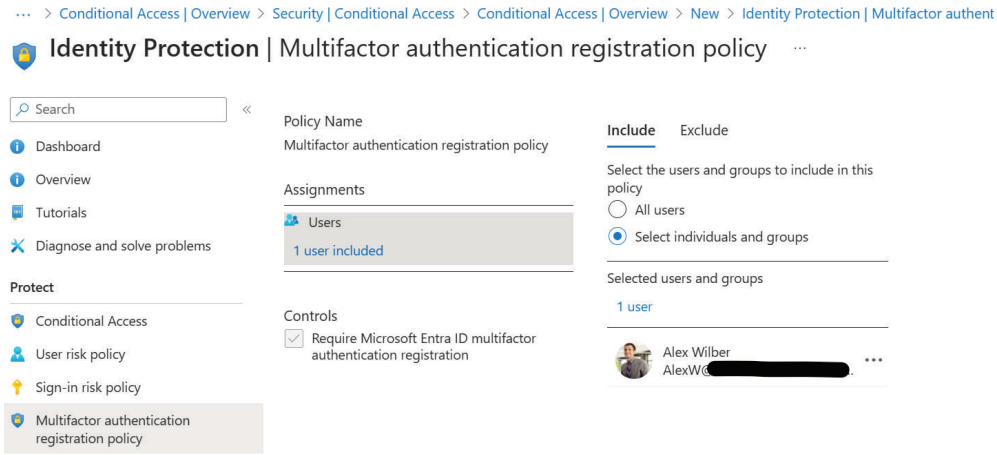


Figure 2.15: Selecting users for MFA registration

4. Ensure that the **Policy enforcement** toggle is set to **Enabled** and click on **Save** as follows:



Figure 2.16: Policy enforcement toggle

Microsoft Entra ID will now prompt users to register for MFA the next time they sign in interactively. The users can skip the registration process for 14 days after which they will not be allowed to sign in unless they register.

You can also use Conditional Access policies to roll out MFA. However, the MFA registration policy is the most efficient way to roll out MFA as it is not dependent on the user trying to access a specific application. Once you have turned on the MFA registration policy, you can use additional Conditional Access policies to prompt users to complete an MFA challenge based on certain conditions.

Now let us discuss the different authentication methods available for users in Microsoft Entra ID.

Authentication methods

Microsoft Entra ID offers several authentication methods, ranging from simple passwords to MFA methods like SMS and tokens, and even passwordless solutions like Windows Hello for Business and passkeys. Microsoft recommends passwordless authentication as the most secure method of authentication and the best user sign-in experience. The following figure shows the various authentication methods available in Microsoft Entra ID:

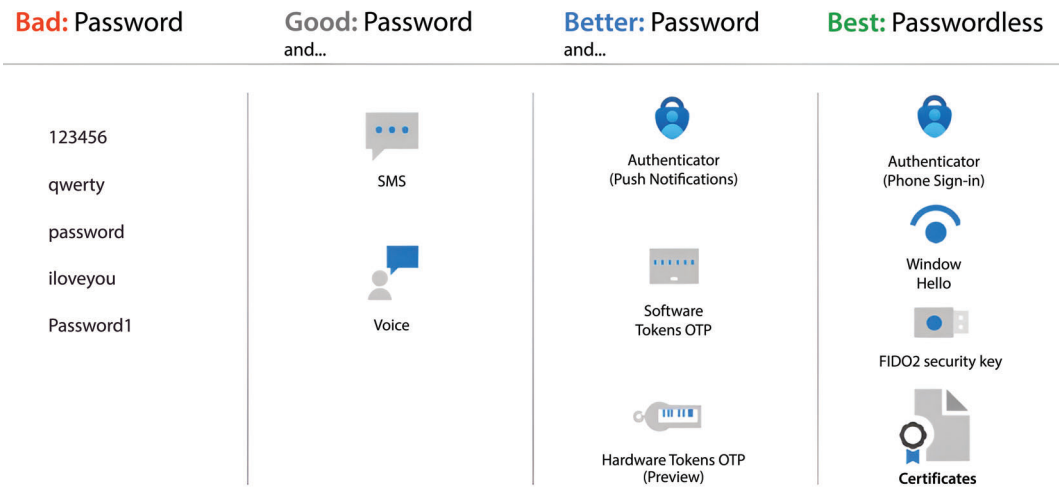


Figure 2.17: Microsoft Entra ID authentication methods

Some of these authentication methods can be used for both MFA and SSPR. Users can register for both MFA and SSPR in a single step. It is recommended that users register for more than one method so if one is not available, they can use the other one. Some of these methods like FIDO security keys can be used as the primary method. Others are only available as a secondary method.

These authentication methods can be managed using the **Authentication methods policy** in the Microsoft Entra admin center. The **Authentication Policy Administrator** role is required to manage this policy. Once an authentication method is enabled in the policy, it can be used both for MFA and SSPR. The **Authentication strengths** feature in Conditional Access provides more control over which method can be used in which scenario.

Let's now discuss each of these authentication methods in detail.

Temporary Access Pass

When a new employee joins the organization, the IT admin creates a user account for them and assigns a temporary password. Usually, this password is the same for all new user accounts

and it is shared with the new employee using insecure channels like personal email accounts. This poses obvious security concerns. Instead of issuing a standard password, administrators can use a **Temporary Access Pass (TAP)**, which is a time-limited code. The TAP can be configured for use once or multiple times. TAP brings users one step closer to being passwordless by enabling simple onboarding to passwordless methods like passkeys and Microsoft Authenticator app sign in. It also simplifies account recovery.

The following steps explain creating and using TAP:

1. Sign in to `https://entra.microsoft.com` as an **Authentication Policy Administrator**.
2. In the left pane, navigate to **Entra ID | Authentication methods | Policies**.
3. Click on **Temporary Access Pass**.
4. Switch the **Enable** toggle to on. You can either choose to turn it on for all users or select specific groups, as shown in the following figure:

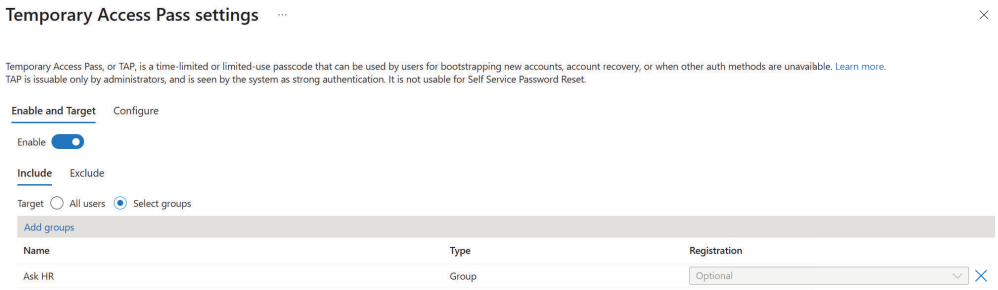


Figure 2.18: Enable TAP

5. Click **Configure** to configure additional settings. The following screenshot shows the settings available:

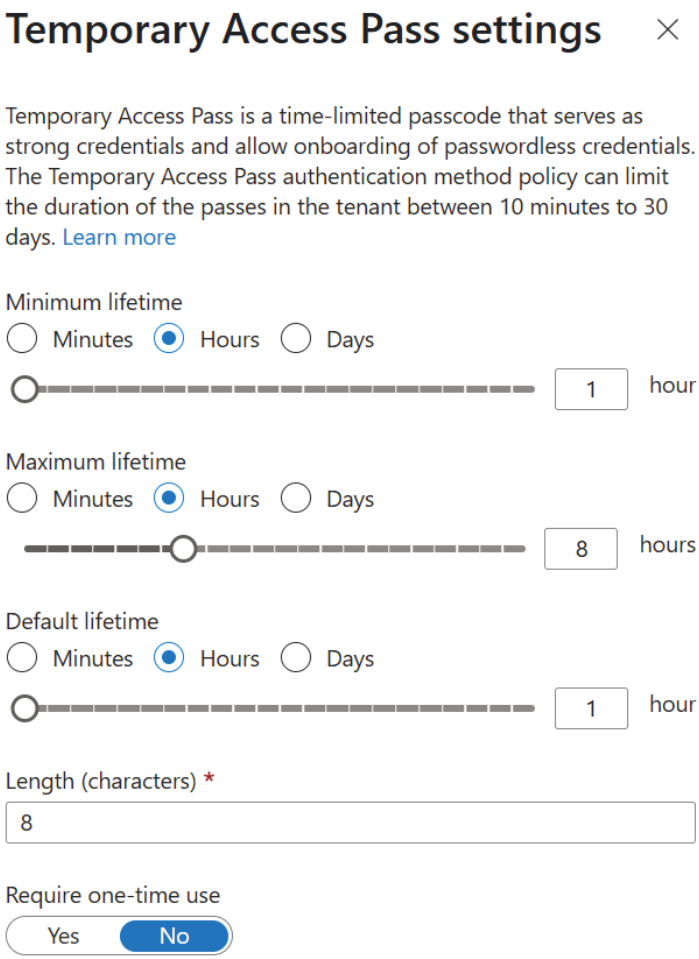


Figure 2.19: TAP settings

6. Once done save your settings.

7.

The following Entra ID roles can perform actions on a TAP:

- **Privileged Authentication Administrators**: They can create, delete, and view a TAP for everyone except themselves.
- **Authentication Administrators**: They can create, delete, and view a TAP for members except themselves.
- **Authentication Policy Administrators**: They can enable and manage the TAP authentication methods policy.
- **Global Readers**: They can view the TAP details for users. However, they cannot read the code itself.

Now you can create a TAP for users using the following steps:

1. Sign in to `https://entra.microsoft.com` and navigate to **Users | All users**.
2. Select the user for whom you want to create the TAP.
3. On the user page, click on **Authentication methods | Add authentication method**.
4. In the pop-up pane, select **Temporary Access Pass**. Define the **Activation duration**. Select **Yes** if the TAP is only to be used once. Click **Add**. Refer to the following figure:

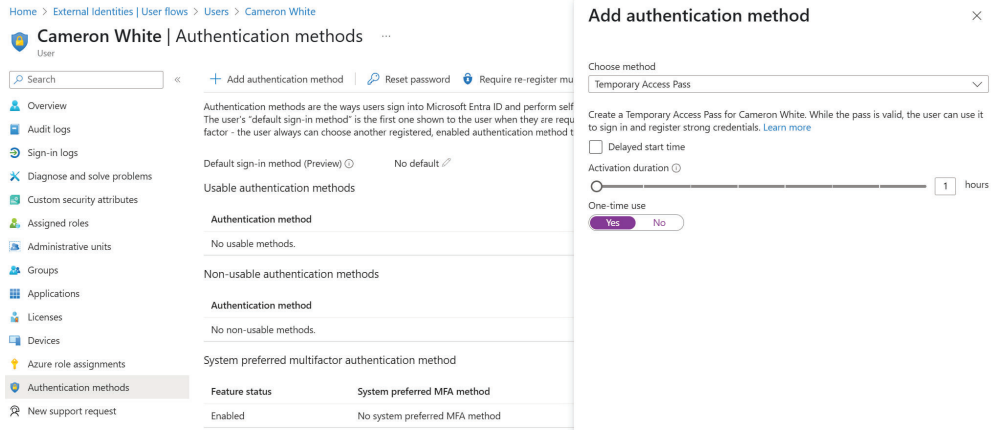


Figure 2.20: Adding TAP

5. The TAP details are shown. Provide the TAP to the user. It is important to save the TAP at this time as once you click **Ok** it won't be visible. Refer to *Figure 2.21*.

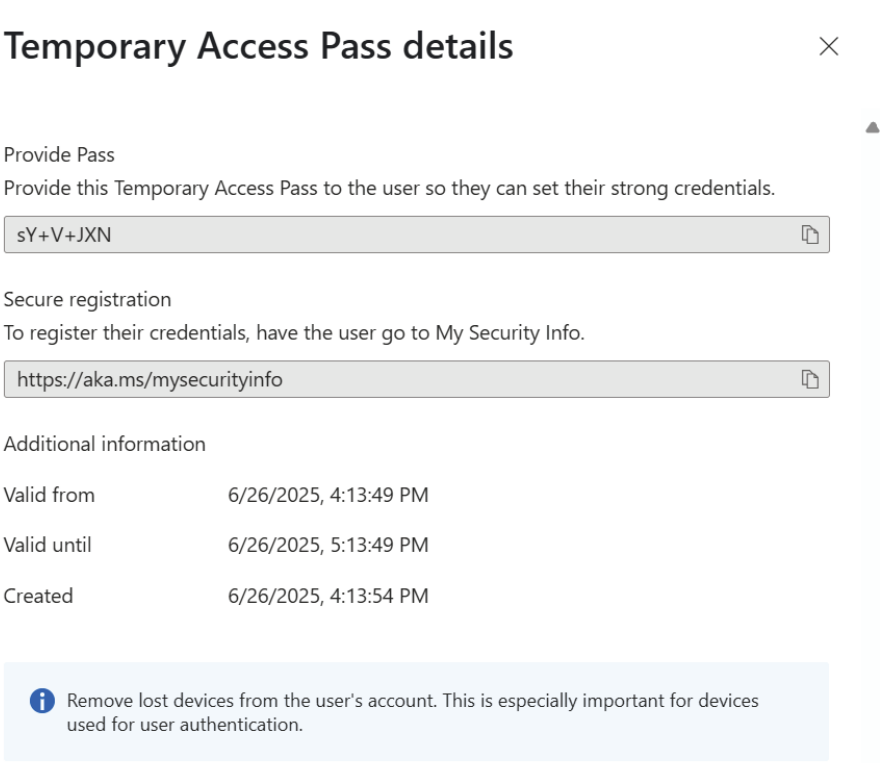


Figure 2.21: TAP details

Once a user receives this TAP, they can then use it to create stronger authentication methods for themselves like passwords, Authenticator App, and Passkeys.

Now let's discuss the various passwordless methods available with Microsoft Entra ID.

Passwordless authentication

MFA helps secure the organization, but it also causes users to get frustrated if they must answer frequent MFA prompts. Passwordless methods completely eliminate the need for passwords, offer a more user-friendly experience by removing the need to remember and change passwords, and satisfy MFA requirements. Microsoft Entra ID offers several passwordless sign-in methods. Let's explore them.

Windows Hello for Business

Windows Hello for Business is a passwordless authentication method using which users can sign into Windows devices using biometrics such as facial recognition or fingerprint or a PIN, instead of a password. It is a phishing-resistant, two-factor authentication that has brute-force

protection built in. When used with FIDO/WebAuthN, Windows Hello for Business can also be used to sign into various websites, thus eliminating the need to remember multiple passwords.

Windows Hello for Business offers the following benefits:

- It protects against credential theft. An attacker must have both the device and the PIN to gain access.
- Since no passwords are used, it circumvents phishing and brute force attacks. It also prevents server breaches and replay attacks, as credentials are asymmetric and generated within the **Trusted Platform Module (TPM)**.
- The PIN can only be used with the device it was configured with. So even if an attacker knows the PIN, they will still need the device to access the data. Moreover, Windows Hello for Business has brute-force protection built in.

Windows Hello for Business uses a two-factor authentication that combines device-specific credentials with a biometric. The credential is tied to Microsoft Entra ID. During provisioning, Windows Hello is set up on the device and the user is asked to provide a gesture that will be used to verify their identity and unlock the device. The biometric data is stored on the Windows device making it impossible to steal as it never leaves the device.

Windows Hello for Business supports facial recognition, fingerprint scanning, and iris recognition. Major hardware vendors are now shipping hardware devices that are compatible with Windows Hello for Business.

The following steps describe how the sign-in process works:

1. When a user signs into their Windows device using biometric or PIN, it unlocks their Windows Hello for Business private key. This key is then securely transmitted to the **Cloud Authentication Provider (CloudAP)**.
2. The CloudAP requests a **nonce** from Microsoft Entra ID. A nonce is a random number that can be used once and is valid for 5 minutes.
3. Once it receives the nonce from Microsoft Entra ID, the CloudAP signs it with the user's private key and sends it back to Microsoft Entra ID.
4. Microsoft Entra ID uses the user's public key to validate the nonce. It then creates a **Primary Refresh Token (PRT)** using the session key, which is encrypted with the device's transport key and sends it back to CloudAP.
5. CloudAP leverages the device's private transport key to securely receive the session key, which is then protected by the device's **Trusted Platform Module (TPM)**.
6. The CloudAP informs Windows that the authentication was successful. The user can now log in to Windows and get SSO access to cloud and on-premises applications.

Windows Hello for Business provides secure, passwordless authentication using device-specific credentials and biometrics, enabling users to access Windows devices and cloud resources with enhanced protection against phishing and brute-force attacks.

Platform Credential for macOS

Platform Credential for macOS leverages Microsoft Enterprise Single Sign-On Extension (SSOe) to provide enhanced security. It establishes a secure enclave supported by a hardware-bound cryptographic key, which facilitates single sign-on for applications that authenticate using Microsoft Entra ID. Users still need to sign in to macOS using the local account and password. Using this method, users can go passwordless. Users may utilize Touch ID to unlock their device, and employ phishing-resistant credentials that are compliant with Windows Hello for Business. This helps customers eliminate security keys and implement zero trust. Platform Credential for macOS may serve as a phishing-resistant solution for WebAuthn challenges, including scenarios such as browser re-authentication. This uses the **Passkey (FIDO2)** authentication method.

Platform SSO on macOS with SmartCard

This method allows users to go passwordless on Mac devices by using external smart cards or smart-card compatible hardware tokens like YubiKey. After the device is unlocked, the smart card utilizes Microsoft Entra ID to provide SSO capabilities across applications. This method uses **certificate-based authentication (CBA)**. Platform SSO can be configured using Microsoft Intune or any other **Mobile Device Management (MDM)** solution.

Microsoft Authenticator

Many organizations already use the Microsoft Authenticator app as an MFA method. It is also a convenient method to help organizations implement passwordless. Using this, users can sign in to any platform or application by approving a notification on their phone or matching a number displayed on the screen. Biometrics like face or fingerprint or a PIN can be used to validate the user's identity. Passwordless authentication with Microsoft Authenticator follows a similar process to Windows Hello for Business. The primary distinction is that user identification is required so Entra ID can locate the appropriate Authenticator app and determine its version. The following steps describe the authentication flow:

1. On the computer, the user enters their username on the application they want to access.
2. Microsoft Entra ID detects that the user is registered for passwordless. Depending on the device, it sends a notification to the app via **Apple Push Notification Service (APNS)** or **Firebase Cloud Messaging (FCM)**.
3. The user receives the push notification and opens the app, which then calls Microsoft Entra ID to obtain a proof-of-presence challenge and nonce.

4. The user completes the challenge by providing a biometric input or by entering their PIN which unlocks their private key.
5. This action signs the nonce using the private key and sends it to Microsoft Entra ID.
6. The key is validated by Microsoft Entra ID and the token is returned.

Before users can use the Microsoft Authenticator app as a passwordless method, administrators must enable it in authentication methods. The following steps explain how:

1. Sign in to `https://entra.microsoft.com` as an **Authentication Policy Administrator**
2. In the left pane, navigate to **Entra ID | Authentication methods | Policies**
3. Click on **Microsoft Authenticator** and turn it on. You can choose to enable it for all users or selected groups.
4. Under the **Authentication mode**, select **Passwordless** as shown in the following image:

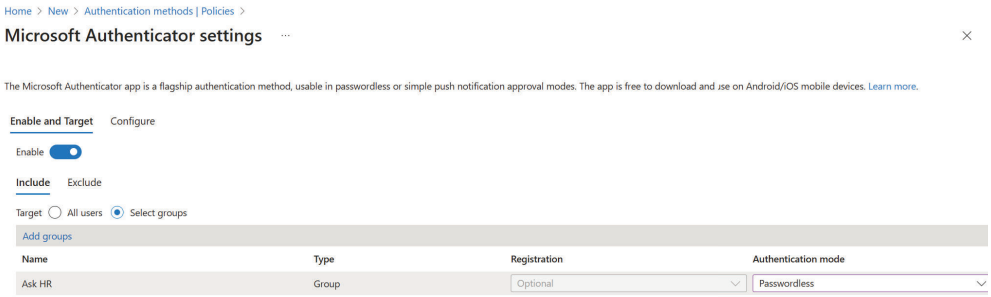


Figure 2.22: Microsoft authenticator app configured for passwordless sign-in

If users are already using the Microsoft Authenticator app for multifactor authentication, the following are the steps to enable passwordless sign-in:

1. On your Android or iOS device, open the Microsoft Authenticator app.
2. Select the account for which you would like to enable phone sign-in and tap on **Enable phone sign-in**. Follow the on-screen instructions to complete the configuration for passwordless sign-in.

First-time users can register for passwordless authentication from within the Microsoft Authenticator app without first needing to register the authenticator app. They will need to download the Microsoft Authenticator app on their smartphones and obtain a TAP from the administrator. The following are the steps on their iOS or Android device:

1. On the device, open the Microsoft Authenticator app and tap on **Add account** and choose **Work or School account**.

2. Click on **Sign-in**. Enter the Microsoft Entra ID username.
3. Users will be prompted to provide the TAP. Follow the on-screen instructions to complete the registration.
4. Once complete, follow the above steps to enable phone sign-in for the account.

The Microsoft Authenticator app serves both as a passwordless authentication method and as a second factor authentication method when Push mode is enabled. This is described in the *Microsoft Authenticator in Push mode* section.

Passkey (FIDO2) authentication

Passkeys, developed by the **FIDO (Fast Identity Online)** Alliance, offer an innovative approach to secure authentication. They eliminate the need for traditional passwords by leveraging FIDO2 standards. These keys depend on public key cryptography to authenticate identities, offering a higher level of security by minimizing vulnerabilities such as phishing, password-related breaches, and weak passwords. By replacing passwords with cryptographic credentials, passkeys simplify the sign-in process while enhancing protection against cyber threats.

Passkeys are supported on modern systems like Windows 10 (version 1903 or higher) and are integrated into tools like the Microsoft Authenticator, empowering organizations to adopt robust, password-free security solutions.

As per the FIDO2 specification, each security key vendor must provide an **Authenticator Attestation GUID (AAGUID)**. The **AAGUID** is a 128-bit identifier that specifies the key type. Passkey providers on desktops and mobiles are also expected to provide an AAGUID during registration. Before enabling passkeys, ensure that the following requirements have been met:

- Microsoft Entra multifactor authentication should be enabled in the organization.
- Users should have the Microsoft Authenticator app installed on their devices.
- User devices should support passkey authentication. The following devices are supported:
    - Entra ID joined devices should be running Windows 10 version 1903 or higher.
    - Hybrid joined devices should be running Windows 10 version 2004 or higher.

Now let's learn how to enable and use passkeys.

Enabling passkeys

The following are the steps to enable passkey as an authentication method:

1. Log in to `https://entra.microsoft.com` with an account that has the **Authentication Policy Administrator** role assigned.
2. Navigate to **Entra ID** | **Authentication methods** | **Policies**.

3. Click on **Passkey (FIDO2)** and click on **Enable**. Select the groups to include or exclude from policy.
4. Click on **Configure** and make the settings as shown in the following figure:

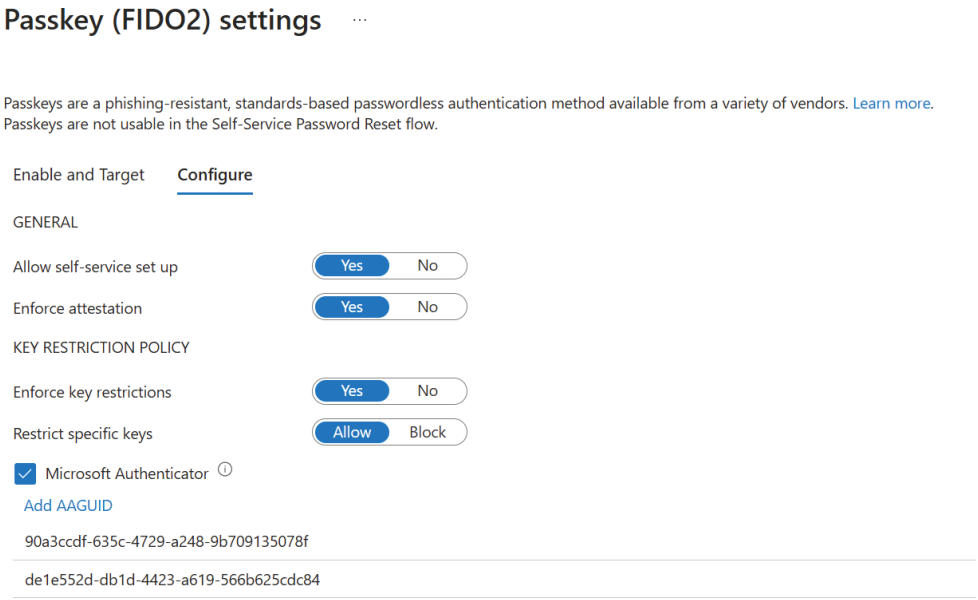


Figure 2.23: Passkey configuration

   - Set **Allow self-service set up** to **Yes** to enable users to register for a passkey using their **Security info** page.
   - Set **Enforce attestation** to **Yes** to ensure that the FIDO2 security keys are from a genuine and legitimate vendor.
   - Set **Enforce key restrictions** to **Yes** to specify allowed or blocked key models or passkey providers by their AAGUID. If enabled, you can add Microsoft Authenticator AAGUIDs automatically to the restriction list.
5. Once done, click **Save**.
6. You can now create a Conditional Access policy to require users to register and use passkeys.

Once an administrator enables the use of passkeys for the organization, users must register to use passkeys. This is explained in the next section.

Registering a passkey

Users can manually register for a passkey using the following steps:

1. As an end user, go to `https://mysignins.microsoft.com`.
2. In the left pane, click on **Security info**.
3. In the right pane, click on **Add sign-in method** and then click on **Passkey**.
4. Before adding a passkey, you will have to complete MFA. If you don't have an MFA method registered, you will have to do so before being able to add a passkey.
5. A dialog box will open asking where you would like to store your passkey as shown in the following figure:

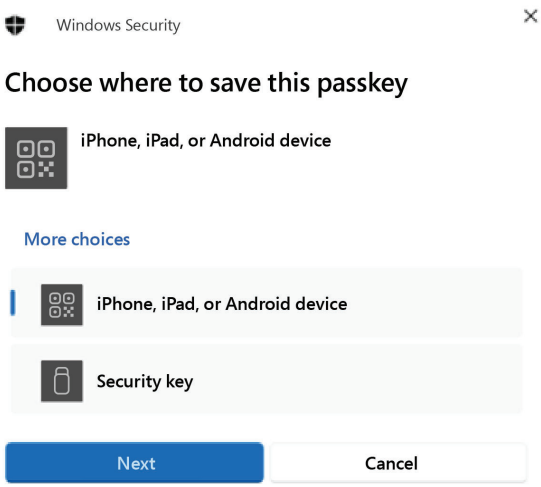


Figure 2.24: Save passkey

6. Choose **iPhone, iPad, or Android device** and follow the guidance on the screen to save your passkey to your Microsoft Authenticator app.

With passkeys enabled and registered, users are now ready to go passwordless and start using passkeys.

Signing in with a passkey

Once a user has stored a passkey on their authenticator app, they can use it to sign in without a password using the following steps:

1. Go to `https://portal.office.com` and enter your username and click on **Next**.
2. Click on **Sign-in options** and select **Face, fingerprint, PIN or security key**. Click **Next**.

3. Choose **iPhone, iPad, or Android device** and click **Next**.
4. A QR code will be displayed. Scan the QR code using your device camera. Tap **Sign-in with a passkey** on your device. The device will connect to your computer using Bluetooth.
5. Click **Continue** on your device to sign in using the passkey.

Passkeys allow users to sign in securely without a password by authenticating through their device using facial recognition, fingerprint, PIN, or a security key.

Certificate-based authentication

This method allows users to authenticate using an X.509 certificate against applications that use Microsoft Entra ID browser sign-in. Using this method, customers can enable phishing-resistant authentication using their PKI. It is secure, easy to deploy and administer, and provides a great user experience. During sign-in, users are asked to authenticate using a certificate instead of entering a username and password. If multiple certificates are found, the user is asked to select one. Once the certificate is validated, the user can sign in. The following image shows how **certificate-based authentication (CBA)** in Microsoft Entra works:

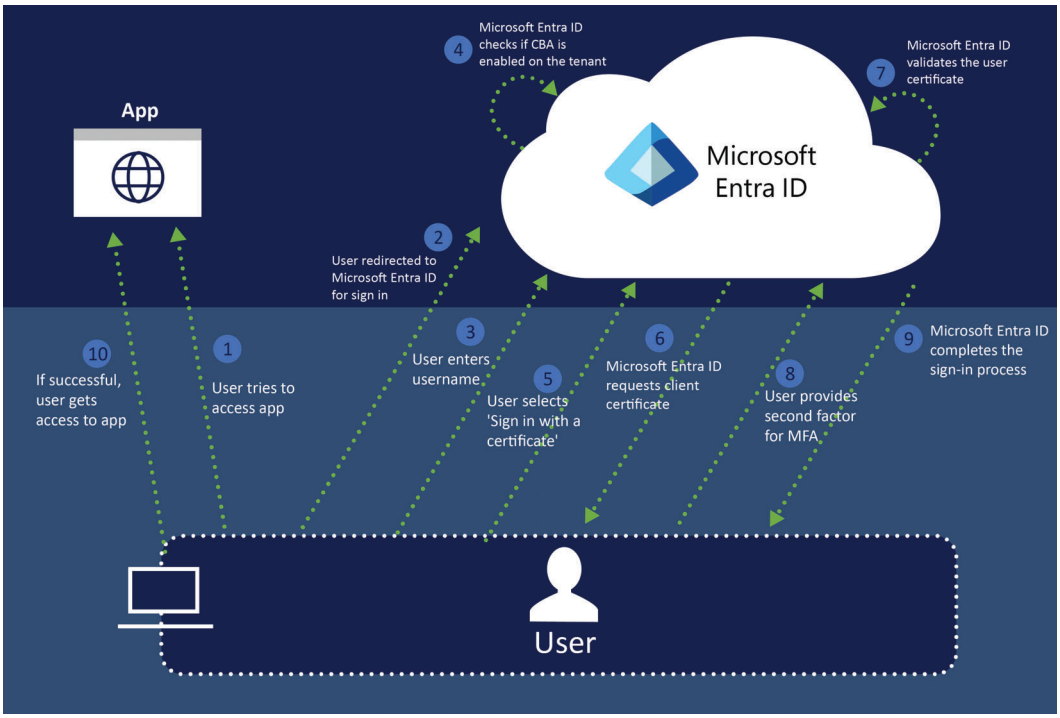


Figure 2.25: CBA in Microsoft Entra

The following prerequisites should be met for CBA to work:

- At least one **Certificate Authority (CA)** should be configured in Microsoft Entra ID.
- Users should have access to a user certificate from a trusted **Public Key Infrastructure (PKI)**.
- Each CA should have a **Certificate Revocation List (CRL)** that must be accessible from the internet.

Certificate-based authentication allows users to securely sign in to applications by validating a user certificate instead of a password, providing phishing-resistant access and a seamless user experience.

Microsoft Authenticator in Push mode

The Microsoft Authenticator app can be used as an MFA option to approve or deny sign-in requests when in **Push** mode. Users can view the prompt on their authenticator app and click on **Approve** if it is a legitimate request; otherwise, click on **Deny**. The device should have internet connectivity to be able to receive Push notifications.

It can also be used as a software token to generate OATH verification codes. The users can then enter the verification code at the sign-in stage.

Figure 2.26 shows an example of the Microsoft Authenticator app generating OATH verification codes:

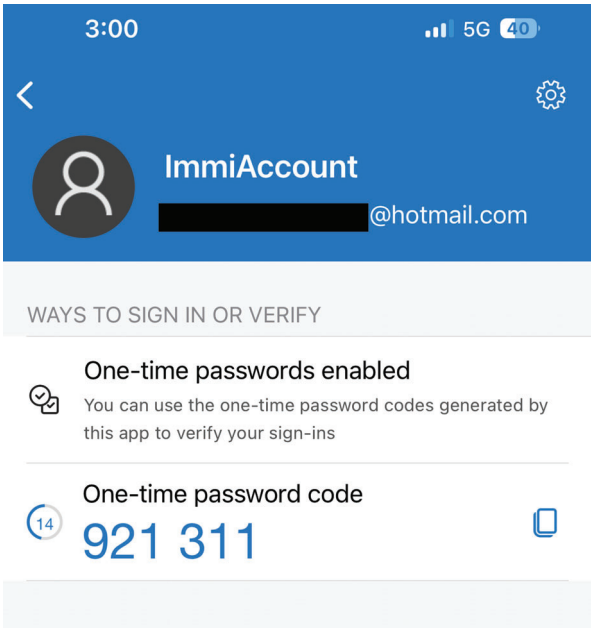


Figure 2.26: OATH codes in Microsoft Authenticator app

Note

OATH codes are not supported for certificate-based authentication. Users can have a maximum of five OATH tokens or authenticator applications configured for use at any time.

Before users can use the Microsoft Authenticator app as an MFA method, an administrator must enable it in authentication methods. Ensure that the **Push** mode is selected as shown in the following figure:

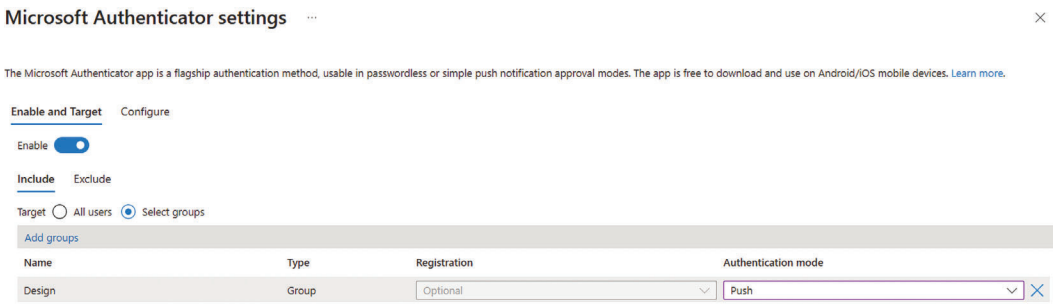


Figure 2.27: Enable Microsoft Authenticator app in Push mode

To register the Microsoft Authenticator app as an MFA method, users use the **Security info** page. The following are the steps:

1. Log in to `https://aka.ms/mysecurityinfo` with your Entra ID credentials.
2. Make sure you are on the **Security info** page.
3. Click on **Add sign-in method**. In the drop down, select **Authenticator app** and click on **Add** as follows:

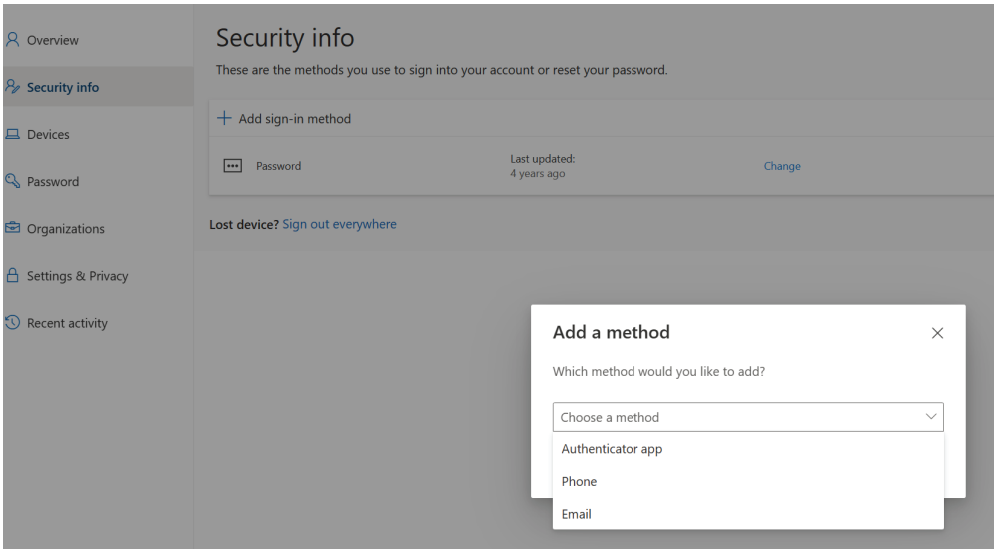


Figure 2.28: User registering to use the Microsoft Authenticator app

4. You will be prompted to install the app. Install the app from your iOS or Android store and click **Next**.

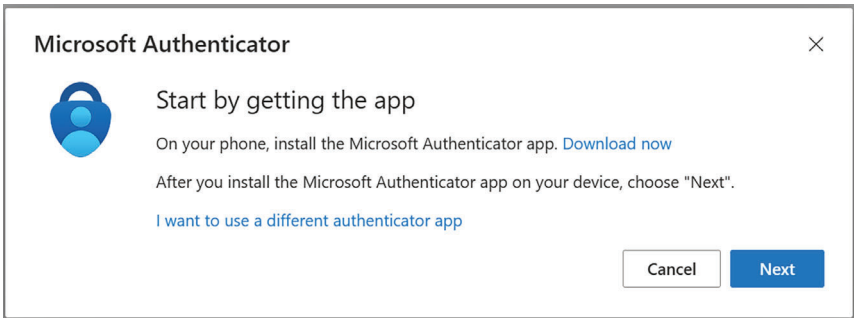


Figure 2.29: Install the Authenticator app

5. On the **Set up your account** screen, click **Next** as shown in the following figure:

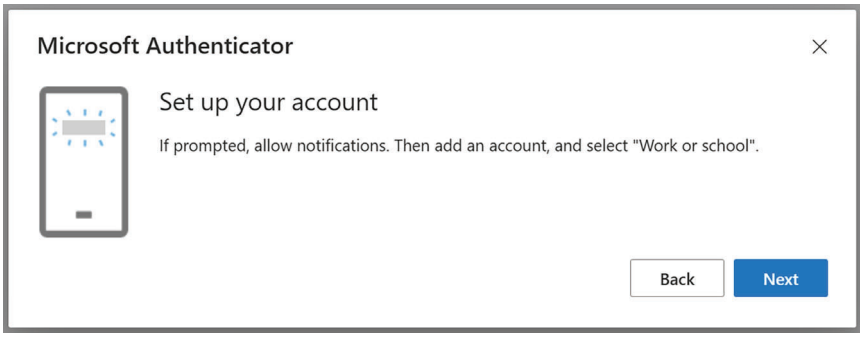


Figure 2.30: Set up your account

6. Next, you will be prompted to scan the QR code to use the app. This will connect the app with your account. On your smart phone, open the Authenticator app and click on the **+** sign on the top right. Select **Work or school account** and select **Scan QR code**. This will open the camera, using which you can scan the QR Code displayed on the screen. This will add the account to your Authenticator app. On the screen below, click **Next** as shown in the following figure:

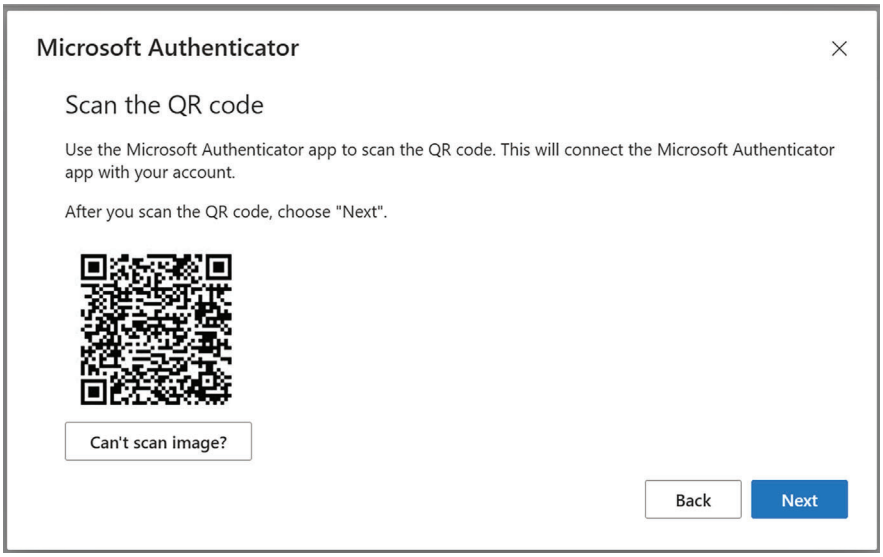


Figure 2.31: Scan QR Code

7. You might be prompted to confirm by entering a code on a prompt in the app. Enter the code to confirm. The following figure shows the **Security info** page displaying a code that the user must input into the Microsoft Authenticator app on their mobile phone to complete the process:

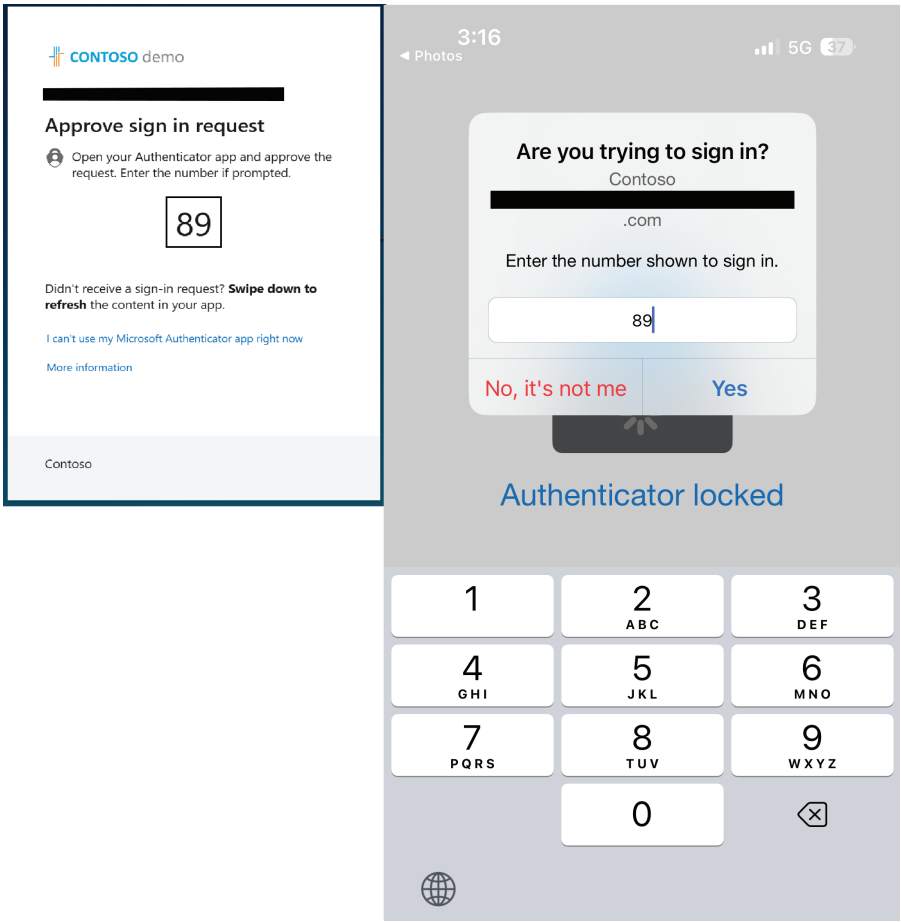


Figure 2.32: Validate authenticator

8. You will be prompted with a screen saying **Notification approved**. Click **Next**. Microsoft Authenticator will now be displayed on the **Security info** page as an authentication method, as shown in the following figure:

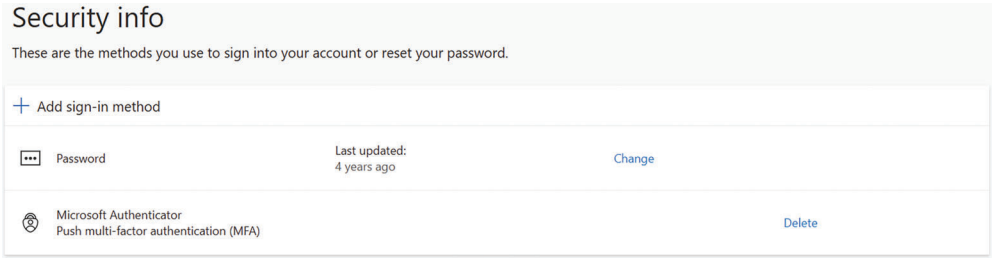


Figure 2.33: Authentication methods listed on MySecurityInfo page

When the Microsoft Authenticator app is used in Push mode, it can be used to approve or deny MFA requests and as an OATH software token. Microsoft Entra ID supports other OATH software tokens as well.

OATH software token

OATH software tokens are applications, such as the Microsoft Authenticator app, that generate a secret key or seed that is entered into the app and used to generate OTP. When the Microsoft Authenticator app is set up to receive push notifications, it also automatically generates **time-based one-time passcodes** (**TOTP**) as a backup, so that a user can sign in even without internet connectivity. To enable users to use an OATH software token as an MFA authentication method, an administrator will need to enable it in the Microsoft Entra ID portal.

OATH hardware token

OATH hardware tokens are small devices that display a 6-digit number that refreshes every 30 or 60 seconds. With Microsoft Entra ID you can use OATH-TOTP SHA-1 tokens. There are several vendors that sell these types of hardware tokens. One such hardware token is shown in the following figure:



Figure 2.34: OATH hardware token

OATH hardware tokens usually come with a secret key or seed pre-programmed into the token. These keys must be entered into Microsoft Entra ID. Secret keys are limited to 128 characters, and can only contain *a-z* characters in upper or lower case and digits *2-7*. They must be encoded in *Base32*.

To enable users to use OATH hardware tokens, administrators will need to configure them in the Microsoft Entra ID tenant.

The following are the steps:

1. Acquire the hardware tokens from a supported vendor.
2. Log in to `https://entra.microsoft.com` as an **Authentication Policy Administrator**.
3. Navigate to **Entra ID** | **Authentication methods** | **Policies**.
4. In the right pane, click on **Hardware OATH tokens**. In the next screen, switch the toggle next to **Enable** to on. You can choose to enable this for all users in the tenant or selected groups. Once done, click on **Save**.
5. Now the tokens must be uploaded into the portal. To do this, the details of the hardware tokens will have to be entered in a `.csv` file. You can download the format of the `.csv` file by going to **Protection** | **Multifactor authentication** | **OATH tokens**. In the right pane, click on **Download**. Complete the `.csv` file with the details of the hardware tokens and upload it by clicking on the **Upload** button as shown in the following figure:

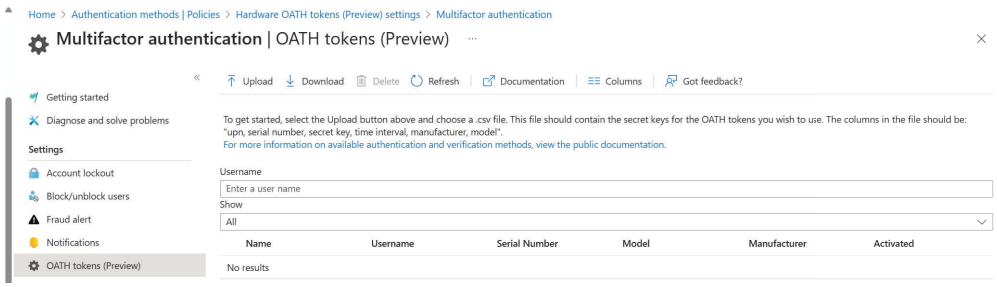


Figure 2.35: Upload OATH hardware tokens

The `.csv` file can take a few minutes to process, depending on its size. You can check the status by clicking on the **Refresh** button. If there are errors, download the file, fix the errors, and upload again. Once all errors are fixed, the tokens will be available in the Entra ID portal. You can then activate each token by clicking on **Activate** next to each token and entering the OTP displayed on the token. A maximum of 200 OATH tokens can be activated every five minutes.

Users can manage and add OATH tokens by registering them on the **Security info** page by going to `https://aka.ms/mysecurityinfo`. Once registered, when the user is prompted for MFA during sign-in, they can check the digits displayed on the hardware token and enter the same digits in the MFA prompt on their screen. If the number matches, the user is allowed access.

OATH tokens are very useful in highly regulated industries like banking or defense, where users may not be allowed to carry their mobile phones, thus being unable to use the Microsoft Authenticator app.

> **Note**
>
> At the time of this writing, OATH Hardware tokens were in public preview.

QR code

This method is useful for frontline workers that use shared devices. Users can use a unique QR code and a PIN for secure sign-in. The QR code is unique for each user, and it can be downloaded from Microsoft Entra admin center and printed on the user's badge for ease of use. QR code is a single-factor authentication method. The following steps enable users to use QR code authentication:

1. Log in to `https://entra.microsoft.com` with an account that has the **Authentication Policy Administrator** role assigned.
2. Navigate to **Entra ID** | **Authentication methods** | **Policies**.
3. In the right pane, click on QR code and click on **Enable**. Select the groups to include or exclude from the policy.
4. Click **Configure** and select the PIN length (8-20 digits) and QR code validity (1-395 days) as shown in the following figure:

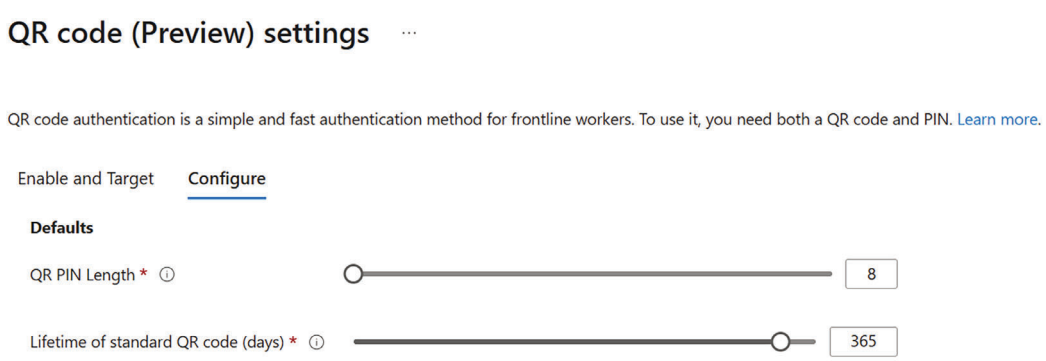


Figure 2.36: QR code settings

5. Click **Save**.

Now, follow these steps to generate a QR code and PIN for a user:

1. Navigate to **Users | All users**.
2. In the right pane, click on the user you want to generate the QR code for. Click on **Authentication methods | Add authentication method**.
3. In the fly out pane, select **QR code** from the drop-down menu. You can choose to activate the QR code right away or later. Enter a PIN or click on **Generate PIN** to generate a PIN. This PIN will be given to the user, which they can change at first logon. Click **Add**.

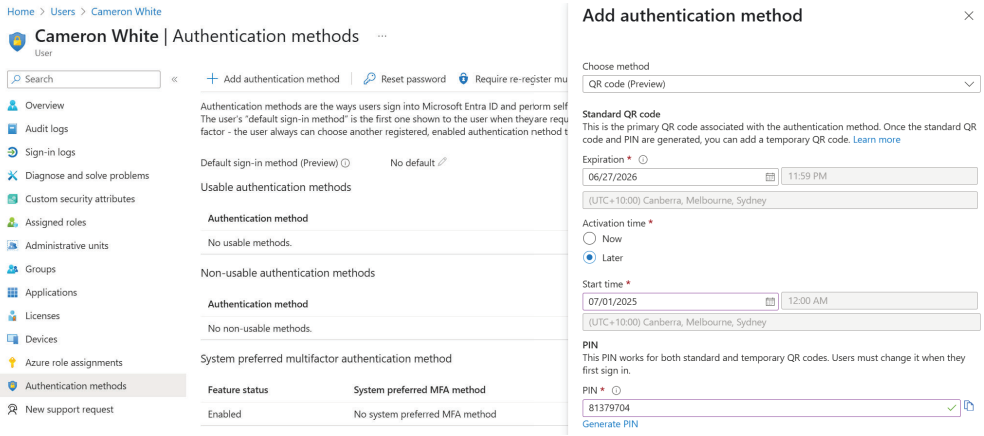


Figure 2.37: Add QR code

4. A QR code will be displayed. Click **Download image** and share it with the user. Note that this code is available for download only once.

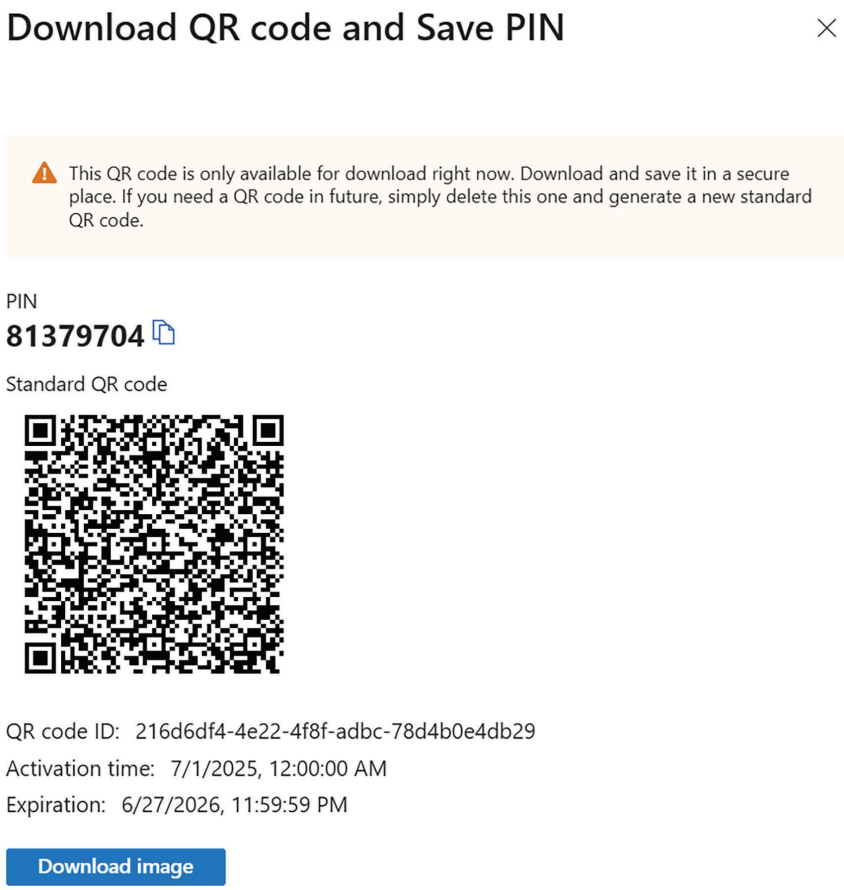


Figure 2.38: Download QR code

Now the users can use this QR code to sign in using the web sign-in experience or an optimized app sign-in experience.

Note

At the time of this writing QR code is in Public Preview.

Conditional Access

Conditional Access is the main policy engine in Microsoft Entra ID. As the security perimeter now extends beyond the traditional boundaries, organizations need to use new identity-driven measures to secure corporate resources. Conditional Access is Microsoft's Zero Trust policy engine. It takes signals from various sources and then enforces policy decisions. In simplest

terms, Conditional Access policies can be defined as *if-then* statements. For example, if a user wants to access their email, they must complete an MFA challenge. Using Conditional Access administrators can help users be productive anywhere and anytime, while protecting the organization's resources. Conditional Access policies are enforced after the user has been authenticated.

The minimum license required to use Conditional Access is **Microsoft Entra ID P1**.

Conditional Access receives signals from a variety of sources before enforcing decisions as shown in the following figure:

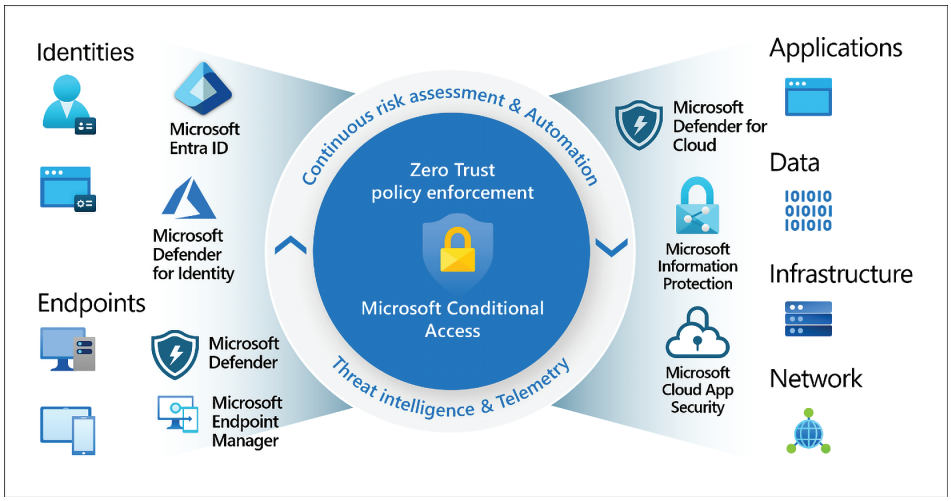


Figure 2.39: Conditional Access overview

Using Conditional Access policies, an administrator can define conditions under which a user is granted or denied access to corporate resources based on their sign-in conditions. For example, if a user is accessing a corporate resource from a company-managed laptop on a trusted network location, they can be allowed access to the corporate resource. If they are accessing a corporate resource from a company-managed laptop but from an untrusted network location, they may be prompted for MFA before access is granted. However, if they are accessing corporate resources from an airport kiosk, they can be completely denied access to the corporate resources.

Using Conditional Access policies, you can define granular control over access to corporate resources based on user and sign-in signals.

Following are the common signals that Conditional Access policy decisions are based on:

- **User or group**: Policies can be applied to individual users or based on group membership.

- **User location**: Policies can be applied based on the user's network location. Organizations can define a list of trusted locations like their corporate or VPN IP address ranges to be excluded from policy.
- **Device**: Various device states such as operating system version, patch level, and compliance level can be taken into consideration while applying a policy.
- **Application**: Conditional Access policies can be triggered depending on the application or the corporate resource the user is attempting to access.

Based on the above signals, one of the following decisions can be made:

- Block access
- Grant access
- Grant access subject to user satisfying conditions like MFA, ensuring device compliance, forcing password change, accepting terms of use, and so on

An administrator can create Conditional Access policies from the Microsoft Entra administrator portal. The following are the steps:

1. Log in to `https://entra.microsoft.com` as a**Conditional Access Administrator**.
2. Navigate to **Entra ID | Conditional Access**.
3. In the right-pane, click on **Create new policy** to configure your policy.

Note

There are several controls available in Conditional Access. Discussing each control is beyond the scope of this book. It is recommended to read Microsoft's online documentation.

Protected actions

Protected actions are Microsoft Entra ID permissions that are protected by Conditional Access policies. They are used when organizations want to add an additional layer of security. They can be applied to actions that require strong protection regardless of the role carrying out that action.

Conditional Access policies can be applied to a small subset of permissions in Microsoft Entra ID.

Following are the areas where protected actions can be applied:

- Conditional Access policy management
- Cross-tenant access settings management

- Custom rules that define network locations
- Protected action management

The Conditional Access policy applied to the permission triggers when the user attempts to carry out the action and not during user sign-in.

Protected actions can be used along with PIM role activation to further strengthen security. PIM role activation can also be protected using Conditional Access policies. In this case, a Conditional Access policy is applied when the user attempts to activate the privileged role, while protected actions protect the high-impact permissions regardless of the user role.

The minimum license required to use protected actions is **Microsoft Entra ID P1**.

The following are the steps to use protected actions. These steps should be followed in sequence for proper configuration:

1. Log in to `https://entra.microsoft.com`.
2. Navigate to **Entra ID | Conditional Access**.
3. Click on **Authentication contexts,** and in the right pane, click on **New authentication context**. In the fly out pane, give the authentication context a name and click **Save** as shown in the following figure:

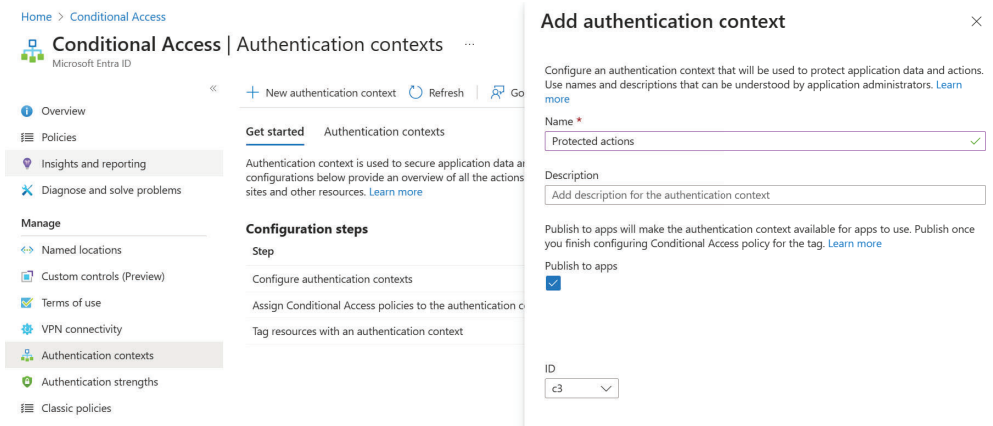


Figure 2.40: New authentication context

4. Navigate to **Entra ID | Roles & admins | All roles**.
5. Click on **Protected actions** and in the right pane click on **Add protected actions**.
6. In the Conditional Access authentication context, select the authentication context created in *Step 3*. Click on **Select permissions** and from the fly out pane select the

permissions that you want to protect and click on **Add** and then click on **Save** as shown in the following figure:

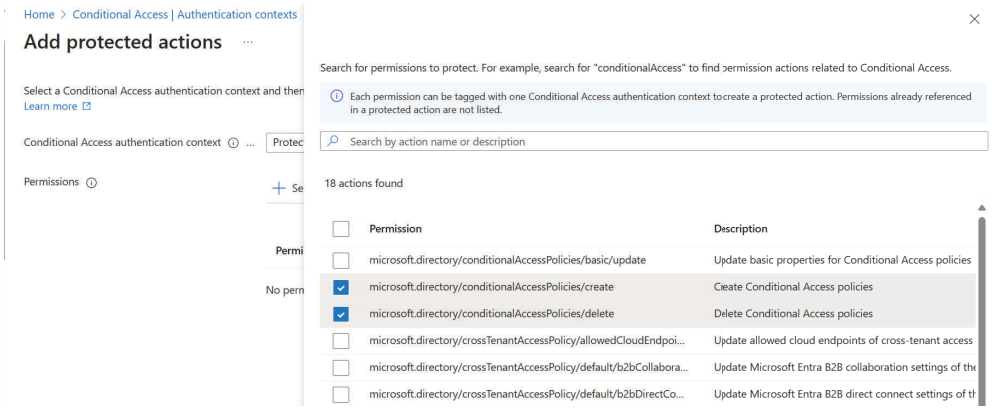


Figure 2.41: Add protected actions to authentication context

7. Once this is done, you can create a Conditional Access policy using this authentication context.

Protected actions in Microsoft Entra allow administrators to safeguard sensitive permissions by requiring additional authentication context and Conditional Access policies before those actions can be performed.

Summary

This chapter explained the fundamental concepts of Microsoft Entra ID. You learned about role-based access control in Microsoft Entra ID. You can use the available built-in roles and create custom roles if required. You also learned how roles can be assigned to users or to role-assignable groups. Further, you learned about SSO and MFA. The section on authentication methods talked about the various authentication options available to end users and how to implement them using Microsoft Entra ID. Lastly, this chapter explained protected actions and how you can implement them and more using Conditional Access. In the next chapter, you will learn how to set up Entra ID in cloud-only and hybrid modes.

Exercises

1. You are developing a new application for your organization and want that users should be able to sign in with their existing Entra ID credentials without having to sign in again. Which of the following is the best option?
    a. Password-based SSO

   b. SAML
   c. Linked SSO
   d. OIDC and OAuth
2. Which of the following is not a passwordless sign-in method in Microsoft Entra ID?
   a. Windows Hello for Business
   b. Push notifications on the Microsoft Authenticator app
   c. Certificates
   d. Passkeys
3. What are the ways in which Microsoft Authenticator app can be used?
   a. TOTP
   b. Push notifications
   c. Passwordless
   d. All of the above

Answers

1. D
2. B
3. D

Additional resources

- Role-based access control in Microsoft Entra: `https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/custom-overview`
- Best practices: `https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/best-practices`
- Protected actions: `https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/protected-actions-overview`
- Conditional Access: `https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview`
- Multifactor authentication: `https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mfa-howitworks`
- Authentication methods: `https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-methods`

Join us on Discord

For discussions around the book and to connect with your peers, join us on Discord at `packt.link/discordcloud` or scan the QR code below:



3

Implementing Microsoft Entra ID

A good identity infrastructure is essential for an enterprise, as it enables better security and user productivity. When you design an identity infrastructure for your organization, you must consider various factors like the current identity model, the future desired state, the security strategy, and the regulatory landscape the organization is subject to. Microsoft Entra ID supports various implementation methods. Organizations born in the cloud can run completely in the cloud without having any on-premises **Active Directory (AD)** servers. However, most organizations have a significant on-premises infrastructure that is required to run their business. Such organizations can run Microsoft Entra ID in hybrid mode, where objects from on-premises AD can synchronize to Microsoft Entra ID. Depending on the identity model an organization chooses, there are various options to synchronize on-premises objects to Microsoft Entra ID. Microsoft Entra ID also offers robust methods like Administrative Units and end user self-service options to decentralize user and group management. It has strong built-in security controls which provide a baseline level of security for all organizations.

This chapter will cover:

- Determining and implementing the right identity model
- Managing users and groups in Microsoft Entra ID
- Administrative units
- End-user self service
- Fundamental security settings

Determining the identity model

The first decision while deciding on an identity model would be to decide between cloud-only identity and hybrid identity. This will vary based on your organization's identity requirements,

whether you have an on-premises Active Directory infrastructure, how much you rely on it, and the need to keep it.

The following table explains the two identity models:

Attribute	**Cloud-only identity**	**Hybrid identity**
Definition	User accounts exist only in the Microsoft Entra tenant	User accounts exist in on-premises Active Directory and are synchronized to the Microsoft Entra ID tenant
Management	Entra ID portal or PowerShell	User accounts are primarily managed in the on-premises Active Directory and changes are synchronized to the cloud
Authentication	The Microsoft Entra ID tenant performs authentication for the identities	Authentication can be handled either by on-premises Active Directory or the Microsoft Entra ID tenant, depending on how the synchronization is set up
Best for	Organizations that do not need an on-premises Active Directory infrastructure	Organizations that have investments and dependencies on their on-premises Active Directory
Advantage	Simple, easy to set up and use	Users can use the same credentials when accessing legacy and cloud-based applications
Limitation	Limited password policy customization	Complex to set up and maintain

Table 3.1: Cloud identity models

Setting up Microsoft Entra ID tenant

Regardless of which identity model you choose, the first step is to create a Microsoft Entra ID tenant. A Microsoft Entra ID tenant is a dedicated, cloud-based directory service that organizations use to manage user identities and resources in Microsoft's cloud environment. If

your organization is using any Microsoft online services such as Microsoft 365 or Azure, you will already have a Microsoft Entra tenant created. To check the tenant, sign in to `https://entra.microsoft.com` with at least a **Tenant Creator** role. If a tenant exists, you will automatically be signed in. You can see the tenant name and tenant ID if you hover over your name in the top right corner. If a tenant does not exist, you will see a GUID instead.

If you don't have a tenant or if you would like to create additional tenants for development or testing purposes, you must have an Azure subscription.

> **Note**
>
> If you do not have an Azure subscription, create a free account by going to `https://azure.microsoft.com/en-us/free/`.

Follow these steps to create a new Microsoft Entra ID tenant:

1. Log in to `https://portal.azure.com`.
2. In the left navigation pane, click on **Microsoft Entra ID**.
3. Navigate to **Overview | Manage Tenants** and then click **Create**.
4. On the **Basics** page, select **Microsoft Entra ID** and click **Next: Configuration** as shown in the following screenshot:

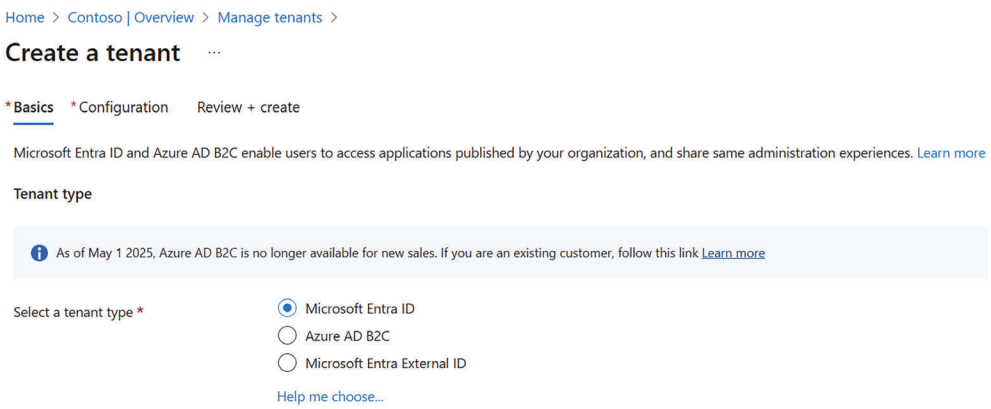


Figure 3.1: Creating a new tenant

5. On the Configuration page, enter the **Organization name**, **Initial domain name**, and **Location** and click **Next: Review + create**. Refer to the following figure. Exercise caution while selecting these details as it is not possible to change them later. When

you create a new Microsoft Entra tenant, you become the **Global Administrator** of the tenant. You are also listed as the technical contact for the tenant.

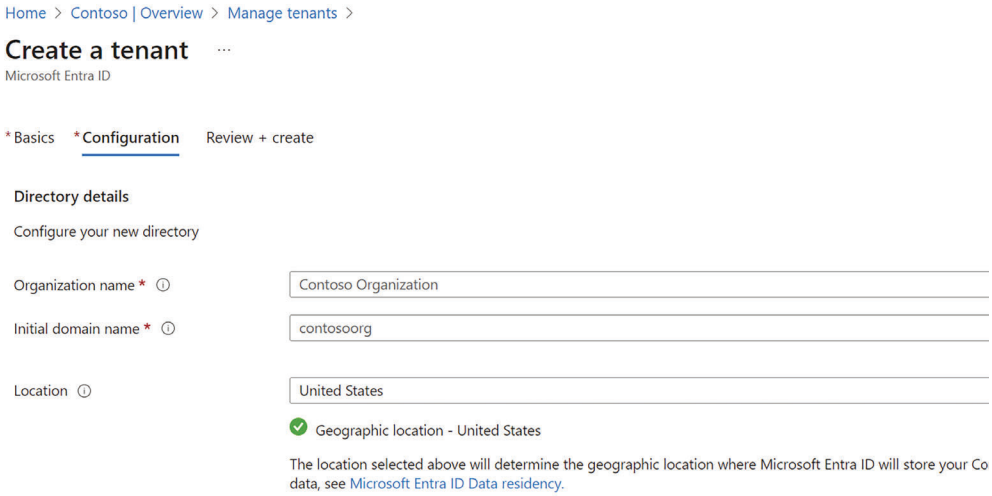


Figure 3.2: Enter organization details

Microsoft Entra tenants are created with an initial domain like `yourorganizationname.onmicrosoft.com`. The user IDs are therefore in the format `user1@yourorganizationname.onmicrosoft.com`. This cannot be changed or deleted, but an additional domain name can be added to the tenant. This creates an additional domain name that is familiar to the users, such as `user1@yourorganizationname.com`.

Follow these steps to add a custom domain name:

1. Log in to `https://entra.microsoft.com` with an ID that has the **Domain Name Administrator** role assigned.
2. Browse to **Entra ID | Domain names | Custom domain names**.
3. In the right pane, click on **Add custom domain**. Enter your organization's domain and click **Add domain**.

> **Note**
>
> The custom domain name must include `.com`, `.net`, or any other top-level extension for this to work. The organization should already have a top-level domain registered with a domain registrar.

4. The unverified domain is added, showing the DNS information as in the following screenshot. This will be required to validate your ownership of the domain. Save this information.

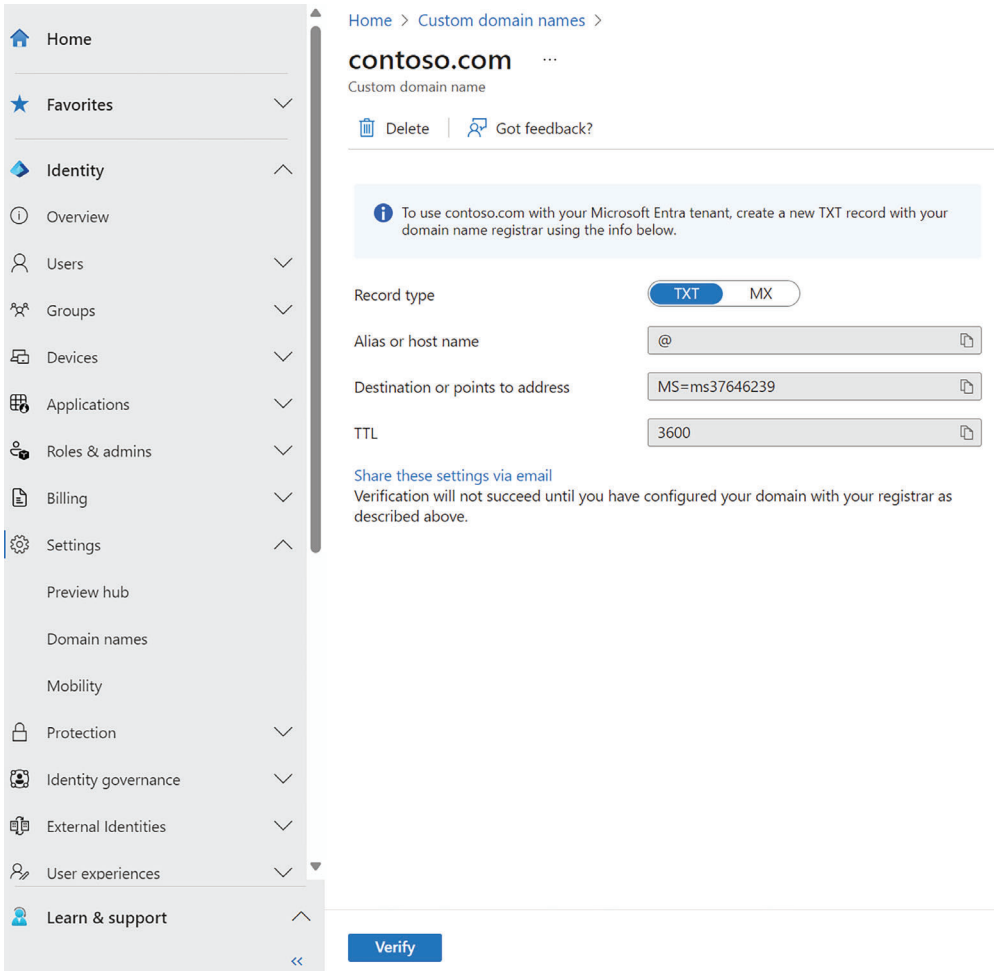


Figure 3.3: Unverified domain added

5. Next, update your record with your domain registrar with this DNS information by creating a TXT or MX record.

> **Note**
>
> You can add as many custom domains with your domain registrar as you like, but keep in mind that each domain gets its own TXT or MX record. If you add incorrect or duplicate information, you will have to wait for the **time to live (TTL)** to expire before you can try again.

6. After adding the DNS information with the domain registrar, ensure that the domain is valid in Microsoft Entra. On the page shown in *Figure 3.3*, click the **Verify** button to verify the domain name. The following figure shows the Microsoft Entra ID tenant with the domain name verified.

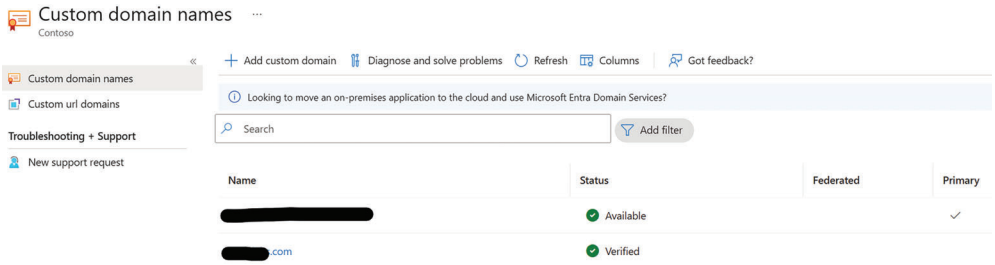


Figure 3.4: Verified domain name

Sometimes there can be issues while verifying a domain name. If you cannot verify a custom domain name, try again after an hour, ensure there are no errors in the domain information and ensure the domain is not in use in another directory.

Now that you have your Microsoft Entra ID tenant set up, you can proceed with implementing the identity model you chose for your organization.

Cloud-only identity

If you chose to use the cloud-only identity model, you begin by creating a Microsoft Entra ID tenant as described in the previous section. Once the tenant is created, you can proceed with managing your tenant. For most organizations, this would mean creating and managing user accounts and groups. For organizations that use cloud-only identity, user accounts and groups are created and managed in Microsoft Entra ID.

Creating users

With this method, administrators would use the Microsoft Entra ID portal to create the user accounts. Following are the steps for the same:

1. Log in to `https://entra.microsoft.com` with an account that has the **User Administrator** role assigned.
2. Navigate to **Entra ID | Users | All users**.
3. In the right pane, click on **New user | Create new user**.
4. On the **Create new user** page, fill in the **Display name** and **User principal name**. The user principal name must be unique in the directory. Ensure that the boxes **Derive from user principal name**, **Auto-generate password**, and **Account enabled** are checked, as shown in the following figure. Once done, click the **Next: Properties** button.

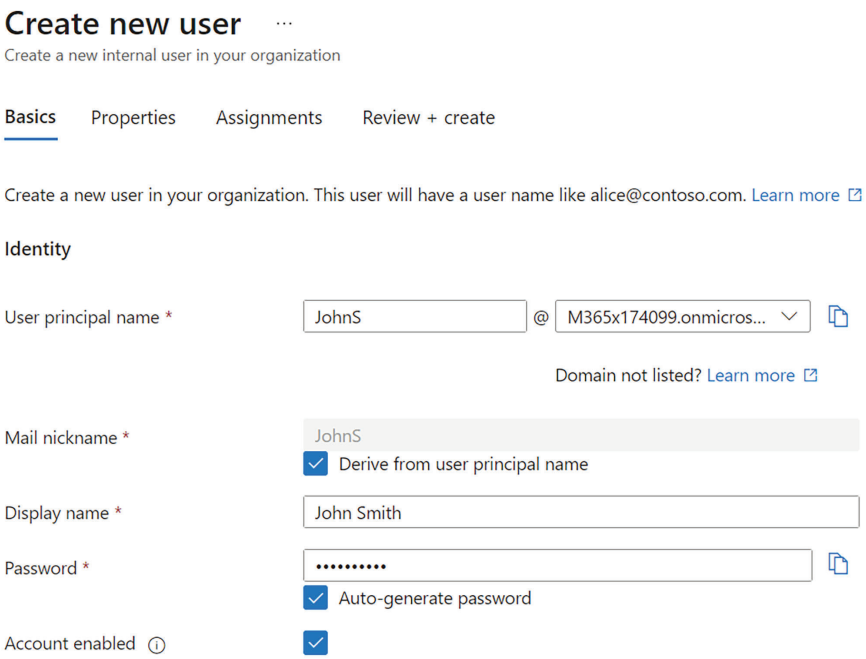


Figure 3.5: Create a new user account

5. On the **Properties** page, enter the user details like first name, last name, job title, department as appropriate and click on **Next: Assignments**.

6. On the **Assignments** page, you can assign the user to appropriate **Administrative Units**, **Groups**, and **Roles**. Click **Next: Review + create**.
7. On the **Review + create** page, click **Create**

Creating groups

With Microsoft Entra ID, you can use groups to make management of user accounts easier. Using groups enables administrators to grant permissions and assign licenses to groups rather than individual users. You can also manage access to applications using groups. There are two types of groups available in Microsoft Entra ID as follows:

- **Security**: These groups are used to manage user access to shared resources.
- **Microsoft 365**: These groups offer collaboration capabilities across shared mailboxes, SharePoint sites, and more.

Group membership can be managed in three ways as follows:

- **Assigned**: Administrators can add each individual user to groups.
- **Dynamic user**: Using this method, administrators can use rules to dynamically assign users to groups. For example, you could create a group for all users in the **Legal** department. This is based on the users' Microsoft Entra ID attributes. Once created, all users whose **Department** field in Microsoft Entra ID is *Legal* will be dynamically added to this group. As and when the user's Entra ID attributes are updated, the group membership is dynamically updated.
- **Dynamic device**: Using this group type, you can dynamically add or remove devices to a group based on their attributes.

The steps to create a group are explained in *Chapter 2, Fundamentals of Microsoft Entra ID*, under the *Using role-assignable groups* section.

Hybrid identity

In a hybrid identity model, user accounts are created in on-premises AD and are synchronized to Microsoft Entra ID. Most user account changes flow from on-premises to Microsoft Entra ID. When hybrid identity is implemented, the on-premises AD remains authoritative for account information. This means that you will be performing administrative tasks on-premises and changes will be synchronized to Microsoft Entra ID. Provisioning and synchronization are key concepts in hybrid identity. **Provisioning** means creating, updating, and deleting an object based on certain conditions. **Synchronization** means ensuring that on-premises identity information matches that in the cloud.

Microsoft Entra ID supports the following types of provisioning:

- **HR-driven provisioning**: It involves creating user accounts in Microsoft Entra ID directly from a supported HR system. When a new employee joins a company, they are entered into the HR system. When this happens, their ID is automatically created in the Microsoft Entra ID tenant. It also supports employee attribute changes such as when employees move across teams and their attributes such as manager name, department, etc., are updated. When employees leave the organization and their account in the HR system is terminated the same is updated in Microsoft Entra ID as well.
- **App provisioning**: This process encompasses the automated creation, lifecycle management, and deprovisioning of user identities across cloud-based applications. It ensures that users are granted appropriate access to the services required for their roles, while also maintaining compliance and security standards. Common scenarios include provisioning Microsoft Entra user accounts into third-party SaaS platforms such as Dropbox, Salesforce, ServiceNow, and other enterprise applications.
- **Directory provisioning**: This involves provisioning from on-premises AD forests to Microsoft Entra ID. This chapter will focus on directory provisioning using Microsoft Entra Connect Sync and Microsoft Entra Connect cloud provisioning.

Microsoft Entra Cloud Sync

Microsoft Entra Cloud Sync is a service from Microsoft that synchronizes on-premises Active Directory and Microsoft Entra ID using Microsoft online services. A lightweight agent acts as a bridge between Microsoft Entra ID and Active Directory and stores the configuration in Microsoft Entra ID. The agent provides cloud sync and on-premises app provisioning capabilities. It uses SCIM and provides the following benefits:

- Synchronize multiple disconnected Active Directory forests to a single Microsoft Entra tenant.
- Simple installation using a lightweight provisioning agent.
- Supports groups with up to 50,000 members. If you have groups that have more than 50,000 members you will have to use Microsoft Entra Connect Sync.
- Multiple provisioning agents can be used to address high availability scenarios.

Deployment scenarios

Microsoft Entra Cloud Sync supports the following deployment scenarios:

- Integrate a single Active Directory Forest with a single Microsoft Entra tenant.
- Integrate multiple Active Directory forests with a single Microsoft Entra tenant.

- There is already an existing forest with Microsoft Entra Connect, and a new forest is synchronized using Microsoft Entra Cloud Sync.
- Synchronize disconnected Active Directory forests to a single Microsoft Entra tenant.

Key components

There are two key components of Microsoft Entra Cloud Sync:

- **A provisioning agent**: Built on the same server-side technology as Application Proxy and Pass-through Authentication, the provisioning agent requires only outbound connections to the Microsoft Cloud. The agent is auto updated.
- **A provisioning service**: This is the service responsible for updating changes to the Microsoft Entra ID tenant every two minutes.

Installing Microsoft Entra Cloud Sync

The following sections explain the prerequisites and the steps to install and configure Microsoft Entra Cloud Sync in your environment.

Prerequisites

Before you install the Microsoft Cloud Sync agent, ensure that the following requirements are met:

- A **Domain Administrator** or **Enterprise Administrator** account.
- A Microsoft Entra tenant with a custom domain name verified.
- A **Hybrid Identity Administrator** account created as a user in Microsoft Entra ID.
- An on-premises server or virtual machine running Windows 2016 or later with 4GB RAM and .NET 4.7.1+ runtime. TLS 1.2 should be enabled. NTLM should not be enabled.
- The agent must be installed on a domain-joined server that is running Windows Server 2022 or Windows Server 2016. Windows Server 2025 is not supported.
- The agent should be able to make outbound requests to Microsoft Entra ID over ports 80, 443, and 8080.
- The agent must be able to communicate with domain controllers on TCP ports 389 and 3268.
- The PowerShell execution policy on the server should be set to *Undefined* or *RemoteSigned*.
- **Group Managed Service Accounts (gMSAs)** are specialized domain accounts that streamline service identity management by providing automatic password management, simplified **Service Principal Name** (**SPN**) handling, delegated administration capabilities, and support for use across multiple servers. These

accounts enhance security and reduce administrative overhead by eliminating the need for manual password rotation and enabling controlled delegation of management tasks. The creation of a gMSA requires administrative credentials, and the accounts are represented in the format `domain\provAgentgMSA$`.

Note

Creating and configuring Group Managed Service Accounts is beyond the scope of this book. Refer to the Microsoft online documentation for the detailed steps.

Installation steps

The following steps must be completed on the server selected to run the Cloud Sync agent:

1. Go to `https://entra.microsoft.com` and navigate to **Entra ID** | **Entra Connect**.
2. On the Microsoft Entra Connect page, in the left pane, click on **Cloud Sync**.
3. On the **Cloud Sync** page, in the left pane, click on **Agents**.
4. In the right pane, click on **Download on-premises agent**. In the flyout pane, click on **Accept terms and download**.
5. Once the package has downloaded, double-click on `AADConnectProvisioningAgentSetup.exe` to start the installation.
6. On the splash screen, accept the license terms and conditions, and click on **Install**.
7. Once the installation is complete, the configuration wizard will start. Click **Next** to start the configuration.
8. On the **Select Extension** page, select **HR-driven provisioning (Workday and SuccessFactors)/Azure AD Connect Cloud Sync** and click **Next**.
9. On the next page, click on **Authenticate** and sign in with your Microsoft Entra Global Administrator or Hybrid Identity Administrator credentials.
10. On the **Configure Service Account** page, choose the option **Create gMSA** and enter your Active Directory Domain Administrator credentials to create the `provAgentgMSA$`. This will be created in the same domain where your sync server has joined. You can also choose to **Use custom gMSA** to specify a gMSA that you may have manually created for this purpose. However, it is recommended to let the tool create the gMSA for you. Once done, click **Next**.
11. On the **Connect Active Directory** page, if your domain is listed under **Configured Domain**, proceed to the next step. If not, enter your Active Directory domain name, and

click on **Add Directory**. Enter your Domain Administrator credentials, click **OK**, and then click **Next**.

12. On the **Configuration complete** page, click **Confirm** to register and restart the agent.
13. Once complete, you will see a message **Your agent configuration was successfully verified**. Click on **Exit** to close the configuration wizard.

Verifying the installation

You would need to verify that the cloud sync agent is successfully installed and working. This must be done both in the Microsoft Entra ID tenant and on the local server.

To verify the installation in Microsoft Entra ID tenant, follow these steps:

1. Go to `https://entra.microsoft.com` and navigate to **Entra ID** | **Entra Connect**.
2. On the Microsoft Entra Connect page, in the left pane, click on **Cloud sync**.
3. On the Cloud Sync page, you will see the agents installed. Confirm that the agent is displayed, and the status is **Healthy**.

Follow the steps below on the local server to confirm:

1. Sign into the server with a **Local Administrator** account
2. Open the Services snap-in and ensure that the status of the below services is **Running**
    a. **Microsoft Entra Connect Agent Updater**
    b. **Microsoft Connect Provisioning Agent**

Microsoft Entra Connect

Earlier called Azure AD Connect, this is an on-premises application that is designed to synchronize identities from on-premises Active Directory to Microsoft Entra ID. This involves installing an on-premises infrastructure, that includes SQL Server. If you are just starting with your cloud synchronization journey, consider using Microsoft Entra Cloud Sync. However, there might be several scenarios where you would still need to use Microsoft Entra Connect:

- You do not want to synchronize your user account passwords to the cloud
- You want to connect to LDAP directories
- You want to allow advanced customization for attribute flows
- You need support for merging user attributes from multiple domains
- You need support for unlimited objects per AD domain
- You have large groups with up to 250,000 members
- You have a large-scale deployment that will benefit from the performance and stability provided by a backend SQL server

Microsoft Entra ID Connect offers password hash synchronization, pass-through authentication, and federation. These are discussed in detail in the next section.

Microsoft Entra Connect Synchronization services (Microsoft Entra Connect Sync) is the main component of Microsoft Entra Connect. This is the service that synchronizes identity data between on-premises AD and Cloud. This sync service consists of two components: the on-premises **Microsoft Entra Connect Sync** and the service-side component called **Microsoft Entra Connect Sync** service. Earlier, this service was called DirSync and then Azure AD Sync. It also provides robust monitoring in a central location within the Microsoft Entra admin center.

Installation requirements

Before you proceed with the installation of Microsoft Entra Connect, ensure that the following requirements are met:

- A cloud-only identity with the **Hybrid Identity Administrator** permissions.
- A Microsoft Entra ID tenant with a verified domain name.
- Prepare your on-premises data using the **IdFix** tool to identify errors such as duplicates or formatting issues before synchronizing to the cloud.
- An on-premises Active Directory environment with schema version and forest functional level at Windows Server 2003 or later.
- PowerShell execution policy set to **RemoteSigned**.
- Connectivity to a DNS server, to enable name resolution for both internet and intranet.
- Network connectivity to all configured domains and to the root domain of all configured forests.
- Open Microsoft Entra Connect ports if you are using firewalls on your intranet. For a complete list of ports, refer to `https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/reference-connect-ports`.
- Allow the Office 365 URLs in your firewall to ensure connectivity to Microsoft Online Services. For a complete list of URLs refer to Microsoft online documentation.

Note

The IdFix tool is used to perform remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Microsoft Entra ID. It can be downloaded from GitHub at `https://github.com/Microsoft/idfix`.

The following are some important considerations:

- Read-only domain controllers are not supported.
- Using on-premises forests or domains that contain dot (.) NetBIOS names is not supported.
- Enabling Active Directory recycle bin is recommended.
- Microsoft Entra Connect cannot be installed on Small Business Server or Windows Server Essentials before 2019.
- The server should have full GUI support. Windows Server Core is not supported.
- There is a known issue with Windows Server 2025. If you are using Windows Server 2025, install the **October 20, 2025 – KB5070773** hotfix or later.
- Windows Server 2019 is in extended support, and you may require a paid support plan if using this version.
- Breaking and analyzing traffic between Microsoft Entra Connect and Microsoft Entra ID is not supported.

Connect server requirements

The server on which the Microsoft Entra Connect Sync will be installed should meet the following requirements:

- A domain-joined Windows Server 2016 or later. Windows Server 2022 is recommended.
- .NET Framework version 4.7.2 or later.
- Microsoft PowerShell 5.0 or later.
- TLS 1.2 enabled.

The memory, CPU, and hard disk requirements differ according to the number of objects to be synchronized from the on-premises Active Directory. Refer to the following table for the exact requirements:

Number of objects in Active Directory	CPU	Memory	Hard drive size
Fewer than 10,000	1.6 GHz	6 GB	70 GB
10,000–50,000	1.6 GHz	6 GB	70 GB

Number of objects in Active Directory	CPU	Memory	Hard drive size
50,000–100,000	1.6 GHz	16 GB	100 GB
100,000 – 300,000	1.6 GHz	32 GB	300 GB
300,000 - 600,000	1.6 GHz	32 GB	450 GB
More than 600,000	1.6 GHz	32 GB	500 GB

Table 3.2: Minimum hardware requirements for Entra Connect

SQL server requirements

Microsoft Entra Connect uses a SQL database to store identity data. By default, a SQL Server 2019 Express LocalDB is installed. This enables you to manage 100,000 objects. If your Active Directory contains more than 100,000 objects, you need to install the full version of SQL. For performance reasons, it is recommended to install the SQL server on the same server as the Microsoft Entra Connect tool.

Installation types

Microsoft Entra Connect offers two installation choices. Refer to the following table to decide which one is appropriate for your environment:

Express	Custom
You have a single Active Directory forest on-premises.	You have or want to synchronize more than one AD forest.
You have an Enterprise Administrator account	You do not have access to an Enterprise Administrator account
You have fewer than 100,000 objects in on-premises AD	You have more than 100,000 objects in on-premises AD

Express	Custom
You plan to use password hash sync for authentication	You plan to use federation or pass-through authentication
You want to synchronize all objects in the domain or OU	You want to synchronize a subset of the objects

Table 3.3: Express vs custom settings

Installation steps

The steps to install Microsoft Entra Connect differ depending on the options you choose. Before you begin the installation, log in as **Local Administrator** on the server you want to install Microsoft Entra Connect. Download the tool from `https://www.microsoft.com/en-us/download/details.aspx?id=47594` and execute `AzureADConnect.msi` to launch the installation wizard.

From here, the steps will differ depending on the authentication method you choose. Those steps will be discussed in detail when we discuss the authentication methods in the next section.

Object filtering

By default, Microsoft Entra Connect synchronizes all objects from the on-premises Active Directory to Microsoft Entra ID, which is the recommended configuration. In some scenarios, you might want to control which objects are synchronized to Microsoft Entra ID. The following are some possible scenarios:

- You are running a pilot and want to test with a subset of users first.
- You have non-personal accounts, like service accounts, that you do not want to synchronize to Microsoft Entra ID.
- You do not delete on-premises accounts, but you want only active accounts in Microsoft Entra ID.

In these scenarios, you can use object filtering to synchronize only a subset of the accounts. There are four filtering options available:

- **Group-based filtering**: Filtering based on a single group is only possible during the initial installation of Microsoft Entra Connect, when using custom installation in the installation wizard. This option is used when running a pilot deployment. Once the pilot is complete, you can use one of the other filtering methods. Once group-based filtering is disabled, it cannot be re-enabled.

- **Domain-based filtering**: This option enables you to choose which domains you want to synchronize to Microsoft Entra ID. You can do this at the first install of the Microsoft Entra Connect tool when using the custom installation settings and selecting the domains to synchronize on the **Domain/OU filtering** page. This can also be done at a later stage by re-running the Microsoft Entra Connect installation wizard.
- **Organizational Unit (OU)-based filtering**: This option enables you to select specific OUs to synchronize to Microsoft Entra ID. You can do this at the first install of the Microsoft Entra Connect when using custom installation settings and selecting the OUs to synchronize on the **Domain/OU filtering** page. This can also be done at a later stage by re-running the Microsoft Entra Connect installation wizard.
- **Attribute-based filtering**: This is the most flexible method of object filtering as you can control nearly every aspect of the objects synchronized. This uses the user account attributes to determine which user account should be synchronized to Microsoft Entra ID.

Microsoft Entra Connect Health

Installed along with Microsoft Entra Connect, Microsoft Entra Connect Health provides monitoring for your on-premises identity infrastructure. Log in to the Microsoft Entra Connect Health portal via `https://aka.ms/aadconnecthealth` to view alerts, performance metrics, and usage analytics.

Authentication methods

There are various methods of enabling authentication when on-premises identities are synchronized to Microsoft Entra ID. Choosing the right authentication type is the first concern for organizations wanting to move to the cloud. This is a very important decision because:

- It is the first decision an organization will make when they plan to move to the cloud
- Authentication controls access to all cloud data and resources
- It is the foundation of all other advanced security measures that will be implemented in the future
- It is difficult to change and requires careful planning

Microsoft Entra Connect offers three authentication choices: password hash sync, pass-through authentication, and federated authentication. We will learn more about these in the following sections.

Password hash sync

Password hash sync is the simplest method to enable authentication for on-premises Active Directory objects in the cloud. In this method, password hashes are synchronized to Microsoft Entra ID. The users can use the same usernames and passwords for all on-premises and cloud applications. It offers the following key advantages:

- Requires the least amount of administrative effort in terms of deployment, infrastructure, and maintenance.
- Advanced identity protection features like leaked credential reports are available only with this method.
- Provides business continuity. If your on-premises Active Directory infrastructure is not available, the users will still be able to authenticate.
- Password hash sync can be used as a fallback mechanism for the other two authentication methods. If you have certain business requirements that are not met by password hash sync, you can use one of the other two methods and use password hash sync as a fallback method to continue providing authentication services to your end users in case your on-premises infrastructure is unavailable.
- It also enables leaked credentials detection for hybrid accounts. Microsoft works with security researchers and law enforcement to find username/password pairs that are publicly available. If such accounts are found, Microsoft Entra flags them as high risk.

The on-premises Active Directory stores user passwords as an MD4 hash value of the original password. This is the result of a hashing algorithm, which is a one-way mathematical function. There is no way that a hashed value can be reversed to obtain the original password.

Microsoft Entra Connect sync extracts the password hash from Active Directory and applies additional security to the hashed password before synchronizing it with Microsoft Entra ID. The passwords are synchronized every two minutes, and this interval cannot be modified.

On the first run, all passwords of in-scope users are synchronized to Microsoft Entra ID. You can use staged rollout to test user groups with capabilities like MFA, Conditional Access, Identity Protection, and Identity Governance. The following figure shows how password hash sync works between Active Directory and Microsoft Entra ID.

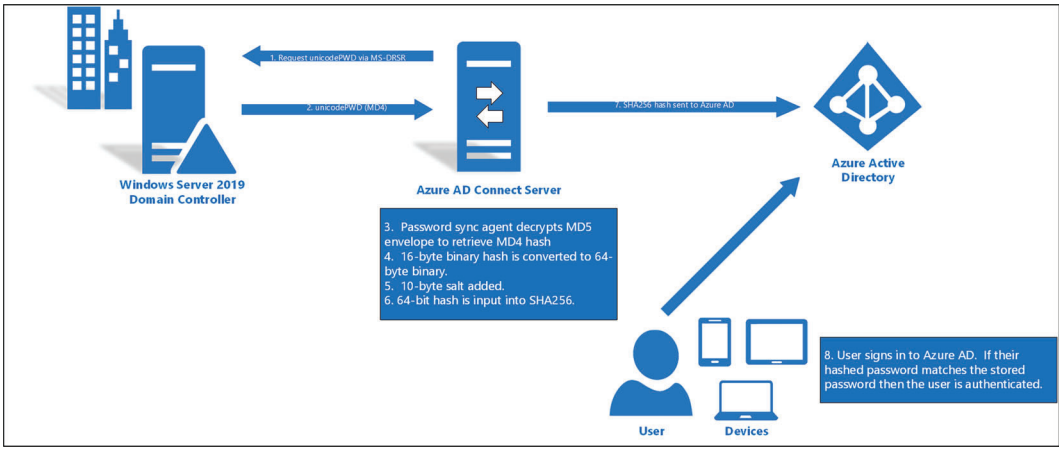


Figure 3.6: Password hash sync

The following are some important considerations for password hash synchronization:

- The plain-text passwords are never exposed to the password hash synchronization agent or to Microsoft Entra ID.
- The passwords are never stored in SQL. They are only processed in memory and then sent to Microsoft Entra ID.
- Users are authenticated against the passwords stored in Microsoft Entra and not on the on-premises Active Directory.
- Since the MD4 hash is not transmitted to Microsoft Entra ID, if the Microsoft Entra ID password is stolen, it cannot be deciphered back to the original password stored in on-premises Active Directory. This protects the passwords from pass-the-hash attacks.
- For synchronized users, the on-premises Active Directory password complexity policies override the password complexity policies in Microsoft Entra ID. Users created directly in the cloud still get the Microsoft Entra ID password complexity policy.
- For synchronized users, the password in Microsoft Entra ID is set to Never Expire. The account expiry attribute is not synchronized to Microsoft Entra ID from on-premises Active Directory. It is possible for users to log in to cloud services even if their on-premises password has expired. It is recommended to use a PowerShell script, using the `Set-ADUser` cmdlet, that disables a user's Entra ID account once their on-premises Active Directory account expires.
- Organizations usually provide a temporary password to new users and turn on the flag **User must change password at next logon**. To turn on temporary password support

in Microsoft Entra ID for synchronized users, you should run the following command on your Entra Connect server:

```
Set-ADSyncAADCompanyFeature -ForcePasswordChangeOnLogOn $true
```

This feature should only be used if you have Self Service Password Reset and Password Writeback enabled in your tenant.

Selective password hash synchronization

Once you enable password hash synchronization, all users' passwords will be synchronized to Microsoft Entra ID. If you would like to synchronize a subset of the users, you can use selective password hash synchronization.

The first decision you would need to make is the number of users whose passwords you would like to synchronize to Microsoft Entra ID. To reduce administrative effort, the steps you follow are different if the included users are more than the excluded users, and vice versa.

Both the scenarios use the `adminDescription` attribute. Rules are applied based on the value of this attribute and that is what makes selective password hash synchronization work. If the number of excluded users is less than the number of included users, the value of the `adminDescription` attribute should be `PHSFiltered`. If the number of excluded users is more than the included users, the value should be `PHSIncluded`.

Setting up password hash synchronization

Password Hash Synchronization is automatically enabled when you install Microsoft Entra Connect using the **Express settings** by following the steps below:

1. Sign in as **Local Administrator** on the server where you want to install Microsoft Entra Connect. This will serve as the sync server.
2. Download Microsoft Entra Connect from the Microsoft Download Center. Double-click `AzureADConnect.msi` to start the installation.
3. Accept the licensing terms and click **Continue**.
4. On the **Express settings** page, click on the button **Use express settings**.
5. On the **Connect to Azure AD** page, enter the username and password of an account that has the Hybrid Identity Administrator role assigned.
6. On the **Connect to AD DS** page, enter the username and password of the **Enterprise Administrator** account.
7. On the **Ready to configure** page, click **Install**. You can check the box **Start the synchronization process when configuration completes** if you want to start

synchronization immediately. You can clear this box if you want to add filtering. You also have the option to enable hybrid deployment of Exchange. You can use this option if you plan to have mailboxes both in Exchange Online and on-premises Exchange Servers.

8. Click **Exit** once the installation is complete.

Pass-through authentication

This is an alternative to the password hash sync method offering the same benefits of users being able to use the same username and password for both on-premises and cloud services. However, some organizations that want to enforce their own Active Directory security and password policies can choose pass-through authentication. In this method, passwords remain stored on the on-premises Active Directory. When the user tries to access an application, Microsoft Entra ID sends the authentication request to the pass-through authentication agent. The agent validates the user's password against Active Directory and if the password matches, the user is allowed access. Pass-through authentication offers the following benefits:

- Users can use the same username and password to access both on-premises and cloud applications.
- It is easy to deploy and administer. A simple lightweight agent is deployed.
- On-premises passwords are never stored in the cloud in any form.
- The agent makes only outbound connections from your network.
- Administrators can enforce on-premises password policies.

The following figure illustrates the components involved in pass-through authentication:

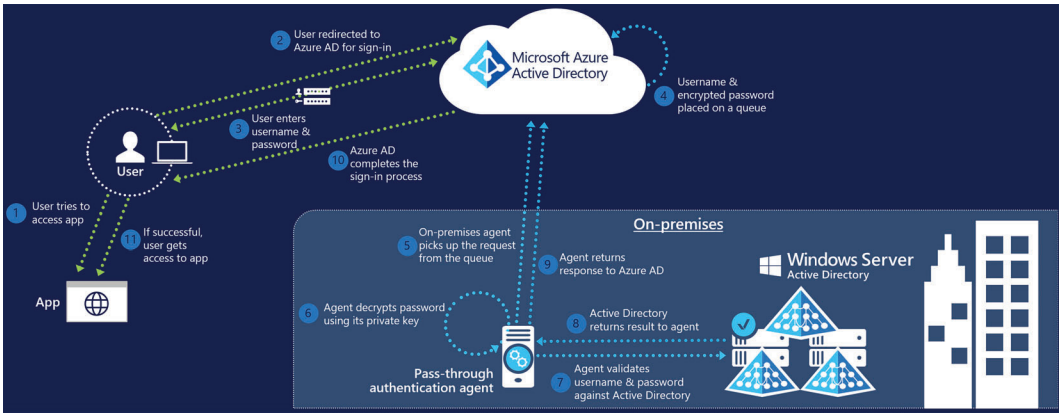


Figure 3.7: Pass-through authentication

Configuration prerequisites

Before configuring pass-through authentication, ensure that the following requirements are met:

- A cloud-only account with the **Hybrid Identity Administrator** permissions
- One or more custom domain names added to the Microsoft Entra tenant
- A server running Windows Server 2016 or later with Microsoft Entra Connect installed
- If you have a firewall between the servers and your Entra ID tenant, the following configuration is required:
    - Authentication agents should be able to make outbound requests over ports 80, 443, and 8080
    - Add the following URLs to the allow list: `*.msappproxy.net` and `*.servicebus.windows.net`
    - The authentication agent should be able to access `login.windows.net` and `login.microsoftonline.com`
    - Unblock the following URLs to validate certificates: `crl3.digicert.com:80`, `crl4.digicert.com:80`, `ocsp.digicert.com:80`, `www.d-trust.net:80`, `root-c3-ca2-2009.ocsp.d-trust.net:80`, `crl.microsoft.com:80`, `oneocsp.microsoft.com:80`, and `ocsp.msocsp.com:80`
    - Allow the URL `autologon.microsoftazuread-sso.com` if you have an outgoing HTTP proxy
    - Inline inspection and termination on outbound TLS communications should be avoided between the pass-through authentication agent and Microsoft Entra ID

Enabling pass-through authentication

Pass-through authentication is configured through the Microsoft Entra Connect custom settings. Within the **User Sign-in** configuration page, the **Pass-through Authentication** option must be selected as the designated sign-in method. The Pass-through Authentication agent is deployed on the same server hosting Microsoft Entra Connect, and once installed, the feature is activated at the tenant level to enable secure credential validation against the on-premises Active Directory.

Testing pass-through authentication

Follow the steps below to confirm that the configuration was completed successfully:

1. Sign in to `https://entra.microsoft.com` as **Hybrid Identity Administrator** and navigate to **Entra ID** | **Entra Connect** | **Connect sync**.
2. Confirm that **Pass-through authentication** is enabled.
3. Click on **Pass-through authentication**. The page should list the servers where the Authentication Agent is installed.

Federated authentication

Federation is a collection of domains that have a trust relationship. The on-premises Active Directory can be federated with Microsoft Entra ID using AD FS or another identity provider, allowing on-prem AD to authenticate users. This method ensures that all authentication occurs on the on-premises Active Directory servers and allows for the implementation of more rigorous levels of access controls. Using federation, you can enable users to sign in to cloud services using on-premises passwords.

Microsoft Entra ID Connect supports federation with **Active Directory Federation Service (AD FS)** and **PingFederate**.

Federation typically requires significant investment in on-premises infrastructure. Most organizations that choose this option already have an on-premises federated environment. It is arduous to maintain and will require significant hardware investment to provide load balancing and business continuity. You would typically use federation if you:

- Want to apply AD security policies like account expiry, disabled account, password expiry, sign-in hours, and account lockout
- Sign in using non-Microsoft authentication solutions
- Use multi-site on-premises authentication solution

Federated authentication is illustrated in *Figure 3.8*:

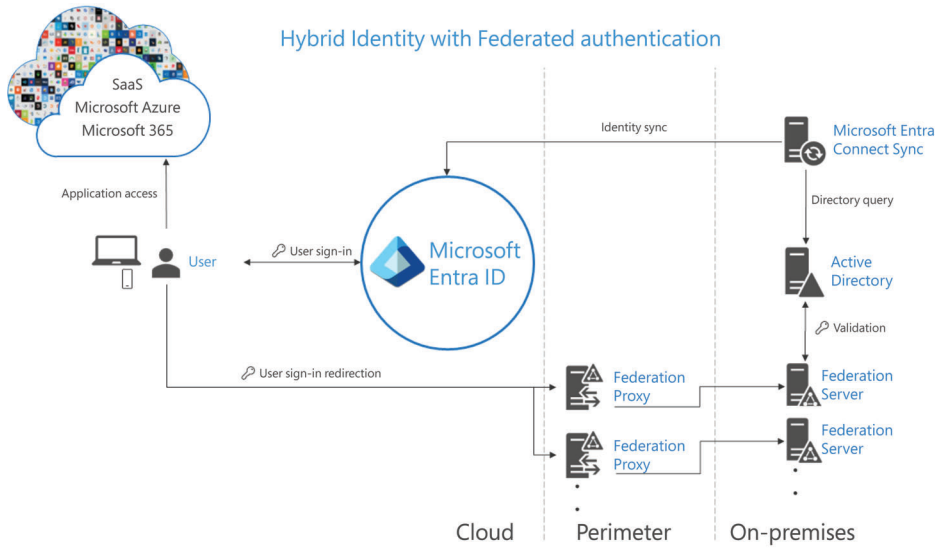


Figure 3.8: Federated authentication

Choosing the right method

Following is a handy decision tree that you can use to determine which authentication method is best suited to your business needs:

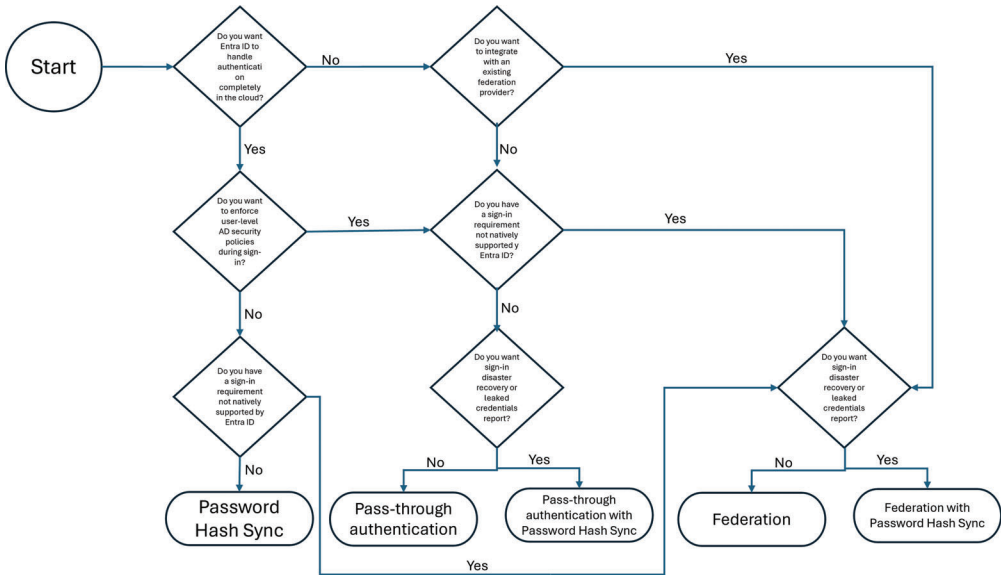


Figure 3.9: Authentication decision tree

Administrative units

Administrative units allow you to segment your organization into smaller blocks based on location, department, business unit, etc. This allows specific administrators to manage only members of that unit. For example, you could have separate admin units for Americas, EMEA, and Asia. You can then assign separate admins to control access, manage users, and set policies for those specific geographies.

It is important to note that a single object can be included in multiple administrative units depending on its scope. In the above example, if the organization has further administrative units for departments such as Marketing, Finance, and HR, a marketing user in EMEA could be a member of two administrative units, that is, EMEA and Marketing.

To create admin units, you need a Microsoft Entra P1 license for each administrative unit administrator.

Restricted management administrative units

In some scenarios, organizations might want to protect specific objects from modification by anyone other than a specific set of administrators. For example, you might want to protect the C-level executives and their devices from modification by the first-level helpdesk. You could assign them to a restricted management administrative unit and assign a separate administrator to that admin unit.

Users, devices, and security groups can be added to a restricted management administrative unit. Only roles that are assigned as administrators at the restricted management administrative unit scope level can perform all actions related to users, devices, and security groups in that admin unit. Other roles, including Global Administrator, cannot perform all actions. *Table 3.4* summarizes the allowed and disallowed actions for roles that are not assigned as administrators at the restricted management administrative unit scope level:

Action	**Blocked**	**Allowed**
Read standard user properties like name, photo		Y
Modify properties of the user, device or group	Y	
Delete the user, device or group	Y	
Reset the password for a user	Y	
Modify group members or owners	Y	

Action	Blocked	Allowed
Add users, groups, or devices to other groups		Y
Modify email and mailbox settings for users in Exchange		Y
Apply Intune policies to a device		Y
Add or remove a group as a site owner in SharePoint		Y

Table 3.4: Actions for the restricted management admin unit scope

Table 3.5 summarizes which administrators can modify the Microsoft Entra properties of objects (users, devices, and security groups) in a restricted management admin unit:

User role	Blocked	Allowed
Global administrator	Y	
Tenant-scoped administrator	Y	
Administrators assigned to the restricted management admin unit		Y
Administrators assigned to another restricted management admin unit of which the object is a member		Y
Administrators assigned to another regular admin unit of which the object is a member	Y	
Administrators assigned at the scope of a resource	Y	
Owners of groups and devices added to restricted management admin units	Y	

Table 3.5: Blocked and allowed actions by administrative scope

Restricted management administrative units have the following limitations:

- Restricted management administrative units can be configured only at the time of creation. This setting cannot be changed later.
- Groups in restricted management administrative units cannot be managed using Microsoft Entra ID Governance capabilities.
- Membership of a role-assignable group cannot be modified once it is added to a restricted management administrative unit.
- Group owners cannot modify the membership of a group that is included in a restricted management administrative unit. Only Global Administrator and Privileged Role Administrator can modify membership.
- Some actions cannot be performed on objects that are in a restricted management administrative group. For example, if a Global Administrator account is in a restricted management administrative unit, another administrator cannot reset their password. They will have to be removed from the admin unit to do this.
- Distribution groups, mail-enabled groups, and Microsoft 365 groups cannot be members of the restricted management administrative units.
- There can be a maximum of 100 restricted management administrative units in a tenant.

Creating an administrative unit

Following are the steps for creating an administrative unit:

1. Log in to `https://entra.microsoft.com` and navigate to **Entra ID** | **Roles & admins** | **Admin Units**.
2. In the right pane, click on **Add**.
3. Enter a name for the admin unit and optionally enter a description.
4. If you want to create a **Restricted management administrative unit**, switch the toggle to **Yes**. Click on **Next: Assign roles** as shown in the following figure:



Figure 3.10: Creating an administrative unit

5. Click on Next: Review + create to create the administrative unit.

Adding members to an administrative unit

Following are the steps to add members to an administrative unit:

1. Log in to `https://microsoft.entra.com` with an account that has the Privileged Role Administrator or Global Administrator role assigned.
2. Navigate to **Entra ID | Roles & admins | Admin Units**. In the right pane, select the newly created admin unit.
3. Click on **Users** and in the right pane click on **Add member** to pick the members from the list. You can also add users in bulk by clicking on **Bulk operations | Bulk add members**. You will be prompted to upload a `.csv` file as shown in the following figure:

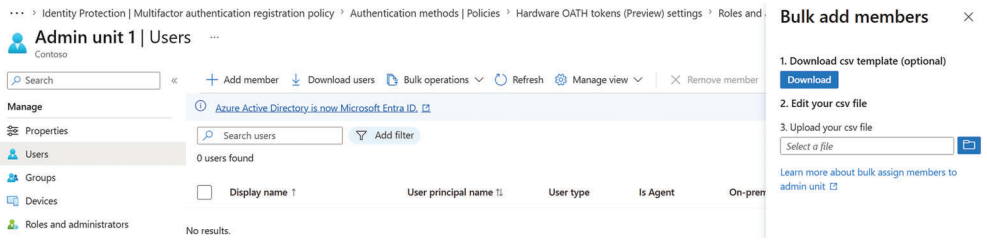


Figure 3.11: Adding users to an administrative unit

4. To add groups, click on **Groups** and in the right pane click on **Add** and pick the group from the list. You can also create a new group from within the admin unit by clicking **New group** as shown in the following screenshot. This will take you to the page to create a new group as shown in the following figure:

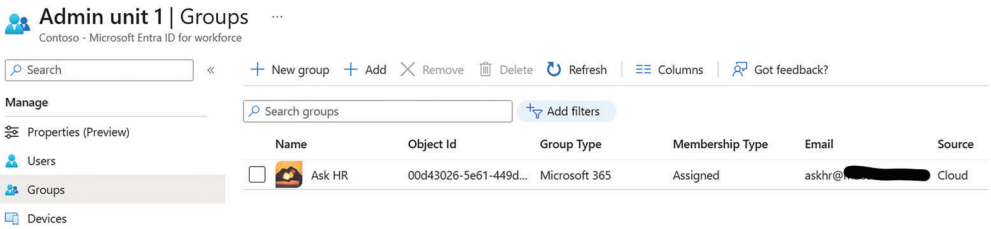


Figure 3.12: Adding groups to administrative units

Note

To create a new group from within the administrative unit, you should have the Global Administrator role assigned.

1. To add devices, click on **Devices** and in the right pane click on **Add device**. Pick the devices from the list.

Dynamically add members to an administrative unit

Adding individual members to administrative units can be quite cumbersome. When users move between departments or locations, the administrative unit membership will have to be manually updated. This can be quite a big administrative overhead. To make this simpler and automated, you can dynamically add members to an administrative unit using object attributes.

> **Note**
>
> To dynamically assign members to an administrative unit, a Microsoft Entra ID P1 license is required for each admin unit administrator and member.

Following are the steps to dynamically add members to an administrative unit:

1. Log in to `https://microsoft.entra.com` with an account that has the Privileged Role Administrator or Global Administrator role assigned.
2. Navigate to **Entra ID | Roles & admins | Admin Units**. In the right pane, select the newly created admin unit.
3. Click on **Properties** and change the **Membership type** to **Dynamic User** or **Dynamic Device** as shown in the following figure:

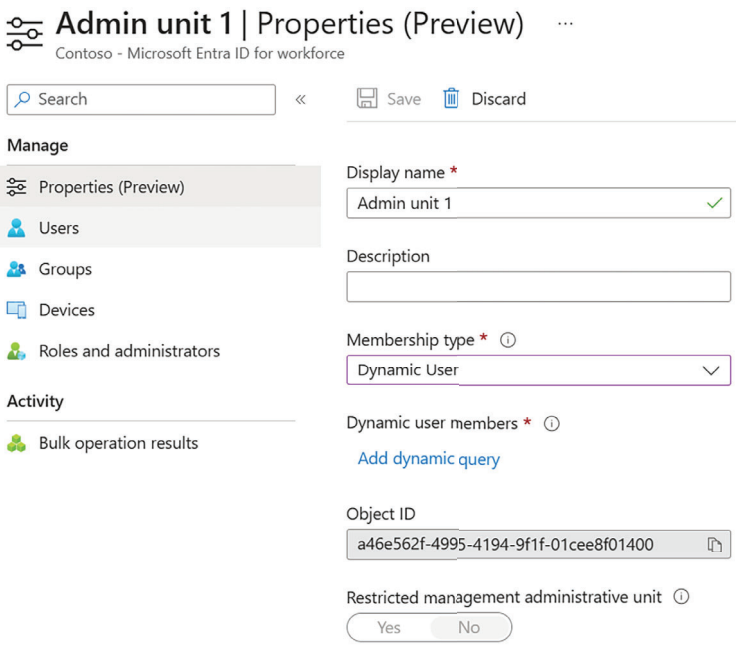


Figure 3.13: Change admin unit membership to Dynamic User

4. Click on **Add dynamic query**. In the next screen, select the **Property**, **Operator**, and type in the **Value**. You can build complex queries to meet your requirements. Once done, click on **Save** as shown in the following screenshot:

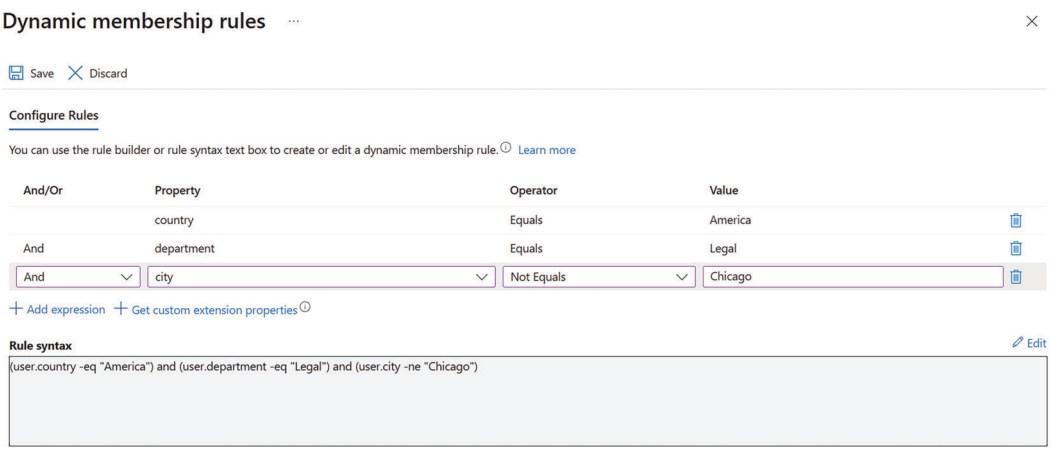


Figure 3.14: Dynamic membership rules in admin units

Assigning administrative roles to an administrative unit

Once you have created an administrative unit and added members to it, either manually or dynamically, the next step would be to determine which users, groups, or service principals can perform administrative actions on members of that administrative unit. This is done by assigning roles to that administrative unit scope. Members of that role will then have permissions only on the objects within the administrative unit scope and not on other objects in the tenant. For example, if the Helpdesk Administrator role is assigned to admin unit 1, members of the Helpdesk Administrator role group will be able to reset passwords for only users in admin unit 1 and not for other users in the tenant. Only the following Microsoft Entra roles can be assigned to an administrative unit scope:

- Authentication administrator
- Cloud device administrator
- Groups administrator
- Helpdesk administrator
- License administrator
- Password administrator
- Printer administrator
- SharePoint administrator
- Teams administrator
- Teams devices administrator
- User administrator

In addition, custom roles can also be assigned to an administrative scope if the custom role has permissions relevant to users, groups, or devices. The following permissions are restricted if the target of the operation is another administrator:

- Read or modify user authentication methods or reset passwords
- Modify user properties like phone numbers, alternate email addresses, or OAuth secret keys
- Delete or restore user accounts

The following security principals can be assigned a role at the administrative unit scope:

- Users
- Role-assignable groups
- Service principals

Service principals and guest user accounts do not receive directory read permissions by default so they cannot be assigned to an administrative unit scope unless they are also assigned permissions to read the objects that are members of the administrative unit.

Following are the steps to assign a role to an administrative unit:

1. Log in to `https://microsoft.entra.com` with an account that has the Privileged Role Administrator or Global Administrator role assigned.
2. Navigate to **Entra ID | Roles & admins | Admin Units**.
3. In the right pane, click the admin unit that was just created and click on **Roles and administrators**.
4. In the right pane, select the role that you would like to assign to this administrative unit as shown in the following figure:

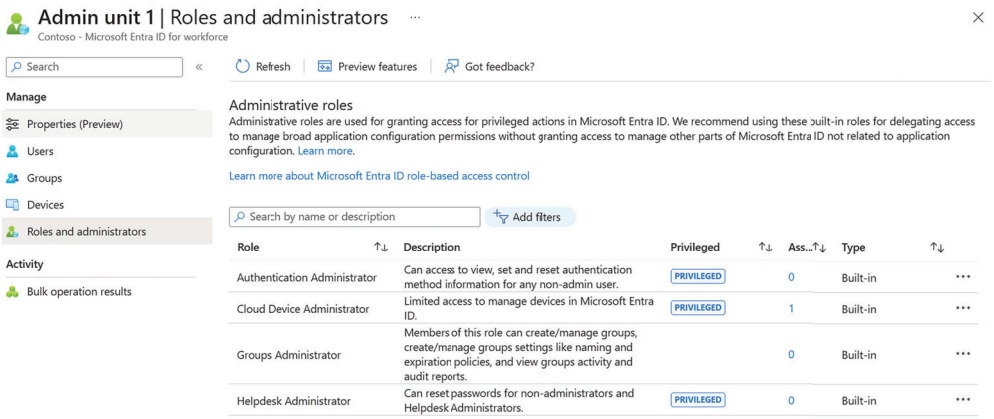


Figure 3.15: Adding roles to an administrative unit

5. Click on **Add assignments** as shown in the following figure:

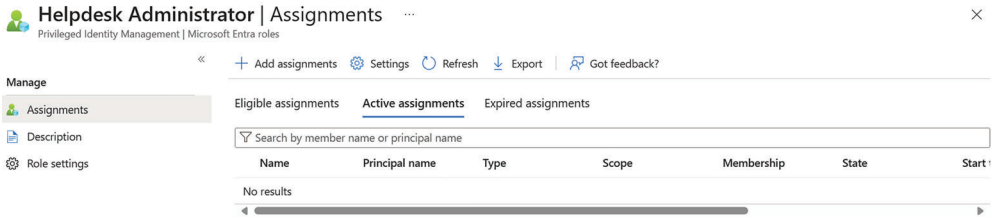


Figure 3.16: Adding role assignment

6. Under membership, click on **No member selected** and from the list pick the user, group, or service principal and click on **Select** as shown in the following figure:

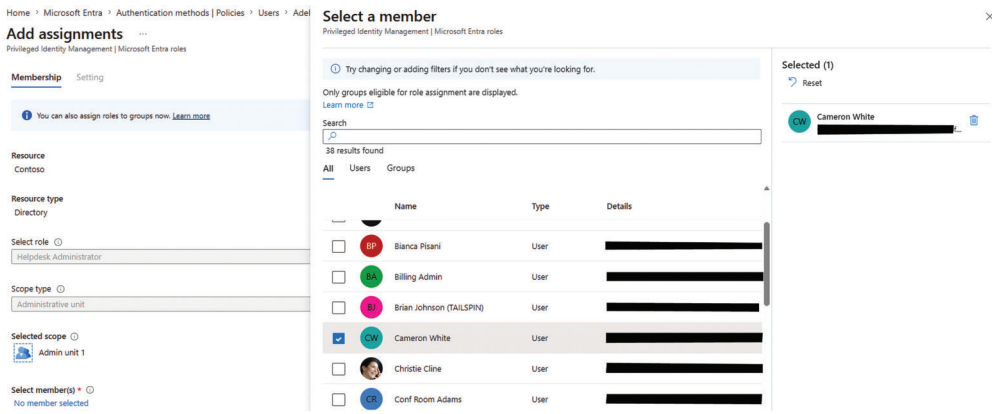


Figure 3.17: Select the security principal

7. Click **Next**. On the **Settings** page, make the appropriate selections and click **Assign** as shown in the following figure:

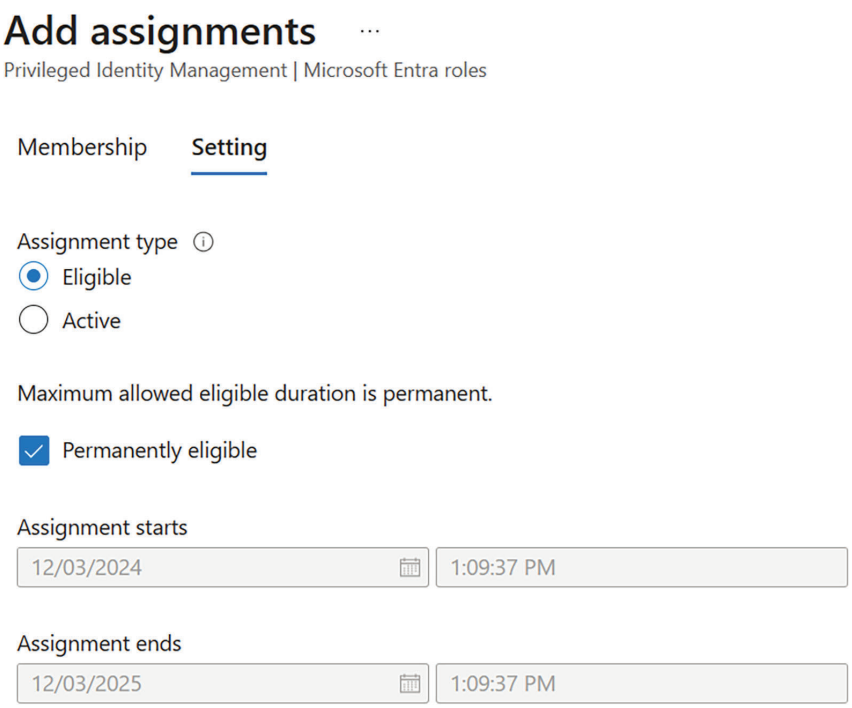


Figure 3.18: Select assignment type

End-user self-service

Microsoft Entra ID offers several end user self-service capabilities to ease the administrative overhead, empower the workforce, and reduce helpdesk calls. This section explores some of these self-service options. These options are available from the **My Account portal**.

The following features require that users be assigned a Microsoft Entra ID P1 license.

Self-service password reset

If a user account is locked or if they forget their password, they can unlock it or reset their own password without calling the helpdesk. This feature has added security as the user is resetting their own password, and the helpdesk does not have to verify the identity of the user calling for a password reset.

SSPR is a capability of Microsoft Entra ID that relies on the authentication methods explained in *Chapter 2, Fundamentals of Microsoft Entra ID*. Users must register at least one authentication method that is enabled for SSPR to enable them to reset their own passwords. Administrators must register two methods.

These following methods are enabled for SSPR:

- **Mobile application notification**: Users will receive a notification on the Microsoft Authenticator app on their mobile phones.
- **Mobile application code**: Users will receive a code on the Microsoft Authenticator app on their mobile and they will have to enter the same code on the self-service portal.
- **Email**: Users can configure an alternative email address to use during the verification process.
- **Mobile phone**: Users will receive a call or text on their configured mobile phone
- **Office phone**: Users will receive a call on their configured office phone.
- **Security questions**: Users can configure security questions and answers. They will be asked to answer one or more of the security questions during the verification process. Security questions will be retired in March 2027 and won't be available for SSPR. If your organization relies on security questions, it is recommended to move users to other methods.

Follow these steps to configure end user self-service password reset:

1. Log in into`https://entra.microsoft.com` as Authentication Policy Administrator.
2. In the left pane, click on **Entra ID** | **Password reset**.

3. Click on **Properties**, and in the right pane, select if you want to enable password reset for all users or selected users. If you choose selected users, you will be prompted to select the group for which you want to enable SSPR. Once done, click **Save**. Refer to *Figure 3.19*:

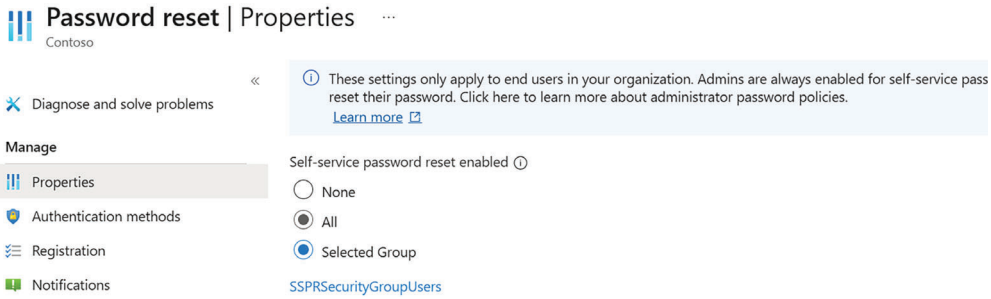


Figure 3.19: Configure SSPR group

4. Navigate to **Entra ID | Authentication methods**. In the right pane, enable one or more SSPR capable authentication methods listed above. This will enable users to register for these methods and be able to reset their passwords. Refer to *Figure 3.20*:

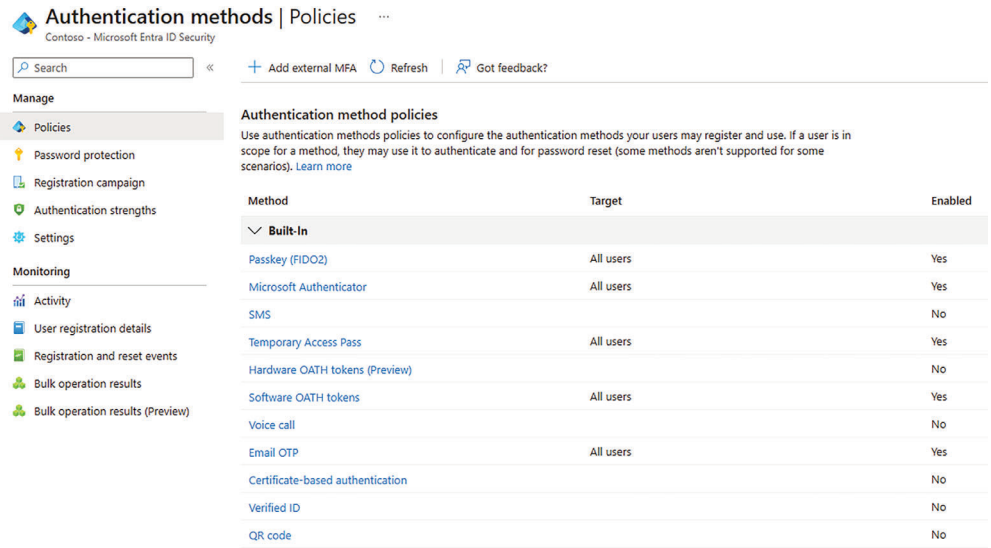


Figure 3.20: SSPR methods

Note

These settings only affect user accounts. Administrative user accounts are mandatorily enabled for self-service password reset and must use two authentication methods to successfully reset their passwords.

If an end user must reset their password, they should go to `https://aka.ms/sspr`. The first time, they will be prompted to set up the authentication methods you configured above.

Self-service group management

Using Microsoft Entra ID, you can enable users to create and manage their own Microsoft 365 or Security groups. This offloads a considerable amount of work from IT to the end users. The group owners are responsible for maintaining group membership. To set up self-service group management, follow these steps:

1. Log in to`https://entra.microsoft.com` as a Group Administrator.
2. In the left pane, click on **Entra ID** | **Groups**.
3. In the **General** page, make the following settings:
    a. **Owners can manage group membership requests in the Access Panel**: **Yes**
    b. **Restrict user ability to access group features in the Access Panel**: **No**

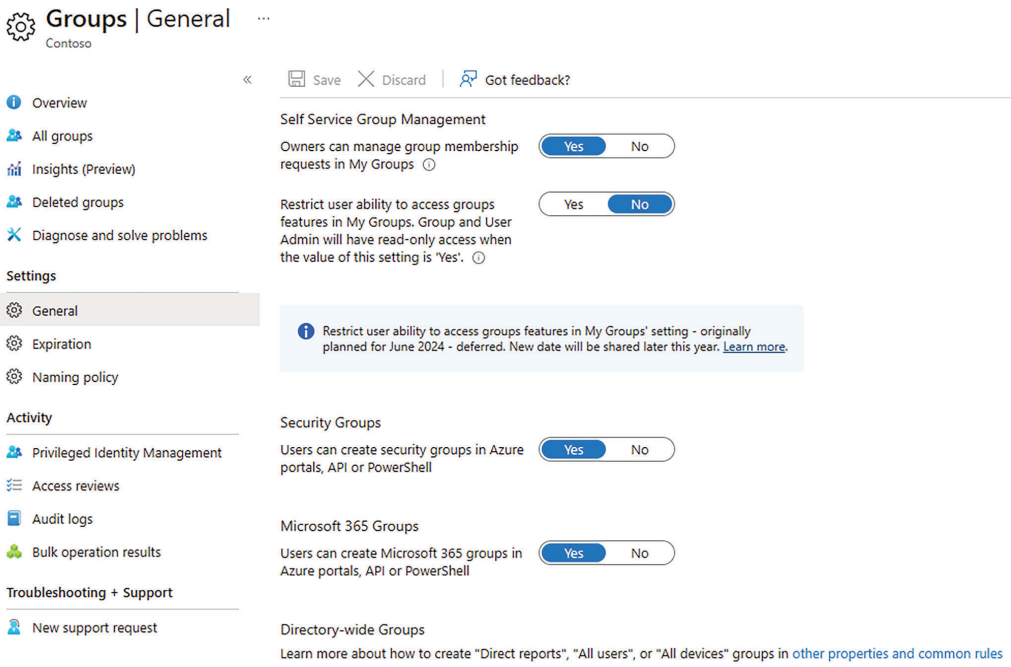


Figure 3.21: Self-service group management settings

4. Click **Save**.

Tip

End users can create and manage groups from the **My Groups** access panel in **My Account** portal. Go to `https://myaccount.microsoft.com`, select **My Groups** from the left pane.

Self-service application assignment

Microsoft Entra allows users to discover applications from the MyApps portal. With this feature, admins can:

- Add users to preconfigured groups that have access to applications
- Allow up to 10 business users to approve or deny application requests
- Allow business users to set application passwords that users can use to sign into applications
- Automatically assign applications to business users based on their role

> **Note**
>
> Single sign-on for the application should be enabled before self-service can be configured.

Follow the steps to enable self-service application assignment:

1. Log in to `https://entra.microsoft.com` as a Cloud Application Administrator.
2. Navigate to **Entra ID | Enterprise Applications | All applications**.
3. In the list of applications, find the application that you want to enable self-service for. Click on the application name. In the page that opens, click on **Self-service**.
4. In the right pane, switch the toggle next to **Allow users to request access to this application?** to **Yes**.
5. Click on **Select group**, next to **To which group should assigned users be added?**, select a group, and click **Select**. When a user request is approved, they are added to this group.
6. If business approval is required before user access is approved, select **Yes** next to **Require approval before granting access to this application?**
7. Click on **Select approvers**, next to **Who is allowed to approve access to this application?**, and select the user(s) who can approve access. Groups are not supported. Up to 10 users can be selected as approvers. If multiple approvers are selected, any one user can approve the request.

8. Choose the role to which these users should be assigned by clicking on **Select a role** next to **To which role should users be assigned in this application?**. This option is to assign users to a role within the application.
9. Click on **Save**. Refer to *Figure 3.22*:

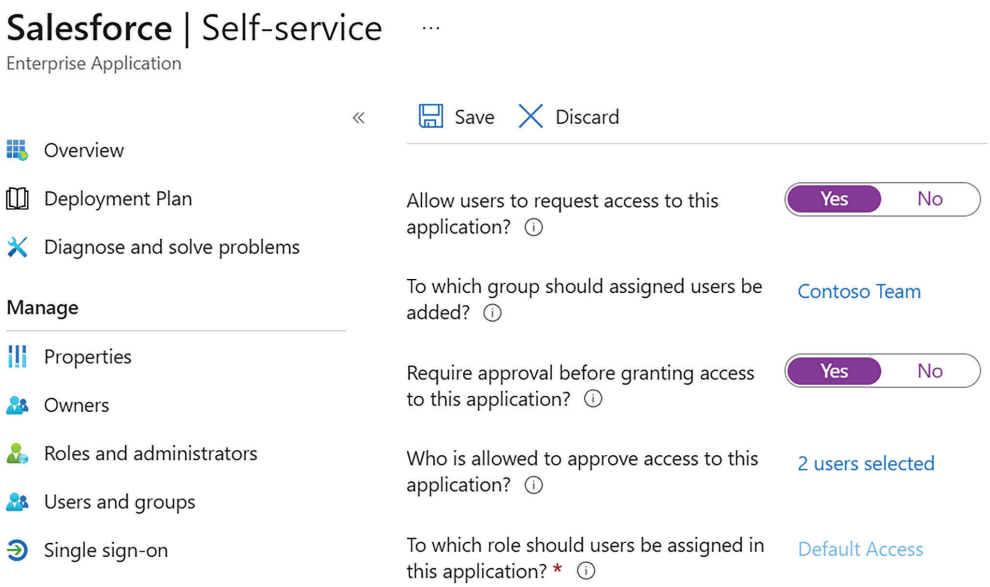


Figure 3.22: Application self-service options

In addition to the self-service options discussed above, the **My Account** portal offers other self-service options as well, such as:

- **My Sign-ins**: Users can access their own sign-in activity and report any malicious sign-ins to their organization.
- **My Access**: Employees and guests can request access to different application packages, which enable them to get access to applications and services.
- **Devices**: Users can view and manage the list of devices connected to their Microsoft Entra ID account.
- **Security info**: Users can update their verification methods.

Fundamental security settings

This section outlines some fundamental security settings that should be enabled in Microsoft Entra wherever licenses are available. These settings provide a strong foundation for other resources that build on top of Microsoft Entra.

- **Privileged access**:
  - Privileged accounts should be cloud-native
  - Privileged accounts should have phishing-resistant methods enabled
  - Enable just-in-time access for privileged accounts
  - Limit permissions to create new tenants to the Tenant Creator role
  - Global administrators should not have standing access to Azure subscriptions
  - Configure approval workflow and reporting for privileged role activation
  - Guest accounts should not be assigned privileged roles
  - Configure Conditional Access policies for Privileged Access Workstations
- **Credential management**:
  - Configure strong authentication methods for all users
  - Configure notifications for privileged accounts' password reset
  - Disable password expiration
- **Access control**:
  - Block legacy authentication
  - Restrict access for high-risk users
  - Require MFA for device join and device registration actions
  - Use password hash sync
  - Configure password protection
- **Application management**:
  - Inactive applications should not have high privileged Graph API permissions or built-in roles
  - Applications should not have client secrets configured
  - Application certificates should expire within 180 days
  - Rotate application certificates regularly
  - Restrict creation of new applications and service principals to privileged users

- **External collaboration**:
  - Guests should not be able to invite other guests
  - Guests should have restricted access
  - Guest accounts should be protected with strong authentication methods
  - Remove inactive guests from the tenant
  - Guests should have a sponsor
- **Monitoring**:
  - Configure diagnostic settings for Microsoft Entra logs
  - Triage all high-risk users and sign-ins
  - Address all high-priority Entra recommendations
  - Enable ID Protection notifications
- **Free security features**:
  - Enable security defaults if not using Conditional Access

Summary

In this chapter, we learned how to determine the appropriate identity model for your organization and how to implement it. This chapter explained how you can configure hybrid identity using Microsoft Entra Cloud Sync and Microsoft Entra Connect. It further explained the authentication methods available for hybrid identity and how to choose the appropriate method for your organization. Lastly this chapter covered Administrative Units, end user self-service options and some fundamental security settings recommended by Microsoft. With this chapter we have covered the fundamentals of Microsoft Entra ID. In the next chapter, we will learn about Microsoft Entra Domain Services.

Exercises

1. Your organization has been using on-premises Active Directory for the last 15 years. You decide to move to the cloud and choose Microsoft Entra ID as your identity provider. The organization wants to provide single sign-on for all applications. The on-premises Active Directory should remain authoritative for user authentication. You need to implement a solution with the least amount of administrative effort and infrastructure requirements. Which identity model is best suited?
   a. Cloud-only identity
   b. Hybrid identity with password hash synchronization

   c. Hybrid identity with pass-through authentication
   d. Hybrid identity with federation

2. Which of the following is possible only if Microsoft Entra Connect Sync is used?
   a. Connecting multiple on-premises AD forests to Microsoft Entra ID
   b. Support for federation
   c. Support for groups with up to 250,000 members
   d. Support for Seamless SSO
3. As an IT administrator you want to reduce the number of helpdesk calls by providing user self-service capabilities. What are some of the user self-service capabilities available with Microsoft Entra ID? Select all that apply.
   a. Users can be enabled to reset their own passwords
   b. Managers can be enabled to reset passwords for their team
   c. Users can be enabled to create and manage groups
   d. Managers can be enabled to create user accounts for their team

Answers

1. c
2. c
3. a, c

Additional resources

- Microsoft Entra Cloud Sync FAQ: `https://learn.microsoft.com/en-us/entra/identity/hybrid/cloud-sync/reference-cloud-sync-faq`
- Microsoft Entra Connect FAQ: `https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/reference-connect-faq`
- Microsoft Entra Connect Health FAQ: `https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/reference-connect-health-faq`

Get this book's PDF version and more

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.





Note: Keep your invoice handy. Purchases made directly from Packt don't require an invoice.

4

Microsoft Entra Domain Services

In the last few years, we have seen a major shift to cloud services. However, many organizations still have a significant portion of their infrastructure on premises. While Microsoft Entra provides identity and access management services in the cloud, some organizations still rely on Active Directory services like domain join, group policy, and **Lightweight Directory Access Protocol** (**LDAP**)/**Kerberos authentication**. **Microsoft Entra Domain Services** provides managed domain services in the cloud to organizations with such requirements. It enables organizations to use familiar Active Directory features without deploying, managing, or patching domain controllers. This is especially useful for scenarios where an organization wants to reduce its on-premises footprint, but a hybrid identity solution is necessary to support both on-premises and cloud resources. Using this solution, organizations can migrate legacy, directory-dependent applications to the cloud with minimal redevelopment. This chapter will cover:

- Introduction to Microsoft Entra Domain Services
- Common deployment scenarios
- Deploying Microsoft Entra Domain Services
- Administering Microsoft Entra Domain Services
- Securing Microsoft Entra Domain Services

Cloud-based directory services

As organizations increasingly transition their workloads to the cloud, the need for legacy support remains, particularly for applications and resources that depend on directory services like domain join, LDAP, Kerberos authentication, and group policy. Microsoft offers two ways that provide traditional **Active Directory Domain Services** (**AD DS**) in the cloud.

Self-managed domain

A **self-managed domain** can be created using resources like **Virtual Machines (VMs)**, Windows Server, and AD DS. This is like installing and maintaining a traditional AD DS environment in the cloud. Instead of physical servers, it is installed on VMs in the cloud. The organization is responsible for managing, patching, and securing the **Domain Controllers (DCs)** and related infrastructure. Common deployment models for using a self-managed AD DS environment include:

- **Standalone cloud-only AD DS**: This is a completely independent AD DS environment and does not integrate with an on-premises AD DS environment. This is useful for organizations that would like to lift and shift their on-premises AD DS infrastructure to the cloud.
- **Extend on-premises domain to Azure**: In this approach, the on-premises **Active Directory Domain Services** (**AD DS**) domain is extended into Azure by establishing connectivity between an Azure virtual network and the on-premises network through either a VPN or an ExpressRoute connection. Azure virtual machines are then joined to this virtual network, enabling them to participate in and authenticate against the on-premises AD DS environment. Azure VMs can also be promoted as additional DCs that replicate over the VPN or ExpressRoute connection.

While this may be a quick and viable option for some organizations, they still retain the overhead and management of the servers running the domain controllers. A managed domain solves this problem as explained in the next section.

Overview of Microsoft Entra Domain Services

Microsoft Entra Domain Services offers a seamless way to extend Active Directory capabilities to the cloud without the operational overhead of deploying, managing, or patching VMs. By integrating with Microsoft Entra ID, it enables organizations to create a hybrid identity infrastructure that supports both legacy and cloud-native applications, fostering modernization and flexibility. Domain Services offers a smaller subset of features as compared to self-managed domain, thereby reducing complexity. For example, there are no AD forests, domain sites, or replication links to manage.

With this managed service, businesses can migrate directory-dependent workloads to the cloud more efficiently, minimizing redevelopment and ensuring continuity for critical systems. Entra Domain Services also helps improve security posture by leveraging cloud-based updates and monitoring, reducing the risks associated with on-premises infrastructure. It is ideal for organizations looking to reduce their on-premises footprint while maintaining compatibility with established authentication and policy management tools. As enterprises embrace cloud-

first strategies, Microsoft Entra Domain Services plays a vital role in simplifying identity management and accelerating digital transformation.

A **Domain Services managed domain** lets organizations run legacy applications that cannot use modern authentication in the cloud. Using Domain Services managed domain, organizations can lift and shift these legacy applications to the cloud without having to manage an extensive Active Directory environment in the cloud.

The following table provides a comparison between a self-managed and a managed domain:

Feature	**Managed domain**	**Self-managed**
Managed service	Yes	No
Secure deployments	Yes	Administrator must secure deployment
DNS server	Managed service	Yes
Domain admin privileges	No	Yes
Domain join	Yes	Yes
NTLM/Kerberos	Yes	Yes
Kerberos constrained delegation	Resource-based	Resource and account-based
Custom OU structure	Yes	Yes
Group Policy	Yes	Yes
Schema extensions	No	Yes
AD domain/forest trusts	Requires Enterprise SKU or higher	Yes
Secure LDAP	Yes	Yes
LDAP read	Yes	Yes
LDAP write	Only within the managed domain	Yes

Feature	Managed domain	Self-managed
Geo-distributed deployment	Yes	Yes

Table 4.1: Managed domain and self-managed AD DS feature comparison

This chapter will focus on Microsoft Entra Domain Services managed domain. Let's dive deeper.

Microsoft Entra Domain Services managed domain

When existing workloads are migrated to the cloud, directory-dependent applications use LDAP for read and write access to AD DS directory. Applications that run on Windows Server are normally deployed on domain joined VMs so that they can be joined to the AD DS domain and managed using Group Policy. To authenticate users, these applications use Kerberos or **NT LAN Manager (NTLM)** authentication.

Organizations use one of the following ways to migrate such workloads to the cloud:

- Configure a site-to-site **Virtual Private Network (VPN)** connection between Azure workloads and on-premises AD DS environments to enable on-premises DCs to provide authentication services via VPN.
- Create replica DCs in Azure VMs to extend the on-premises domain to the cloud. Authentication is provided by these DCs. They replicate directory information from the on-premises DCs.
- Deploy a stand-alone AD DS environment in Azure using DCs that run on Azure VMs. This is a completely separate AD DS environment and information is not replicated from on-premises AD DS.

In all these approaches, VPN connections become a bottleneck which are vulnerable to network glitches and outages. Domain Services provides an alternative approach to reduce complexity and increase reliability to create an integrated identity solution for both hybrid and cloud-only environments.

The following deployment scenarios are supported:

- **Microsoft Entra Domain Services for hybrid organizations**: Organizations that run a hybrid infrastructure where the on-premises AD DS environment is synchronized with Microsoft Entra ID using Microsoft Entra Connect.
- **Microsoft Entra Domain Services for cloud-only organizations**: Organizations that don't have an on-premises AD DS environment and whose identities are completely managed in the cloud.

To get started, organizations must first create a Domain Services managed domain by defining a unique namespace, which serves as the domain name, such as `mydomainservices.com`.

Basic concepts

Before we proceed with creating a managed domain, let's understand some important concepts as there are some differences in how Domain Services behaves in comparison to an on-premises AD DS environment.

Replica sets

When a managed domain is provisioned, Azure automatically deploys two Windows DCs within the selected Azure region. This deployment, referred to as a replica set, provides redundancy and high availability for the managed domain. A key advantage of using a managed domain is that organizations are relieved of the responsibility for maintaining these domain controllers, as Azure fully manages them as part of the service. This management includes built-in features such as automated backups and encryption of data at rest, ensuring both operational resilience and security compliance.

Managed domains can be expanded to include more than one replica set per Microsoft Entra tenant. Replica sets can be added to any peered virtual network in any Azure region. This provides geographical disaster recovery in case an Azure region becomes unavailable. All replica sets share the same namespace and configuration and contain the same data. Any changes, such as configuration, user identity, groups, or Group Policy objects are applied to all replica sets using AD DS replication.

Each replica set is created in a virtual network that must be peered with every other virtual network containing a replica set. A single virtual network can host multiple replica sets if each one resides in a different subnet. You can create up to five replica sets per managed domain.

Forests and trusts

Forest is a logical unit in Active Directory that can contain one or more **domains**. User objects, groups, and devices are stored in domains. Domains also provide authentication services. In Domain Services, a forest can contain only one domain.

A forest **trust** can be created with another domain to allow users access to resources. Depending on requirements, the following types of trusts can be created:

- **Two-way**: Users in both domains can access each other's resources.

- **One-way outgoing**: Users in the on-premises domain access resources in the managed domain but users in the managed domain cannot access resources in the on-premises domain.
- **One-way incoming**: Users in the managed domain can access resources in the on-premises domain but users in the on-premises domain cannot access resources in the managed domain.

Synchronization

An automatic one-way synchronization is configured from Microsoft Entra ID to a managed domain. This means that resources created in Microsoft Entra ID are synchronized to the managed domain, but the resources created in the managed domain are not synchronized to Microsoft Entra ID. Applications and services in the Azure environment connected to the managed domain can take advantage of features like domain join, group policy, LDAP, and Kerberos.

If organizations have a hybrid environment with on-premises AD that is connected to Microsoft Entra ID using Microsoft Entra Connect, resources from on-premises AD are synchronized to Microsoft Entra ID and from there they are automatically synchronized to the managed domain. The following figure shows this:

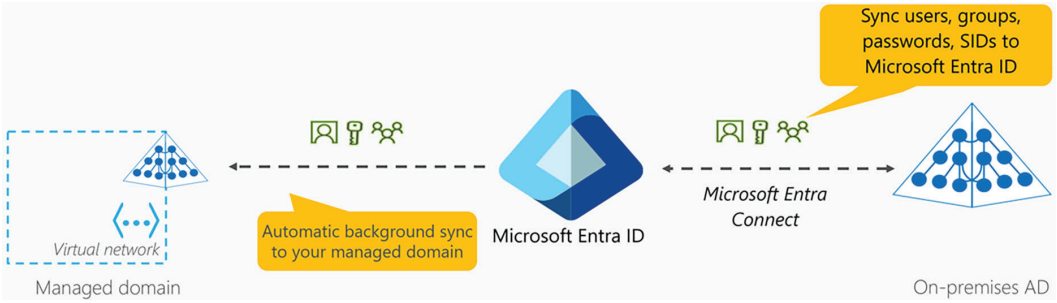


Figure 4.1: Replication in a hybrid environment

The initial synchronization may take a few days to complete depending on the number of objects to be synchronized. After the initial synchronization is complete, changes made in Microsoft Entra ID are automatically synchronized to Domain Services.

It is possible to scope user synchronization to only the users that originated in the cloud. This way users from the on-premises AD DS environment will not be synchronized to the managed domain.

Domain management

A managed domain is a DNS namespace and directory. The DCs that contain all resources like users and groups are part of the managed service and users cannot sign in to these DCs. A VM

is created that is joined to the managed domain. All domain management tools such as AD Administrative Center, Group Policy objects, and DNS snap-ins are installed on this VM and used to perform all administrative tasks. A managed domain is largely read-only. Administrators can create custom **Organizational Units (OUs)** with the managed domain but cannot make changes to user attributes, passwords, or group memberships.

While creating a managed domain, you will be asked to specify a **DNS domain name**. There are some considerations when choosing a domain name as described below:

- **Built-in domain name**: By default, the managed domain is assigned a name with the `.onmicrosoft.com` suffix. This default naming convention is not recommended when planning to use secure LDAP for internet-based access to the managed domain. Because Microsoft retains ownership of the `.onmicrosoft.com` namespace, organizations cannot obtain a publicly trusted digital certificate for this domain. As a result, **Certificate Authorities (CAs)** will not issue a certificate to secure LDAP connections using the default domain name.
- **Custom domain names**: It is recommended to use a custom domain that the organization owns and is routable.
- **Non-routable domain suffixes**: It is not recommended to use a non-routable domain name such as `litware.local`. Because these domains are not routable, they can cause issues with DNS resolution.

The following DNS name restrictions apply:

- Managed domain names cannot contain a prefix that is longer than 15 characters.
- The name should be unique in your virtual network. The following scenarios could cause a conflict:
    - If you have an AD domain with the same DNS domain name on the Azure virtual network.
    - If the virtual network on which you plan to enable the managed domain is connected to your on-premises AD domain via VPN, make sure that the on-premises network does not have a domain with the same DNS domain name.
    - If you have an existing Azure cloud service with the same name on the virtual network.

Consider all the above points to accurately create your domain before synchronizing users from Active Directory.

User account creation

User accounts are synchronized from the connected Microsoft Entra ID tenant which can also include accounts synchronized from any on-premises AD DS environment. Users can also be created directly in the managed domain. However, these users will not be synchronized back to Microsoft Entra ID.

Password policy

Domain Services has its own default password policy that includes settings for account lockout, maximum password age, and password complexity. Policies are distributed through group association.

Account lockout policy applies to all users in the managed domain regardless of how they were created. The following settings apply:

- Account lockout duration: 30 minutes
- Number of failed logon attempts allowed: 5
- Reset failed login attempts count after: 2 minutes
- Maximum password age: 90 days

Account lockouts only occur within the managed domain and only due to failed sign-in attempts against resources within the managed domain. Users who are synchronized from Microsoft Entra ID are not locked out in their source directory.

Other policies like password length and password complexity apply only to the users created directly in the managed domain. The following settings apply:

- Minimum password length: 7 characters
- Passwords must meet complexity requirements

The account lockout or password settings in the default policy cannot be modified. Administrators can create their own custom password policies and configure them to override the default password policy. The custom policies can be scoped to user groups.

Licensing

The performance and features are based on the type of license model selected. When you first create a managed domain, you can start with any of the models. As business requirements change, you can easily switch to an alternate licensing model. The following table summarizes the types of licenses with their capabilities:

Capability	Standard	Enterprise	Premium
Suggested Auth Load (peak, per hour)	0-3000	3000-10000	10000-70000
Suggested object count	0-25000	25000-100000	100000-500000
Backup frequency	Every 5 days	Every 3 Days	Daily
Additional replica sets	No	Yes	Yes
Extra sync options	No	Yes	Yes
Trusts	No	Yes	Yes

Table 4.2: Licensing for Domain Services

Keep the following considerations in mind while deciding on the appropriate licensing model for your organization:

- There is no limit on the number of objects that can be created in any of the licensing models. The object count in the table above is given as guidance; it is not a hard limit.
- Domain performance depends on how authentication is implemented. Compute resources available to the managed domain increase as you go from Standard to Premium. The transactions in the above table are a guideline and not an SLA.
- Daily backups are retained for 7 days with every third backup retained for 30 days.

Now that we understand the key concepts and licensing, we can proceed with creating a managed domain.

Creating a managed domain

Now that you understand the basic concepts, let's get started with creating a managed domain. The first step is to ensure that the following prerequisites have been met:

- An Azure subscription with a Microsoft Entra tenant associated.
- An account with the **Application Administrator** and **Group Administrator** Microsoft Entra role assigned.
- An account with the **Domain Services Contributor** Azure role assigned.
- A virtual network with DNS servers that can perform general internet queries.

Following are the steps to create a managed domain:

1. Sign in to `https://entra.microsoft.com` and navigate to **Entra ID | Domain services**.
2. Click on **Create Microsoft Entra Domain Services**.
3. Select the Azure subscription in which you would like to create the managed domain.
4. Choose an existing resource group or create a new one.
5. Specify a **DNS Domain Name**, **Region** and licensing model (**SKU**). Click **Next**.
6. On the **Networking** page, specify the **Virtual network** and **Subnet**. You can choose from existing ones or let the wizard create new ones. Click **Next**.
7. On the Administration page, a new group called AAD DC Administrators is created. The members of this group can manage Domain Services. Click on **Manage group membership** to add members to the group. Select who gets notified if any warning or critical alert is generated. Refer to the following figure. Click **Next**.

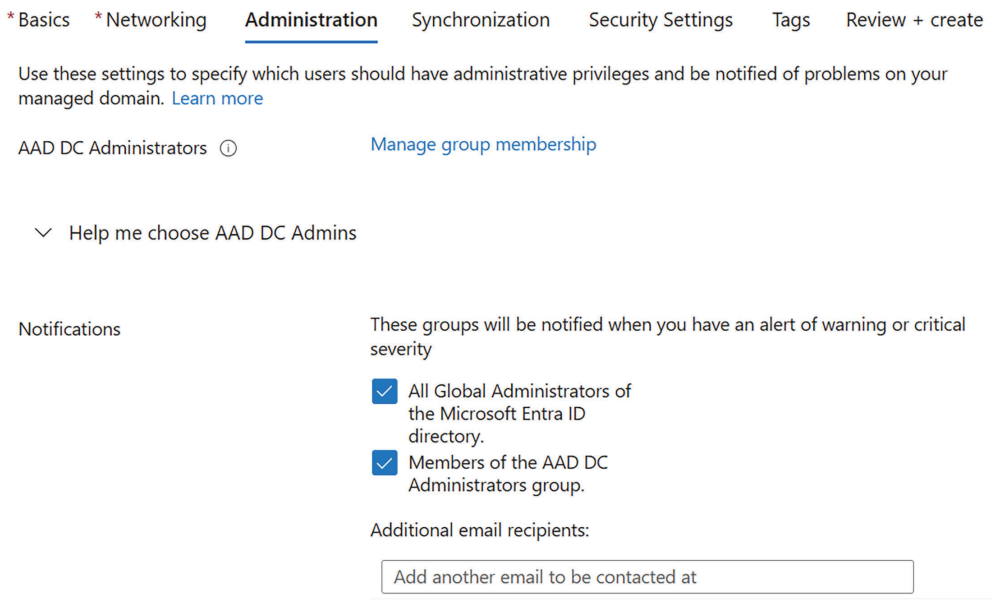


Figure 4.2: Administration settings

8. On the **Synchronization** page, select if you want to synchronize all users or cloud-only users. If you would like to synchronize only select groups, check the **Filter by group entitlements** box and then click **Select groups** to choose the groups. Click **Next**.

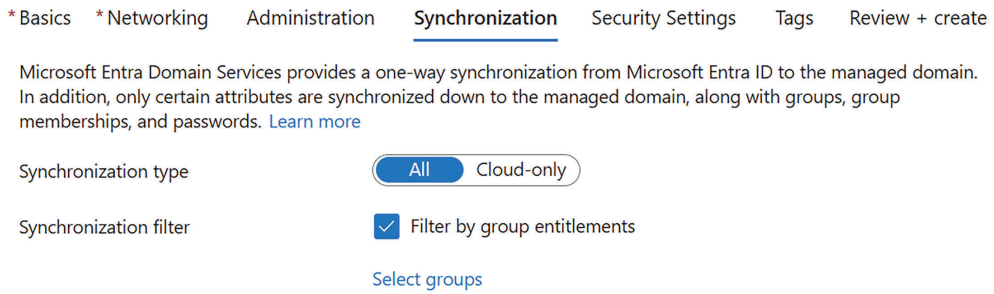


Figure 4.3: Synchronization settings

9. Accept the defaults on the **Security Settings** page. These settings can be changed later. Click **Review + create**. Click **Create**. In the box that pops up, click **OK** to create the managed domain.

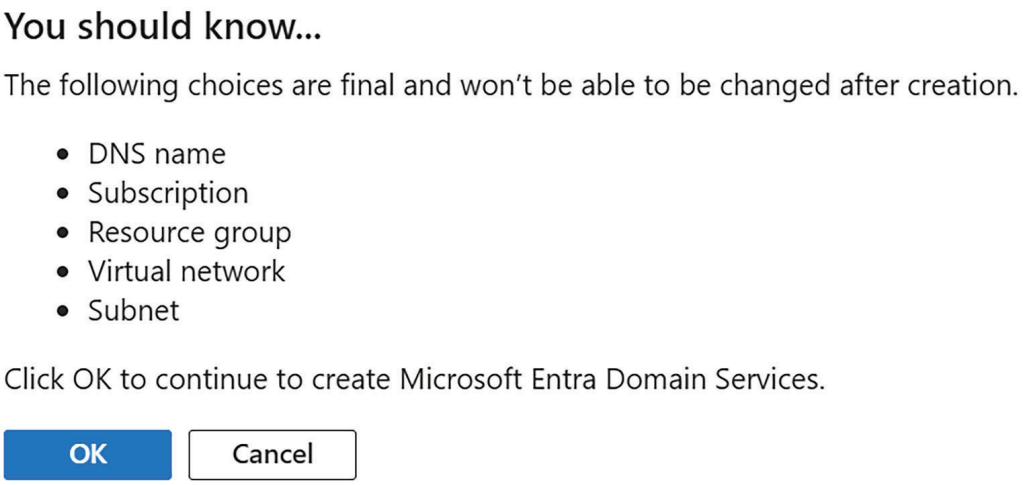


Figure 4.4: Create the managed domain

It can take up to an hour to provision the managed domain. Once provisioning is complete, the **Overview** tab shows the domain status as *Running*.

Enabling applications to use the managed domain

After Domain Services is deployed, the associated Azure virtual network must be configured to enable connected services to access the managed domain. This configuration is achieved by updating the virtual network's DNS settings to reference the two IP addresses assigned to the managed domain deployment. Follow the steps below:

1. On the **Overview** tab for the managed domain, click on the banner to run configuration diagnostics.
2. On the next page, click on **Run**. Wait for the diagnostics to complete running and expand **DNS records**. Click **Fix**. A screen will pop up displaying further information. Click **Fix** to update the DNS settings.

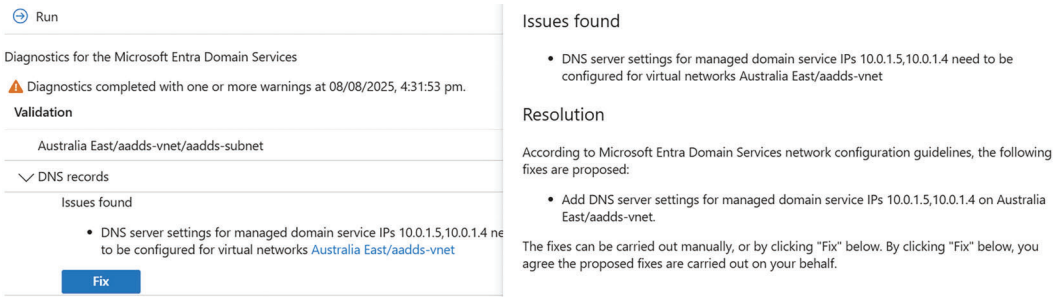


Figure 4.5: Update DNS settings

Now let's learn how to enable user accounts.

Enabling user accounts for Domain Services

Domain Services needs password hashes in a format that is suitable for NTLM and Kerberos authentication. Microsoft Entra ID does not generate or store password hashes in this format until Domain Services is enabled in the tenant. Cloud-only users must change their passwords before they can sign in to a managed domain. The password change generates the password hashes for Kerberos and NTLM authentication and stores them in Microsoft Entra ID. User accounts are not synchronized to Domain Services until the password is changed. For users that are synchronized to Microsoft Entra ID from on-premises AD DS environments, synchronization of password hashes must be enabled in Microsoft Entra Connect settings.

Once configured, the password hashes are stored within the managed domain. If the managed domain is deleted, all associated password hashes are permanently removed. Credential information synchronized in Entra ID cannot be reused when provisioning another managed domain. Microsoft Entra ID must generate and store fresh password hashes in the newly created managed domain.

Configuring virtual networking for managed domains

The virtual network subnet in which the managed domain is deployed should not be used for any other purpose. VMs and applications that rely on the managed domain should be deployed in separate virtual subnets or in a virtual network that is peered to the Domain Services virtual network. The network connectivity between the VMs and the managed domain can be provided in two ways as described below.

Virtual network subnet in the same virtual network

Create a virtual network subnet in the managed domain's virtual network. The VMs will be deployed in this virtual network subnet. Because the VMs reside within the same virtual network, they can automatically perform name resolution and establish communication with the Domain Services DCs.

Follow the steps below to create a virtual network subnet:

1. Sign in to `https://entra.microsoft.com` and navigate to **Entra ID | Domain services**.
2. In the right pane click the resource group name.
3. From the list of resources choose the default virtual network like `aadds-vnet`.
4. Click on **Address space in the left hand menu**. By default, the virtual network is provisioned with a single address space that is associated with the default subnet. To expand the configuration, add additional IP address ranges to the virtual network as shown in the following figure. Click **Save**.

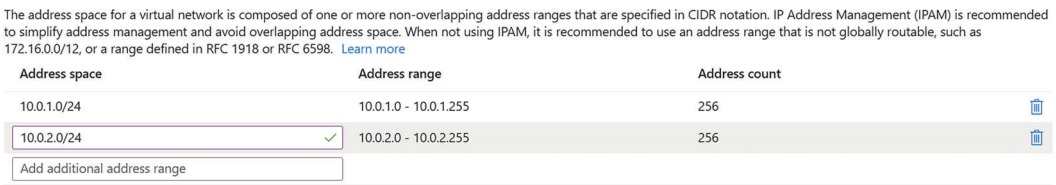


Figure 4.6: Add address ranges

5. In the left pane click on **Subnets** and in the right pane click on **Subnet** to add a subnet.
6. Enter a name for the subnet. Ensure that the newly created address space is selected under **IPv4 address range** and click **Add** to add the subnet.

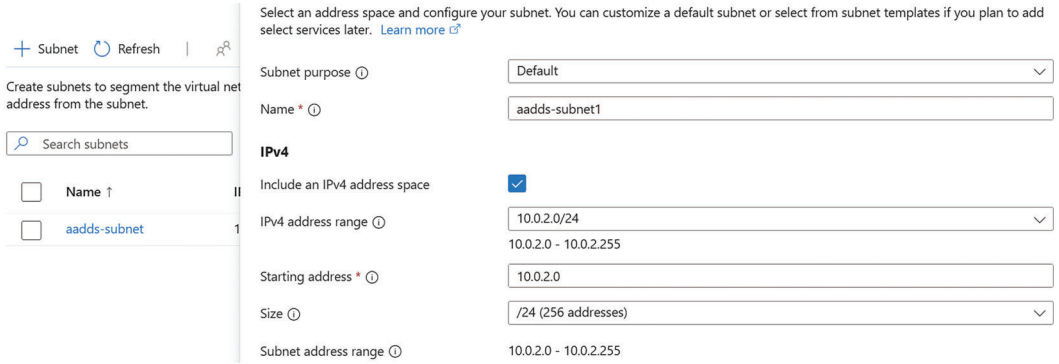


Figure 4.7: Add virtual network subnet

Now when you create VMs that need to use the managed domain, select this virtual network subnet.

Virtual network subnet in a separate Azure virtual network

Organizations can choose to create a separate Azure virtual network and deploy the VMs in it. If you choose this option, you will have to configure Azure virtual network peering between this network and the managed domain's virtual network. While configuring peering, configure the DNS settings to use name resolution back to the Domain Services DCs.

Following are the steps to configure virtual network peering to enable communication between the two subnets:

1. Sign in to `https://entra.microsoft.com` and navigate to **Entra ID | Domain services**.
2. In the right pane click on the resource group name.
3. From the list of resources choose the default virtual network such as `aadds-vnet`.
4. In the left pane, click on **Peerings** and in the right pane click on **Add**.
5. Enter a name for the peering link under **Remote virtual network summary**. Select **Virtual network** as the **Virtual network deployment model**.
6. Select the **Subscription** and the **Virtual network** with which you want to peer.
7. Peering is created in both directions so enter a name for the peering link name under the **Local virtual network summary**. Click **Add** to create the peering.

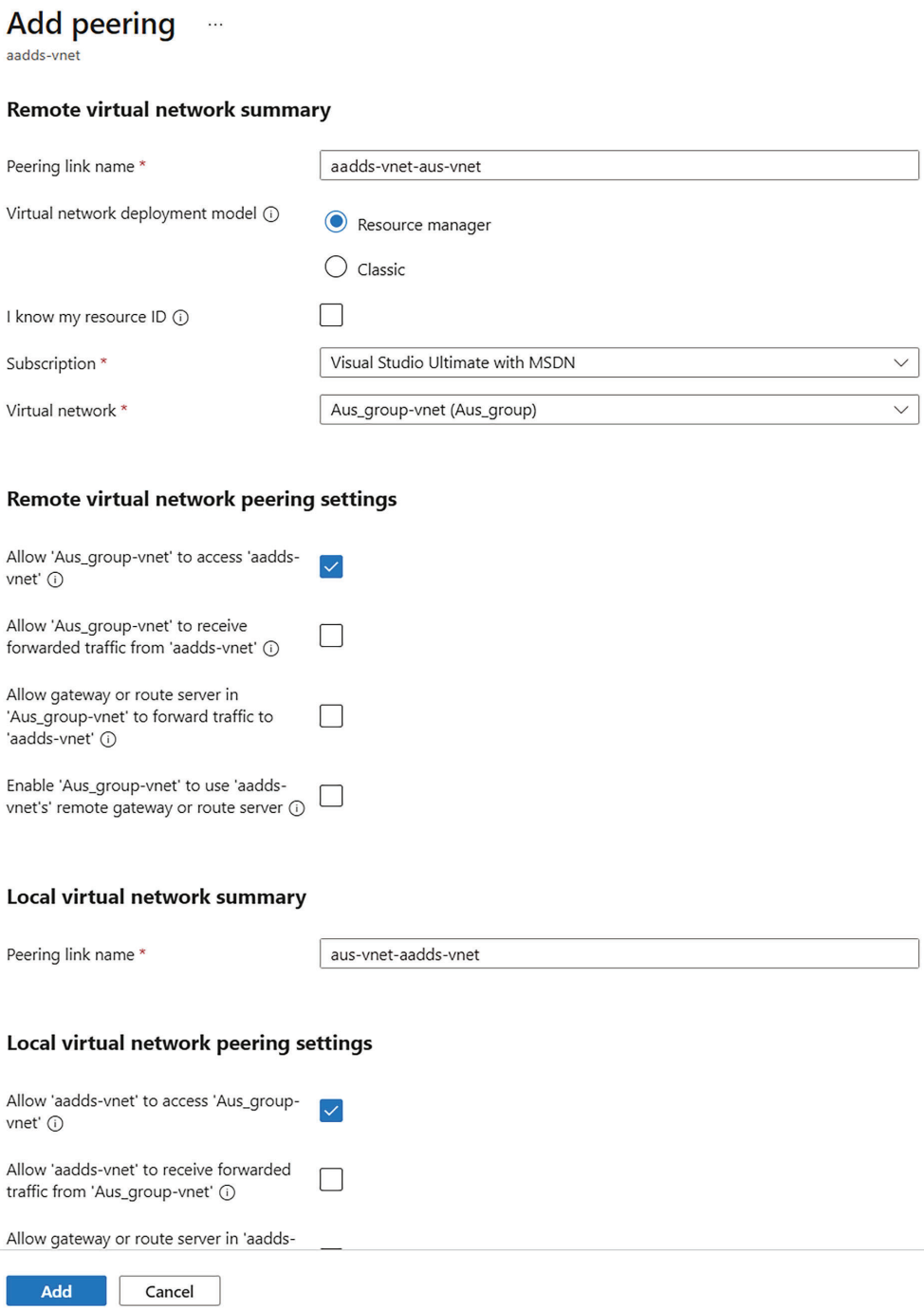

Add peering
aadds-vnet
Remote virtual network summary
Peering link name *
aadds-vnet-aus-vnet
Virtual network deployment model
Resource manager
Classic
I know my resource ID
Subscription *
Visual Studio Ultimate with MSDN
Virtual network *
Aus_group-vnet (Aus_group)
Remote virtual network peering settings
Allow 'Aus_group-vnet' to access 'aadds-vnet'
Allow 'Aus_group-vnet' to receive forwarded traffic from 'aadds-vnet'
Allow gateway or route server in 'Aus_group-vnet' to forward traffic to 'aadds-vnet'
Enable 'Aus_group-vnet' to use 'aadds-vnet's' remote gateway or route server
Local virtual network summary
Peering link name *
aus-vnet-aadds-vnet
Local virtual network peering settings
Allow 'aadds-vnet' to access 'Aus_group-vnet'
Allow 'aadds-vnet' to receive forwarded traffic from 'Aus_group-vnet'
Allow gateway or route server in 'aadds-
Add
Cancel

Figure 4.8: Configure virtual network peering

8. Once the peering is configured, the Peering state will show **Connected** as shown in the following figure:

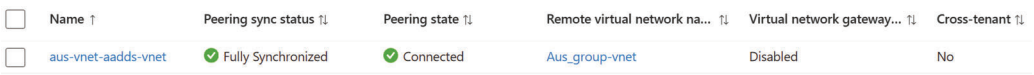


Figure 4.9: Virtual network peering

For VMs in the peered virtual network to successfully communicate with the managed domain, the IP addresses of the Domain Services DCs must be specified as the DNS servers for that peered virtual network. Follow the steps below:

1. Sign in to `https://entra.microsoft.com` and navigate to **Entra ID | Domain services**.
2. In the right pane, click on the resource group name.
3. From the list of resources, choose the peered virtual network.
4. In the left pane, click on **DNS servers**.
5. By default, a virtual network uses built-in Azure-provided DNS servers. Choose **Custom** and enter the IP address for the Domain Services domain controllers. Click **Save**.
6. To apply the updated DNS settings to the VMs, restart the VMs connected to the peered virtual network.

Once the virtual network is correctly configured, proceed with creating the replica set.

Creating a replica set

As explained earlier, when you configure Domain Services, a single replica set gets created. To provide geographical disaster recovery, additional replica sets can be added by following the steps below:

1. Sign in to `https://entra.microsoft.com` and navigate to **Entra ID | Domain services**.
2. In the right pane, click on the managed domain name.
3. On the left-hand side, click on **Replica sets**, and on the right pane, click on **Add**.
4. In the Add a replica set window, select the **Region** and a **Virtual network** and **Subnet** in the destination region. Click **Save** to create the replica set as shown in the following picture:

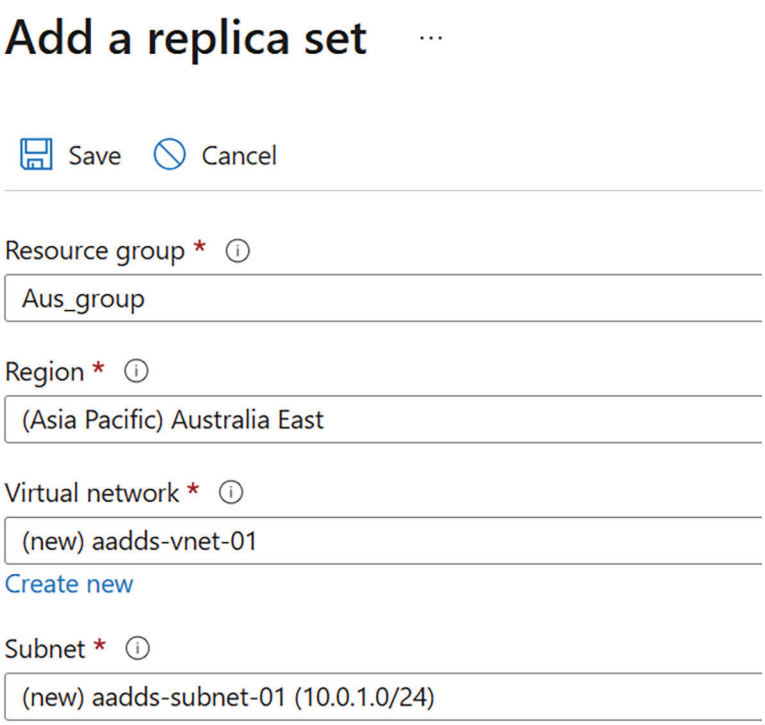


Figure 4.10: Add a replica set

5. The replica set status will show as **Provisioning** while deployment is in progress. Once complete, it will show **Running** as shown in the following picture:

Region	Virtual network/Subnet	IP addresses	Status	
Australia East	aadds-vnet/aadds-vnet/aadds-subnet	10.0.0.4,10.0.0.5	Running	•••
Australia East	aadds-vnet-01/aadds-vnet-01/aadds-subnet-01		Running	•••

Figure 4.11: Additional replica sets

Replica sets provide high availability and load distribution, so it is advisable to spend some time planning them appropriately.

Creating a forest trust

A trust relationship can be created between a managed domain and an on-premises AD DS environment. This trust enables users, applications, and devices from a managed domain to authenticate against an on-premises domain and vice versa. A forest trust helps users access resources in environments where password hashes cannot be synchronized or in passwordless scenarios such as smart cards. It also enables access in hybrid environments that require access to on-premises environments.

To enable forest trust, the following prerequisites must be met:

- An active Azure subscription with a Microsoft Entra tenant associated. The Entra tenant could be cloud-only or synchronized with an on-premises domain.
- A Domain Services managed domain configured with a custom DNS and a valid SSL certificate.
- An on-premises domain that is reachable either via ExpressRoute or VPN connectivity. The network must meet the following requirements:
    - Any firewall ports and DCs must allow traffic that is necessary to create a trust. All DCs that need to have a trust with the managed domain must have these ports open.
    - Use static private IP addresses.
    - Avoid overlapping IP address spaces to ensure successful communication between Azure and on-premises.
    - Domain Services must have its own subnet.
    - Peered virtual networks should not be transitive.
    - Ensure continuous connectivity and DNS name resolution between Azure and on-premises.
- An account with **Application Administrator** and **Groups Administrator** role assigned.
- A **Domain Administrator** account for the on-premises domain.

Creating a trust between domain services and on-premises requires three steps:

1. **Configure DNS in the on-premises domain**: To resolve the managed domain from the on-premises environment, forwarders may need to be added to the existing DNS servers.
2. **Create a two-way trust in the on-premises domain**: A two-way trust on the on-premises domain must be manually created.

> **Note**
>
> The above steps are completed in the on-premises AD environment. Detailed steps are beyond the scope of this book: `https://learn.microsoft.com/en-us/entra/identity/domain-services/tutorial-create-forest-trust`

3. **Create a two-way trust in the managed domain**: The following are the steps to create a two-way trust in the managed domain:
    a. Sign in to `https://entra.microsoft.com` and navigate to **Entra ID | Domain services**.
    b. In the right pane, click on the managed domain name.
    c. In the left pane, click on **Trusts** and then click **Add**.
    d. Enter a **Display name** for the trust.
    e. Under **Trusted domain DNS name**, enter the name of the on-premises AD DS domain.
    f. Select the **Trust direction** as **Two-way**.
    g. Provide and confirm a **Trust password**. This is the same password that is used to configure the two-way trust for the on-premises domain.
    h. Provide at least two DNS servers for the on-premises domain.
    i. Once done, click **Save**. Refer to the following figure:

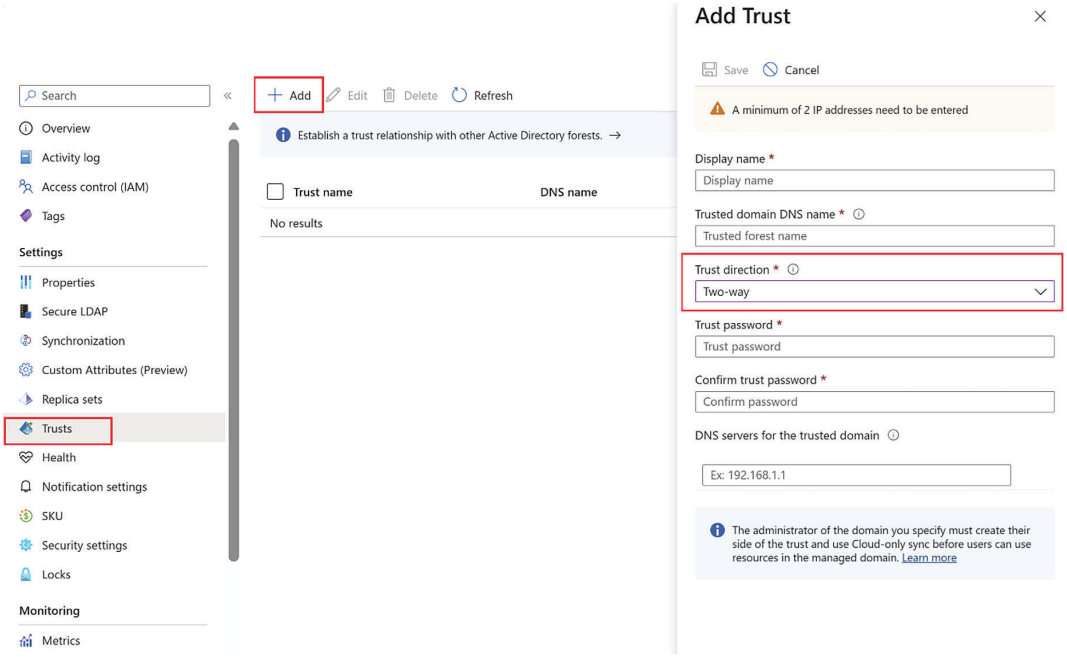


Figure 4.12: Create a two-way trust

You can verify the trust using either **Active Directory Domains and Trusts** console on the on-premises DCs or the **nltest** tool.

Administering a managed domain

Now that we have learned how to create and configure a managed domain, let's learn some basic administration tasks.

Creating an administrator VM

To administer a managed domain, you need to have a management machine. This is usually a Windows Server VM joined to the managed domain. You can either domain-join an existing Windows Server VM running in Azure or create a new Windows Server VM in Azure and join it to the managed domain. The following are the high-level steps:

1. Create a Windows Server VM in Azure and add it to the managed domain.

> **Note**
>
> The steps to create a Windows Server VM in Azure are beyond the scope of this book. The steps to add a Windows Server VM to a managed domain are the same as adding it to an on-premises AD DS domain.

2. Install Active Directory administrative tools on the VM.

This machine can now be used to perform administrative tasks in the managed domain such as creating and managing OUs, configuring GPOs, and administering DNS settings.

Creating an OU

OUs in an AD DS environment let you logically group user accounts, service accounts, and computer accounts. Specific administrators and group policies can then be assigned to specific OUs. In a managed domain, the following two built-in OUs exist:

- **AADDC Computers**: This container stores the computer objects for all computers that are joined to the managed domain.
- **AADDC Users**: This container stores the users and groups synchronized from the Microsoft Entra tenant.

OUs created in a hybrid on-premises AD DS domain are not synchronized to the managed domain. Instead, managed domains maintain a flat OU hierarchy, and all user accounts synchronized from the on-premises AD DS environment are placed in the **AADDC Users** OU.

Administrators can create custom OUs in the managed domain to meet the specific needs of their organization.

Before creating an OU, the following prerequisites must be met:

- An active Azure subscription with a Microsoft Entra tenant associated. The Entra tenant could either be cloud-only or synchronized with an on-premises domain.
- A management VM running Windows Server, joined to the managed domain.
- A user account in the Microsoft Entra tenant with membership of the *Microsoft Entra DC administrators* group.

There are some limitations and considerations when creating a custom OU in a managed domain. They are as follows:

- Use a user account with membership in the *AAD DC administrators* group to create an OU.

- The user who creates a custom OU is granted administrative privileges over that OU. The *AAD DC administrators* group also retains overarching administrative privileges to manage all custom OUs within the domain.
- Users or groups from the *AADDC Users* OU cannot be moved to a custom OU. Only users and groups created directly in the managed domain can be moved to the custom OU.
- Users and groups created in the custom OU are not available in the Microsoft Entra tenant.

To create an OU, log in to the Windows Server admin VM and use the **Active Directory Administrative Center** to create and manage OUs.

Administering GPOs

In AD, settings for users and computer objects are configured and managed through GPOs. Domain Services includes built-in GPOs for the *AADDC Users* and *AADDC Computers* OUs. Administrators can customize the settings in these GPOs to suit their organization's requirements. Members of the *AAD DC administrators* have Group Policy administration rights in the managed domain. They can also create custom GPOs and OUs.

In a hybrid environment, GPOs configured in the on-premises AD DS domain are not synchronized to the managed domain. To define settings for users or computer objects, edit the built-in GPO or create a custom GPO.

You can install and use the **Group Policy Management** console on the Windows Server admin VM to create and manage GPOs.

Managing DNS

Domain Services incorporates an integrated DNS server that delivers name resolution services for the managed domain. This DNS server is preconfigured with essential system records required to ensure the proper operation of the service. As applications and services are added to the managed domain, DNS records may need to be created to provide name resolution for these services. Members of the **AAD DC administrators** group can create and edit DNS records in the managed domain.

In a hybrid environment, DNS information configured in the on-premises AD domain is not synchronized to the managed domain. To resolve resources in the managed domain, conditional forwarders need to be created that point to DNS servers in the environment.

Since Domain Services communicates with several Azure endpoints for normal operations, redirecting zones like `file.core.windows.net` or `blob.core.windows.net` puts the managed domain in an unsupported state. It is recommended to not redirect DNS zones related to `windowsazure.com` or `core.windows.net`. If DNS redirection is a requirement, the redirection must be limited to individual host names and not zones.

To administer DNS, you must install and use the **DNS Server Tools** on the Windows admin VM.

> **Note**
>
> Do not modify or delete any built-in DNS records as they are used by Domain Services.

Checking health status

Microsoft Entra Domain Services run background tasks like taking backups, applying security updates, and synchronizing data from Entra ID. These are required to keep the managed domain healthy and updated. If there are any issues with Domain Services, these tasks may not complete. The health status of a managed domain can be monitored in Entra admin center to review and resolve any issues.

Following are the steps to check the health status:

1. Sign in to `https://entra.microsoft.com` as a **Global Administrator**.
2. Navigate to **Entra ID | Domain services**. In the right pane, click on the managed domain name.
3. Click on **Health**. The following image shows the status of a managed domain with the date and time of the last backup and last synchronization.

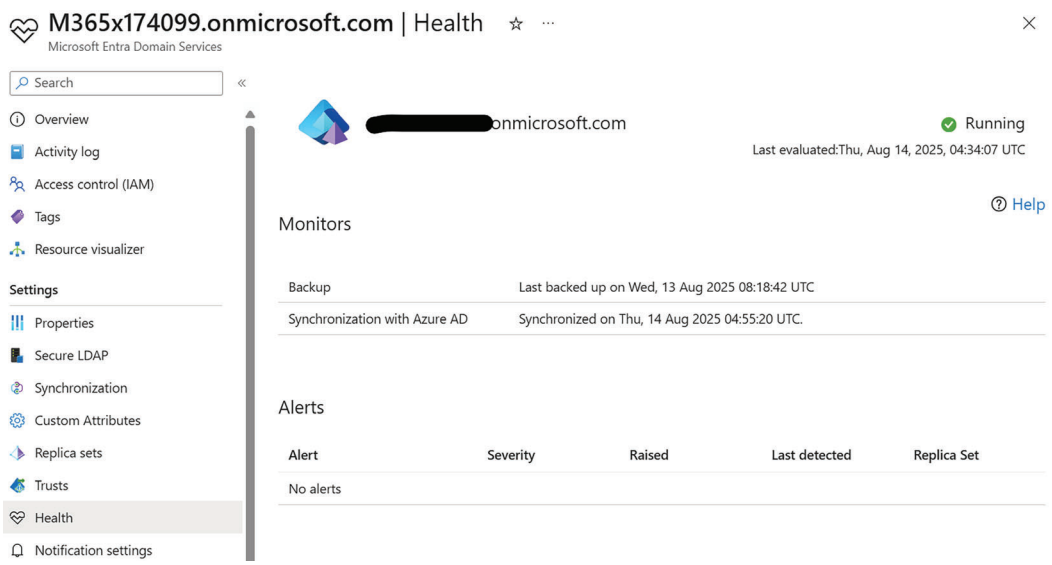


Figure 4.13: Managed domain health status

The last evaluated time indicates when the managed domain was most recently assessed. Domain health checks are performed on an hourly basis. Following any configuration changes, the updated health status will be reflected in the next evaluation cycle.

The status on the top right indicates the health of the managed domain. The following statuses are possible:

- **Running**: The managed domain is running fine and there are no critical or warning alerts. There may be some informational alerts.
- **Needs attention (warning)**: There are no critical alerts but there may be warning alerts that should be addressed.
- **Needs attention (critical)**: There are critical alerts that must be addressed immediately.
- **Deploying**: The managed domain is being deployed.

If critical or warning alerts are generated in the managed domain, email notifications are sent out. By default, all **Global Administrators** in Microsoft Entra ID and members of the **AAD DC Administrators** group receive the alerts. A notification is sent out as soon as a critical or warning alert is generated. If the alert is not resolved, a reminder is sent every four days. You can change the recipients of the email notifications by clicking on **Notification settings** and making the appropriate selections as shown in the following figure:

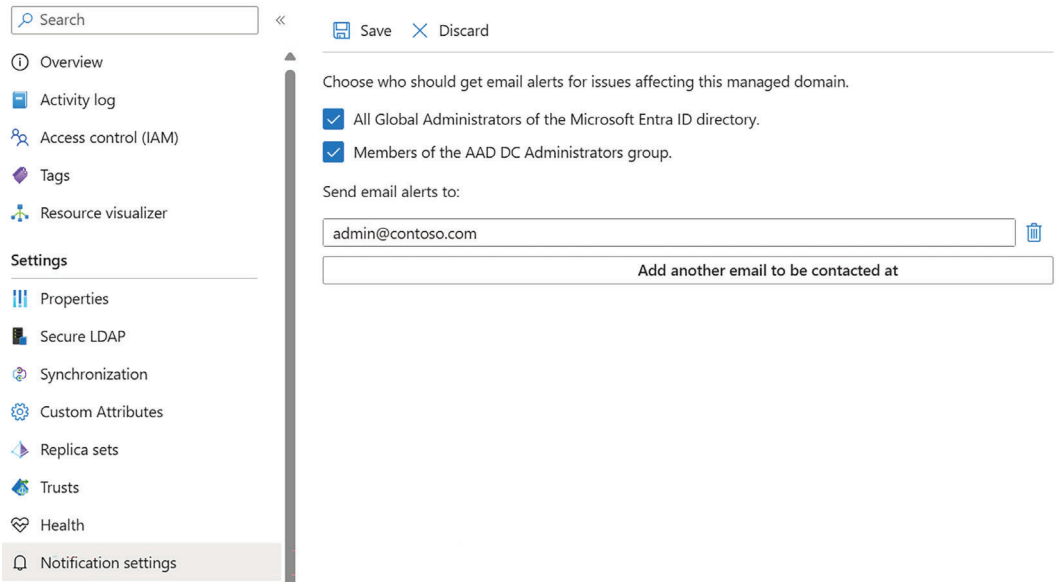


Figure 4.14: Notification settings

Administrators can use these notifications to ensure proper functioning of the managed domain.

Securing Domain Services

The following section explains some of the key security settings that must be enabled to secure your Domain Services managed domain.

Securing managed domain

Microsoft Entra Domain Services allows the use of NTLM v1 and TLS v1 by default. These ciphers may be required for some legacy applications to run, but they are considered insecure and weak and must be disabled if there are no applications that need them. Microsoft is deprecating the use of TLS 1.0 and TLS 1.1. TLS 1.2 and later versions offer improved security features such as perfect forward secrecy and stronger cipher suites.

To manage security settings for the managed domain, follow the steps below:

1. Sign in to `https://entra.microsoft.com` as a **Global Administrator**.
2. Navigate to **Entra ID | Domain services**. In the right pane, click on the managed domain name.

3. Click on **Security settings**. Click on **Enable** or **Disable** for the following settings:
    a. **TLS 1.2 Only Mode**: Before enabling TLS 1.2 only mode, ensure that there are no applications that still use earlier versions of TLS.
    b. **NTLM v1 Authentication**: If this mode is enabled, all NTLM v1 requests will fail.
    c. **Password synchronization from On-premises**: If this setting is disabled, on-premises user accounts will not be able to authenticate in the managed domain.
    d. **NTLM Password Synchronization**: If this setting is disabled, synchronized user accounts will not be able to use NTLM authentication in the managed domain.
    e. **Kerberos RC4 Encryption**: If this is disabled, all Kerberos requests that use RC4 encryption will fail.
    f. **Kerberos Armoring**: Enabling this setting will provide a secure channel between Kerberos client and the **Kerberos Distribution Center** (**KDC**).
    g. **LDAP Signing**: Enabling this setting will require all LDAP clients to request signing during bind time.
    h. **LDAP Channel Binding**: Enabling this setting will require all LDAP clients to provide channel binding information while communicating with the directory.
4. Once done, click **Save**.

Carefully consider the NTLM and TLS requirements for your organization and configure them appropriately to ensure that applications continue to work without compromising security.

Configuring Kerberos constrained delegation

Some applications need to access resources in the context of a different user. AD DS supports a mechanism called **Kerberos delegation** that lets one account impersonate another account to access resources. For example, a website can impersonate another user to access back-end resources. Kerberos delegation is considered insecure because it does not restrict which resources an impersonating account can access. In contrast, **Kerberos Constrained Delegation** (**KCD**) allows administrators to explicitly define the resources that can be accessed on behalf of another user. Configuring KCD requires domain administrator privileges to enable a domain account for a specific service, and the delegated account is limited to operating within a single domain. A managed domain does not give Domain Administrator privileges, so *account-based KCD* cannot be used. Domain Services managed domains use a more secure *resource-based KCD*, available in Windows Server 2012 and later. This capability enables administrators to configure constrained delegation for their services. Using resource-based KCD, back-end service administrators can explicitly allow or deny specific front-end services from performing delegation, thereby providing finer grained control over authentication flows.

Resource-based KCD can be configured for computer accounts or user accounts using PowerShell as per the steps below:

1. Create a custom OU in the managed domain.
2. Domain join the VMs that run the back-end application to the managed domain. Create the computer account of this VM in the custom OU.
3. To configure resource-based KCD for the computer account, use the following PowerShell command:

```
$ImpersonatingAccount = Get-ADComputer -Identity contoso-
webapp.aaddscontoso.com
Set-ADComputer contoso-api.aaddscontoso.com -
PrincipalsAllowedToDelegateToAccount $ImpersonatingAccount
```

4. To configure resource-based KCD for user account, use the following PowerShell command:

```
$ImpersonatingAccount = Get-ADUser -Identity appsvc
Set-ADUser backendsvc -PrincipalsAllowedToDelegateToAccount
$ImpersonatingAccount
```

While creating a KCD, keep the following points in mind:

- Resource-based KCD cannot be configured for accounts in the built-in *Microsoft Entra DC Computers* or *Microsoft Entra DC Users* containers.
- User accounts synchronized from Microsoft Entra ID cannot be used to set up resource-based KCD.
- You must be a member of the *Microsoft Entra DC administrators* group to run the PowerShell commands.

Configuring Kerberos constrained delegation allows a service to securely act on behalf of a user only to specific permitted services, limiting impersonation scope and reducing lateral-movement risk.

Enabling security audit events

Domain Services can collect events related to system security, Logon/Logoff, DNS events, policy change, and many more. These events can then be sent to Azure Storage, Azure Event Hubs, Azure Log Analytics Workspace, or a partner solution. Depending on the purpose for which these events are being collected, you can choose the appropriate service for collection, as summarized below:

- **Azure Storage**: Use this option when the primary purpose of event collection is archival.
- **Azure Event Hubs**: Use this option when the primary purpose is to share security events with additional services for data analysis or **security information and event management** (**SIEM**).
- **Azure Log Analytics Workspace**: Use this option when the primary purpose is to analyze and review security audits.

The following steps show how to enable security audit event collection:

1. Create the service where you want to collect the audit events by logging in to the Azure portal.
2. Sign in to `https://entra.microsoft.com` as a **Global Administrator**.
3. Navigate to **Entra ID** | **Domain services**. In the right pane, click on the managed domain name.
4. Click on **Diagnostic settings**. In the right pane, click on **Add diagnostic setting**.
5. Make the applicable selections as shown in the following figure and click **Save**.

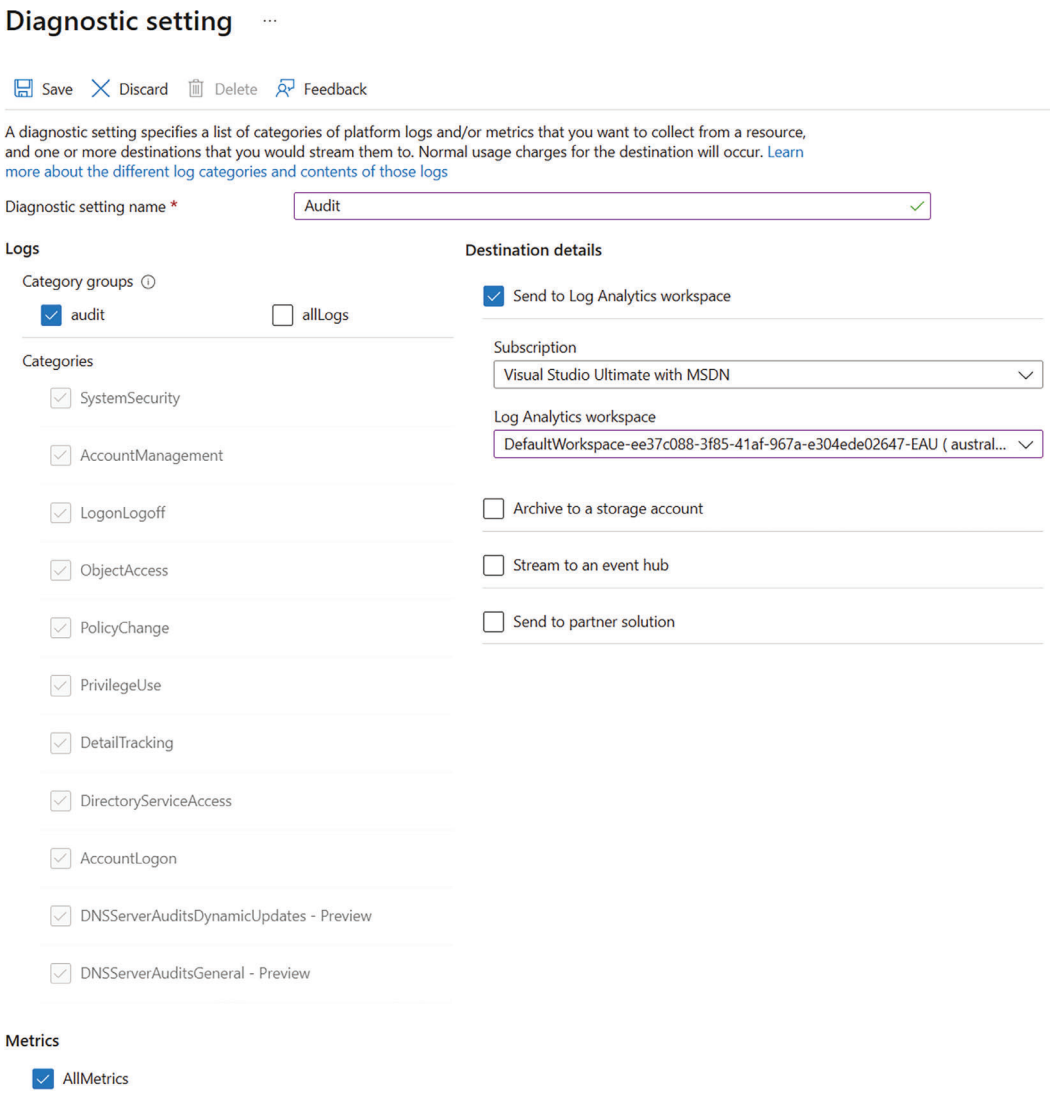


Figure 4.15: Diagnostic settings

Once these events are collected you can use Azure Monitor to analyze and identify issues in the managed domain. Using Azure Monitor Workbooks, you can visualize this data to identify issues sooner and make quick decisions. Domain Services offers two workbooks to visualize the data.

- **Security overview report**: This report contains a summary of sign-in attempts and a list of some accounts to check in on.
- **Account activity report**: Detailed sign-in and account management event logs for a specific user account.

These workbooks can be accessed by clicking on **Workbooks** in the managed domain. Click on a workbook to see the data. While these two workbooks provide a good place to start with data analysis, you can create your own workbooks if you would like to get more granular.

Summary

This chapter covers how organizations with dependency on legacy methods like LDAP and Kerberos can seamlessly transition to the cloud. It explained how organizations can use Microsoft Entra Domain Services to provide these capabilities in the cloud with minimum administrative overhead. It began by explaining the difference between a self-managed domain and a managed domain. It then went deep into managed domains outlining the basic concepts required for creating and managing a managed domain. It explained how to create, manage and administer a managed domain. In the next chapter, we will learn about Security Copilot in Microsoft Entra.

Exercises

1. You are the IT administrator for an organization that has a significant investment in on-premises infrastructure. You have DCs that support legacy applications for LDAP and Kerberos. Your management wants to accelerate the move to the cloud to reduce costs; however, your applications are not ready for modern authentication and hence, have a dependency on the on-premises AD DS domain. What should you do to accelerate the move to the cloud?
    a. Retire all applications that require LDAP and Kerberos.
    b. Implement a self-managed domain in Microsoft Entra.
    c. Modernize all applications and then move to Microsoft Entra.
    d. Implement a Microsoft Entra Domain Services managed domain.

2. You have implemented a Microsoft Entra Domain Services managed domain. You want to provide geographical disaster recovery in case one Azure region becomes unavailable. What should you do?
    a. Implement Microsoft Entra Domain Services managed domain in multiple Azure regions.
    b. It is not possible to provide geographical disaster recovery for Domain Services.
    c. Configure additional replica sets.
    d. Keep an on-premises AD DS domain as backup and quickly switch to it if the Azure region fails.
3. Your organization's security team requires that users created directly in the managed domain have a 12-character password. How can you best meet this requirement?
    a. Edit the managed domain password policy.
    b. Create a new custom password policy.
    c. Use a self-managed domain instead.
    d. It is not possible to configure password length in a managed domain.

Answers

1. d
2. c
3. b

Additional resources

- Microsoft Entra Domain Services documentation: `https://learn.microsoft.com/en-us/entra/identity/domain-services/`

Join us on Discord

For discussions around the book and to connect with your peers, join us on Discord at `packt.link/discordcloud` or scan the QR code below:



5

AI in Microsoft Entra

The integration of **Artificial Intelligence (AI)** in cybersecurity has revolutionized how organizations approach the protection of their digital assets. AI systems can analyze vast amounts of data at speeds that far surpass human capabilities, allowing for the rapid identification of potential threats and vulnerabilities. Machine learning algorithms, for instance, can detect unusual patterns of behavior that may indicate a cyber-attack, such as unauthorized access, phishing attempts, or malware infections. By continuously learning from new data, these systems become increasingly adept at recognizing both known and emerging threats, reducing the window of opportunity for malicious actors.

Moreover, AI-powered tools can automate routine security tasks, such as monitoring network traffic, updating access controls, and responding to incidents. This not only improves the efficiency of cybersecurity operations but also frees human experts to focus on more complex challenges. In environments like Microsoft Entra, solutions such as Security Copilot leverage AI to provide actionable insights, streamline investigations, and enhance overall security posture.

This chapter will cover the following topics:

- Overview of Microsoft Security Copilot
- Security Copilot in Microsoft Entra
- Security Copilot agents in Microsoft Entra
- Microsoft Entra Agent ID

Microsoft Security Copilot

Microsoft Security Copilot is an advanced, AI-driven cybersecurity solution designed to empower security teams with intelligent insights and faster response capabilities. By leveraging the power of generative AI and deep integration with Microsoft's security ecosystem, Security Copilot helps organizations identify, investigate, and remediate threats

with unprecedented speed and accuracy. It acts as a virtual assistant for security professionals, automating routine tasks such as incident triage, alert prioritization, and threat hunting, thereby freeing up valuable time for analysts to focus on strategic initiatives.

Security Copilot integrates seamlessly with platforms like Microsoft Entra, Microsoft Defender XDR, Microsoft Intune, and non-Microsoft services like Jamf and Red Canary allowing it to access and analyze data across a wide range of environments. It continuously learns from new threat intelligence and user feedback, adapting to emerging risks and evolving tactics employed by malicious actors. The solution presents findings in clear, actionable formats, enabling teams to understand complex threat scenarios and make informed decisions quickly. Additionally, Security Copilot enhances collaboration by providing guided investigation workflows, recommended remediation steps, and detailed reporting, making it an essential tool for modern security operations centers.

Support professionals can interact with Security Copilot in natural language to address end-to-end scenarios, such as incident response, threat hunting, and posture management. This service utilizes OpenAI to generate contextual responses to user prompts, drawing on security plugins that integrate organization specific data, authoritative sources, and globally available threat intelligence.

Security Copilot assists defenders in the following cases:

- **Investigate and remediate threats**: With Security Copilot, defenders can rapidly establish context around incidents, transforming complex security alerts into actionable summaries that streamline triage and accelerate remediation.
- **Build KQL queries**: Defenders can use natural language to generate complex KQL queries eliminating the need to learn and write the query language.
- **Reverse engineer scripts**: Security Copilot can also analyze existing scripts and translate them to natural language for better understanding.
- **Improve security posture**: Security Copilot can help understand and prioritize the risks faced by an organization and suggest remediation to improve the security posture.
- **Manage security policies**: Security Copilot can help define security policies and compare them with existing policies to highlight policy gaps, conflicts, and overlaps.
- **Reporting**: Security Copilot can help generate reports that can be shared with stakeholders.

A user's interaction with Security Copilot can be explained as follows:

1. User asks a question in natural language. This is called a **prompt**.

2. Security Copilot preprocesses this prompt to improve the specificity and help generate answers that are relevant to the prompt. This process is called **grounding**.
3. This modified prompt is sent to the language model.
4. The language model processes the prompt and generates a response. This response is sent back to Security Copilot.
5. Security Copilot receives the response and enriches it with contextualized information from the plugin. This is called **post-processing**.
6. The final response is then sent back to the user.

The following picture explains how Security Copilot works:

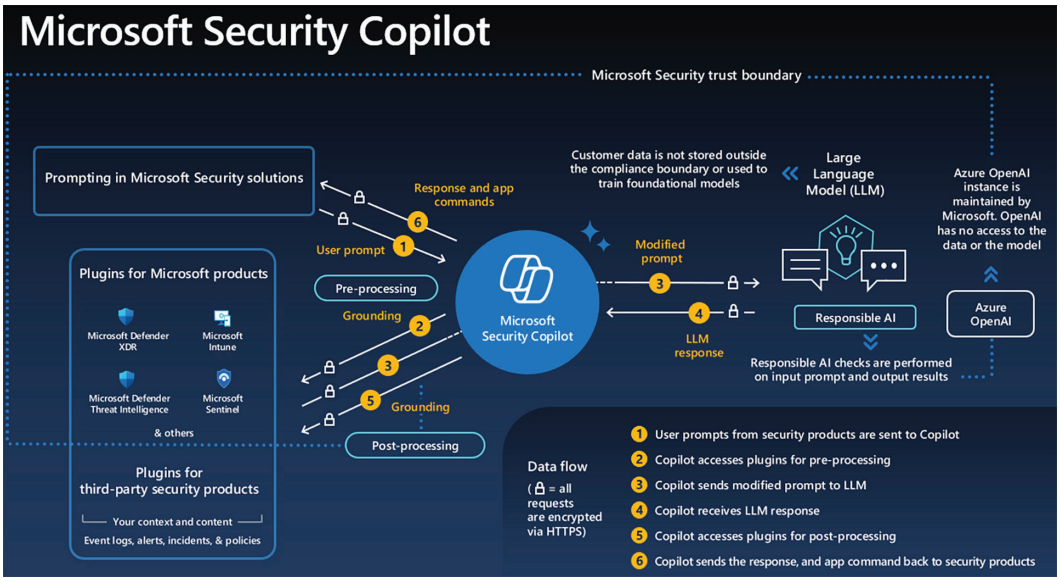


Figure 5.1: Microsoft Security Copilot

Security Copilot experiences

Security Copilot meets the user where they are. It offers two types of experiences as described below.

Standalone experience

When Security Copilot is accessed through `https://securitycopilot.microsoft.com`, it is the standalone experience. The following picture shows the Security Copilot standalone experience:

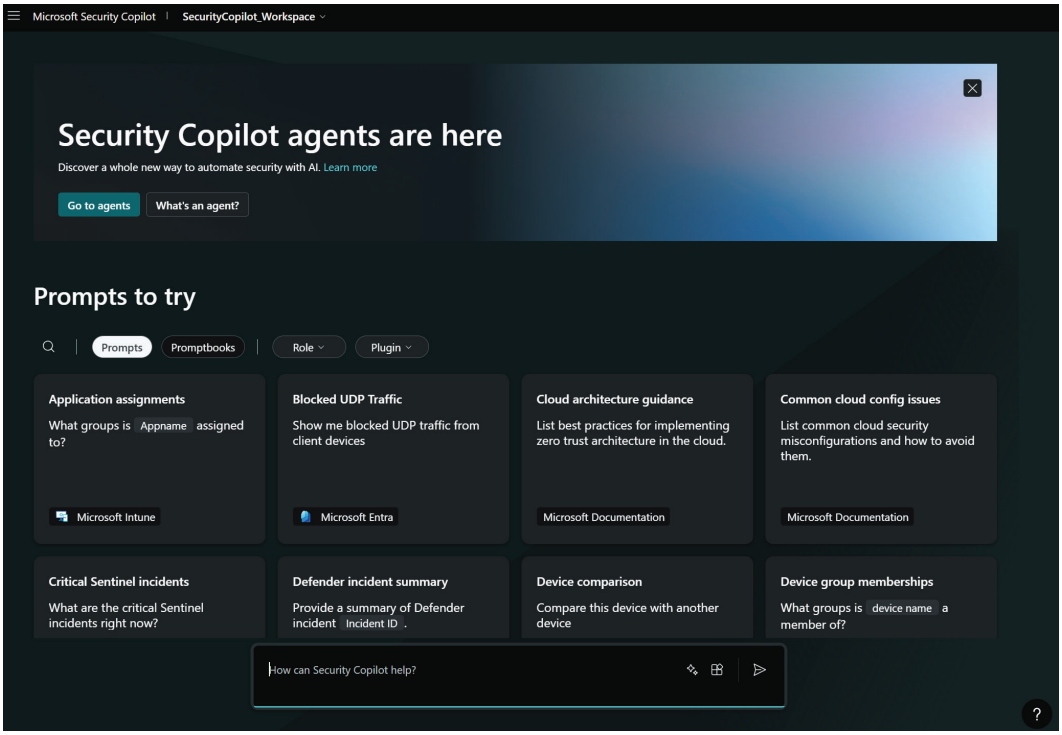


Figure 5.2: Security Copilot standalone experience

Users can start typing their prompts in the box that says **How can Security Copilot help?** to start the conversation.

Embedded experience

When Security Copilot is accessed from within one of the other Microsoft security product portals like Microsoft Entra, it is called an embedded experience. The following picture shows the Security Copilot embedded experience in the Microsoft Entra portal:

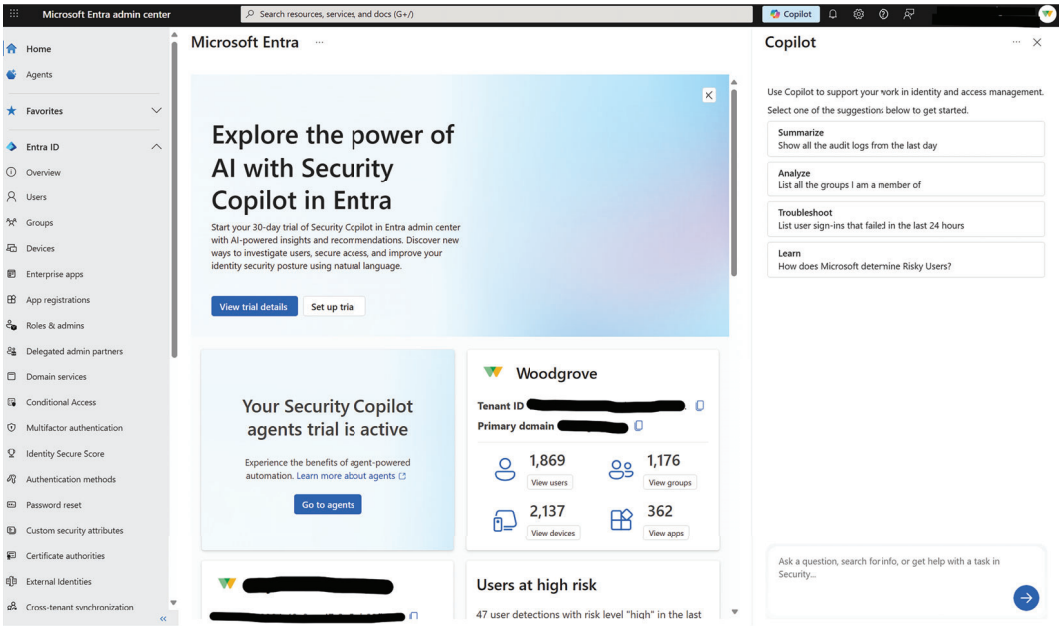


Figure 5.3: Security Copilot embedded experience

Clicking on **Copilot** in the top ribbon opens the panel which is called **Copilot sidecar**.

Privacy and data security

Microsoft Security Copilot stores and processes **Customer Data** and **system-generated logs** as part of the service.

Microsoft defines Customer Data as all data such as text, sound, video, image file, and software that are provided to Microsoft by the customer through the use of its online services. It does not include information used to configure the service, such as settings or names of resources. In Security Copilot, Customer Data includes user submitted prompts, information retrieved to generate responses, responses, and file uploads.

When customers use Microsoft online services, system-generated logs are created as part of service operations. These logs record system activity over time so that Microsoft can monitor whether the service is operating as expected. The storage and processing of these logs are essential to identify and respond to policy violations and fraud. This also aids in optimizing system, network, and application performance, helps with security investigations, and ensures compliance with laws and regulations. System-generated logs include account information such as tenant ID, account ID, and licensing details, as well as usage and performance data and internal system behavior information.

By default, data sharing is turned on. This can be changed by Global Administrators and Security Administrators who have the Capacity Contributor role. This data is only used by Microsoft to improve product performance. It is not used to train Azure OpenAI models, shared with OpenAI or third parties, nor is it used for sales.

Security Copilot integrates with other Microsoft 365 and Microsoft security services that an organization is licensed to use. Organizations have the option to allow users to query information from those services both in the embedded and standalone experiences.

Data storage locations

Data is stored in the location you select when you onboard to Security Copilot. Once this selection is made, the data storage location cannot be changed. If data sharing is enabled, Customer Data (except uploaded files) may be stored outside of the chosen workspace location. Uploaded files remain in the chosen workspace location. If content from an uploaded file is part of the response, that content may be stored outside the chosen workspace location. Uploaded files are only available to the user who uploaded them.

Data retention

Customer Data is stored in the organization's tenant for as long as the organization has an active Security Copilot subscription. It is deleted within 180 days if the organization deletes all provisioned capacity or when the organization requests that their data be deleted. This is done within 30 days of Microsoft receiving the request.

If data sharing is opted in, Customer Data is retained for 90 days before being deleted by the team evaluating the data. If organizations opt out of data sharing, all Customer Data is deleted within 30 days.

Prompt evaluation locations

While setting up Security Copilot, you will be asked to select a location for prompt evaluation. One of the following locations can be selected:

- Australia (ANZ)
- Europe (EU)
- United Kingdom (UK)
- United States (US)

It is, however, recommended that the prompts be evaluated anywhere in the world depending on capacity.

Getting started with Security Copilot

To enable and use Security Copilot in your organization, you need to take several steps. This includes provisioning capacity, assigning roles, managing plugins, and more. Security Copilot

usage is measured in terms of **Security Compute Units (SCUs)**. These are the compute resources that are needed for Security Copilot to work. Security Copilot works on provisioned capacity and overage capacity. **Provisioned capacity** is billed by the hour, whereas **overage capacity** is billed usage. SCUs can be provisioned flexibly to accommodate regular and peak workload. To handle unexpected workload spikes, overage capacity can be provisioned that makes additional SCUs available when the originally provisioned ones are used during unexpected workload spikes. The overage units are billed on demand and can be set to unlimited or be capped at a maximum amount. SCUs are billed on hourly blocks and have a minimum of one hour. Let's understand this with the help of an example.

Let's assume that an organization has one SCU provisioned with no overage. If this one SCU gets consumed within 45 minutes, Security Copilot will not process further prompts till the hour is reset. If the organization now provisions an additional SCU as overage and the provisioned SCU gets consumed within 45 minutes, the overage SCU will be used, and Security Copilot will continue to process requests. If the provisioned SCU does not get consumed within the hour, the overage SCU is not used, and the organization is not charged for it.

Prerequisites

To get started with Security Copilot, ensure that the following prerequisites are met:

- An Azure subscription with Azure Owner or Contributor role
- At least 1 SCU is required for non M365 E5 or E7 customers

It is recommended to use roles with fewest permissions to improve security for your organization. Other supported roles include but are not limited to Billing Admin, Intune Admin, Entra Compliance Admin.

Provisioning capacity

To onboard Security Copilot, you must first provision capacity. When you first go to `https://securitycopilot.microsoft.com`, a wizard will take you through the steps to set up Security Copilot. These are described as follows:

1. In a browser window, go to `https://securitycopilot.microsoft.com`.
2. Click on **Get started**.
3. You will be asked to set up a **workspace**. A workspace is a dedicated environment where users can collaborate, manage security insights, and organize resources for threat investigation and response. Enter a **Workspace name** and click on **Continue**.
4. Next set up security capacity. To do this, choose the **Azure subscription** and **Resource group**. Give the capacity a name, select the **Capacity region** and **Prompt evaluation**

location. Lastly, specify the number of SCUs you would like to provision and whether you want to configure overage units. Refer to the following screenshot:

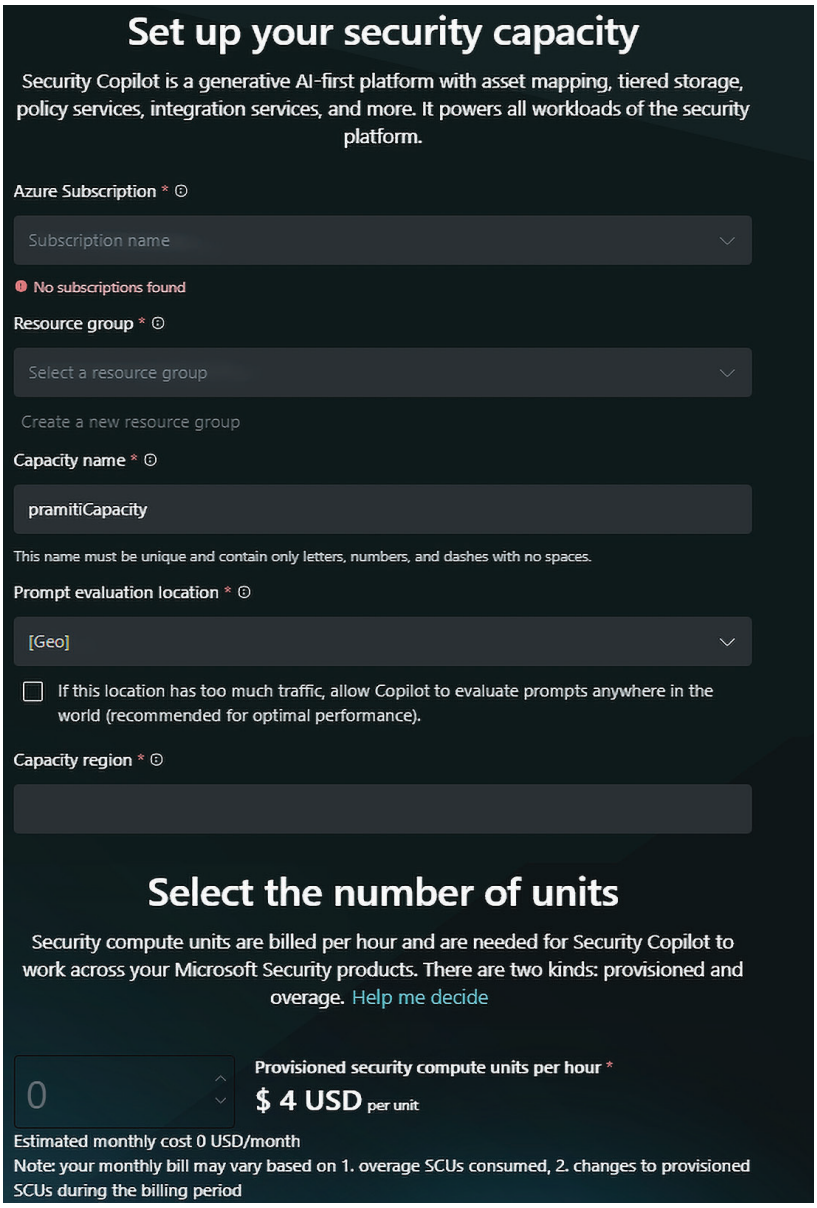


Figure 5.4: Provision Security Copilot capacity

5. Next, select the data sharing options and click **Continue**.

6. Acknowledge and agree to the terms and conditions and click **Continue**. It will take a few minutes to deploy the Azure resources.
7. Select if you want Security Copilot to store admin and user actions and system responses and click **Continue**.
8. Select the roles that can access Security Copilot and click **Continue**.
9. On the confirmation page, click **Finish**.

Understanding authentication

Security Copilot works in the user context. It operates on behalf of the logged-in user. Specific Security Copilot roles must be assigned to users for them to be able to access the Security Copilot platform. Security Copilot has the following two roles that work like access groups:

- Copilot owner
- Copilot contributor

These are not Microsoft Entra roles. They control access to the Security Copilot platform and by themselves do not provide access to any security data. Users must be assigned additional roles within the service to be able to run prompts in Security Copilot. This can be done using the **Recommended Microsoft Security roles** group.



Figure 5.5: Recommended Microsoft Security roles

The Global Administrator and Security Administrator roles in Microsoft Entra automatically inherit the Copilot owner permission. This ensures that Security Copilot has at least one owner.

Security Copilot in Microsoft Entra

Security Copilot has several Microsoft and non-Microsoft plugins available out of the box that can be used to extend its capabilities. In addition, developers can also write their own plugins that can be used to perform specialized tasks. Microsoft Entra is one of the Microsoft plugins that enables Security Copilot to query information from Microsoft Entra. Using this plugin, administrators can investigate and resolve identity related risks, assess identities, and complete complex tasks efficiently. Security Copilot gets information from Microsoft Entra users, groups, sign-in logs, audit logs, conditional access policies, lifecycle workflow, access reviews, and much more.

In Microsoft Entra, Security Copilot includes the standalone experience, the embedded experience in the Microsoft Entra portal, and agents that can perform tasks.

As described earlier, Security Copilot can be accessed from the Microsoft Entra portal by clicking on the Copilot button to bring up the sidecar experience. You can choose from a set of starter prompts that are shown in the sidecar or enter your own prompts to start the conversation with Copilot. Once you click on a starter prompt or enter your own prompt, Copilot shows some suggested prompts that help you continue the conversation. The following picture shows the use of starter prompts and the suggested prompts:

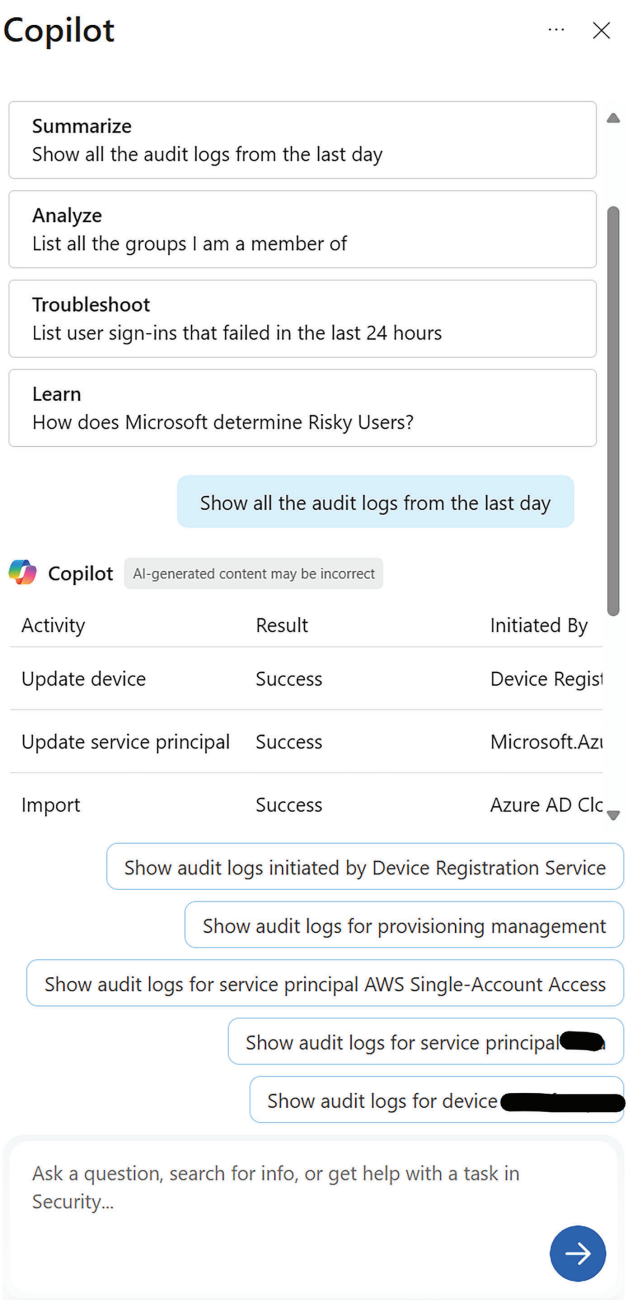


Figure 5.6: Starter prompts and suggested prompts

Let's explore some of the scenarios supported by Security Copilot in Entra.

Supported scenarios

Currently, Security Copilot in Entra supports the following scenarios with more being added continuously.

Tenants

Administrators can now ask natural language questions about their tenants such as their tenant ID, active licenses, and more. The following are some example prompts that you can use:

- *What is my tenant ID?*
- *Who is the security compliance contact for my tenant?*
- *What are the assigned licenses in my tenant?*
- *What is my tenant's display name?*

A **Global Reader** role and Microsoft Entra ID license are required for this feature.

Users

Using Security Copilot, identity administrators can quickly view user details, manage roles, and troubleshoot access issues using natural language queries. This feature helps secure user identities and increase the efficiency of identity administrators by reducing the time spent navigating across portals. The following are some example prompts that you can use:

- *How many guest users are there in my tenant?*
- *Tell me more about user <user's name>?*
- *List all the users in <department name>?*
- *Are there any users that have <license type> assigned?*

A **User administrator** role and Microsoft Entra ID license are required for this feature.

Groups

Security Copilot simplifies group management by enabling identity administrators to query group configurations, manage memberships, and maintain group hygiene using natural language. The following are some example prompts that you can use:

- *How many groups in my tenant don't have owners?*
- *Show me all users in the group <group name>?*
- *What directory roles are assigned to the group <group name>?*
- *List the number of groups under each group type.*

This feature is available with the free version of Microsoft Entra. Users with **Directory Writer**, **Groups Administrator** and **User Administrator** roles can use this feature.

Devices

With Security Copilot, identity administrators can investigate user devices using natural language. Information such as device ID, compliance status, and join type can be queried. The following are some example prompts that you can use:

- *Show me all non-compliant devices in my tenant?*
- *List all devices that are Entra ID registered.*
- *List devices running <operating system name>?*
- *How many devices are running <operating system version>?*

This feature is available with the free version of Microsoft Entra ID and to any user in the tenant.

Roles and administrators

IT admins can now use Security Copilot to investigate Microsoft Entra roles. The following are some example prompts that you can use:

- *How many users in my tenant have the global administrator role?*
- *Which users are eligible for the Security Administrator role?*
- *What transitive roles does the user <user's name> have?*
- *What are the scheduled roles group <group name> has?*

Users with **Directory Reader** or **Global Reader** roles can use this feature.

Domain Services

Security Copilot for Entra includes Domain Services support, enabling IT admins to efficiently monitor and investigate domain-related activities within their environment. Using this feature, admins can easily verify DNS records and manage domain settings using natural language. The following are some example prompts that you can use:

- *List details of <domain name>.*
- *Show me DNS verification records of <domain name>.*
- *What is my initial domain name?*

A **Domain Name Administrator** role and Microsoft Entra ID license is required for this feature.

Conditional Access

Conditional Access in Security Copilot for Entra empowers IT administrators to implement and manage policies that restrict access to organizational resources based on specific conditions. This capability enhances security by allowing admins to enforce rules, monitor compliance,

and respond to potential threats using adaptive controls and intuitive, natural language queries. The following are some example prompts that you can use:

- *How many Conditional Access policies in my tenant enforce MFA?*
- *Do any of these policies have users or groups in the exclude list?*
- *Are there any conflicting Conditional Access policies in my tenant?*
- *Which Conditional Access policies in my tenant are currently active?*

Users with **Security Administrator**, **Global Reader** or **Security Reader** roles can use this feature. This feature requires a Microsoft Entra ID P1 license.

Authentication

This feature enables identity admins to manage authentication methods in their tenant. Using natural language, they can query which authentication methods are enabled, understand user registration status, and identify gaps. The following are some example prompts that you can use:

- *Which authentication methods are enabled in my tenant?*
- *How many users have the FIDO2 method registered?*
- *What authentication methods are registered for <UPN>?*
- *Is Microsoft Authenticator app enabled in my tenant?*

To use this feature, users must have the **Authentication Policy Administrator** role for tenant level configurations or **Privileged Authentication Administrator** for user level configurations. This feature can be used with a Microsoft Entra ID license.

Sign-in logs

Using this feature, identity administrators can easily review and troubleshoot sign-in problems instead of manually traversing through the logs. They can ask natural language questions about sign-in problems in their tenant and receive actionable answers. Copilot also suggests recommended follow-up prompts that support the troubleshooting process and guide next steps. When the Copilot sidecar is opened from within the Sign-in logs blade, it shows the starter prompts tailored to the sign-in data analysis. The following are some example prompts that you can use:

- *Show all sign-ins without MFA.*
- *Show suspicious login activities.*
- *Show me risky sign-ins in my tenant in the last 24 hours.*
- *Show sign-ins from non-compliant devices.*

Users must be assigned **Reports Reader**, **Security Reader**, **Global Reader**, or **Security Administrator** role to query sign-in logs. This feature requires a Microsoft Entra P1 license.

Audit logs

Using this feature, admins can easily investigate and troubleshoot audit logs using natural language without having to manually search through them. This saves the admins precious time. The admins can analyze audit activities, identify issues, and receive actionable answers. Copilot also suggests recommended follow-up prompts that support the troubleshooting process and guide next steps. The following are some example prompts that you can use:

- *Show me the groups that were recently deleted from my tenant.*
- *Who created the group <group name>?*
- *Show me the groups created by risky users in the tenant?*
- *Show me all groups created by <user's name>?*

Users must be assigned **Reports Reader**, **Security Reader**, **Global Reader** or **Security Administrator** role to query sign-in logs. This feature is available with the free version of Microsoft Entra ID.

Recommendations

Recommendations in Microsoft Entra provide actionable insights to help administrators optimize security and compliance within their organization. By analyzing audit logs and sign-in activities, Entra suggests specific steps to resolve issues, enhance configuration, and mitigate risks. These recommendations support proactive management and continuous improvement of identity and access controls. Using Security Copilot, identity admins can interact with these recommendations in natural language enabling them to keep the tenant in a secure and healthy state. The following are some example prompts that you can use:

- *List all Microsoft Entra recommendations.*
- *Show all Microsoft Entra recommendations for Conditional Access.*
- *List recommendations to improve the identity security posture.*
- *Which applications have credentials that are about to expire?*

The following roles can use this feature – Application Administrator, Identity Governance Administrator, Privileged Role Administrator, Conditional Access Administrator, Security Administrator, Hybrid Identity Administrator, Authentication Policy Administrator, and Authentication Administrator. This feature requires that the organization has at least a Microsoft Entra ID P1 license.

Health monitoring alerts

Microsoft Entra ID includes a feature called **External Health Monitoring** that analyzes scenario-specific metrics for each tenant. It detects anomalies and raises alerts in Microsoft Entra for admins to investigate potential issues. The following are some example prompts that you can use:

- *List the health alerts in my tenant.*
- *Which users are impacted according to the health monitoring alerts?*
- *Show me compliant device health monitoring alerts.*
- *Show me health monitoring alerts details for alert ID <alert ID>?*

The following roles can use this feature – **Reports Reader**, **Helpdesk Administrator**, **Security Operator**, **Security Administrator**, **Security Reader**, and **Global Reader**. This feature requires a Microsoft Entra ID P2 license.

Service level agreement

Microsoft Entra has a **Service Level Agreement** (**SLA**) of 99.99% for authentication availability. If the availability dips below this level in a month, customers may be eligible for service credits. Microsoft Entra Health provides reporting on this SLA. Using Security Copilot, identity admins can query the Microsoft Entra Health SLA reporting. Following are some example prompts:

- *What is my SLA for Microsoft Entra ID authentication?*
- *Show me my tenant's authentication availability.*
- *Has my tenant had an SLA breach in the last X months?*
- *What is the SLA for Microsoft Entra ID?*

The **Reports Reader** role is required to use this feature.

Risky users

Security Copilot uses Microsoft Entra ID Protection to summarize a user's risk level and provide insights. Identity admins can now generate a summary for a risky user. Security Copilot summarizes in natural language the risks found for the selected user. It also provides recommendations on what to do next and links to some helpful documentation. This feature requires the **Identity Governance Administrator** role and a Microsoft Entra ID P2 license.

Application risk

Identity admins can now use Security Copilot to identify risky applications by using natural language. Admins can easily discover unused apps, overprivileged apps, and the risk level of applications. When the Copilot sidecar is opened from within the Enterprise Applications

blade, it shows the starter prompts tailored to the application scenario. Using this feature, administrators can address the following use cases:

- Identify risky service principals.
- Identify risky applications.
- View permissions granted to a service principal.
- Identify unused applications
- Identify applications from outside the tenant.

Following are some example prompts:

- *Show me risky apps in my tenant.*
- *Give me details about the service principal <service principal name>?*
- *Which applications in my tenant have high privileged permissions?*
- *Show me apps from outside my tenant.*

This feature requires the **Application Administrator** or **Cloud Application Administrator** role. The tenant must have a Microsoft Entra ID P2 and Workload Identity Premium license.

Entitlement Management

Security Copilot can be used with Microsoft Entra ID Governance to quickly access information about access packages, connected organizations, and catalogs using natural language. The following are some example prompts that can be used:

- *How many resources are there in catalog <catalog name>?*
- *Which access packages are a part of catalog <catalog name>?*
- *Who are the external users from connected organization <organization name>?*
- *What access package assignments does the user <user's name> have?*

Administrators must have the **Identity Governance Administrator** role to use this feature. It also requires that the tenant has Microsoft Entra ID P2 licenses.

Access reviews

Security Copilot can also be used to query data related to Microsoft ID Governance Access Reviews. This allows administrators to track access reviews at scale by identifying who approved access, who took no action, and who overrode AI recommendations. Following are some example prompts that can be used:

- *Show me the top pending access reviews.*
- *Who approved or denied access for <access review name>?*

- *List where the user <user's name> is the assigned approver.*
- *Which access review decisions overrode AI suggested actions?*

Administrators must have the **Identity Governance Administrator** role to use this feature. It also requires that the tenant have Microsoft Entra ID P2 licenses.

Privileged Identity Management

Security Copilot integrates with Microsoft Entra **Privileged Identity Management** (**PIM**) to deliver information on just-in-time role assignments, group memberships, and access to important resources. It uses AI-based analytics to help administrators determine which users have active or eligible PIM assignments. Following are some example prompts that can be used:

- *Which PIM roles are assigned to user <user's name>?*
- *Who has PIM eligible assignments of <role name>?*
- *Who has PIM active assignments of <role name>?*
- *Which PIM eligible roles are assigned to user <user's name>?*

Using this feature requires a **Security Administrator**, **Global Reader**, or **Security Reader** role. It also requires a Microsoft Entra ID P2 license.

Lifecycle workflows

Security Copilot also works with Microsoft Entra ID Governance Lifecycle Workflows to help identity admins manage the lifecycle of users. Using Security Copilot, identity admins can use natural language to create and manage workflows across the identity lifecycle. The following use cases can be accomplished:

- Create a new lifecycle workflow
- Explore available workflows
- Analyze active workflows
- Troubleshoot a Lifecycle Workflow run
- Compare lifecycle workflow versions

Following are some example prompts that you could use:

- *List all the supported workflow templates.*
- *List all leaver workflows in my tenant.*
- *How many times did the workflow <workflow name> run in the last 7 days?*
- *Which workflows failed the most in the last 7 days?*

Using this feature requires a **Lifecycle Workflows Administrator** role and a **Microsoft Entra ID Governance** license.

License usage

Security Copilot simplifies tracking license usage across the Microsoft Entra tenant. Administrators can ask questions in natural language about license usage. The following are some prompts that can be used:

- *How many Microsoft Entra P2 licenses are in use?*
- *How many users are using Conditional Access?*
- *Show me the Microsoft Entra P2 feature utilization.*

Using this feature requires a **Global Reader** role and a **Microsoft Entra ID Governance** license.

Security Copilot serves as a useful assistant to identity admins by simplifying complex tasks and saving precious time.

Global Secure Access

Microsoft Security Copilot can get insights by analyzing the GSA traffic logs. This enables administrators to investigate and monitor network traffic usage using natural language. This saves precious time as administrators no longer need to manually sift through logs for troubleshooting or threat hunting. The following are some sample prompts that can be used:

- *Show the top 5 users who have the highest data consumption in the last 24 hours.*
- *Which high risk applications were accessed in the last 24 hours?*
- *Show all blocked traffic for <username> in the last 24 hours.*

Using this feature requires a **Security Administrator**, **Global Reader**, **Global Secure Access Administrator** or **Global Secure Access Log Reader** role. Microsoft Entra P1 license is required to query Microsoft 365 traffic logs. Microsoft Entra Private Access license is required to query private access traffic and Microsoft Entra Internet Access license is required to query internet access traffic.

Security Copilot agents in Microsoft Entra

AI agents are intelligent software programs designed to perform tasks autonomously, using artificial intelligence techniques to interpret data, make decisions, and take actions on behalf of users. These agents can handle repetitive or complex tasks, such as monitoring security events, processing requests, or managing workflows, allowing humans to focus on higher-value activities. In environments like Microsoft Entra, AI agents assist administrators by analyzing vast amounts of information, identifying potential issues, and providing actionable insights. This not only enhances efficiency but also helps in maintaining a secure and well-governed IT environment, saving time and reducing the risk of human error.

Each agent performs a different set of tasks and therefore they need specific configuration to operate. A unique agent identity is created when the agent is turned on. Specific roles and permissions may be required for the agent to perform its tasks. Administrators need specific roles to set up and configure the agents.

Agents don't require any special training or licensing. They fit seamlessly into the existing workflows. They consume SCUs like the other Security Copilot features. Agents learn based on feedback and keep the users in control of the actions they take.

All agents published by Microsoft and partners are available in the **Security Store** in the Microsoft Entra admin center as shown in the screenshot below:

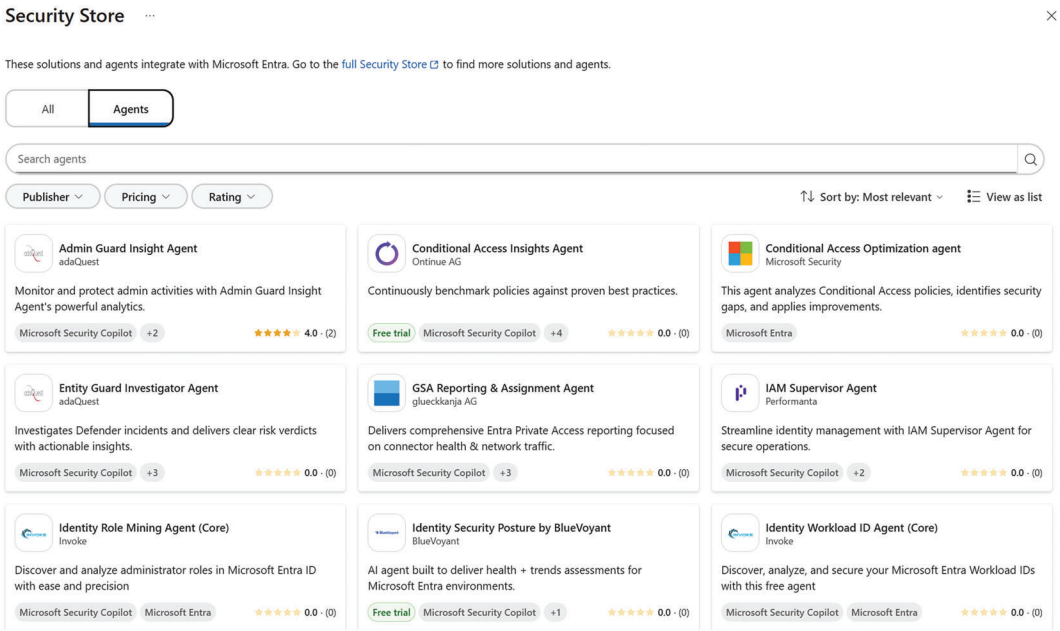


Figure 5.7: Agents in Security store

Click on any agent to view details and install.

Conditional Access optimization agent

The Conditional Access optimization agent ensures that all users are protected by Conditional Access policies. It can recommend new policies and update existing policies based on zero trust best practices. It also creates policy review reports that provide insights that might indicate policy misconfiguration.

The Conditional Access agent scans the tenant to identify users, applications and agent identities created in the last 24 hours that are not protected by Conditional Access policies. If it finds unprotected users, applications or agent identities, it provides recommendations like creating a new policy or adding users and applications to an existing policy.

The following steps are executed each time the agent runs. These steps do not consume SCUs:

1. All Conditional Access policies in the tenant are scanned.
2. Policy gaps and any overlapping policies are identified.
3. Previous suggestions are reviewed so that the agent does not repeat suggestions.

If the agent identifies something that was not suggested before, the following steps are taken. These steps consume SCUs:

1. Policy gaps or pairs of policies that can be consolidated are identified.
2. Any custom instructions provided by the admin are reviewed.
3. New policies are created in report-only mode or suggestions are provided to modify existing policies.

The agent can include the following policy suggestions:

- **Require MFA**: The agent identifies users created in the last 24 hours who are not covered by a Conditional Access policy that enforces MFA. It can also update the policy.
- **Require device-based controls**: The agent can enforce controls such as device compliance, app protection policies, and domain-joined devices.
- **Block legacy authentication**: The agent blocks user accounts that use legacy authentication from signing in.
- **Block device code flow**: The agent looks for any policy that blocks device code flow authentication.
- **Risky users**: The agent checks for a Conditional Access policy that forces password change for high-risk users. This requires an Entra ID P2 license.
- **Risky sign-ins**: The agent checks for a Conditional Access policy that enforces MFA for high-risk sign-ins. This requires an Entra ID P2 license.

- **Risky agents:** The agent looks for other risky agents and suggests blocking them from accessing the environment. This requires an Entra ID P2 license.
- **Policy consolidation**: The agent scans the policies for overlapping settings and suggests policy merge.
- **Deep analysis**: The agent looks for policies covering key scenarios and identifies policies that have gaps in coverage due to too many exceptions or possible lockout due to no exceptions.
- **Deep analysis for MFA gaps**: The agent scans all policies to identify users who are not covered by any MFA policy. This analyses the entire tenant configuration and is not limited to the last 24 hours.
- **Least-privileged access for agent identities**: The agent identifies agent identities that have overprivileged Microsoft Graph permissions and recommends least privileged permissions to be applied. It recommends removing unused permissions.

The agent does not make any changes to the configuration unless an administrator approves the suggestions. If the agent creates any new policies, they are created in *report-only* mode.

Prerequisites

The following are the prerequisites to running the Conditional Access optimization agent:

- Microsoft Entra ID P1 license.
- At least 1 SCU.
- Appropriate Microsoft Entra role.
    - Security Administrator or Global Administrator to onboard the agent the first time.
    - Security Reader or Global Reader can view the agent and any suggestions. They cannot take any actions.
    - Conditional Access Administrator, Security Administrator, or Global Administrator can view the agent and act on suggestions.
- Using device-based controls requires Microsoft Intune licenses.

Limitations

Before installing the agent please be aware of the following limitations:

- Once the agent is started, it cannot be stopped or paused.
- For policy consolidation, the agent looks at 40 similar policy pairs.
- Scanning is limited to a 24-hour period.
- The agent can evaluate up to 300 users and 150 applications in a single run.
- The agent suggestions cannot be modified or overridden.
- Now let's proceed with learning how to onboard the agent.

Onboarding the agent

Following are the steps to enable the agent in your tenant:

1. Log in to `https://entra.microsoft.com` as a **Security Administrator**.
2. In the left pane, click on **Agents**.
3. You will see the **Conditional Access Optimization Agent** in the right pane. Click on **View details** as shown in the following screenshot:

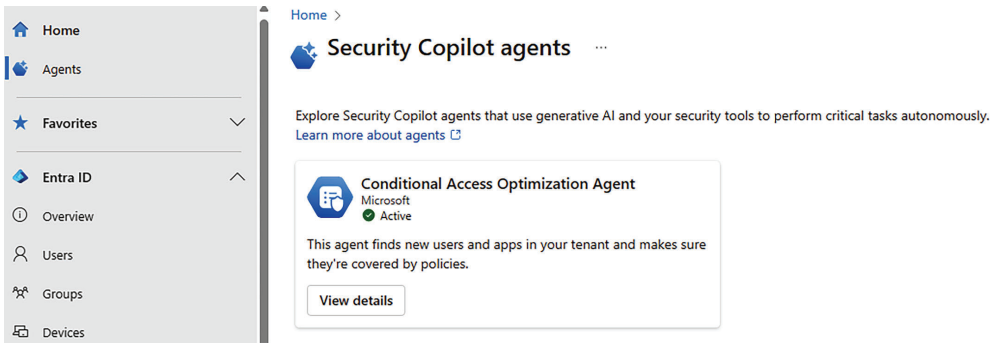


Figure 5.8: Security Copilot agents

4. Click on **Start agent** to start the first run. The following screenshot shows the agent page after it has completed at least one run:

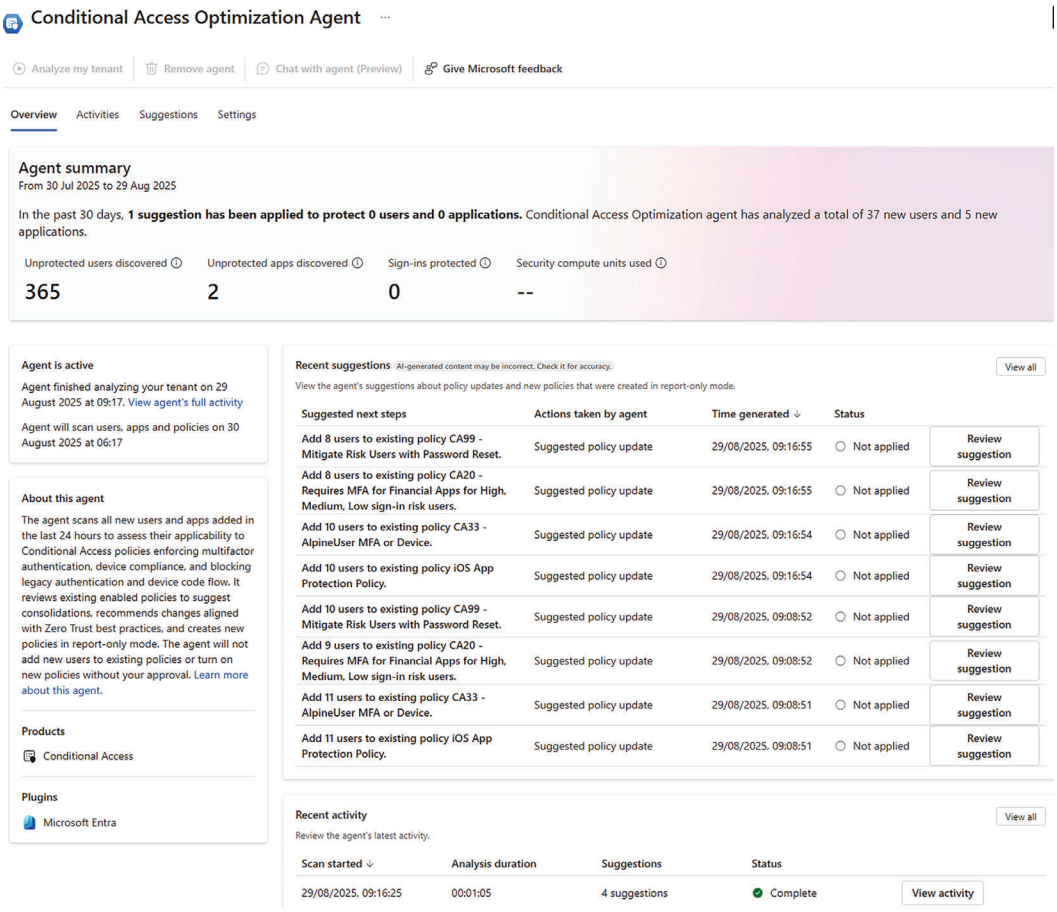


Figure 5.9: Conditional Access Optimization Agent

Adjusting settings

Once the agent has been enabled, you can adjust its settings by clicking on **Settings.** The following settings are available.

Trigger

The agent is scheduled to run every 24 hours from the time it was first enabled. For example, if you first enable the agent at 1:00 PM, it will run every day at 1:00 PM. This can be changed by unchecking the box **Schedule the agent to run every 24 hours**. Once this is done, the agent can be run manually.

In addition to running on schedule, the agent can also be enabled to run if there are changes to turned-on policies by checking the box **Automatically analyze tenant each time there are changes to policies that are turned on**.

Microsoft Entra objects to monitor

By default, the agent monitors newly created users and applications. This can be changed by unchecking the relevant options under this section.

Agent capabilities

This setting specifies whether the agent will create new Conditional Access policies in report-only mode or not. This setting is on by default. You can turn this off by unchecking the box **Allow agent to autonomously create new policies in report-only mode**.

Phased rollout

When the agent creates new policies in report-only mode, the policy is rolled out in phases. Gradual deployment minimizes the chance of a mass disruption to end users and saves time by reducing the need for manual analysis and planning. The agent intelligently assigns groups to different phases; however, administrators can review and edit the group selection. Administrators can also configure the days between phases. Phased rollout is on by default. It can be turned off, if required.

Once the agent selects the groups for each phase, it creates a duplicate Conditional Access policy that only includes the group of the first phase. The original policy remains in report-only mode to enable administrators to collect data. When the deployment advances to the next phase, the next batch of groups is added to the enabled Conditional Access policy. The agent continues to monitor each stage for sign-in failures. If the successful sign-ins drop below 90%, the agent stops the deployment, and the enabled policy is changed to report-only mode. Administrators can then review logs to determine the cause of sign-in failures before restarting the rollout.

Passkey adoption campaigns

The agent can help organizations develop adoption campaigns that guide users to adopt stronger authentication methods. The agent can assess user and device readiness, generate a deployment plan and guide users through the required steps. It can also create a Conditional Access policy.

Passkeys must be enabled in the **Authentication methods** policy in your tenant. Once done check the box **Allow agent to create passkey adoption campaigns**. After this setting is enabled, the agent analyzes the tenant to identify eligible users. Users having privileged administrator roles are automatically targeted. Once the campaign is ready, it shows up as one of the suggestions on the agent overview page. From this suggestion, the administrator can

adjust the settings like editing the included users list, grace period, and more. They can then deploy and monitor the campaign.

Once the campaign is active, the agent guides users to adopt passkeys. Users needing device updates receive notifications in Microsoft Teams prompting them to update their device, and users needing to set up a passkey receive notifications in Microsoft Teams with complete guidance on setting up passkeys. Once at least one user is ready, the agent creates a Conditional Access policy that enforces passkeys. This policy is created in report-only mode.

Notifications

The agent can send Teams messages to specified users and groups when new suggestions are available.

Knowledge sources

Organizations can now upload a PDF or Word document containing specific information about their organization. This can include policies and guidelines. The agent uses these files to generate suggestions that are more relevant to the organization.

Administrators can also give the agent standing instructions that the agent will consider while providing suggestions. You could include custom instructions to exclude members of certain groups from being evaluated for inclusion in a Conditional Access policy. For example, you might want to exclude guest users from being included in a Conditional Access policy.

Plugins

The agent integrates with ServiceNow and can automatically create a change management request for each suggestion. The ServiceNow connector needs to be configured for Security Copilot before the agent can start creating tickets.

Permissions

The agent operates under its own identity. This page shows the permissions the agent identity has in the tenant.

Review suggestions

The Conditional Access optimization agent provides suggestions to create or update Conditional Access policies. It also creates reports for activities related to those policies. An administrator needs to review these suggestions and decide whether to accept or reject them. Depending on the settings and your environment, the agent might run and not find any unprotected users or applications and hence not recommend any changes. In other cases, it might find unprotected users or applications and create new Conditional Access policies in report-only mode, suggest modifying an existing policy, or suggest merging overlapping policies. With each suggestion, the agent provides detailed reasons for making those suggestions so admins can make informed decisions. To review any suggestion, click on the

Review suggestion button as shown in *Figure 5.9*. The following actions can be taken from the fly out pane as shown in *Figure 5.10*:

1. Review the details of the suggestion by clicking on **Review policy changes**. This page lists the users and other details of the policy that will change if the suggestion is applied. Policy details can be viewed both in a list format as well as in JSON format, with the suggested changes highlighted. If a policy change affects users or applications, a JSON file containing the affected users or applications can be downloaded.
2. Click on **Apply suggestions** to accept the policy suggestions and make changes.
    - If the recommendation was to modify an existing policy, choosing this option will make changes to the policy.
    - When the agent suggests a new policy, it creates the policy in report-only mode. Admins can review the policy and choose to turn it on from within the agent by clicking on **Turn on policy**.
3. Click on **View agent's full activity** to open the agent activity map. This helps admins understand the logic behind the suggestion so that they can make informed decisions about whether to apply the suggestion or not.
4. Click on **Review phases** to view and edit the groups included in each phase.
5. Click on **Chat with agent** to interact with the agent in natural language. This makes it easier to understand the suggestions, request more information, and apply the recommendations. Following are some sample prompts that you can use:
    - *Prioritize the suggestions.*
    - *Tell me more about the first suggestion.*
    - *Why was this policy selected for update and not others?*
6. Click on **Policy impact** to see a graphical view of the potential impact of the policy.

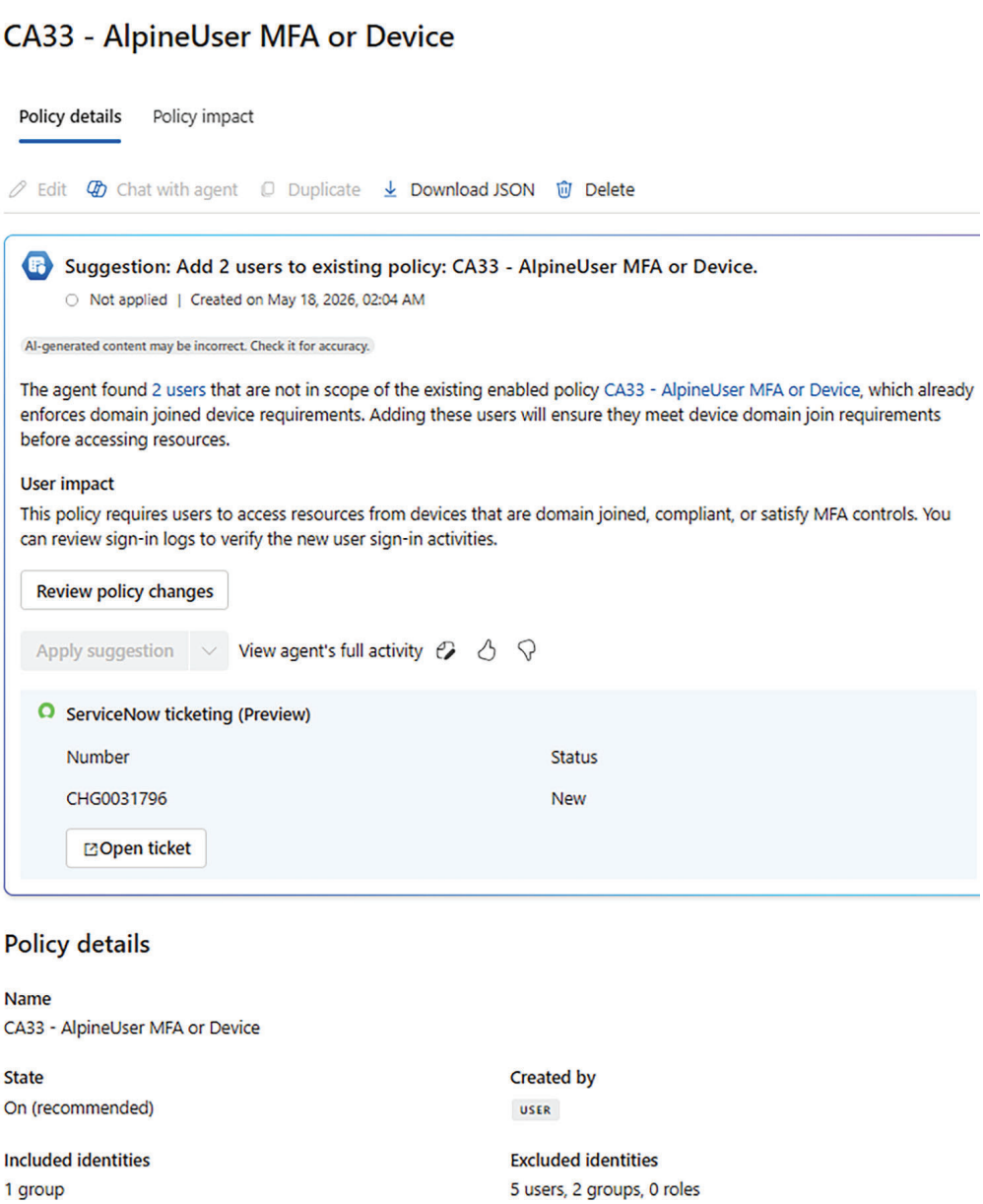


Figure 5.10: Review policy suggestions

Conditional Access optimization helps administrators enhance and streamline their organization's access policies. It provides actionable recommendations, such as modifying existing policies or suggesting new ones in report-only mode, allowing for careful review

before implementation. The agent offers transparency by displaying its full activity map and logic, empowering admins to make informed decisions. Users can review and edit groups for phased rollouts, chat with the agent for clarification, and visualize the potential policy impact through graphical summaries. Overall, the agent simplifies policy management and supports proactive security optimization.

Microsoft Entra Agent ID

As organizations accelerate the adoption of AI agents across productivity, security, and business operations, a critical challenge emerges: how do you manage, secure, and govern autonomous software that acts on behalf of users and systems? Microsoft Entra Agent ID addresses this gap by introducing a dedicated identity framework for AI agents, built on top of the proven Microsoft Entra ID platform.

Unlike traditional application identities or service principals, Agent ID treats AI agents as first-class identities alongside users, devices, and applications. This means every agent, whether built in Microsoft Copilot Studio, Azure AI Foundry, or through third-party platforms using the Entra SDK, receives a verifiable, auditable, and governable digital identity.

The agent identity architecture follows a hierarchical model designed for scalable, centralized management. Understanding these constructs is essential for IT administrators planning to onboard AI agents into their identity infrastructure.

Concept	Description
Agent Identity	The primary account used by an AI agent to authenticate to systems and access resources. Agent identities do not have credentials of their own; they authenticate using tokens issued by their agent identity blueprint.
Agent Identity Blueprint	A reusable template and authentication foundation in Entra ID. The blueprint holds credentials, acquires tokens on behalf of all agent identities created from it, and serves as the policy enforcement point for Conditional Access.
Blueprint Principal	A service principal object created when a blueprint is registered in a tenant. It enables the blueprint to acquire tokens and appear in audit logs within that tenant.

Concept	Description
Agent User Account	An optional user-type account paired 1:1 with an agent identity. Required only when the agent must access systems that need a user object, such as Exchange Online mailboxes or Teams channels.
Agent Registry	A centralized directory that stores agent metadata, facilitates controlled discovery, and enables agent-to-agent collaboration using the A2A protocol. It serves as the authoritative control plane for all operational agents.

Table 5.1: Agent ID core concepts

Agents created in Microsoft first-party platforms such as Copilot Studio and Azure AI Foundry automatically receive an Agent ID upon creation and appear in the Entra admin center. For non-Microsoft platforms, the Entra SDK for Agent ID enables programmatic registration and management.

Organizations have historically relied on two identity paradigms: human identities tied to credentials and lifecycle events, and application identities (service principals) designed for long-lived, stable services. AI agents break both models:

- **Dynamic creation at scale**: Agents may be spun up and destroyed thousands of times per day, making manual service principal management impractical.
- **Autonomous behavior**: Agents act without per-request human prompts, requiring authorization and approval gating that traditional apps do not need.
- **Hybrid access patterns**: Some agents use delegated (on-behalf-of) access, while others operate autonomously with app-only permissions, and many shift between both modes.

Agent ID addresses these challenges by providing purpose-built identity constructs that carry richer context, including metadata such as purpose, environment, and ownership, along with custom security attributes that integrate directly with policy enforcement.

Microsoft Entra Agent ID extends the full breadth of Entra security controls to agent identities. The following capabilities are available.

Capability	Description
Conditional Access	Extends Zero Trust policies to agent token requests. Supports agent risk as a condition and block as a grant control. User-based CA policies apply when agents operate on behalf of users. Conditional Access for agents requires Entra ID P1 license.
Identity Protection	Detects anomalous agent behavior including unfamiliar resource access, sign-in spikes, failed access attempts, and sign-ins by risky users. Flags agents for risk with remediation through CA policies. Identity Protection for agent requires Entra ID P2 license.
Identity Governance	Lifecycle management from deployment to decommissioning. Includes owner and sponsor assignment, access packages, access reviews, and automated handling of inactive agents to prevent orphaned identities. Identity Governance for agents requires Entra ID P1 license.
Global Secure Access	Logs all agent network calls, enforces consistent access policies, and provides prompt injection protection and network DLP. Integrates with SIEM and Microsoft Sentinel. This capability requires Microsoft Entra Internet Access or Microsoft Entra Private Access license.

Capability	Description
Session Management	Enables revocation of compromised agent credentials, dynamic adaptation to permission changes, and Continuous Access Evaluation (CAE) for near real-time token revocation.

Table 5.2: Agent ID capabilities

For IT administrators, the Entra admin center provides a dedicated Agent ID section with an overview dashboard, agent identity listings, the Agent Registry, and agent collections filtered by trust level and visibility. Conditional Access policies can target agent identities using agent-specific risk signals, and block controls can prevent high-risk agents from accessing sensitive resources.

To begin working with Agent ID, administrators need the following:

- A Microsoft Entra ID tenant
- Access to Microsoft Copilot Studio, Azure AI Foundry, or the Entra SDK for Agent ID for non-Microsoft agent platforms

Microsoft Entra Agent ID extends the same identity, access, and governance controls you already rely on for your workforce to AI agents. By treating agents as first-class identities, organizations gain the visibility and policy enforcement needed to scale AI adoption securely.

Summary

In this chapter, we learned about the Generative AI capabilities available in Microsoft Entra. Microsoft Security Copilot assists identity administrators by enabling them to ask natural language questions to get a quick understanding of their identity landscape. AI agents act as assistants that run autonomously and perform mundane and repetitive tasks, freeing up administrators' time for activities that require human judgment. This chapter also introduced the new concept of Microsoft Entra Agent ID and how agents are treated as first class citizens in Microsoft Entra. In the next chapter, we will learn about Microsoft Entra's identity governance capabilities.

Exercises

1. Your organization uses Microsoft Entra ID and wants to adopt generative AI capabilities where identity administrators can ask natural language questions to get insights about the identity landscape. Which tool is best suited for this purpose?
    a. Microsoft 365 Copilot
    b. Chat GPT
    c. Microsoft Security Copilot
    d. Google Bard
2. Your organization decides to adopt Microsoft Security Copilot. What is the first step to enable you to start using Microsoft Security Copilot?
    a. Go to `https://securitycopilot.microsoft.com` and start the conversation with Microsoft Security Copilot.
    b. Enable capacity by provisioning Security Compute Units (SCUs).
    c. Contact Microsoft and buy licenses for Microsoft Security Copilot.
    d. Check if the organization has an Azure subscription.
3. Your organization has provisioned 3 SCUs for Microsoft Security Copilot. You are using it actively but while chatting with Copilot you receive a message "You have reached your provisioned Security Compute Unit (SCU) capacity. Please provision additional SCUs to continue using Microsoft Security Copilot." There is no budget to provision additional SCUs. What will you do?
    a. Wait till the hour is up and then continue.
    b. Add overage SCUs.
    c. Add more provisioned SCUs.
    d. Contact Microsoft Support to fix the problem.

Answers

1. c
2. d
3. a

Additional resources

- Microsoft Security Copilot: `https://learn.microsoft.com/en-us/copilot/security/`
- Security Copilot in Microsoft Entra: `https://learn.microsoft.com/en-us/entra/fundamentals/copilot-security-entra`
- Security Copilot Ninja training: `https://techcommunity.microsoft.com/blog/securitycopilotblog/how-to-become-a-microsoft-security-copilot-ninja-the-complete-level-400-training/4106928`
- Microsoft Entra Agent ID: `https://learn.microsoft.com/en-us/entra/agent-id/what-is-microsoft-entra-agent-id`
- Entra Agent ID SDK: `https://learn.microsoft.com/en-us/entra/msidweb/agent-id-sdk/overview`

Get this book's PDF version and more

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.





Note: Keep your invoice handy. Purchases made directly from Packt don't require an invoice.

Part 2

The Entra Governance Stack

Part 2 explores the governance and control mechanisms that ensure identities receive the right access, at the right time, with the right level of oversight. This section examines how Microsoft Entra Entitlement Management streamlines access to applications and resources through structured access packages. It then delves into Lifecycle Workflows, enabling automated, policy-driven identity processes from onboarding to offboarding. Finally, it covers Privileged Identity Management, which safeguards elevated roles and sensitive operations. Together, these chapters provide a comprehensive understanding of how Microsoft Entra enforces accountability, reduces risk, and strengthens organizational security through modern identity governance.

This part of the book includes the following chapters:

- *Chapter 6, Microsoft Entra Entitlement Management*
- *Chapter 7, Microsoft Entra Lifecycle Workflows*
- *Chapter 8, Microsoft Entra Privileged Identity Management*

6

Microsoft Entra Entitlement Management

Identity Governance (**IG**) is a critical aspect of modern enterprise security and operational efficiency. As organizations increasingly rely on digital platforms and cloud services, the need to manage user identities, access rights, and entitlements has become more complex and essential. Effective identity governance ensures that only authorized individuals have access to sensitive data and resources, reducing the risk of data breaches, insider threats, and compliance violations. By implementing robust policies and controls, organizations can enforce the principle of least privilege, ensuring that users have the minimum level of access necessary to perform their jobs.

Additionally, identity governance streamlines the onboarding and offboarding processes, making it easier to grant or revoke access as employees join, move within, or leave the organization. This not only enhances security but also improves operational agility and user productivity. Automated identity governance solutions provide continuous monitoring and auditing capabilities, enabling organizations to detect anomalies and respond to potential security incidents swiftly.

In this chapter, we will cover:

- Microsoft Entra ID Governance
- Principle of least privilege
- Entitlement management
- Access reviews

Microsoft Entra ID Governance

Microsoft Entra ID Governance is a comprehensive identity governance solution designed to help organizations manage, monitor, and control user identities and access within their digital environments. As the complexity of enterprise infrastructures grows, so does the challenge of ensuring that only the right individuals have the appropriate levels of access to critical resources. Microsoft Entra ID Governance addresses these challenges by providing advanced tools for automating and enforcing access policies, streamlining the user lifecycle, and maintaining regulatory compliance.

At its core, Microsoft Entra ID Governance empowers organizations to apply the principle of least privilege, ensuring users are granted only the permissions necessary for their roles. The platform offers capabilities such as automated provisioning and deprovisioning, access reviews, entitlement management, and privileged identity management. These features enable IT administrators to efficiently grant, review, and revoke access as users join, transition, or leave the organization, reducing the risk of unauthorized access and data breaches.

It helps organizations address the following critical concerns:

- Ensuring that users have access to the right resources.
- Monitoring how the users are using that access.
- Implementing organizational controls to manage access.
- Ensuring auditors can verify that the controls are working effectively.

With Microsoft Entra ID Governance, organizations can govern the identity and access lifecycle while providing secure privileged access for administration.

Each identity follows a lifecycle that begins when a user joins an organization and ends when they depart. Upon joining, an identity is created—this stage is referred to as the *joiner*. Users are then granted access necessary to fulfill their job responsibilities. During their time with the organization, users may transition between different roles; this is known as the *mover* stage. At this point, access must be updated to reflect the requirements of the new role, while access from previous roles should be revoked. When users leave the organization, their identity is removed from the system—referred to as the *leaver* stage—and all associated access to organizational resources is withdrawn. This process is illustrated in the following figure:

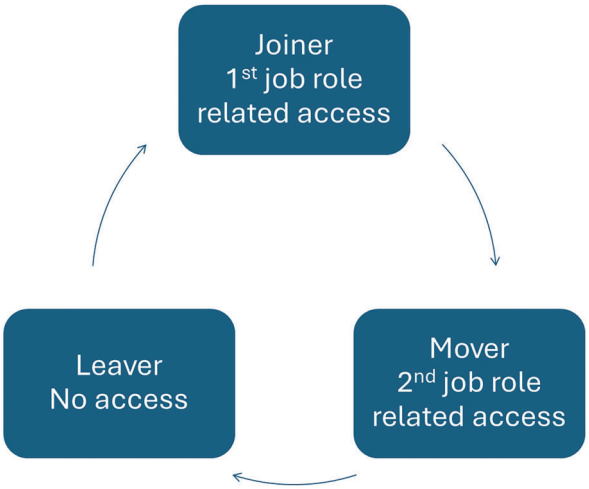


Figure 6.1: Identity and access lifecycle

Most organizations struggle with managing these changes at scale. They must ensure that the users' identities are provisioned and reprovisioned quickly and accurately to minimize risk and to ensure that the users are productive as soon as possible. Using **Entitlement Management Access Packages** and **Access Reviews** features of Microsoft Entra ID Governance, organizations can manage provisioning of new users at scale, ensuring that users have access to the resources they need to do their job, maintain user access as they move across roles and remove access once they leave the organization.

Microsoft Entra ID Governance allows organizations to meet the following use cases:

- **Govern employee and guest lifecycle**: Governing the lifecycle of employee identities is the core requirement of effective identity governance. Similar governance processes also need to be applied to guest accounts in the organization. These guest accounts could belong to business partners, contractors, or suppliers. Microsoft Entra ID Governance offers the same capabilities to govern guest user access as it does for employees.
- **Govern access to applications**: Using the features of Microsoft Entra ID Governance, organizations can manage access beyond what was originally provisioned for the user. This also enables the organization to efficiently scale and enforce access policies and controls on an ongoing basis.

These cases demonstrate the importance of identity governance in maintaining security and compliance.

The Microsoft Entra ID Governance dashboard displays usage information about the ID governance features configured in the tenant. It provides an overview of the state of ID governance including action buttons and links to documentation. It is accessible from the Entra admin portal by navigating to **ID Governance | Dashboard**. The following screenshot shows the dashboard:

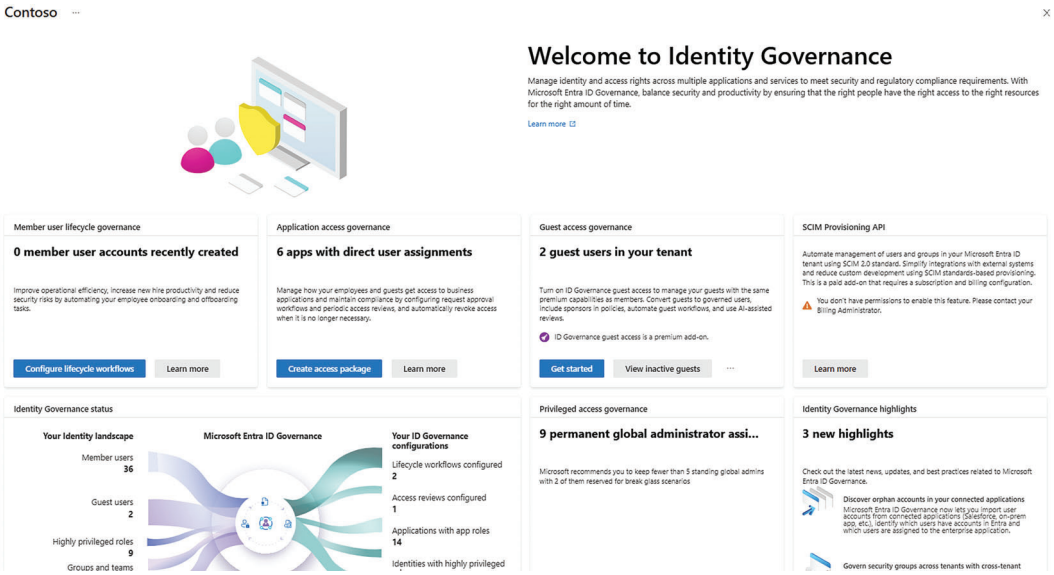


Figure 6.2: ID Governance dashboard

The dashboard displays data about governance of workforce users, guest users, privileged identities, and application access. It highlights the ID Governance features that are configured in the tenant. If a feature is not configured, it shows a button to open the configuration page for that feature.

Whether you are just getting started with ID Governance or have already deployed some capabilities, this dashboard helps you understand the coverage, identify implementation gaps, and assists you in assessing the complexity of your IT landscape.

Principle of least privilege

The principle of least privilege is a foundational concept of identity governance that ensures users are granted only the minimum access necessary to perform their job functions. By limiting permissions, organizations can reduce the risk of accidental or malicious misuse of sensitive data and resources. This approach helps contain potential security breaches, as compromised accounts are restricted in what they can access. Implementing least privilege also supports compliance with regulatory requirements by enforcing strict access controls.

Regularly reviewing and adjusting user permissions is essential to maintain this principle, especially as employees change roles or leave the organization, ensuring that unnecessary access is promptly revoked.

The following are some key concepts of the principles of least privilege:

- **Access to only the required resources**: This is the foundation of the principle of least privilege. Users are given access to resources only if they have a genuine need to access those resources to fulfill their job duties. This prevents unauthorized data access and limits the impact of a security breach. **Lifecycle workflows** is a feature in identity governance that helps organizations automate lifecycle processes.
- **Role-based Access Control (RBAC)**: Access is based on the role and job functions of the user. Each role has the minimum permissions assigned that are necessary to fulfill job requirements. Microsoft Entra RBAC manages access to Microsoft Entra resources.
- **Just-In-Time access**: Users are granted access to resources only for the duration for which they are needed and revoked when they are no longer required. This minimizes the timeframe during which attackers could potentially exploit elevated privileges. **Microsoft Entra Privileged Identity Management** is a solution that helps manage, control, and monitor just-in-time access.
- **Regular audit and review**: Organizations must perform periodic reviews of user access to ensure that they still require the permissions that they have. This helps ensure that there is no permission creep. **Access reviews** is a feature in Microsoft Entra ID Governance that helps organizations automate access reviews.
- **Default deny**: The principle of least privilege works on default deny. This means that, by default, users are denied access, and access is explicitly granted only for approved purposes.

By following these principles, organizations can reduce risk and ensure alignment with business needs.

Entitlement management

When users join an organization, they require access to various resources such as SharePoint sites, Teams channels, and applications. New employees may not initially know which resources are necessary. After joining, they often need time to determine what access is required and to identify the appropriate approvers for their access requests. This process can delay the point at which the employee becomes fully productive. The situation can become more complex when collaborating with other organizations, as it may be unclear who in the external organization requires access to specific resources.

Entitlement management is a Microsoft Entra ID Governance feature designed to streamline identity and access lifecycle management for both users and guests. It automates the processes of requesting and assigning access by utilizing access packages, which are organized within catalogs to oversee and maintain user access.

Understanding catalogs

A catalog is a container of resources and access packages. A catalog is created when all related resources need to be grouped together. For example, you might want to group all marketing resources into one catalog. This catalog might include Microsoft 365 (M365) groups and teams related to marketing, marketing SharePoint sites, and some marketing applications. This catalog can then be used to create access packages for marketing users. An access package might contain all or a subset of resources from the catalog.

By default, a Global Administrator and Identity Governance Administrator can manage all aspects of entitlement management such as creating catalogs and access packages. However, they may not know to which business resources access has to be granted and for how long. This is further complicated as each business unit may have different requirements. An IT administrator can delegate the task of creating and assigning catalogs and access packages to administrators in the business units.

There are three ways of delegating access.

- The Identity Governance Administrator can create the catalog and then assign catalog owners to add resources and manage the catalog going forward.
- If resources don't have owners, administrators can create catalogs and add the resources. They can then assign catalog owners to manage the catalog going forward.
- If resources have owners, administrators can grant the **Catalog Creator** role to non-IT administrators who can then create their own catalogs.

Understanding access packages

An access package is a bundle of all resources that employees might need to perform their job duties. The following resources can be included in an access package:

- Microsoft Entra security groups
- M365 Groups and Teams
- Microsoft Entra enterprise applications
- SharePoint Online sites
- Microsoft Entra roles (Preview)
- Azure Resources (Preview)
- API Permissions

An administrator can create an access package containing the resources required for a job role. For example, an access package for a user in the marketing department could include membership of the marketing Teams channel, membership of marketing security groups, access to the marketing application, and the marketing SharePoint site. Policies can then be defined based on which the assignment of the access package can be controlled.

A policy can define:

- Which users or guests can request access to this access package.
- Whether the request is automatically approved or requires approval by designated approvers.
- Whether and when the access package assignment expires.

Connected organizations

A connected organization is an external organization that your organization works with and needs to share resources such as applications and SharePoint sites. Mostly, users in external organizations do not exist in your Microsoft Entra directory. You can use entitlement management to bring them into your directory as needed.

Connected organizations provide a way for users in these external organizations to request an access package and be able to access applications and SharePoint sites. There are four methods for defining users that make up a connected organization:

- Users from another Microsoft Entra tenant.
- Users from a non-Microsoft directory configured for SAML/WS-Fed IdP federation.
- Users from a non-Microsoft directory whose email addresses share the same domain name. Email one-time passcode authentication must be enabled for these users to allow authentication when requesting access and later when accessing resources.
- Users with a Microsoft account such as *hotmail.com*.

Using connected organizations, administrators do not need to invite individual guest users to their tenant.

Adding a connected organization

To add an external Microsoft Entra directory or domain as a connected organization, users must have the **Global Administrator** or **Identity Governance Administrator** role. Follow the steps below to add a connected organization:

1. Log in to `https://entra.microsoft.com` and navigate to **ID Governance** | **Entitlement management** | **Connected organizations**.
2. Click on **Add connected organizations**.

3. On the **Basics** page, enter a **Name** and **Description**. The state will be automatically set as **Configured**.

    a. A configured connected organization is one that is fully connected and allows users to request access. It has been manually created and configured by the administrator.

    b. A proposed connected organization is an automatically created connected organization that the administrator has not added. This happens when an external user who is not a part of any connected organization is assigned to or requests an access package.

    Refer to the picture below. Click on **Next: Directory + domain**.

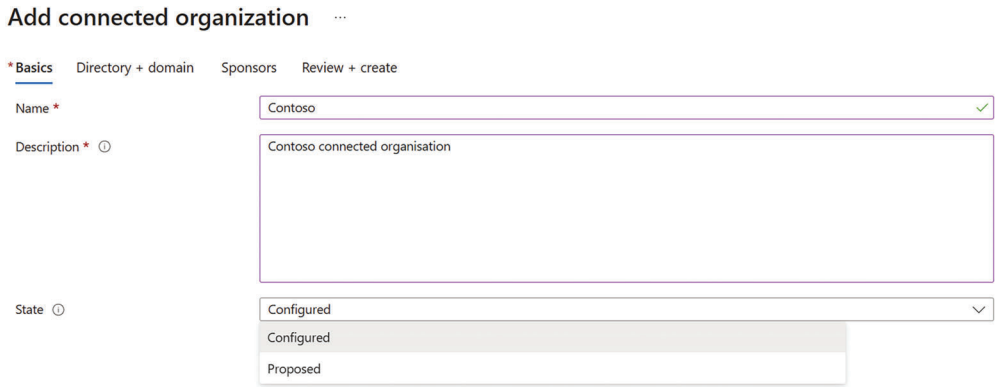


Figure 6.3: Connected organization basics

4. Click on **Add directory + domain**. In the fly out pane, type the name of the external Microsoft Entra domain name. You can also add a non-Microsoft Entra domain name. Ensure that you type the entire domain name correctly. The following screenshot shows examples of a Microsoft Entra ID domain and non-Microsoft Entra domain name being added as connected organizations. Once done, click on **Add** and then click on **Select**. Click **Next: Sponsors**.

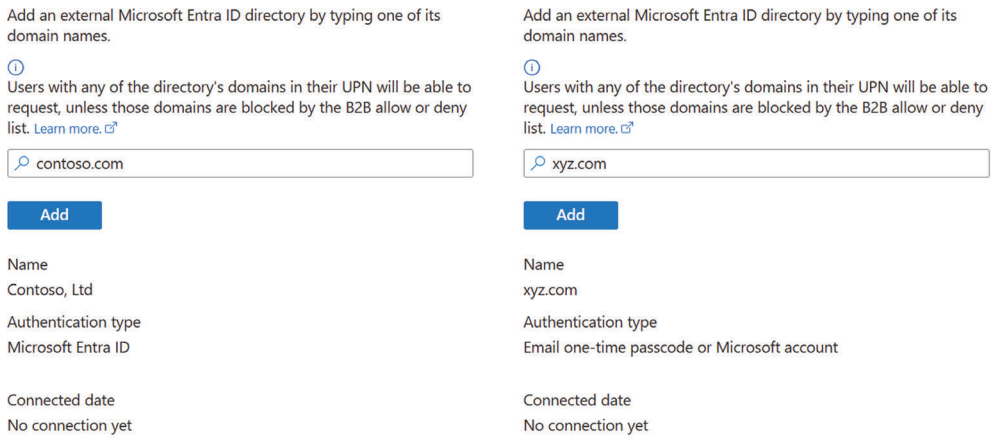


Figure 6.4: Adding connected organization domain name

5. Sponsors are internal or external individuals who manage the relationship between the two organizations. Internal sponsors are users within your organization. External sponsors are external guests that already exist in your directory and are the points of contact for these connected organizations. Sponsors can be used as approvers when users in the connected organizations request an access package. Refer to the picture below. Click **Review + create**.

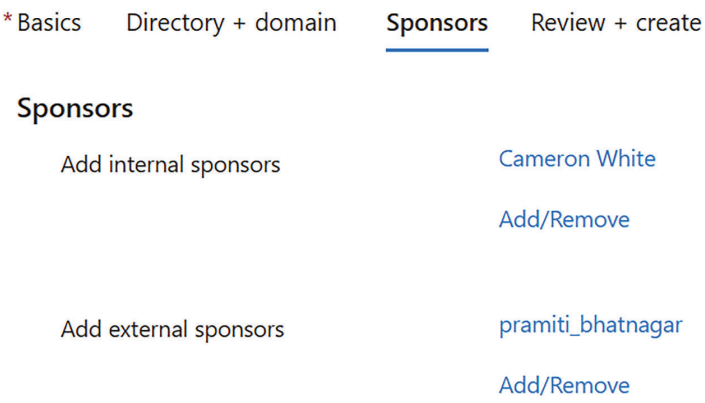


Figure 6.5: Adding internal and external sponsors

6. On the **Review + create** page, click on **Create**.

Roles in entitlement management

Entitlement management has roles that allow non-IT administrators to manage catalogs and access packages. These roles are summarized in the following table:

Role	Description
Catalog creator	Can create and manage catalogs. Typically assigned to non-IT administrators to create catalogs. The person who creates the catalog automatically becomes the first catalog owner and then can add more owners. They can only see and manage the catalogs they create.
Catalog owner	Can add, edit, and manage access packages and other resources within a catalog. They must be listed as the owners of the resources before they can add the resource to a catalog.
Catalog reader	Can view existing access packages within a catalog.
Access package manager	Can edit and manage existing access packages within a catalog.
Access package assignment manager	Can edit and manage existing access packages' assignments.

Table 6.1: Entitlement Management roles

Licensing requirements

Entitlement management requires a **Microsoft Entra ID Governance or Entra Suite** license. The following are the licensing requirements to be able to use Microsoft Entra entitlement management:

- Each user that can request an access package must have a license.
- Identity Governance Administrators do not need a license.
- A license is required for *each* auto-assignment policy.

It is important to note that users do not need to be assigned licenses individually. The tenant must have enough licenses for users in scope.

Getting started with entitlement management

Now that we understand the components of entitlement management, let's walk through the steps of creating a catalog, assigning non-IT administrators, and creating and assigning access packages. We will also walk through the end user experience of requesting access.

Delegating to catalog creator

If you would like to delegate creation of catalogs to non-IT administrators, you will have to give them the **Catalog Creator** role. Follow the steps below to add catalog creators:

1. Log in to `https://entra.microsoft.com` and navigate to **ID Governance** | **Entitlement management** | **Roles and administrators**. At the top, click on **Add catalog creator**.
2. From the list, select the users who you want to grant the catalog creator role to and click on **Select**. The selected user will now be able to create catalogs.

You should have the **Identity Governance Administrator** or **Global Administrator** role for this.

Allowing access to Microsoft Entra portal

By default, delegated roles like catalog creators cannot access the Microsoft Entra admin portal. To allow them to log in to the portal, follow the steps below:

1. Log in to `https://entra.microsoft.com` and navigate to **Entra ID** | **Users** | **User settings**.
2. As shown in the following screenshot, ensure the **Restrict access to Microsoft Entra admin center** toggle is set to **No**. Click **Save**.

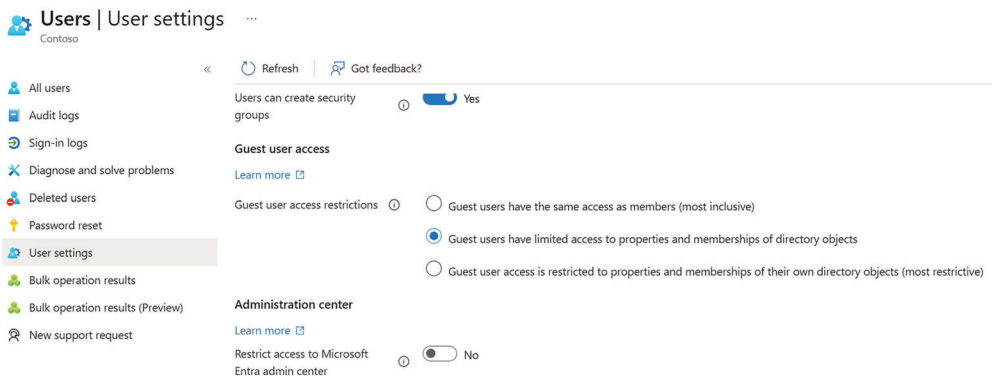


Figure 6.6: Allow access to Microsoft Entra portal

You should have the **Identity Governance Administrator** or **Global Administrator** role for this.

Creating a catalog

Users who have the **Identity Governance Administrator**, **Global Administrator**, or **Catalog Creator** can create a new catalog as per the following steps:

1. Log in to `https://entra.microsoft.com` and navigate to **ID Governance | Entitlement management | Catalogs**.
2. In the right pane, click on **New catalog**.
3. Give a **Name** and **Description** for the new catalog.
4. Make sure **Enabled** toggle is set to **Yes**.
5. If you want to make this catalog available for external users, switch **Enabled for external users** to **Yes**. Refer to the following screenshot:

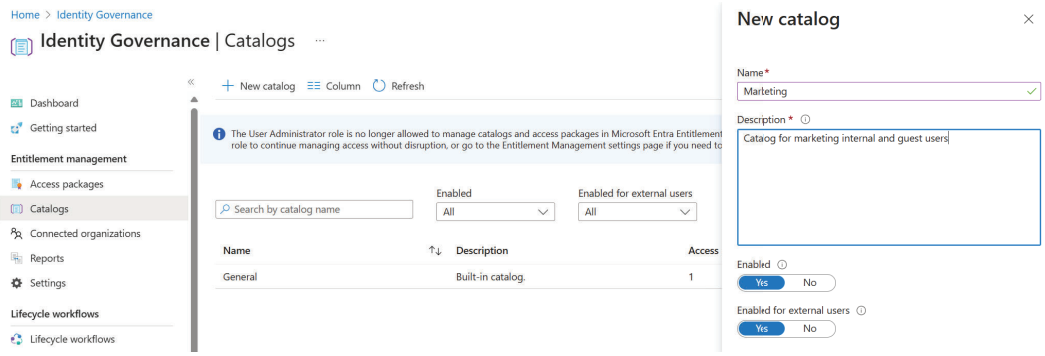


Figure 6.7: Catalog creation

6. Click **Create**.

Once the catalog has been created, access packages can be created based on the catalog.

Adding additional roles

The user who creates the catalog becomes the first catalog owner. They can optionally add additional roles to the catalog to further delegate management of the catalog to others. Follow the steps below.

On the **Catalogs** page, select the newly created catalog. Click on **Roles and administrators**. You will see the page in the following screenshot. From this page you can add catalog owners, catalog readers, access package managers, and access package assignment managers.

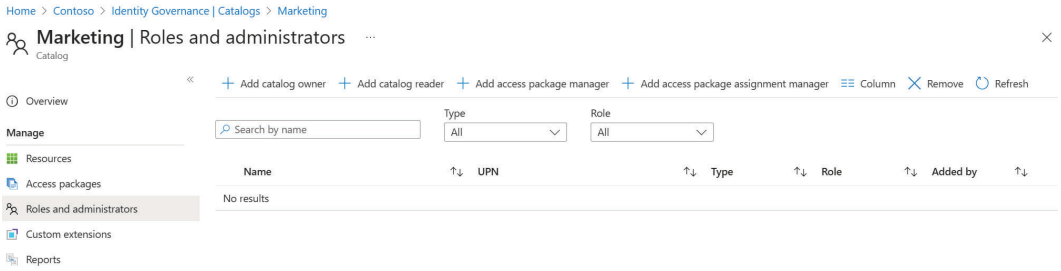


Figure 6.8: Add additional roles to catalog

As a best practice, it is recommended to add additional owners to catalogs.

Adding resources to the catalog

Now that the catalog has been created, resources should be added to the catalog. These resources will be available to be added to access packages. M365 groups and Teams, Applications, SharePoint Online sites, and Microsoft Entra roles are the resources that can be added to the catalog. Follow the steps below to add resources to the newly created catalog:

1. Click on the catalog that was just created and click on **Resources**. In the right pane, click on **Add resources**. At the top, click on each of the buttons to add the relevant resources. Refer to the following screenshot:

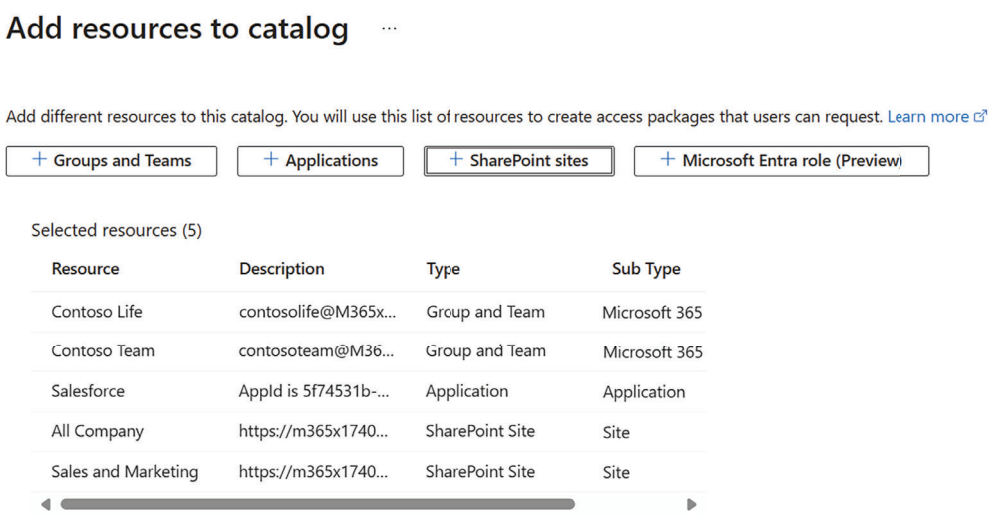


Figure 6.9: Add resources to the catalog

2. Once all resources have been added, click **Add**.

You need to have the **Identity Governance Administrator**, **Global Administrator**, or **catalog owner** role for this.

Adding resource attributes to the catalog

Administrators can collect optional information from requestors when they request access packages. This is done using resource attributes. The answers provided by requestors will be shown to the approvers and stamped on the requestor's user object in Microsoft Entra ID. All attributes configured require an answer when the user requests an access package. If an answer is not provided, the request cannot be submitted. To configure attributes for access requests, follow the steps below:

1. Click on the ellipsis next to the newly added resource and select **Require attributes** as shown in the following screenshot:

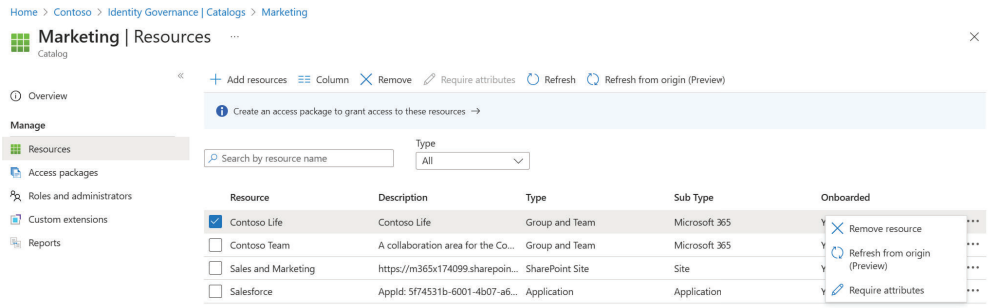


Figure 6.10: Adding attributes to resources

2. You can choose from **Built-in** or **Directory schema extension** attribute types. The built-in ones correspond to the default Microsoft Entra user profile attributes. Directory schema extension provides a mechanism to store additional custom data within Microsoft Entra user objects. If you choose **Built-in** attribute, in the **Attribute** dropdown list, select the attribute from the dropdown. If you choose **Directory schema extension** attribute, you will have to type the name of the attribute.

> **Note**
>
> To add directory schema extensions to a user account in Microsoft Entra ID Microsoft Graph or PowerShell can be used. This will only be required if you require an attribute that is not already present in the Microsoft Entra ID user object or synchronized from on-premises Active Directory.

3. In the **Default display string**, type the question you want the user to see.

4. Select the **Answer format**. You can choose from *Short text*, *Long text*, or *Multiple choice*.
5. Under **Attribute value is editable** select **Yes** to allow the attribute value to be modified during assignment and self-service requests. If **No** is selected and the attribute value is empty, the users can provide a value for the attribute. Once the value is saved, the attribute cannot be edited. If the attribute value is not empty, the user will not be able to update the attribute.
6. After making the changes, click **Save**. Refer to the following screenshot as an example:

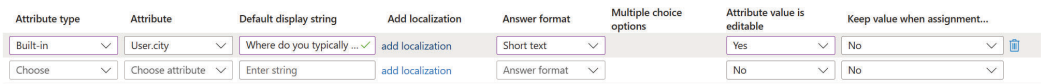


Figure 6.11: Editing attribute values

You need to have the **Identity Governance Administrator**, **Global Administrator**, or **catalog owner** role for this.

Creating an access package

Now that the catalog is ready, an access package can be created as per the following steps:

1. Log in to `https://entra.microsoft.com` and navigate to **ID Governance | Entitlement management | Access packages**.
2. In the right pane, click on **New access package**.
3. Enter the name and description of the access package and select the catalog you want to base the access package on. Click on **Next: Resource roles**. Refer to the following screenshot:

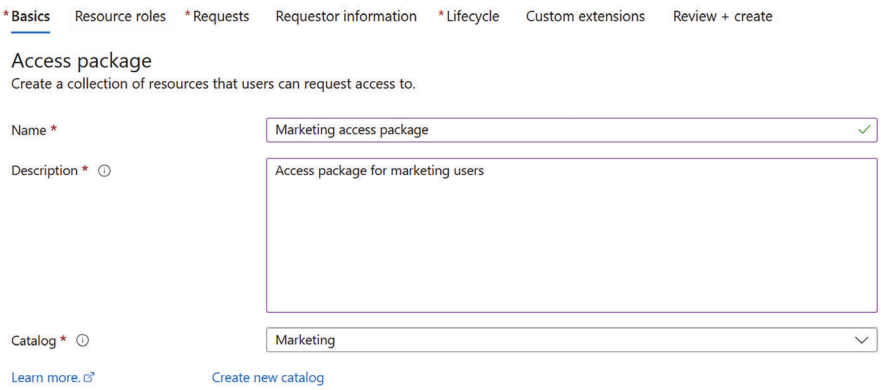


Figure 6.12: New access package

4. On the **Resource roles** page, click on each of the options to add the resources to the access package. The following screenshot shows the Groups and Teams available to be

added to the access package. Notice that these are the same resources that were added to the catalog above. You can add all available resources or choose a few. Click on **Select** to add the resource to the access package.

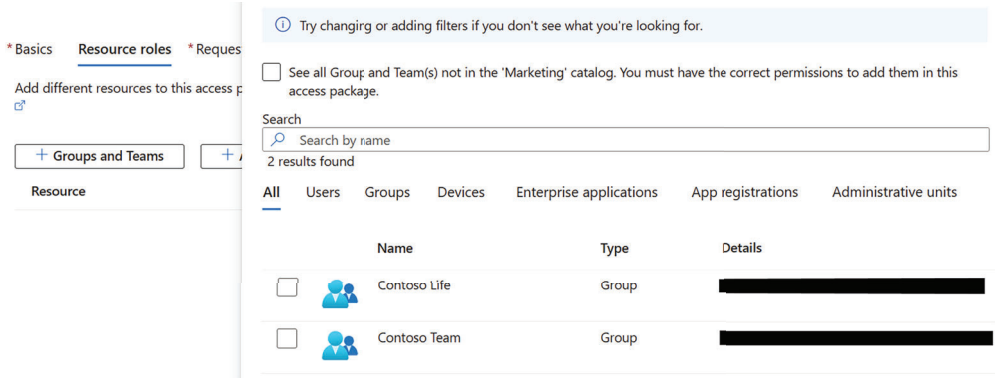


Figure 6.13: Add resources to access package

5. In the **Role** drop down menu, select the appropriate role you want to assign to the users on that resource. The roles differ by resource type. The following screenshot shows an example of the available roles for an M365 group, Salesforce application, and a SharePoint site. Once all roles have been selected, click **Next: Requests**.

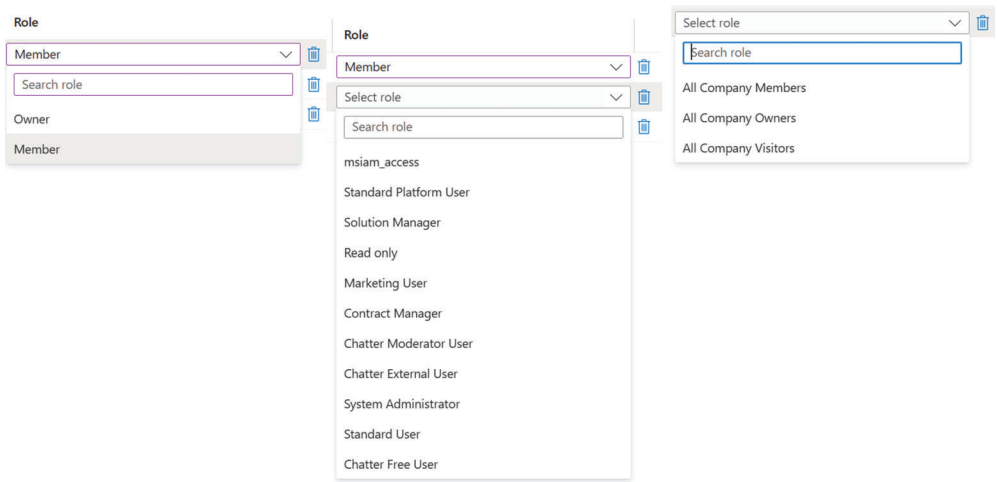


Figure 6.14: Add roles to resources

6. On the **Requests** page, you can select who can request this access package. The following options are available:

    a. **For users in your directory** – Review the options in the following screenshot:

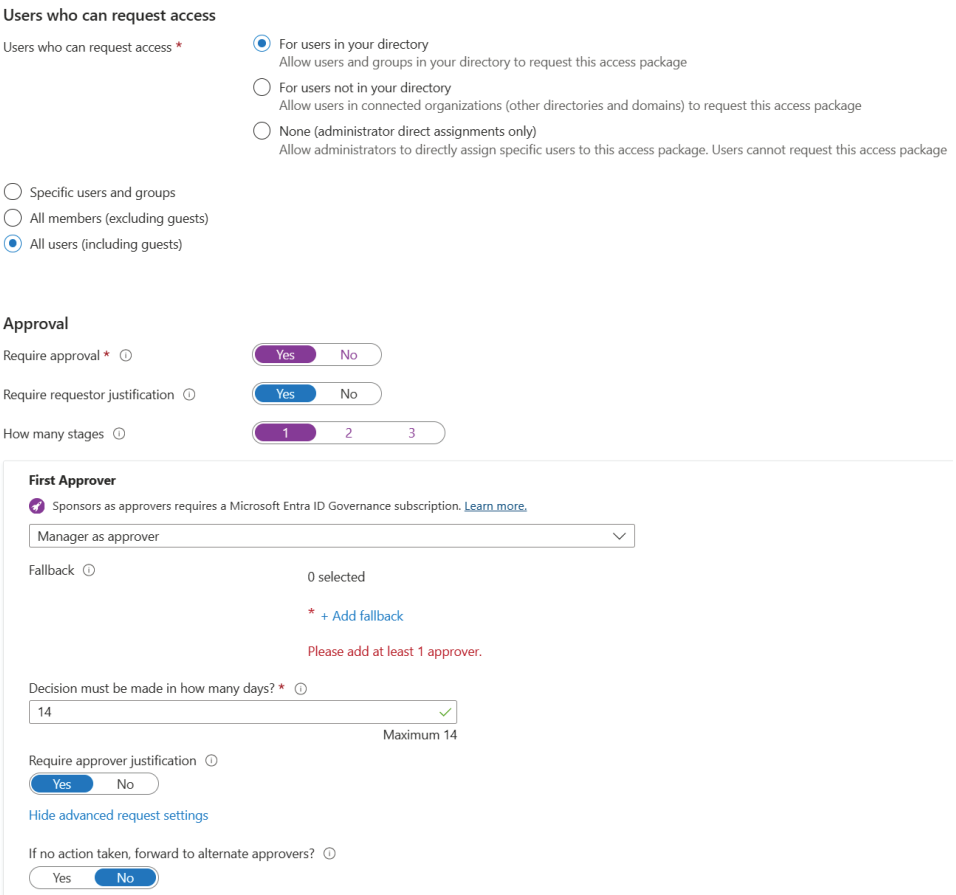


Figure 6.15: Access package for users in your directory

b. **For users not in your directory** – This option allows external users to request this access package. You can choose specific connected organizations, all connected organizations or all external users. Connected organizations include only the organizations in Configured state. Review the options in the following screenshot:

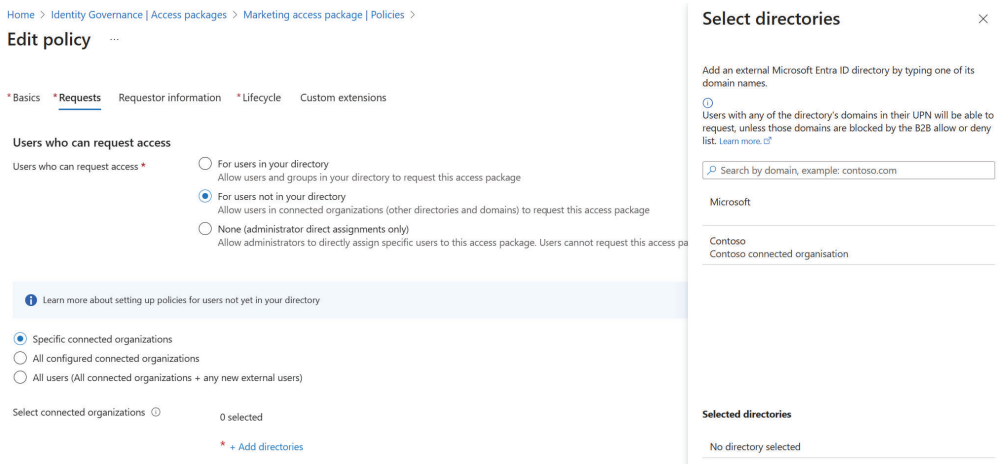


Figure 6.16: Access package for guests

c. **None** – Selecting this option makes the access package unavailable for requests and only administrators can directly assign it to users.

Ensure that the toggle is **Yes** for **Enable new request**. If it is set to **No**, new requests to this access package cannot be made. Click on **Next: Requestor Information**.

7. Use the **Requestor information** page to collect more information about the requestor. This page can be configured to ask the requestor questions, which will be shown on the request form. Review the options in the following screenshot and click on **Next: Lifecycle**:

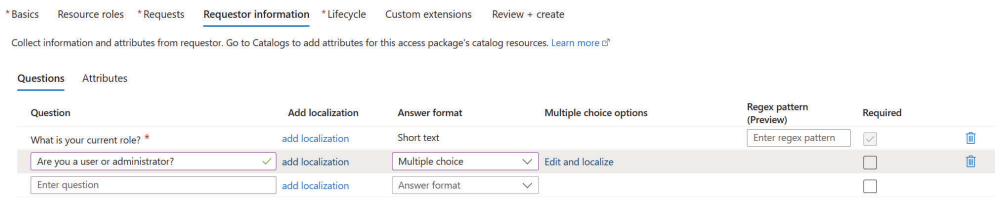


Figure 6.17: Collecting requestor information

8. On the **Lifecycle** page, you can choose if and when the access package expires and if access reviews are required for this access package. Review the options in the following picture and click **Next: Rules**:

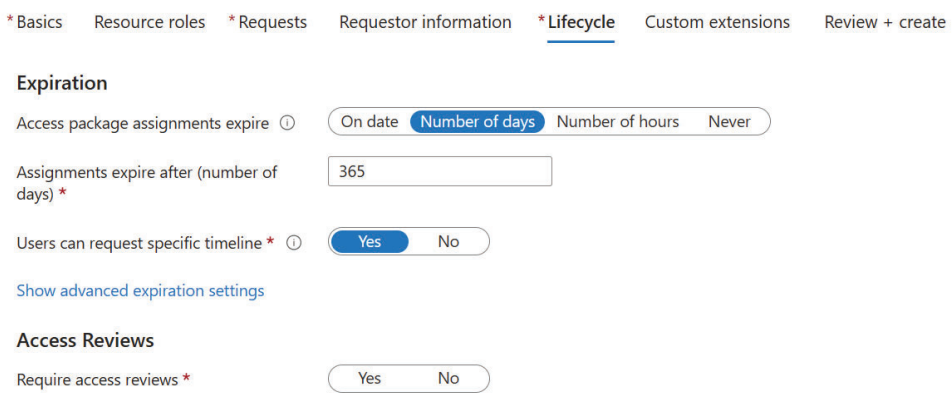


Figure 6.18: Access package lifecycle

9. Skip the **Custom extensions** step and click **Next: Review + create**. On the **Review + create** page, review the selected settings and click **Create**.
10. Once the access package is created, the **My access portal link** will be displayed as in the following screenshot. This is the link the users will use to request this access package. Copy this link and provide it to the users.

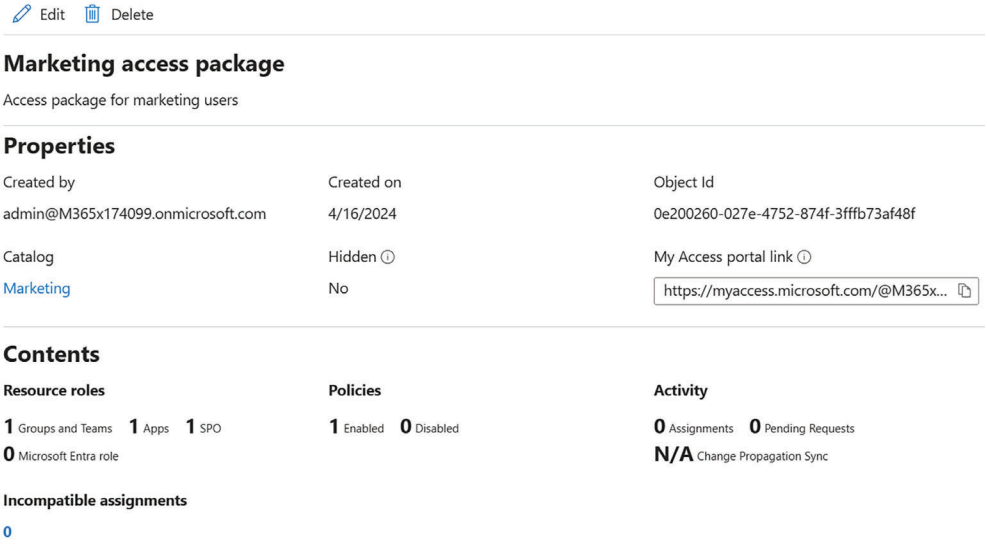


Figure 6.19: My access portal link

Users with the **Identity Governance Administrator**, **Global Administrator**, **Catalog owner**, or **Access package manager** role can create an access package.

Requesting access

As an end user, follow the steps below to request access to the *Marketing access package*:

1. Open a new browser window and go to the My Access portal link copied in the previous step. Enter your Microsoft Entra ID credentials.
2. As shown in the following screenshot, you should see the **Marketing access package** pop up on the screen. You can view the details of the access package. Select the **Resources** tab to see the resources that the access package provides access to. Click **Continue**.

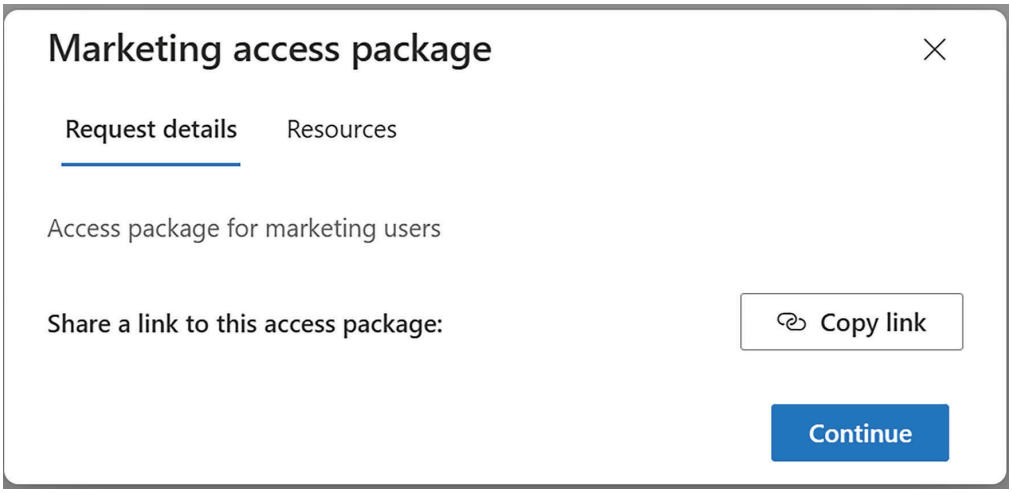


Figure 6.20: Access package on My Access page

3. You will now see the questions configured while creating the access package. Answer the questions and click on **Submit request** as shown in the following screenshot:

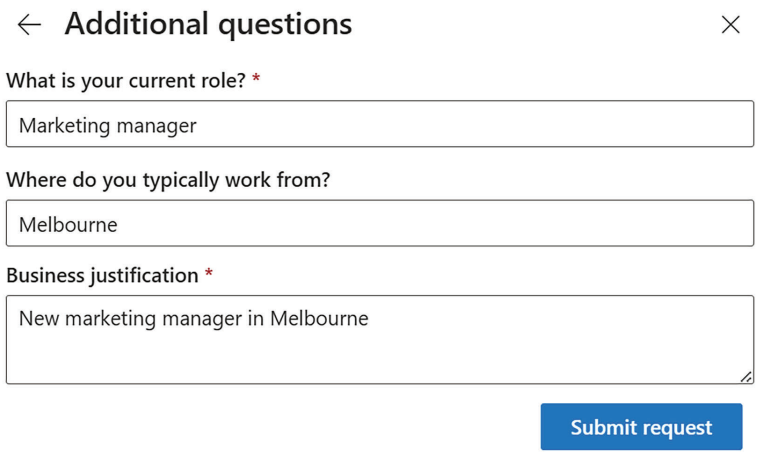


Figure 6.21: Additional questions while requesting access package

If the access package is subject to approval, the approvers will be notified. If not, the end user will get access to the resources.

Approving access

If the access package is subject to manual approvals, the access request will have to be approved before it is delivered to the end user. As the access package approver, log in to `https://myaccess.microsoft.com`. In the left pane, click on **Approvals**. The right pane will display all the pending access requests. Click on **Review** to review the inputs made by the user. Click on **Approve** or **Deny**. Enter a reason for your decision and click on **Submit** as shown in the following screenshot:

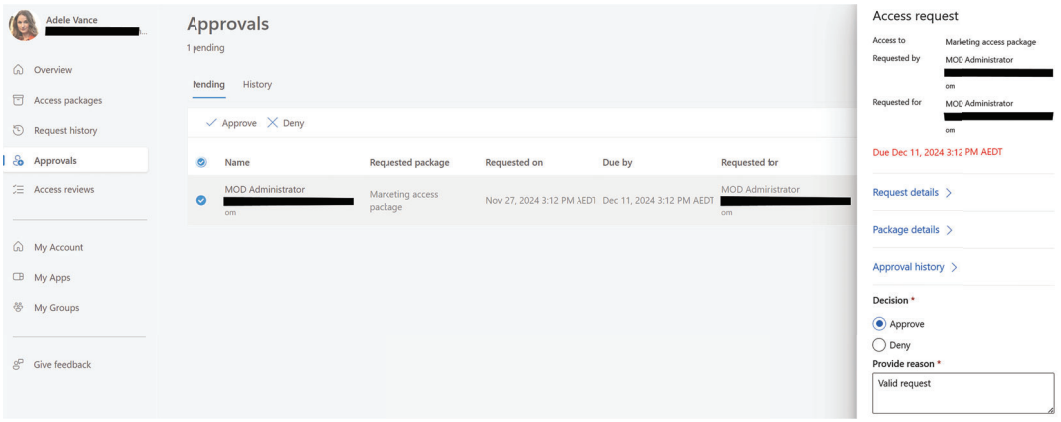


Figure 6.22: Approve or deny access requests

The access package will now be delivered, and the user will get access to the resources.

Validating that it worked

An **Identity Governance Administrator**, **Global Administrator**, **Catalog owner**, **Access package manager**, or **Access package assignment manager** can validate that the access package has been successfully delivered to the user. Follow the steps below:

1. Log in to `https://entra.microsoft.com` and navigate to **ID Governance** | **Entitlement management**.
2. Click on **Access packages**. Select the appropriate access package and click on **Requests**.
3. In the right pane, ensure that the **Status** column displays **Delivered**.

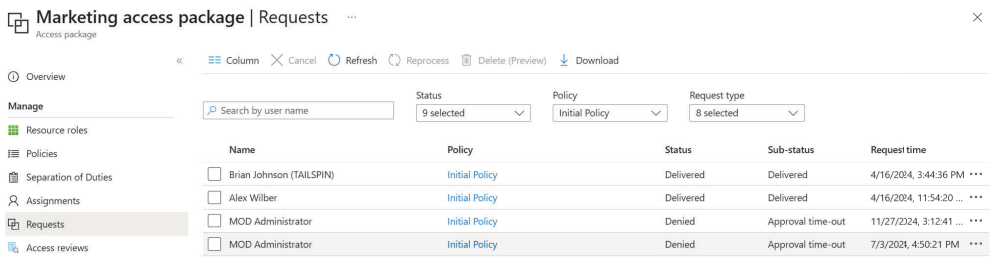


Figure 6.23: Access package status

If a status other than **Delivered** is shown, the administrator can troubleshoot and ensure that the user receives the required access.

Assigning an access package manually

If the access package has been created with the option **None (administrator direct assignment only)**, administrators will have to manually assign the access package to users.

Follow the steps below to manually assign an access package:

1. Log in to `https://entra.microsoft.com` and navigate to **ID Governance** | **Entitlement management**.
2. Click on **Access packages** and select the access package to which you want to assign users.
3. Click on **Assignments**.
4. Click on **New assignment**. Fill in the required details and click on **Add**. Refer to the following screenshot:

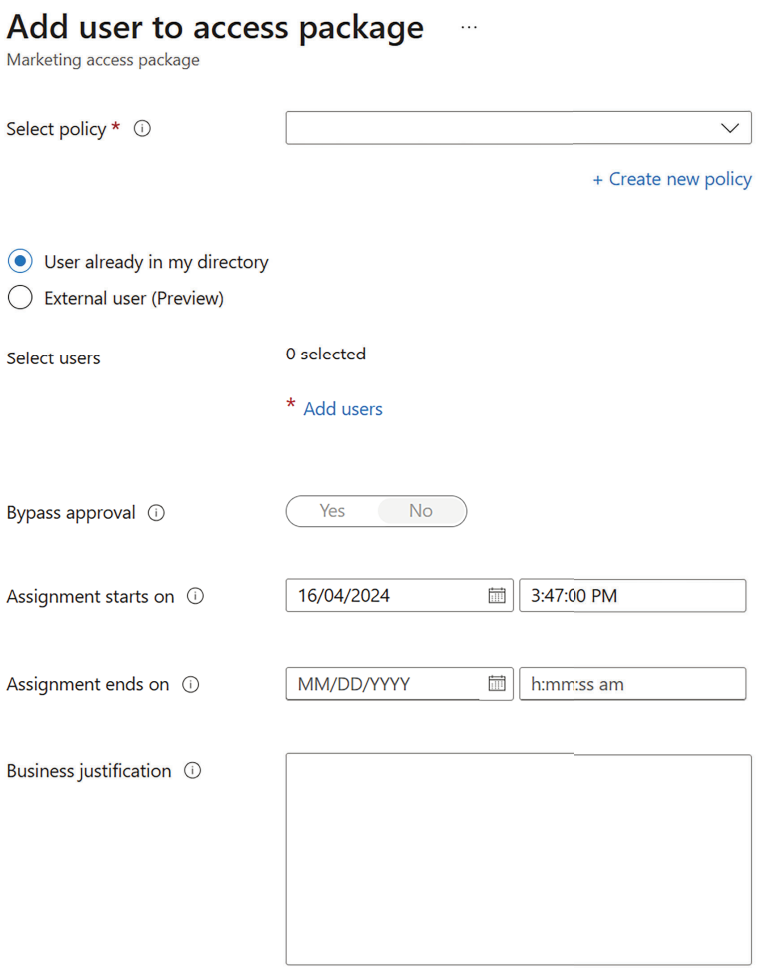


Figure 6.24: Manually add users to access package

Users with **Identity Governance Administrator**, **Global Administrator**, **Catalog owner**, **Access package manager**, or **Access package assignment manager** roles can manually assign access packages.

Auto-assigning users to an access package

In some situations, you might want to automatically add users to access packages based on their Microsoft Entra ID attributes. For example, you might want to add all users in the marketing department to the Marketing access package. Follow the steps below to auto-assign an access package based on user attributes:

1. Log in to `https://entra.microsoft.com` and navigate to **ID Governance** | **Entitlement management**.
2. Click on **Access packages** and select the access package to which you want to assign users.
3. Click on **Policies**.
4. Click on **Add auto assignment policy**.
5. Click on **Edit** next to the **Rule Syntax.** Select the user property from the **Property** drop down and select the appropriate **Operator**. In the **Value** box, type in the value of the user property. See example in *Figure 6.25*. Click **Save** to save the rule.
6. The boxes to **Automatically create assignments** and **Automatically remove assignments** are already checked. Doing this ensures that the users are automatically added and removed from the access package as their configured Microsoft Entra ID attributes change. For example, when a new user joins the Marketing department, they will be automatically added to this access package based on their Entra ID user attribute. Now, if the user moves from Marketing to Sales and their Entra ID user attribute is updated, they will be automatically removed from this access package and lose access to all resources that this access package grants access to. You can also configure a grace period to retain user access to this access package for a pre-defined period once they go out of scope. Refer to the following screenshot. Click on **Next**.

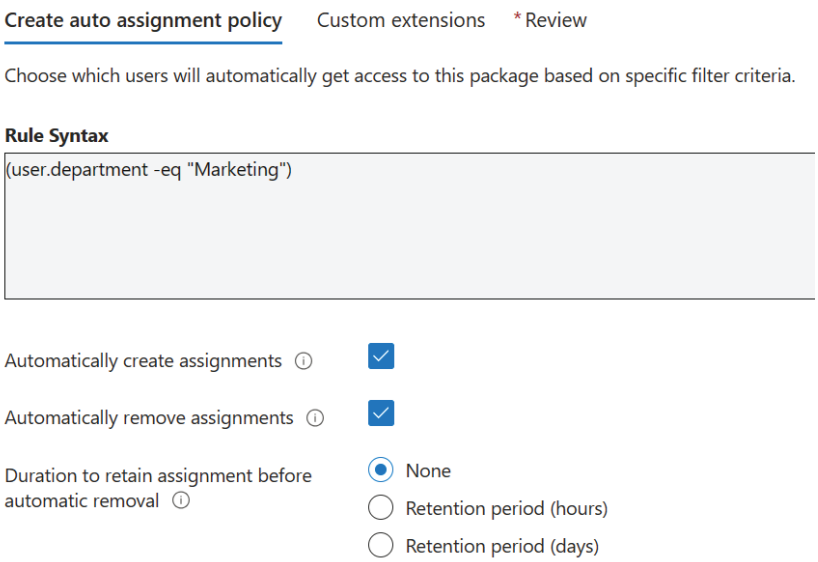


Figure 6.25: Create a dynamic rule

7. Skip the **Custom extensions** page and click **Next**.
8. On the **Review** page, type in **Name** and **Description** and click **Create**.

Users with the **Global Administrator** or **Identity Governance Administrator** can create auto assign policies. Only one automatic assignment policy is allowed per access package, as multiple policies can lead to processing and access issues.

Understanding access reviews

Using Microsoft Entra ID, users in the organization can collaborate with other internal users and with external guests. The self-service capabilities in Microsoft Entra ID make it easy for internal users and external guests to request and receive access to resources. However, this poses a new challenge: users may have access to resources for longer than required or have more access than required to do their job. Checks and balances should be in place to ensure that users need continued access to the resources. Using access reviews, organizations can review users' access to security and M365 groups, applications, access packages, Microsoft Entra roles, and Azure resource roles. Some scenarios where access reviews could be used are:

- There are too many users in privileged roles.
- Automation is not possible. For example, HR data cannot be synchronized with Microsoft Entra ID.

- If you want to repurpose a group for a different use.
- When users have access to business-critical data or applications, you might want to periodically review their access to ensure their job role still requires them to access that data or application.

The following are some key features of access reviews:

- They can be ad-hoc or scheduled.
- They can be delegated to non-IT administrators or business owners.
- Users can self-attest their access or reviewers can be designated.
- Insights can be used to decide whether a user's access should be continued or discontinued.
- Outcomes such as continuing or removing access can be automated.
- They can be tracked for compliance or policy reasons.

The following figure shows the access review workflow:

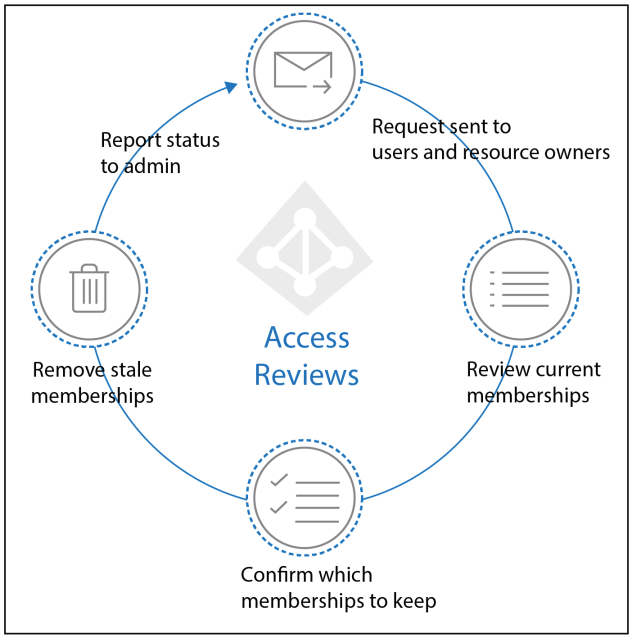


Figure 6.26: Access review workflow

The administrator creates access reviews in the Entra portal. Once the access review starts, the users and resource owners receive requests to review the access. They review current memberships and make decisions about keeping or revoking access.

Multi-stage reviews

Access reviews support up to three review stages. This enables multiple approvers to review access to resources before a decision is made. It helps organizations meet certification and audit requirements, design more efficient reviews, and reduce the number of decisions each reviewer is responsible for.

Multi-stage reviews help meet the following use cases:

- **Reach consensus across multiple reviewers**: This might be useful when access to highly critical resources is being reviewed or when there is a diverse set of reviewees, and it is hard for a single reviewer to make the decision.
- **Get input on unreviewed decisions**: If the first stage approvers are unable to decide, second stage and third stage reviewers can help.
- **Reduce burden on later-stage reviewers**: Reviews can be configured in such a way that if a deny decision is made at an earlier stage, those users are not reviewed at the later stages. This way the subsequent stage approvers see a filtered down list.

The options available while configuring multi-stage review are:

- **Reviewers**: Group owners, selected users or groups, users themselves, or managers of users can be configured as reviewers. For group owners, selected users or groups and managers of users, *fallback reviewers* can be configured. These will be used if primary reviewers do not exist.
- **Stage duration**: This specifies the number of days within which reviewers at each stage must respond to the review request.
- **Show previous stage(s) decision to later stage reviewers**: You can choose to reveal or hide the decision taken by earlier stage reviewers by selecting or deselecting this box.
- **Review recurrence**: You can specify if the access review is one time or recurring. The available options are **One time**, **Weekly**, **Monthly**, **Quarterly**, **Semi-annually**, and **Annually**. If you choose a recurring review, you can specify start date and end options like **Never**, **End on specific date**, or **End after number of occurrences**.
- **Reviewees going to next stage**: Lastly, you can choose to send all or only a subset of reviewees to the next stage. The available options are **All**, **Approved reviewees**, **Denied reviewees**, **Not reviewed reviewees**, and **Reviewees marked as "Don't know"**.

Refer to the following screenshot for these options:

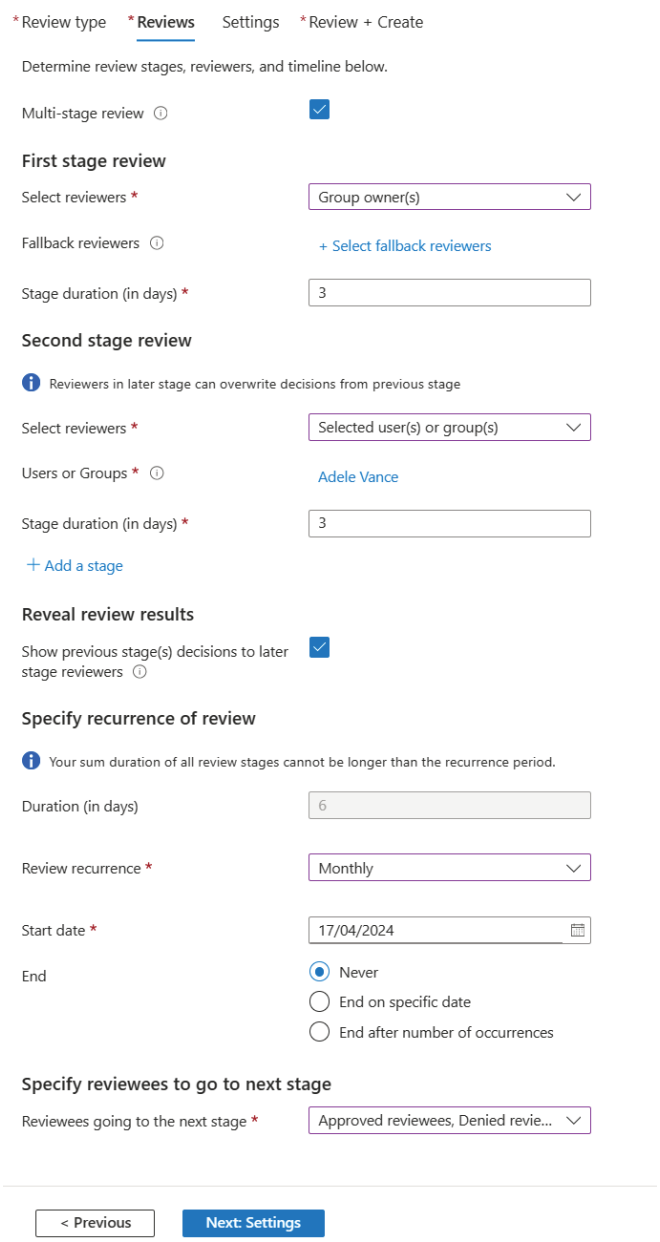


Figure 6.27: Configuring multi-stage review

It is recommended to use multi-stage access reviews for critical resources to ensure that the correct access decisions are made.

Guest user reviews

Guest user reviews help organizations that use B2B collaboration. Guest access should be reviewed regularly to ensure that they still need access to the resources. When access reviews are configured with scope Guest users only, an additional setting is available that allows:

- Removing guest user access from the resource.
- Blocking the guest user access for 30 days and then removing the user from the tenant.

> **Note**
>
> This option is not available if the review scope is **All Microsoft 365 groups with guest users**.

Refer to the following screenshot:

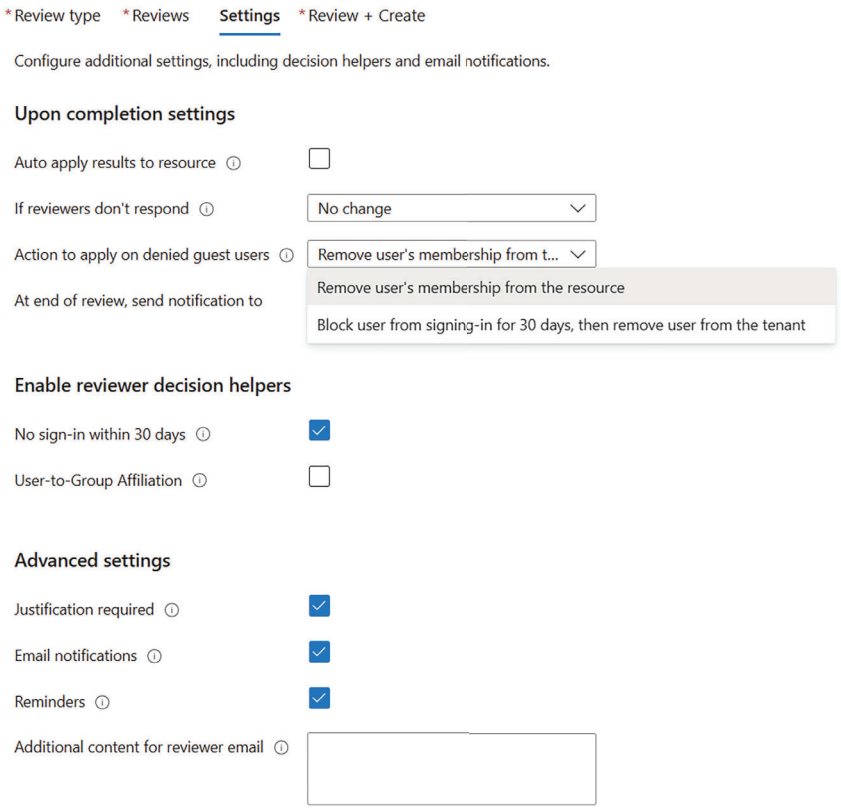


Figure 6.28: Review guest user access

Now let's explore how access reviews are created and managed for groups and applications, access packages, and Entra and Azure roles.

Access reviews for groups and applications

To be able to perform access reviews on applications, they must be integrated with Microsoft Entra ID and be listed on the Microsoft Entra admin portal under **Entra ID | Enterprise apps**. To ensure that a listed application is ready for access review, click on the application and switch to the **Properties** page for that application. The **Assignment required?** toggle must be set to **Yes** as shown in the following screenshot. If it is set to **No**, users can access the application but access reviews cannot be performed.

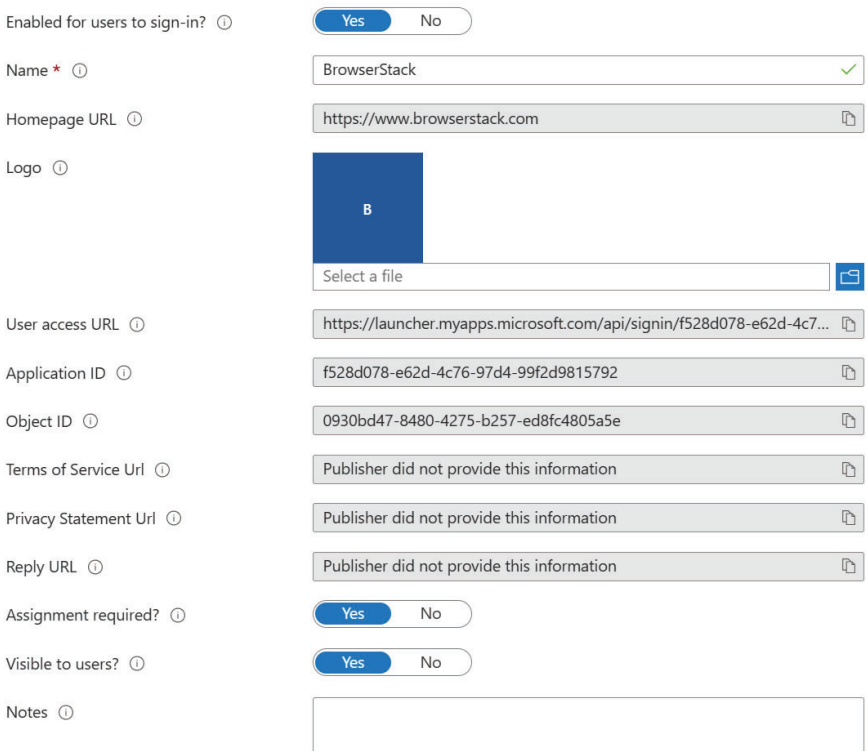


Figure 6.29: Prepare application for access review

Access reviews can be performed on groups created directly in Microsoft Entra ID. While access reviews can be scheduled and maintained for groups synchronized from Active Directory, group membership cannot be changed as the source of authority for these groups is Active Directory. To bypass this limitation, use **group writeback** or use a custom script to apply the results to Active Directory.

Creating an access review

Now that we have learned the basics about access reviews, let's learn how to create one. Users need appropriate roles, such as Global administrator or Identity Governance administrator, to create access reviews.

Follow the steps below to create an access review for groups and applications:

1. Log in to `https://entra.microsoft.com` and navigate to **ID Governance** | **Access reviews**.
2. In the right pane, click on **New access review**.
3. In the **Select what to review** field, select the appropriate option. If you choose: **Teams + Groups** you have the option to select:

    a. **All Microsoft 365 groups with guest users**: You can choose to exclude some groups from the scope of the access review. The **Scope** will be automatically selected as **Guest users only**. You have the option to perform the access review on only inactive guest users by checking the **Inactive users** box. Dynamic groups and role-assignable groups are not included. You can specify the number of days of inactivity as shown in the following screenshot:

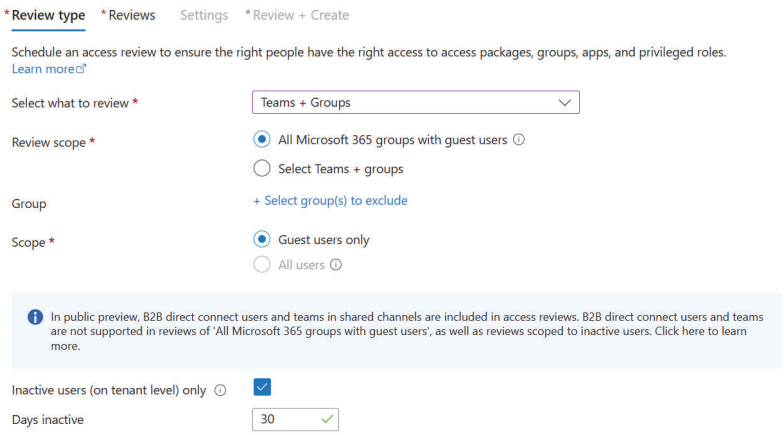


Figure 6.30: Access review for guest users

    b. **Select Teams + groups**: You can select the Teams and groups you want to perform the access review on. Review the options in the following screenshot:

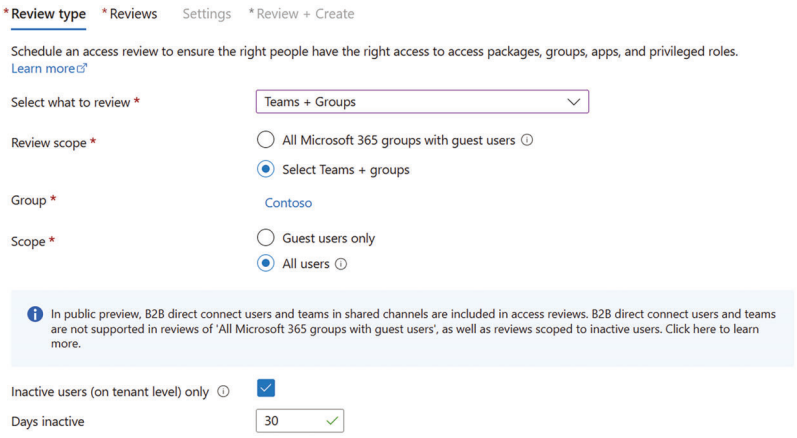


Figure 6.31: Access review for Teams and groups

c. **Applications**: Choose the applications for access review and choose if you want to review access only for guest users or all users. Click **Next: Reviews**. Refer to the following screenshot:

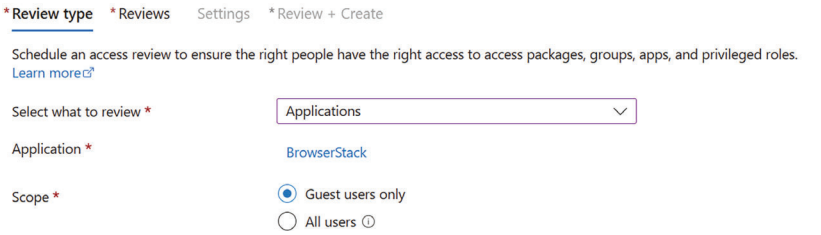


Figure 6.32: Access review for applications

4. On the **Reviews** page, choose if you want to configure a **Multi-stage review**. The various options are explained in the *Multi-stage reviews* section. Refer to *Figure 6.26*. Click **Next: Settings**.
5. On the **Settings** page, select the appropriate options. The key ones are explained as follows:
    a. **Auto apply results to resource** automatically applies the decision of the access review to the resource. For example, if a user's access is denied, their access to the resource will be revoked once the review is completed.
    b. **If reviewers don't respond** specifies the action that will be taken if the reviewers don't respond. The available options are **No change**, **Remove access**, **Approve access**, and **Take recommendations**.

c. **Enable reviewer decision helpers** provides insights to reviewers, such as identifying users who haven't signed in during the last 30 days and highlighting users with low affiliation to others within the group.

d. If you chose the scope as **Guest users only**, two additional options are available. These are explained in the *Guest user reviews* section earlier.

6. Review the other settings on the page shown in the following screenshot and click **Next: Review + Create**:

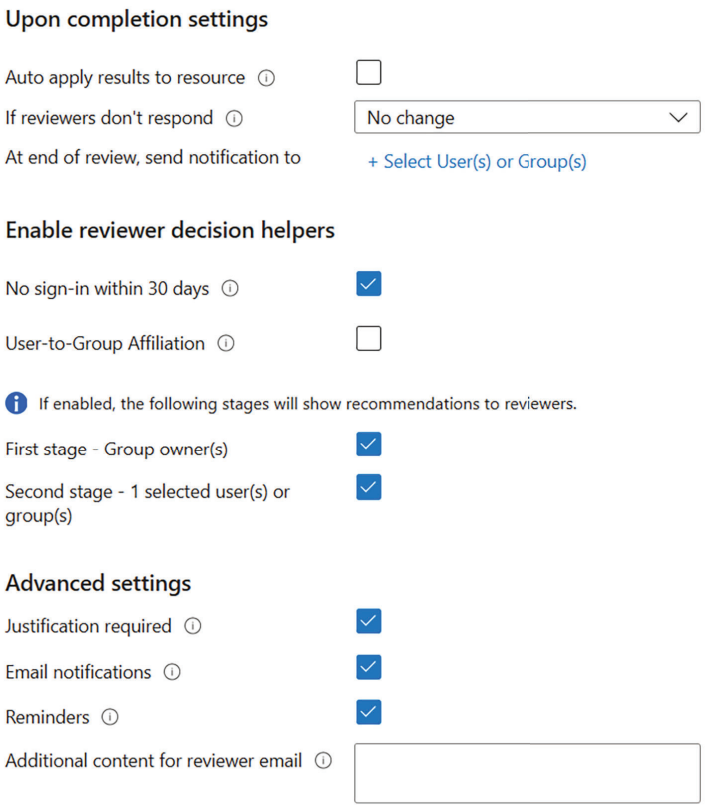


Figure 6.33: Upon completion settings

7. On the **Review + Create** page, add a **Review name** and click **Create**.

Once the access reviews are created by the administrator, the reviewers will start receiving notifications that access reviews are due.

Reviewing access

If email notifications have been configured, the access reviewer will receive an email asking them to start the review. They can click on **Start review** in the email or directly go to the **My Access** portal. From there follow the following steps:

1. Navigate to **My Access** | **Access reviews** on `https://myaccess.microsoft.com`. The right pane will show the access reviews as shown in the following screenshot:

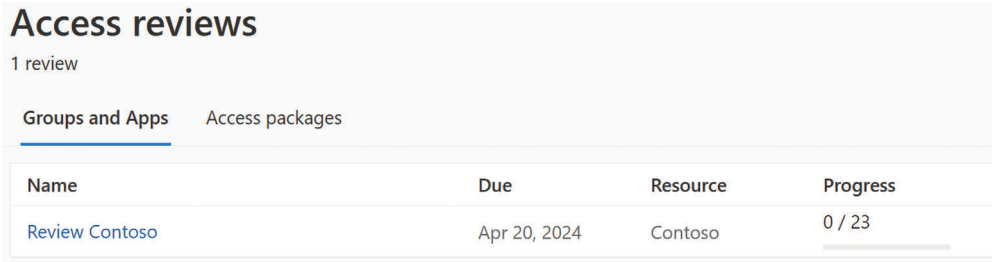


Figure 6.34: Access reviews on My Access portal

2. Click on the access review name to view a list of users. Click on **Details** to view the available options. In the following screenshot, you can see the recommendation is to deny user access as the user has not signed into the tenant in the last 30 days. Review the other available options. Click on **Submit** once done. You can select multiple users and click on **Approve**, **Deny**, or **Don't know** to take bulk actions. You can also click on **Accept Recommendations** to accept the recommendations provided by access review.

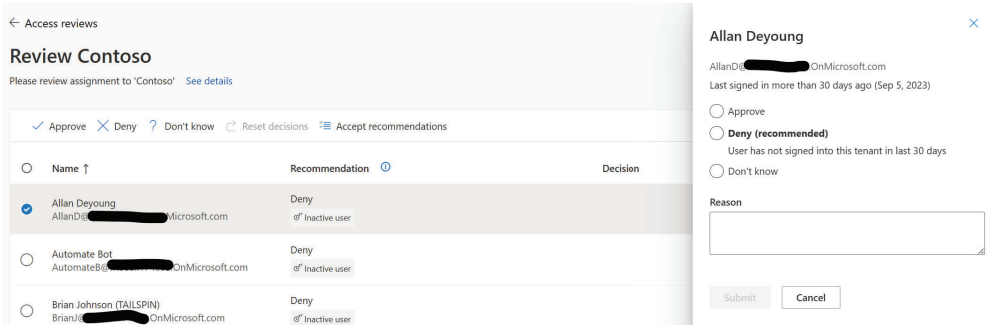


Figure 6.35: View user details

If you are the second or third stage reviewer, you will also see the decisions made by the earlier-stage approvers, provided the administrator enabled that setting while creating the access review.

Access reviews for access packages

You can create access reviews for an access package at the time of creation or by editing an existing access package assignment policy.

Creating an access review

To create an access review for an access package at the time of creation, follow the steps in the *Creating an access package* section earlier in this chapter. On the **Lifecycle** page, switch the **Require access reviews** toggle to **Yes**. Review the available options in the following screenshot:

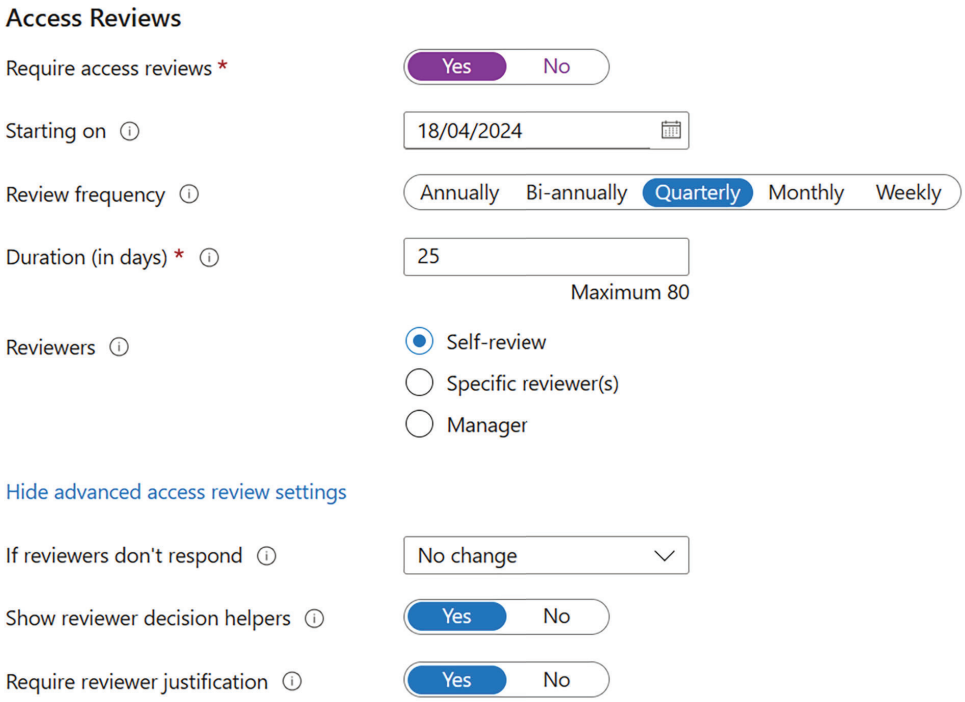


Figure 6.36: Access review for access package

To add an access review to an already created access package, follow the steps below:

1. In the Microsoft Entra admin center, navigate to **ID Governance | Entitlement management | Access packages.** Select the access package from the right pane and select **Policies**.
2. From the list of policies, select the policy to which you want to add the access review. Click on the ellipses and select **Edit**.
3. In the policy, navigate to the **Lifecycle** page and add the access review.

Users need to be a Global administrator, Identity Governance administrator, Catalog owner, or Access package manager to be able to create access reviews for access packages.

Reviewing access

Like reviewing access for groups and applications, access for access packages is also reviewed from the **My Access** portal. Once you log in to the **My Access** portal as an access reviewer, navigate to **My Access | Access reviews** and in the right pane, click on **Access packages**. Refer to *Figure 6.35*. All access reviews for access packages where you are listed as reviewer will be displayed. Follow the steps described in the *Reviewing access* section covered under the *Access reviews for groups and applications* section to complete the access reviews.

Access reviews for Microsoft Entra and Azure resource roles

Access reviews can be created for Microsoft Entra roles by a Global Administrator or Privileged Role Administrator. For Azure resource roles, the Resource Owner or User Access Administrator role is required.

Creating an access review

To configure access reviews for Microsoft Entra roles, follow the steps below:

1. Log in to `https://entra.microsoft.com` and navigate to **ID Governance | Privileged Identity Management**. In the right pane, select either **Microsoft Entra roles** or **Azure resources** and then click on **Access reviews**.
2. At the top, click **New**. Review the options on the page shown in the following screenshot and make the appropriate settings:

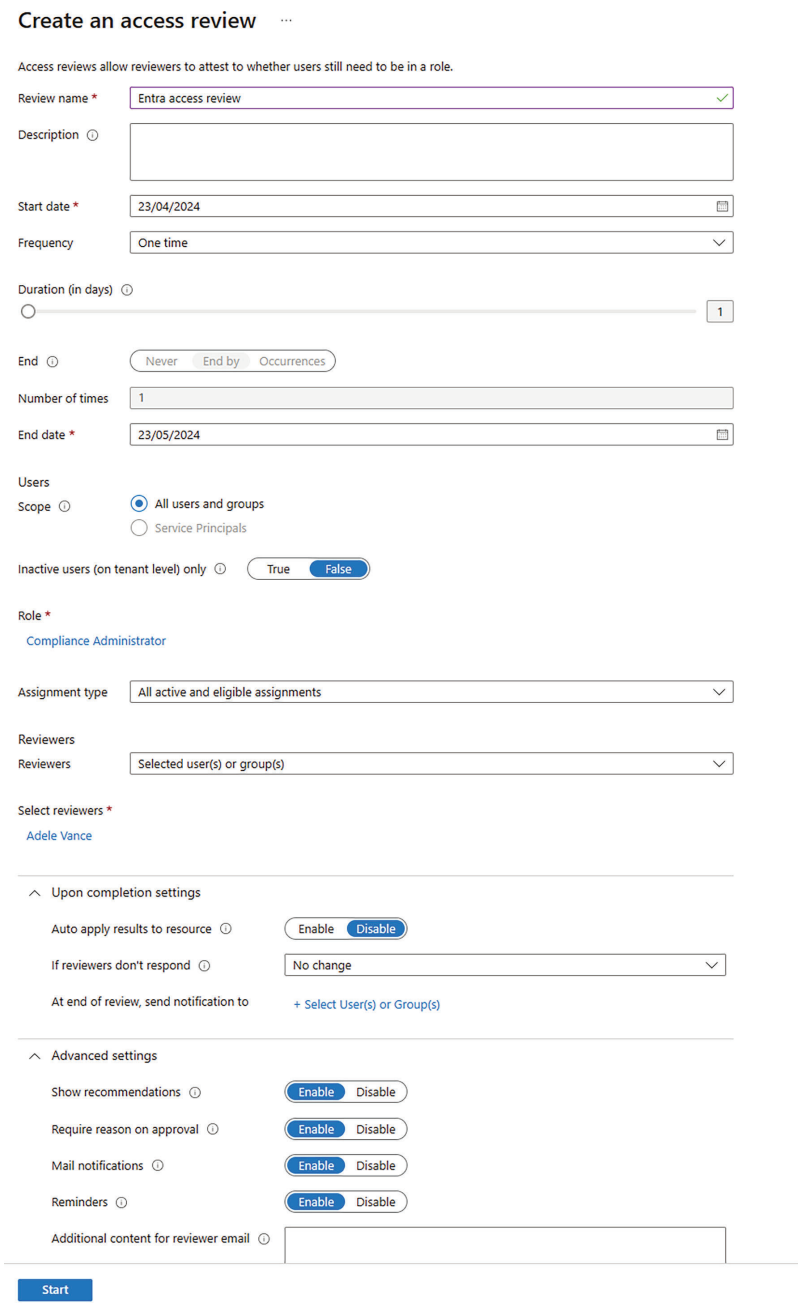


Figure 6.37: Access review for Entra roles

3. Click on **Start.**

Reviewing access

If communications are configured, the reviewer might get an email that an access review has been initiated. To review access, the reviewer can either click on the link in the email or go to the Microsoft Entra admin center directly. Follow the steps below:

1. Log in to `https://entra.microsoft.com` and navigate to **ID Governance | Privileged Identity Management | Review access**.
2. The right pane will show the available access reviews. Click on the name of the access review. The next page will show the user accounts whose access needs to be reviewed. Select the user to **Approve** or **Deny** access as shown in the following screenshot:

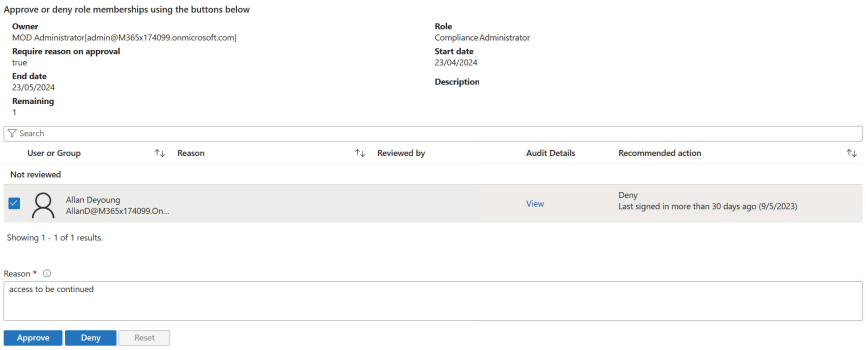


Figure 6.38: Review access for Entra roles

Reporting

Administrators can create a downloadable report to get more insight into the decisions taken by reviewers. The reports can be created for specific access reviews and for different time frames. These reports can be accessed by any user who is authorized to view access reviews. Users with Privileged Role Administrator, Identity Governance Administrator, User Administrator, Security Reader, Global Reader, and Security Administrator roles can create the reports. The following are the steps to create a report:

1. Sign in to `https://entra.microsoft.com` and navigate to **ID Governance | Access reviews | Review history**.
2. In the right pane, click **New report**.
3. In the fly out pane, enter a **Report name** and date range.
4. Select one or more **Review types**. The available options are **Applications**, **Groups**, **Azure resource roles**, **Entra ID roles**, and **Access package entitlements**.

5. Select the **Review results** to be included in the report. The available options are **Approved**, **Denied**, **Not reviewed**, **Don't know**, and **Not notified**.
6. Click **Create**.

Once the report is created, it is available for download from the portal for 30 days in CSV format.

License requirements

The following are the licensing requirements to use access review:

- Access reviews require a Microsoft Entra ID Governance license.
- All users who are reviewing access or having their access reviewed must have a Microsoft Entra ID Governance or Entra Suite license.

Microsoft Entra Access Reviews help organizations regularly evaluate and validate user access to ensure compliance and minimize risk.

Summary

In this chapter, you explored the fundamentals of Microsoft Entra ID Governance, with a specific focus on the principle of least privilege—ensuring users have only the necessary permissions to perform their roles. The chapter provided comprehensive guidance on how to create and effectively manage Entitlement Management access packages, enabling you to bundle and deliver the right resources to users based on business needs. Additionally, you learned how to implement and conduct access reviews, a critical process for periodically validating that users retain only appropriate access rights. By leveraging these features, you are now equipped to implement robust identity governance strategies, allowing you to administer, monitor, and control user identities and access at scale across your organization. In the next chapter, we will explore the Lifecycle Workflows feature of Microsoft Entra ID Governance.

Exercises

1. You are an IT administrator and are tasked with ensuring that new joiners have access to all the resources they need to do their job. Which Microsoft Entra ID Governance feature will you use?
    a. Lifecycle Management
    b. Entitlement Management
    c. Access Reviews
    d. Privileged Identity Management

2. You are the designated approver for access packages. As users request access packages you need to approve them so that the access packages can be delivered to them. Which portal should you use?
    a. Microsoft Entra Administrator portal
    b. Intune portal
    c. Your mailbox
    d. My Access portal
3. Which Microsoft Entra ID Governance feature allows you to regularly evaluate and confirm that users have the appropriate access to resources?
    a. Lifecycle Management
    b. Entitlement Management
    c. Access Reviews
    d. Privileged Identity Management

Answers

1. b
2. d
3. c

Additional resources

- Microsoft Entra ID Governance: `https://learn.microsoft.com/en-us/entra/id-governance/identity-governance-overview`
- Entitlement management: `https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-overview`
- Access reviews: `https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-overview`
- My access portal: `https://learn.microsoft.com/en-us/entra/id-governance/my-access-portal-overview`
- Microsoft Entra ID Governance licensing: `https://learn.microsoft.com/en-us/entra/id-governance/licensing-fundamentals`

Join us on Discord

For discussions around the book and to connect with your peers, join us on Discord at `packt.link/discordcloud` or scan the QR code below:



7

Microsoft Entra Lifecycle Workflows

Lifecycle workflows play a critical role in modern identity and access management by streamlining and automating the processes associated with a user's journey within an organization. From the moment a new employee joins (the joiner), through internal changes such as promotions or department transfers (the mover), to when they leave the company (the leaver), each stage demands precise updates to access rights and group memberships to maintain both productivity and security. Manual management of these transitions is not only time-consuming but also prone to errors, which can lead to unauthorized access or overlooked permissions, posing significant security risks.

By leveraging lifecycle workflows, organizations can ensure that user accounts are provisioned, updated, and deprovisioned automatically and consistently. This automation supports compliance with regulatory requirements by providing clear audit trails of access changes and minimizing the risk of data breaches due to lingering or excessive permissions. Additionally, lifecycle workflows improve operational efficiency by reducing the administrative burden on IT teams, allowing them to focus on more strategic initiatives. The use of predefined templates and integration with HR tools further accelerates deployment and ensures that the workflows reflect organizational policies and best practices.

This chapter will cover:

- Introduction to Microsoft Entra Lifecycle Workflows
- LCW and Zero Trust
- Create and manage lifecycle workflows

Introduction to Microsoft Entra Lifecycle Workflows

Lifecycle Workflows (LCW) is a feature in Microsoft Entra ID Governance that enables organizations to manage users by automating the lifecycle processes of joiner, mover, and leaver. Workflows contain processes that run automatically for users as they move through the identity lifecycle.

Organizations that want to modernize their identity lifecycle management process need to ensure that users have the correct access to the correct resources, groups, and applications on the day they join the organization. They also must ensure that access is revoked in a timely manner for users who have left the organization. It is also important that the process of provisioning and revoking access is not overly complicated and time-consuming for administrators. Administrators should also be able to troubleshoot problems and have access to logs that help with troubleshooting, audit, and compliance.

There are several reasons why an organization would like to use lifecycle workflows. Some of the key ones are as follows:

- Extend the HR-driven provisioning process with other workflows to simplify and automate tasks.
- Centralize the workflow process to be able to create and manage all workflows in one location.
- Troubleshoot workflow scenarios using audit logs and workflow history.
- Manage the identity and access management lifecycle at scale.
- Automate manual tasks.
- Use logic apps to extend the capability for more complex scenarios.

The capabilities in lifecycle workflows help remove dependencies and increase efficiency in new employee onboarding and offboarding of former employees.

LCW are best suited for the following scenarios:

- **Automatic user provisioning from HR tools**: For most organizations, a relationship with a new employee begins by onboarding them to their **Human Resource Management System (HRMS)**. These user identities must then be created in Microsoft Entra for the new employees to be able to access the IT systems. Using LCW, organizations can automate onboarding tasks like account creation, generating temporary passwords, and sending emails.
- **Automate dynamic group membership**: Organizations that have well defined groups can automate user membership of those groups. Lifecycle workflows are different from dynamic groups in the following ways:
    - They can manage static groups, so you don't need to manage dynamic group rules.
    - You are not limited to one rule per group. Lifecycle workflow rules determine the scope of users against whom the workflow is executed.
    - Attributes beyond the ones supported by dynamic groups are available. For example, `employeeHireDate`.
    - Lifecycle workflows can perform actions on groups, and not just membership.
- **Workflow history and audit**: An audit trail of the user lifecycle process can be created.
- **Automate user account management**: Lifecycle workflows can help ensure that users who are leaving the organization have their access revoked in a timely manner.
- **Automate access package assignment**: Using lifecycle workflows, access packages can be automatically assigned and removed based on user attribute changes.
- **Logic apps integration**: Lifecycle workflows can be integrated with logic apps for more complex scenarios.

Microsoft Entra provides predefined **templates** ready for use by the administrator. This helps with quicker deployment of workflows. The following screenshot shows examples of these templates:

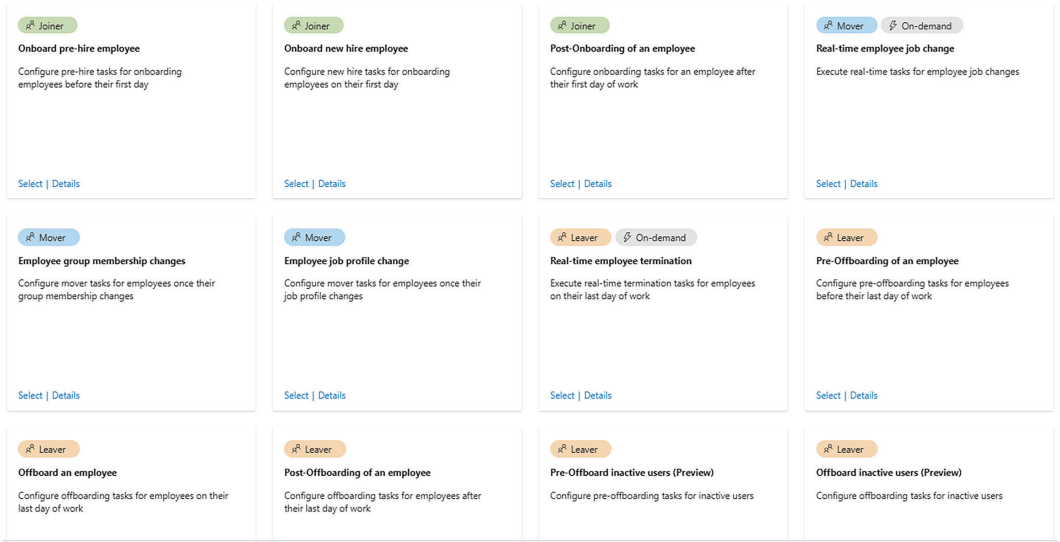


Figure 7.1: Lifecycle Workflow templates

Most workflows require that certain conditions be met for them to execute. These conditions are called **triggers**. Some are on-demand workflows and do not use a trigger.

LCW as a Zero Trust control

The Zero Trust security model operates on three foundational principles: verify explicitly, use least-privilege access, and assume breach. In environments where identity has replaced the network perimeter as the primary control plane, these principles demand that every user account be continuously validated, scoped to the minimum necessary permissions, and treated as a potential vector for compromise.

LCW provides the automation framework that translates these Zero Trust principles into operational reality. By orchestrating identity actions across the **joiner-mover-leaver** cycle, LCW ensures that access is granted, adjusted, and revoked in a timely, policy-driven manner, eliminating the manual gaps that attackers exploit.

Every active identity in a directory represents a potential entry point for an attacker. The identity attack surface grows not only with the number of accounts, but also with the privileges those accounts hold and the duration for which those privileges persist. Lifecycle workflows reduce this surface across all three dimensions:

- **Account proliferation control:** Joiner workflows ensure that accounts are created through governed, template-driven processes with predefined group memberships,

license assignments, and access packages. This prevents the ad hoc account creation that leads to ungoverned identities.

- **Privilege scoping:** Mover workflows automatically adjust access when users change roles, departments, or locations. Rather than accumulating permissions across job changes, users receive only what their current role requires, enforcing the least-privilege principle at every transition.
- **Timely deprovisioning:** Leaver workflows disable accounts, revoke group memberships, remove licenses, and schedule account deletion based on the `employeeLeaveDateTime` attribute, ensuring that departing users cannot retain access beyond their last day.

Together, these automated actions produce a continuously right-sized identity footprint. Rather than relying on periodic manual reviews to discover and remediate over-provisioned or stale accounts, LCW maintains hygiene as a continuous, event-driven process.

Let's explore how LCW acts as a Zero Trust control in each phase of the identity lifecycle.

Joiner phase

The joiner phase is where Zero Trust begins. New employees often wait days for access to the tools they need and when access finally arrives, it is frequently over-provisioned because administrators grant broad permissions to avoid repeated requests.

LCW joiner workflows solve both problems simultaneously. By defining access packages tied to specific roles and departments, the workflow grants exactly the permissions new employees need, before their first day. This approach delivers immediate productivity while enforcing the principle of least privilege from the moment the identity is created.

Pre-hire tasks can include generating a Temporary Access Pass, sending a welcome email with onboarding instructions, and adding the user to their department's Microsoft Teams channels and security groups. These tasks can be triggered automatically based on the `employeeHireDate` attribute.

Mover phase

When users change roles, they gradually accumulate permissions as their previous access is seldom revoked. This privilege drift is one of the most persistent and insidious violations of the least privilege principle. In organizations without mover automation, a user who moves from finance to marketing may retain access to financial systems, sensitive reports, and administrative tools that are no longer relevant to their role.

Over time, these accumulated permissions create accounts with far more access than any single role requires. These over-privileged accounts are prime targets for attackers because compromising one account yields access to multiple organizational functions.

LCW mover workflows address privilege drift by automatically detecting attribute changes like updates to department or job title and executing a defined sequence of access adjustments. Previous group memberships are removed, new role-appropriate access packages are assigned, and the transition is logged for audit purposes. This approach enforces the principle of least privilege access.

Leaver phase

The leaver phase represents the highest risk moment in the identity lifecycle from a Zero Trust perspective. A departing employee's account, if left active, becomes an unmonitored identity with valid credentials and established permissions. These serve as gold mines for attackers as they can compromise these accounts and launch multi-stage attacks that can compromise hybrid cloud environments, perform lateral movement, exfiltrate data, steal credentials, and deploy ransomware in the environment.

Hybrid environments introduce a particular challenge for deprovisioning. When an employee departs, their identity typically exists in multiple locations such as on-premises AD, Entra ID, connected SaaS applications, and potentially downstream systems provisioned through SCIM or custom connectors.

In organizations that rely on manual or ticket-based deprovisioning, the delay between an employee's departure and the revocation of their access across all systems can range from days to weeks. During that interval, the risk profile is severe. Even if the cloud account is disabled, an on-premises AD account may remain active, providing access to file shares, VPN gateways, and domain-joined resources. Applications provisioned outside the core identity platform may not receive deprovisioning signals, leaving orphaned access in downstream systems.

LCW leaver workflows transform deprovisioning from a reactive, ticket-based process into a deterministic, policy-driven operation. Whether triggered by the `employeeLeaveDateTime` attribute for planned departures or executed on demand for immediate terminations, the workflow ensures consistent, complete, and auditable offboarding across configured identity systems. This approach enforces the principles of assume breach and least privilege access.

Lifecycle workflows are not merely an operational convenience. They are a foundational Zero Trust control. In an environment where identity is the perimeter, the hygiene of the identity directory directly determines the organization's security posture. LCW ensures that:

- Every identity is created with the minimum necessary permissions (verify explicitly, least privilege).

- Every role change triggers an automatic rebalancing of access (least privilege, continuous verification).
- Every departure results in timely, complete deprovisioning (assume breach, attack surface reduction).

By automating the joiner–mover–leaver cycle, organizations move from a model of periodic, manual identity governance to one of continuous, policy-driven enforcement.

Components of lifecycle workflows

Lifecycle workflows contain processes that are executed against users as they move through the identity lifecycle. Workflows consist of **tasks** and **execution conditions**. Execution conditions consist of **triggers** and **scope**.

Tasks

Tasks are the specific actions that run automatically each time a workflow is triggered. Each lifecycle workflow template contains several built-in tasks that are designed to automate common lifecycle management scenarios. These tasks can also be used to build custom workflows. Tasks are categorized based on the joiner-mover-leaver model so that administrators can easily identify them and place them in appropriate workflows. These tasks can send a welcome email to new employees, generate a Temporary Access Pass and email it to the manager, add users to groups and Microsoft Teams, and do much more. In addition to built-in tasks, **custom task extensions** can be used for more complex scenarios. The following table lists the built-in tasks and their relevant scenarios:

Task	Scenario
Add users to groups	Joiner-Mover-Leaver
Add users to selected teams	Joiner-Mover-Leaver
Assign licenses to users	Joiner-Mover
Delete user account	Leaver
Disable user account	Joiner-Leaver
Enable user account	Joiner-Leaver
Generate TAP and send email	Joiner

Task	Scenario
Remove all licenses of user	Leaver
Remove user from all groups	Leaver
Remove user from all Teams	Leaver
Remove user from selected groups	Joiner-Mover-Leaver
Remove users from selected Teams	Joiner-Mover-Leaver
Run a custom task extension	Joiner-Mover-Leaver
Send email after user's last day	Leaver
Send email before user's last day	Leaver
Send welcome email	Joiner
Send onboarding reminder email	Joiner
Request user access package assignment	Joiner-Leaver
Remove access package assignment for user	Leaver-Mover
Remove all access package assignments for user	Leaver- Mover
Remove selected license assignments from user	Leaver-Mover
Cancel all pending access package assignment requests for user	Leaver

Table 7.1: Built-in tasks

Tasks define what actions the workflow performs and triggers determine when a workflow runs.

Triggers

Triggers define when the workflow will run for the users in scope. The trigger type depends on the type of workflow selected. The following are the available trigger types:

- **Time based attribute**: If this is selected, the workflow will run when the selected date time attribute values are reached. The options available for time-based attributes depend on the type of workflow selected. Time based attributes are only available for joiner and some leaver workflows. The following table summarizes the options for different workflows:

Workflow name	Workflow type	Available attribute values
Onboard pre-hire employee	Joiner	`employeeHireDate`
Onboard new hire employee	Joiner	`createdDateTime` `employeeHireDate`
Post-Onboarding of an employee	Joiner	`createdDateTime` `employeeHireDate`
Pre-offboarding of an employee	Leaver	`employeeLeaveDateTime`
Offboard an employee	Leaver	`employeeLeaveDateTime`
Post-Offboarding of an employee	Leaver	`employeeLeaveDateTime`

Table 7.2: Time based attribute triggers

The `createdDateTime` attribute is the date and time when the user's account was created in Microsoft Entra ID. The `employeeHireDate` attribute can be set in the user account in Microsoft Entra ID. However, it is best practice to synchronize this attribute via HR provisioning. The `employeeLeaveDateTime` is not available in Microsoft Entra ID, so it is recommended to synchronize it via HR provisioning. You can also configure it using Graph API. Refer to `https://learn.microsoft.com/en-us/graph/tutorial-lifecycle-workflows-set-employeeleavedatetime?tabs=http`.

Note

If you are synchronizing users from on-premises Active Directory, and want to use Lifecycle Workflows, you will have to use custom attributes as there is no `employeeHireDate` or `employeeLeaveDateTime` in on-premises Active Directory.

- **Attribute changes**: If this is selected, the workflow is run when the selected user attribute changes. Attributes include the user's department, job title, office location, country, and so on. This trigger is available for all workflows.
- **Group membership changes**: If this is selected, the workflow will run when the user is added or removed from selected groups. This trigger is available for all workflows.
- **Sign-in inactivity**: This trigger allows a workflow to run when a certain number of days have passed since the user last logged in. This trigger is available only for some leaver workflows. Using this trigger administrators can automatically offboard users who have been inactive for a certain time. A value between 30 days and 730 days can be defined.
- **On-demand**: This trigger is set when administrators want to run the workflow manually. Workflows with this trigger do not run on schedule.

When the workflow is run based on the trigger, the defined tasks are executed against the scope.

The following table summarizes the workflows and the triggers available for each:

Workflow name	**Workflow type**	**Available triggers**
Onboard pre-hire employee	Joiner	Time based attribute Attribute changes Group membership changes
Onboard new hire employee	Joiner	Time based attribute Attribute changes Group membership changes

Workflow name	**Workflow type**	**Available triggers**
Post-Onboarding of an employee	Joiner	Time based attribute Attribute changes Group membership changes
Real-time employee job change	Mover	On-demand
Employee group membership changes	Mover	Attribute changes Group membership changes
Employee job profile change	Mover	Attribute changes Group membership changes
Real-time employee termination	Leaver	On-demand
Pre-Offboarding of an employee	Leaver	Time based attribute Attribute changes Group membership changes
Offboard an employee	Leaver	Time based attribute Attribute changes Group membership changes
Post-Offboarding of an employee	Leaver	Time based attribute Attribute changes Group membership changes

Workflow name	Workflow type	Available triggers
Pre-Offboard inactive users	Leaver	Attribute changes Group membership changes Sign-in inactivity
Offboard inactive users	Leaver	Attribute changes Group membership changes Sign-in inactivity

Table 7.3: Workflows and attributes

Triggers define when a lifecycle workflow should run for the users in scope by evaluating conditions.

Scope

Scope defines who the workflow will affect. Depending on the triggers selected, the scope options will change. This is explained as follows:

- **Time based attribute**: When a time-based attribute trigger is selected, administrators must define rules to determine the users who will be in scope of the workflow. The scope query must contain the value of the attribute as it appears in the user object in Entra ID. For example, department equals *Marketing*.
- **Attribute changes**: Administrator must first select the attribute that will trigger the workflow to run. The scope query must include the value of the attribute as it appears in the user object in Entra ID. For example, department equals *Marketing*.
- **Group membership changes**: The scope query must include the group from which the user must be added or removed. Only one group can be selected at a time.
- **Sign in activity**: Administrator must define rules to determine the users who will be in scope of the workflow. For example, user type is *Guest*.
- **On-demand**: For on-demand workflows, administrators have the choice to select the users while creating the workflow or when the workflow is run.

The scope should be carefully defined as it can directly affect the users.

Role requirements

A **Global Administrator** or **Lifecycle Workflows Administrator** Microsoft Entra role is required to create and manage all aspects of workflows and tasks.

Licensing requirements

Using Lifecycle workflows requires a Microsoft Entra ID Governance license. In addition, each Lifecycle Workflow Administrator requires a license and each user who is in the scope of a workflow requires a license.

Limits

Lifecycle workflows are subject to certain limits as summarized in the following table:

Category	Limit
Maximum number of workflows per tenant	100
Maximum number of tasks per workflow	25
Maximum number of custom task extensions per tenant	100
Workflow schedule interval in hours	1-24
Number of users per on-demand selection	10

Table 7.4: Lifecycle workflows limits

Keep in mind these limits while designing your lifecycle workflows. Now that we understand the basics, let's proceed further.

Getting started with lifecycle workflows

Lifecycle workflows help organizations manage Microsoft Entra users efficiently by increasing automation. Along with other Microsoft Entra ID Governance solutions such as entitlement management, access reviews, and Privileged Identity Management, they help organizations address key access management questions. It is important to plan the deployment of lifecycle workflows to achieve the desired governance strategy. Consider the organizational needs and involve the right stakeholders to ensure that there are no mismatched expectations about impact, outcomes, and responsibilities.

Communication is often the key to the success of any new business process. Lifecycle workflows shift responsibility for manual processes to business owners. It decouples the onboarding and offboarding process from the IT department. This is a cultural shift and requires accountability from resource owners. Therefore, proactive communication is imperative, and resource owners must be trained to enable them to make the right decisions.

Prerequisites

Before an organization starts creating and using lifecycle workflows, it is important to ensure that the following technologies are in place:

Inbound provisioning

Most organizations have a process to create new employee records in their HRMS tool like SuccessFactors or Workday. These employee records must be synchronized with Microsoft Entra ID so that user accounts are auto provisioned. Microsoft Entra ID supports out-of-the-box integration with SuccessFactors and Workday.

Microsoft Entra ID supports direct synchronization of user accounts from Workday and SuccessFactors to on-premises Active Directory. Once the accounts are provisioned in on-premises AD, they can be synchronized with Microsoft Entra ID using Microsoft Entra Connect or Microsoft Entra cloud sync.

For organizations that use other systems of record, such as an HR app, a payroll app, a spreadsheet, or a SQL database, Microsoft Entra ID supports API-driven provisioning.

Before starting off with lifecycle workflows, ensure that the user accounts are synchronized to Microsoft Entra ID.

Attribute synchronization

Ensure that the accounts in Microsoft Entra ID have the `employeeHireDate` and `employeeLeaveDateTime` attributes populated either manually or via HR provisioning.

Creating a lifecycle workflow

Now that we have understood the various aspects of lifecycle workflows, let's learn how to create a workflow from the available templates:

1. Login to `https://entra.microsoft.com` and navigate to **ID Governance | Lifecycle workflows**. In the right pane click on **Create workflow**.
2. You will see all the workflow templates as shown in *Figure 7.1*. Click **Select** on the workflow that you want to create.

3. On the **Basics** tab, enter a name and description for the workflow. Select the **Trigger type** and configure the corresponding conditions. Refer to the following screenshot as an example. Click **Next: Configure scope**.

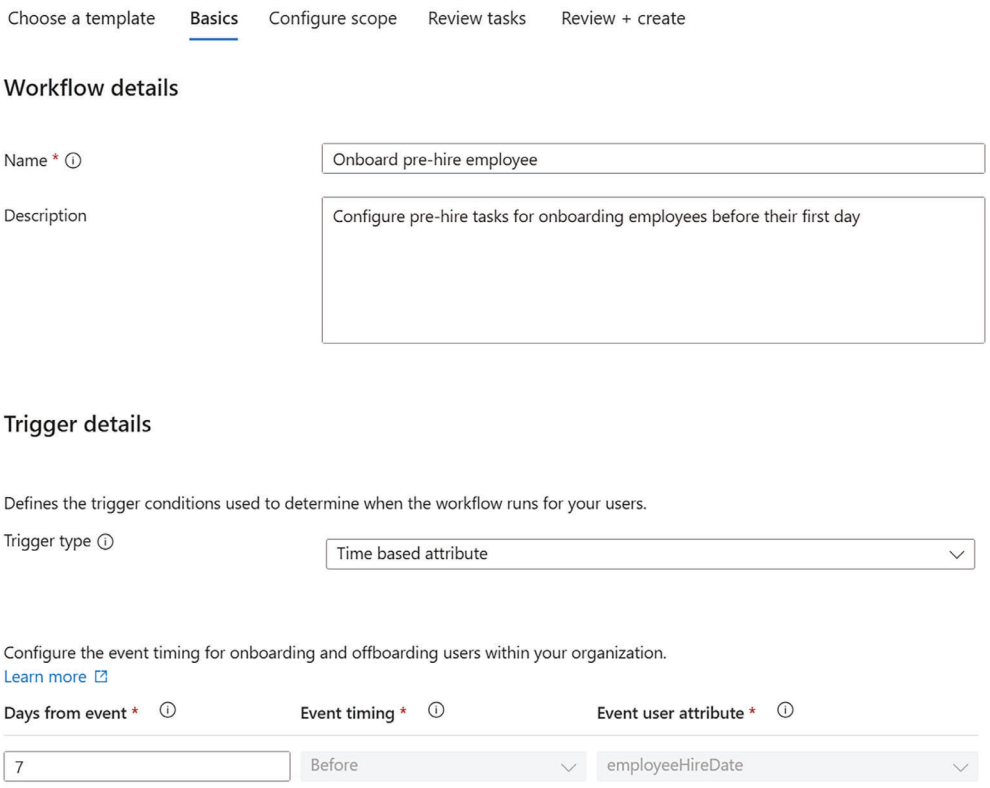


Figure 7.2: Workflow basics

4. On the **Configure scope** page, make the appropriate selections and click **Next: Review tasks**. Refer to *Figure 7.3*:

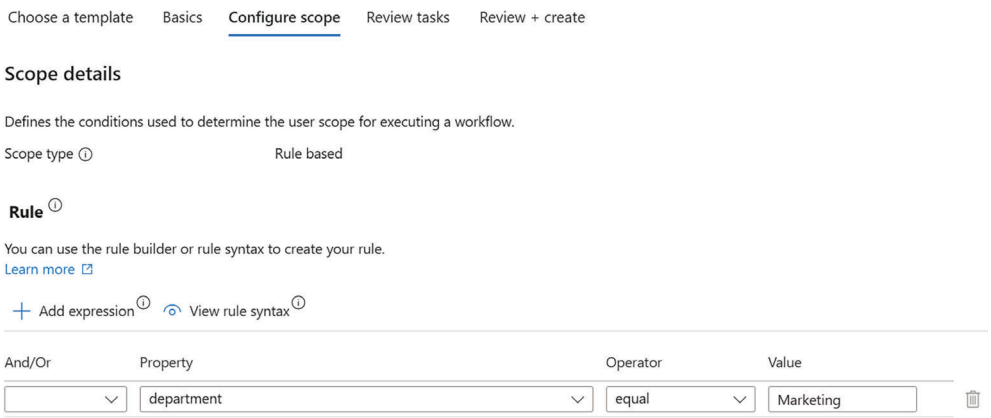


Figure 7.3: Configure scope

5. On the **Review tasks** page, tasks will be added as per the selected template. You can create more tasks by clicking on **Add task**. Individual tasks can be enabled or disabled. Refer to the following screenshot:

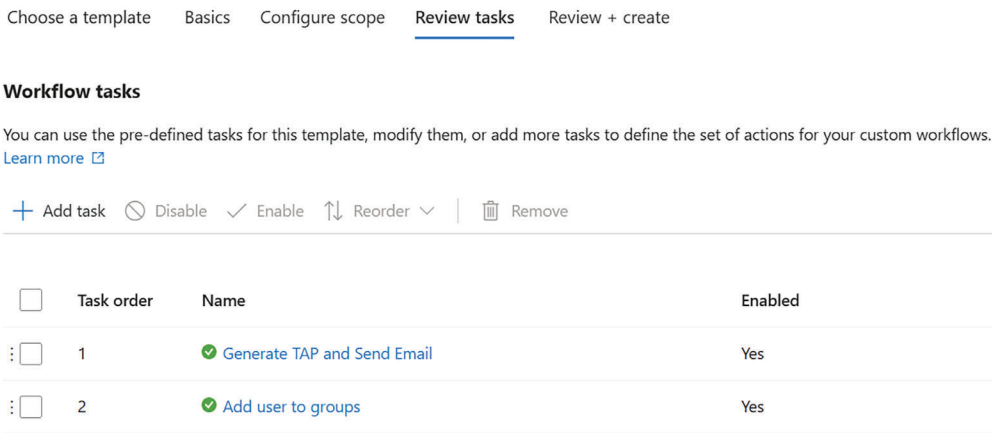


Figure 7.4: Add tasks

6. Once done click **Next: Review + create**. Review the selected options and check the box **Enable schedule** if you would like to run the workflow on schedule and click **Create**. Refer *Figure 7.5*. You can choose to keep the workflow disabled while you test it by unchecking the **Enable schedule** box.

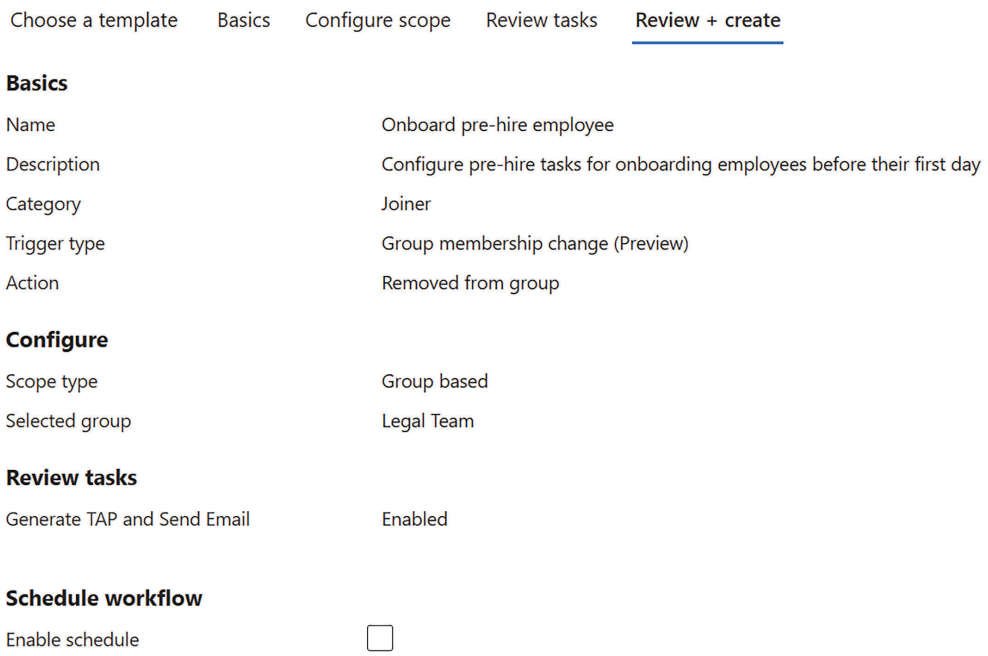


Figure 7.5: Create workflow

You can check the users who will fall under the scope of this workflow by selecting the workflow and clicking on **Execution conditions | Execution User Scope**. This will give the administrator an understanding that the workflow has been configured correctly and the correct users are selected by the workflow.

Running workflow on demand

Before you enable the workflow, you can test it by running it on demand. To run a workflow on demand, follow the steps below:

1. Navigate to **ID Governance | Lifecycle workflows | Workflows**.
2. Select the workflow and click on **Run on demand** as shown in the following screenshot:

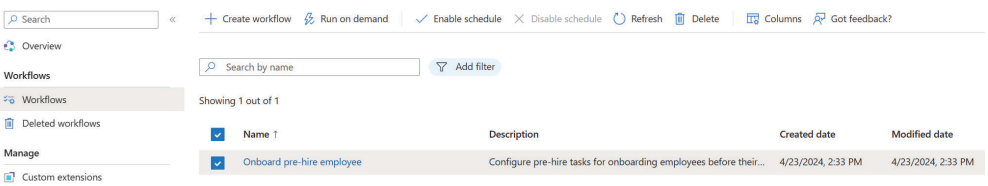


Figure 7.6: Run on demand

3. You will be prompted to select users. Select a set of users to test this workflow on and click on **Run workflow**.
4. To view the status of the workflow, click on the workflow to open it and click on **Workflow history**. On this screen, you can see a summary of the workflow runs, the users processed by the workflow, and the tasks that ran and failed. Refer to the following screenshot:

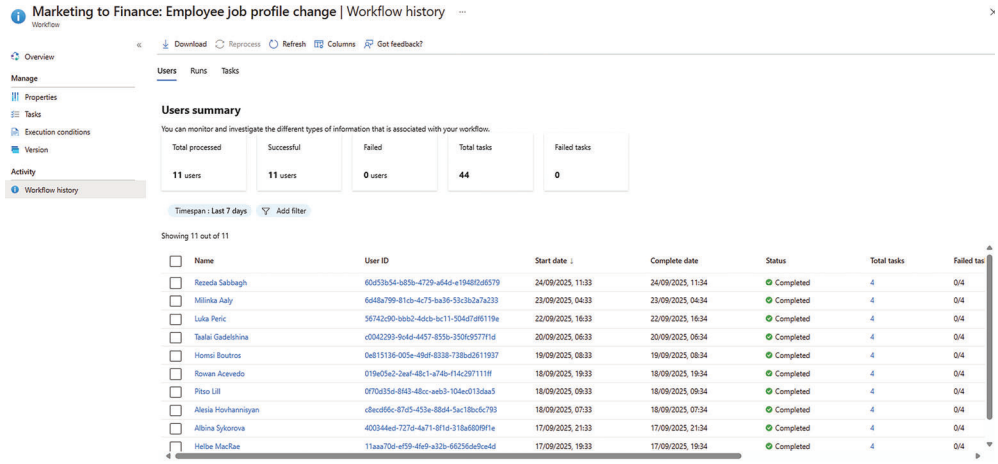


Figure 7.7: Workflow history

5. Click on the number in the **Total tasks** column to view the successful tasks and the ones that failed. You can also see if any tasks are in progress.

Once you have tested the workflow, you can enable it to run on a schedule.

Scheduling the workflow

To enable the workflow to run on schedule follow the steps below:

1. Navigate to **ID Governance | Lifecycle workflows | Workflows**.
2. Select the workflow you would like to schedule and click **Enable schedule**.

By default, workflows are scheduled to run every 3 hours. This can be changed by following the steps below:

1. Navigate to **ID Governance | Lifecycle workflows | Workflow settings**.
2. Adjust the **Workflow schedule** slider to customize the schedule. A value between 1 hour and 24 hours can be selected.

Lifecycle workflows are designed to adapt and grow with your organization. The next section explains how you can manage the workflows as your organization's needs evolve.

Managing lifecycle workflows

Now that you have learned how to create lifecycle workflows, you can manage them in various ways. In this section, we will learn how to manage lifecycle workflows.

Manage workflow properties

Once the workflow is created, you may need to edit its basic properties such as:

- Display name
- Description
- Enabling or disabling the workflow
- If the workflow runs on a defined schedule or is executed manually
- Task name
- Task description

Following are the steps to modify the basic properties of the workflow:

1. Login to `https://entra.microsoft.com` and navigate to **ID Governance | Lifecycle workflows | Workflows**.
2. Select the workflow that you want to edit and click on **Properties**. On this screen, you can modify the name and description. You can also enable or disable the workflow or enable the workflow to run on a schedule.

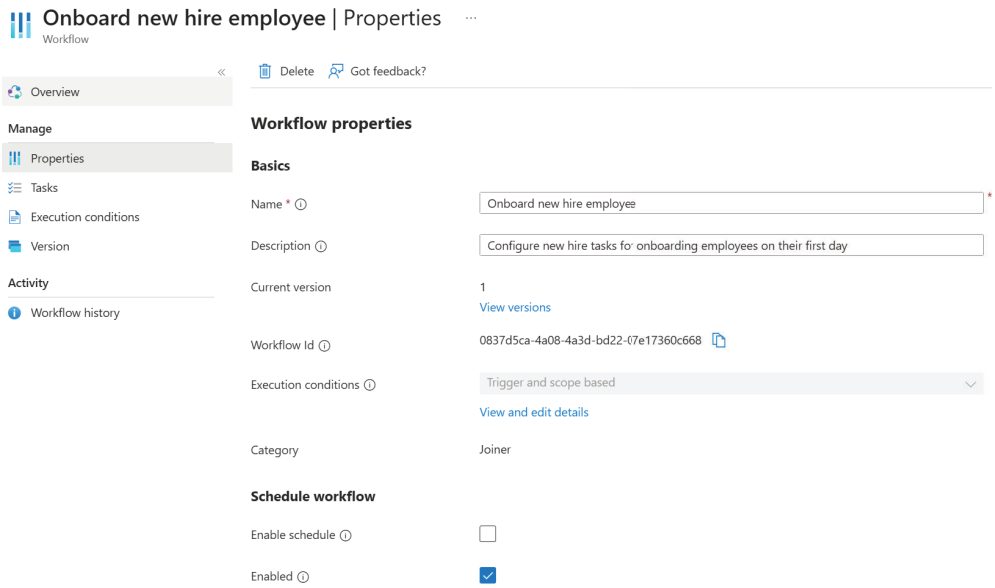


Figure 7.8: Edit workflow properties

3. To modify tasks, click on **Tasks**. From the list of tasks, select the task you want to edit. In the flyout pane, you can modify the task name and description as shown in the following screenshot:

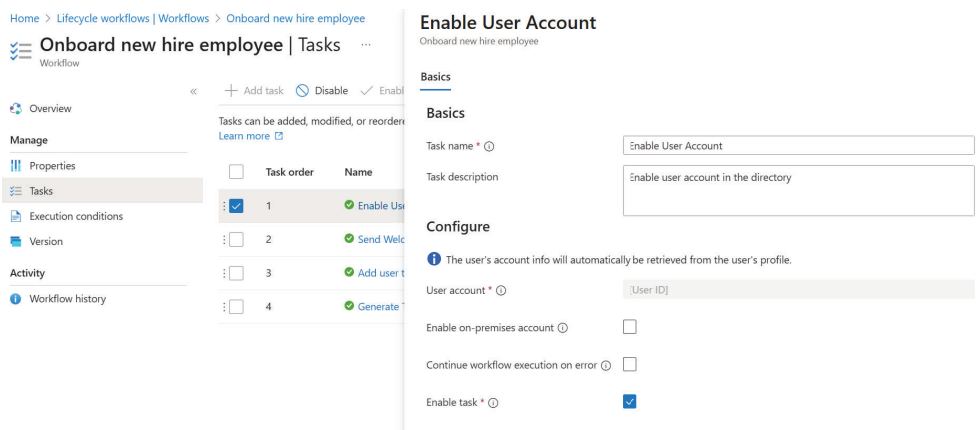


Figure 7.9: Edit workflow tasks

4. Once done, click **Save**.

You can also use Microsoft Graph to edit the properties of a workflow. For more details, refer to `https://learn.microsoft.com/en-us/graph/api/identitygovernance-workflow-update?view=graph-rest-1.0&tabs=http`.

Versioning

Lifecycle workflows are designed to grow and adapt to the changing needs of the organization. To manage updates in workflows, Lifecycle workflows have the concept of versions. If tasks and execution conditions are changed, a new version of the workflow is created. Versions provide many benefits like improved reporting for troubleshooting and record keeping. Versions allow for longer retention of information over just audit logs. While audit logs retain information for only 30 days, with versioning you can keep track of workflow information from the time it was created. It also allows you to trace which version of the workflow processed a particular user.

Following are the steps to edit the workflow using the Microsoft Admin center:

1. Login to `https://entra.microsoft.com` and navigate to **ID Governance | Lifecycle workflows | Workflows**.
2. Select the workflow that you want to edit and click on **Tasks**
3. On this screen, you can add tasks by clicking on the **Add task** button. You can enable or disable tasks and reorder tasks. You can also remove a task from the workflow using the **Remove** button. Click **Save** to make changes.
4. In the left pane, click on **Execution conditions**. Here you can change the **Trigger details** and **Scope details**. Click **Save**.
5. Making these changes creates new versions of the workflow. To view the versions, click **Version** in the left pane. You can see the versions as shown in the following screenshot:

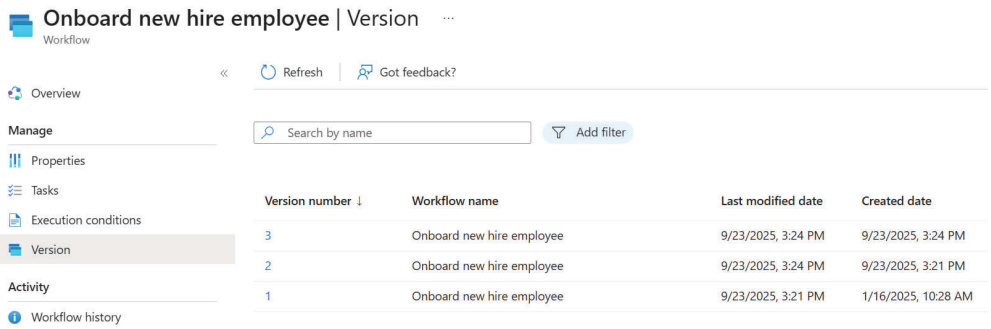


Figure 7.10: Workflow versions

6. Click on any version number to view details. Refer to *Figure 7.11*.

Version information

Version number	3
Last modified date	9/23/2025, 3:24 PM
Last modified by	Alex Wilber
Created date	9/23/2025, 3:24 PM
Created by	Alex Wilber

Basics

Name	Onboard new hire employee
Description	Configure new hire tasks for onboarding employees on their first day
Category	Joiner
Trigger type	Time based attribute
Days from event	0
Event timing	On
Event user attribute	employeeHireDate

Configure

Scope type	Rule based
Rule	(department eq 'Marketing') and (country eq 'United States')

Review tasks

Enable User Account	Enabled
Send Welcome email	Enabled
Add user to groups	Enabled
Generate TAP and Send Email	Enabled
Add user to selected teams	Enabled

Workflow schedule

Schedule enabled	No
Enabled	Yes

Figure 7.11: Workflow version details

If you use the Microsoft Entra Admin center to change workflow tasks or execution conditions, a new version of the workflow is created automatically. If these changes are made using Microsoft Graph, the new workflow version must be created manually. Refer to `https://learn.microsoft.com/en-us/graph/api/identitygovernance-workflow-createnewversion?view=graph-rest-1.0&tabs=http`.

Email customization

Lifecycle workflows include several tasks that send email notifications. These email notifications can be customized to suit the organization's needs. The following attributes of an email can be customized:

- Recipients
- Sender domain
- Organizational branding
- Subject
- Message body
- Email language

The default email template includes a security disclaimer. It is recommended to enable custom sender domain and organizational branding to remove this. If you choose to use the default email template, the text is automatically translated to the recipient's preferred language. If you specify a custom subject or body, the email is not translated. HTML formatting can be used to customize email text as follows:

- Bold the text by enclosing it within `<b></b>` brackets.
- Italicize the text by enclosing it within `<i></i>` brackets.
- Underline the text by enclosing it within `<u></u>` brackets.
- Insert hyperlinks using `<a href=></a>` brackets.

In addition to the above, you can also personalize emails using dynamic attributes. Place dynamic attributes within emails to insert the user's name, manager's email, or their Temporary Access Pass. The following is a list of the dynamic attributes that can be used to customize emails:

- `userDisplayName`
- `userEmployeeHireDate`
- `userEmployeeLeaveDateTime`
- `managerDisplayName`
- `temporaryAccessPass`
- `userPrincipalName`
- `managerEmail`

- `userSurname`
- `userGivenName`

It is important that the dynamic attributes are formatted properly. The correct format is `{{dynamic attribute}}`. Following is an example of an email using dynamic attributes:

```
Welcome to the team, {{userGivenName}}
We're excited to have you join our growing team and look forward to a successful
and memorable journey together.
We've already set up a few things to help you get started quickly and make your
onboarding process as smooth as possible.
For more information and next steps, please contact your manager,
{{managerDisplayName}}
```

To customize emails, follow the steps below:

1. Login to `https://entra.microsoft.com` and navigate to **ID Governance | Lifecycle workflows | Workflows**.
2. Select the workflow that contains the email task you want to customize.
3. Click on **Tasks** and select the task that contains the email.
4. In the **Basics** section, make changes as needed.
5. Click on **Email Customization** to make changes to the email subject, body and language.
6. Click **Save** once done.

Organizations can also customize emails sent by lifecycle workflows to include their own company branding and use their company domain. If organizations opt in to use custom branding, all emails sent using lifecycle workflows will use this branding. To be able to use custom branding in lifecycle workflows the organization must have a verified domain added and custom branding must be enabled within Microsoft Entra ID. This has been explained in *Chapter 3, Implementing Microsoft Entra ID*.

Once the above prerequisites have been met, follow the steps below:

1. Login to `https://entra.microsoft.com` and navigate to **ID Governance | Lifecycle workflows | Workflow settings**.
2. On this page, you can select the email domain that you want to use for email communications. You can also select if you want lifecycle workflows to use the company branding logo you configure as shown in the following screenshot:

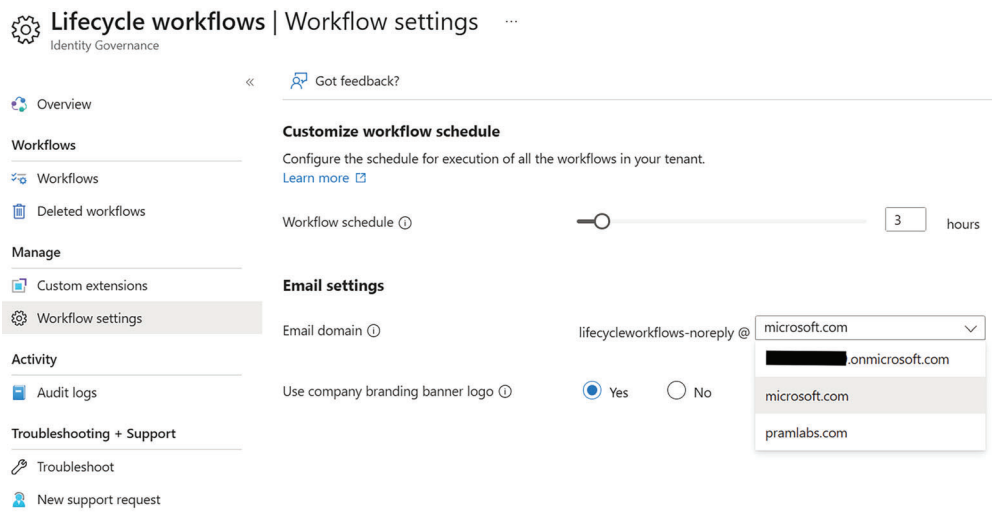


Figure 7.12: Email customization settings

3. Click **Save** once done.

You can also turn on custom branding and domain using Microsoft Graph. Refer to `https://learn.microsoft.com/en-us/graph/api/resources/identitygovernance-lifecyclemanagementsettings?view=graph-rest-1.0`.

Reprocessing workflows

Sometimes workflows fail and don't run as intended. The reprocess workflow feature allows administrators to run the workflow again to ensure that it is operating correctly. The following are the steps to reprocess a workflow:

1. Login to `https://entra.microsoft.com` and navigate to **ID Governance** | **Lifecycle workflows** | **Workflows**.
2. Select the workflow that you want to reprocess and select **Workflow history**
3. The **Users** tab will show the number of users processed by the workflow. Select the user(s) that you want to reprocess and click on **Reprocess**. Up to 10 users can be reprocessed at a time.
4. If you would like to reprocess a workflow based on runs, click on the **Runs** tab. Select the runs you would like to reprocess and click on **Reprocess**. Only one run can be reprocessed at a time.

Using this feature, administrators can quickly and efficiently manage workflows for specific runs or users.

Workflow history reports

Using the lifecycle workflow history feature, administrators can see the status of each workflow run, processed users, and failed tasks. This information is available in the Microsoft Entra Admin center for up to 30 days. If administrators would like to store this information for longer, they can download the history report in the form of a CSV report. Following are the steps to download the workflow history report:

1. Login to `https://entra.microsoft.com` and navigate to **ID Governance | Lifecycle workflows | Workflows**.
2. Select the workflow for which you want to download the report and select **Workflow history**
3. Select the appropriate option (**Users**, **Runs**, **Tasks**) for which you want to download the report.
4. Click on **Download** to download the report. Any filters applied are included in the report.
5. In the flyout pane, click **Download** as shown in the following figure:

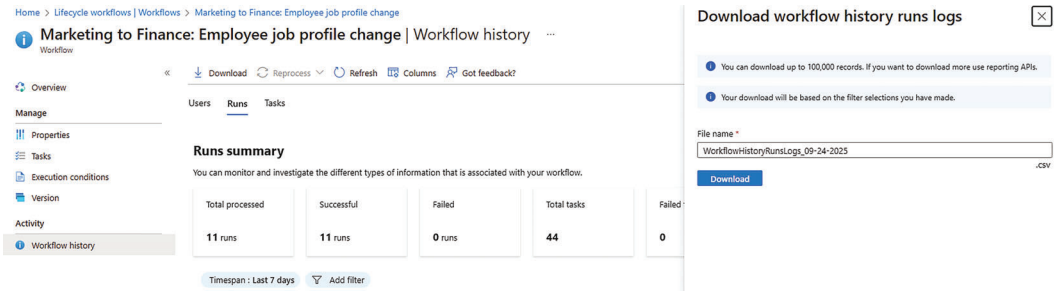


Figure 7.13: Download workflow history report

Up to 100,000 records can be downloaded from the Microsoft Entra Admin center. To download more records, use the Lifecycle Workflow reporting API. `https://learn.microsoft.com/en-us/graph/api/resources/identitygovernance-lifecycleworkflows-reporting-overview?view=graph-rest-1.0`

Managing inactive users

The leaver tasks in lifecycle workflows use the sign-in inactivity trigger to automatically disable and delete accounts of inactive users. Following are the steps:

1. Login to `https://entra.microsoft.com` and navigate to **ID Governance | Lifecycle workflows**

2. Choose one of the inactive user leaver workflow templates.
3. Select the **Trigger type** as Sign-in inactivity and select the number of days for which a user should be inactive. Click **Next: Configure scope**.
4. Define the scope for which the workflow will run. Refer example below. Click **Next: Review tasks**.

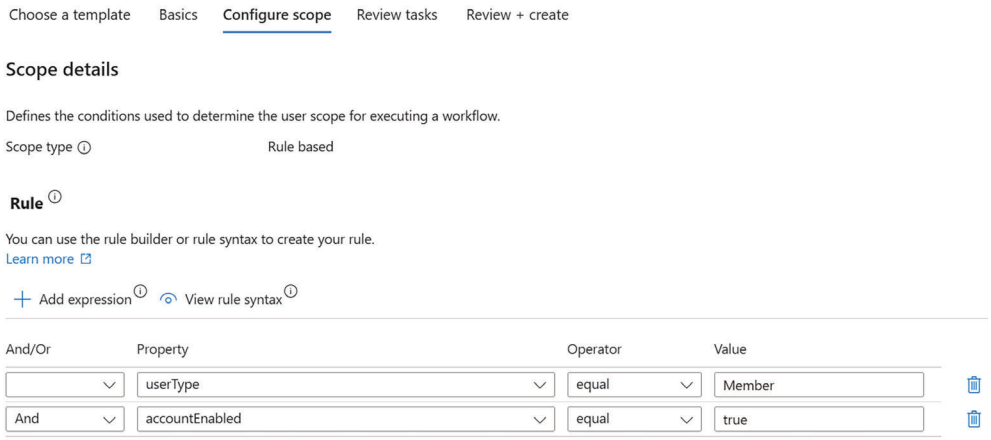


Figure 7.14: Offboard inactive users

5. These workflows come with a built-in task that sends an email informing recipients about the user's inactivity. This can be sent to the user themselves or the user's manager. In the case of guests, it can be sent to their sponsors. You can also choose to send emails to specific recipients.
6. Finally, you can choose to delete or disable the user's account. For users synchronized from on-premises Active Directory, lifecycle workflows can also delete or disable a user's on-premises account. Refer to the following screenshot:

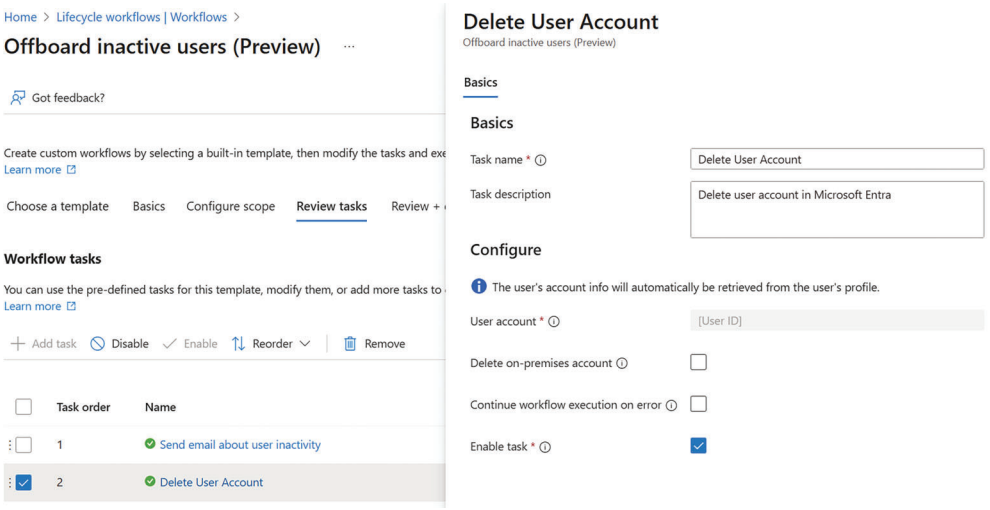


Figure 7.15: Delete inactive user account

7. Click **Next: Review + create**. Review the selected options, enable the workflow schedule and click **Create**.

The workflow will now run as per the configured schedule. This is an efficient way to manage inactive users in your environment.

Custom task extensions

As we have learned, lifecycle workflows have several built-in tasks that can be used in various joiner, mover, and leaver scenarios. These tasks may not be enough for some organizations. Lifecycle workflows offers the flexibility to create custom task extensions to call external systems as part of the workflow. For example, you may have a requirement that assigns the ownership of a user's OneDrive account and mailbox to a manager when the user leaves the organization. Lifecycle workflows use Azure Logic Apps to create these custom task extensions.

To use Azure Logic App to create a custom task extension you must have an Azure subscription with a resource group. You must also have the required permissions to create a new consumption-based Azure Logic App. You must have Logic App contributor, Contributor, or Owner Azure role on the Logic App, or at the resource group, subscription, or management group level.

Custom task extensions interact with lifecycle workflows in one of the following two ways:

- **Launch and continue**: If this is used when the workflow does not expect a response or feedback from the Azure Logic App. If the Logic App started successfully, it is considered a success. The next task in the workflow is immediately executed.
- **Launch and wait**: This is used when the workflow requires a response from the Logic App before executing the next task. A time duration is specified for how long the workflow should wait for the Logic App to respond. If the Logic App does not respond in that time frame, the task is considered failed.
  When a custom extension waits for a response from a Logic App, the administrator can define which application can send a response. The response can be sent by:
  - **System-assigned managed identity**: This is the default option and uses the managed identity assigned to the Logic App.
  - **No authorization**: If using this option, administrators must manually assign application permissions (`LifecycleWorkflows.ReadWrite.All`) or role assignment (Lifecycle Workflows Administrator). This is not recommended as this does not follow the principle of least privilege.
  - **Existing application**: Choose an existing application or a system or user-assigned managed identity to respond.

The following are the high-level steps to use Azure Logic Apps with lifecycle workflows:

1. Create a consumption-based Azure Logic App.
2. Configure the Azure Logic App to be compatible with Lifecycle Workflows. Refer to `https://learn.microsoft.com/en-us/entra/id-governance/configure-logic-app-lifecycle-workflows`.
3. Build the business logic within the Azure Logic App.
4. Create a lifecycle workflow custom extension to hold the information about the Azure Logic App. Following are the detailed steps:
   a. Login to `https://entra.microsoft.com` and navigate to **ID Governance | Lifecycle workflows | Custom extensions**.
   b. Click **Add a custom extension**.
   c. On the **Basics** page, give a name and description for the custom extension. Click **Next: Task behavior**.
   d. Under the **Task behavior** tab, select the task behavior as either **Launch and continue** or **Launch and wait**. Select the other options and click **Next: Details**.

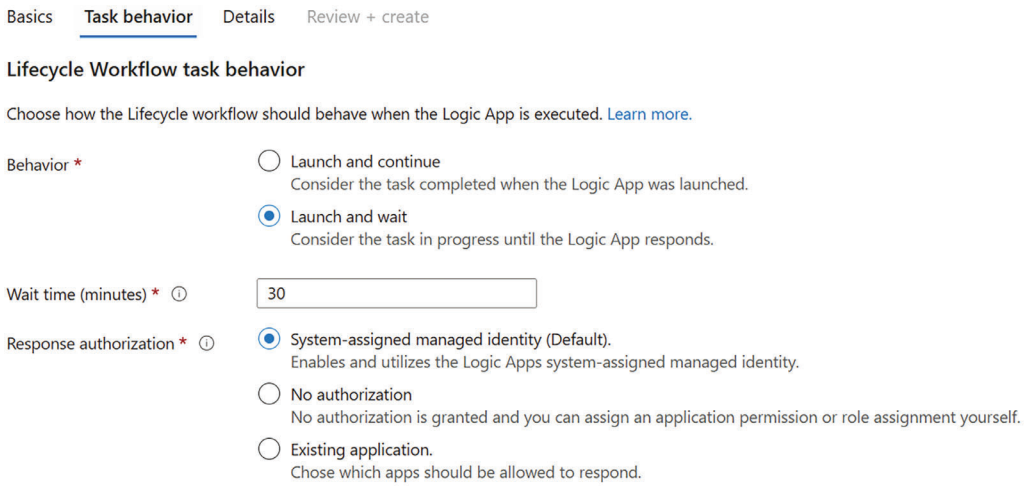


Figure 7.16: Define task behavior

e. On the **Details** page, select **Yes** if you want to create a new Logic App. Select **No** if you want to use an existing Logic App that has already been made compatible or was created using lifecycle workflows. Refer to the following figure. Click **Next: Review + create**.

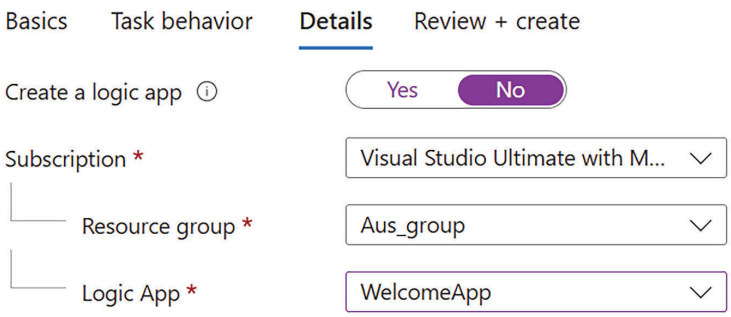


Figure 7.17: Create a Logic App

f. Review the settings and click **Create** to create the custom extension.

5. Create a lifecycle workflow with the **Run a custom task extension task** and refer to the custom extension just created. Refer to the section, *Creating a lifecycle workflow*.

Using Logic Apps with lifecycle workflows provides seamless automation and integration, allowing for efficient management of complex processes across various services.

Workflow insights

Workflow insights provide administrators with a quick view of workflow execution and their effectiveness. It provides summaries of the number of successful workflows and tasks and the users processed. To access workflow insights, login to `https://entra.microsoft.com` and navigate to **ID Governance | Lifecycle workflows | Overview | Workflow insights**. The following figure shows an example of the dashboard:

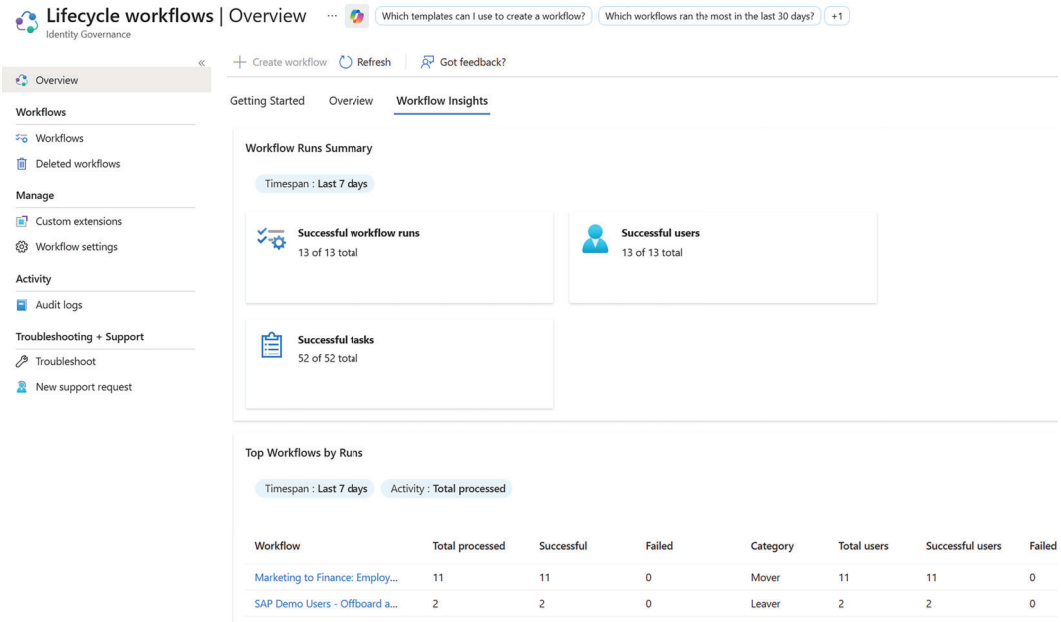


Figure 7.18: Workflow insights

You can change the **Timespan** to see the workflows from the past 7, 14, or 30 days.

Effective lifecycle workflows are defined by how reliably they deliver the right identity, access, and governance outcomes at scale. To evaluate whether a workflow is performing as intended, organizations can rely on a set of measurable **Key Performance Indicators** (**KPIs**). Workflow insights provide some KPIs that help administrators measure the effectiveness of LCW in their organization.

In addition, organizations can gauge the user and stakeholder experience by measuring the percentage of users that are provisioned with the correct access before the joining date, joiner satisfaction score that indicates how quickly new hires become productive, average time taken to deprovision a user and more.

Summary

In this chapter, we learned how we can use Lifecycle workflows to automate the identity lifecycle across the joiner, mover and leaver scenarios. This chapter went deep into explaining the components of Lifecycle Workflows, roles and licensing requirements. You also learned how to create lifecycle workflows to manage the different stages of the identity lifecycle. This chapter also explained the various options available in lifecycle workflows like versioning, email customization and reports. You also learned how to efficiently manage inactive users. Finally, the chapter explained how you can expand the scope of lifecycle workflows using Azure Logic Apps. In the next chapter, we will learn how to protect privileged accounts using Microsoft Entra Privileged Identity Management.

Exercises

1. Which of the following best describes the purpose of a lifecycle workflow in identity management systems?
    a. To monitor network traffic and detect anomalies
    b. To automate user provisioning, deprovisioning, and access updates based on role or status changes
    c. To encrypt user credentials during authentication
    d. To manage software updates across enterprise devices
2. In a lifecycle workflow, which of the following would most likely serve as a trigger for initiating a user deprovisioning process?
    a. A user's department changes from Sales to Marketing
    b. A user's last login exceeds 30 days
    c. A user's employment status changes to "Terminated"
    d. A user requests access to a new application
3. Which of the following actions can be automated using a lifecycle workflow when a user transitions to a new role within an organization?
    a. Sending a company-wide announcement email
    b. Updating the user's profile picture
    c. Assigning new group memberships and revoking outdated access
    d. Changing the user's preferred language setting

Answers

1. b
2. c
3. c

Additional resources

- Automatic user provisioning from Workday to Microsoft Entra ID: `https://learn.microsoft.com/en-us/entra/identity/saas-apps/workday-inbound-cloud-only-tutorial`
- Automatic user provisioning from SuccessFactors to Microsoft Entra ID: `https://learn.microsoft.com/en-us/entra/identity/saas-apps/sap-successfactors-inbound-provisioning-cloud-only-tutorial`
- Automatic user provisioning from Workday to Active Directory: `https://learn.microsoft.com/en-us/entra/identity/saas-apps/workday-inbound-tutorial`
- Automatic user provisioning from SuccessFactors to Active Directory: `https://learn.microsoft.com/en-us/entra/identity/saas-apps/sap-successfactors-inbound-provisioning-tutorial`
- API-driven inbound provisioning: `https://learn.microsoft.com/en-us/entra/identity/app-provisioning/inbound-provisioning-api-configure-app`
- Attribute synchronization for lifecycle workflows: `https://learn.microsoft.com/en-us/entra/id-governance/how-to-lifecycle-workflow-sync-attributes`

Get this book's PDF version and more

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.





Note: Keep your invoice handy. Purchases made directly from Packt don't require an invoice.

8

Microsoft Entra Privileged Identity Management

Privileged identities are a critical component in modern security strategies, particularly for organizations utilizing cloud and hybrid environments. These identities refer to accounts or users that are granted elevated permissions, enabling them to perform sensitive operations, such as managing user access, configuring systems, or administering critical resources. Because these accounts hold the keys to an organization's most important assets, their management must be robust, systematic, and auditable.

Effective management of privileged identities involves several best practices. Firstly, access should be granted only when absolutely necessary, following the principle of least privilege. This means limiting the scope and duration of elevated access, so that users only have the necessary permissions for the task at hand and only for as long as needed. **Microsoft Entra Privileged Identity Management (PIM)** facilitates this by providing just-in-time and time-bound access, requiring approval workflows, and enforcing multi-factor authentication for role activation. Additionally, regular access reviews and justification requests ensure that privileges are not retained longer than required, reducing the risk of misuse or compromise.

By centralizing and automating the management of privileged identities, organizations can significantly reduce their attack surface, maintain compliance with regulatory requirements, and improve overall security posture.

This chapter will cover:

- Introduction to privileged identities
- Deploying Privileged Identity Management
- Managing Privileged Identity Management
- Auditing PIM

Introduction to privileged identities

Privileged identities are specialized accounts or users within an organization that have been granted elevated permissions, allowing them to perform critical and sensitive operations that go beyond what standard users can do. These identities are central to the administration of IT systems, cloud services, and data resources because they have the authority to manage user access, configure infrastructure, oversee system security, and even alter or delete vital data. In a modern business environment the concept of privileged identities has become a cornerstone in the defense against cyber threats and the assurance of regulatory compliance.

Service accounts used by applications to access databases or perform automated tasks may also be considered privileged if they are granted broad access rights. Because these identities hold the "keys to the kingdom," they are highly attractive targets for cyber attackers. If compromised, a privileged account can be used to escalate attacks, exfiltrate sensitive data, or disrupt business operations on a large scale.

Managing privileged identities effectively is critical. The management of privileged identities involves several key strategies. First, access to privileged roles should be time-bound and just-in-time. Instead of granting permanent elevated access, organizations should provide privileged access only when it is needed and for a limited duration. **Microsoft Entra Privileged Identity Management (PIM)** automates this process by allowing users to activate privileged roles only after passing additional checks or approval workflows. These controls ensure that access is not only temporary but also auditable, providing a clear record of who accessed what resources and when.

In summary, privileged identities are essential but high-risk. Strong controls are essential to protect critical systems and minimize an organization's attack surface.

Now that we understand privileged accounts and their importance, let's explore Microsoft Entra Privileged Identity Management.

Overview of Microsoft Entra Privileged Identity Management

Microsoft Entra Privileged Identity Management (PIM) is a service that enables organizations to manage, control and monitor access to important resources like Microsoft Entra ID, Azure and other Microsoft Online services like Microsoft Intune and Microsoft 365. PIM provides time-based and approval-based role activation that minimizes the risk of excessive, unnecessary or misused access permissions on resources.

Organizations want to restrict the number of users that have privileged access to prevent a bad actor from getting that access or an authorized user inadvertently or maliciously misusing the access. However, IT admins still need privileges to carry out privileged operations in Microsoft Entra ID, Azure or Microsoft 365. Using PIM organizations can give admins just-in-time access to resources and oversee what they are doing with that access.

The following are some key features of PIM:

- It provides *just-in-time* access to Microsoft Entra ID and Azure resources
- It provides *time-bound* access to resources
- It can require *approval* to activate privileged roles
- It can enforce *MFA* to activate privileged roles
- It can ask for *justification* to activate the privileged role
- *Access reviews* can be conducted to ensure users still need the roles
- *Notifications* can be sent when privileged roles are activated
- *Audit history* is maintained for internal or external audits

Access to the following resources can be controlled using PIM:

- **Microsoft Entra roles**: Access to both built-in and custom roles can be managed using PIM. All Microsoft 365 roles like Exchange Administrator and SharePoint Administrator can be managed by PIM. However, service specific roles within Exchange RBAC or SharePoint RBAC are not supported.
- **Azure resource roles**: These include built-in and custom roles that grant access to management groups, subscriptions, resources groups and resources in Azure. Classic subscription administrator roles like Account Administrator, Service Administrator and Co-Administrator cannot be managed using PIM.
- **Groups**: Using PIM just-in-time access can be set up to assign users as members or owners of a Microsoft Entra security group or a Microsoft 365 group.

Using PIM, **Users** and **Groups** can be assigned to any of the above.

Role requirements

The following table explains the roles required to manage PIM for Microsoft Entra and Azure roles:

Resource type	Roles	Scope
Microsoft Entra roles	• Privileged Role Administrator • Global Administrator	Manage assignments for other administrators.
Microsoft Entra roles	• Global Administrators • Security Administrators • Global Readers • Security Readers	View assignments to Microsoft Entra roles.
Azure resource roles	• Owner or User Access Administrator at the target Azure scope	Manage assignments for other administrators.

Table 8.1: RBAC for PIM

Following the principle of Zero Trust, ensure that administrators are assigned the right roles to manage PIM.

Terminology

Before going further let's review some frequently used terms in PIM. They will be helpful in understanding further concepts explained in this chapter.

Term	Role assignment category	Description
Eligible	Type	If a user is *eligible* for a role, they must *activate* a role to be able to perform tasks associated with the role.
Active	Type	If a user has an *active* role, they can always perform the tasks associated with the role without any further action.

Term	Role assignment category	Description
Activate		The action performed by a user to turn an *eligible* role into an *active* one.
Assigned	State	A user that has an *active* role assignment.
Activated	State	When a user with an *eligible* role, *activates* the role and the role is now *active*.
Permanent eligible	Duration	A role assignment where the user is always *eligible* to *activate* the role.
Permanent active	Duration	A role assignment where the user has a permanently *active* role.
Time-bound eligible	Duration	A role assignment where the user is *eligible* to *activate* role for a limited duration.
Time-bound active	Duration	A role assignment where the user has an *active* role for a limited duration.

Table 8.2: PIM terminology

It is recommended to have zero permanently active members for roles other than two cloud-only emergency accounts permanently assigned the Global Administrator role.

Emergency access accounts

Organizations need to ensure that administrators are not accidentally locked out of Microsoft Entra because they cannot sign in or activate a role. This can be done by creating **emergency access accounts**. These accounts, also called **break glass accounts**, are limited to emergency scenarios where normal administrative accounts cannot be used.

Break glass accounts may be required in the following situations:

- The user accounts are federated from on-premises Active Directory and federation is unavailable.
- The administrators are registered to use MFA, and devices are unavailable or the service is unavailable.

- The last Global Administrator left the organization. While Microsoft Entra ID prevents the deletion of the last Global Administrator account, it can still be disabled or deleted on-premises.
- Natural disasters due to which cellular or other services are unavailable.
- If activating the Global Administrator or Privileged Role Administrator role requires approval and no approvers are assigned or all approvers are removed from the directory.

Follow the steps below to create an emergency access account. These should be cloud-only accounts that use the `*.onmicrosoft.com` domain and are not synchronized from on-premises Active Directory.

1. Create a new user account and permanently assign the Global Administrator role.
2. Select a passwordless authentication method like Passkey or certificate-based authentication to satisfy the mandatory MFA requirements.
3. Configure the emergency account to use the assigned passwordless authentication method.
4. Create a Conditional Access policy to require phishing resistant MFA for the emergency accounts.
5. Store account credentials safely.
6. Regularly monitor the sign-in and audit logs for any unusual activity on these accounts.
7. Validate the accounts regularly.

In most organizations, emergency access accounts are not associated with any user. Credentials are set to never expire and are stored in a secure location known to multiple members of the IT staff. These accounts are not connected to employee devices. A secure access workstation must be used to use these accounts.

Role assignment overview

Several people are involved in the PIM process. It starts with a privileged role administrator who sets up PIM for eligible users. An eligible user then requests activation of a role to complete an associated task. An approver reviews this request and approves or rejects it. The requestor completes the task. If required, the requestor can extend or renew their access. The following table summarizes these personas with their permissions:

Persona	Permissions
Privileged Role administrator	Enable approval for specific roles. Specify approvers to approve requests. View request and approval history for all privileged roles.
Approver	View pending approval requests. Approve or reject requests. Provide business justification for approval or rejection.
Eligible role user	Request activation of a role. View the status of the request.

Table 8.3: PIM personas and permissions

Following the principle of Zero Trust, the above personas must be separate individuals. This ensures that the person who applies for a PIM elevated role and the approvers are not the same individual.

Licensing requirements

Following are the licensing requirements to use PIM:

- PIM requires a Microsoft Entra ID P2 or Microsoft Entra ID Governance license.
- Users with eligible and/or time-bound assignments to Microsoft Entra ID or Azure roles must be assigned a license.
- Users with eligible and/or time-bound assignments as members or owners of PIM for Groups must be assigned a license.
- Users who can approve or reject activation requests must be assigned a license.

Ensure that these requirements are met before proceeding further.

PIM vs direct role assignment

A major decision organizations must make is when to use PIM and when to assign roles directly to a user. The following table provides a comparison of governance, risk and operational factors that help administrators decide when to apply least privilege while balancing productivity and scalability:

Criteria	Use PIM	Use Direct Role Assignment
Access Type	Privileged, high-impact, or sensitive roles (Global Admin, Security Admin, etc.)	Low-impact or routine roles (Reader or narrowly scoped custom roles)
Access Frequency	Occasional, project-based, or on-call	Continuous, daily operational need
Governance Requirements	Requires MFA, approval, justification, audit logs, or access reviews	Minimal governance; direct oversight acceptable
Risk Tolerance	Low tolerance for standing privileges or credential exposure	Moderate tolerance; trusted, stable identities
Team Size / Role Sharing	Multiple users share the same privileged role (use PIM for Groups)	Few users; individual accountability preferred
Compliance / Audit Needs	High compliance or regulatory oversight	Internal or low-risk environments
Operational Overhead	Reduces overhead by automating elevation and reviews	Simpler when user count is small
Scalability	Scales easily with dynamic teams and lifecycle management	Manual updates required for each user
Identity Hygiene	Eliminates standing admin rights; enforces least privilege	Acceptable for permanent, low-risk access

Criteria	Use PIM	Use Direct Role Assignment
Zero-Trust Alignment	Fully aligned (just-in-time, least privilege, verified trust)	Partial alignment; relies on static trust model

Table 8.4: PIM vs direct role assignment

Using this table, organizations can decide when to use PIM and when to use direct role assignment.

Plan PIM deployment

Planning a PIM deployment is a critical step for organizations aiming to enhance their security posture and manage access to sensitive resources effectively. Without thorough planning, organizations may face challenges in assigning the correct roles, ensuring compliance, and maintaining visibility over privileged activities. A well-conceived deployment plan helps identify which roles require PIM, ensures that all licensing requirements are met, and establishes clear processes for approval and activation workflows. This preparation not only minimizes the risk of unauthorized access but also streamlines the user experience for those who legitimately need elevated privileges.

Furthermore, planning allows organizations to align PIM implementation with broader IT governance and compliance objectives. By mapping out business needs, regulatory requirements, and operational processes beforehand, organizations can configure PIM settings —such as approval requirements, notification policies, and auditing mechanisms—in a way that supports both security and productivity. It also provides an opportunity to educate stakeholders about the new processes, reducing confusion and resistance during rollout. A strategic approach to PIM deployment ensures that privileged access is granted only when necessary, for the right duration, and under proper oversight, thereby reducing the attack surface and supporting ongoing risk management efforts.

It is recommended to start with a pilot which will consist of a small set of test users to ensure that PIM behaves as expected. Develop test cases to test all aspects of PIM, like PIM for Entra roles, Azure roles, and groups. This should include members of a group, members of a role, IT service owner, subscription or resource owner in Azure and owners of groups. This way you can verify that all configuration is set up correctly and move to production with confidence. Communication is critical for the success of PIM. Proactively communicate with users and educate them on how their experience will change and how they can get support if required. It is also important to have a rollback plan in place in case PIM fails to work as desired.

Microsoft Entra and Azure roles

Before starting implementation, it is important to plan. The following steps will assist you in preparing to manage Microsoft Entra and Azure roles using PIM:

1. **Discover privileged roles**: List users that have privileged roles in the tenant. Review their access, identify users who don't need that access and remove it if required. You can use Microsoft Entra access reviews to automate this process.
2. **Identify the roles to be managed by PIM**: Prioritize the roles that have the most permissions to be managed by PIM first. Ensure that Global Administrator and Security Administrator are PIM managed as those are highly privileged and can cause the most harm if compromised. Next, consider the roles that may be most susceptible to attack. Microsoft Entra identifies privileged roles with a PRIVILEGED label. Use that to identify other privileged roles.
   For Azure, it is recommended that all Subscription Owner and User Access Administrator roles be managed using PIM.
3. **Configure settings**: Identify the settings you would like to configure for the identified roles. For example, you might want all requests for the Global Administrator role to be manually approved, and the role be activated for only one hour.

Once this groundwork is done you can proceed with creating role assignments for eligible users.

> **Note**
>
> When a role is assigned, the assignment cannot be for less than five minutes, and it cannot be removed within five minutes of assignment.

Groups

Sometimes users could have multiple eligible assignments in Microsoft Entra. They would have to activate each role individually. To make matters worse, they may have multiple Azure resources assigned to them for which they need to elevate permissions using PIM. This is where **PIM for Groups** helps. PIM for Groups can be used to govern access to resources like Microsoft Entra roles, Azure roles, Azure SQL, Azure Key Vault, Intune and other applications. It is important to identify the groups that you would like to manage using PIM. Any cloud-only Microsoft 365 or Security group with static membership can be enabled for PIM for Groups. Using nested groups is not recommended. These groups are assigned permanent active access to resources, and their membership or ownership is then managed using PIM. Both **role-assignable groups** and **non-role-assignable groups** can be enabled for PIM for Groups. If you

want to assign Microsoft Entra roles to a group, a role-assignable group must be created. Role-assignable groups is explained in *Chapter 2, Fundamentals of Microsoft Entra ID*.

It is recommended to create a role-assignable group even if you don't intend to assign roles to the group, but the group provides access to sensitive resources. This is because role-assignable groups have extra protection built in, such as:

- Only Global Administrators, Privileged Role Administrators, or the group owner can manage a role-assignable group.
- No other user can change the credentials of members of a role-assignable group. This prevents an administrator from elevating to a higher privileged role without going through an approval process.

Microsoft Entra ID does not allow removal of the last active owner of a group. For example, if a group has an active owner user A and an eligible owner user B, user B activates their ownership of the group using PIM. Meanwhile, user A is removed from group ownership or from the tenant. In this case, the deactivation of the owner role for user B will not succeed as they are the last active owner. PIM will try to deactivate the owner role for user B for 30 days and if another owner is not added within 30 days, PIM will stop attempting the deactivation and user B will continue as the owner of the group.

Start using PIM

With all the basics covered, you are now ready to start using PIM. You can now create eligible or time-bound assignments for Microsoft Entra and Azure roles. The following sections explain the PIM process for Microsoft Entra roles, Azure roles, and groups.

Microsoft Entra roles

By enabling PIM for Entra roles, organizations can move from standing admin access to just-in-time, time-bound elevation, dramatically reducing the attack surface. Using PIM for Entra roles, administrators can request elevated permissions when they need to carry out a privileged task, such as password resets or creating Conditional Access policies. This access can be time-bound and automatically revoked after a predetermined time. By eliminating unnecessary permanent assignments and adding oversight to high-impact roles, PIM helps organizations prevent misuse, contain credential compromise, and maintain a clean, least-privileged environment that aligns with zero-trust principles.

Enabling PIM for Microsoft Entra roles has a few steps. These are detailed below.

Preparing a role for PIM

In preparation to use PIM for Microsoft Entra roles, it is recommended that the roles be prepared for PIM. A Global Administrator or Privileged Role Administrator is required to edit

role settings. These settings define the activation duration for a role, whether Conditional Access is required to activate the role or if approvals are required. Follow the steps below to configure role settings:

1. Sign in to `https://entra.microsoft.com` and navigate to **ID Governance | Privileged Identity Management | Microsoft Entra roles | Roles**. The right pane will display all roles available in Microsoft Entra ID that can be configured with PIM.
2. Select a role and click on **Role settings**. Click on **Edit**.

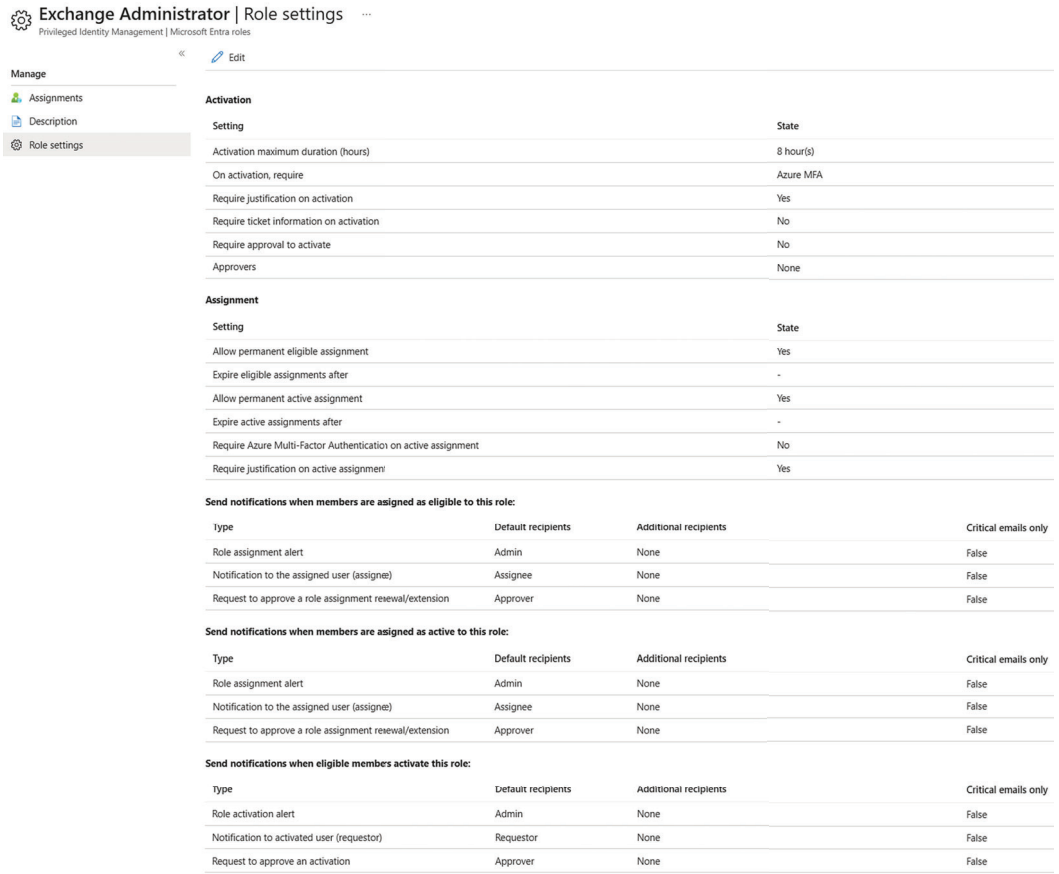


Figure 8.1: Role settings

3. On the **Activation** page, you can select options like maximum activation duration, approvers and more. Review the options in the following figure. Click **Next: Assignment**.

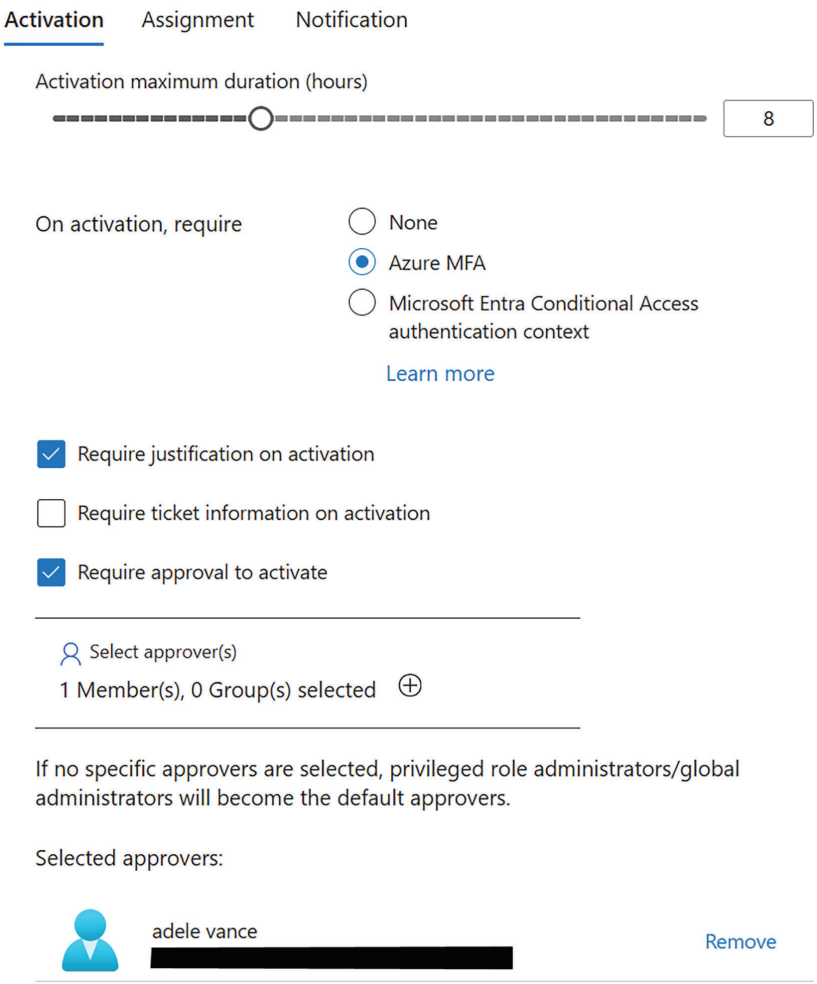


Figure 8.2: Role activation settings

4. On the **Assignment** page, select the duration after which permanent eligible assignments will expire and if the role will allow permanent active assignments. Click **Next: Notification**.

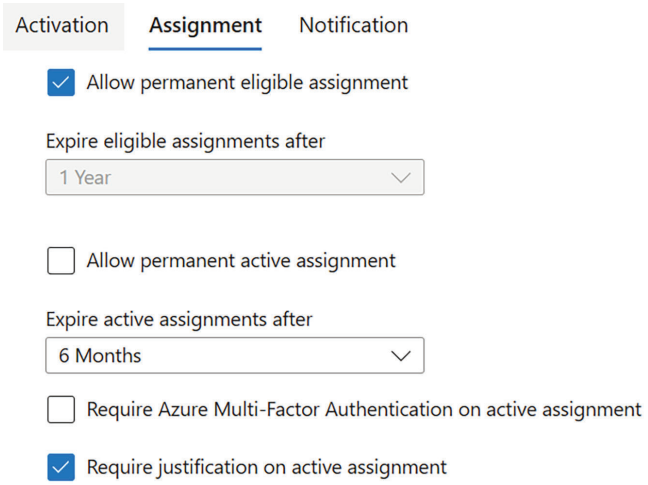


Figure 8.3: Role assignment settings

5. On the **Notification** page, select when and to whom notifications are sent. Click **Update**.

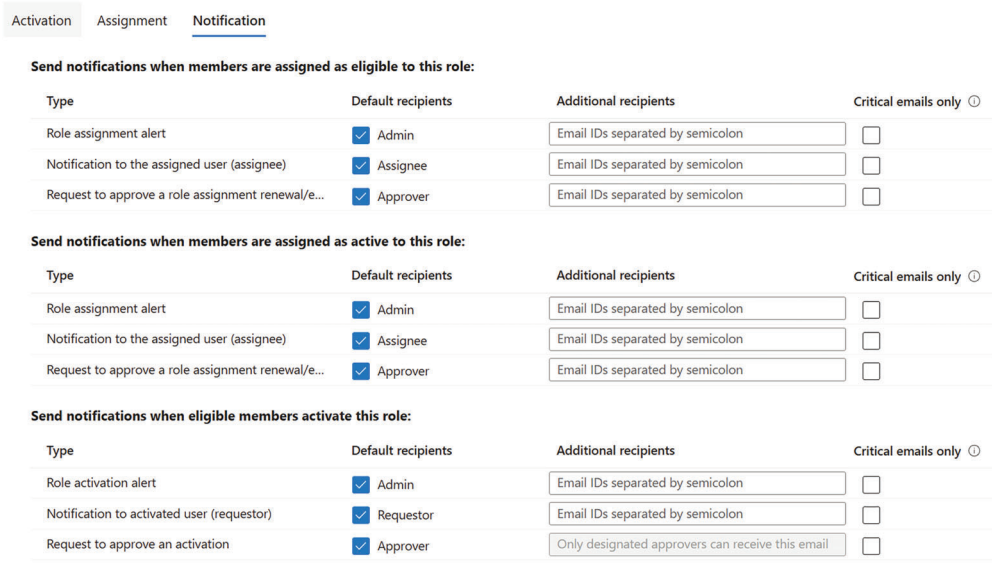


Figure 8.4: Role notification settings

Configure these settings for each role that will be managed using PIM.

Assigning a role

Roles in Microsoft Entra ID can be assigned at a tenant scope, administrative unit scope or app registration scope.

Assigning roles with tenant scope

Assigning a role with tenant scope means that the user with the role will be able to make changes that affect the entire Microsoft Entra tenant. Only users with the Global Administrator or Privileged Role Administrator role can assign roles. Follow the steps below to assign a role:

1. In the Entra portal, navigate to **ID Governance | Privileged Identity Management | Microsoft Entra roles | Roles**.
2. Select the role for which assignments need to be added and click on **Add assignments** at the top.
3. On the **Membership** page, click on **No member selected** to select members. In the flyout pane select the users you want to add to the role and click on **Select**. On the next screen click **Next**. Refer to *Figure 8.5*:

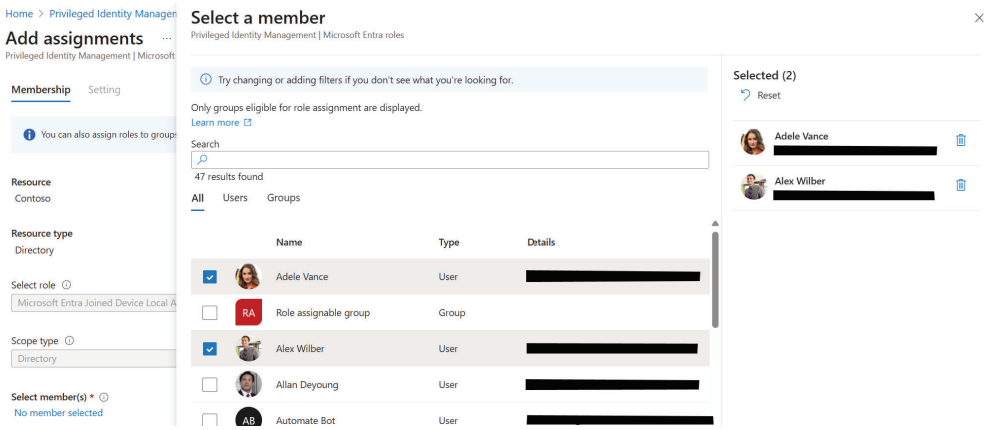


Figure 8.5: Add users to role

4. On the **Setting** page select if the assignment type is **Eligible** or **Active**. Unchecking the **Permanently eligible** box will make the role time-bound, and a start and end date can be selected. Refer to picture below. Click on **Assign**.

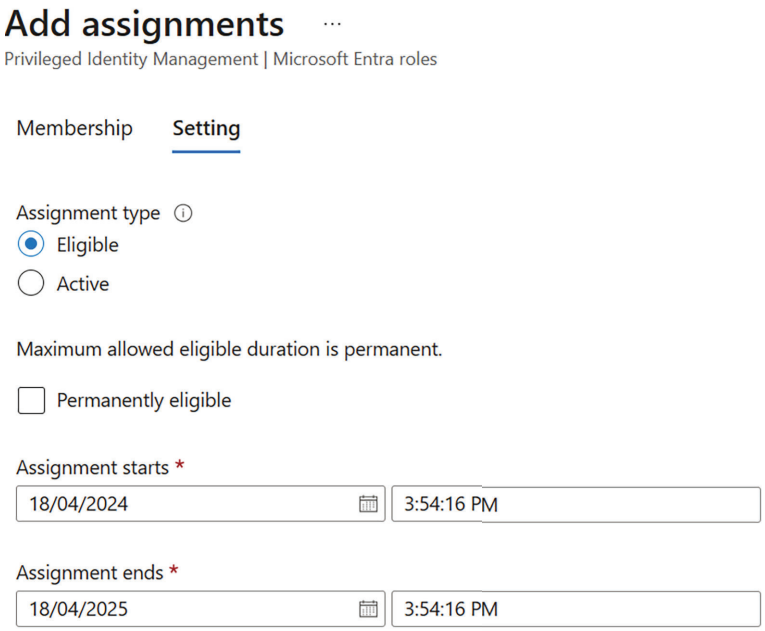


Figure 8.6: Role assignment settings

An eligible selected user will now be able to activate the role.

Assigning roles with app registration scope

By default, custom and built-in roles are assigned at the tenant level and grant access over all app registrations in the tenant. All custom roles and some built-in roles can also be assigned at the scope of a single Microsoft Entra application. This allows organizations to give users access to update the properties of a single app without having to create multiple custom roles. To assign a role with the app registration scope follow the steps below:

1. Sign in to `https://entra.microsoft.com` as an **Application Developer**.
2. Navigate to **Entra ID | App registrations**.
3. Select the application and click on **Roles and administrators**. The left pane will show a list of all roles that can be assigned to the selected application. Select the desired role.

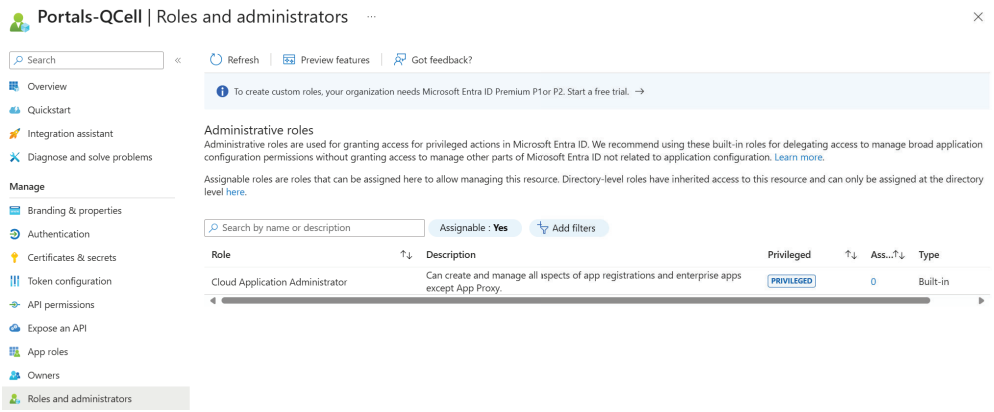


Figure 8.7: Assign role at app registration scope

Tip

All Microsoft Entra roles will not show up in this list. This is expected, as by design only the roles that have permissions to manage the app registration are displayed.

4. Select a role and click on **Add assignments**. Select the users or groups that you want to assign this role to and click on **Add**.

This will give the selected users and groups permission only to manage the selected app registration.

Assigning role with administrative unit scope

Most roles in Microsoft Entra are assigned at the tenant level. There are some roles that can be assigned at an **Administrative Unit** level. This enables decentralized administration and granular control. Administrative Units are explained in *Chapter 3, Implementing Microsoft Entra ID*. The following roles can be assigned at an administrative unit level:

- Authentication Administrator
- Attribute Assignment Administrator
- Attribute Assignment Reader
- Cloud Device Administrator
- Groups Administrator
- Helpdesk Administrator
- License Administrator

- Password Administrator
- Printer Administrator
- Privileged Authentication Administrator
- SharePoint Administrator
- Teams Administrator
- Teams Devices Administrator
- User Administrator

In addition, any custom role can be assigned with administrative unit scope if the custom role includes at least one permission relevant to users, groups or devices.

Certain permissions apply only to non-administrative users when applied at the administrative unit level. For example, a Helpdesk Administrator can reset passwords of only non-administrative users in the administrative unit. Following is the list of actions that cannot be carried out if the target of the action is another administrator:

- Reading or modifying user authentication methods.
- Resetting passwords.
- Modifying sensitive properties like phone numbers, email addresses, or OAuth secret keys.
- Deleting or restoring user accounts.

Users, Microsoft Entra role-assignable groups and service principals can be assigned to a role with an administrative unit scope.

Following are the steps to assign a role with an administrative unit scope:

1. Sign in to `https://entra.microsoft.com` as a **Privileged Role Administrator**.
2. Navigate to **ID Governance** | **Microsoft Entra roles** | **Roles**.
3. Click on **Add assignments**.
4. From the **Select role** drop-down box, select a role from the above list.
5. From the **Scope type** drop down box, select **Administrative unit**.
6. Under **Selected scope**, click on **No scope selected** and select the appropriate administrative unit(s) and click **Select**.

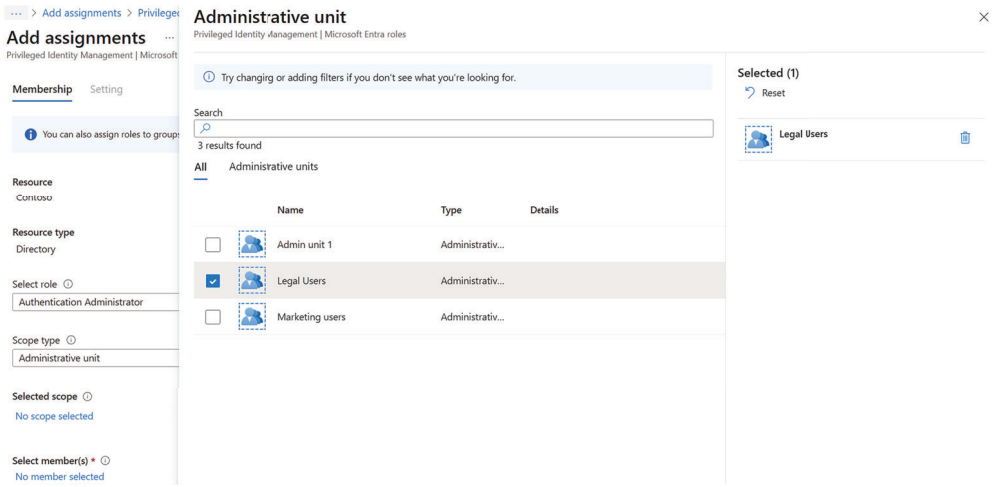


Figure 8.8: Select administrative unit scope

7. Click on **No members selected** and select the users. Click **Next**.
8. On the **Setting** page select if the assignment type is **Eligible** or **Active**. Unchecking the **Permanently eligible** box will make the role time-bound, and a start and end date can be selected. Refer to picture below. Click on **Assign**.

The selected users will now have the selected role in the selected administrative unit.

Activating a role

If a user has been assigned an *active* role assignment, they are added to the role group with no further action from their end. However, if they were made *eligible* for the role, they will have to *activate* the role before they can perform privileged actions. To *activate* a role, follow the steps below:

1. In the Microsoft Entra admin center, navigate to **ID Governance | Privileged Identity Management | My roles**. The right pane will list all the **Eligible assignments**. Refer to *Figure 8.9*.

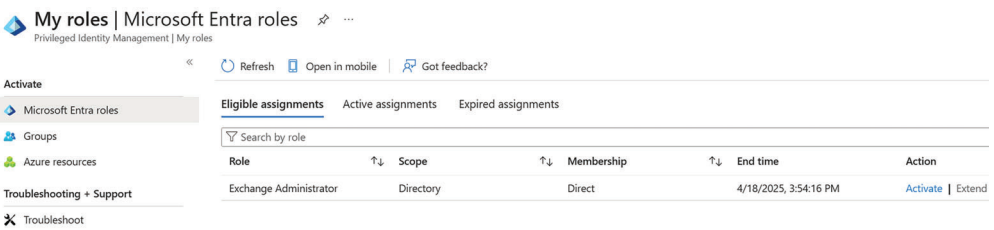


Figure 8.9: Eligible assignments

2. Click on **Activate**. In the flyout pane, enter an activation duration and provide a reason for activation. You can also choose a custom activation start time. If this is selected, the activation will start from that time. In the below example, the role will be activated on 18th April 2024 at 4:30PM and will be active for 2 hours.

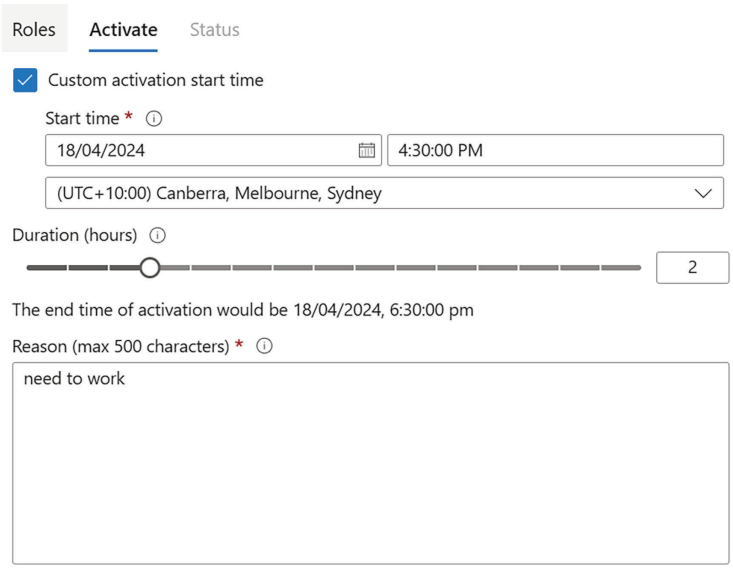


Figure 8.10: Activate the role

3. If role activation is subject to additional verification like completing MFA, as configured in the role settings, a banner will appear asking the user to complete additional verification. Click on the banner to follow the instructions to provide additional verification. Once complete, click on **Activate**.

Note

When a role is activated, PIM creates active assignments (adds user to the role) within seconds. When the activation expires, either due to expiry of time or due to manual deactivation, PIM removes the active assignment (removes user from the role) within seconds.

If the role settings require that role activation be approved, a designated approver will be required to approve the request before the role is activated.

Approving assignments

Depending on the communication settings configured in the role settings, the approver(s) will receive an email notifying them that a request is pending approval. To approve PIM requests, approvers must login to `https://entra.microsoft.com` and navigate to **ID Governance** | **Privileged identity management** | **Approve requests**. Under **Request for role activations** review each request and click on **Approve** or **Deny**. Refer to picture below:

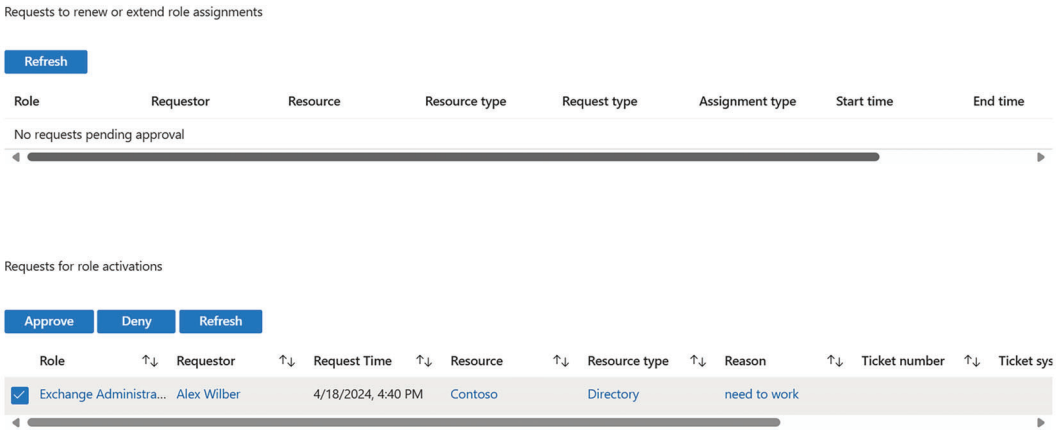


Figure 8.11: Approve requests

Now the requester can complete the task for which they had requested this role activation.

Extending assignment

Only Global Administrators and Privileged Role Administrators can extend Microsoft Entra role assignments. Both active and eligible assignments become eligible for extension 14 days prior to expiry. In the above example, the assignment for the Exchange Administrator is set to expire on 18th April 2025. Refer to *Figure 8.9*. On 4th April 2025, this assignment will become eligible for extension and the **Extend** link will be activated. To request an extension, the user can click on the **Extend** link and enter a justification for the extension request. The approver can approve or reject the extension request from the **Request to renew or extend role assignments** section of the portal. Refer to the following figure:

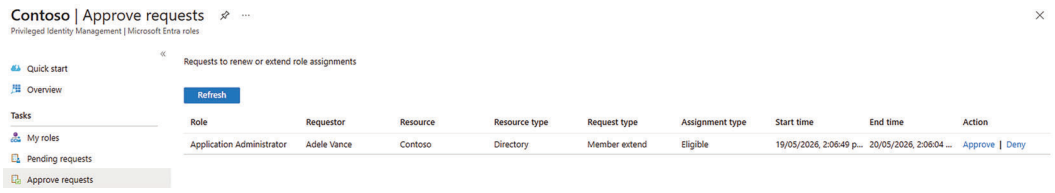


Figure 8.12: Extension request approval

Approvers can also extend the request without the user having to request an extension. This can be done from the **Assignments** page of the selected role. Refer to the following figure:

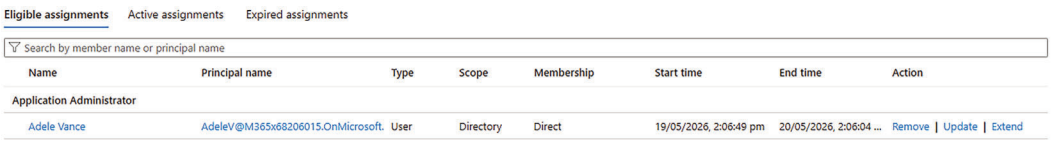


Figure 8.13: Admin initiated extension

Azure resource roles

Organizations that use PIM to protect Microsoft Entra roles can also use it to protect Azure resource roles. Enabling PIM for Azure roles is critical to reducing risk and enforcing least-privilege access across cloud environments. Azure admin roles are powerful and leaving them permanently assigned creates unnecessary exposure to credential theft, misuse, or lateral movement.

Selecting Azure resources

You need to have **Microsoft.Authorization/roleAssignments/write** permissions to the Azure resources. User Access Administrator and Owner roles have this permission. The following are the steps to discover Azure resources in PIM:

1. In the Microsoft Entra admin center navigate to **ID Governance | Privileged Identity Management | Azure resources**.
2. You can search at Management groups level, Subscriptions level, Resource groups level or Resources level. Make the appropriate selections and click on **Manage resource**. In the below picture, the resource group *Purview* is being chosen for management.

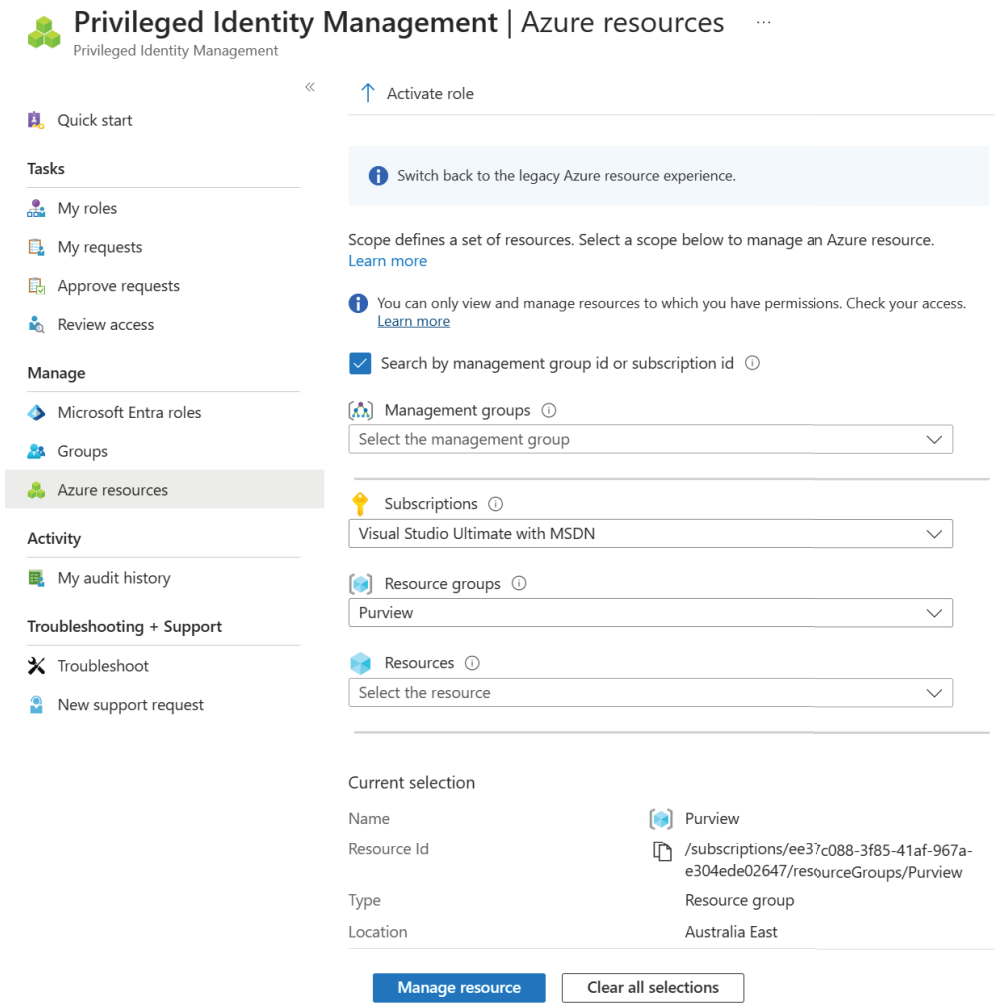


Figure 8.14: Manage Azure resources

This will bring the selected resources under PIM management. Once a management group or subscription is managed, it cannot be unmanaged.

Preparing a role for PIM

Like preparing a Microsoft Entra role for PIM, you must also prepare an Azure role for PIM. Resource Administrator permissions are required to manage PIM for resources. Users assigned to the User Access Administrator or Owner subscription roles and Microsoft Entra Global Administrator role have this permission and can manage role settings. Follow the steps below:

1. In the Microsoft Entra admin center navigate to **ID Governance | Privileged Identity Management | Azure resources**. You will see a list of managed Azure resources. Click on the resource you want to prepare the role for.
2. The next page will show a summary of role activations for the selected resource as shown in the following figure:

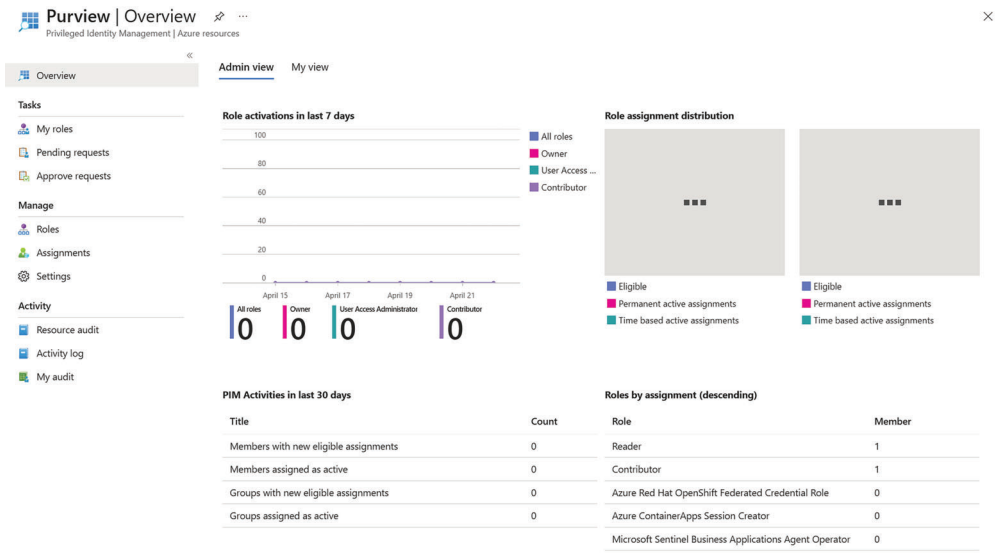


Figure 8.15: PIM activity

3. Click on **Settings**. The screen will list all the available roles. Select the role you want to prepare and make the appropriate changes by clicking on **Edit**.

The steps and settings available for Azure resource roles are the same as Microsoft Entra roles. These are described in the previous section.

Assigning a role

PIM can manage custom roles and built-in Azure resource roles like Owner, User Access Administrator, Contributor, and more. Resource Administrator permissions are required to manage PIM for resources. Users assigned to the User Access Administrator or Owner

subscription roles and Microsoft Entra Global Administrator role have this permission and can assign roles.

Azure attribute-based access control (Azure ABAC) can be used to add conditions on eligible role assignments. These conditions enable you to limit a user's permissions to a resource using fine-grained conditions. It also helps secure the role assignment with time-bound settings, approval workflow, and auditing. Conditions can be added to Storage Blob Data Contributor, Storage Blob Data Owner and Storage Blob Data Reader roles.

Follow the steps below to assign a role:

1. In *Figure 8.15*, click on **Roles** and at the top click on **Add assignments**.
2. On the **Membership** page, select the role you want to assign to the selected resource by picking from the **Select role** drop-down box.
3. Click on **No member selected** and from the flyout pane select the user to whom the role must be assigned to as shown in the following picture. Click **Select** and then click **Next**.

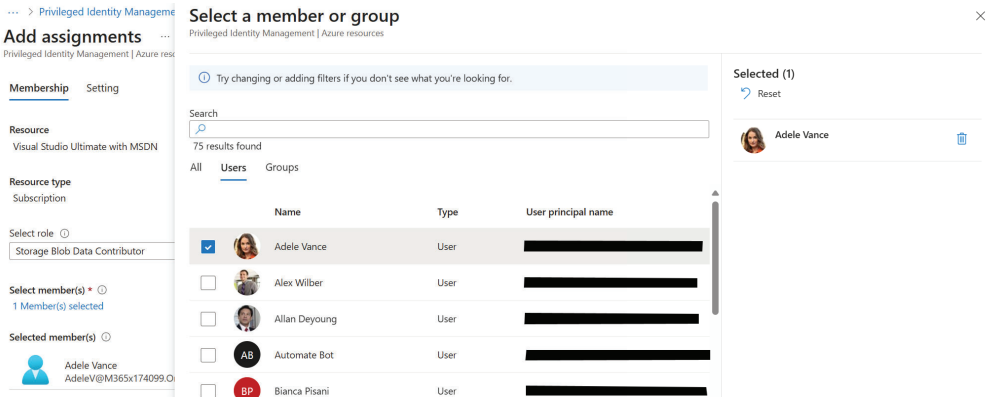


Figure 8.16: Assign a role

4. On the **Setting** page, select the appropriate **Assignment type** and select the start and end time.
5. If you have selected one of the Azure ABAC eligible roles, an additional option to add role assignment conditions will appear. Click on **Add condition** to launch the expression builder. Build the condition and click **Save**.

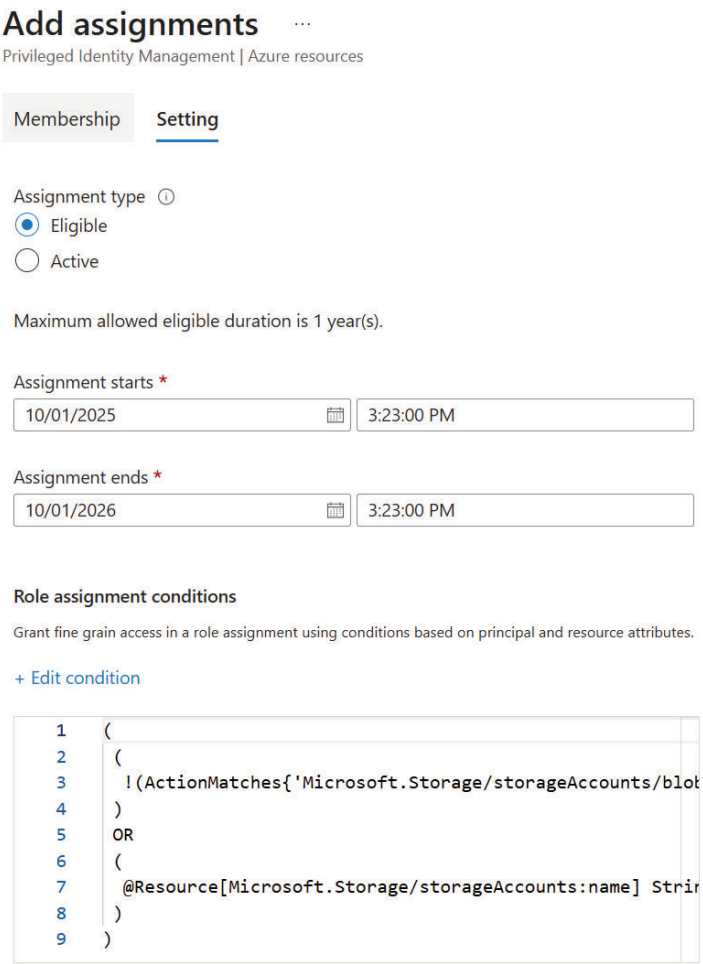


Figure 8.17: Assignment settings

6. Click **Assign** to assign the role.

The steps to activate, approve, and extend Azure roles are the same as those for activating, approving, and extending a Microsoft Entra role. Refer to the previous section for the exact steps.

Groups

Group memberships often grant broad, high-impact access across Azure and Microsoft 365. When groups are assigned to privileged roles, any permanent membership becomes a standing vulnerability. Using PIM, you can provide just-in-time membership or ownership of a group. PIM supports Microsoft Entra Security groups or M365 groups.

Bringing groups into PIM

Before a role can be managed using PIM, it must be brought under PIM management. The following table summarizes the roles required to bring groups under PIM management:

Group type	Roles required
Role-assignable group	Privileged Role Administrator Group Owner
Non-role assignable groups	Directory Writer Groups Administrator Identity Governance Administrator User Administrator Group Owner

Table 8.5: Roles required for groups

To bring a group under PIM management follow the steps below:

1. In the Microsoft Entra Admin center navigate to **ID Governance | Privileged Identity Management | Groups**. This page displays groups that are already enabled for PIM for Groups.

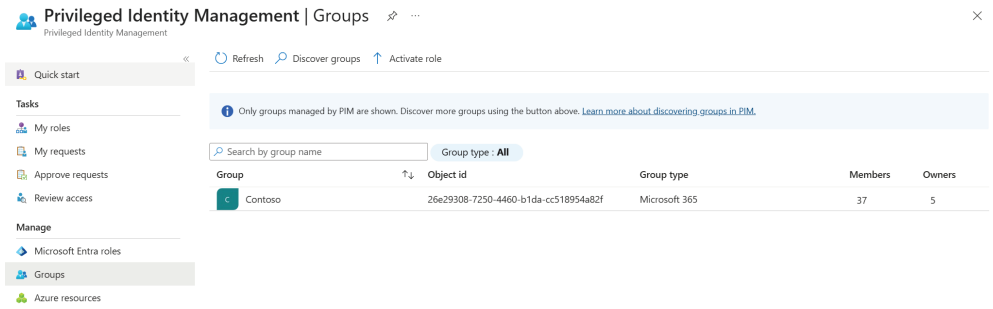


Figure 8.18: PIM for Groups

2. Click on **Discover groups** and select the group that you want to enable for PIM. Click **Manage groups**. In the pop-up box, click **OK**.

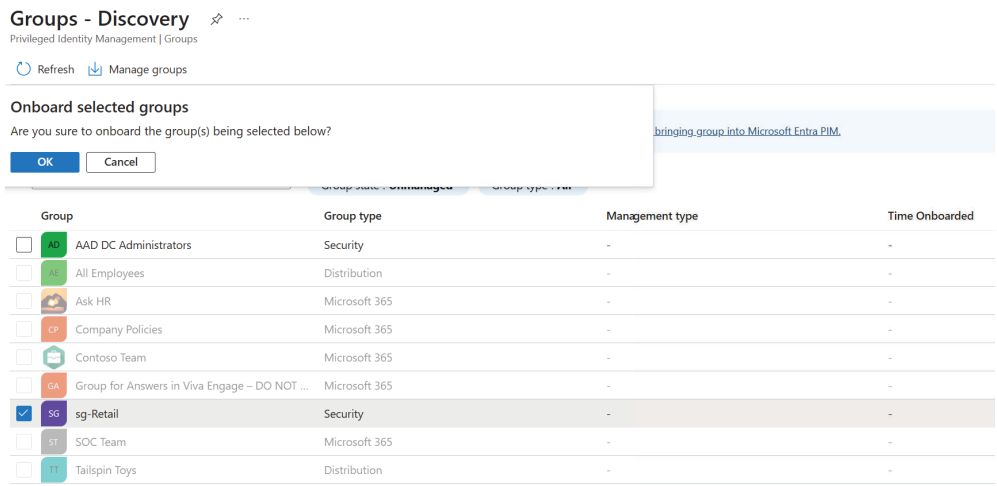


Figure 8.19: Manage groups

Alternatively, you can use the Groups pane to bring groups under PIM using the following steps:

1. In the Microsoft Entra Admin center navigate to **Entra ID | Groups | All groups**.
2. Select the group that you want to enable for PIM and click on **Privileged Identity Management**.
3. Click on **Enable PIM for this group** as shown in the following picture:

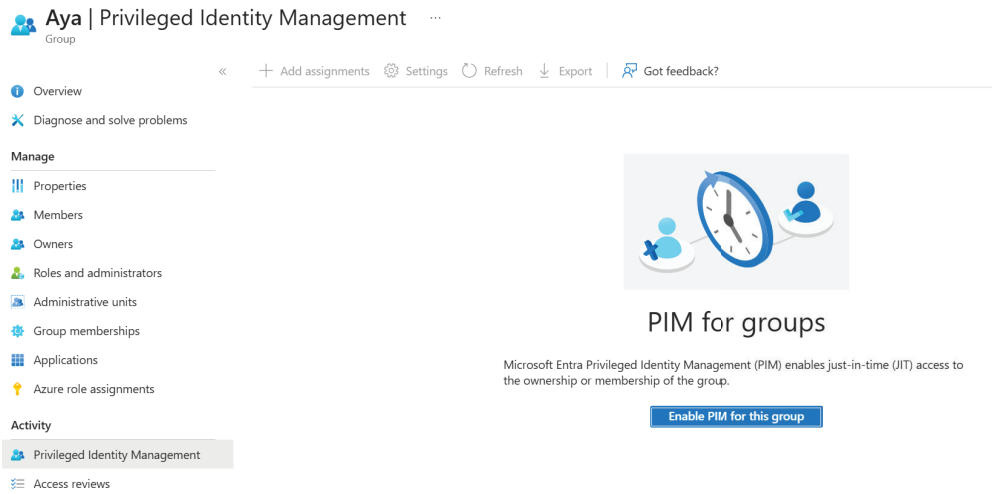


Figure 8.20: Enable PIM for a group

Once a group is managed, it cannot be removed from management.

Preparing the group for PIM

Once a group is added under PIM scope, various settings can be configured as described in the steps below:

1. In the Microsoft Entra Admin center navigate to **ID Governance | Privileged Identity Management | Groups**. You will see a list of groups that are already enabled for PIM for Groups.
2. Select the group you want to manage and click on **Settings**. You will see options for **Owner** and **Member** as shown in the following figure:



Figure 8.21: Group settings

3. Click on any one of them to open its settings. Click on **Edit** to make changes.

The steps and settings available for group members and owners are the same as Microsoft Entra roles. These are described in the previous section. Make the appropriate selections.

Assigning eligibility

When membership or ownership of a group is assigned using PIM, the assignment cannot be for less than five minutes, and it cannot be removed within five minutes of being assigned. Follow the steps below to make a user an eligible member or owner of a group:

1. In the Microsoft Entra Admin center navigate to **ID Governance | Privileged Identity Management | Groups**. You will see a list of groups that are already enabled for PIM for Groups.
2. Select the group you want to manage and click on **Roles**. This page will show the number of current active and eligible members and owners. Refer to the following figure.

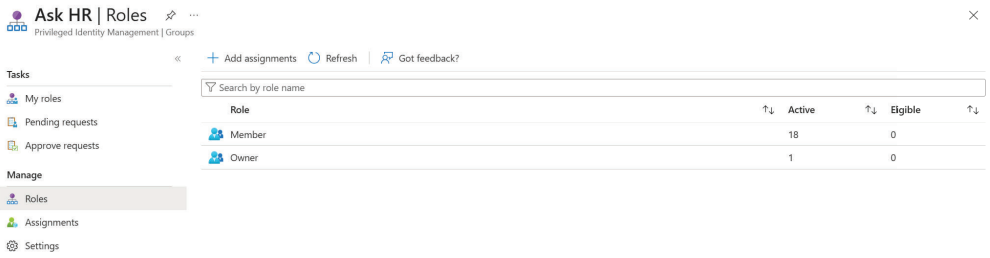


Figure 8.22: Assign group eligibility

3. Click on **Add assignments** and select the role from the dropdown list. **Member** and **Owner** are the choices available.
4. Click on **No member selected** to bring up a list of users. Select the user(s) you want to assign to the group and click on **Select**. Then click **Next**.

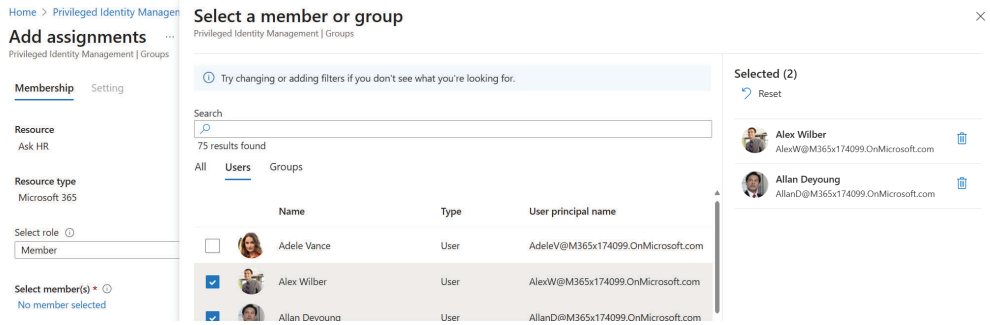


Figure 8.23: Select owners or members

5. On the **Setting** page, select the **Assignment type** as **Eligible** or **Active**. Select the start and end time and click on **Assign**.

The steps to activate, approve, and extend group assignments are the same as those for activating, approving, and extending a Microsoft Entra role. Refer to the previous section for the exact steps.

Alerts

PIM generates alerts when it detects suspicious activity in the Microsoft Entra ID tenant. When alerts are generated, they show up in the Microsoft Entra admin center. Administrators can select the alert to investigate further. Alerts are generated for Microsoft Entra and Azure roles. One event in PIM can generate email alerts to assignees, approvers, and administrators. The maximum number of emails sent per event is 1000. If the number of recipients exceeds 1000 only the first 1000 recipients will receive email notifications.

Microsoft Entra roles

The following table lists the events that will generate alerts for Microsoft Entra roles.

Alert	Severity
The organization doesn't have Entra ID Premium P2	High
Roles don't require multi-factor authentication	Medium
Eligible administrators aren't activating their privileged roles	Low
Roles are being assigned outside of Privileged Identity Management	High
Roles are being activated too frequently	Medium
There are too many global administrators	Low
Potential stale accounts in a privileged role	Medium

Table 8.6: Alerts for Entra roles

Some of these alerts have settings that can be customized by the administrator. The following are the steps to customize the alert settings:

1. In the Microsoft Entra Admin center navigate to **ID Governance | Privileged Identity Management | Microsoft Entra roles | Alerts | Settings**.
2. Click on the alert whose settings you would like to customize, make the necessary changes and click **Save**. Refer to the picture below.

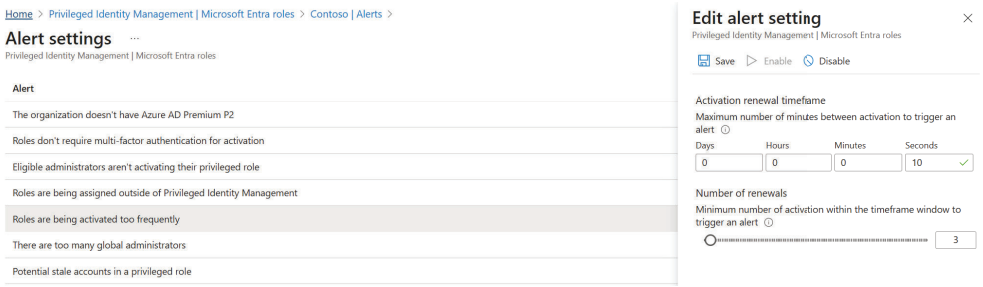


Figure 8.24: Edit alert settings

3. Once an alert is generated it will show up under **ID Governance | Privileged Identity Management | Microsoft Entra roles | Alerts** as shown in the following figure.

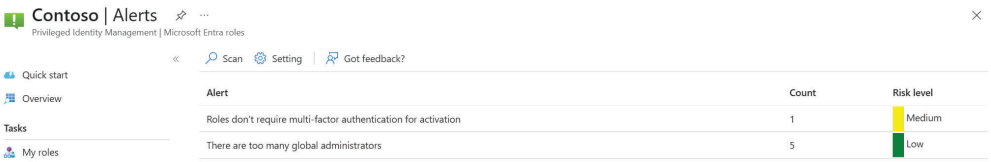


Figure 8.25: Alerts for Entra roles

4. Select the alert you want to work with, review the details and take action to resolve them. Once done, click on **Fix** to resolve the alert. Refer to the following figure. Alternatively, you can click on **Dismiss** to accept the risk.

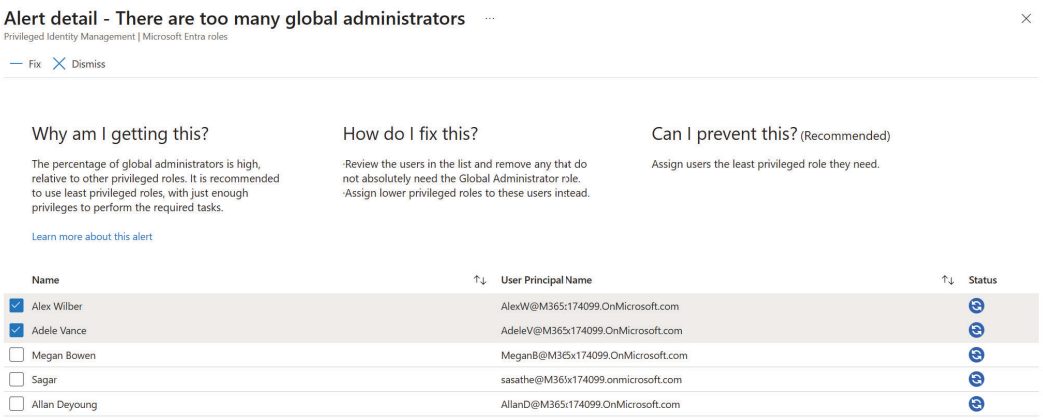


Figure 8.26: Resolve alerts

Users must have the Global Administrator, Privileged role administrator, Global Reader, Security Administrator, or Security Reader role to be able to read PIM alerts for Microsoft Entra roles.

Azure roles

The following table lists the events that will generate alerts for Azure roles:

Alert	Severity
Too many owners assigned to a resource	Medium
Too many permanent owners assigned to a resource	Medium
Duplicate role created	Medium
Roles are being assigned outside of Privileged Identity Management	High

Table 8.7: Alerts for Azure roles

Some of these alerts have settings that can be customized by the administrator. The following are the steps to customize the alert settings:

1. In the Microsoft Entra Admin center navigate to **ID Governance** | **Privileged Identity Management** | **Azure resources**.
2. Select the subscription and click **Alerts** | **Settings**.
3. Click on the alert whose settings you would like to customize, make the necessary changes and click **Save**.
4. Once an alert is generated it will show up under **ID Governance** | **Privileged Identity Management** | **Azure resources** | **Alerts**.
5. Select the alert you want to work with, review the details and take action to resolve them. Once done, click on **Fix** to resolve the alert. Refer to the following figure. Alternatively, you can click on **Dismiss** to accept the risk.

Resolving PIM alerts promptly is crucial to maintaining the security and compliance of privileged access within your Azure environment.

Auditing PIM

The **Resource audit** section of PIM shows all assignments and activations for Microsoft Entra roles, Azure resource roles, and Groups for the past 30 days. To retain audit data for longer than 30 days you can use Azure Monitor to send it to an Azure storage account. To access the Resource audit section, navigate to **ID Governance | Privileged Identity Management** and select **Microsoft Entra roles**, **Azure resources** or **Groups**. Then select **Resource audit**. The following screen shows an example of the resource audit page for Microsoft Entra roles. You can click on **Export** to download the results in a .csv format.

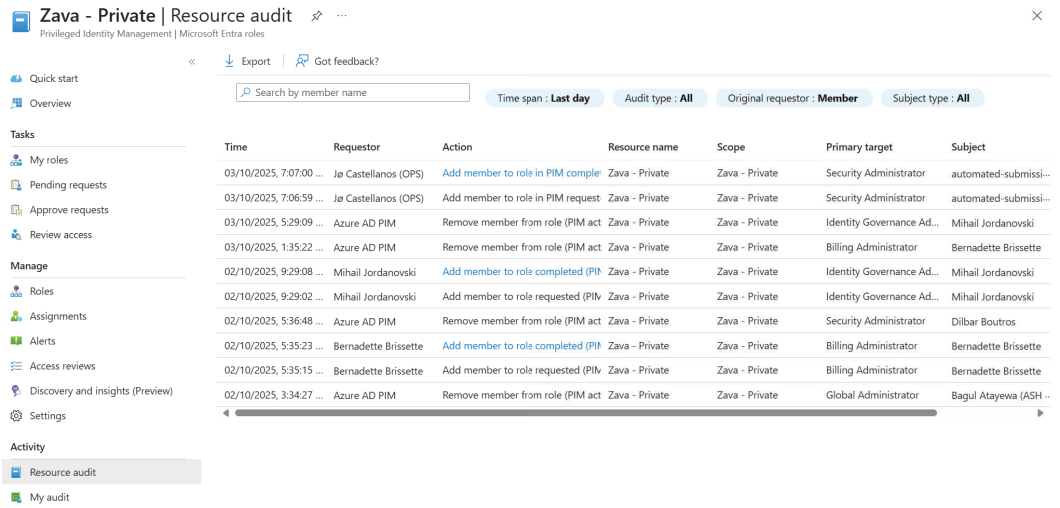


Figure 8.27: Resource audit

To view a list of all activities performed by the logged-in user account, click on **My audit** on the screen above.

Discovery and insights

Before an organization starts using PIM, all privileged role assignments are permanent. Discovery and insights is an analysis and action tool that shows you which users have privileged roles assigned in your tenant. Using this information, you can quickly convert permanent access into just-in-time access. The following steps explain how to use this feature:

1. In the Microsoft Entra Admin center navigate to **ID Governance | Privileged Identity Management | Microsoft Entra roles | Discovery and insights**. This page will give you information about the use of privileged roles in your tenant.

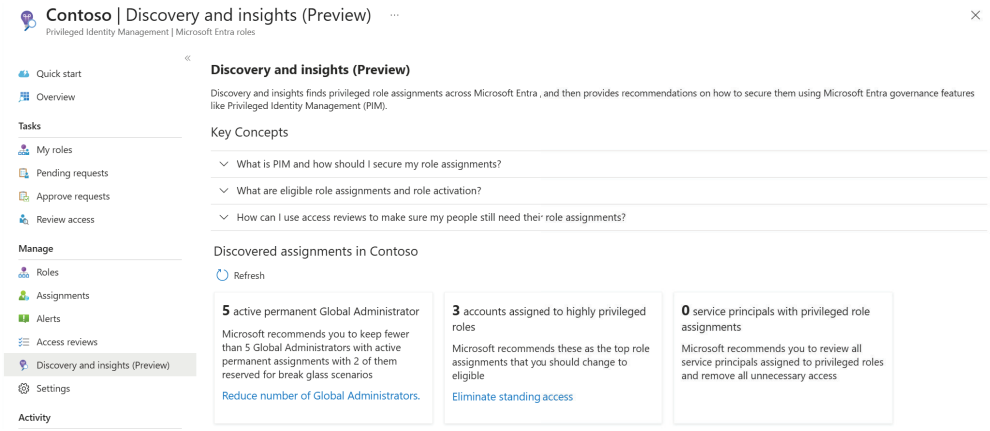


Figure 8.28: Discovery and insights

2. Select **Reduce number of Global Administrators**. The flyout pane shows you all users who have the Global Administrator role in the tenant. From this screen, you can choose to either change the permanent assignment into an eligible assignment by clicking on the **Make eligible** button or you can choose to **Remove assignment** of selected users.

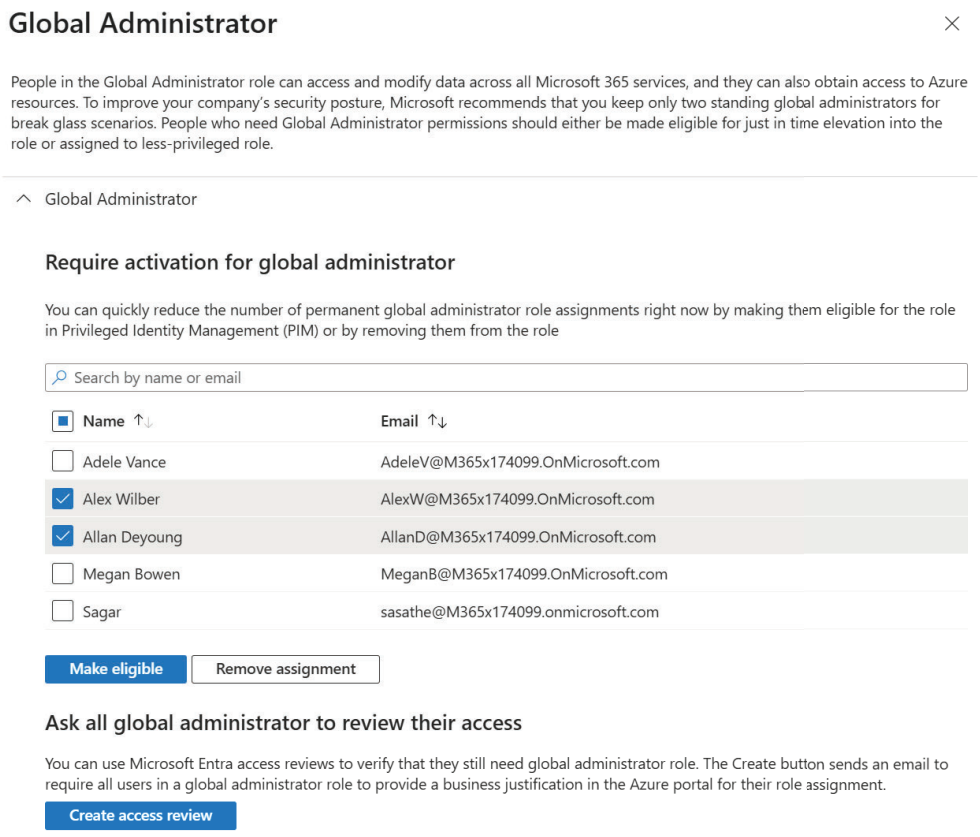


Figure 8.29: Take action for the Global Administrator role

3. You can also have all global administrators review their access by creating an access review. Click on **Create access review** and then click **OK** to automatically create an access review.

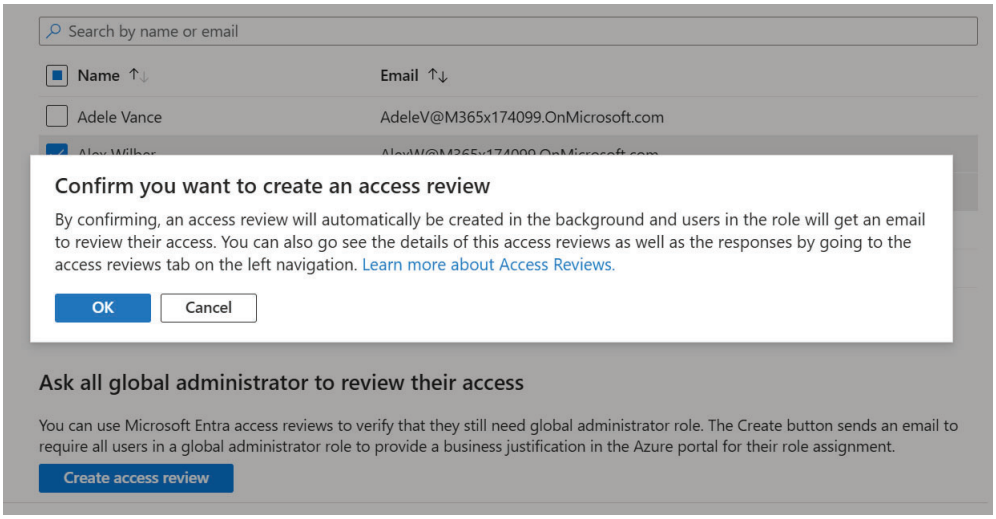


Figure 8.30: Create access review

Similarly, you can click on **Eliminate standing access** (*Figure 8.28*) and take similar actions for other privileged roles. You can also click on Review service principals to remove unnecessary access.

Discovery and insights is a useful tool that helps organizations get started with PIM.

Best practices

Here are the best practices for deploying **Privileged Identity Management (PIM)** in Microsoft Entra, written to be crisp, actionable, and aligned with strong governance principles.

Best practices for PIM

The following are some best practices that help organizations get the most value out of PIM:

- **Enforce Just-in-Time access:** Convert all standing privileged assignments into eligible roles. This reduces the attack surface and aligns with Zero-Trust by ensuring admin rights exist only when needed.
- **Require MFA for activation:** Make MFA mandatory for every privileged activation. This blocks compromised credentials from being used to elevate access.
- **Use approval workflows for high-impact roles:** Roles such as Global Administrator, Privileged Role Administrator, and User Administrator should require explicit approval before activation.

- **Set short activation durations:** Keep activation windows minimal, just long enough to complete the task. Shorter windows reduce exposure and limit misuse.
- **Require justification for every activation:** Require business justification for each elevation. This strengthens auditability and supports compliance reviews.
- **Enable alerts for suspicious or excessive activations:** Monitor unusual patterns such as repeated activations, after-hours use, or unexpected role requests.
- **Use access reviews regularly:** Schedule periodic reviews for eligible role assignments, active assignments, and PIM-enabled groups. This keeps privileged access clean and current.
- **Prefer PIM for groups for shared access:** When multiple users need the same privileged role, manage it through PIM for Groups to simplify lifecycle management and reduce admin overhead.
- **Integrate PIM with Conditional Access:** Use Conditional Access to enforce compliant devices, trusted locations, and risk-based controls. This adds layered protection to privileged activations.
- **Audit and log everything:** Ensure all PIM activities feed into Microsoft Entra audit logs. Consider sending alerts to a SIEM such as Microsoft Sentinel. Visibility is essential for governance and incident response.
- **Avoid permanent assignments except for break-glass accounts:** Keep only two emergency accounts with permanent Global Administrator rights, protected by long, complex passwords and strict monitoring.
- **Communicate and train admins:** Ensure admins understand how to activate roles and why PIM is required.

These best practices ensure that organizations adequately protect the accounts that hold the keys to the kingdom.

Summary

This chapter started with explaining the concept of privileged identities and went on to explain how Microsoft Entra PIM manages privileged identities. It explained the terminology used in PIM, how roles are assigned and the licensing requirements. This chapter taught you how you can plan PIM deployment for Microsoft Entra and Azure roles and Groups. It then explained the detailed steps in configuring and managing PIM for Microsoft Entra roles, Azure roles, and Groups. It ended with introducing alerts and auditing. It also covered how organizations starting their PIM journey can utilize the discovery and insights feature. In the next chapter, we will learn how to protect user identities using Microsoft Entra ID Protection.

Exercises

1. Which of the following CANNOT be managed using PIM?
    a. Microsoft Entra roles
    b. SharePoint sites
    c. Azure roles
    d. M365 Groups
2. Which of the following is a key benefit of using PIM?
    a. Automatically grants permanent admin access to all users
    b. Enables just-in-time access to privileged roles
    c. Disables multi-factor authentication for role assignments
    d. Allows unrestricted access to external identities
3. Which Microsoft Entra license is required to use PIM features such as just-in-time role activation and approval workflows?
    a. Microsoft Entra ID Free
    b. Microsoft Entra ID P1
    c. Microsoft Entra ID P2
    d. Microsoft 365 E3

Answers

1. b
2. b
3. c

Additional resources

- Role security planning: `https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-planning`
- Product documentation: `https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure`

- Microsoft Entra role APIs: `https://learn.microsoft.com/en-us/graph/api/resources/privilegedidentitymanagementv3-overview?view=graph-rest-1.0`
- PIM for Group APIs: `https://learn.microsoft.com/en-us/graph/api/resources/privilegedidentitymanagement-for-groups-api-overview?view=graph-rest-1.0`

Join us on Discord

For discussions around the book and to connect with your peers, join us on Discord at `packt.link/discordcloud` or scan the QR code below:



Part 3

Identity Assurance and Protection

Part 3 focuses on strengthening trust across every identity that interacts with your environment: human, device, and workload. It begins with Microsoft Entra ID Protection, which provides continuous risk detection and adaptive safeguards to defend against compromised identities. This section then explores Microsoft Entra Verified ID, enabling decentralized, verifiable credentials that enhance privacy and assurance. Finally, it examines Workload ID, the identity foundation for applications, services, and automation. Together, these chapters illustrate how Microsoft Entra builds a resilient trust fabric that protects access, validates authenticity, and secures the expanding digital ecosystem.

This part of the book includes the following chapters:

- *Chapter 9*, *Microsoft Entra ID Protection*
- *Chapter 10*, *Microsoft Entra Verified ID*
- *Chapter 11*, *Microsoft Entra Workload ID*

9

Microsoft Entra ID Protection

Identity protection is a critical component of modern cybersecurity strategies, particularly as organizations increasingly adopt cloud-based and hybrid environments. The goal of identity protection is to safeguard digital identities from unauthorized access, misuse, or compromise. This involves a combination of proactive measures, continuous monitoring, and responsive actions to detect and address potential threats.

One of the fundamental aspects of identity protection is implementing robust authentication mechanisms. **Multi-factor authentication (MFA)** is commonly used to add an additional layer of security, ensuring that even if a password is compromised, unauthorized users are less likely to gain access. Alongside MFA, policies such as conditional access help organizations control who can access resources, under what circumstances, and from which locations or devices.

Advanced identity protection solutions, like **Microsoft Entra ID Protection**, go further by leveraging machine learning and behavioral analytics to detect suspicious activities in real time. These systems can identify anomalies such as impossible travel, unusual sign-in patterns, or atypical device usage. When a risk is detected, automated responses can be triggered, such as prompting for additional verification, blocking access, or alerting security teams. By integrating with SIEM tools, identity protection systems also support broader threat detection and incident response efforts, contributing to a holistic security posture.

This chapter will cover:

- Risk conditions
- Risk-based Conditional Access
- Investigating and remediating risks

Introduction to Microsoft Entra ID Protection

Microsoft Entra ID Protection helps organizations detect, investigate, and remediate identity-based risks. It helps safeguard user identities by detecting risky sign-ins and accounts using signals collected from a vast global ecosystem. These signals come from trillions of Microsoft services and devices—such as Microsoft Accounts, Xbox, Windows, and Azure—which provide data on user behavior, device health, and sign-in patterns. Microsoft also collaborates with security researchers and law enforcement to track known threats like malicious IPs and hacker tools. Additionally, feedback from users and administrators helps refine the system's accuracy. All these inputs are processed by Microsoft's risk evaluation engine, which uses machine learning to identify suspicious activities like impossible travel, password spray attacks, or anonymous browser usage. Based on these detections, Entra ID Protection can automatically trigger security responses, such as requiring multi-factor authentication or blocking access.

The following picture explains Microsoft Entra ID Protection:

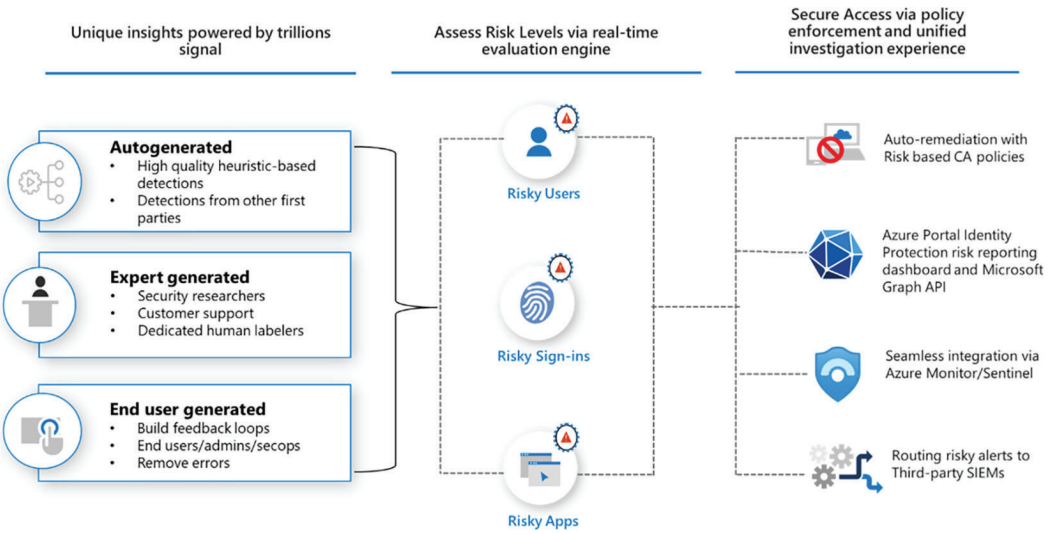


Figure 9.1: Microsoft Entra ID protection

Any identified risks are tracked and reported in reports such as Risk detections, Risky users, and Risky sign-ins which administrators can use to investigate and remediate risks.

From an attacker's point of view, the biggest obstacle today isn't stealing passwords. It is getting past MFA. Modern adversaries increasingly use **Adversary-in-the-Middle (AiTM)** phishing kits, which sit between the user and the legitimate sign-in page. These kits don't

break MFA; instead, they trick the user into completing MFA on a fake page, then quietly capture the resulting session token.

To the attacker, this token is gold. It lets them impersonate the user without needing the password or MFA again, because the session is already authenticated. This is why attackers focus on session hijacking: it bypasses the very controls designed to stop them.

But this is also exactly where Identity Protection pushes back. Anomalous Token catches tokens being used in ways that don't match how or where they were issued. AiTM detections identify when a sign-in is routed through malicious infrastructure commonly used by phishing kits.

From the attacker's perspective, this breaks the entire playbook: even if they manage to steal a token, they can't rely on it lasting. The moment risk is detected, the session collapses.

Automation is the key to protecting the organization against risks. **Risk-based Conditional Access policies** can be used to automatically remediate risky sign-ins and risky user detections. Based on the risk level, a phishing-resistant MFA method or password reset could be required. If the user can complete this, the risk is automatically remediated. If automation is not enabled, an administrator will have to manually investigate and remediate risks.

Data from ID Protection can be sent to other tools for archival or further correlation and investigation. ID Protection can seamlessly integrate with **Microsoft Sentinel**, where signals can be correlated with other Microsoft and non-Microsoft security products. Organizations that want to retain data for longer can choose to send the data to a Log Analytics workspace, an Azure storage account or Azure Event Hub.

Role requirements

The following table summarizes the various roles in ID Protection and the tasks they can and cannot perform:

Role	Can do	Cannot do
Global Reader	• Read-only access	• Write access
User Administrator	• Reset user passwords	• Read or write
Conditional Access Administrator	• Create risk-based Conditional Access policies	• Read or write to legacy ID Protection policies

Role	Can do	Cannot do
Security Reader	• View all ID Protection reports	• Configure or change policies • Reset user password • Configure alerts • Give feedback on detections
Security Operator	• View all ID Protection reports • Dismiss user risk, confirm safe sign-in, confirm compromise	• Configure or change policies • Reset user password • Configure alerts
Security Administrator	• Full access	• Reset user password

Table 9.1: Roles in ID Protection

Use this table to configure personas and roles to manage ID Protection.

License requirements

The full set of Microsoft Entra ID Protection features is available with **Microsoft Entra ID P2** licenses.

Microsoft Entra ID Protection also receives signals from Microsoft Defender for some risk detections. You may need appropriate licenses to receive those signals. The following are the signals and the Microsoft Defender product that owns the signal.

Microsoft Defender products	Signal
Microsoft Defender for Cloud Apps	• Activity from anonymous IP address • Impossible travel • Mass access to sensitive files • New country
Microsoft Defender for Office 365	• Suspicious inbox rules

Microsoft Defender products	Signal
Microsoft Defender for Endpoint	• Possible attempt to access Primary Refresh Token

Table 9.2: Microsoft Defender signals

You should have the appropriate licenses for the products that own the signal you are interested in. Alternatively, Microsoft 365 E5 Security or Microsoft 365 E5 covers all signals.

Microsoft Entra ID Protection dashboard

Microsoft Entra ID Protection offers a robust dashboard using which customers can analyze their security posture, understand how well they are protected, identify vulnerabilities and carry out recommended actions. The dashboard is available in the Microsoft Entra Admin center by navigating to **ID Protection | Dashboard**. It enables organizations to gain rich insights and get actionable recommendations tailored to their tenant. This provides a better view of their security posture so that they can take appropriate actions to protect their tenant. They have access to risk metrics, attack graphics, and a map highlighting risky locations.

The following is an example of the ID Protection dashboard:

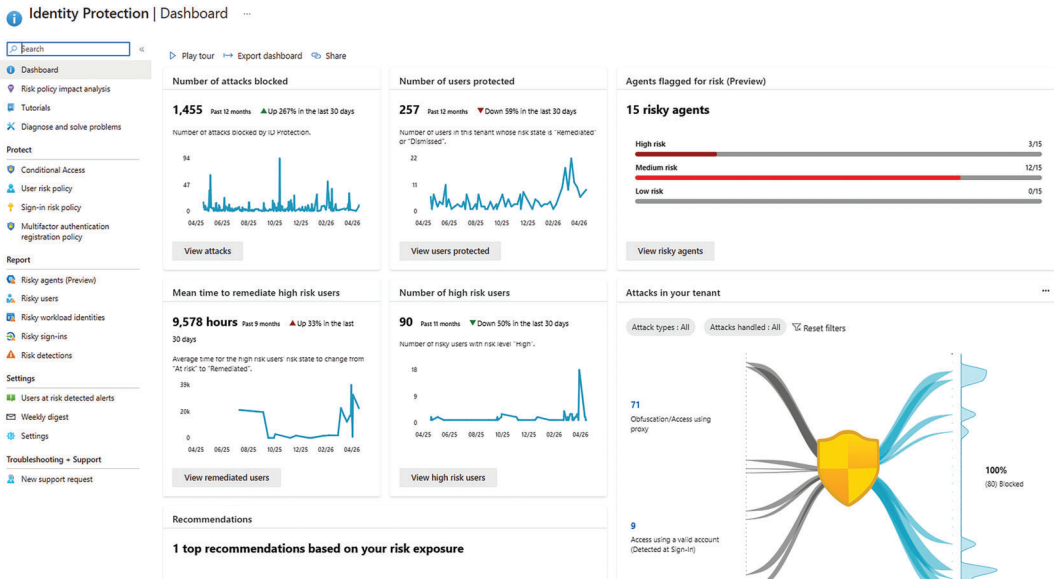


Figure 9.2: ID Protection dashboard

This dashboard is available with any Microsoft Entra ID license. However, a Microsoft Entra ID P2 license is required to view a comprehensive list of applications and select recommended

action links. For some risk detections, a Microsoft 365 E5 or Microsoft Enterprise Mobility + Security E5 license may be required. A user must be at least a **Security Reader** to be able to view the dashboard.

The dashboard provides four key metrics that help organizations understand the effectiveness of the security measures that are implemented. These are the top 4 cards in *Figure 9.2*. These are explained in the following table.

Metric	**Definition**	**Refresh frequency**	**Action**
Number of attacks blocked	This shows the number of risky sign-ins interrupted by a policy each day.	24 hours	View the risk detection in the **Risk detections** report.
Number of users protected	Number of users whose risk state changed from **At risk** to **Remediated** or **Dismissed**.	24 hours	View protected users on the **Risky users** page.
Mean time to remediate user risk	Time taken for user's risk state to change from **At risk** to **Remediated**.	24 hours	View remediated users on the **Risky users** page.
Number of new high-risk users detected	Number of new high-risk users detected every day.	24 hours	View **Risky users** page.

Table 9.3: Risk metrics

Following is a definition of the risk states.

- **At risk**: Microsoft ID Protection identified that a user is risky.
- **Remediated**: If a user self-remediates their risk by responding to a MFA challenge or completing a secure password reset, thereby protecting their account, their state is set to Remediated.
- **Dismissed**: A user's risk state is set to Dismissed, if an administrator dismisses the user risk because the user account is assessed to be safe.

Risk-based Conditional Access policies should be deployed to reduce the self-remediation time in the tenant.

In Microsoft Entra ID Protection, an attack is an event where a bad actor is attempting to sign in to a tenant. These attacks are detected by Microsoft's advanced risk detections and trigger a real-time risk detection that is mapped to a MITRE ATT&CK technique. This is depicted by the **Attacks in your tenant** graphic in *Figure 9.2*. This graphic shows attacks that impacted the tenant over the last 30 days and if they were blocked during sign-in. The left side shows the volume of each attack type during sign-in, and the right side shows the number of attacks blocked or not remediated.

- An attack is considered **Blocked** if the risky sign-in is interrupted by a Conditional Access policy and the attacker is unsuccessful.
- An attack is considered **Not remediated** if risky sign-ins were not interrupted and need human intervention to be remediated. These risky sign-ins are available in the **Risky sign-ins** report.

This graphic updates every 24 hour and shows the real-time sign risks.

> **Tip**
>
> To learn more about MITRE ATT&CK refer to `https://attack.mitre.org/`.

To view the attack details, you can either click on the count of attacks on the left side of the graphic or use the **Risk detections** page.

In addition to the above, the dashboard also provides a handy graph that displays the location of the risky sign-ins for the tenant. The size of the red circle depicts the volume of attacks from that location. Hovering over the red circle shows more details like the country name and the number of risky sign-ins detected from that place.

Microsoft Entra ID Protection also shows recommendations based on the attacks detected in the tenant over the last 30 days. This assists the administrators in taking quick actions to improve their identity security posture.

Lastly, a recent activity summary is also displayed which shows the recent risk-related activity in the tenant.

Understanding risk detections

Microsoft Entra ID Protection provides a continuous, intelligence-driven layer of defense by detecting risky user behavior, sign-ins, and credentials across your identity estate. At its core, ID Protection uses signals from Microsoft's global threat intelligence spanning billions of daily authentications, endpoint telemetry, and threat actor activity to identify anomalies that may

indicate compromise. Microsoft Entra ID Protection provides a broad range of risk detections that help identify suspicious activity in the tenant.

Risk types

Risk detections can be linked to a user or a sign-in event. Both user risk and sign-in risk contribute to the user risk score found in the **Risky user** report.

- **User risk**: A user risk is detected at the user level. These identify when a user account is at risk. For example, a bad actor may gain access to the account by compromising the user's credentials or the user's credentials are found on the dark web. User risk is cumulative and persists until remediated, making it a strong indicator for requiring secure password reset or step-up verification. A user risk is cleared once a user performs a secure password reset.
- **Sign-in risk**: Sign-in risk is the possibility that the sign-in attempt is made by someone other than the owner of the account. This highlights anomalies such as sign-ins from anonymous browsers, suspicious token replay, and more. Sign-in risk is real-time and transient, enabling conditional access policies to block or challenge risky attempts immediately. Sign-in risk feeds user risk. A pattern of risky sign-ins (or a single high-confidence one like leaked credentials) raises the user's risk level. One risky sign-in usually won't flip a user to high risk but repeated or strong-signal sign-ins will. A sign-in risk is cleared once a user successfully completes an MFA prompt.

It is important to understand that user risk reflects state and sign-in risk reflects events. Sign-in risk is transient (about this login). User risk is cumulative (about the identity). Even if today's sign-in looks clean, a user can still be flagged "high risk" because of past evidence.

Risk levels

Risk is categorized into three levels: low, medium, and high. **Risk levels** are calculated by Microsoft's machine learning algorithms and depict how confident Microsoft is that a particular user or sign-in is suspicious. Some detections can be categorized at all three levels depending on the sign-in properties, while some may always be categorized as high, medium or low. Risk levels play an important role in prioritizing, investigating, and remediating risk detections. They also play an important role in configuring risk-based Conditional Access policies. Each policy can be set to trigger at a particular risk level. The risk levels are explained below.

- **High**: Microsoft is highly confident that an account is compromised. Signals like threat intelligence and known attack patterns are used to determine the confidence level of risk detection.

- **Medium**: One or more moderate severity anomalies are detected but there is less confidence that the account is compromised.
- **Low**: Anomalies may be present in the sign-in or user account but there is less confidence that the account has been compromised.

Organizations can configure Conditional Access policies based on these risk levels. For example, most organizations block access if the risk level is high, enforce MFA if it is medium and allow access for low risk.

Detection types

Risks can be calculated in **Real-time** or **Offline**. This is designed to improve the precision of user and sign-in risk detection.

- **Real-time risk detection**: Detecting risks in real-time gives the opportunity to act early and use risk-based Conditional Access policies to help users self-remediate and prevent a bad actor from gaining access to the tenant. These risks show up in reporting within 5-10 minutes.
- **Offline risk detections**: These are calculated after authentication is complete. They can provide more insight into how a bad actor gained access to the account. Offline risks might show up in 48 hours.

The following table explains the real-time and offline risk detections for both user and sign-in risk.

Detection type	Sign-in risk	User risk
Real-time	Suspicious sign-in attempt is detected and can be remediated in real-time by enabling a Conditional Access policy to enforce MFA.	User account has been confirmed compromised and can be remediated in real-time by enabling a Conditional Access policy to force a user to perform a secure password reset.
Offline	Risk is detected after authentication. If not remediated it might escalate into user risk if more risks are detected and aggregated.	User is identified as risky after sign-in. If a Conditional Access policy is configured, user will be blocked from signing in until they perform a secure password reset.

Table 9.4: Risk detection types

Some detections can be triggered both in real-time and offline, thereby providing more confidence in detection.

Risks detected by Microsoft Entra ID Protection

Now that we have understood the basics of risk detection, detection types and levels, let us learn the specific risks that can be detected by Microsoft Entra ID Protection. The table below summarizes the risk types, license requirements and detection type.

Risk detection	Description	Detection type	Minimum License requirement
Sign-in risk			
Activity from anonymous IP address	Identifies if users were active from an anonymous proxy IP address.	Offline	Microsoft Entra ID P2 + Microsoft Defender for Cloud Apps
Additional risk detected (sign-in)	If a risk is detected that is only available for Microsoft Entra ID P2 customers, it is labeled as **Additional risk detected**.	Real-time or Offline	Microsoft Entra ID Free
Admin confirmed user compromised	Indicates that admin confirmed that a user was compromised via the portal or the **riskyUsers** API.	Offline	Microsoft Entra ID Free
Anomalous token (sign-in)	Detects abnormal characteristics in a refresh or session token.	Real-time or Offline	Microsoft Entra ID P2
Anonymous IP address	Detects sign-ins from anonymous IP addresses like Tor browser	Real-time	Microsoft Entra ID Free
Atypical travel	Detects sign in from a location that a user does not usually sign-in from.	Offline	Microsoft Entra ID P2

Risk detection	**Description**	**Detection type**	**Minimum License requirement**
Impossible travel	Identifies user activity from geographically distant locations within a short period of time.	Offline	Microsoft Entra ID P2 + Microsoft Defender for Cloud Apps
Malicious IP address	Detects activity from an IP address detected as malicious.	Offline	Microsoft Entra ID P2
Mass Access to Sensitive Files	Triggered when user accesses a large number of files containing sensitive information from SharePoint Online or OneDrive for Business.	Offline	Microsoft Entra ID P2 + Microsoft Defender for Cloud Apps
Microsoft Entra threat intelligence	Detects unusual user activity or activity consistent with known attack patterns.	Real-time or Offline	Microsoft Entra ID Free
Password spray	Detects password spray attacks on a user account.	Real-time or Offline	Microsoft Entra ID P2
New country	Detects activity from a location never used by the user earlier.	Offline	Microsoft Entra ID P2 + Microsoft Defender for Cloud Apps
Suspicious browser	Detects anomalous behavior based on suspicious activity across multiple tenants from different regions from the same browser.	Offline	Microsoft Entra ID P2

Risk detection	Description	Detection type	Minimum License requirement
Suspicious inbox forwarding	Detects suspicious inbox forwarding rules.	Offline	Microsoft Entra ID P2 + Microsoft Defender for Cloud Apps
Suspicious inbox manipulation rules	Detects when suspicious rules that move or delete messages are created in a user's mailbox.	Offline	Microsoft Entra ID P2 + Microsoft Defender for Cloud Apps
Token issuer anomaly	Detects if the SAML token issuer is compromised.	Offline	Microsoft Entra ID P2
Unfamiliar sign-in properties	Considers past sign-in history to look for anomalous sign-ins.	Real-time	Microsoft Entra ID P2
Verified threat actor IP	Indicates sign-in activity consistent with known IP addresses associated with nation state actors or cyber crime groups.	Real-time	Microsoft Entra ID P2
User risk			
Additional risk detected (user)	If a risk is detected that is only available for Microsoft Entra ID P2 customers, it is labeled as **Additional risk detected**.	Real-time or Offline	Microsoft Entra ID Free
Anomalous token (user)	Detects abnormal characteristics in a refresh or session token.	Real-time or Offline	Microsoft Entra ID P2
Anomalous user activity	Detects suspicious administrative activity in the tenant.	Offline	Microsoft Entra ID P2

Risk detection	**Description**	**Detection type**	**Minimum License requirement**
Attacker in the middle	Triggered when an authentication session is linked to a malicious reverse proxy.	Offline	Microsoft Entra ID P2 + Microsoft Defender for Cloud Apps
Leaked credentials	Detects when a user's credentials are found on the dark web.	Offline	Microsoft Entra ID Free
Microsoft Entra threat intelligence (user)	Identifies unusual user activity or activity that is consistent with known attack patterns.	Offline	Microsoft Entra ID Free
Possible attempt to access Primary Refresh Token (PRT)	Detected by Microsoft Defender for Endpoint, this detects when attackers try to access resources by moving laterally in a network.	Offline	Microsoft Entra ID P2 + Microsoft Defender for Cloud Apps
Suspicious API traffic	Identifies abnormal GraphAPI traffic or directory enumeration.	Offline	Microsoft Entra ID P2
User reported suspicious activity	Reported when a user denies a MFA prompt and reports it as suspicious.	Offline	Microsoft Entra ID P2
Suspicious sending patterns	Detected by Microsoft Defender for Office 365, it detects when someone sends suspicious email and is at risk of being restricted from sending email.	Offline	Microsoft Entra ID P2 + Microsoft Defender for Cloud Apps

Table 9.5: Risk types and detection

Now that you understand the risk detections in detail, let's learn how we can use risk-based access policies to mitigate these risks.

Risk-based access policies

Conditional Access policies can be applied to protect organizations when a sign-in or user risk is detected. This is called **risk-based Conditional Access (RBCA)**. The following graphic explains how risk-based Conditional Access policies work to protect an organization's critical resources.

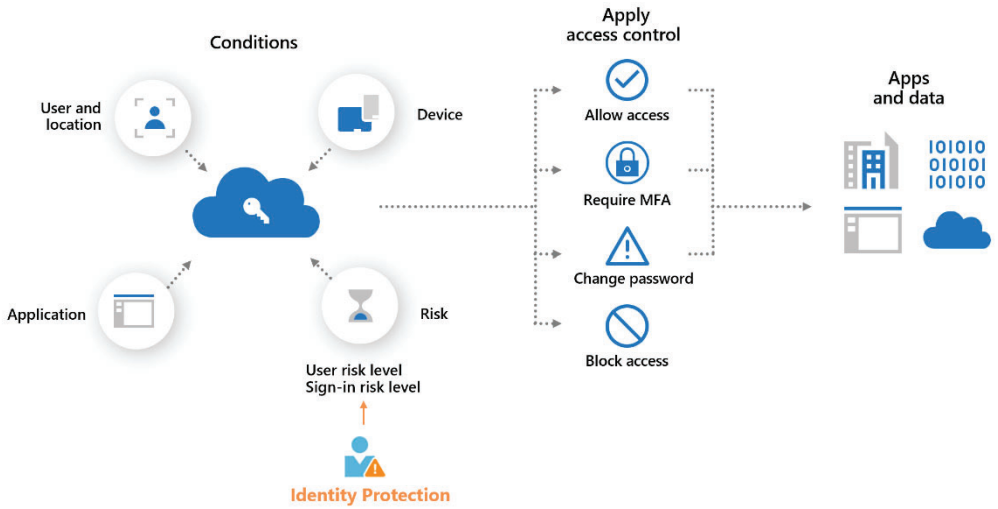


Figure 9.3: Risk-based Conditional Access

In Microsoft Entra Conditional Access, there are two conditions for user-specific risk conditions that are powered by Microsoft Entra ID Protection. These are **Sign-in risk** and **User risk**. When administrators create these Conditional Access policies, they can configure these conditions to take specific actions based on the identified risk level. During each sign-in, Microsoft Entra ID Protection sends the detected risk level to Conditional Access. The policies apply if the conditions are satisfied. For example, you might want a user to be prompted for MFA only when the sign-in risk is medium or high. The main benefit of using RBCA is automatic risk remediation. When a user successfully completes the required access control, such as responding to MFA, their risk is remediated. No further action is needed from the administrator. This reduces the burden of investigating and remediating the risk from the administrator.

Prerequisites

Before configuring risk-based Conditional Access policies, ensure that the following prerequisites are met.

- Ensure that the users are registered for MFA. Use the MFA registration policy explained later in this section.
- Ensure that users are registered for **self-service password reset** (**SSPR**). This has been explained in *Chapter 3, Implementing Microsoft Entra ID*.
- Configure emergency access accounts. This has been explained in *Chapter 8, Microsoft Entra Privileged Identity Management*.
- Configure named locations in Conditional Access. This should include your corporate and VPN IP ranges. IP-based locations can be marked as trusted. Sign-ins from trusted named locations lower sign-in risk and improve the accuracy of ID Protection risk calculations.

Once all the prerequisites have been met, you can proceed with creating the sign-in risk and user risk policies.

Sign-in risk policy

Microsoft Entra ID Protection analyzes hundreds of signals in real-time to calculate a sign-in risk level for each sign-in. This risk level is sent to Conditional Access where administrators can configure policies to enforce the following controls based on the risk level:

- Block access
- Allow access requiring MFA

The picture below shows where you can configure the user risk and sign-in risk while configuring a Conditional Access policy.

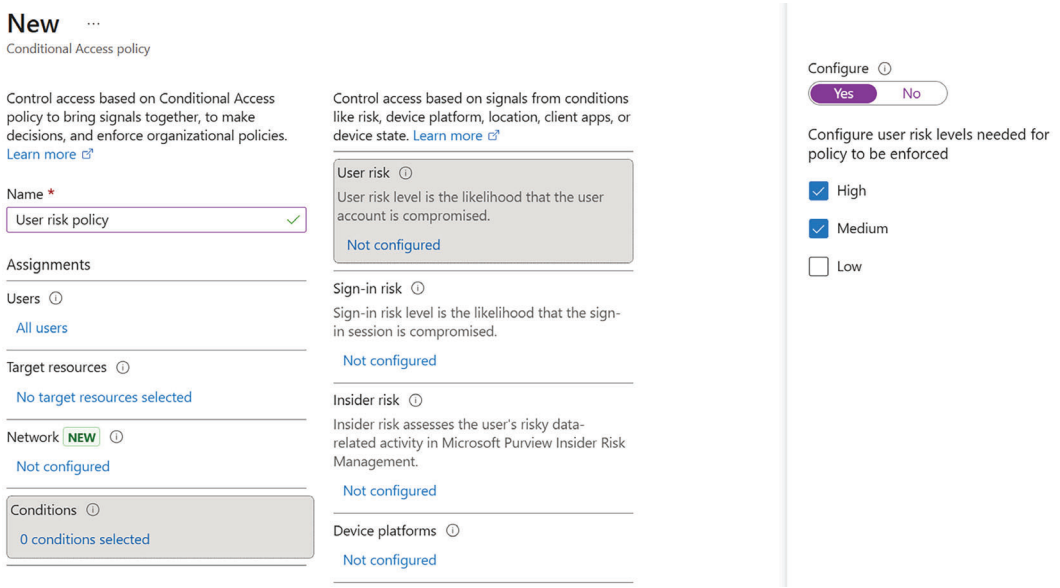


Figure 9.4: Configuring risk-based Conditional Access policy

Note

If risks are detected, during sign-in, the user can take the action as enforced by the policy to self-remediate. Users must be registered for Microsoft Entra MFA to enforce a sign-in risk policy.

Organizations must choose the appropriate risk level to configure, balancing user experience and security. Choosing to apply access policies to **High** risk level reduces the number of times a policy is enforced. While this minimizes friction for users, it might not block all attacks. Selecting **Low** risk level will increase the number of times users are interrupted. Microsoft recommends requiring MFA for **Medium** and **High** sign-in risk levels. A successful MFA is the only way to remediate a sign-in risk, regardless of the risk level.

User risk policy

Microsoft Entra ID Protection analyzes signals about user risk to calculate a risk level. Behaviors like risky sign-ins and credential leaks are used to calculate the user risk level. These signals are then fed into Conditional Access where administrators can configure policies to enforce the following controls based on the risk level:

- Block access

- For users with passwords, allow access but force a secure password change
- For passwordless users, identity protection can revoke sessions and require secure reauthentication, ensuring effective containment of token theft and AiTM attacks

If risk is detected, users can perform a secure password reset to remediate the risky event and close the event thereby, reducing noise for the administrator.

> **Note**
>
> Users must be registered for **self-service password reset (SSPR)** to be able to change their passwords when forced by a risk-based Conditional Access policy.

Organizations must choose the appropriate risk level to configure, balancing user experience and security. Choosing to apply access policies to **High** risk level reduces the number of times a policy is enforced. While this minimizes friction for users, it might not block all attacks. Selecting **Low** risk level will increase the number of times users are blocked from signing in.

> **Note**
>
> User risk and sign-in risk conditions are now available in Conditional Access. Organizations that have configured these policies under ID Protection must migrate them to Conditional Access policies before October 1, 2026.

The following table provides a quick decision matrix on detected risk type, risk level, and suggested action:

Risk type	Risk level	Remediation
Sign-in risk	Medium or High	Require MFA
User risk	High	Secure password reset

Table 9.6: RBCA decision matrix

As a best practice avoid combining the user risk and sign-in risk in one policy as these conditions rarely occur together. It is recommended to create separate policies – one for user risk and one for sign-in risk.

MFA registration policy

Microsoft Entra ID Protection helps organizations roll out MFA by requiring them to register for MFA at sign-in. Organizations can enable **Multifactor authentication registration policy**

which will prompt users to register for MFA at first sign-in. Since MFA is an important part in self-remediating user and sign-in risks, organizations must use this to ensure users are registered for MFA. Following are the steps to configure MFA registration policy:

1. Login to `https://entra.microsoft.com` as a **Security Administrator**.
2. Navigate to **ID Protection | Dashboard | Multifactor authentication registration policy**.
3. In the right pane, select whether you want to enable this policy for all users or specific users and groups.

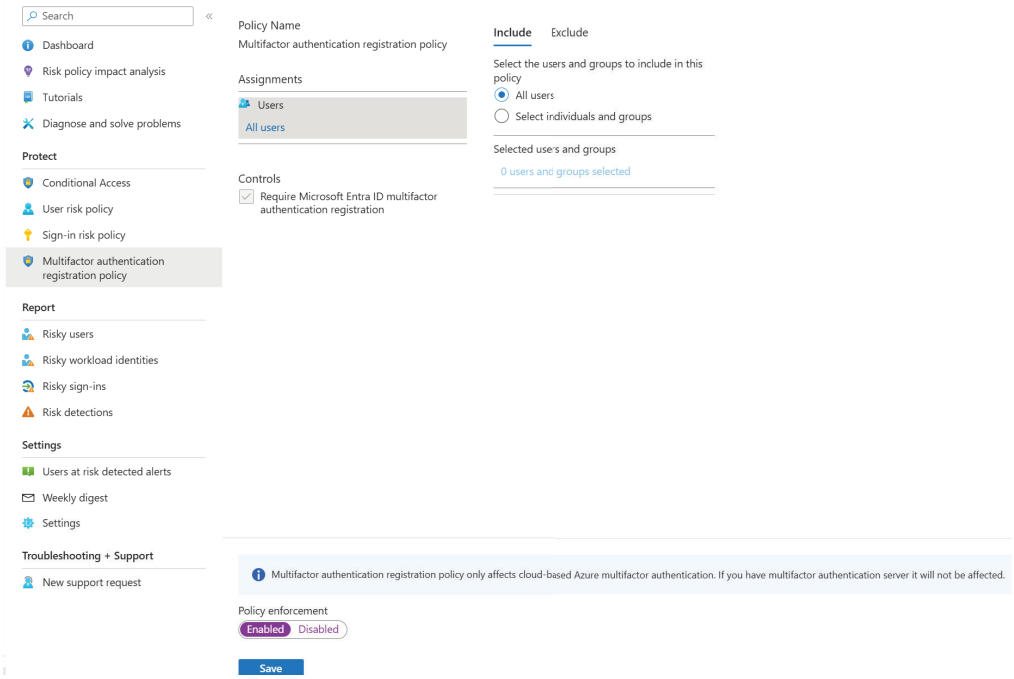


Figure 9.5: MFA registration policy

4. Switch the **Policy enforcement** toggle to **Enabled** and click **Save**.

The next time a user signs in, Microsoft Entra ID Protection will now prompt them to register for MFA. If MFA is not a required condition for sign-in, they will be able to bypass the prompt for 14 days, after which they must complete the registration to continue.

Test risk policies

Once the risk policies are created, it is important to ensure that they are working.

To test a **user risk** policy, start with the policy in either **Off** or **Report-only** mode. Elevate the risk level of a user by simulating one or more risk detections. Wait for some time to confirm if the risk level is elevated. If not, simulate additional risk detections until the risk level is elevated. Now turn the user risk policy **On** and sign in as the user with elevated risk level.

To test a **sign-in** risk policy, ensure that the policy is **On**. Now try to sign in using the Tor browser.

The policies should be triggered, and you should either be prompted to carry out the self-remediation steps as defined in the policy or access should be blocked as per policy settings.

Impact analysis workbook

The deployment of risk-based Conditional Access policies requires careful planning, time, and change management. It is also critical to ensure that implementing these policies does not cause disruptions to users and their ability to connect to resources to do their jobs. Administrators must also be able to confidently convince the leadership that these policies will not cause unwanted disruptions. One way to analyze the potential impact of these policies is to create them in **report-only mode** and then wait for a few weeks or months to have the results. This can delay the actual rollout of the policies, thereby exposing the organization to longer risk periods and preventing you from enjoying the advantages. A quicker way of understanding the potential impact is to use the **Impact analysis of risk-based access policies workbook**.

This workbook helps you understand your environment before enabling the policies that could potentially block users from signing in, enforce MFA, or require a password reset. It provides the following information for a time range of your choosing.

- Impact summary of recommended risk-based policies including user risk, sign-in risk and trusted network scenarios.
- Impact details for user risk scenarios like high-risk user not blocked or prompted for password change, users who performed a password change and remediated risk etc.
- Impact details for sign-in risk scenarios like high-risk sign-ins not blocked or prompted for MFA or high-risk sign-ins that completed MFA and self-remediated.
- Network details like top IP addresses are not listed as trusted network locations.

This information can be used to identify which users will be impacted if risk-based Conditional Access policies are implemented.

Using this workbook does not require creating risk-based Conditional Access policies beforehand. However, you must have sign-in logs sent to a Log Analytics workspace in Azure.

For more information on how to do this, refer to `https://learn.microsoft.com/en-us/entra/identity/monitoring-health/howto-use-workbooks`.

To access this workbook in the Microsoft Entra admin center, navigate to **ID Protection | Dashboard | Risk policy impact workbook**. You can use **Kusto Query Language (KQL)** to edit the queries that populate the workbook.

The first section of the workbook shows a summary of users or sign-ins impacted during the selected date range. Refer to *Figure 9.6*. The most important sections on this page are the **User risk scenarios** and **Sign-in risk & trusted network scenarios**.

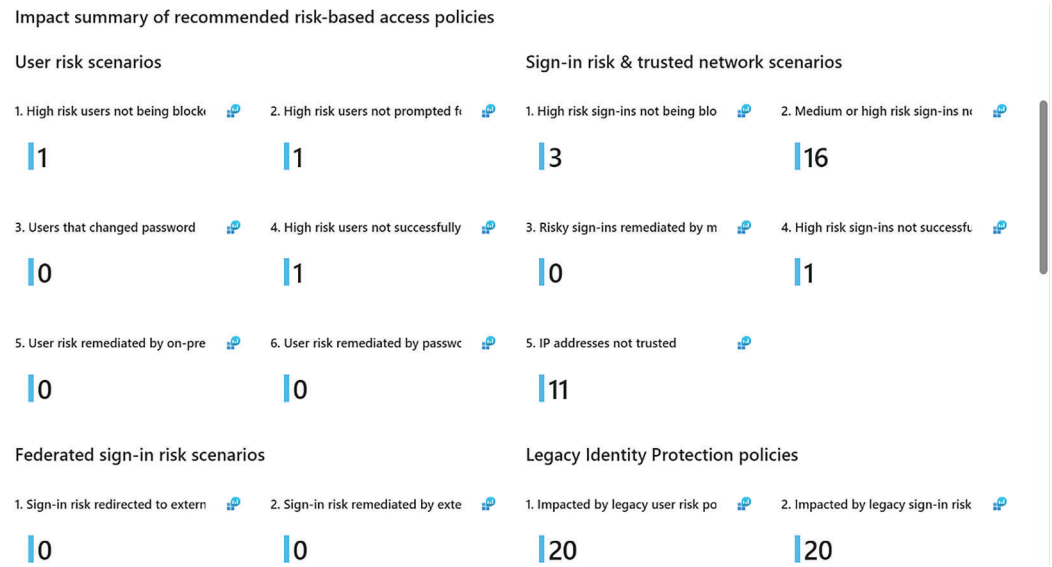


Figure 9.6: Impact analysis workbook summary

Click on **User risk scenarios** to see high-risk users and sign-ins not blocked. This indicates that high-risk users are still in the environment. Refer to *Figure 9.7*. Scrolling down, you can see the details of who those users are. If you already have risk-based policies in your environment, focus on scenarios 3 and 4. These show users who changed their passwords or were blocked because of the existing risk-based policies. If there are still users in scenarios 1 and 2, it might indicate that there is a gap in your policies. Scenarios 5 and 6 show that remediation is happening and users are changing passwords on-premises or using **self-service password reset (SSPR)**.

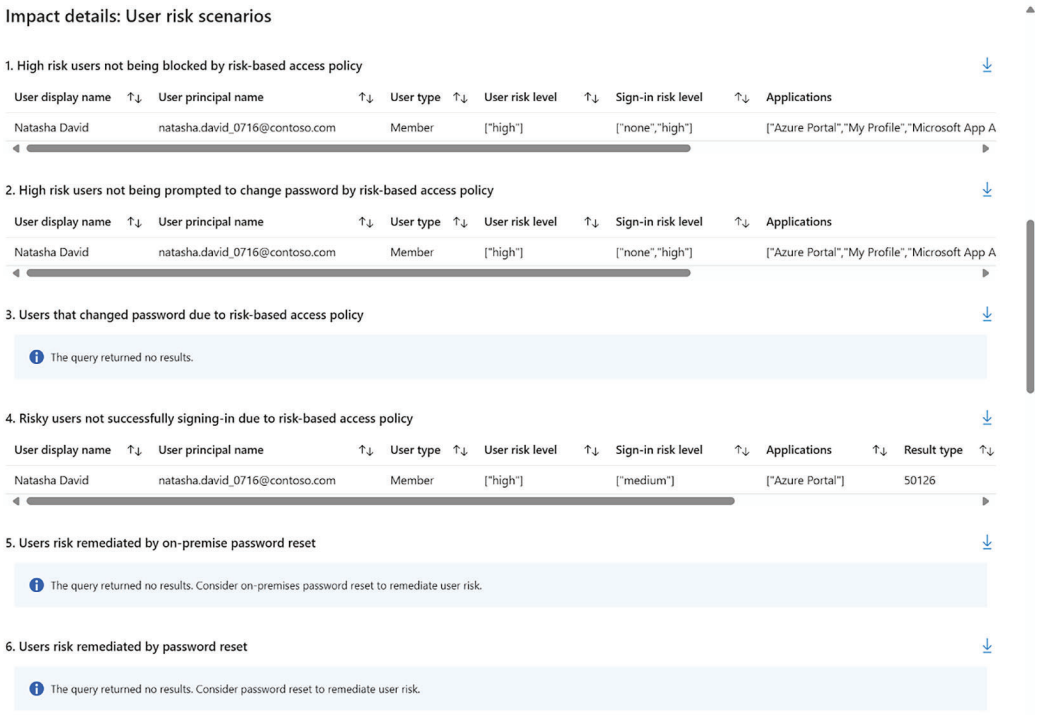
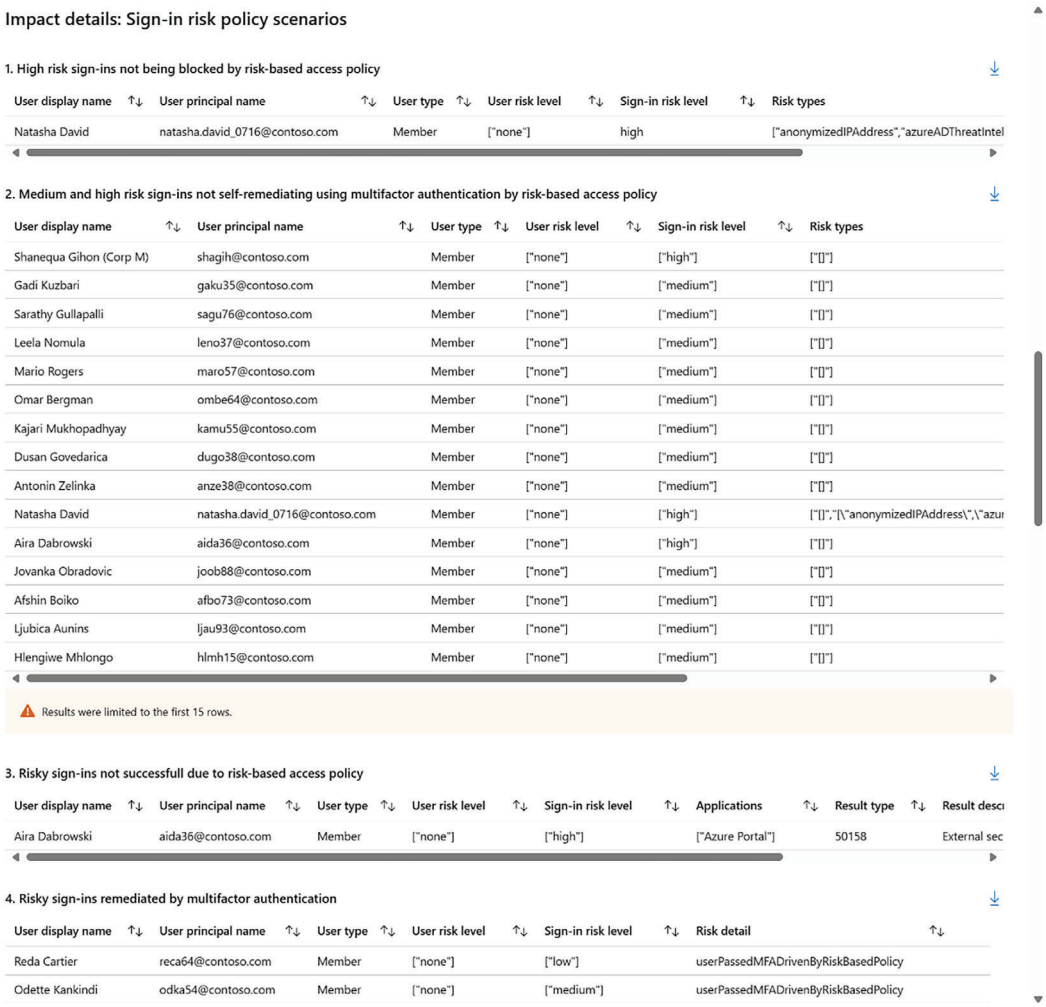


Figure 9.7: User risk scenarios

In *Figure 9.6*, click on **Sign-in risk & trusted network scenarios** to explore further as shown in *Figure 9.8*. If you have Conditional Access policies that enforce MFA, you should see some activity in scenario 4 even if they are not risk-based policies. Completing MFA automatically remediates sign-in risk. If you have risk-based policies that block access, scenario 3 will show users who were blocked from signing in. But if you see activity in scenarios 1 and 2, there might be gaps in your policies.



Impact details: Sign-in risk policy scenarios

1. High risk sign-ins not being blocked by risk-based access policy

User display name	User principal name	User type	User risk level	Sign-in risk level	Risk types
Natasha David	natasha.david_0716@contoso.com	Member	["none"]	high	["anonymizedIPAddress","azureADThreatIntel

2. Medium and high risk sign-ins not self-remediating using multifactor authentication by risk-based access policy

User display name	User principal name	User type	User risk level	Sign-in risk level	Risk types
Shanequa Gihon (Corp M)	shagih@contoso.com	Member	["none"]	["high"]	["[]"]
Gadi Kuzbari	gaku35@contoso.com	Member	["none"]	["medium"]	["[]"]
Sarathy Gullapalli	sagu76@contoso.com	Member	["none"]	["medium"]	["[]"]
Leela Nomula	leno37@contoso.com	Member	["none"]	["medium"]	["[]"]
Mario Rogers	maro57@contoso.com	Member	["none"]	["medium"]	["[]"]
Omar Bergman	ombe64@contoso.com	Member	["none"]	["medium"]	["[]"]
Kajari Mukhopadhyay	kamu55@contoso.com	Member	["none"]	["medium"]	["[]"]
Dusan Govedarica	dugo38@contoso.com	Member	["none"]	["medium"]	["[]"]
Antonin Zelinka	anze38@contoso.com	Member	["none"]	["medium"]	["[]"]
Natasha David	natasha.david_0716@contoso.com	Member	["none"]	["high"]	["[]","[\"anonymizedIPAddress\",\"azur
Aira Dabrowski	aida36@contoso.com	Member	["none"]	["high"]	["[]"]
Jovanka Obradovic	joob88@contoso.com	Member	["none"]	["medium"]	["[]"]
Afshin Boiko	afbo73@contoso.com	Member	["none"]	["medium"]	["[]"]
Ljubica Aunins	ljau93@contoso.com	Member	["none"]	["medium"]	["[]"]
Hlengiwe Mhlongo	hlmh15@contoso.com	Member	["none"]	["medium"]	["[]"]

Results were limited to the first 15 rows.

3. Risky sign-ins not successfull due to risk-based access policy

User display name	User principal name	User type	User risk level	Sign-in risk level	Applications	Result type	Result desc
Aira Dabrowski	aida36@contoso.com	Member	["none"]	["high"]	["Azure Portal"]	50158	External sec

4. Risky sign-ins remediated by multifactor authentication

User display name	User principal name	User type	User risk level	Sign-in risk level	Risk detail
Reda Cartier	reca64@contoso.com	Member	["none"]	["low"]	userPassedMFADrivenByRiskBasedPolicy
Odette Kankindi	odka54@contoso.com	Member	["none"]	["medium"]	userPassedMFADrivenByRiskBasedPolicy

Figure 9.8: Sign-in risk scenarios

The section, **Federated sign-in risk scenarios** (*Figure 9.6*), is useful for customers using multiple identity providers. Here they can check if any risky sessions are being redirected to those external providers for MFA or any other form of remediation.

The section, **Legacy Identity Protection policies** (*Figure 9.6*), helps track how many users have moved from the legacy identity protection policies to Conditional Access policies.

Continuous Access Evaluation

Continuous Access Evaluation (CAE) keeps access decisions alive instead of fixed at sign-in. It lets apps check back with Entra ID whenever something meaningful changes like risk, location, or device posture so sessions stay aligned with real-time conditions. CAE turns identity from a one-time check into an ongoing, adaptive trust signal. For example, a user signs in to Outlook from their corporate network. Later, they walk next door and connect their laptop to the café's public Wi-Fi. Without CAE, their Outlook session would continue because Conditional Access was only evaluated at sign-in. With CAE, Entra detects the shift to an untrusted network and signals Outlook to re-check the session immediately. Outlook forces re-authentication, Conditional Access is re-evaluated, and access is either blocked or MFA-challenged in near real-time without waiting for token expiry.

For CAE to work the client must be CAE-capable, the workload must support CAE and Microsoft Entra ID must send real-time signals. SharePoint Online, Exchange Online, Teams, and Microsoft Graph already support CAE and enforce real-time Conditional Access decisions. Organizations can enable their applications for CAE by using CAE-aware authentication libraries (like MSAL) and implement logic to handle CAE-specific error responses from the resource API, prompting the app to re-authenticate when Entra ID signals that conditions have changed.

CAE is auto enabled in all Microsoft Entra tenants. Organizations wishing to disable it can do so using the session control in Conditional Access policies. Disabling CAE only works when applied to all applications. It can, however, be applied to all users or selected users and groups.

Scenarios

CAE enables two key scenarios as described below:

Critical event evaluation

CAE is achieved by allowing services such as Exchange Online, SharePoint Online, and Teams to subscribe to essential Microsoft Entra events. This approach facilitates the prompt evaluation of these events and ensures that controls are enforced in near real time. Critical events evaluated are:

- User account deleted or disabled
- User password changed
- MFA enabled for user
- Administrator revokes user refresh tokens
- High risk users detected by Microsoft Entra ID Protection

When CAE is enabled, if any of the above critical events are detected, users can lose access to Exchange Online, SharePoint Online, and Teams almost instantaneously.

Conditional Access policy evaluation

Exchange Online, SharePoint Online, Teams and MS Graph can synchronize key Conditional Access policies for evaluation within their own service so that they don't have to call back to Entra ID every time to know whether a session is still allowed. They can locally evaluate key Conditional Access policies because Entra has already synchronized the relevant policy signals into the workload. This then lets them detect changes in conditions like location and risk and enforce CAE immediately.

Client capabilities

Without CAE, clients like Outlook, Teams and OneDrive can replay a user's access token from their cache as long as it is not expired. With CAE, a token can be rejected even if it is not expired. A mechanism called **claim challenge** is used to inform a client to bypass its cache. The latest versions of Outlook, Teams and OneDrive support claim challenge.

With CAE, access tokens no longer rely on short, fixed lifetimes. CAE-capable clients use real-time policy and risk evaluation, so tokens can safely last up to 28 hours. Security comes from instant revocation when conditions change and not from expiring tokens. Clients that aren't CAE-aware continue using the traditional 1-hour token lifetime or any custom lifetime configured using **Configurable Token Lifetime** settings.

Securing workload identities

In addition to user and sign-in risk, Microsoft Entra ID Protection also helps in securing workload identities helping detect, investigate, and remediate risks related to applications and service principals. A **workload identity** is an identity assigned to an application and allows it to access resources. Unlike a user account, a workload identity cannot perform MFA and often does not have a lifecycle. But they do need a secure location to store their credentials or secrets. Due to this, they are more vulnerable to attacks. To make use of the workload identity risk report, the following pre-requisites must be met.

- Administrator should have the **Security Administrator**, **Security Operator**, or **Security Reader** role assigned
- To use risk as a condition while creating Conditional Access policies, the **Conditional Access Administrator** role must be assigned
- To take action on risky workload identities using risk based Conditional Access policies, you must have a **Workload Identities Premium** license

Microsoft Entra ID Protection detects risks related to workload identities across sign-in behavior and offline indicators of compromise. The detections are summarized in the following table.

Detection name	**Detection type**	**Description**
Microsoft Entra Threat Intelligence	Offline	Detects activity that is consistent with known attack patterns based on Microsoft's Threat Intelligence sources.
Suspicious sign-ins	Offline	Indicates sign-in patterns which are unusual for the service principal. These patterns are learned over 60 days and the alert is generated if one of the following unfamiliar properties are detected in subsequent sign-ins • IP Address • Target resource • User agent • Hosting/non-hosting IP change • IP country • Credential type
Admin confirmed service principal compromised	Offline	Indicates that an administrator has selected **Confirmed compromised** in the **Risky workload identities** report.
Leaked credentials	Offline	Indicated if the accounts credentials are leaked. This can happen if someone checks in code in GitHub with the credentials or if the credentials are stolen and published on the dark web.

Detection name	Detection type	Description
Malicious application	Offline	This combines signal from Microsoft Defender for Cloud Apps and Microsoft Entra ID Protection to identify applications that have been disabled for violating Microsoft's terms of use. It is recommended to perform a thorough investigation before enabling the application.
Suspicious application	Offline	This indicates that Microsoft Entra ID Protection or Microsoft Defender for Cloud Apps have identified anomalous behavior in an application but have not disabled it.
Anomalous service principal activity	Offline	Identified activity in the service principal that is different from the learnt baseline.
Suspicious API traffic	Offline	Reported with unusual GraphAPI traffic or directory enumeration of a service principal is observed, indicating reconnaissance or data exfiltration attempts.

Table 9.7: Risk detections for workload identities

Microsoft Entra ID Protection assigns one of the three risk levels to each identified risk: low, medium and high. Risk-based Conditional Access policies can be applied to block access for accounts that have been marked "At risk" by Microsoft Entra ID Protection. The risky workload identities can be viewed in the Microsoft Entra admin center under the **Risky workload identities** report.

Configure notifications

Microsoft Entra ID Protection sends automated notifications that help manage user risk and risk detections. A Microsoft Entra ID P2 license is required to use this feature.

Users at risk detected email

When a risky user is detected, Microsoft Entra ID generates an email alert. This email has a link to the **Users flagged for risk** report. It is recommended to immediately investigate these users. Users that have the Global Administrator, Security Administrator and Security Reader roles are

automatically added to the list of users who receive these emails. These users must have a valid email or alternate email configured in Microsoft Entra ID. If a user is enrolled in PIM and these roles are only elevated by PIM activation, the user will receive the email only if their role was elevated when the email was sent.

You can configure the specific user risk level for which you want to receive these alerts. Emails are triggered when a user risk level reaches the configured level. For example, if you configure to be notified each time a user risk reaches **Medium**, an email will be triggered when a user's risk level changes from **Low** to **Medium**. If later the same user's risk level changes from **Medium** to **High**, another email will be triggered. You will only receive one email within a 5-second period. If multiple users move to the specified risk level during the same period, an aggregated email including all users is sent.

To configure these settings, in the Entra admin center, navigate to **ID Protection | Dashboard | User at risk detected alerts** as a **Security Administrator**. Refer to the following picture for the available options.

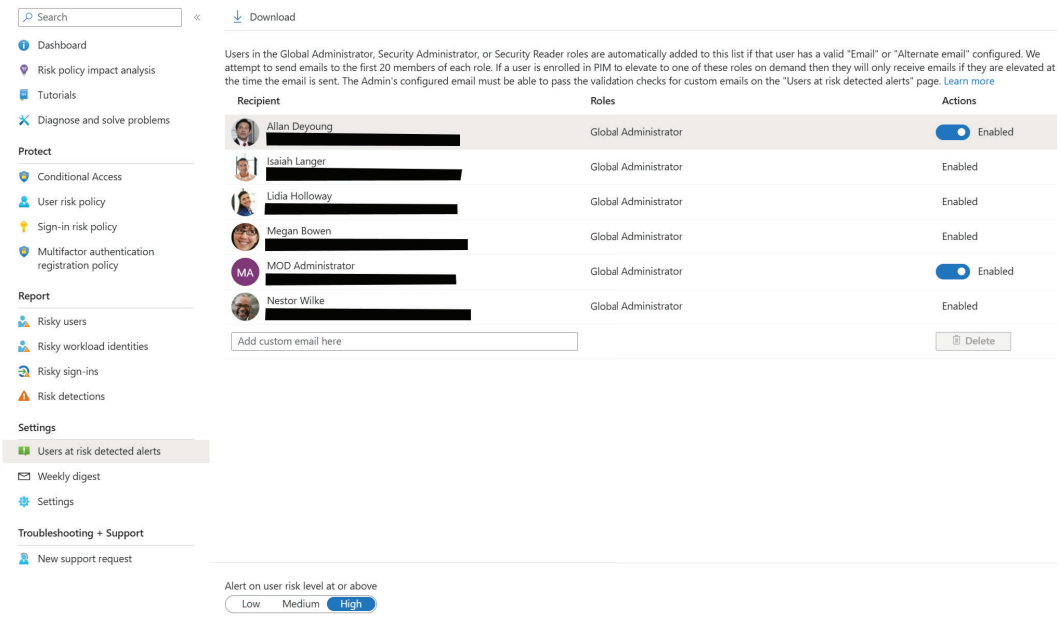


Figure 9.9: User at risk detected alerts

As an administrator you can configure the people who receive these emails and the risk level at which the email is triggered.

Weekly digest email

Microsoft Entra ID Protection sends a weekly email that includes newly detected risky users, newly detected risk sign-ins, and links to reports in ID Protection. Users that have the Global Administrator, Security Administrator, and Security Reader role are automatically added to the list of users who receive these emails. These users must have a valid email or alternate email configured in Microsoft Entra ID. The Weekly digest emails are sent by default. As an administrator you can choose to turn them off in the Entra admin center. You can also disable specific administrators from receiving these emails. Navigate to **ID Protection | Dashboard | Weekly digest** as a **Security Administrator**. Refer to the following picture for the available options.

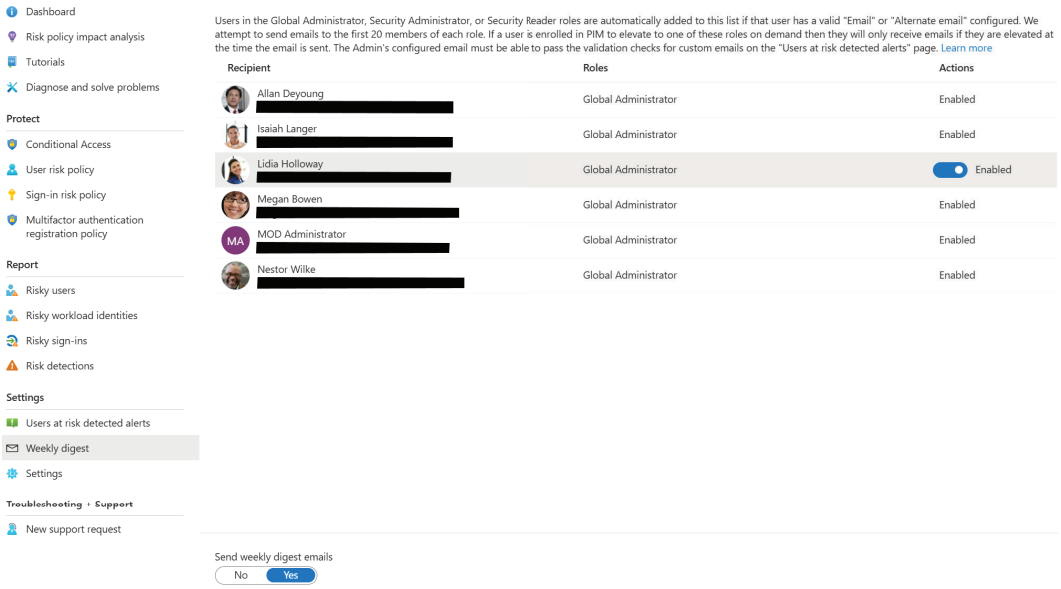


Figure 9.10: Weekly digest mail settings

Weekly digest emails in Microsoft Entra ID Protection provide security teams with a concise summary of identity risks and trends, enabling timely investigation and proactive threat mitigation across user and workload identities.

Investigate and remediate risks

Using Microsoft Entra ID Protection, administrators can access reporting that can be used to investigate user risk, sign-in risk, risky workload identities, and risk detections. A Microsoft Entra ID P2 license is required. Users must have at least the **Security Reader** role to be able to access the risk reports.

Risky users

The risky users report lists all user accounts that are considered at risk of compromise. Administrators can investigate risky users and take appropriate action to remediate the user account to prevent unauthorized access to resources. A user account can be listed in the risky users report if they have performed one or more risky sign-ins or risks are detected in the user account.

To investigate a risky user, access the **Risky users** report by navigating to **ID Protection | Dashboard** in the Microsoft Entra admin center. The screenshot below shows the **Risky users** report.

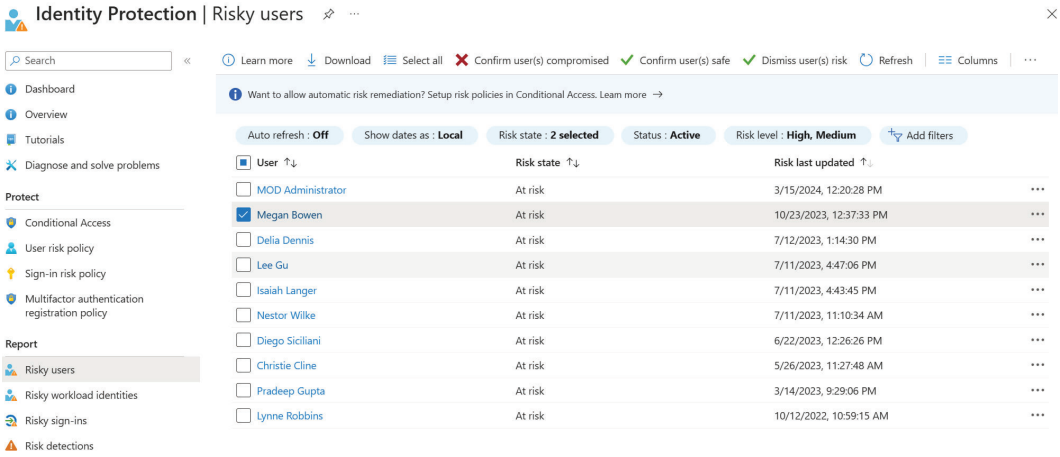


Figure 9.11: Risky users report

Click on any user account to view the details of the risk detection. See example below. Also note the various administrative actions available. If any of the action buttons are grayed out, you need higher permissions.

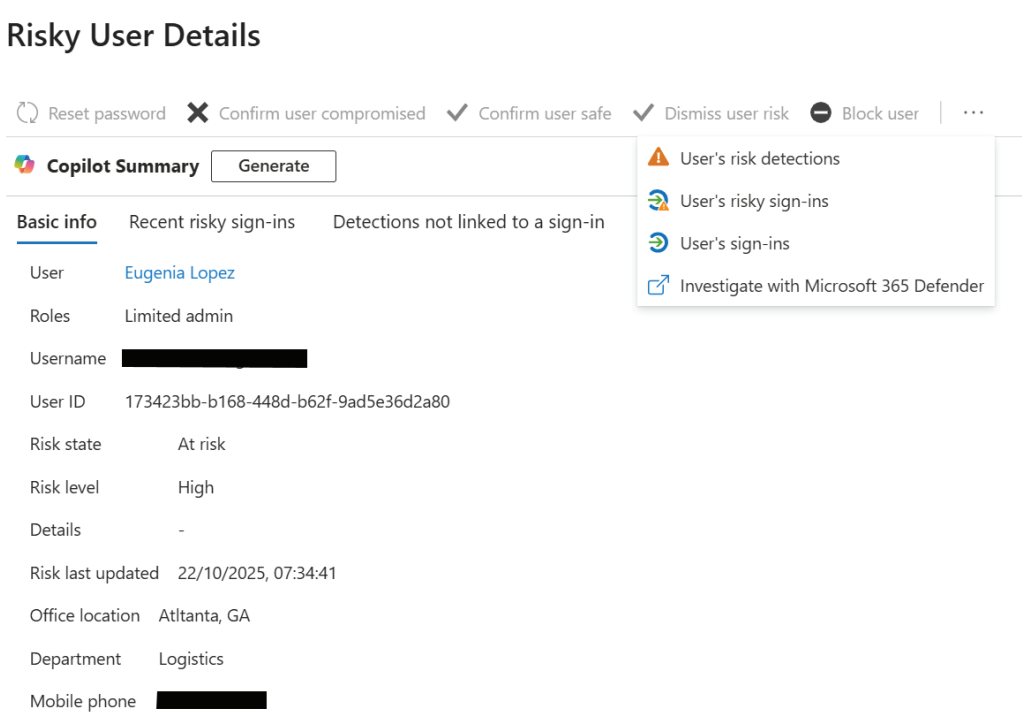


Figure 9.12: Risky user details

The available administrative actions are explained as follows:

- **Reset password**: This action revokes the user's current session.
- **Confirm user compromised**: The user risk level is set to **High** and **Admin confirmed user compromised** detection is added. The user is considered risky till remediation is performed.
- **Confirmed user safe**: Take this action if this is a false positive. This removes risks and detections from this account. ID Protection places the user account in learning mode to relearn usage properties.
- **Dismiss user risk**: Take this action when the user risk is real but not malicious. Actions taken by penetration testers may fall in this category. Similar users will continue being detected for risk going forward.
- **Block user**: This blocks the user from signing in.
- **Investigate with Microsoft 365 Defender**: This action takes the administrator to the Microsoft Defender portal for further investigation.

The **Risk history** tab shows all the events in the last 90 days that caused the user risk level to change. It includes user actions that increased the risk. It can also include admin or user remediation actions that may have lowered the user risk.

Risky sign-ins

The Risky sign-ins report shows the risky sign-in events for up to the last one month. With this report, administrators can find which sign-ins are classified as at risk, if they are confirmed compromise, confirmed safe, remediated or dismissed. This report shows both interactive and non-interactive sign-ins. Administrators can also find the device information, MFA details, if any Conditional Access policies were applied and much more. They can then decide to either confirm the sign-in as compromised or safe. The following screenshot shows the Risky sign-ins report. Click on any sign-in to view more details and take action. The following actions can be carried out:

- **Confirm sign-in compromised**: This confirms that the sign-in was risky and remediation steps need to be taken.
- **Confirm sign-in safe**: This is a false positive and future similar sign-ins should not be considered risky.
- **Dismiss sign-in risk**: The sign-in risk detected was real but not malicious. Similar sign-ins will be continued to be evaluated for risk.

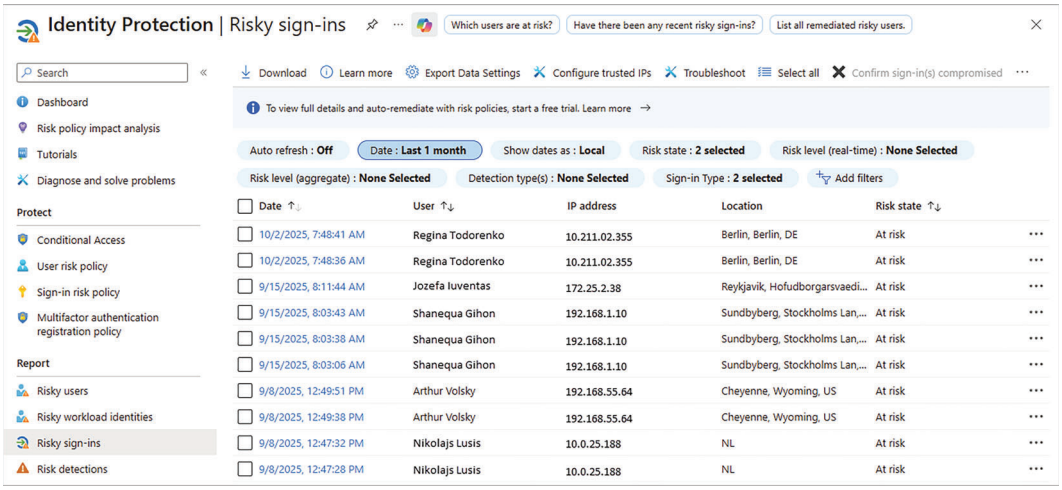


Figure 9.13: Risky sign-ins report

The Risky sign-ins report in Microsoft Entra ID Protection identifies and details suspicious login attempts—such as those from unfamiliar locations, malicious IPs, or unusual devices—enabling security teams to investigate and respond to potential identity threats.

Risky workload identities

A workload identity is an identity used by an application to access a resource. To find risky workload identities, navigate to the **Risky workload identities** section of the reports. For each risky workload identity listed, ID Protection includes the Service Principal ID, Risk state, Risk level and risk history. Refer to the following screenshot and note the various options available to administrators to remediate the identified risk.

Following are some guidelines for remediating risky workload identities:

1. Identify the credentials assigned to risky workload identities.
2. Add new credentials. It is recommended to use x.509 certificates.
3. Remove all the compromised credentials.
4. If the Service Principal has access to secrets stored in Azure Key Vault remediate them by rotating them.

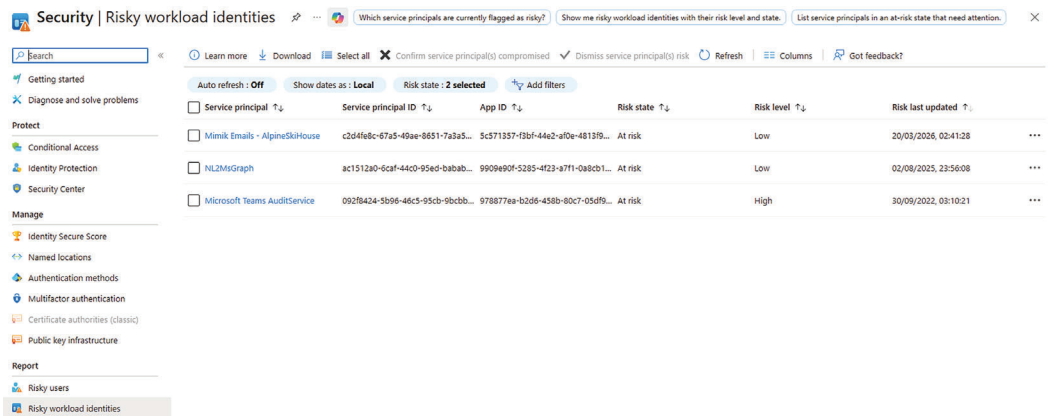


Figure 9.14: Risky workload identities report

The Risky Workload Identities report in Microsoft Entra ID Protection identifies applications and service principals exhibiting suspicious behavior—such as anomalous sign-ins or compromised credentials—enabling security teams to investigate and remediate threats to non-human identities.

Risk detections

The risk detections report shows detected risks from the last 90 days. With this report administrators can find details about various risk detections, the sign-ins it pertains to and the current status of that risk. Click on any risk detection to view the **Risk detection details** page, which gives more information about the detection type, risk state, risk level, attack type, and

source of the risk detection, like ID Protection or Microsoft Defender for Endpoint. The following screenshot shows the **Risk detections** report.

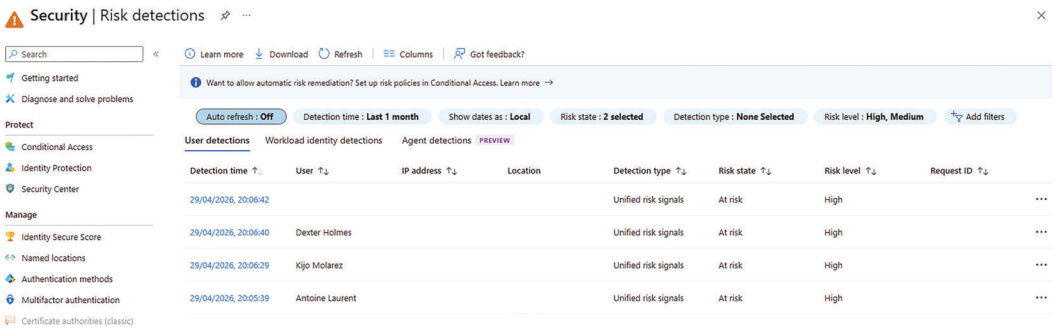


Figure 9.15: Risk detections report

With this report, administrators can find information about each risk detection, the attack type based on the MITRE ATT&CK framework, other risks triggered at that time, and the sign-in attempt location. This gives administrators additional information that they can use to take actions in the **Risky users** and **Risky sign-ins** reports.

Simulate risk detections

Microsoft Entra ID Protection enables administrators to simulate risk detections to test risk-based Conditional Access policies. This section explains the risk detections that can be simulated in a secure manner.

Anonymous IP address

To simulate sign in from an anonymous IP address you will have to use the Tor browser. If your organization restricts the use of Tor browser, consider using a virtual machine. From the Tor browser sign in to `https://myapps.microsoft.com` using a newly created user account that is not yet registered for MFA. The sign-in will show up in the report within 10-15 minutes.

Unfamiliar sign-in properties

To simulate unfamiliar sign-in properties, you will need a location and device that the test account has not used earlier. You can consider using a VPN on a virtual machine to simulate this. The test account should have 30 days of sign-in history and a usable MFA method registered. This ensures that Microsoft Entra ID Protection has learned its usual behavior and will be able to flag unfamiliar properties. To simulate, use the VPN on the virtual machine and navigate to `https://myapps.microsoft.com`. Fail the MFA challenge. The sign-in will show up in the report within 10-15 minutes.

Atypical travel

This detection is not easy to simulate because Microsoft Entra ID Protection uses a machine learning algorithm that identifies false positives like the use of VPN which is typically used to simulate atypical travel from a familiar device. The algorithm also requires 14 days of sign-in history or 10 sign-ins before it can start identifying atypical travel. Due to these complexities, it is possible that you may not be able to simulate this detection. Follow the steps below to simulate:

1. Use your regular browser and sign in to `https://myaccess.microsoft.com`.
2. Change your user agent in Microsoft Edge using Developer Tools (F12). This mimics using a different machine.
3. Change your IP address using a Tor browser, a VPN or an Azure virtual machine in another region.
4. Sign in to `https://myapps.microsoft.com` using the previous credentials.

The sign-in should show up in the report within 2-4 hours.

Leaked credentials for workload identities

As discussed earlier, leaked credentials for workload identities can happen if someone checks in code with credentials in GitHub. To simulate this detection, you must have a GitHub account. From the **App registrations** page in Microsoft Entra admin center, collect the application's client secret, **Application (client) ID**, and **Directory (tenant) ID**. Ensure that the application is disabled in the **Enterprise apps** page. Create a `.txt` file as below:

```
"AadClientId": "<Application (client) ID>",
"AadSecret": "<client secret>",
"AadTenantDomain": "XXXX.onmicrosoft.com",
"AadTenantId": "<Directory (tenant) ID",
```

Create a public GitHub repository and add the above file as a .txt extension and commit changes. In about 8 hours, the leaked credentials detection should be available in the **Risk detections** report.

Export risk data

Microsoft Entra stores reports for a limited period. For customers using the free version of Microsoft Entra ID, sign-in logs, audit logs and risky sign-ins are stored for 7 days. With Microsoft Entra ID P1 and P2, this information is stored for 30 days. MFA usage logs are stored for 30 days regardless of the license. Organizations wanting to retain this data for longer have

the option to export it to an Azure Log Analytics workspace, stream it to Azure Event hub, or archive it in an Azure storage account. Data can also be exported to a partner solution.

Once you have the relevant destination set up, configure diagnostic settings in Microsoft Entra ID to export the data using the following steps:

1. Sign in to `https://entra.microsoft.com` as **Security Administrator**.
2. Navigate to **Entra ID | Monitoring & health | Diagnostic settings**.
3. Click **+ Add diagnostic setting**, enter a diagnostic setting name and select the relevant log categories.
4. Click **Save**.

The following are of most interest to identity administrators:

- **RiskyUsers**: Exports the Risky users data.
- **UserRiskEvents**: Exports the Risk detections data.
- **RiskyServicePrincipals**: Exports the Risky workload identities data.
- **ServicePrincipalsRiskEvents**: Exports the Workload identity detection data.

It can take up to 15 minutes for the exported logs to start appearing in the destination.

Provide feedback to Microsoft

Organizations can provide feedback on the risk assessment provided by Microsoft Entra ID Protection. This feedback helps Microsoft optimize detections and improve accuracy. If you find that a Microsoft Entra ID Protection risk detection is incorrect or you have validated that the risk detection was accurate, you can provide feedback to help Microsoft improve the accuracy of its detection. There may be scenarios where you use a non-Microsoft product to remediate the user risk. In such cases the user risk is not adjusted automatically. You can provide feedback to Microsoft to adjust the user risk.

Microsoft uses this feedback to update the risk of the underlying user and sign-in, helping to secure end users. This feedback is processed offline and may take some time to be effective.

Summary

In this chapter, we learned how we can use Microsoft Entra ID Protection to identify risky users and risky sign-ins. We learned about the various risk detections and how they are calculated. We also learned how to use risk-based Conditional Access policies to help users self-remediate the risk. We saw how we can simulate risk detection and use the impact analysis workbook to analyze the impact of the risk-based policies. Lastly, we learned how to export risk data for long term storage and analysis and how to provide feedback to Microsoft. You should now be

able to implement and manage Microsoft Entra ID Protection in your organization. In the next chapter we will learn how to manage digital identities using Microsoft Entra Verified ID.

Exercises

1. What are the two main categories of risk detections in Microsoft Entra ID Protection? Choose two.
    a. Sign-in Risk
    b. Atypical travel
    c. Anomalous token
    d. User risk
2. How does Microsoft Entra ID detect risk? Choose two.
    a. Low
    b. Real-time
    c. Offline
    d. Medium
3. What is the best way to auto-remediate user and sign-in risk in Microsoft Entra ID Protection?
    a. Force all users to reset their passwords
    b. Block all users from signing in
    c. Use risk-based Conditional Access policies
    d. Implement the MFA registration policy

Answers

1. a, d
2. b, c
3. c

Additional resources

- Microsoft Entra ID Protection product documentation:`https://learn.microsoft.com/en-us/entra/id-protection/`

- Frequently asked questions: `https://learn.microsoft.com/en-us/entra/id-protection/id-protection-faq`
- Configurable token lifetimes in Microsoft Entra: `https://learn.microsoft.com/en-us/entra/identity-platform/configurable-token-lifetimes`

Get this book's PDF version and more

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.





Note: Keep your invoice handy. Purchases made directly from Packt don't require an invoice.

10

Microsoft Entra Verified ID

In today's world, we use identities at work, at home, and across various devices and applications. These identities represent us as individuals and are made up of everything we do or experience, such as online shopping, booking a cab, or ordering dinner. Our identities and digital interactions depend on many applications to which we grant access to our data. Often, we are not aware which applications have access to which pieces of our personal information. In the enterprise world, collaboration with customers and partners requires orchestration to exchange information. This introduces the risk of identity theft and data breaches. Decentralized identities are digital identities that are owned and controlled by individuals, giving them greater control over which application has access to which of their personal data. Using decentralized technologies, users can create, manage, and share their identity securely with full privacy and autonomy. This approach reduces reliance on traditional identity systems that store sensitive information in centralized databases, which can be vulnerable to data breaches or misuse. We need decentralized identities to empower people with more control over their personal information, enhance privacy, reduce identity theft, and make it easier to verify identity across different organizations and platforms without sharing excess data.

In this chapter, we will cover:

- Introduction to decentralized identities
- Introduction to verifiable credentials
- Microsoft Entra Verified ID
- Verified ID Face Check
- Account recovery
- Opt out of Verified ID

Introduction to decentralized identities

Decentralized identities represent a significant shift from traditional, centralized identity management systems. In conventional models, identity data such as usernames, passwords, and personal information is stored and managed by a central authority—typically an organization or service provider. This centralization makes sensitive data a prime target for cyberattacks and puts users at risk of identity theft, loss of privacy, and unauthorized access. In contrast, **decentralized identities (DIDs)** empower individuals to own, control, and manage their digital identity without relying on a single provider or intermediary.

At the core of decentralized identity is the concept of **self-sovereign identity (SSI)**, where individuals have full ownership and autonomy over their personal data. Rather than having identity information scattered across multiple organizations, users create and manage a digital identity that is stored in a secure digital wallet—often on their own device. This wallet can contain various verifiable credentials, such as government-issued IDs, educational certificates, or employment records, which are cryptographically signed by trusted issuers. When a user needs to prove their identity, they can selectively share only the necessary credentials, thereby minimizing data exposure and enhancing privacy.

Decentralized identities leverage distributed ledger technologies, such as blockchains, to provide a secure and tamper-evident infrastructure for managing identity data. Blockchains are used to anchor **decentralized identifiers**, which are unique, persistent identifiers created and controlled by the user. Unlike traditional identifiers, decentralized identifiers are not dependent on any central registry, authority, or intermediary. This design allows for greater interoperability between systems and organizations, making it easier for users to interact across different platforms without repeatedly creating new identities or sharing sensitive information unnecessarily.

One of the key benefits of decentralized identities is enhanced privacy. With traditional identity systems, users often have little visibility into which organizations have access to their personal information or how that data is being used. DIDs give users granular control over their data, allowing them to grant or revoke access as needed. For example, instead of providing a full copy of a driver's license to verify age, a user could share only a cryptographic proof that they are over a certain age, without revealing their exact birthdate or other personal details.

Security is another major advantage. Since identity data is not stored in a single, centralized location, the risk of large-scale data breaches is significantly reduced. In decentralized systems, even if one credential issuer is compromised, the user's other credentials remain secure, as each is independently managed and cryptographically protected. Furthermore, decentralized

identities can help prevent identity fraud by enabling real-time verification of credentials and reducing the reliance on easily stolen or forged information.

Decentralized identities also promote inclusivity and accessibility. Individuals who lack traditional identity documents or live in regions with limited infrastructure can create digital identities that are recognized globally. This enables access to services such as banking, healthcare, and education, regardless of geographic location or socioeconomic status. The portability of decentralized identities means users can carry their credentials across borders and platforms, fostering seamless digital interactions in an increasingly connected world.

Decentralized identities offer a transformative approach to digital identity management. By shifting control from centralized authorities to individuals, DIDs enhance privacy, security, and user autonomy. They reduce the risks associated with data breaches and identity theft, streamline the verification process, and open up opportunities for people who are underserved by traditional systems. As technology and standards continue to evolve, decentralized identities are poised to become a cornerstone of secure, user-centric digital ecosystems.

A digital identity represents who a person is in a digital space. Verifiable credentials help prove specific claims about that person when needed.

Introduction to verifiable credentials

Verifiable credentials are a foundational concept in the emerging landscape of decentralized identity systems. They provide a secure, privacy-preserving, and interoperable way to prove attributes, qualifications, or claims about an individual, organization, or device in the digital world. Unlike traditional credentials, such as plastic ID cards or paper certificates, verifiable credentials are digitally signed and can be presented, validated, and revoked with cryptographic assurance. This approach not only streamlines the process of sharing and verifying information but also gives individuals greater control over their personal data, reducing the risk of identity theft, fraud, and data misuse.

At their core, verifiable credentials are digital statements made by a trusted issuer about a person. These statements, or claims, can represent a wide range of information—from government-issued identification and academic qualifications to professional licenses and memberships. Each credential is composed of three main components: the *issuer* (who creates and signs the credential), the *subject* (the person to whom the credential pertains), and the *verifier* (who checks the authenticity of the credential). The credentials themselves are typically encoded in a standard data model, such as the **World Wide Web Consortium (W3C) Verifiable Credentials** standard, ensuring interoperability across different platforms and organizations.

The lifecycle of a verifiable credential begins when an issuer, such as a university or government agency, generates a digital credential for a subject. This credential is cryptographically signed to guarantee its authenticity and integrity. The subject then stores the credential in a secure digital wallet, often managed on their own device. When the subject needs to prove a claim—such as their age, educational attainment, or professional status—they can present the relevant credential to a verifier, such as an employer or service provider. The verifier checks the digital signature and, if necessary, queries the issuer or a decentralized ledger to confirm the credential's validity and revocation status.

One of the most significant benefits of verifiable credentials is enhanced privacy. Subjects can choose to share only the minimum amount of information required for a specific transaction, rather than disclosing their entire identity or sensitive personal details. For example, to prove eligibility for a senior discount, a user could present a credential that confirms they are over a certain age without revealing their exact birthdate or other identifying information. This concept, known as *selective disclosure*, is enabled by advanced cryptographic techniques such as *zero-knowledge proofs*.

Verifiable credentials also foster trust in digital ecosystems by ensuring that credentials can be independently verified without relying on a single central authority. Because credentials are digitally signed by trusted issuers and anchored to decentralized identifiers, verifiers can validate their authenticity in real time. This reduces opportunities for forgery or tampering and simplifies compliance with regulatory requirements for identity verification, such as Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations. Additionally, revocation mechanisms allow issuers to invalidate credentials if they are found to be compromised or no longer valid, further enhancing security and trust.

The applications of verifiable credentials are broad and rapidly expanding. In education, digital diplomas, and transcripts can be issued as verifiable credentials, allowing graduates to share their achievements instantly with employers or other institutions. In healthcare, verifiable credentials can represent professional medical licenses or proof of vaccination status, streamlining access to services and improving patient privacy. In finance, banks and fintech companies can use verifiable credentials to onboard customers more efficiently while maintaining regulatory compliance. Even everyday scenarios, such as age verification for online purchases or access control for events, can benefit from verifiable, privacy-preserving credentials.

Interoperability is a key consideration in the adoption of verifiable credentials. W3C has established open standards for verifiable credentials and decentralized identifiers, enabling seamless interaction between different identity systems and service providers. Organizations like the **Decentralized Identity Foundation (DIF)** and the **W3C Credentials Community**

Group are driving the development and adoption of these standards, ensuring that verifiable credentials can be used globally across a variety of platforms and industries.

Despite their promise, verifiable credentials face several challenges. Achieving widespread adoption requires collaboration among issuers, wallet providers, verifiers, and regulators to establish trusted ecosystems and governance frameworks. Ensuring usability and accessibility for all users, including those with limited technical skills or resources, is essential for inclusion. There are also ongoing discussions about privacy, data protection, and interoperability, as well as the need for robust mechanisms to handle credential revocation and recovery in case of device loss or compromise.

Verifiable credentials represent a transformative step forward in digital identity management. They empower individuals to control their personal information, reduce reliance on centralized authorities, and create new possibilities for secure, privacy-preserving interactions online. As standards mature and adoption grows, verifiable credentials are poised to become a cornerstone of decentralized, user-centric digital ecosystems, supporting a wide range of services and enabling trusted digital interactions around the world.

Now that we understand the core concepts, let's look at how digital identity and verifiable credentials are implemented in Microsoft Entra.

Understanding Microsoft Entra Verified ID

Microsoft Entra Verified ID is a cutting-edge solution designed to enable secure, privacy-respecting digital identity verification for individuals and organizations. Built on open standards such as W3C Verifiable Credentials and Decentralized Identifiers (DIDs), Entra Verified ID empowers users to obtain, manage, and present digital credentials in a trustworthy and interoperable manner. With Entra Verified ID, organizations can issue digital credentials—such as proof of employment, educational qualifications, or professional certifications—that users store securely in their own digital wallets. When users need to verify their identity or claims, they can selectively disclose only the necessary information to verifiers, maintaining control over their personal data and enhancing privacy.

Microsoft Entra Verified ID integrates seamlessly with existing identity systems and platforms, making it easier for businesses to adopt decentralized identity solutions without overhauling their infrastructure. The platform supports robust security measures, including cryptographic signatures, and real-time revocation, to ensure that credentials are authentic and up to date. By removing the need for centralized authorities and enabling user-centric identity management, Entra Verified ID reduces the risk of fraud, streamlines onboarding, and verification processes, and fosters trust in digital interactions. As digital ecosystems continue to evolve, Microsoft Entra Verified ID stands at the forefront of enabling secure, user-controlled, and scalable identity solutions for the modern world.

As can be understood, a new form of identity requires new innovations. Decentralized identities are made up of five key innovations as shown in the following figure:

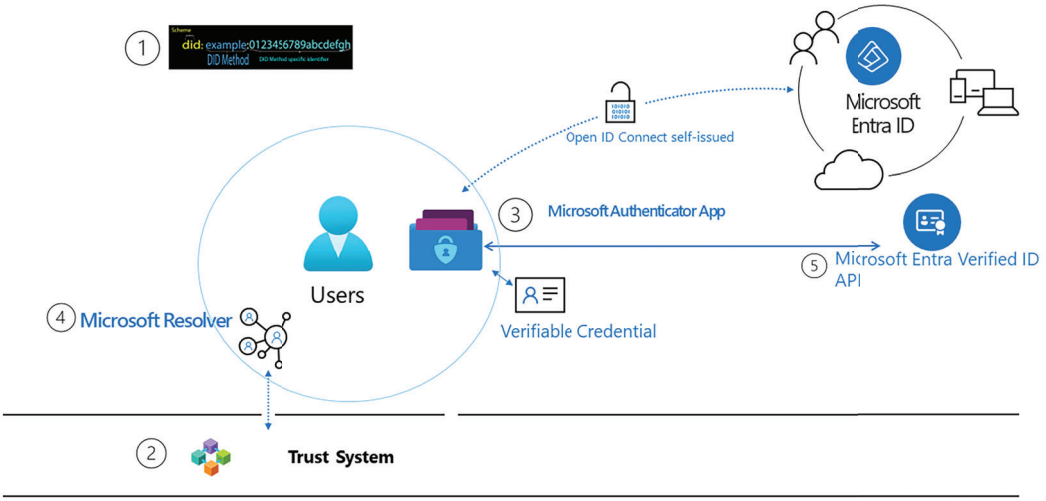


Figure 10.1: Decentralized identity

The following points explain each of the components in *Figure 10.1*:

1. **W3C Decentralized identifiers**: Everything starts with a DID that users can create, own and control independently. DIDs are unique identifiers that are linked to **Decentralized Public Key Infrastructure (DPKI)**. DID documents are JSON documents that contain public key material, authentication descriptors and service endpoints.
2. **Trust system**: At the core is a trust system that is used to resolve the DIDs. Microsoft leverages the `did:web` trust system, which allows trust using a domain's reputation.
3. **Microsoft Authenticator App**: This is the user agent or wallet where the users can store and present their DIDs and Verifiable Credentials.
4. **Microsoft Resolver**: This API facilitates the lookup and resolution of a DID utilizing the `did:web` method.
5. **Microsoft Entra Verified ID**: This is the issuance and verification service that enables subjects to create, own and present their DIDs. This is the basis of the trust between issuers, holders and verifiers.

> **Note**
>
> The `did:web` method lets organizations publish their DID documents directly on their web domain using HTTPS and DNS. This approach leverages existing web infrastructure for trust and discovery rather than blockchain anchoring.

Let's understand this with the help of an example. Bob is an employee of Litware Inc. Due to his employment with Litware Inc., he gets discounts from his gym. To get the discount he must prove that he is an employee of Litware Inc. Litware Inc. issues verifiable credentials to all its employees that Bob stores in his Microsoft Authenticator App. He can now present this credential on the gym website to prove his employment and avail the discount. This transaction is logged to help Bob track who he has presented his credential to.

When organizations setup Microsoft Entra Verified ID, their DIDs are registered with **Microsoft Entra Verified ID Network**. This is a discovery and trust framework that makes it easy for verifiers to find issuers' DIDs and credential types. This enables streamlined credential verification across organizations.

Microsoft also partners with third-party providers of identity services such as AU10TIX, IDEMIA and LexisNexis. These are government ID verification partners that are available in the **Microsoft Security Store**. Organizations can choose to require employees and business guests to provide a government identification proof and perform a face check against that as a part of the verification process. This is particularly useful in cases of remote onboarding and total loss recovery – when employees have lost all access to their account and need to recover.

Licensing

Organizations can issue, verify or revoke up to 50,000 transactions per month with the free version of Microsoft Entra. After this, Microsoft Entra P1 or P2 is required to continue using Verified ID.

Now that we understand the basic concepts, let's dive deeper into Microsoft Entra Verified ID.

Get started with Microsoft Entra Verified ID

Now that you have understood the basic concepts of decentralized identities and verifiable credentials, let's get started with setting up Microsoft Entra Verified ID. Microsoft Entra Verified ID can be set up using a quick setup or a custom setup.

Using quick setup

If you have a custom domain name configured in your Microsoft Entra tenant, you can use quick setup to automate all configuration steps and start issuing verified credentials within

minutes. Setting up a custom domain is explained in *Chapter 3, Implementing Microsoft Entra ID*. Quick setup creates your signing keys, registers DIDs, verifies domain ownership and creates a **Verified Employee** credential, all with the click of a button. The shared signing key is managed by Microsoft. To set up Microsoft Entra Verified ID, follow the steps below:

1. Sign in to `https://entra.microsoft.com` as **Authentication Policy Administrator**.
2. Navigate to **Verified ID | Overview**.
3. If you have a custom domain verified, you will see the **Get started** button as shown in the screenshot below. If not, the screen will default to the custom setup experience. Click on **Get started**.

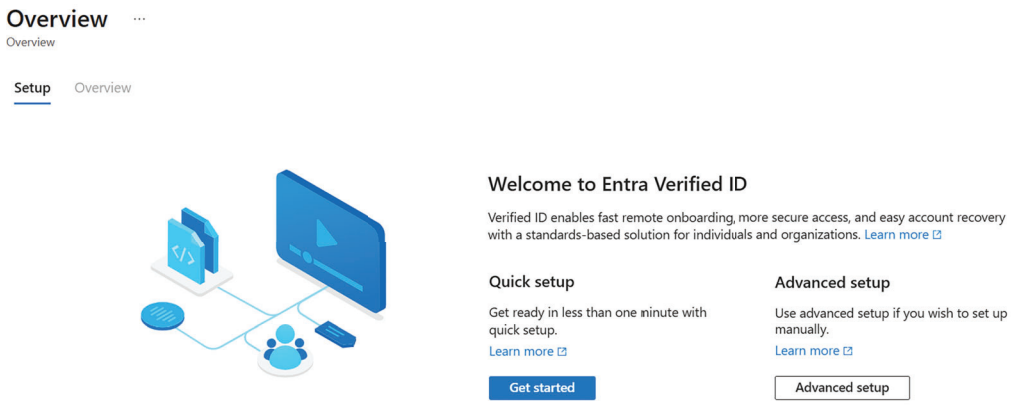


Figure 10.2: Quick setup experience

4. If you have multiple custom domains set up, you will have to choose the domain for which you would like to use Verified ID. If you do not have multiple custom domains, the setup will complete in a minute.
5. Once the setup is complete, you will be able to view and customize the verified credential that will be issued to your employees. Refer to *Figure 10.3*:

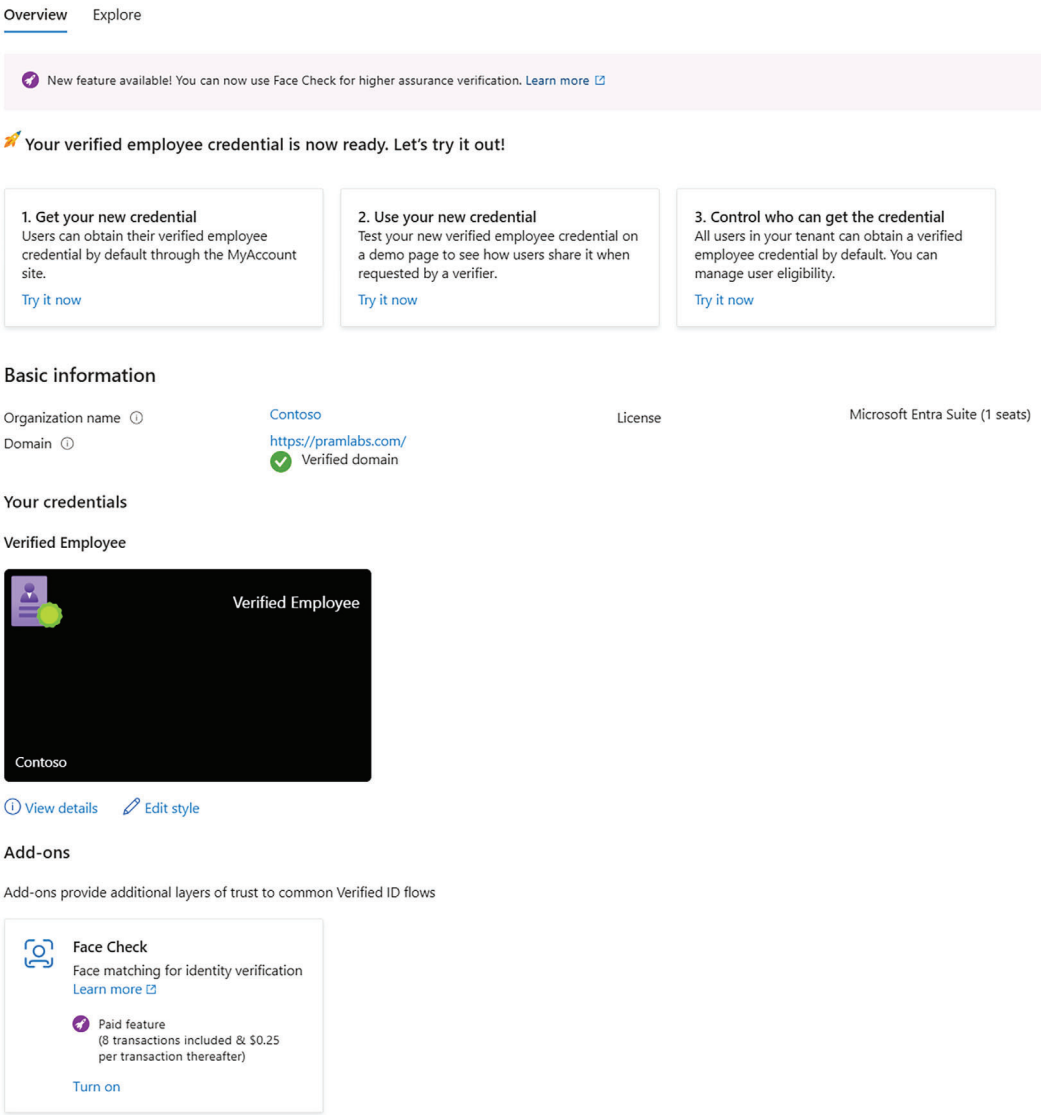


Figure 10.3: Verified credential

By default, employees can get their Verified ID from the **My Account** portal. If organizations desire, they can create a custom application for issuing Verified ID. This is explained later in this chapter under the section *Custom credentials.*

Administrators can also specify groups of users who can use **My Account** to download Verified ID. These options are available by clicking on **View details** under the **Verified Employee** credential as shown in *Figure 10.3* and then selecting **Issue a credential**. Refer to the following screenshot:

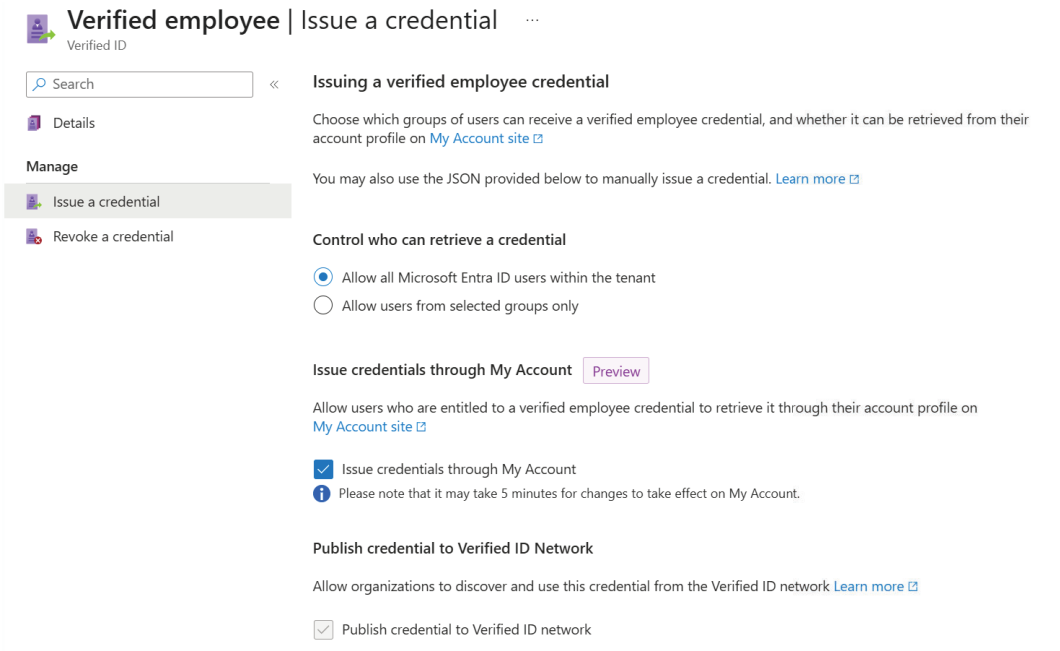


Figure 10.4: Verified credentials settings

Notice that you can control which users receive a credential and whether you want employees to be able to use the **My Account** portal to download their Verified IDs.

End user experience

To download verifiable credentials from **My Account**, follow the steps below:

1. Sign in to `https://myaccount.microsoft.com`.

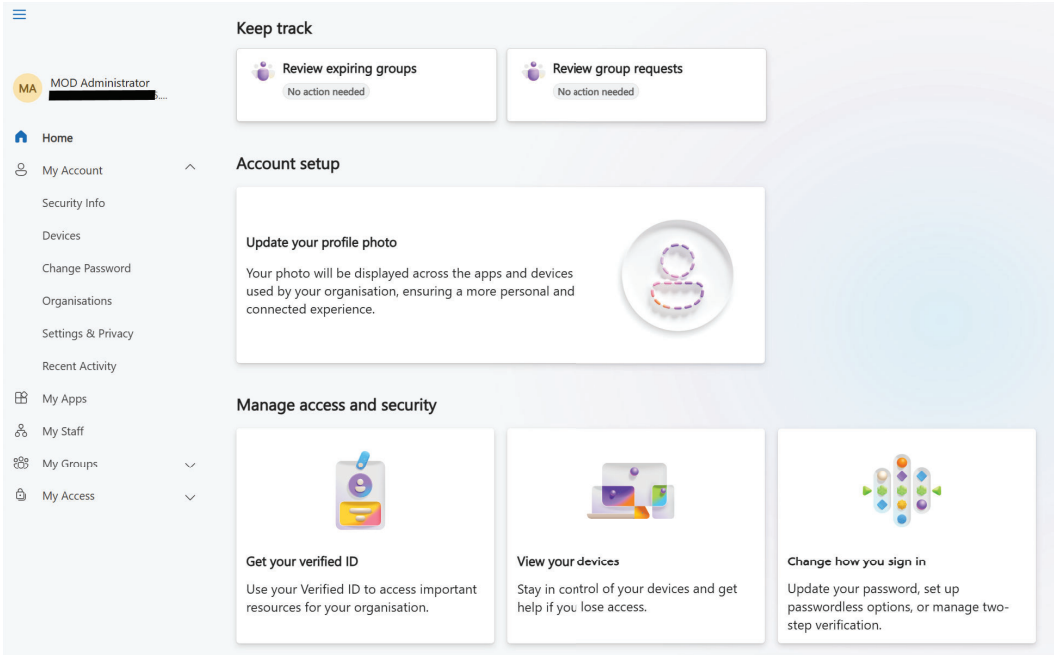


Figure 10.5: Get Verified ID from My Access page

2. On the **Home** page, click on **Get your verified ID**. A QR code will be displayed. If you don't have the Microsoft Authenticator app, you will be prompted to download it. If you have it, you can scan the QR code using the app and save the Verified ID in the app as shown in the screenshot below.

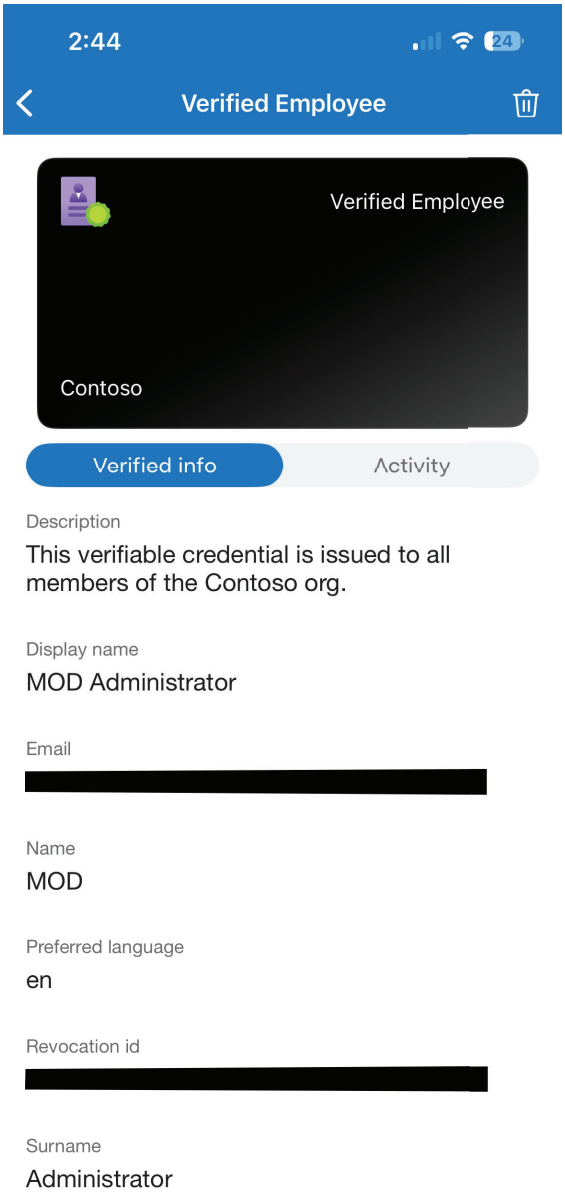


Figure 10.6: Verified credentials in Microsoft Authenticator app

Verified IDs are valid for 6 months, after which employees must go back to the **My Account** portal and download them again.

Using advanced setup

If you do not have a custom domain verified in your tenant or if you want more control over configuring your DIDs, you can use advanced setup. This gives the administrator full control over the configuration process. Using advanced setup, organizations can issue custom credentials that they design from scratch. At a high-level, advanced setup includes the following steps:

1. Configuring Azure Key Vault to store the keys for signing and verifying credentials.
2. Creating and registering decentralized identifiers.
3. Linking your domain to the DID to provide a trusted source for credentials.

Let's go through them in detail.

Creating a key vault

Azure Key Vault is an Azure service to securely store secrets and keys. It also enables access management of secrets and keys. The Verified ID service leverages Azure Key Vault to store public and private keys used to sign and verify credentials.

Note

The detailed steps to create a key vault are beyond the scope of this book. To create a key vault, refer to `https://learn.microsoft.com/en-us/azure/key-vault/general/quick-create-portal`.

Keep the following considerations in mind while creating the key vault:

- You must have the **contributor** role on the Azure subscription or resource group where the key vault will be deployed.
- The permission model on the key vault must be set to **Key Vault Access Policy** instead of Azure role-based access control.

By default, the account that created the key vault is the only one that can access it. The Verified ID service needs to access the key vault. Authenticate the key vault to allow the account used to configure Verified ID to create and delete keys. Also ensure that the account has permissions to sign to enable it to create the domain binding for Verified ID.

Tip

There is no built-in role in Microsoft Entra ID called Verified ID Administrator. Verified ID relies on other built-in roles like Global Administrator or Security Administrator. While using the advanced setup ensure that you have the **Authentication Policy Administrator** and the **Application Administrator** roles as Verified ID relies on App

registrations. The Global Administrator has all permissions; however, to ensure least privilege, avoid using it.

Setting up Verified ID

To set up Verified ID using the advanced setup, follow the steps below:

1. Sign in to `https://entra.microsoft.com` as **Authentication Policy Administrator**.
2. Navigate to **Verified ID | Overview**.
3. If you don't have a custom domain configured, this will default to the advanced setup. If you have a custom domain, in the right pane, click on **Advanced setup**. Refer to *Figure 10.2*.
4. Click on **Configure** under **Configure organization settings**.

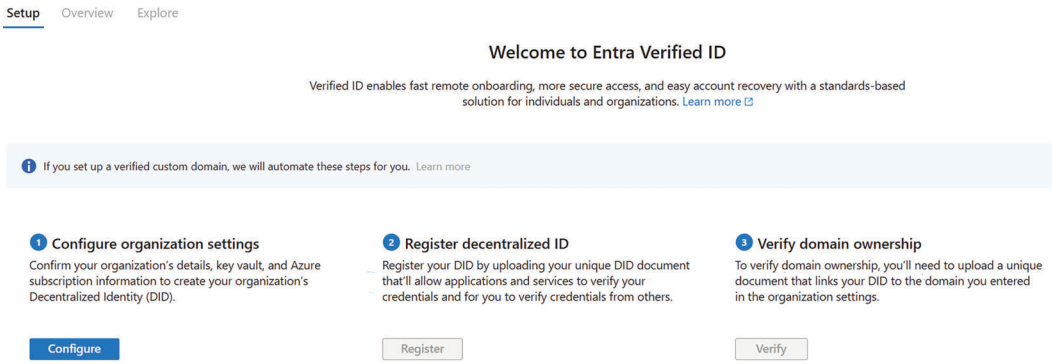


Figure 10.7: Advanced setup experience

5. Enter your **Organization name**. This is a name that identifies your business within Verified IDs. It is not visible to customers.
6. Enter a **Trusted domain** name. This name is added to a service endpoint in the DID document. This is what binds the DID to your business. Digital wallets like Microsoft Authenticator use this information to validate that the DID is linked to your domain.

> **Tip**
>
> This domain should not be a redirect or the DID domain cannot be linked. Ensure that you use HTTPS for the domain. For example, `https://did.contoso.com`.

7. Click on **Select keys** to select the Azure Key Vault created earlier and click **Save** as shown in the following screenshot.

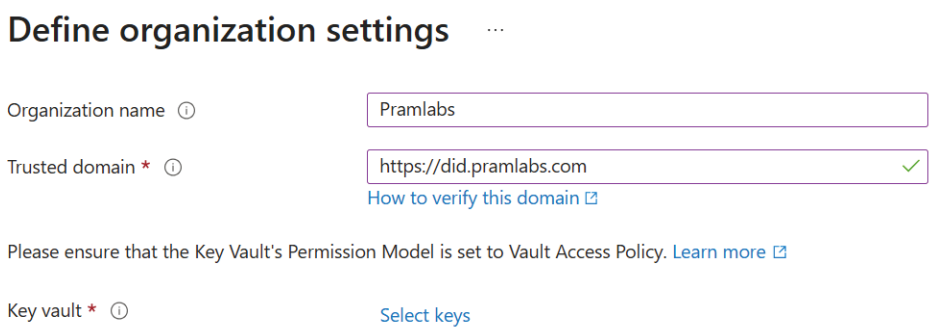


Figure 10.8: Verified ID advanced setup

Behind the scenes, the Verified ID service provisions a service principal called **Verifiable Credentials Service Request**. This service principal represents the Verified ID service in your tenant and is used to handle issuance and verification requests for verifiable credentials. You can navigate to **Entra ID | Enterprise Applications** to ensure that the service principal has been created.

Registering an application

While using advanced setup, the administrator will need to register an app to act as the issuer identity (DID owner). The actual distribution of credentials is performed by a separate issuing application that you build and host elsewhere. Follow the steps below to register an app in Entra ID.

1. Sign in to `https://entra.microsoft.com` as **Application Administrator**.
2. Navigate to **Entra ID | App registrations | New registration**.
3. Enter a display name for the app.
4. Under **Supported account types**, select **Accounts in this organizational directory only (Default directory only - Single tenant)**. Click on **Register** to create the application.

5. Now that the application is created, permissions need to be granted to the **Verifiable Credentials Service Request** service principal. In the left pane click on **API permissions | Add a permission**.
6. Click on **APIs my organization uses**. Search for **Verifiable Credentials Service Request** and select it.
7. Click on **Application permissions** and select **VerifiableCredential.Create.All** and click **Add permissions**.
8. Click **Grant admin consent for <tenant name>**.

Once Azure Key Vault has been created and the service has a signing key, we must now register the DID.

Registering a DID

Your DID needs to be registered so that it can issue and verify credentials. This information must be made available on the organization's website; otherwise, the public key is not made public. Following are the steps:

1. Sign in to `https://entra.microsoft.com` as **Authentication Policy Administrator**.
2. Navigate to **Verified ID | Overview**.
3. Click on **Register** under **Register decentralized ID**. A window will open with your DID document. Click on **Download** and save it. This file should have a name like `did.json`.
4. This file must be uploaded to the organization's web server under `/.well-known/did.json`.
5. Once uploaded, click on **Refresh registration status** to ensure that the service can request the file.

The DID document contains public keys which are used by the wallet, like the authenticator app, both when issuing and presenting verified credentials. If signing keys are rotated or the linked domain is changed, the `did.json` file must be republished on the web server.

Verifying domain ownership

The domain you verify must be under your control and must be in the format `https://www.domain.com`.

1. Sign in to `https://entra.microsoft.com` as **Authentication Policy Administrator**.
2. Navigate to **Verified ID | Overview**
3. Under **Verify domain ownership**, click on **Verify**.
4. In the window that opens, click on **Download** to save the `did-configuration.json` file.

5. Host the `did-configuration.json` file on your web server under `https://www.domain.com/.well-known/did-configuration.json`.
6. Once the file is publicly available, you can verify it by clicking on **Refresh verification status**. The portal verifies that the `did-configuration.json` file is reachable over the internet and valid.

Verifying DID domain ownership is an important step as it establishes the relationship between a DID and a domain. This solves the trust problem by allowing an entity like a mobile wallet or the Microsoft Authenticator app to validate the relationship between a DID and a domain.

Microsoft Entra Verified ID uses the **well-known DID configuration** specification to create a link between DIDs and domains. The verifiable credentials service links the DID and domains. It includes the domain information that was provided in the DID to generate the well-known configuration file.

Advanced setup supports building real, custom, enterprise-grade verifiable credentials tailored to your organization's identity, governance, and automation needs.

Custom credentials

Microsoft Entra Verified ID can issue any verifiable credential you define, from employment and education credentials to KYC, age, membership, and entitlement credentials. Plus, it supports consuming pre-built credentials from the Verified ID Network.

Let's understand how you can issue and verify custom credentials.

Issuing custom credentials

Once the Verified ID setup is complete, you will be able to create custom credentials using the following steps:

1. Sign in to `https://entra.microsoft.com` as **Authentication Policy Administrator**.
2. Navigate to **Verified ID | Credentials**. In the right pane click on **Create credential**.
3. On the **Create credential** page, select **Custom credential** and click **Next**.
4. Enter a name in the **Credential name** box. This name is used to identify the credential.
5. Enter the **Display definition** and **Rules definition** in JSON format and click **Create** to create the credential.

Note

A **display definition** is the part of the custom credential that controls how the credential looks to the user in their wallet. It includes its branding, layout, colors, icons,

and the human-readable labels for each claim. Think of it as the presentation layer of your verifiable credential.

A **rules definition** is the part of the custom credential that defines what the credential is. It defines the data model, claims, constraints, and issuance logic.

The following figure shows the custom credential creation page:

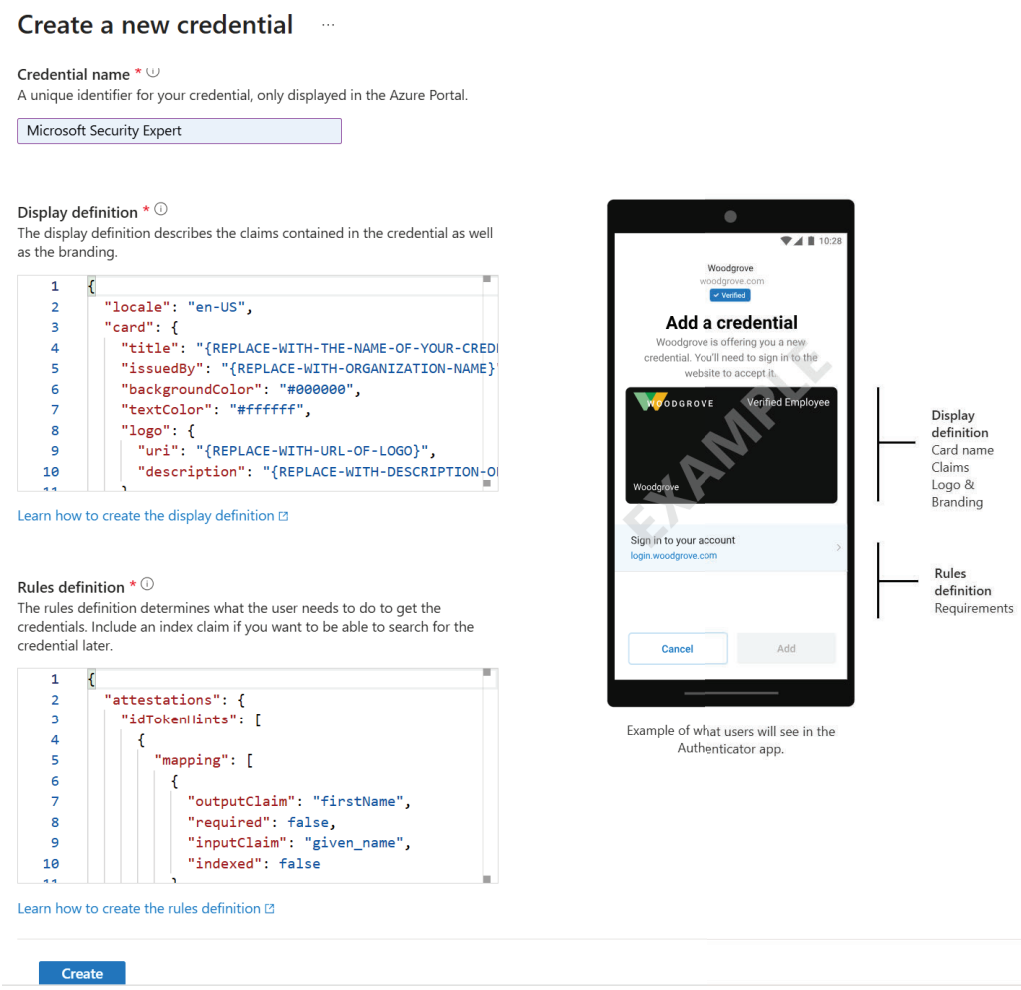


Figure 10.9: Creating a custom credential

Once the credential is created, the following pieces of information are required to configure the application that is used to verify the credential:

- **Authority**: This is the decentralized identifier.
- **Manifest URL**: This is the URL that the Authenticator app evaluates before showing the verifiable credentials issuance requirements to the user.
- **Tenant ID**: This is the **Globally Unique Identifier** (**GUID**) in the manifest URL as shown in the box below.

This information is available by clicking on **Issue a credential** on the custom credential page as shown in the following screenshot.

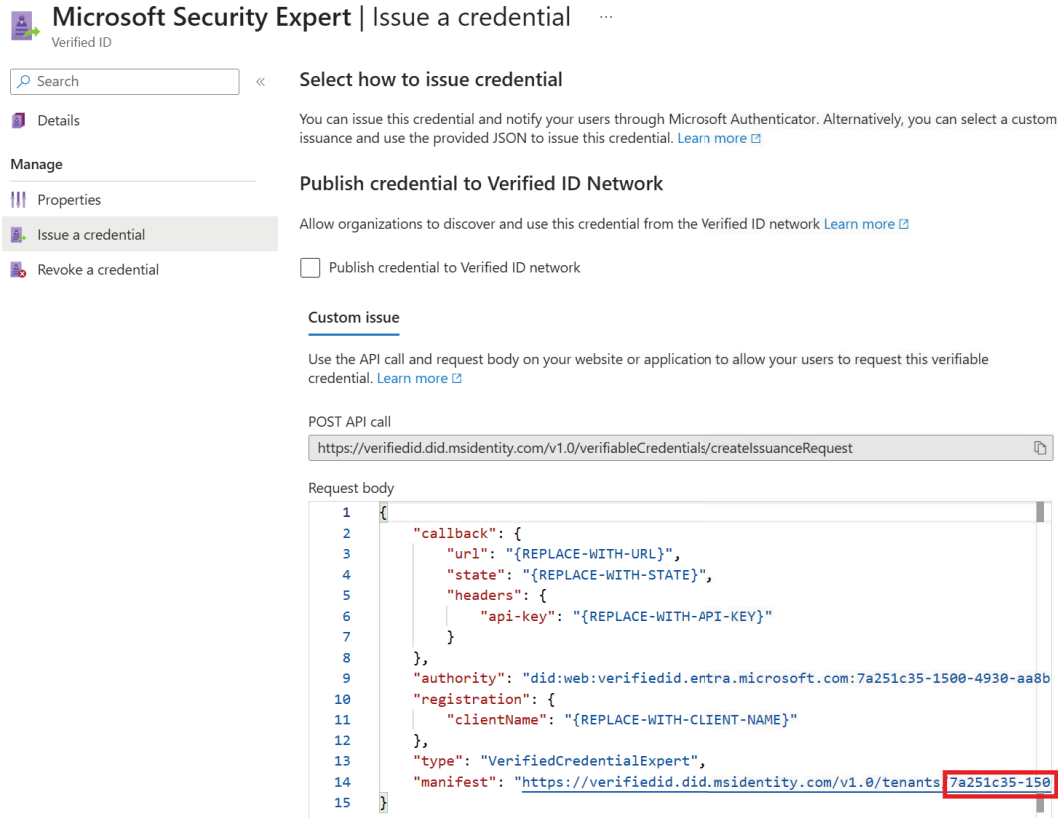


Figure 10.10: Capture information

Once you have this information, add a client secret to the verifiable credentials app created in the *Registering an application* section. The following are the steps:

1. Navigate to **Entra ID | App registrations | All applications** and select the application created earlier. Copy the **Application (client) ID** and save it.
2. Click on **Certificates & secrets | New client secret**.
3. Enter a description and expiry and click **Add**. Record the secret's value. This is the only time the secret's value is displayed. Make sure you copy it before navigating away from this screen.

At this point you must have the authority URL, manifest URL, tenant id, application (client) ID and client secret to configure the application that issues credentials.

> **Note**
>
> Manifest URL is only needed for issuing credentials. If your app is only going to verify credentials, it is not required.

Creating the issuing app

The application that issues verifiable credentials is not the app registration created during advanced setup. It is your own backend application, running on Azure, on-prem, AWS, or GCP. Following are the high-level steps to configure this application:

1. Create an app registration in Microsoft Entra for the issuing application and assign a client secret. This application must have the `VerifiableCredential.Create.All` API permission. Grant admin consent to the app.
2. The application must obtain an access token from Entra ID using the OAuth 2.0 client credentials flow. Use the following information to configure the app:
   - Token endpoint: `https://login.microsoftonline.com/{tenantId}/oauth2/v2.0/token`
   - Scope: `https://verifiedid.did.msidentity.com/.default`

   This token is required to call the **Issuance API**.
3. Call the **Issuance API** to create an issuance request. Your app must send the following POST request to the Issuance API:

```
POST https://verifiedid.did.msidentity.com/v1.0/verifiableCredentials/
createIssuanceRequest
```

The request body must include authority, credential type (default or custom), claims (values your app provides), callback URL (your app's endpoint), and manifest URL.

Your app will receive a response containing a QR code, a request ID, and a URL for deep linking into the wallet.

4. Your app must host a callback endpoint to receive issuance results. Verified ID will post `requestId`, `state`, `subject`, and `issuanceStatus`. The app will use this to mark the issuance as successful, trigger the onboarding flow and notify the user. This callback is essential; otherwise, the app will not know if the issuance succeeded.

> **Note**
>
> A sample application in .NET is available on GitHub. You can download the sample code from `https://github.com/Azure-Samples/active-directory-verifiable-credentials-dotnet`. Open the code in Visual Studio Code and update the app code with the information collected.

Once the application code is configured, it is now ready to issue credentials.

Verifying credentials

In a real-world scenario, organizations will need to verify credentials issued by another organization.

Setting up Verified ID

To be able to verify credentials, the verifying organization must have Microsoft Entra Verified ID set up. Next, start gathering the credentials and environment details to configure the verifier application. These are described below.

1. In the Microsoft Entra admin center, navigate to **Verified ID | Organizational settings** and copy the **Tenant identifier** and **Decentralized identifier (DID)**.
2. As a part of the setup, the verifier organization would have created an app registration in Microsoft Entra as described in the section *Registering an application*. From that app registration, copy the Application (client) ID. Create a client secret and copy the value of the client secret.

Ensure that you have your Tenant ID, Application (client) ID, client secret, decentralized identifier and CredentialType to configure the application that will verify credentials.

Creating the verifier app

Just like the issuer organization, the verifier organization needs an application that will perform the verification of the presented credential. The application that verifies credentials is not the app registration created during advanced setup. It is your own backend application, running on Azure, on-prem, AWS, or GCP. Following are the high-level steps to create the verifier app.

1. Create an app registration in Microsoft Entra for the verifier application and assign a client secret. This application must have the `VerifiableCredential.Create.All` API permission. Grant admin consent to the app.
2. The application must obtain an access token from Entra ID using the OAuth 2.0 client credentials flow. Use the following information to configure the app.
   a. Token endpoint: `https://login.microsoftonline.com/{tenantId}/oauth2/v2.0/token`
   b. Scope: `https://verifiedid.did.msidentity.com/.default`

   This token is required to call the **Presentation API**.
3. Call the **Presentation API** to create a verification request. Your app must send the following POST request to the Presentation API:

   ```
   POST https://verifiedid.did.msidentity.com/v1.0/verifiableCredentials/
   createPresentationRequest
   ```

   The request body must include authority, the credential type you want the user to present, required claims and the callback URL (your app's endpoint).

   Your app will receive a response containing a QR code, a request ID, and a URL for deep linking into the wallet. The app will display the QR code or link to the user.
4. Your app must host a callback endpoint to receive verification results. Verified ID will post `requestId`, `state`, `subject`, `verifiedCredentialsData` (claims that were requested) and `presentationStatus`. The app will use this to approve or deny access, log the verification and trigger downstream flows. This callback is essential, else the app will not know if the verification succeeded.

You can use the same sample application introduced in the previous section and configure it to verify credentials.

Now let's learn how we can take identity proofing to the next level by using Verified ID Face Check.

Verified ID Face Check

Verified ID Face Check is a security feature designed to enhance the trustworthiness and integrity of digital identity verification processes. By incorporating biometric authentication, specifically facial recognition, the Verified ID Face Check ensures that the individual presenting a verifiable credential is the legitimate owner. The process typically involves prompting the user to take a real-time selfie, which is then compared against the photo or biometric data stored in their digital credential or on file with a trusted issuer.

This technology is crucial in preventing identity fraud and impersonation since it makes it much harder for malicious actors to use stolen or fake credentials. Face Check can be seamlessly integrated into onboarding workflows, remote access scenarios, or high-value transactions, providing organizations with a robust layer of assurance. Additionally, it supports privacy by processing biometric data in compliance with regulations, often ensuring that sensitive information is not stored or transmitted unnecessarily.

For users, the experience is streamlined and user-friendly, usually requiring only a few moments to complete. The combination of ease of use and enhanced security makes Verified ID Face Check an attractive option for enterprises looking to protect both their assets and their users' identities in a digital-first world.

Enabling Face Check

Face Check can be enabled from within the Microsoft Entra admin center or by using the REST API. The following are the steps to enable Face Check from the Microsoft Entra admin center:

1. Sign in to `https://entra.microsoft.com` as **Authentication Policy Administrator**.
2. Navigate to **Verified ID** | **Overview**.
3. Scroll down. Under **Add-ons** click **Turn on**. Refer *Figure 10.3*.
4. You will have to link an Azure subscription for billing purposes. Select the Subscription, Resource group, and location and click **Validate**.
5. Once validated, click on **Turn on** as shown in the screenshot below:

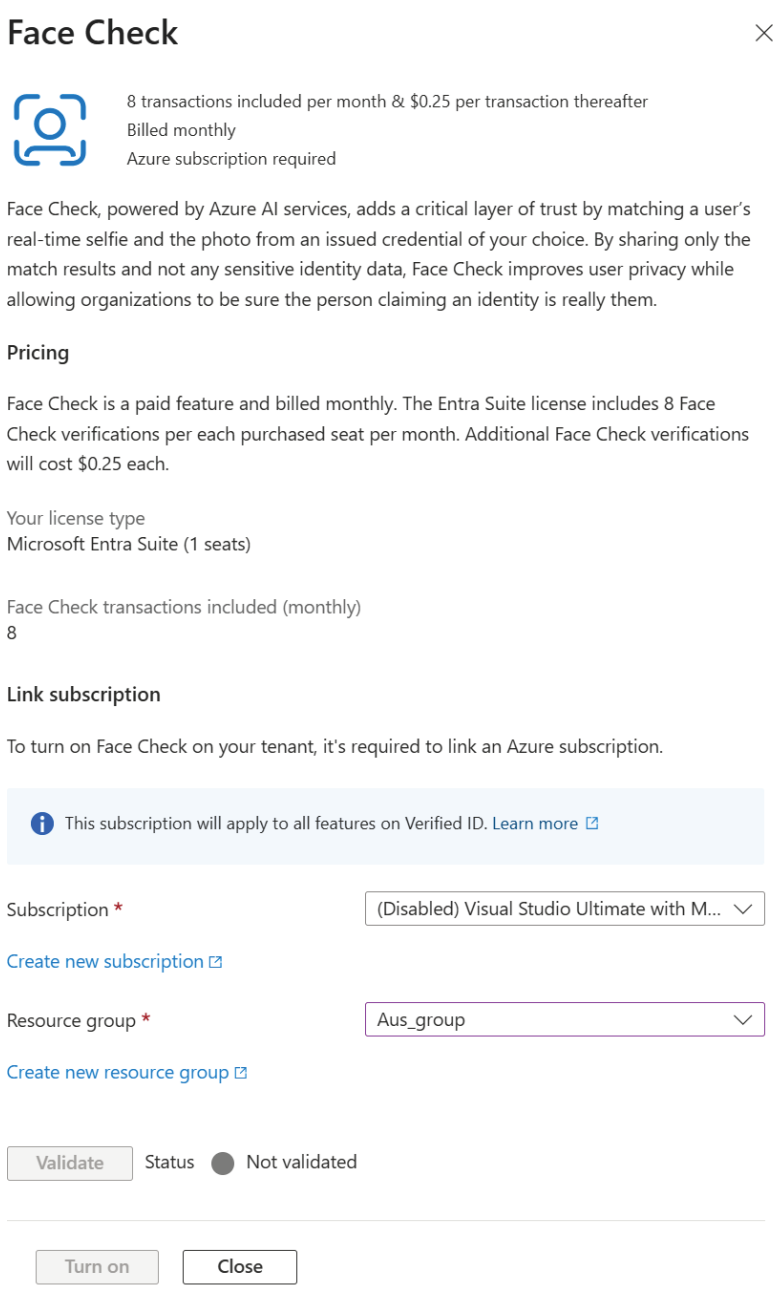


Figure 10.11: Enable Face Check

Organizations can now require users to perform a Face Check when performing high-value transactions like resetting passwords, requesting access packages, or accessing critical resources.

> **Tip**
>
> Since Face Check compares a real-time selfie of the user against a picture on file, ensure that the user Entra ID object has a proper picture uploaded.

The biometric check between the photo and the real time selfie is performed in the cloud using **Azure AI Vision Face API**. This service checks for liveness, which means that it ensures that it is a real person who has captured the picture and that a static 2D picture or video was not used.

The footage is captured on the mobile device and is passed on to Verified ID. Verified ID uses it to involve Azure AI services. Once processing is complete, the image is discarded. It is not saved in the Microsoft Authenticator app or any online services. It is also not shared with the site or service that requested the Face Check. The verifier only gets a likeness match score which is the percentage of confidence that the Face Check was performed by the same individual whose picture it is being compared with.

Licensing

There are two options for licensing for Face Check:

- **Pay-as-you-go**: Organizations with Microsoft Entra Free, P1 or P2 can pay per face check verification.
- **Entra Suite**: Organizations with Entra Suite licenses get 8 face checks per seat per month. These are aggregated at the tenant level. If an organization consumes all of these, they are charged as per the pay-as-you-go model.

Choose the appropriate model depending on your organization's needs and the licenses it owns.

Next, we will learn how to use Verified ID with Microsoft Entra entitlement management.

Verified ID with entitlement management

In Microsoft Entra ID Governance entitlement management, administrators can create access packages for internal users, users in connected organizations or external users. For some critical resources, administrators might want the requester to provide additional proof that they are indeed the person they are claiming to be. With Verified ID integration with entitlement management, administrators can now require requestors to provide a verifiable

credential and complete a face check when requesting access to critical resources. Approvers can view if the requestor's verifiable credentials were validated at the time of the request.

An administrator can add a Verified ID requirement while creating a new access package or by editing the policy on an existing access package. Creating an access package has been explained in *Chapter 6, Microsoft Entra Entitlement Management.*

To add a Verified ID requirement, follow these steps.

1. Sign in to `https://entra.microsoft.com` as **Global Administrator**.
2. Navigate to **ID Governance | Entitlement management | Access packages**.
3. Click on **New access package** and on the **Requests** tab scroll down to **Additional Settings**.
4. Click on **Add issuer** and choose an issuer from the **Microsoft Entra Verified ID network or Security Partners (Third-party providers)** as shown in the following screenshot.

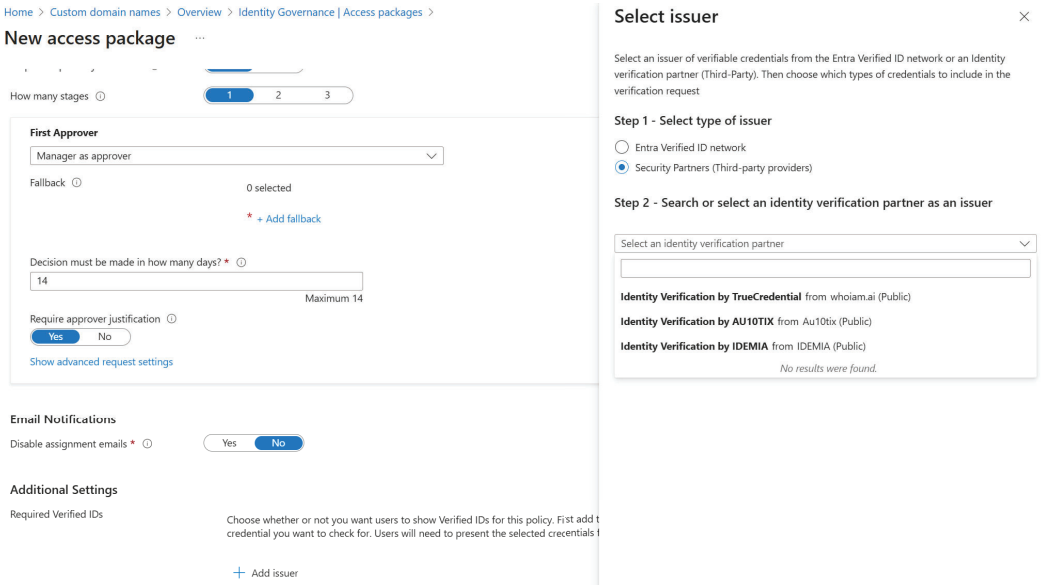


Figure 10.12: Add issuer

5. Select the **credential type(s)** you want users to use while requesting access.

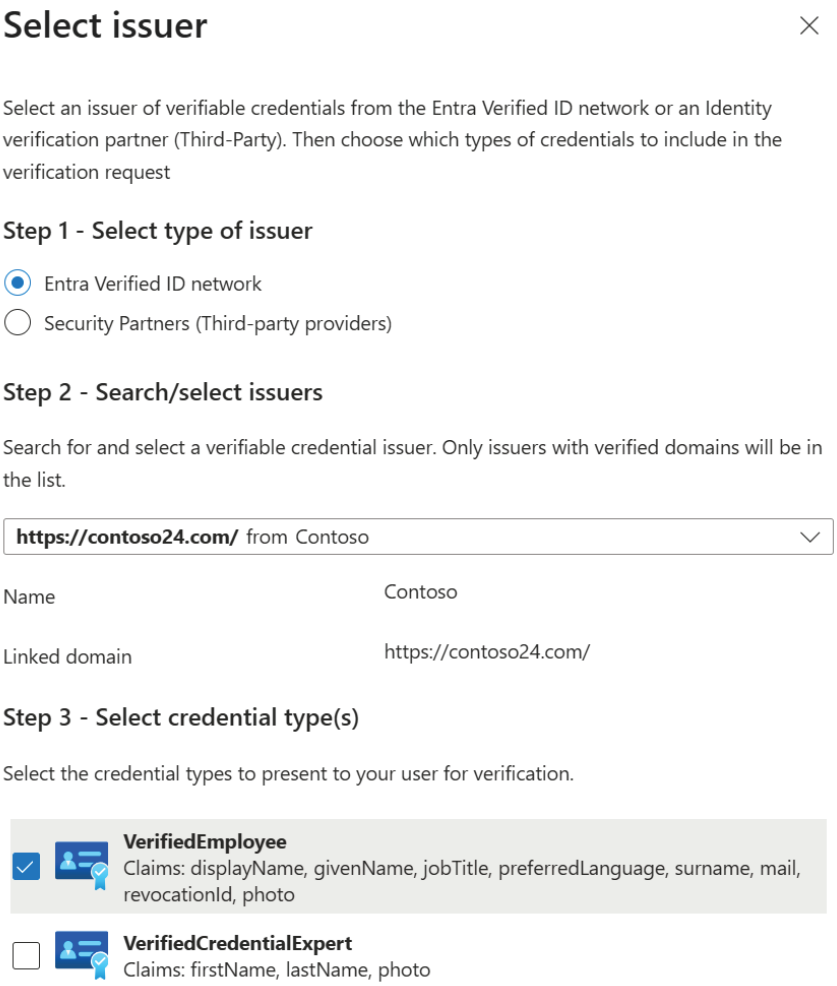


Figure 10.13: Select credential type

6. Click **Add** to add the Verified ID requirement to the access package policy.
7. If you want the users to complete a face check, select the box **Require Face Check**.

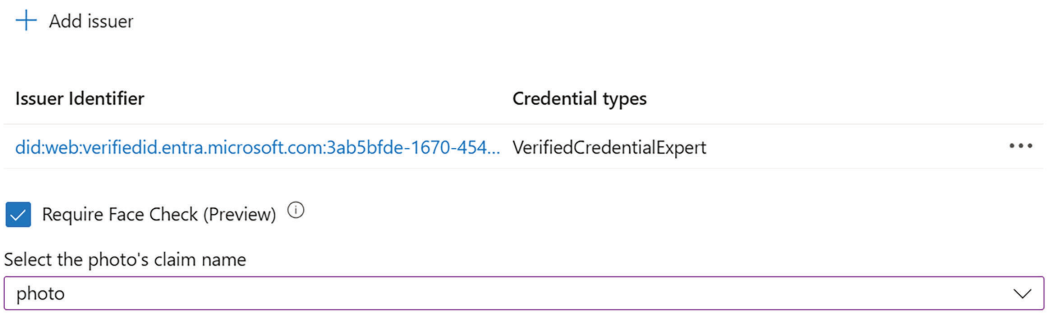


Figure 10.14: Require face check

8. Configure the rest of the settings for the access package and click on **Review + create** to create it.
   Now when the users request access to an access package from the My Access portal, they will be prompted to present a Verified ID and complete a face check. Following is the user experience.
9. User signs into `https://myaccess.microsoft.com` and clicks on **My Access | Access packages**.
10. User selects the access package they want and clicks on **Request**. They see an information banner asking them to present their verified credentials as shown in the following screenshot. Click on **Continue**.

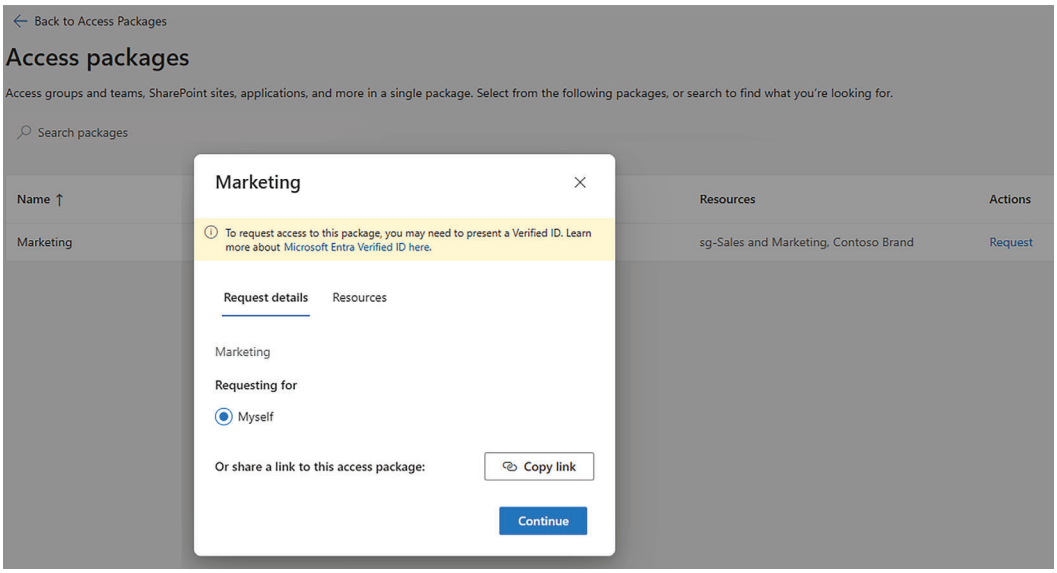


Figure 10.15: Require Verified ID

11. A QR code is displayed, which users can scan using their phone. This launches the Microsoft Authenticator app where their Verified ID is stored. They will be prompted to share the credentials.
12. If Face Check is required, the user will be prompted to complete a Face Check by providing a real-time selfie.
13. Once the verification is complete, the user can proceed with the next steps in requesting the access package.

With this integration between Verified ID and entitlement management, administrators can require high assurance ID proofing before providing access to critical resources.

Licensing

To use this feature, the organization must have Microsoft Entra ID Governance or Entra Suite licenses.

Now let's learn how Microsoft Entra Verified ID helps in situations where users lose their devices and have no way of accessing their accounts.

Account recovery

Most organizations today require users to complete several authentication methods to access resources. Sometimes situations arise where users lose all access to their authentication methods. They lose their primary device, and all backup codes are lost. In such cases, self-service password reset becomes useless as it requires users to provide at least one form of registered authentication method. This is a bigger problem for passwordless users who have no self-service options. In most cases, the user must call the helpdesk. The helpdesk must ensure that the user is who they are claiming to be. Usually, they rely on security questions like mother's maiden name, pet's name or the street someone grew up on. This process has inherent risks as this information is easily discoverable in today's social media world. A bad actor can easily impersonate an employee or, worse, a senior executive.

Microsoft Entra ID Account Recovery addresses these scenarios by enabling users to recover their accounts using robust identity verification processes. Account recovery differs from password reset in that password reset assumes that the user has some form of second factor authentication still available. Account recovery assumes that the user has lost all forms of authentication and a total loss recovery needs to be performed. It shifts the focus from simple password reset to comprehensive identity verification and re-onboarding. It leverages Verified ID to ensure that the person requesting the account recovery is the actual owner of the account.

Account recovery follows an identity-centric approach and shifts the focus from *something you know* (passwords) and *something you have* (MFA options) to *who you are* by using robust ID proofing mechanisms. Account recovery is treated as employee re-onboarding, where the organization must re-establish trust in the employee's identity. Leveraging modern technologies like Verified ID and Face Check, it provides strong assurance of the user identity during the account recovery process.

It is most suited for scenarios where a user has lost their primary device that has all their authentication methods or when a security incident has compromised the user's account.

Account recovery is a self-service process that reduces the burden on helpdesk by providing a secure option for total account recovery. It also improves user experience as they don't have to wait for the helpdesk to be available to help them.

It integrates with trusted third-party identity verification providers to use government-issued IDs for user identification and biometric verification. The following picture shows the account recovery workflow:

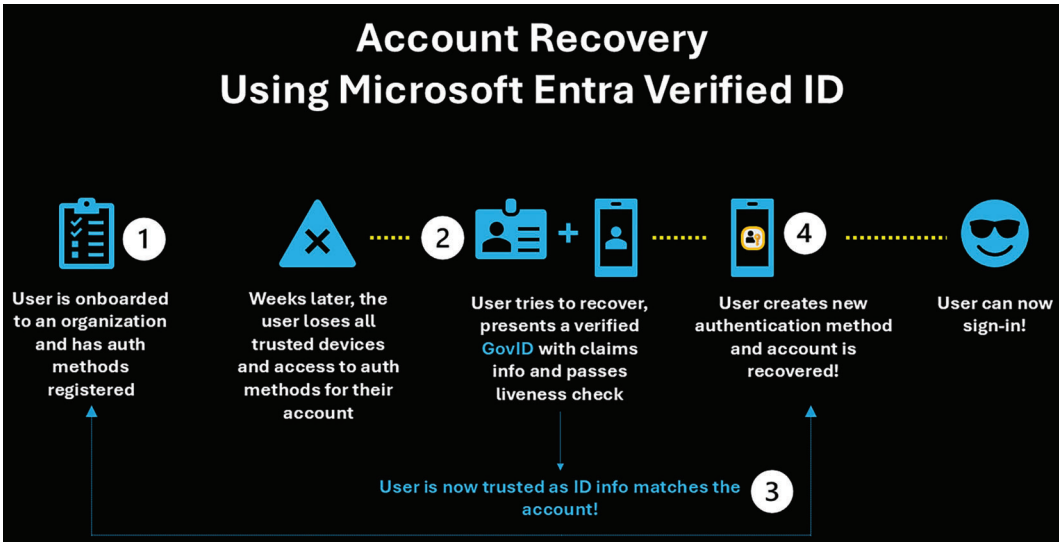


Figure 10.16: Account recovery workflow

The recovery workflow consists of four steps.

1. User is onboarded into the organization. They provide their account identifiers like usernames or email addresses. They register additional authentication methods like Microsoft authenticator app or passkeys. They then lose their trusted devices and hence lose access to their account.

2. The user starts the recovery flow and is prompted to upload a government-issued ID document like a passport or driving license. They are asked to perform a biometric verification against the ID. This could be a face check that matches a real-time selfie with the picture on the uploaded ID document.
3. The user is now trusted as the ID information matches their account.
4. The user is now issued a Verified ID from their organization that they can store in their Microsoft Authenticator app and present to Microsoft Entra ID to recover their account. At this point Entra ID can ask for another Face Check to match the user's selfie with the profile picture on their Entra ID user object. Users are then guided through account recovery and registering new authentication methods.

Account recovery in Entra ID also has a special configuration wizard that enables admins to define recovery requirements, detailing who can recover and which trusted providers can provide identity proofing services. It is a secure by default feature. It has an evaluation mode and is very quick to set up.

Microsoft Entra ID P1 is required to enable account recovery.

> **Note**
>
> At the time of this writing this feature is in Public Preview.

Account recovery in Microsoft Entra ID uses government-issued IDs and biometric verification through a secure, configurable workflow, allowing users to regain access when trusted devices are lost.

Revoking credentials

Once a user is issued a verifiable credential, it is theirs. However, sometimes organizations may need to revoke credentials in scenarios like employee termination. Microsoft Entra Verified ID implements the **W3C Bitstring Status List**, which is a mechanism for publishing the status of verifiable credentials. When Microsoft Entra Verified ID issues a verified credential, it contains a claim called `credentialStatus`, which is where a verified credential has its revocation flag.

Since Microsoft Entra Verified ID does not store verified credentials, the issuer of the credential needs to have one claim so that the credential can be searched. Only one claim can be indexed. If this claim does not exist, the credential cannot be revoked because Microsoft Entra Verified ID cannot find it. This claim is salted and hashed and then stored. Its original value is not stored.

If you used the quick setup to issue verified credentials, you can find the claim by following the steps below.

1. Login to `https://entra.microsoft.com` as an admin user that has the signing key permission on the Azure Key Vault.
2. Navigate to **Verified ID | Credentials**.
3. Select the credential type.
4. On the **Details** page, click on claims as shown in the screenshot below:

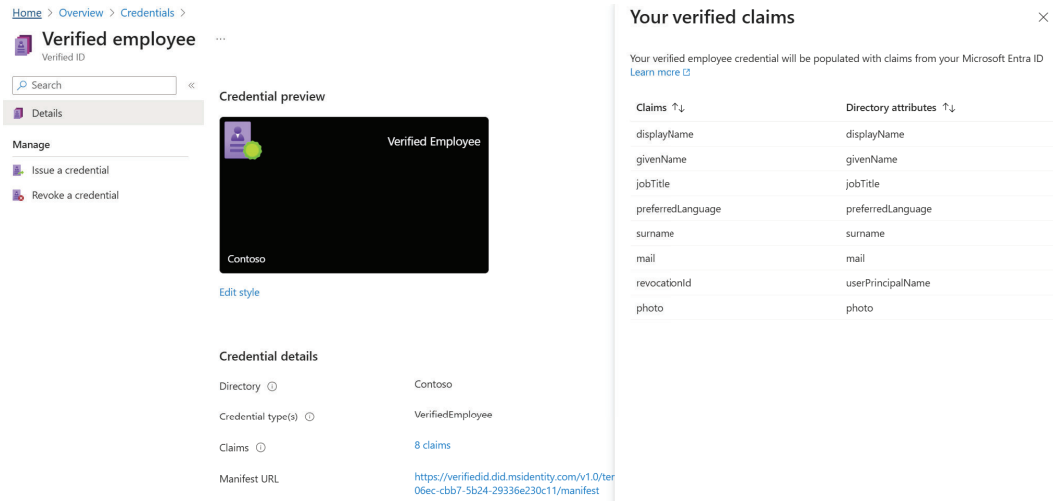


Figure 10.17: Claims in verifiable credentials

5. Note the attribute listed against the claim `revocationId`. This is the indexed claim that will be used to search the verified credential.

To revoke a verified credential, follow the steps below:

1. Click **Revoke a credential**.
2. In the search box, enter the indexed claim for the user whose credential you want to revoke. Since only the hashed value of the claim is stored, only exact matches will yield results. In the above example, the indexed claim is `userPrincipalName`. To revoke a credential, you will have to enter the exact `userPrincipalName` to get results as shown in the screenshot below.

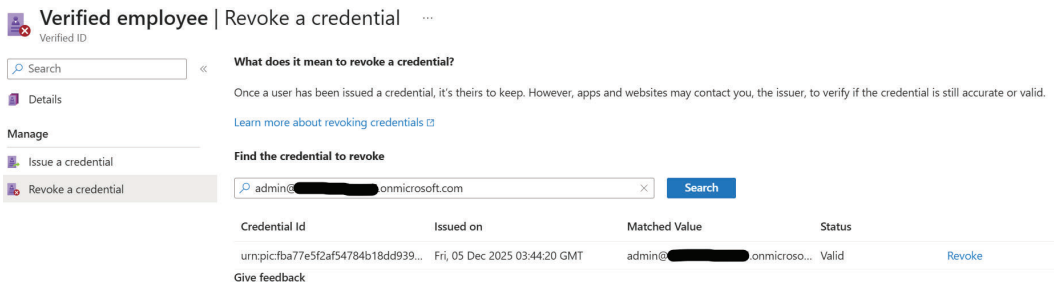


Figure 10.18: Searching for credentials

3. Click on **Revoke**. In the pop-up box, click on **Revoke** again, to revoke the credential.

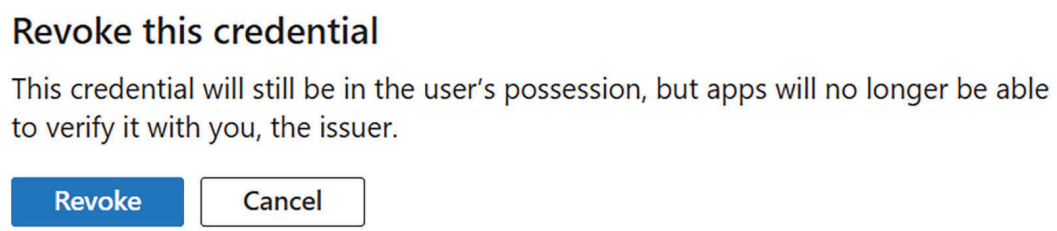


Figure 10.19: Revoking a credential

4. Once the credential is revoked, the status changes to **Revoked** as shown in the following screenshot:

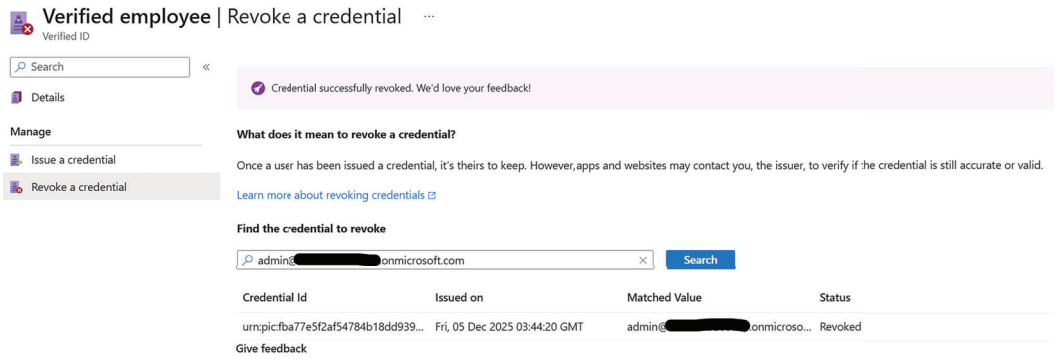


Figure 10.20: Credential revoked

The credential still exists with the user, but a verifier will not be able to verify the credential with the issuer.

Timely revocation of credentials is imperative to ensuring that users are not able to use a credential when their relationship with the issuing organization ends.

Opting out of Verified ID service

Opting out of Verified ID is the process of resetting the service at your Microsoft Entra tenant level. This is a one-way operation and once complete the organization's Verified ID environment is reset to defaults. Organizations might choose to do this if they want to enable new services or reset their existing configuration.

To opt out of the Verified ID service, follow these steps:

1. Login to `https://entra.microsoft.com` as Admin user that has the sign key permission on the Azure Key Vault.
2. Navigate to **Verified ID | Organization settings**. Click on **Delete all credentials and reset service**.
3. In the fly out pane, click on **Delete & opt out**.

When organizations opt out of the Verified ID service, Microsoft deletes the DID keys in Azure Key Vault. The issuer object, tenant identifier, and all verifiable credentials contracts are also deleted. Once the deletion is complete, the DID cannot be recovered and no operations can be conducted on it. If organizations want to use the service, they will have to onboard again which results in the creation of a new environment. The verifiable credentials already issued continue to exist.

Summary

In this chapter, we explored decentralized identities and verifiable credentials. We covered how to use the Microsoft Entra Verified ID service, including both quick and advanced setup methods. The chapter also detailed using Verified ID Face Check for high-assurance identity verification and explained its integration with entitlement management. Additionally, we introduced the basics of the new account recovery feature and discussed its applications in different scenarios. Finally, we learned how to revoke individual verifiable credentials.

Exercises

1. Which of the following best describes the purpose of Microsoft Entra Verified ID?
    a. To issue and verify decentralized identity credentials using open standards
    b. To manage user passwords and reset policies in Entra ID
    c. To encrypt emails in Microsoft 365
    d. To monitor network traffic for security threats

2. Where can administrators find the Verifiable Credentials Service Request service principal after enabling Microsoft Entra Verified ID?
    a. Under **App registrations** in the Entra portal
    b. Under **Enterprise Applications** in the Entra portal
    c. In the **Azure Key Vault** blade
    d. In the **Microsoft Security Store**
3. Which statement about the Microsoft Entra Verified ID Network is correct?
    a. It is a blockchain used to store all issued credentials
    b. It is a discovery and trust framework that helps verifiers find issuers' DIDs and credential types
    c. It is a password vault for storing user credentials securely
    d. It is a monitoring tool for detecting suspicious login attempts

Answers

1. a
2. b
3. b

Additional resources

- Well-known DID configuration: `https://identity.foundation/well-known-did-configuration/resources/did-configuration/`
- Microsoft Entra Verified ID Pricing: `https://azure.microsoft.com/en-us/pricing/details/microsoft-entra-verified-id/`
- Azure AI Vision Face API: `https://learn.microsoft.com/en-us/azure/ai-services/computer-vision/overview-identity`
- Microsoft Security Store: `https://learn.microsoft.com/en-us/security/store/what-is-security-store`
- W3C Bitstring Status List: `https://github.com/w3c/vc-bitstring-status-list/tree/343b8b59cddba4525e1ef355356ae760fc75904e`
- Rules and display definition reference: `https://learn.microsoft.com/en-us/entra/verified-id/rules-and-display-definitions-model`

Join us on Discord

For discussions around the book and to connect with your peers, join us on Discord at `packt.link/discordcloud` or scan the QR code below:



11

Microsoft Entra Workload ID

Each object that interacts with Microsoft Entra ID has an identity. Each user, device, application, service, script, or container has an identity that identifies it uniquely in the directory. This identity is used to authenticate to the directory and access other services and resources. The terminology used for these identities varies across the industry. In Microsoft Entra, a Workload ID refers to a digital identity that represents a non-human entity, such as an application, service, script, or automation running in your environment. Unlike traditional user accounts, which are tied to individual people, Workload IDs are created for resources and workloads that need to authenticate and access resources programmatically. These identities help organizations securely manage and control how their applications and automated processes interact with other resources within Microsoft Entra, Azure, and integrated services.

Microsoft Entra Workload ID makes it easier to automate processes and maintain strong security practices. It supports auditing, monitoring, and compliance efforts, as every action taken by a workload is tracked and can be reviewed. This is particularly important in complex cloud environments where automation and scalability are key.

In this chapter, we will cover

- Applications in Microsoft Entra
- Managed identities in Azure
- Introduction to workload identities
- Workload identity federation
- Security for workload identities

Applications in Microsoft Entra

Most applications require users to authenticate to be able to access them. Application developers often don't want to store and manage user credentials in the application as this

introduces a lot of administrative overhead and security concerns. They would rather want to delegate the identity and access management functions to an **Identity Provider (IdP)** like Microsoft Entra ID.

There are several ways to use applications in Microsoft Entra. Before learning about workload identities, it is important to understand the application types and their behavior.

In **Microsoft Entra App Gallery**, there are SaaS applications that can be added for use in your tenant. These are applications like Box, Salesforce, ServiceNow etc. These applications are published in the application owner's tenant like Box or Salesforce. This is the application's *home* tenant. They can be *added* to your tenant for use by users in your organization. This can be done in the Microsoft Entra admin center by navigating to **Entra ID | Enterprise apps | New application**.

In addition, you can also *register* an application that your organization is developing. These are your line-of-business (LOB) applications. This can be done in the Microsoft Entra admin center by navigating to **Entra ID | App registration | New application**.

Lastly, users or admins consume multi-tenant apps which are apps registered in another tenant. When a user or admin consents to an application, it is an example of consuming a multi-tenant app.

Each of these behaves differently with Microsoft Entra. The following table summarizes these scenarios:

Scenario	**What you do**	**What gets created in your tenant**	**Where it shows up**	**Who owns the app**
Register an app	Go to App registrations and create an app	Application object + service principal object	App registrations + Enterprise applications	Your tenant
Add a gallery app	Go to Enterprise apps and add a gallery app	Tenant local application object + service principal object	App registrations + Enterprise applications	App publisher's tenant

Scenario	What you do	What gets created in your tenant	Where it shows up	Who owns the app
Consume a multi-tenant app	A user/admin consents to use an app published in another tenant	Service principal object	Enterprise apps	App publisher's tenant

Table 11.1: Applications in Microsoft Entra

Understanding these concepts is key to understanding the later concepts in this chapter.

Managed identities for Azure resources

Applications use a variety of secrets like credentials, certificates, and keys. Developers often face challenges with secure handling of these secrets. Manually managing these secrets in the application is prone to errors and security issues. This is where managed identities help. A managed identity is defined as an identity assigned to Azure resources like Azure Virtual Machines, Service Fabric Clusters, Azure Kubernetes clusters, or any app hosting platform supported by Azure. Once a managed identity is assigned to a compute resource, it can be authorized to access other Azure resources like storage accounts, SQL databases and more. Managed identities replace secrets like access keys, passwords, certificates, and other forms of service-to-service authentication dependencies.

Using managed identities eliminates the need to manage credentials. They can be used to authenticate any resource that supports Microsoft Entra authentication.

Managed identities are of two types.

- **System-assigned**: Some Azure resources enable the creation of managed identities directly from the resource. When a system-assigned managed identity is enabled, a service principal representing the managed identity is created in Microsoft Entra. It is tied to the resource and if the Azure resource is deleted, the service principal is also deleted.
- **User-assigned**: A user-assigned identity is an independent identity that can be assigned to Azure resources if they don't support system-assigned managed identity. When a user-assigned managed identity is created, a service principal representing it is created in Microsoft Entra. This service principal is not tied to the Azure resource and

must be managed separately. These can be used in workload identity federation scenarios.

Introduction to workload identities

There are two main types of identities – **human** or **non-human/machine identities**. Human identities are the ones that are assigned to individuals like employees, vendors, business partners, or customers. Non-human/machine identities consist of **workload identities** and **device identities**. Device identities represent devices like computers, mobile devices or IoT devices. Workload identities are assigned to software like an application or service. In Microsoft Entra, workload identities refer to **applications**, **service principals** and **managed identities**. Let's understand each one in detail.

Applications and service principals

Using applications in Microsoft Entra as described in *Table 11.1* creates an identity configuration for the application that allows it to use Microsoft Entra ID as its IdP. Once the application is added or registered with Microsoft Entra ID, a globally unique instance of the application is created in the tenant. This instance has an **App/Client ID** that is globally unique. Secrets and certificates can be added to make the application work. Registering or adding an application creates an **application object** and a **service principal object** in the tenant.

Application object

Each application in Microsoft Entra is defined by its unique application object that is created when the application is registered or added to the tenant. These application objects can be viewed in the Microsoft Entra admin center by navigating to **Entra ID | App registrations | All applications** as shown in the following screenshot.

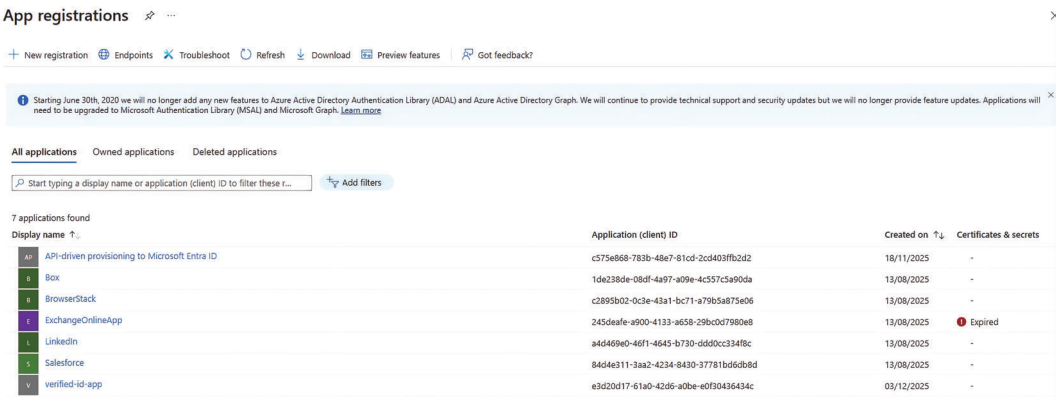


Figure 11.1: Application objects

The application object describes how the IdP issues tokens for application access, the resources that need access to the application and the actions that the application can take.

Service principal object

To access resources secured by Microsoft Entra, the entity requiring access must be represented by a **security principal**. Users are represented by **user principal** and applications are represented by **service principals**. These security principals define the access and permissions that users and applications have in the Microsoft Entra tenant. This enables authentication and authorization for the users or applications when they attempt to access resources. There are three types of service principal:

- **Applications**: These are local representations or instances of global applications in your tenant. It is created from an application object and inherits certain properties from the application object. A service principal is created in each tenant where the application is used and defines what the application can do in that tenant, who can access the application and the resources that the application can access.
- **Managed identity**: This type of service principal represents a managed identity in Azure. When a managed identity is enabled in Azure, a managed identity service principal object is created in Microsoft Entra. These service principals can be granted access and permissions, but they cannot be updated or modified. Unlike application service principals, they do not have an application object associated with them.
- **Legacy**: These are service principals that were created before app registrations were introduced or when an app is created using legacy methods. They can have credentials, service principal names, reply URLs, and other properties. They don't have an associated app registration. Legacy service principals can only be used in the tenant where they were created.

You can view the service principal objects in the Microsoft Entra admin center by navigating to **Entra ID** | **Enterprise apps** | **All applications** as shown in the following screenshot:

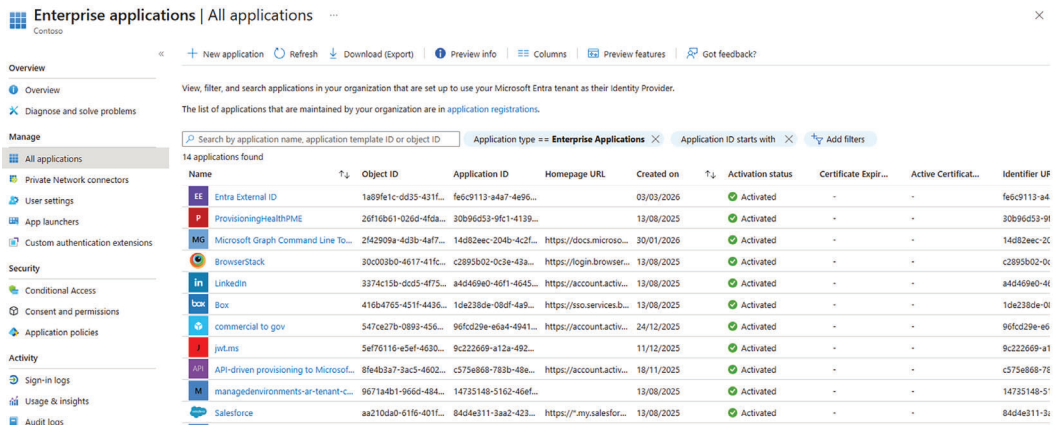


Figure 11.2: Service principal objects

To summarize, an application object is a global representation or master copy of the application and can be viewed under App registrations (*Figure 11.1*). It defines what the application is (its identity, permissions, endpoints, and configuration). A service principal object is the local representation of the application and can be viewed under Enterprise apps (*Figure 11.2*). It defines how the app runs in your tenant (assignments, policies, access control).

Each software application is represented by a single application object in the tenant. An application object can have multiple service principals associated with it as a service principal must be created in each tenant where the application is used.

In the world of AI, an increasing number of services rely on non-human identities to complete tasks. The number of non-human identities is increasing dramatically. Adversaries are targeting these non-human identities, putting applications and the organization's resources at risk. Unlike human identities, non-human identities often lack a formal lifecycle or governance process. It is difficult to track the creation of these identities, making it difficult to govern them and decide when to revoke them. Most identity and access management solutions focus on protecting human identities. Microsoft Entra Workload ID helps address the same concerns for workload identities.

Using Microsoft Entra Workload ID, organizations can

- Bring service principals under the purview of **Conditional Access policies**.
- Enforce Conditional Access location and risk policies using **Continuous Access Evaluation**.
- Detect threats and reduce risk to workload identities by using **Microsoft Entra ID Protection**.

- Use **managed identities** to access Microsoft Entra protected resources without needing to manage secrets for resources that run on Azure.
- Use **workload identity federation** to access Microsoft Entra protected resources in scenarios like GitHub Actions, workloads running on Kubernetes and on non-Azure platforms without needing to manage secrets.
- Use **access review for service principals** to manage service principals and applications that are assigned privileged directory roles in Microsoft Entra ID. Access reviews are explained in detail in *Chapter 6, Microsoft Entra Entitlement Management*.

Let's explore each of these capabilities in detail.

Workload identity federation

Software applications need an identity for authentication and to access and communicate with other resources. If these workloads are running on Azure, you can use managed identities to manage the secrets and provide secure access to Microsoft Entra resources. Workloads running in Kubernetes or non-Azure platforms use application credentials like client secrets or certificates to authenticate to and access Microsoft Entra resources. These application credentials pose a security risk and must be stored securely and properly protected. They should also be regularly rotated. If expired, they can also cause application downtime.

Workload identity federation enables such workloads to securely access Microsoft Entra resources without having to manage secrets. This can be done by configuring a **user-assigned managed identity** or using **app registration** in Microsoft Entra ID, which creates a trust between Entra ID and an external IdP like GitHub or Google. For applications, this is done by configuring **federated identity credentials (FIC)**. Once this trust relationship is established, the external software workload sends trusted tokens from the external IdP to the Microsoft identity platform and receives an access token in return. The access token is then used by the software to access Microsoft Entra resources. There is a limit of 20 federated identity credentials per application object or user-assigned identity.

The following figure explains how workload identity federation works.

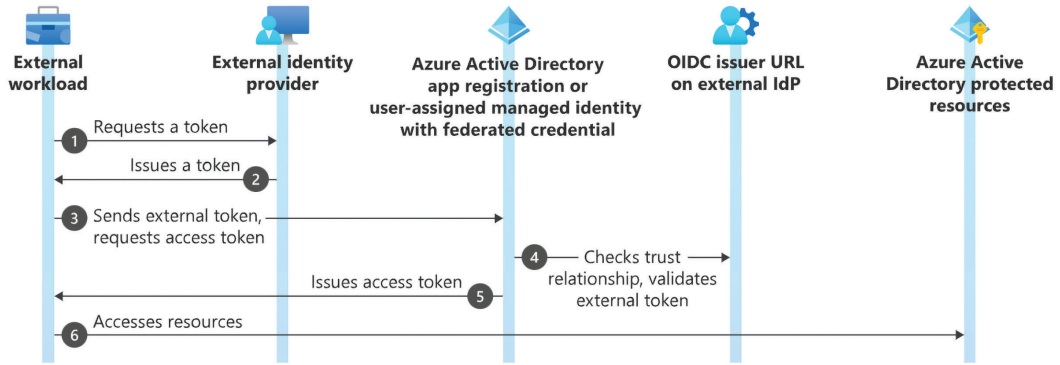


Figure 11.3: Workload identity federation

Using workload identity federation, workloads running on any Kubernetes cluster, Amazon Web Services (AWS), or other cloud platform, GitHub Actions, Google Cloud, and more can securely access resources protected by Microsoft Entra without having to manage secrets.

A federated identity credential is made up of the following:

- **audiences**: This is the audience that appears in the token
- **issuer**: This is the URL of the external IdP
- **subject**: This is the identifier of the software workload in the external IdP
- **name**: This is a string that uniquely identifies the credential

The **issuer** and **subject** combination must be unique for the app. When the external software workload requests the Microsoft identity platform for an access token in exchange for the external token, the Microsoft identity platform checks the **issuer** and **subject** values of the federated identity credential against the `issuer` and `subject` claims in the external token. If the values match, an access token is issued.

Currently federated identity credentials require explicit matching when comparing `subject`, `issuer` and `audience` in the federated identity credential to `subject`, `issuer` and `audience` claims in the external token sent to Microsoft Entra ID. Considering that only 20 federated identity credentials can be created for a single application or user-assigned identity, this can lead to scaling issues. For applications, **flexible federated identity credentials** extend the capabilities of the existing federated identity credentials by allowing the use of a restricted expression language for matching the incoming `subject` claims. They also enable including custom claims, thereby extending the federated identity credential model beyond the `subject`, `issuer` and `audience` claims. This enables multiple federated identity credentials to be managed under a single flexible federated identity credential. These include scenarios like

GitHub repositories with multiple workflows running on a different branch, certain Terraform cloud and reusable GitHub Actions workflows.

> **Note**
>
> At the time of this writing, flexible federated identity credentials are in Public Preview.

Configuring federated identity credentials

To configure a federated identity credential, you must be the owner of the application or have one of the following Entra roles: **Application Administrator**, **Cloud Application Administrator**, **Global Administrator** or **Hybrid Identity Administrator**.

The following are the steps to configure a federated identity credential:

1. Create an app registration or managed identity in Microsoft Entra. Grant the app access to the Azure resources required by the external software workload.
2. From the **App registration** blade in the Microsoft Entra admin center, find and record the **Object ID** of your app registration.
3. From the external software workload, obtain the *subject* and *issuer* information.
4. Log in to `https://entra.microsoft.com` and navigate to **Entra ID** | **App registrations**.
5. Select the app registration created in step 1 and click on **Certificates & secrets**.
6. In the right pane, click on **Federated credentials**, then click **Add credential**.
7. From the **Federated credential scenario** drop-down, select the scenario for which you are adding the credential. Refer to the following screenshot:

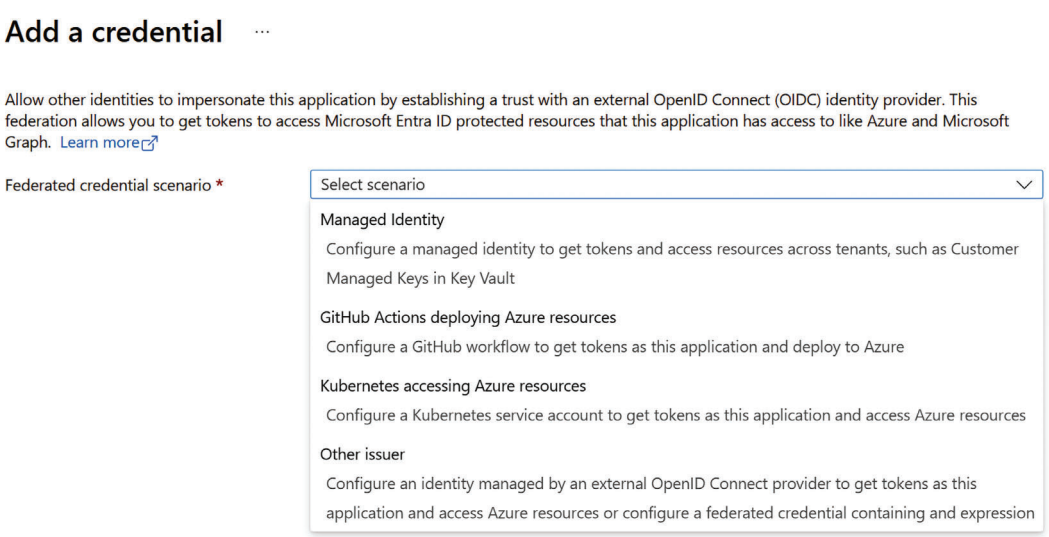


Figure 11.4: Selecting the federated credential scenario

8. The next steps differ depending on the selection made in step 7. You will have to provide the *subject* and *issuer* information obtained in the steps above. If you would like to configure flexible federated identity credentials for your application, select **Other issuer** in the drop down above. Once complete, click **Add** to add the credential.

Securing workload identities

As can be understood by now, workload identities differ from user identities in that they often do not have a proper lifecycle. They also need to store their secrets somewhere and cannot perform multifactor authentication. These differences make workload identities more susceptible to compromise and harder to protect.

Microsoft Entra ID Protection can be used to provide detection, investigation, and remediation services for applications and service principals. The following risk detections are available for workload identities.

- **Microsoft Entra threat intelligence**: This detection indicates some activity that is consistent with known attack patterns.
- **Suspicious sign-ins**: Detects sign-in properties that are unusual for the service principal. It learns and baselines behavior over 2 and 60 days and then generates an alert if unfamiliar properties like IP address, user agent, IP country are detected at subsequent sign-ins.

- **Admin confirmed service principal compromised**: This indicates that an administrator has marked the service principal as compromised in the Microsoft Entra admin portal.
- **Leaked credentials**: This indicates if the service principal's valid credentials are found on the dark web, GitHub or other sources.
- **Malicious applications**: This detection combines signals from Microsoft Defender for Cloud Apps to identify if the application was malicious and has been disabled by Microsoft.
- **Suspicious applications**: This indicates that an application has violated Microsoft's terms of service, but it has not been disabled. Microsoft recommends performing a thorough review of such applications.
- **Anomalous service principal activity**: This detection type baselines normal behavior of the service principal and alerts when it spots anomalous behavior.
- **Suspicious API traffic**: This detects when abnormal GraphAPI or directory enumeration of a service principal takes place. This might indicate abnormal reconnaissance or data exfiltration activity.

To identify risky workload identities, navigate to **ID Protection | Risky workload identities** in the Microsoft Entra admin center. Administrators must be assigned either the **Security Administrator**, **Security Operator** or **Security Reader** role to be able to access these reports. Investigate each workload identity and based on the analysis administrators can either **Confirm service principal(s) compromised** or **Dismiss service principal(s) risk** as shown in the following screenshot.

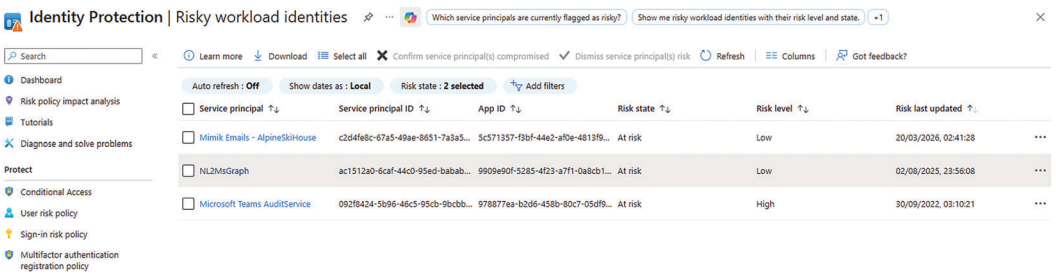


Figure 11.5: Risky workload identities

Securing workload identities is an important part of protecting your identity environment.

Conditional Access for workload identities

Historically, Conditional Access policies could be applied to only user accounts. However, the current surge in attacks on non-human identities requires that this capability be extended to

workload identities as well. Conditional Access for workload identities enables blocking service principals from accessing Microsoft Entra from outside of known IP ranges. Service principals can also be blocked based on their detected risk levels in Microsoft Entra ID Protection. These can be combined with Conditional Access authentication contexts.

This capability requires that the organization has a **Microsoft Entra Workload ID Premium** license.

Following are the steps to create a location-based policy for workload identities.

1. Sign in to `https://entra.microsoft.com` as a **Conditional Access administrator**.
2. Navigate to **Entra ID | Conditional Access**.
3. In the right pane, click on **Create new policy** and give the policy a meaningful name.
4. Under **Users, agents or workload identities**, select **Workload identities** from the drop-down box.
5. Click on **Select service principals** and select the service principal. Managed identities are not covered by Conditional Access policies.
6. Under **Target resources** select **All resources (formerly 'All cloud apps')**. This policy is only applied when a service principal requests a token. Policies can only be applied to single-tenant service principals that are registered in your tenant. Multi-tenant and SaaS apps cannot be included.
7. Select **Network** and change the **Configure** toggle to **Yes** and select **Any network or location**.
8. Click on **Exclude** and select **All trusted network and locations**.
9. Click on **Grant** and choose **Block access**. Access will be blocked when a token is requested by the service principal from outside the trusted network and locations.

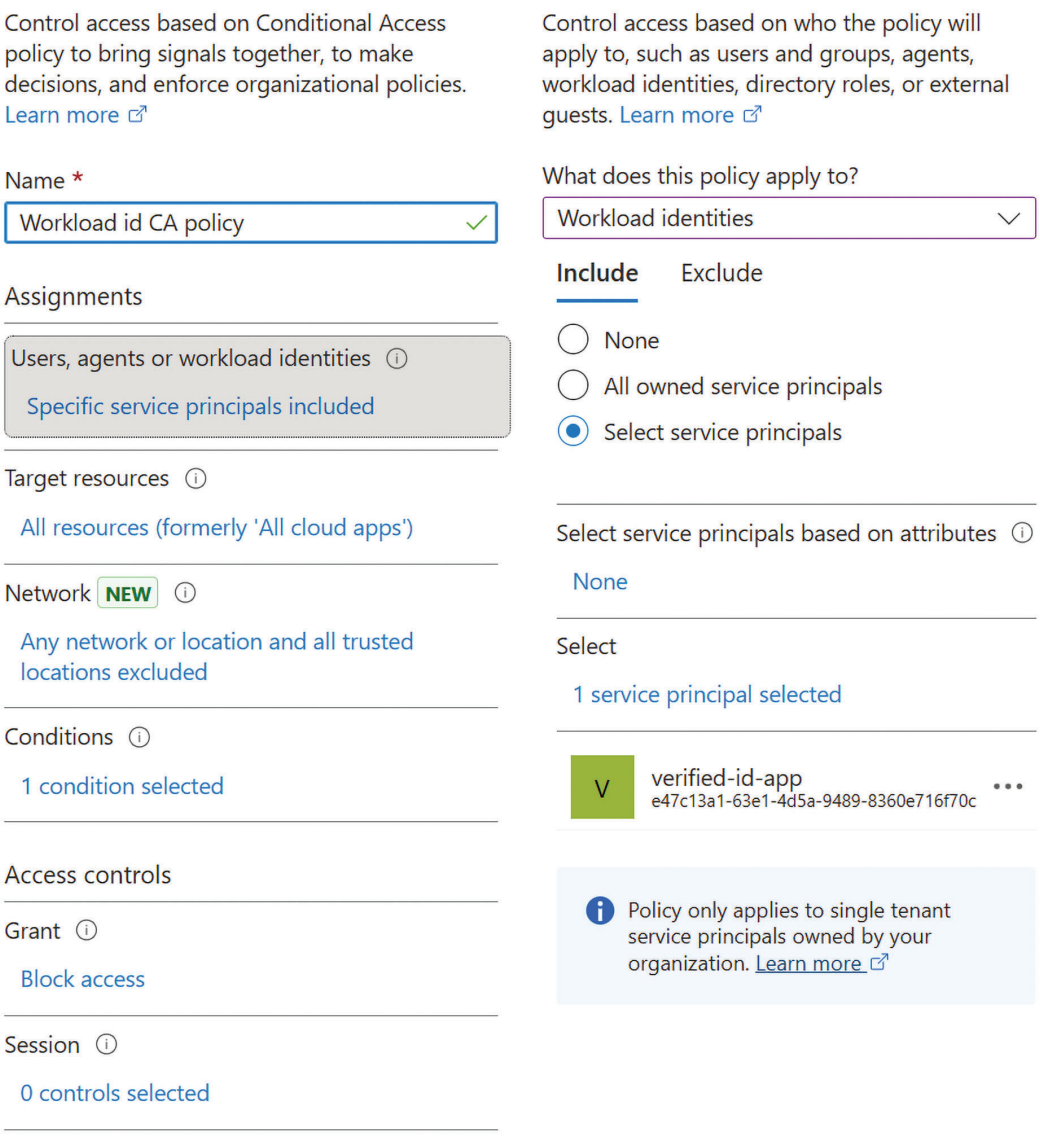


Figure 11.6: Location-based CA policy for workload identities

10. Switch the **Enable policy** toggle to **On** and click **Save**.

To create a conditional access policy that is applied to risky service principals, while creating a Conditional Access policy, under **Conditions**, select **Service principal risk** and select the appropriate risk level as shown in the following figure.

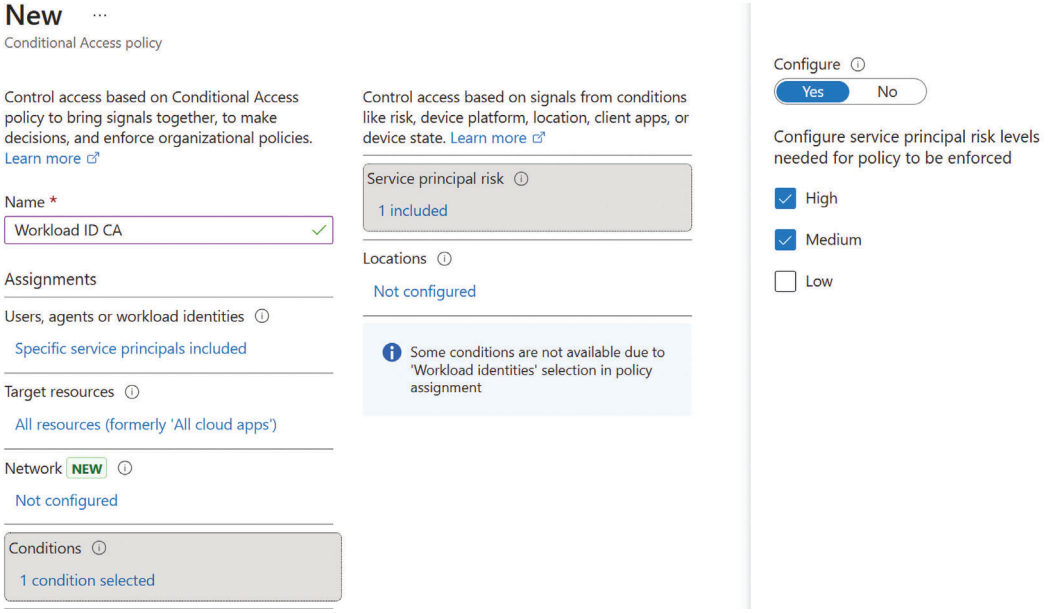


Figure 11.7: Risk-based policy for workload identities

Access will now be blocked for service principals whose risk level detected by Microsoft Entra ID Protection is either medium or high.

Note

If service principals are added to groups and those groups are used in the scope of Conditional Access policies, the policy will not apply to the service principal in the group. Service principals should be assigned directly to the policy.

Sign-in logs can be used to review how policies are being enforced for service principals. The following are the steps:

1. Sign in to `https://entra.microsoft.com` as a **Security Reader**
2. Navigate to **Entra ID | Monitoring & health | Sign-in Logs | Service principal sign-ins**.
3. Select a log entry and click on Conditional access.

If a sign-in has been blocked by a Conditional Access policy, "*Access has been blocked due to Conditional Access policies.*" will be stated as the failure reason.

Continuous Access Evaluation for workload identities

Continuous Access Evaluation (**CAE**) for workload identities improves security by enforcing Conditional Access location and risk policies in real time and instantly revokes the token if risk is identified. The following points must be kept in mind while using CAE for workload identities.

- CAE for workload identities is only supported on access requests sent to Microsoft Graph as the resource provider.
- Service principals for line-of-business applications are supported.

Revocation events supported are:

- Disable a service principal
- Delete a service principal
- High service principal risk

Developers need to enable their application to opt in to CAE for workload identities. This can be done by declaring the `cp1` client capability in their API call when requesting tokens.

When CAE is triggered and a client's session is revoked, the client must reauthenticate. This behavior can be verified from the sign-in logs.

Best practices

Following are some best practices for working with Microsoft Entra Workload ID.

- Use managed identities wherever possible to avoid storing secrets.
- Prefer workload identity federation to eliminate long-lived credentials.
- Enforce least-privilege access using Privileged Identity Management for workload roles.
- Review permissions regularly. Use Microsoft Entra Access Reviews for App roles and service principals.
- Use Microsoft Entra Recommendations to identify expiring client secrets and rotate them before expiry to prevent application outages.
- Automate provisioning and deprovisioning to maintain lifecycle hygiene.
- Apply Conditional Access policies tailored for workload identities.
- Continuously monitor sign-ins, audit logs, and permission changes.

- Use Microsoft Entra Recommendations to identify and remove unused apps, roles, and service principals to reduce attack surface.
- Integrate workload identities into your Zero Trust strategy.

Following these best practices helps maintain a healthy application environment.

Licensing

There are two options to buy Microsoft Entra Workload ID.

- **Free**: Microsoft Entra Workload ID is included with a subscription to services like Azure. It includes basic features like authentication and authorization of workload identities, managed identities and application lifecycle policies.
- **Microsoft Entra Workload ID Premium**: This includes all the features included in the Free tier in addition to advanced features like access reviews, app health recommendations, Conditional Access and ID Protection for workload identities. Microsoft Entra Workload ID Premium is a per workload identity per month license.

Organizations need to license only the workload identities that are using the premium features.

Summary

This chapter covered the concepts of human and non-human identities, as well as workload identities within Microsoft Entra. It detailed the distinctions between applications and service principal objects and described how Microsoft Entra manages application identities and managed identities for Azure resources. Additionally, it addressed workload identity federation, demonstrating how this approach enables applications to access resources protected by Microsoft Entra ID without the need to manage secrets. The chapter also outlined methods for securing workload identities, including Microsoft Entra ID Protection, Conditional Access policies, and Continuous Access Evaluation. It concluded with a discussion of best practices for managing workload identities.

Exercises

1. What is the primary benefit of using workload identity federation in Microsoft Entra?
    a. It enables workloads to bypass Conditional Access policies.
    b. It replaces the need for service principals entirely.
    c. It automatically assigns Global Administrator permissions to workloads.
    d. It allows workloads to authenticate without storing long-lived credentials.

2. Which Entra feature helps identify unused workload identities and stale permissions?
    a. Entra recommendations
    b. Identity Protection risk policies
    c. Conditional Access templates
    d. Privileged Identity Management alerts
3. Which Entra feature helps reduce credential exposure for automated workloads running in Azure?
    a. Long-lived certificates in Key Vault
    b. Unrestricted app role assignments
    c. Client secrets stored in application code
    d. Managed identities for Azure resources

Answers

1. d
2. a
3. d

Additional resources

- Managed identities: `https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/overview`
- Microsoft Entra recommendations:`https://learn.microsoft.com/en-us/entra/identity/monitoring-health/overview-recommendations`
- Frequently asked questions: `https://learn.microsoft.com/en-us/entra/workload-id/workload-identities-faqs`

Get this book's PDF version and more

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.



UNLOCK NOW

Note: Keep your invoice handy. Purchases made directly from Packt don't require an invoice.

Part 4

Extending Identity and Access beyond the Organization

Part 4 explores how Microsoft Entra extends identity and access beyond traditional organizational boundaries. This section begins with External Identities, enabling secure collaboration with partners, contractors, and customers while maintaining strong governance and user experience controls. It then examines Global Secure Access, Microsoft's modern Security Service Edge (SSE) platform that applies Zero Trust principles to network access, ensuring users and devices connect securely from anywhere. Together, these chapters illustrate how Microsoft Entra unifies identity and network trust, allowing organizations to safely expand their digital perimeter while preserving consistent security, policy enforcement, and seamless access across diverse external scenarios.

This part of the book includes the following chapters:

- *Chapter 12*, *External Identities in Workforce Tenants*
- *Chapter 13*, *External Identities in External Tenants*
- *Chapter 14*, *Microsoft Entra Internet Access*
- *Chapter 15*, *Microsoft Entra Private Access*

12

External Identities in Workforce Tenants

In today's interconnected world, organizations cannot operate in silos. They need to collaborate with external entities like contractors, partners, vendors, and consumers. External identities refer to these users or entities outside an organization's core workforce who require access to the organization's resources, systems, or applications. These may include partners, suppliers, contractors, customers, or external consultants. Managing external identities efficiently is crucial for maintaining security and collaboration while ensuring that only the right individuals are granted the appropriate level of access.

External identities can be managed using Microsoft Entra. It supports **business-to-business (B2B)** collaboration, which allows external users to authenticate using their home credentials, reducing the administrative overhead of creating and maintaining separate accounts. Microsoft Entra also offers a **Consumer Identity and Access Management (CIAM)** solution, which is used to manage consumer identities. Conditional Access policies can be applied to external identities, ensuring that access is granted only under specific conditions, such as from trusted locations or devices.

Monitoring and auditing tools are also essential, providing visibility into how external identities interact with organizational resources and enabling timely responses to suspicious activity. A robust strategy for managing external identities balances security, compliance, and productivity.

This chapter will cover

- Introduction to Microsoft Entra External ID
- External ID in the workforce tenant

- Identity providers
- Governance and ID Protection

Introduction to Microsoft Entra External ID

Microsoft Entra External ID is a comprehensive identity management solution designed to help organizations securely collaborate and interact with users outside their immediate workforce. As businesses increasingly operate in a global, interconnected environment, the need to seamlessly engage partners, suppliers, contractors, and customers without compromising security has become paramount. Microsoft Entra External ID addresses this challenge by providing a unified platform for managing external identities, streamlining access, and enforcing robust security policies.

At its core, Microsoft Entra External ID enables organizations to extend their digital ecosystem beyond traditional boundaries. By leveraging B2B collaboration features, external users can access resources using their own existing credentials from their home organizations or even social identity providers. This federated approach reduces the administrative burden of maintaining separate accounts for every external user and enhances the user experience by allowing individuals to use familiar sign-in methods.

A key advantage of Entra External ID is its support for CIAM. This functionality is particularly valuable for organizations with customer-facing applications or services. CIAM allows businesses to create secure, branded sign-up and sign-in experiences for customers, enabling them to register with email addresses or social accounts. Organizations can customize the user journey, including MFA and consent management, all while maintaining compliance with data protection regulations.

Security is central to the design of Microsoft Entra External ID. Organizations can apply Conditional Access policies specifically tailored to external identities. These policies ensure that access to sensitive resources is granted only under predefined conditions, such as from trusted networks, compliant devices, or after satisfying MFA requirements. For example, a contractor working remotely might be required to authenticate using MFA and access certain systems only from approved locations. These granular controls help mitigate risks associated with external access while still enabling productivity.

Another critical aspect of managing external identities is governance. Microsoft Entra External ID provides comprehensive tools for monitoring, auditing, and managing the lifecycle of external accounts. Administrators can track how external users interact with organizational resources, identify suspicious activities, and enforce timely removal of access when a partnership or contract ends. Automated workflows and access reviews streamline the process

of ensuring that only authorized individuals retain access, reducing the risk of lingering or orphaned accounts.

Entra External ID also supports cross-tenant access settings, allowing organizations to define which external tenants can collaborate with their users and which resources are accessible. This feature is particularly useful in scenarios where regulatory compliance or internal policies mandate strict boundaries between different business units or external partners. By enforcing these restrictions, organizations can prevent data leakage and maintain greater control over their digital assets.

Integration with other Microsoft Entra features, such as identity protection and continuous access evaluation, further enhances the security posture. These capabilities enable real-time risk assessment and dynamic policy enforcement, adapting to changing threat landscapes and user behaviors. For example, if an external user's account is compromised, Entra can automatically trigger additional verification steps or block access until the risk is resolved.

Microsoft Entra External ID primarily caters to the following two scenarios:

- **Business-to-consumer**: This is for organizations developing consumer-facing applications like an online grocery store, website for booking air tickets or government departments offering citizen-facing services. These types of applications can use Entra External ID in *external* configuration. This is a separate tenant from the one that contains the organization's employees.
- **Business-to-business**: This is for organizations that need to collaborate with other businesses like partners, vendors, suppliers, etc. They can use Entra External ID in *workforce* configuration which is the same tenant that contains the organization's employees.

Most organizations have both business-to-business and business-to-consumer requirements, and you will find that they have both *external* and *workforce* tenant configurations in Microsoft Entra.

Before moving on, let's learn a little more about external and workforce tenant configurations.

A *tenant* in Microsoft Entra is a directory that contains the organization's employees and resources like applications and devices. In Microsoft Entra, a tenant can be configured in two ways depending on the use case.

- **Workforce tenant**: A workforce tenant is the standard configuration in Microsoft Entra. It contains the organization's employees, business applications, devices, and other resources. In a workforce tenant, the users are the organization's employees.

These employees can collaborate with external entities like business partners, suppliers, and contractors using B2B collaboration.

- **External tenant**: An external tenant is a separate directory that is used exclusively for storing user accounts and applications that are used by an organization's consumers. This is Microsoft's **CIAM** solution and caters to the **business-to-consumer (B2C)** use cases.

The following table highlights the key differences between workforce and external tenants:

Feature	External ID in workforce tenant	External ID in external tenant
Scenario	Allow organization's employees to collaborate with business partners, contractors, vendors and suppliers. Provide access to M365 applications like Teams, SharePoint and line-of-business applications. Example: Share a marketing campaign on SharePoint online with an external marketing agency.	Publish consumer facing applications to the organization's consumers. Example: An e-commerce website where consumers can log in and shop for goods.
Intended for	Collaboration with business partners, contractors, vendors and suppliers.	Providing applications to consumers for business.
User management	B2B users are managed in the workforce tenant. Their user type is *Guest*. They can be subject to the same ID Governance features as employees. Local accounts are created only for the organization's employees.	Users are managed and maintained in the external tenant separate from the organization's employees. Consumers can either bring their own identities or create a local account using the sign-up process.
SSO	Guest users can get SSO to all Microsoft Entra connected apps like M365, Salesforce or on-prem apps.	SSO can be provided to all apps registered in the external tenant. SSO to M365 is not supported.
ID Governance	Supported	Not supported

Feature	External ID in workforce tenant	External ID in external tenant
ID Protection	Supported	Not Supported
Pricing	Pricing is based on **Monthly Active Users (MAU)** for users whose user type is Guest.	Pricing is based on **Monthly Active Users (MAU)** for all users in the external tenant regardless of the user type.

Table 12.1: Workforce tenant vs external tenant

Tip

An active user is a user who signs in at least once a month. Even if the user signs in multiple times in a month, they are still considered one MAU.

The following picture shows a graphical representation of the external and workforce tenants.

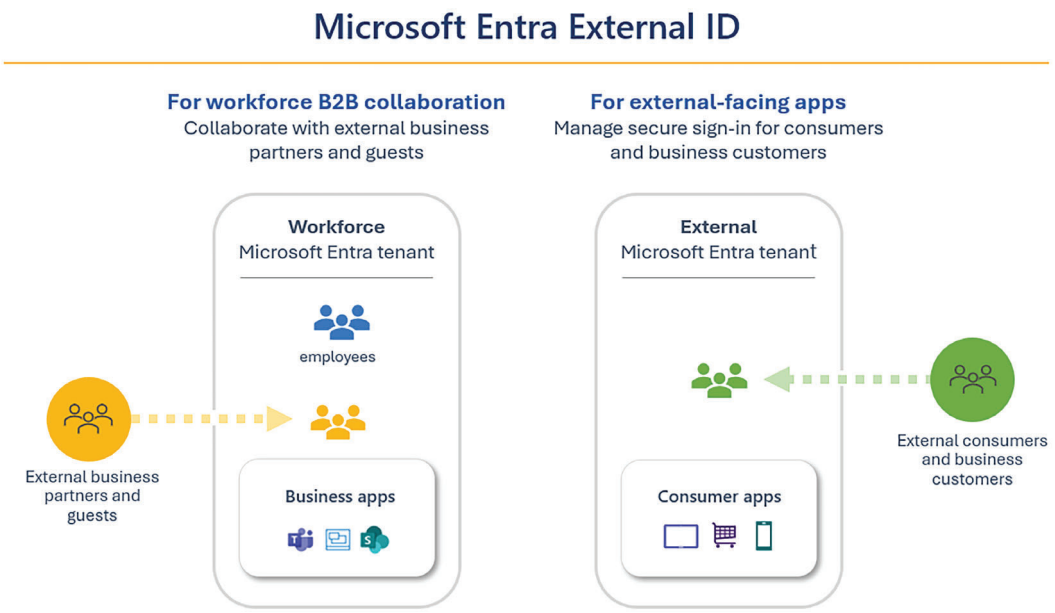


Figure 12.1: Workforce tenant and external tenant

Depending on the organization's needs, it can have one or both of the tenant configurations in Microsoft Entra ID.

Tip

It is important to understand the difference between External ID in the workforce tenant and External ID in the external tenant. Ensure that you are clear on the distinction before moving forward.

External ID in the workforce tenant

Microsoft Entra External ID offers B2B collaboration features to allow employees to work seamlessly and securely with external entities like business partners, contractors, vendors, and suppliers. Using Microsoft Entra External ID organizations can enable this collaboration while still maintaining control over their tenant and corporate data. The external entities do not need to have Microsoft Entra or even an IT department.

External users can be invited to collaborate using a simple invitation process or by configuring an application that enables self-service sign-up. They can use their own identities regardless of whether they have Microsoft Entra or not.

The following types of B2B collaboration users can exist in Entra ID depending on how they authenticate:

- **External guest**: Most external users and guests fall in this category. These users have an account in another Microsoft Entra directory or another IdP and authenticate to it. They have guest-level permissions in your tenant. The user type of these users is *Guest*. They are billed based on MAU.
- **External member**: These are external users and guests who have an account in another Microsoft Entra directory or another IdP and authenticate to it. These users have member level access in your tenant. This is a common scenario in conglomerate organizations that have multiple Microsoft Entra tenants. The user type of these users in your tenant is *Member*. Pricing is based on per user licensing in the user's home tenant.
- **Internal guest**: Before B2B collaboration, organizations used to create accounts of external users in their tenant to enable collaboration. These users had the user type set to *Guest,* but they authenticated to your organization. If you have internal guests in your tenant, you can invite them using B2B collaboration so that they can authenticate

to their own IdP and use their own credentials to access resources in your tenant. They are billed based on MAU.

- **Internal member**: These are the employees of your organization. They authenticate to your Microsoft Entra ID tenant. Their user type is *Member*. Pricing is based on per-user licensing in your tenant.

It is possible to change a user type from *Member* to *Guest* and vice versa. However, since this property shows the relationship of the user with your organization, you should do this only if the relationship changes.

Guest users have restricted permissions in your directory. They can manage their own profile and change their password; however, they cannot read all directory information. B2B guest users cannot be added to Microsoft Teams shared channels. Use B2B direct connect for this purpose. B2B direct connect is explained later in this chapter.

It is possible to give guest users higher privileges by adding them to certain privileged roles. Administrators can also remove the guest user restrictions and give guest users the same privileges as members. This is done in the Microsoft Entra admin center by navigating to **Entra ID | Users | User settings** and making the appropriate selection under **Guest user access**. Refer screenshot below.

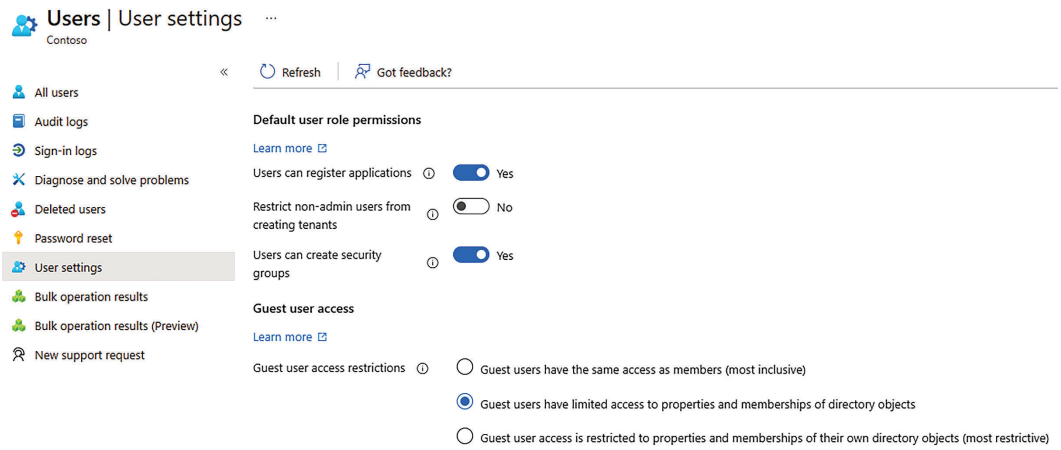


Figure 12.2: Guest user access

Inviting a guest user

Administrators can invite external users to the workforce tenant by following the steps below:

1. Log in to `https://entra.microsoft.com` as a **User Administrator**.
2. Navigate to **Entra ID | Users**.
3. In the right-pane click on **New user | Invite external user**.
4. Enter the user's email address and optionally enter a display name and an invitation message as shown in the following screenshot. Click **Next: Properties**.

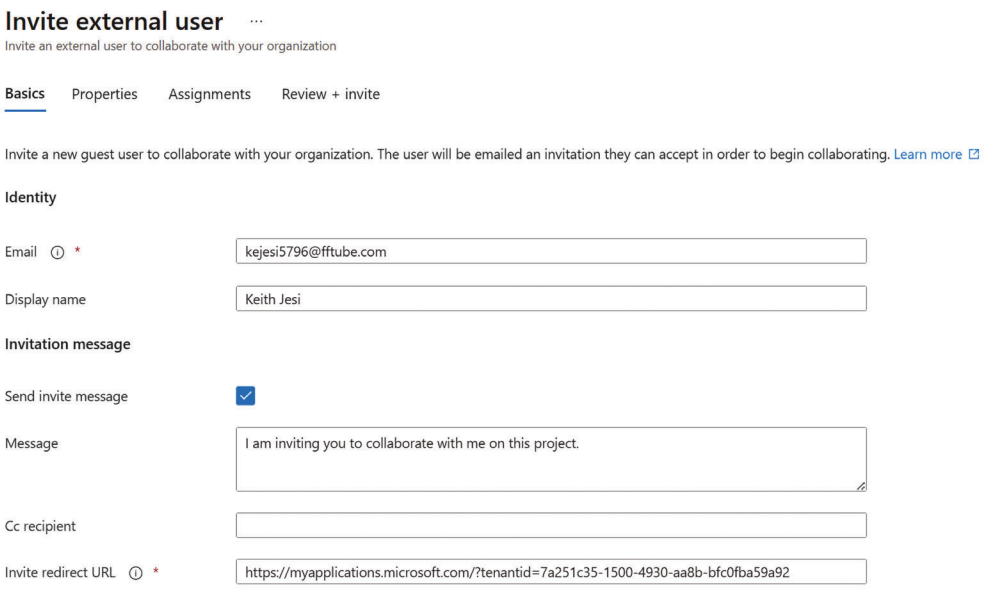


Figure 12.3: External user details

5. On the **Properties** page, enter the user's First name, Last name and other optional details. Review the available options in the screenshot below. Notice that you can add **Sponsors** for guest users. Sponsors are responsible for managing and monitoring the lifecycle of the guest user. Sponsors don't have administrative rights on the user object, but they can be used for approval processes while conducting access reviews. The user who invites the guest automatically becomes the sponsor, unless another sponsor is selected at this stage. Sponsors can also be added after the user has been invited, by editing the user properties. Once done, click **Next: Assignments**.

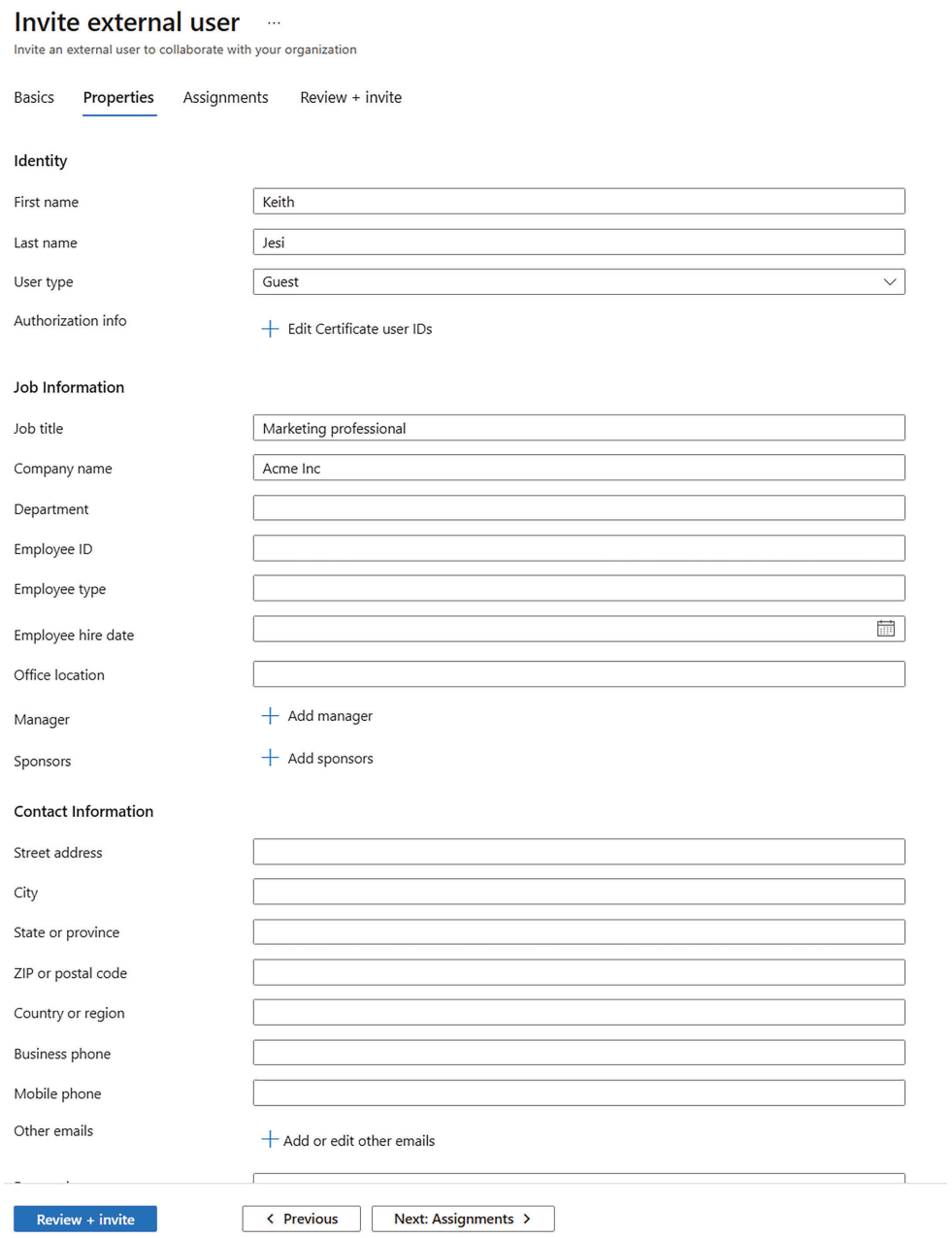


Figure 12.4: Guest user properties

6. On the **Assignments** page, add the user to appropriate groups and roles as required and click **Next: Review + invite**.
7. On the **Review + invite** page, review the settings and click **Invite**.
8. The user will be created in the directory with the **User type** as **Guest** as shown in the following screenshot. Note that the B2B invitation state shows as **Pending acceptance**. You can also **Resend invitation** if required.

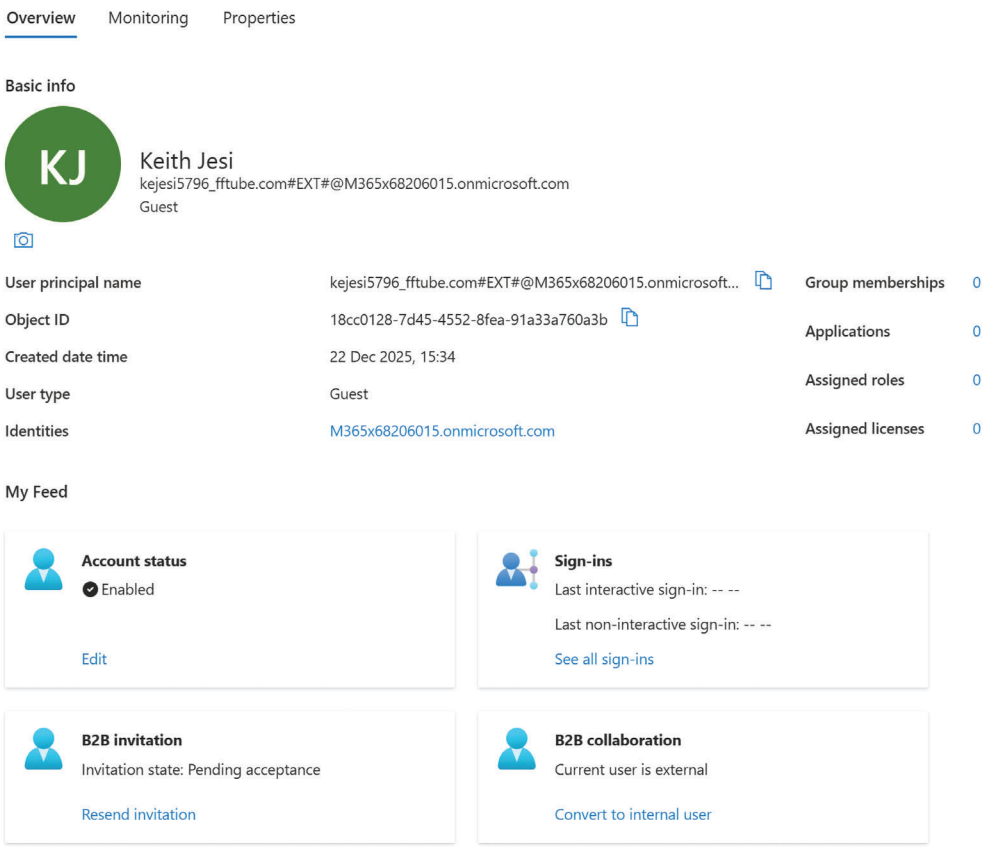


Figure 12.5: Guest user invited

At this stage the guest user will receive an email asking them to accept the invitation as shown in the following screenshot.

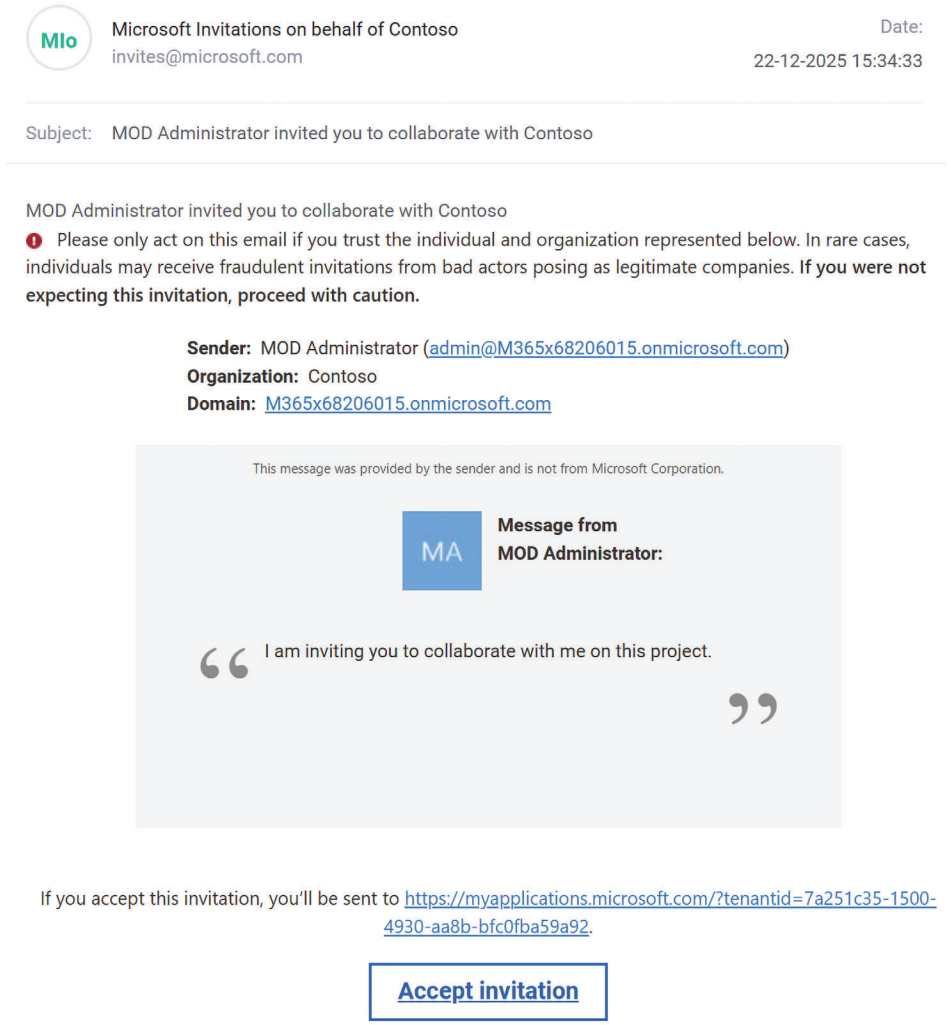


Figure 12.6: Invitation email message

When the user clicks **Accept invitation**, they will receive a **one-time passcode (OTP)** at their email address. This is a default feature for all tenants that have not explicitly turned it off. If turned off, the user will be asked to create a Microsoft Account (MSA).

Once the user enters the OTP, they are asked to consent to permissions requested by the inviting tenant. On clicking **Accept**, they may be asked to register for MFA. They are then redirected to the **My Apps** portal. The B2B invitation state changes to **Accepted**.

Sometimes administrators may need to update the guest user's sign-in information if the guest user wants to sign in using a different email and identity provider or the user moved to another organization but requires the same access in your organization. In scenarios such as these, the guest user's account would have to be deleted and recreated. Microsoft Entra ID now offers the option to reset the redemption status of a guest user. Using this option allows you to reinvite the user while keeping their user object ID, group memberships and app assignments the same. When the user redeems the new invitation, their UPN does not change. Only their sign-in name changes to the new email id. To reset the redemption status, on the user object's **Overview** page click **Reset redemption status** as shown in the following screenshot. You will be asked to confirm your choice, click **Reset**.

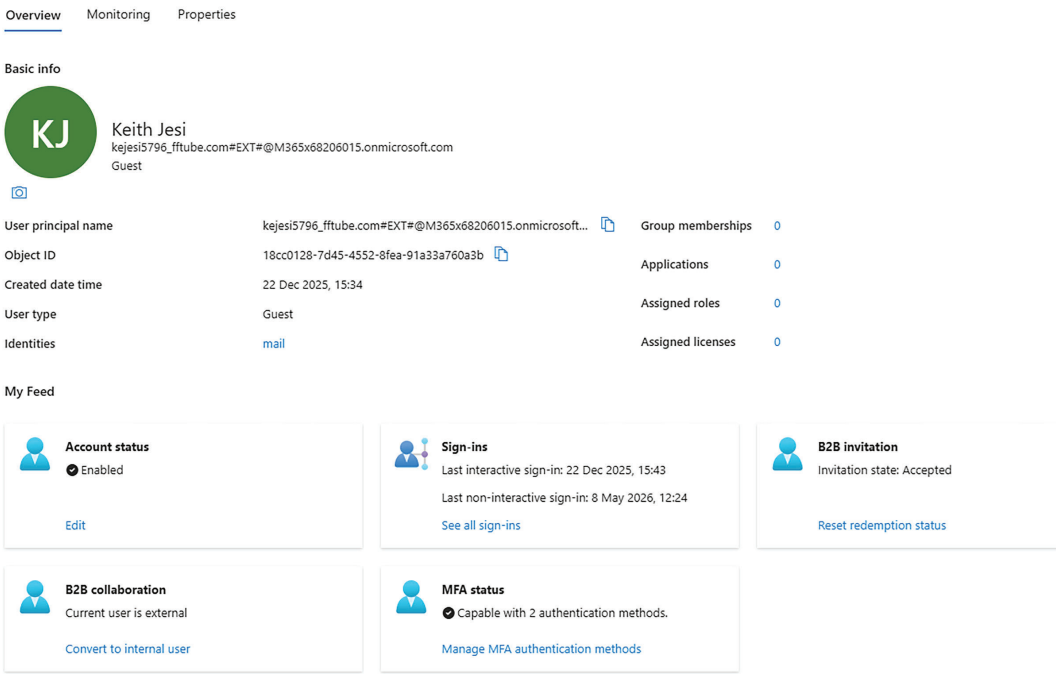


Figure 12.7: Reset redemption status

Members in your tenant can also invite external users as guests. The simple act of adding an external user to a Team or sharing a link from SharePoint or OneDrive will invite the user as a guest in the tenant. By default, all users and guests in a tenant can invite external users. Administrators can control this using external collaboration settings and cross-tenant access settings.

Identity providers

An identity provider (IdP) is a service that authenticates and verifies the identity of users, allowing them to access applications and resources across different systems. Microsoft Entra ID is an IdP that provides such services. When you invite external users to collaborate with your organization, they may already have an identity in another Microsoft Entra tenant, or a Microsoft Account or a social account like Google or Facebook. External ID in the workforce tenant offers collaboration with other IdPs like

- **Other Microsoft Entra accounts**: Invited users can use their own Microsoft Entra accounts from their home tenants to access resources in your tenant. This is enabled by default and if an external user has a Microsoft Entra account, they can redeem your B2B invitation using that account. Just invite the user using the normal invitation flow.
- **Microsoft accounts (MSA)**: Microsoft accounts are consumer accounts, set up by users to access services like Hotmail, Outlook, Xbox etc. Guest users can use their personal MSA to redeem B2B invitations and access resources in your tenant. This is enabled by default and if an external user has an existing MSA, they can redeem your B2B invitation using that account. Just invite the user using the normal invitation flow.
- **Email one-time passcode**: With this option a guest user can redeem an invitation using an email OTP. Each time they try to access a resource in your tenant, they will receive an OTP which they use to authenticate. This is enabled by default and can be used in user flow. Creating user flows is explained in *Chapter 13, External Identities in External Tenants*.
- **Social identities**: Microsoft Entra supports federation with social identity providers such as Google and Facebook. Users can redeem invitations and access resources in your tenant using Google credentials. Facebook federation, however, is supported only for self-service sign-up user flows and cannot be used to redeem invitations. Federation with Google and Facebook can be configured in the Microsoft Entra admin center by navigating to **Entra ID | External identities | All identity providers**.
- **SAML/WS-Fed identity provider federation**: Organizations can also set up federation with any external IdP that supports SAML or WS-Fed protocols. This federation allows users to use their own credentials to access resources in your tenant. This can be configured in the Microsoft Entra admin center by navigating to **Entra ID | External identities | All identity providers | Custom**.

By leveraging these identity providers, organizations can collaborate with external users without having to manage their credentials.

External collaboration settings

External collaboration settings can be used to manage B2B collaboration with non-Microsoft Entra entities. These settings let administrators define which users in the organization can invite external users for B2B collaboration. The following settings are available:

- **Guest user access**: Administrators can determine what external users can see in their Microsoft Entra directory. The following options are available.
    - **Guest users have the same access as members (most inclusive)**: Guest users will have the same level of access on directory data as members.
    - **Guest users have limited access to properties and memberships of directory objects**: This is the default setting and blocks guests from some directory tasks like enumerating users and groups. Guests can see membership of all non-hidden groups.
    - **Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)**: Guest users are not allowed to view profile information of other users or groups. They also cannot view group memberships.
- **Guest invite settings**: By default, all users and guests in a tenant can invite external users. Administrators can restrict this to only certain groups of users or guests. The following options are available.
    - **Anyone in the organization can invite guest users including guests and non-admins (most inclusive)**: This is the default setting and allows all members and guests to invite guests.
    - **Member users and users assigned to specific admin roles can invite guest users including guests with member permissions**: This setting only allows members and users who have specific administrator roles. With this setting enabled guests cannot invite other guests into the directory.
    - **Only users assigned to specific admin roles can invite guest users**: This setting only allows users who have the **User Administrator** or **Guest Inviter** roles to invite guest users.
    - **No one in the organization can invite guest users including admins (most restrictive)**: With this setting enabled no one in the organization will be allowed to invite guests.

- **Enable guest self-service sign up via user flows**: For applications developed by the organization, developers can create user flows to enable guests to sign-up and create a new guest account without having to be explicitly invited. Creating user flows is explained in *Chapter 13, External Identities in External Tenants*.
- **External user leave settings**: This setting allows external users to leave your organization by themselves. It is recommended to keep this setting on.
- **Collaboration restrictions**: Administrators can determine which domains can be invited into the tenant. The following options are available.
    - **Allow invitations to be sent to any domain (most inclusive)**: This is the default setting and allows invitations to be sent to users in any domain.
    - **Deny invitations to the specified domain**: This setting allows administrators to specify domains to which guest invitations cannot be sent. Invitations can be sent to all domains not in this list.
    - **Allow invitations only to the specified domains (most restrictive)**: This setting allows administrators to specify a list of domains to which invitations can be sent. Invitations cannot be sent to domains not in this list.

Microsoft recommends using the most restrictive settings to align with zero trust principles.

To configure external collaboration settings, follow the steps below:

1. Log in to `https://entra.microsoft.com` as a **Global Administrator**.
2. Navigate to **Entra ID** | **External identities** | **External collaboration settings**.
3. Make the necessary selections as per the above and click Save. Refer to the following screenshot:

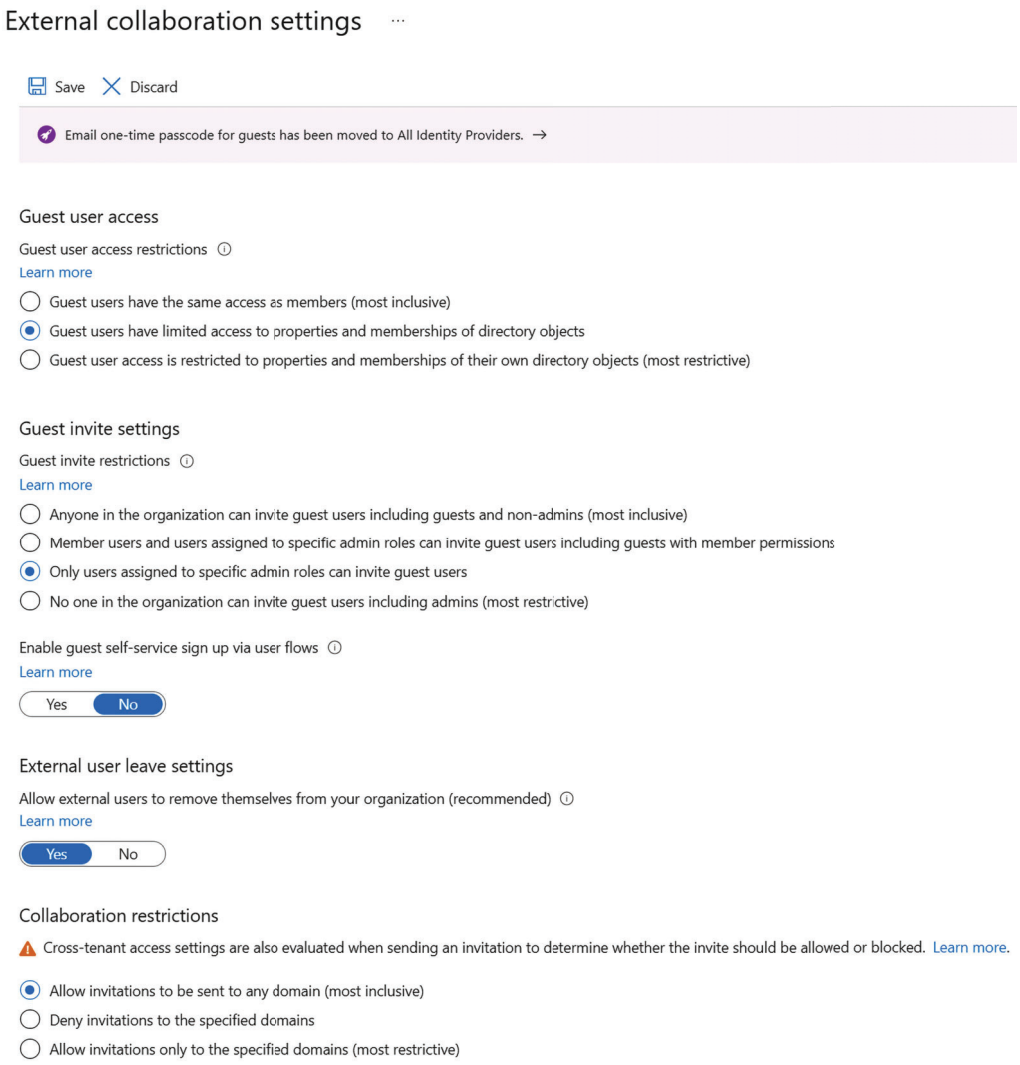


Figure 12.8: External collaboration settings

These settings can also be configured using the Microsoft Graph API.

When a B2B guest user signs in to a resource tenant, sign-in logs are generated both in the home tenant and the resource tenant. These logs include the user's sign-in information like email address, tenant name, application accessed, and more.

Cross-tenant access settings

Cross-tenant access settings are used to manage B2B collaboration with other Microsoft Entra organizations. In Microsoft Entra ID, B2B collaboration is enabled by default. Administrators can control the outbound and inbound B2B collaboration with other organizations using cross-tenant access settings. These settings allow administrators to manage how their organization interacts with other Microsoft Entra tenants.

In Microsoft Entra, a **resource tenant** is the inviting tenant. For example, if you are inviting external users to access resources in your tenant, then your tenant becomes the resource tenant. The tenant where the guest user's identity originates and is managed is called the user's **home tenant**.

Default settings

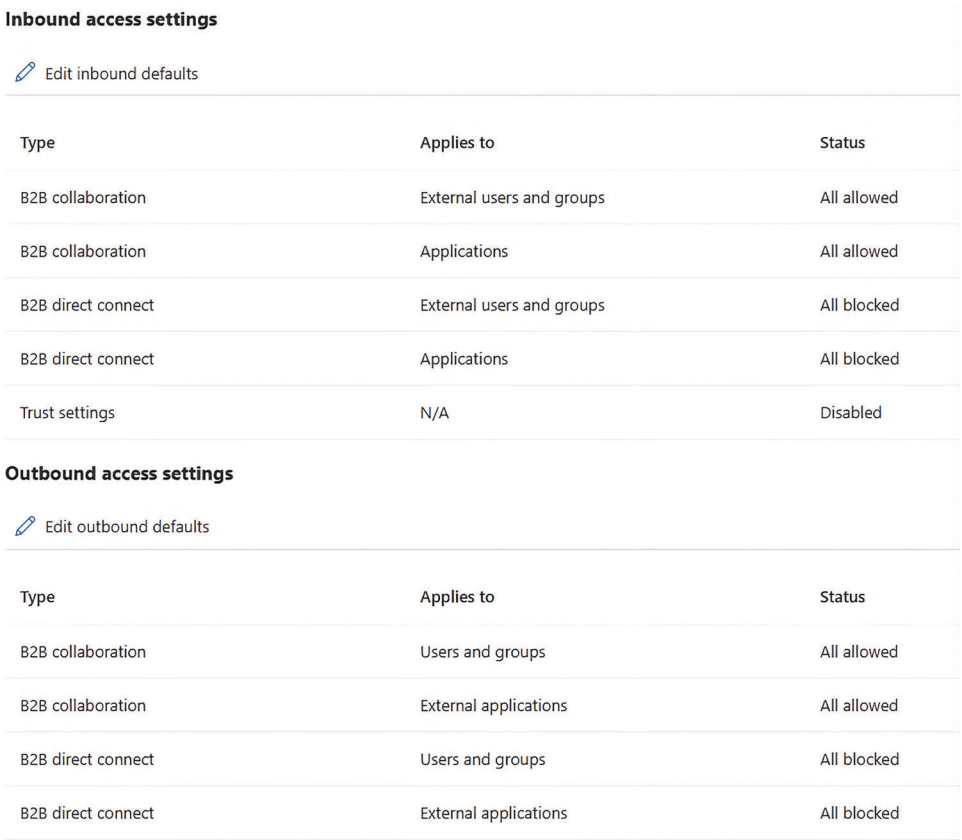
Default cross-tenant access settings can be viewed in the Microsoft Entra portal using the following steps:

1. Log in to `https://entra.microsoft.com` as a **Security Administrator**.
2. Navigate to **Entra ID** | **External identities** | **Cross-tenant access settings**.
3. In the right pane click on **Default settings**.

The following settings are available:

- **Inbound access settings**: These settings determine the level of access guest users have on resources in your tenant.
- **Outbound access settings**: These settings determine the level of access your organization's users will have on resources in other tenants where they are invited as guests.

The following screenshot shows the default inbound and outbound settings:



Inbound access settings

Edit inbound defaults

Type	Applies to	Status
B2B collaboration	External users and groups	All allowed
B2B collaboration	Applications	All allowed
B2B direct connect	External users and groups	All blocked
B2B direct connect	Applications	All blocked
Trust settings	N/A	Disabled

Outbound access settings

Edit outbound defaults

Type	Applies to	Status
B2B collaboration	Users and groups	All allowed
B2B collaboration	External applications	All allowed
B2B direct connect	Users and groups	All blocked
B2B direct connect	External applications	All blocked

Figure 12.9: Default inbound and outbound settings

To make changes to these settings, click on edit and make the appropriate changes. The following table summarizes the settings available:

Setting type	Options
Inbound access settings	• Allow or block all external users to be invited for B2B collaboration. • Allow or block access to all or selected applications for the invited B2B collaboration users. • Redemption order • Trust settings

Setting type	Options
Outbound access settings	• Allow or block all or selected internal users from being invited to external organizations for B2B collaboration. • Allow or block internal users from accessing all or selected external applications.

Table 12.2: Default cross tenant access settings

The above settings apply to all organizations unless **Organizational settings** is configured.

Trust settings

These settings determine whether Conditional Access policies in your tenant trust MFA and compliant device claims from other organizations. If trust settings are configured to trust MFA, users who have already completed MFA in their home tenant will not be required to complete MFA again in the resource tenant. Trust settings are only available in inbound access settings and are turned off by default. Refer to the screenshot below:

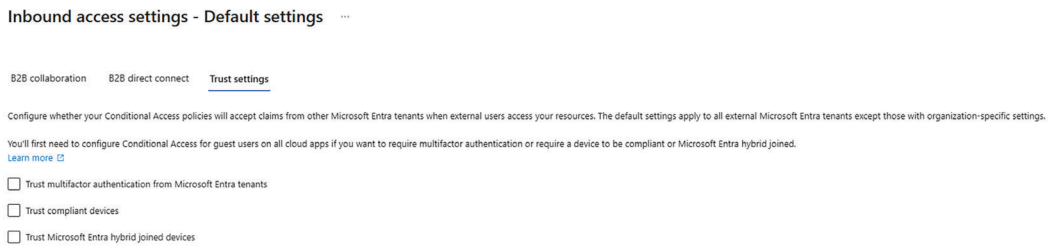


Figure 12.10: Trust settings

To make changes, make the appropriate selections and click **Save**.

Redemption order

Microsoft Entra ID has a default redemption order based on which a guest user's invitation is redeemed. The redemption order is as follows:

1. **Microsoft Entra ID**: When the user clicks on **Accept invitation** in the invitation email, Microsoft Entra ID checks if the user exists in a managed Entra ID tenant. If they do, the user is redirected to their Entra ID tenant to complete sign-up.
2. **SAML/WS-Fed IdP federation**: If the user does not exist in a managed Entra ID tenant and SAML or WS-Fed federation is enabled, Entra ID checks if the user's domain suffix

matches that of a configured SAML or WS- Fed IdP. If found, the user is redirected to that IdP to complete sign-up.

3. **Social providers**: If none of the above match, and if federation with social providers like Google or Facebook is enabled, Entra ID checks if the user has a corresponding account. If so, the user is redirected to the social provider to complete sign-up.
4. **Microsoft Account (MSA)**: Next Entra ID checks if the user has an MSA. If yes, they are prompted to sign up with their existing MSA.

If a user does not match any of the primary identity providers, Microsoft Entra ID uses email OTP or MSA as fallback options. At least one fallback option must always be enabled.

1. **Email OTP**: If the user does not have an MSA, and email OTP is enabled for guest users, they receive an OTP in their email and complete sign up using the OTP.
2. **MSA**: If no home directory is found and email OTP is disabled, the user is prompted to create an MSA and sign up using the newly created MSA.

The following screenshot shows the default redemption order:

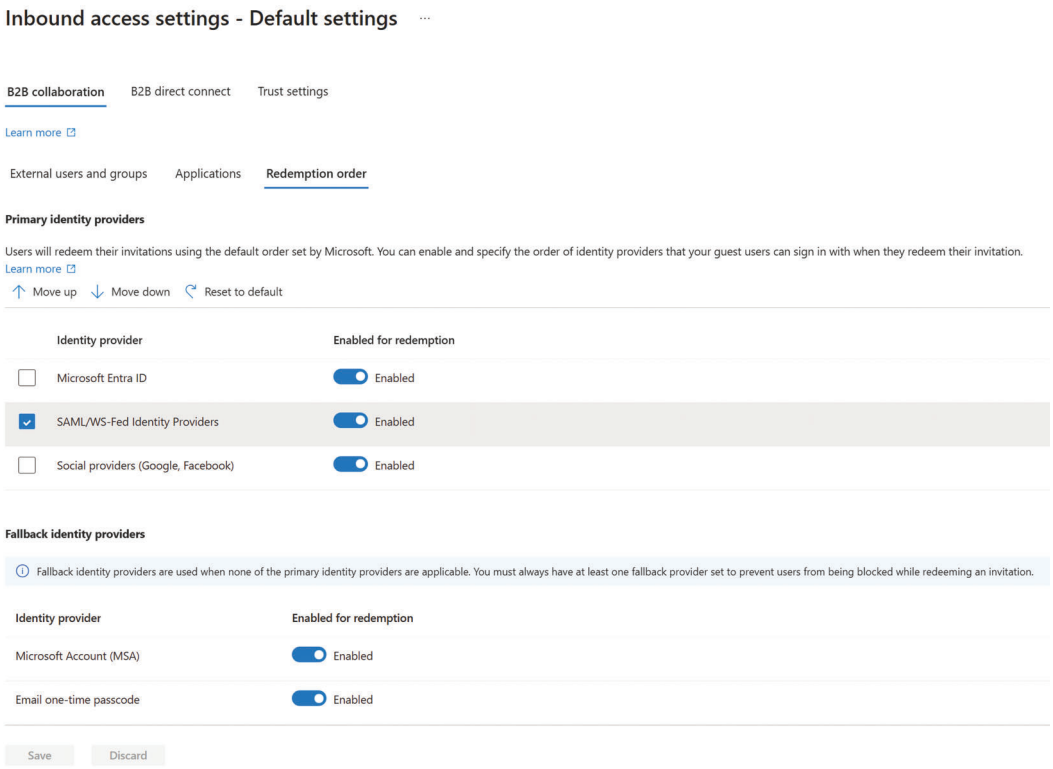


Figure 12.11: Redemption order

Administrators can change this default order by choosing the **Move up** or **Move down** options in the screenshot above.

Organization-specific settings

Organization-specific settings can be configured by adding an organization and modifying the inbound and outbound access settings specific to that organization. The following are the steps:

1. Log in to `https://entra.microsoft.com` as a **Global Administrator**.
2. Navigate to **Entra ID | External identities | Cross-tenant access settings**.
3. In the right pane click on **Organizational settings**.
4. To add an organization, click on **Add organization** and search for the external Microsoft Entra domain name and click **Add** as shown in the following screenshot:

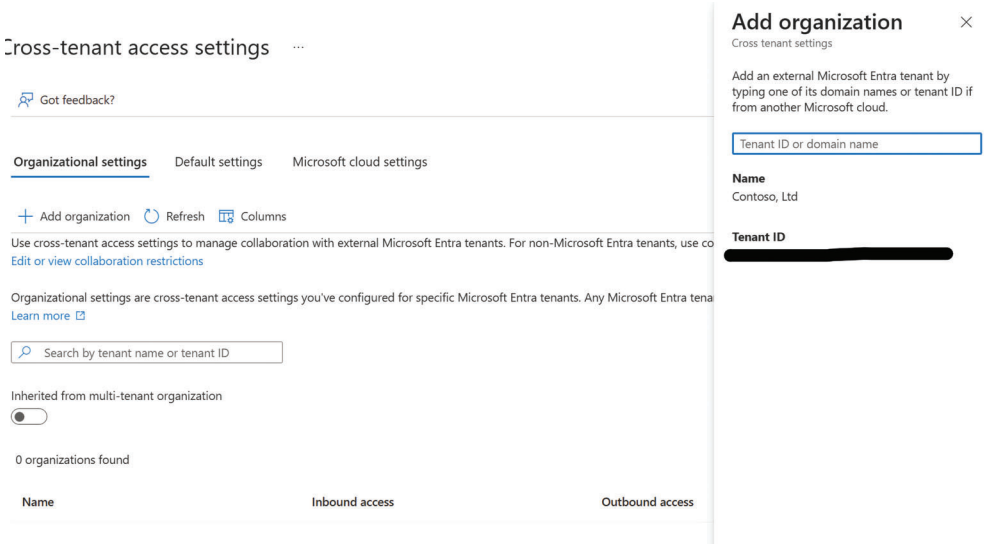


Figure 12.12: Add an organization

5. Once the organization is added, inbound and outbound settings can be customized by clicking on **Inherited from default** as shown in the following screenshot:

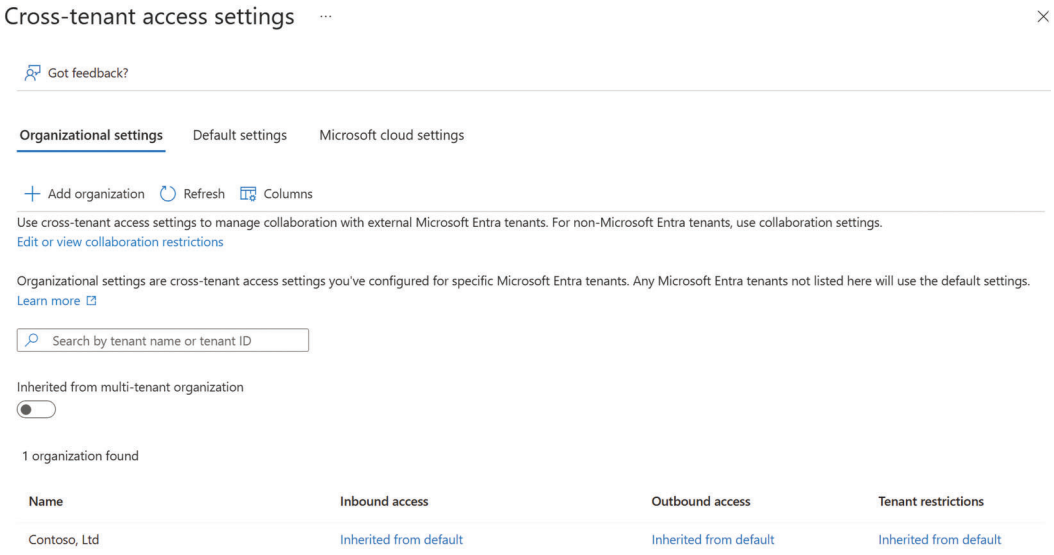


Figure 12.13: Customize organization-specific settings

Using organizational settings, you can manage your inbound and outbound B2B collaboration with different organizations differently. For example, you can choose to trust MFA claims from one organization but not from others. Organizational settings take precedence over default settings.

Automatic redemption

When a resource tenant invites a guest user, they must redeem an invitation to access resources in the resource tenant. **Automatic redemption** setting is a **Trust setting** in **Organizational settings** that allows automatic redemption of invitations so that users don't receive a consent prompt the first time they access the resource tenant. This is an outbound and inbound setting. This setting is available by clicking on **Inherited from default** as shown in *Figure 12.13* and selecting **Trust settings**. Check the box **Automatically redeem invitations with the tenant <target tenant name>**. Refer to the following screenshot:

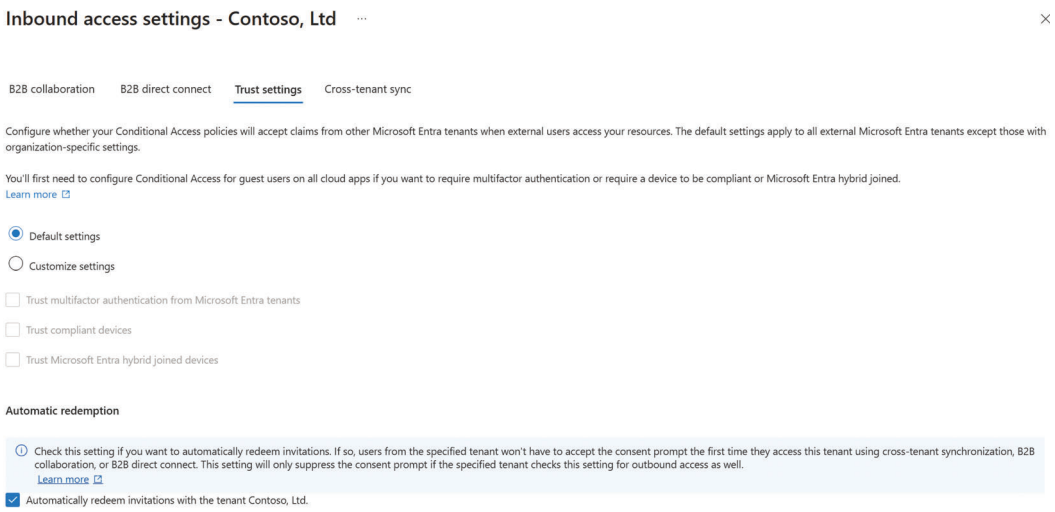


Figure 12.14: Automatic redemption

For invitation emails and consent prompts to be suppressed, the resource tenant as well as the user's home tenant must have this setting enabled.

Cross-tenant sync

Cross-tenant sync is an inbound-only synchronization option available in **Organizational settings**. This enables users and groups to be synchronized into your tenant. Following is a screenshot of cross-tenant sync settings.

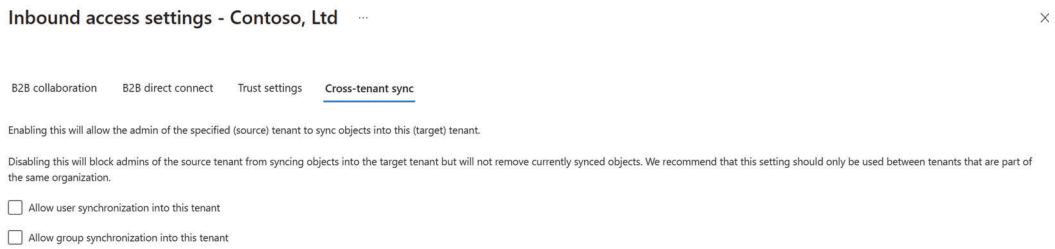


Figure 12.15: Cross-tenant sync

It is recommended that this setting be enabled only between tenants that are part of the same organization.

Tenant restrictions

To secure organizational resources, administrators can limit what their users can access when they use an external account on their home network or devices. This includes accounts that your users create in unknown tenants or accounts that external organizations give to your

users to access resources in their tenant. For example, an external organization invites a user from your organization to access an application in their tenant. As an administrator you can create policies to prevent the user from accessing some or all the external apps when they are using your network or devices. The following picture explains this.

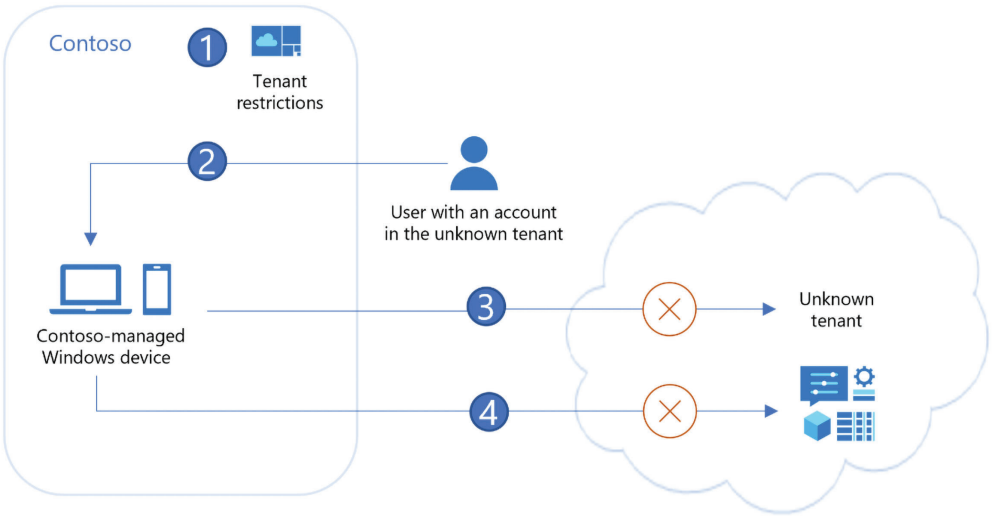


Figure 12.16: Tenant restrictions

The organization has configured tenant restrictions. The user of a Contoso managed device is using an account from an unknown tenant to access applications from the Contoso managed device. Tenant restrictions in Microsoft Entra ID block the user from accessing the external tenant from the Contoso managed device.

Tenant restrictions provide the following protection types:

1. **Authentication plane protection**: This prevents a user using external credentials from accessing an external tenant from the organization's managed device, thereby preventing a malicious insider from exfiltrating information from your tenant.
2. **Data plane protection**: This type of protection prevents attacks that bypass authentication like anonymously joining a Teams meeting or accessing SharePoint sites. This setting forces users to authenticate for resource access. Access is blocked if authentication fails.

Tenant restrictions are independent of the inbound and outbound access settings that are configured in cross-tenant access settings.

Tenant restrictions require a Microsoft Entra ID P1 license. The following are the steps to configure:

1. Log in to `https://entra.microsoft.com` as a **Security Administrator**.
2. Navigate to **Entra ID | External identities | Cross-tenant access settings**.
3. In the right pane click on **Default settings** and click on **Edit tenant restrictions defaults**. Refer to the screenshot below:

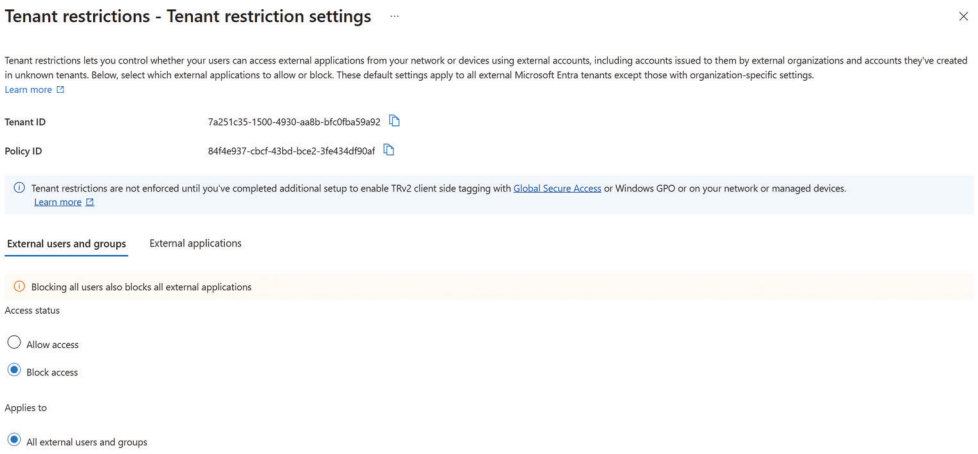


Figure 12.17: Configure tenant restrictions policy

By default, the tenant restrictions policy allows or blocks access for all external users and groups. It cannot be scoped to some external users. The following options are available.

   a. **Allow access**: Allow access to all users signing in with external accounts to access external applications specified in the **External applications** tab.
   b. **Block access**: Block access for all users signing in with external accounts to access external applications specified in the **External applications** tab.

4. Click on **External applications**. The following options are available:
   a. **Allow access**: Allow all users signing in with external accounts to access external applications specified in the **Applies to** section.
   b. **Block access**: Block all users signing in with external accounts from accessing external applications specified in the **Applies to** section.

5. Click on **Select external applications** to select the application to which access will be allowed or blocked. The following options are available.
    a. Click on **Add Microsoft applications** to pick from a list of Microsoft applications.
    b. Click on **Add other applications** and provide the application id of the external application.

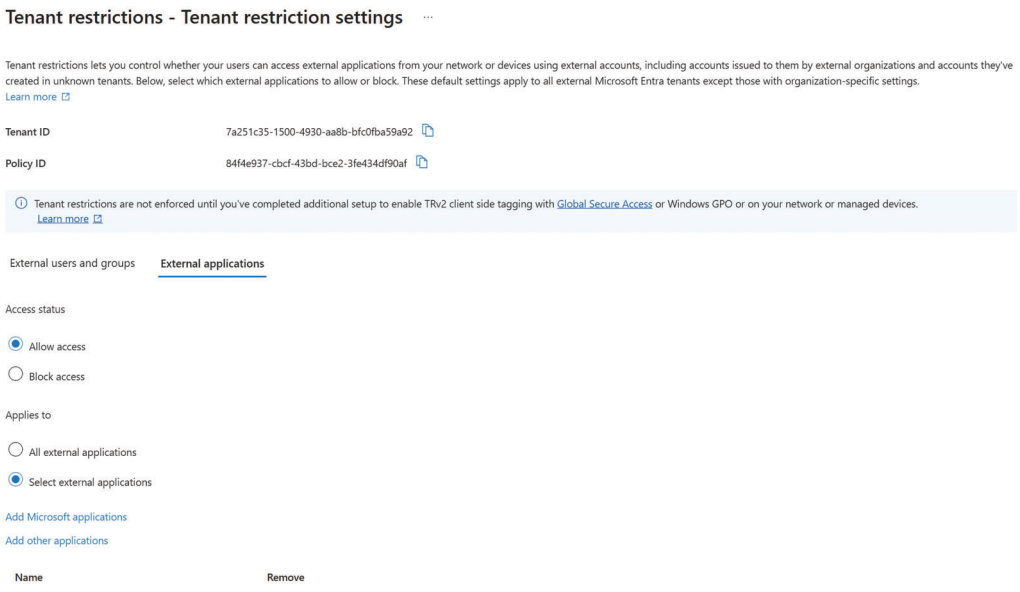


Figure 12.18: Configure application access

6. Click **Save**.

These tenant restrictions apply to all users signing in using external accounts. You might want to block all external users from accessing external applications but might want to allow users from a certain organization to use their credentials to access external applications from your network or devices. This can be configured using **Organizational settings**. The following are the steps:

1. Log in to `https://entra.microsoft.com` as a **Security Administrator**.
2. Navigate to **Entra ID | External identities | Cross-tenant access settings**.
3. In the right pane click on **Organizational settings** and click on **Inherited from default** under **Tenant restrictions**. Refer to *Figure 12.13*.

4. Under **External users and groups**, select **Customize settings**. Under **Access status** select **Allow access**. Under **Applies to** click on **Select <organization name> users and groups | Add external users and groups**.
5. In the fly out pane add the group id or user id and click **Add**.

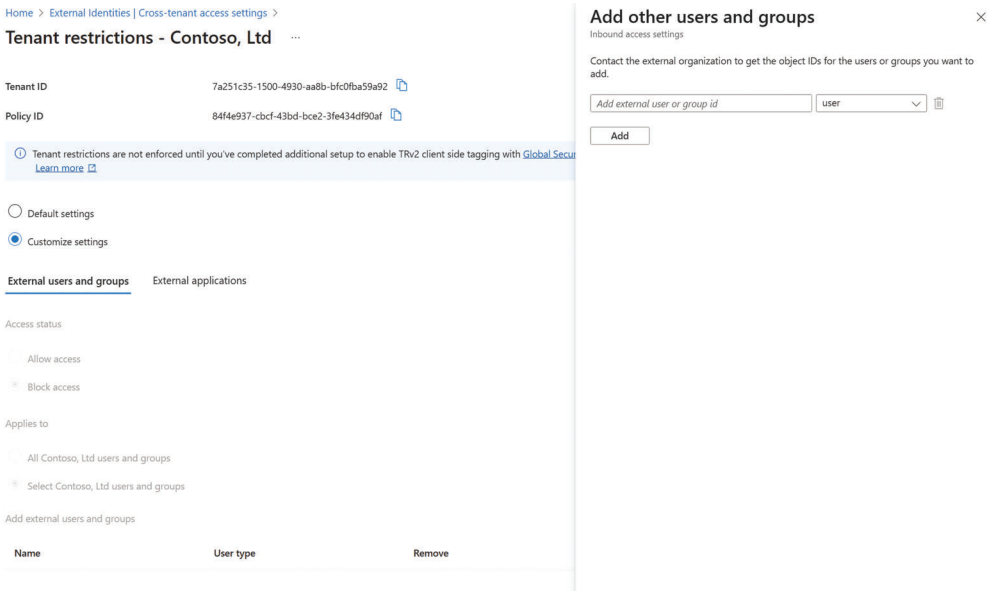


Figure 12.19: Tenant restrictions in organizational settings

Tenant restrictions also need to be configured on the client side to enable access to external applications from your network and devices. This can be done using Global Secure Access or setting up tenant restrictions on your corporate proxy. The detailed steps are beyond the scope of this book. Refer to`https://learn.microsoft.com/en-us/entra/external-id/tenant-restrictions-v2#configure-tenant-restrictions-v2-on-the-client-side`.

Microsoft cloud settings

The Microsoft cloud settings option in cross-tenant access settings allows you to configure collaboration between Azure commercial clouds and Azure Government clouds or Azure China clouds. The following cloud pairs are supported.

- Azure commercial (source) to Azure Government (target)
- Azure Government (source) to Azure commercial (target)
- Azure commercial (source) to Azure China (target)

Before proceeding with configuration, ensure that the following prerequisites are met for the source tenant:

- Microsoft Entra ID Governance license.
- Security Administrator role to configure cross-tenant access settings.
- Hybrid Identity Administrator role to configure cross-tenant collaboration settings.
- Cloud Application Administrator or Application Administrator role to assign users.

To enable this collaboration in the Microsoft Entra admin center, navigate to **Entra ID | External identities | Microsoft cloud settings** and select the clouds you wish to collaborate with. Refer to screenshot below:

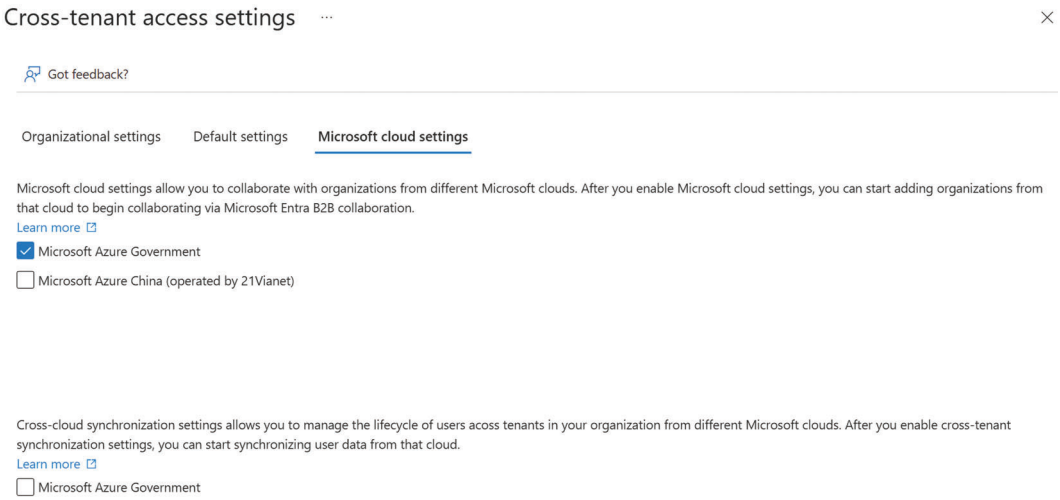


Figure 12.20: Microsoft cloud settings

Once this is enabled, add the target organization tenant by going to **Organizational settings** as shown in *Figure 12.12*. You will need the tenant id to add the target organization as domain name lookup is not supported across clouds. All access settings for this organization are inherited from the default settings. You can customize them as required.

Following are the steps to enable cross-cloud synchronization:

1. Enable cross-cloud access settings in both tenants as shown in *Figure 12.20*.
2. In the target tenant, add the source tenant as an organization, by going to **Organizational settings**. Refer to *Figure 12.12*. Under Inbound access settings of the added tenant, enable cross-tenant sync as shown in *Figure 12.15*.
3. In the source tenant, create a configuration by navigating to **Entra ID | Cross-tenant synchronization | Configurations | New configuration** as shown in the following screenshot and click **Create**:

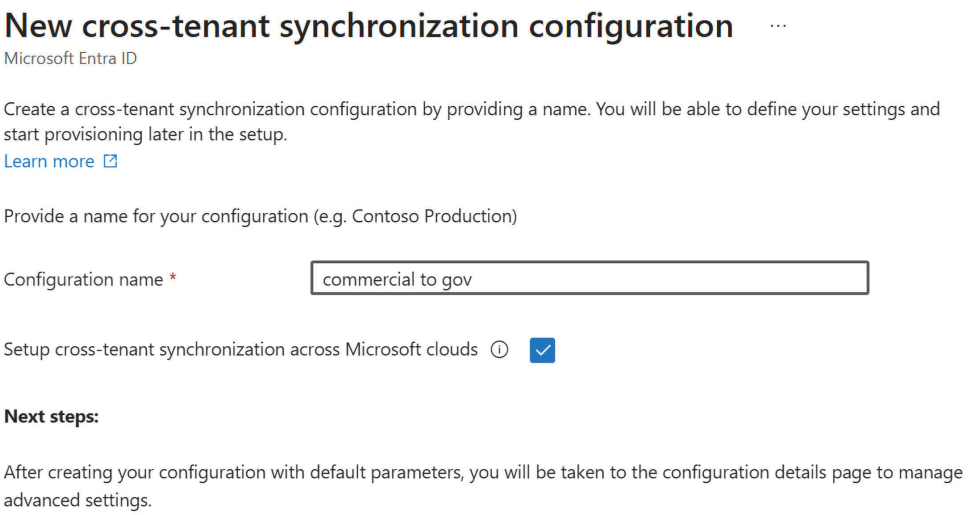


Figure 12.21: Configure cross-tenant synchronization

4. Select the newly created configuration and click **Get started**. Set the **Provisioning mode** to **Automatic**. Under **Admin credentials**, ensure that the **Authentication method** is set to **Cross Tenant Synchronization Policy**. In the **Tenant Id** box, enter the tenant id of the target tenant and click **Test Connection**. You should see a box informing you that the connection is successful. Click **Save**. Refer to the following screenshot:

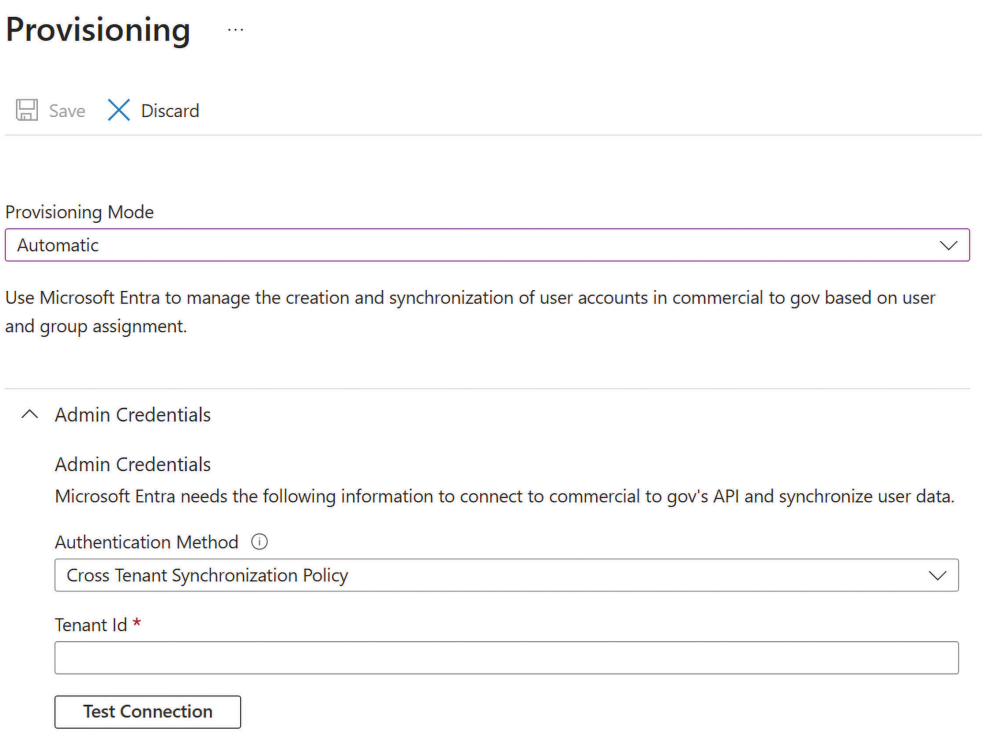


Figure 12.22: Test the configuration

5. In the source tenant, you can define who is in scope for provisioning. You can manually assign users to the configuration or create attribute-based scoping filters. In the newly created configuration, click on **Provisioning** and expand **Settings**. Under **Scope**, select **Sync only assigned users and groups** and click **Save**. Refer to *Figure 12.23*. Ensure that the **Provisioning Status** in **On**.

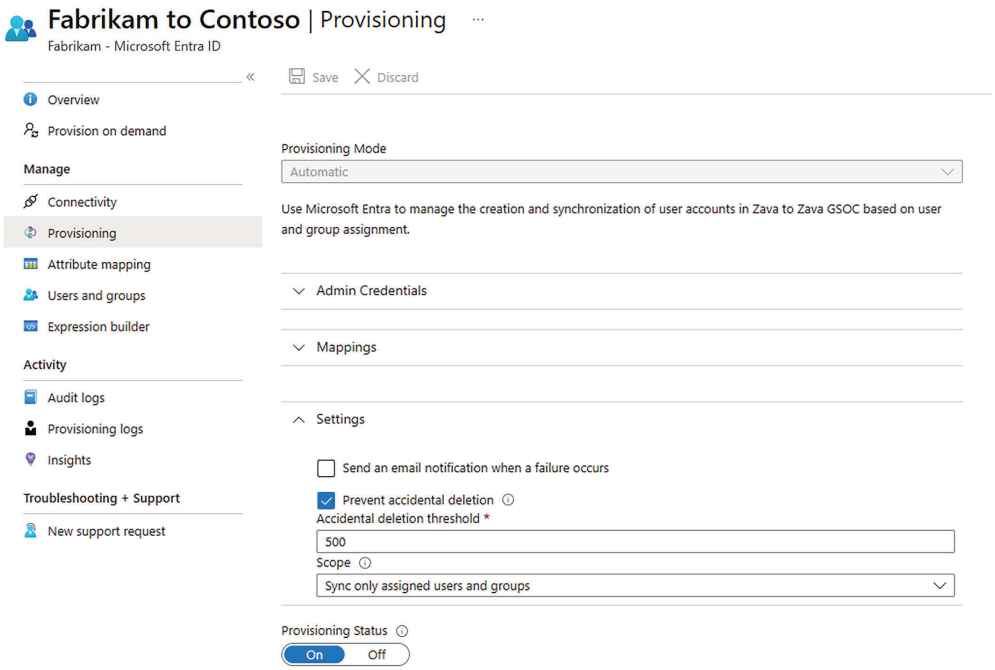


Figure 12.23: Scope users for provisioning

6. Click on **Users and groups** and select the users or groups who you want to provision to the target tenant as shown in the following figure:

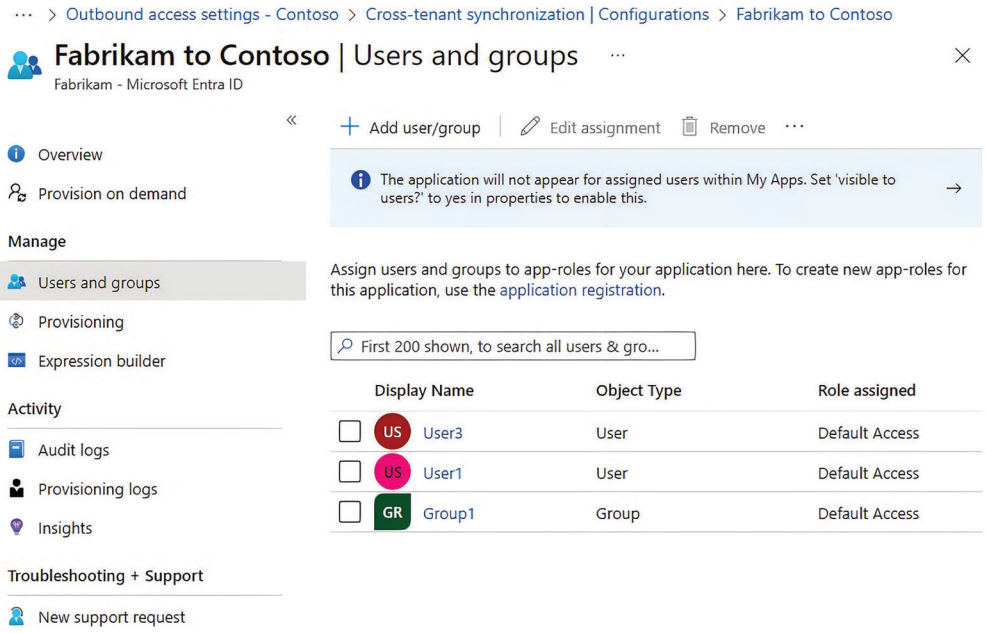


Figure 12.24: Select users and groups in scope

The provisioning job will now start the initial synchronization of the selected users and groups. The first cycle will take longer as complete synchronization needs to be completed. Subsequent cycles will be quicker as only incremental changes are synchronized. Provisioning cycles run every 40 minutes. You can view the progress of provisioning by monitoring the provisioning logs. They are available under the **Provisioning logs** blade.

B2B direct connect

B2B direct connect is a feature that allows organizations to set up a mutual trust relationship with another Microsoft Entra organization. Currently, this feature only supports Microsoft Teams shared channels. With this feature enabled, users from both organizations can collaborate in a shared Teams channel using their home credentials. They don't have to be added to each other's organizations as guests.

For B2B direct connect to work, both tenants must establish mutual trust by enabling the required inbound access settings for each other. Because the trust is configured as an inbound setting, each organization must enable it on their own tenant. B2B direct connect only works when both tenants are in the same Microsoft cloud environment. Refer to *Figure 12.9*. Then users in one organization can create a Microsoft Teams shared channel and invite users from the other organization. The invited user can access the shared channel from within Teams in

their home tenant without having to sign into the organization that hosts the shared Teams channel.

The following settings are available:

Setting type	Options
Inbound access settings	• Allow or block all external users from accessing B2B direct connect. • Allow or block access all or specified applications to be access by B2B connect users. • Redemption order • Trust settings
Outbound access settings	• Allow or block all or selected internal users to access B2B direct connect with external organizations. • Allow or block all or selected external applications from being accessed by B2B connect users.

Table 12.3: B2B direct connect settings

Use **Default settings** to configure B2B connect for all external organizations. If you want to configure specific settings with some organizations, use the **Organizational settings**.

Governance for B2B users

You can audit guest users in the same way as member users. You can use ID Governance access reviews to review access for guest users. Access reviews are explained in *Chapter 6, Microsoft Entra Entitlement Management*.

You can also use Microsoft Entra Lifecycle Workflows to manage the lifecycle of guest users across the joiner, mover, and leaver scenarios. Lifecycle workflows are explained in *Chapter 7, Microsoft Entra Lifecycle Workflows*.

ID Protection for B2B users

Using Microsoft Entra ID Protection, organizations can block users from signing in if their credentials are considered at risk. Microsoft Entra ID Protection detects compromised credentials for B2B users. The user risk for B2B users is evaluated in their home tenant. When these users try to access resources in the resource tenant, their real-time sign-in risk is calculated. Microsoft Entra ID Protection can then enforce risk-based Conditional Access policies for B2B users. Risk-based Conditional Access policies are explained in *Chapter 9, Microsoft Entra ID Protection*.

The following ID Protection limitations apply to B2B users:

- If the user risk policy is triggered and a password reset is required, the user will be blocked. This is because the user's password is maintained in their home directory and not the resource directory.
- Guest users do not show up in the risky users report. This is because user risk for guest users is evaluated in their home directory.
- Administrators in the resource directory cannot dismiss a user risk or remediate risk for a B2B user because the user object is maintained in the user's home directory.

It is recommended to use Microsoft Entra ID Protection for B2B users to protect your tenant even if the user's home tenant has not enabled ID protection.

Leaving an organization

Administrators can enable external users to leave their organization when they want without having to contact the administrator. This can be done in external collaboration settings by setting the **External user leave settings** to **Yes**. Refer to *Figure 12.8*. Leaving an organization ends the relationship between an external user and the resource organization.

A user can leave an organization by following the steps below:

1. Go to `https://myaccount.microsoft.com`
2. Navigate to **My Account** | **Organizations**.
3. Click on **Leave** next to the organization you want to leave, as shown in the following screenshot:

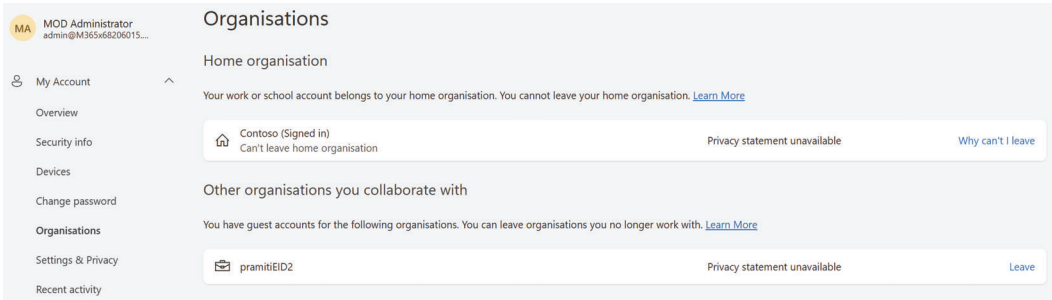


Figure 12.25: Leaving an organization

When a B2B user leaves the organization, the user's account is deleted from the directory and placed in the **Deleted users** area. It remains there for 30 days, during which the administrator can recover the user's account if required. If the account is not restored within 30 days, it is permanently deleted. Data deletion can take an additional 30 days.

Best practices

Effective management of guest users starts with treating every external identity as a temporary, high-variance access point that must be governed with clarity, constraint, and continuous review. Following are some best practices to manage B2B guests in the workforce tenant.

1. Configure the most restrictive external collaboration settings as per the organization's requirements.
2. Enable automatic redemption only for trusted partner organizations.
3. Enforce least privilege for guest users.
4. Disable guest ability to enumerate directory objects.
5. Create guest-specific Conditional Access policies that enforce MFA and location restrictions.
6. Perform periodic access reviews for guest accounts to review guest access to resources and inactive guest accounts.
7. Use access packages to provide birthright access to guests. Configure expiration on access packages.
8. Implement Terms of Use for external users.
9. Use cross-tenant access settings for collaboration with partner organizations.
10. Use federation for guest users. Avoid creating accounts for guests in your tenant.

Strong guest governance isn't a one-time setup. It is a continuous discipline that keeps your tenant secure, predictable, and collaboration-ready through every external identity lifecycle.

Pricing

Entra External ID is billed based on **Monthly Active Users (MAU)**. It offers the first 50,000 MAU for free. Each user who authenticates to the tenant once a month contributes to the MAU. Ensure that there is an Azure subscription attached to your Microsoft Entra ID tenant for billing purposes.

Summary

This chapter began by introducing Microsoft Entra External ID and clarifying the differences between workforce and external tenant setups. It also covered how External ID functions within a workforce tenant. You learned how to invite and manage guest users, set up external collaboration for B2B scenarios, and adjust both default and organization-specific cross-tenant access settings for direct B2B connections and multi-cloud environments. The chapter discussed enabling synchronization between tenants and clouds, outlined the different identity providers for B2B collaboration, and described ways to secure and govern B2B users. The following chapter will explore the CIAM features of Entra ID.

Exercises

1. What is the most appropriate scenario for a workforce tenant configuration?
    a. An e-commerce website.
    b. Providing access to external partners to line-of-business applications.
    c. A citizen-facing service where citizens can log in to view their benefits.
    d. A mobile application providing mental health support to patients.
2. Which of the following is a limitation of B2B guests?
    a. They are created with user type Guest.
    b. By default, they cannot invite other guests to the resource tenant.

   c. Conditional Access policies cannot be applied to them.
   d. B2B guest users cannot be added to Microsoft Teams shared channels.

3. A high-risk B2B user is signing into a resource tenant. The resource tenant has enabled a user risk-based Conditional Access policy for guest users. What will be the user experience?
   a. The user will be able to sign in as the user risk is calculated in the user's home tenant and the resource tenant has no visibility of the risk.
   b. The user will be forced to perform a secure password reset to remediate the risk.
   c. The user will be blocked from signing in as the password is maintained in the user's home directory.
   d. The user will be directed to their home directory to perform a password reset.

Answers

1. b
2. d
3. c

Additional resources

- Tenant restrictions V2: `https://learn.microsoft.com/en-us/entra/external-id/tenant-restrictions-v2`
- Add Google as an identity provider: `https://learn.microsoft.com/en-us/entra/external-id/google-federation`
- Add Facebook as an identity provider: `https://learn.microsoft.com/en-us/entra/external-id/facebook-federation`
- SAML/WS-Fed IdP federation: `https://learn.microsoft.com/en-us/entra/external-id/direct-federation`
- Default user permissions in Microsoft Entra ID: `https://learn.microsoft.com/en-us/entra/fundamentals/users-default-permissions`
- Troubleshooting B2B users: `https://learn.microsoft.com/en-us/entra/external-id/troubleshoot`
- Best practices for B2B collaboration: `https://learn.microsoft.com/en-us/entra/external-id/b2b-fundamentals`

Join us on Discord

For discussions around the book and to connect with your peers, join us on Discord at `packt.link/discordcloud` or scan the QR code below:



13

External Identities in External Tenants

Consumer Identity and Access Management (CIAM) is a specialized branch of identity management focused on providing secure, seamless, and user-friendly digital experiences for external users, such as customers, partners, or citizens. Unlike traditional workforce identity solutions, which manage internal employee access, CIAM solutions are designed to handle the unique challenges of managing large numbers of external users who often interact with an organization through web portals, mobile apps, and other digital services.

At its core, CIAM enables organizations to authenticate, authorize, and manage the identities of their consumers while protecting sensitive information and complying with privacy regulations. Key capabilities typically include self-service registration, social login integration, multi-factor authentication (MFA), consent management, and robust data privacy controls. These features help organizations deliver personalized experiences, foster customer trust, and ensure security without introducing unnecessary friction.

As digital engagement becomes a critical business driver, CIAM platforms must scale to support millions of users and provide high availability. They must also integrate with marketing, analytics, and customer service systems to deliver unified, omnichannel experiences. Ultimately, a well-implemented CIAM solution not only safeguards user data but also helps organizations build lasting relationships and drive business growth.

This chapter will cover

- External ID in the external tenant
- Create an external tenant
- Configure applications for SSO

- Create and customize user journeys
- Securing external tenants
- Migrating to Entra External ID

External ID in external tenants

In addition to B2B collaboration, Microsoft Entra External ID also includes Microsoft's next generation CIAM solution that enables businesses to make their applications available to consumers and business customers, leveraging features like self-service registration, personalized sign-in experiences and customer account management. These CIAM features are built on Microsoft Entra ID enabling organizations to benefit from platform features like security, scalability and compliance.

External ID in external tenants is a separate directory from your workforce tenant which is used by employees and for B2B collaboration. The first step toward enabling external ID for consumers is to create an external tenant. This way you create a distinct tenant that follows the Microsoft Entra model but is configured for consumer scenarios. This external tenant consists of

- **A directory**: This is the location where the consumer identities are stored.
- **Applications**: To make applications available to consumers, they must be registered with Microsoft Entra ID so that it can perform identity and access management for those applications. Applications that use **Security Assertion Markup Language (SAML)** or **OpenID Connect (OIDC)** can be registered in the external tenant.
- **User flows**: Administrators can enable self-service sign-up, sign-in, and password reset experiences for consumers.
- **Extensions**: Custom authentication extensions can be used if user attributes or data from external systems need to be added.
- **Sign-in methods**: Entra External ID offers various sign-in methods like email and password, email and OTP, social IdPs and custom OIDC providers.
- **Encryption keys**: Using Entra External ID application owners can add and manage encryption keys for signing and validating tokens, client secrets, certificates and passwords.

Entra External ID is billed based on **Monthly Active Users (MAU)**.

Note

External ID in external tenants is not available in China and US government clouds.

Creating an external tenant

The first step in getting started with your CIAM journey is to create an external tenant. To create an external tenant, you must have an Azure subscription. The following are the steps to create an external tenant.

1. Login to `https://entra.microsoft.com` as a **Tenant Creator**.
2. Navigate to **Entra ID | Overview | Manage tenants**.
3. Click **Create | External** as shown in the screenshot below. Click **Continue**.

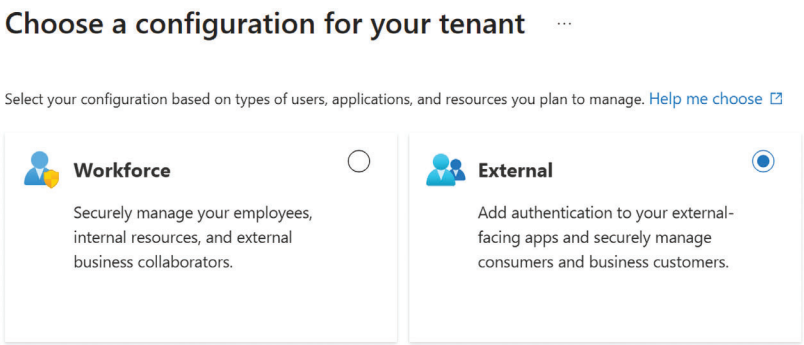


Figure 13.1: Create an external tenant

4. Enter a unique **Tenant Name** and **Domain Name**. Select a location of your choice and click **Next: Add a subscription**.

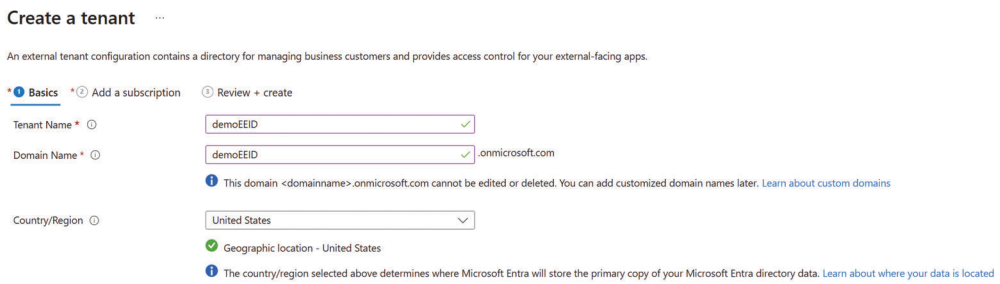


Figure 13.2: Enter the basics

5. On the **Add a subscription** page, select your **Subscription** and **Resource group**. Click **Next: Review + Create**.

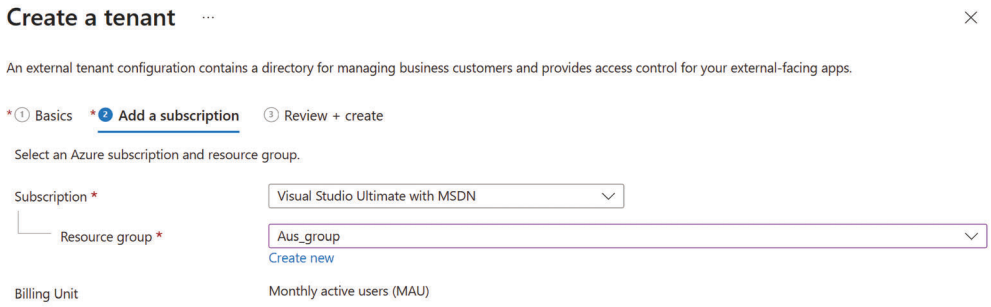


Figure 13.3: Select Azure subscription

6. On the next page, review your selections and click **Create**. Once the tenant is created, it will be visible under **Manage tenants** as shown in the screenshot below.

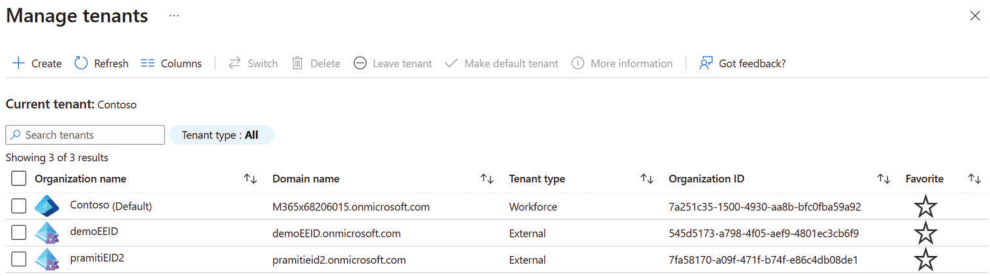


Figure 13.4: Workforce and external tenants

To administer the newly created tenant you will have to switch to that tenant using the steps below.

1. In the Microsoft Entra admin center, click on your name in the top right corner and click on Switch directory.

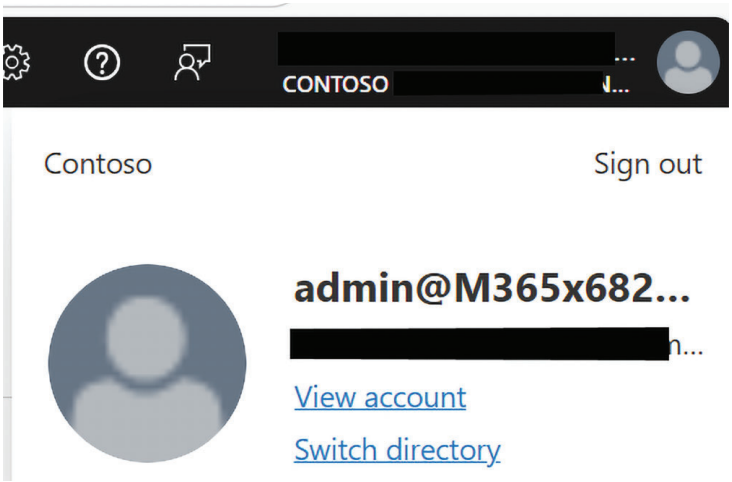


Figure 13.5: Switch directory

2. Click on **Switch** next to the external tenant as shown below. This will take you to the newly created external tenant.

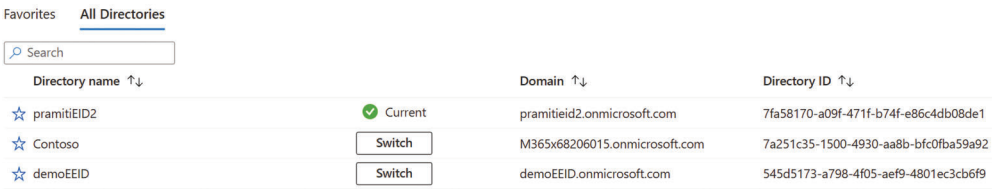


Figure 13.6: Switch to the external tenant

The person who creates the external tenant is the first user in the tenant and is automatically assigned the **Global Administrator** role.

Using the get started guide

Administrators can then use the get started guide to customize the sign-in experience, create the first app, and sign in users. Using this guide is optional. Administrators can choose to configure the tenant without using the guide. To access the guide, follow the steps below.

1. In the Microsoft Entra admin center of the external tenant navigate to **Overview | Get started | Start the guide** as shown below:

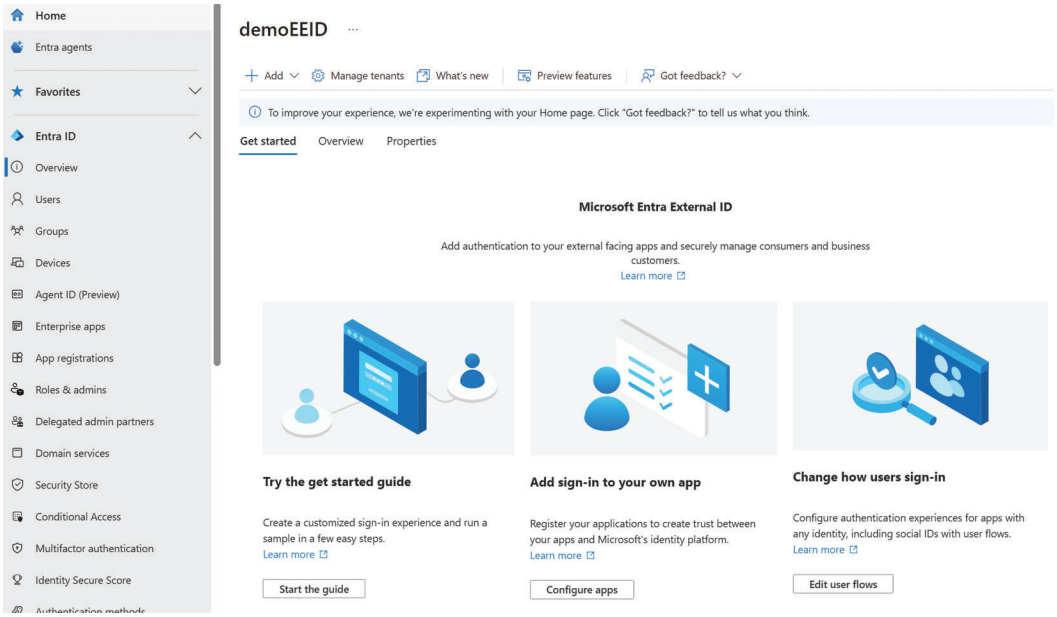


Figure 13.7: Get started guide

2. Click on the **Start the guide**. On the following screen, choose the sign-in method, upload your organization logo, select background color and layout. Click **Continue**.

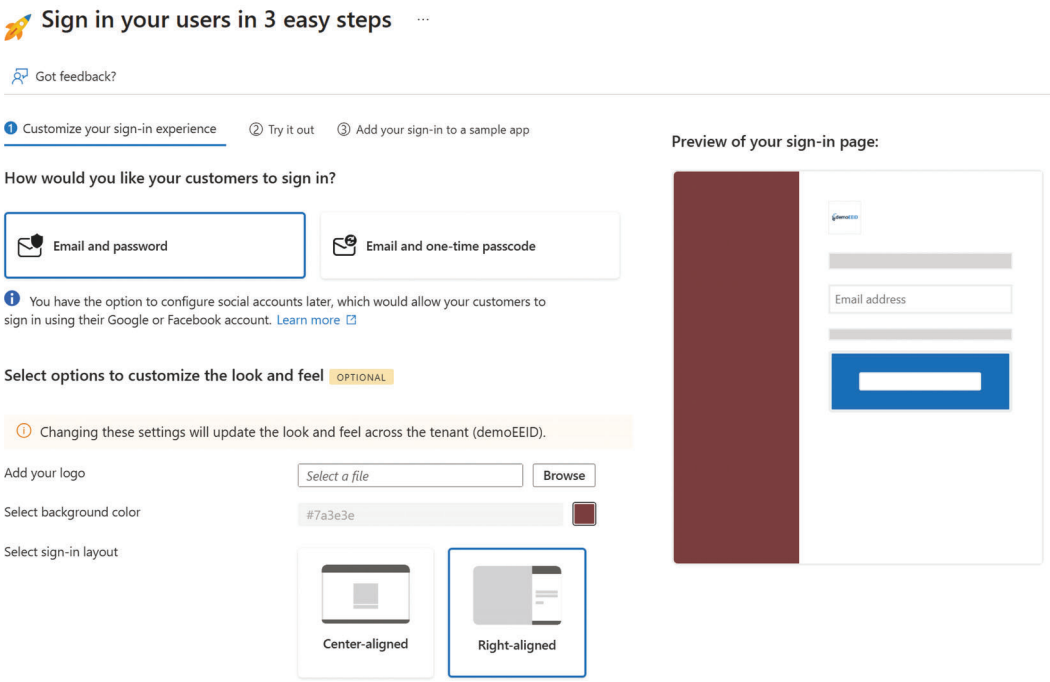


Figure 13.8: Customize sign-in experience

3. On the **Try it out** page, you will be able to open the sign-in experience in a new tab and create your first user. Click on the **Run it now** button. The sign-in experience will open in a new tab where you will be able to create a new user account in the external ID tenant. Once done click **Continue**.

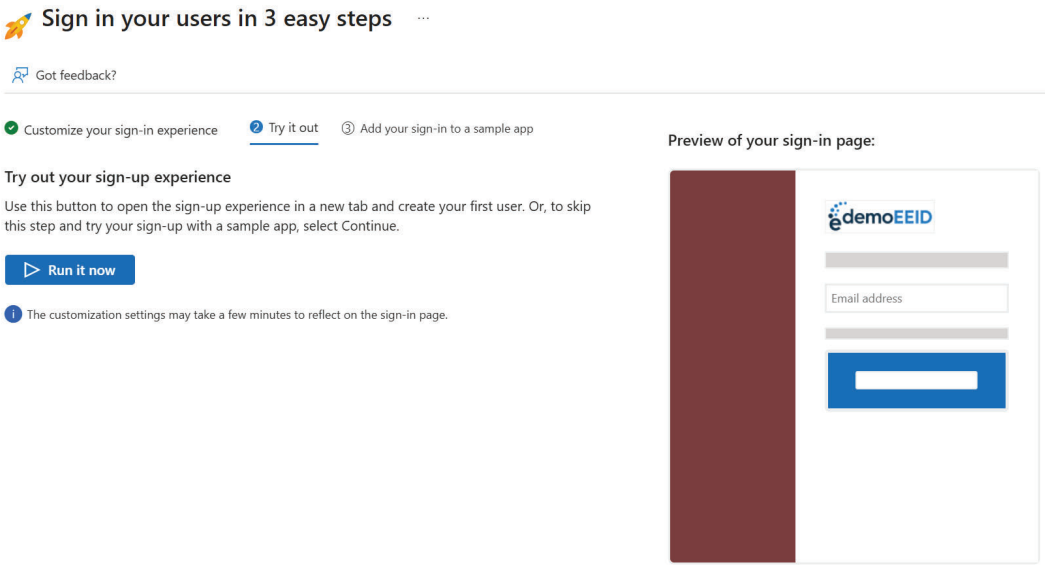


Figure 13.9: Try it out

Tip

For testing, use a different account than the one you used to create your tenant. You can use a temporary email service like `https://temp-mail.org/` to generate temporary email accounts for testing purposes.

On the next page, you will be able to add your application. You can exit the guide at this stage and configure an application directly in the portal. This is explained later in the chapter.

User profile attributes

As with user objects in the workforce tenant, the user objects in the external tenant also store information about the users in user profile attributes. Entra External ID supports the following types of user attributes.

- **Built-in user attributes**: These are default attributes that store information like City, Country, Display Name, and Email Address.
- **Custom user attributes**: Administrators can create additional attributes for any additional information they would like to collect from the users. Custom attributes can collect input from users in the form of string, radio buttons, multiselect checkboxes, numeric text box and single-select checkbox. Checkboxes and radio buttons can

include hyperlinks to other content like a privacy policy or terms of use document. The custom attributes collected from the users are stored in an app called *b2c-extensions-app*. This app is visible on the **App registrations** page in the Entra External ID tenant.

Note

Do not make any changes to the *b2c-extensions-app* as it is used to store user data.

To create a custom user attribute, follow the steps below.

1. In the Microsoft Entra admin center, switch to your Entra External ID tenant and navigate to **Entra ID | External Identities | Custom user attributes**.
2. In the right pane, click **Add**. Refer to *Figure 13.10*.
3. In the flyout pane, enter a **Name** for the attribute and select the **Data Type** as appropriate. The available options are String, Boolean and Int. Click **Create** to create the attribute.

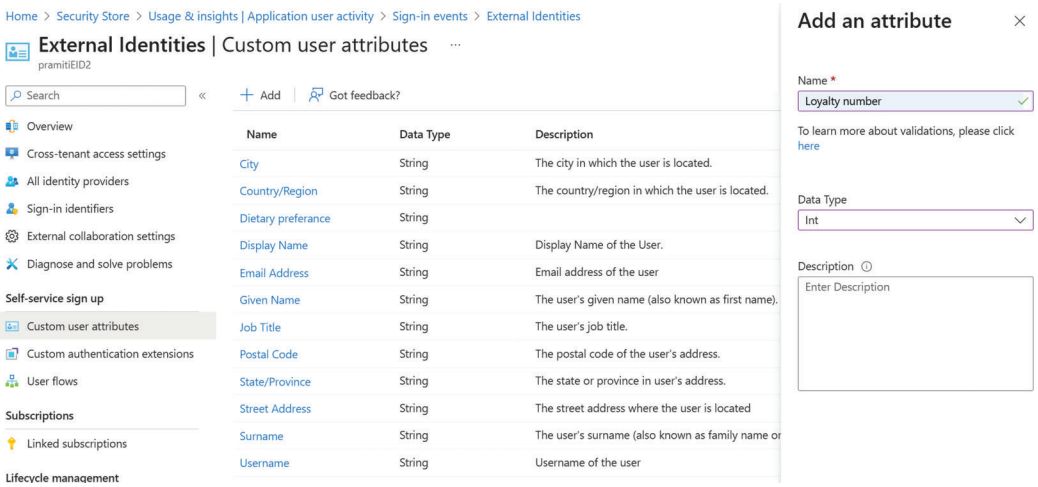


Figure 13.10: User profile attributes

The following table shows a mapping of the data type to the user input type. Make the appropriate selection depending on your requirements.

Data type	User input type
String	`TextBox`

Data type	User input type
String	`RadioSingleSelect`
String	`CheckboxMultiSelect`
Boolean	`CheckboxSingleSelect`
Int	`NumericTextBox`

Table 13.1: Data types mapping to user input type

For example, if you want to collect dietary preference from a list of options, create the custom attribute as a *String*. It can then be configured as a *RadioSingleSelect* or *CheckboxMultiSelect* using the following steps.

1. In the Microsoft Entra admin center, switch to your Entra External ID tenant and navigate to **Entra ID | External identities | User flows**.
2. Select the user flow for which you want to customize the attributes. Click on **User attributes** and add the attributes you want to collect at sign-up. Click **Save**.
3. In the left pane, click on **Page layouts**. Select the attribute to customize. Under **User Input Type**, click on the pencil to select the appropriate type as shown below. If you select **RadioSingleSelect** or **CheckboxMultiSelect**, provide a list of options that the user can choose from. Click **Ok** and then click **Save**.

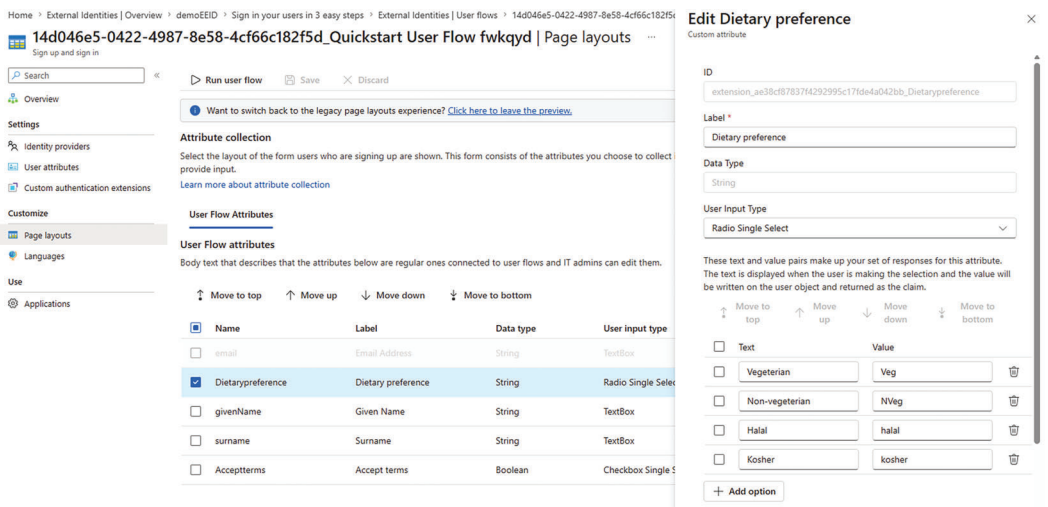


Figure 13.11: Customize the data type

The following picture shows an example of a **RadioSingleSelect** input type as visible to the user on the sign-up form.



Figure 13.12: RadioSingleSelect

Configuring identity providers

Just like in the workforce tenant, external ID in the external tenant offers several ways in which users can sign up. The following options are available:

Email and password

This option is enabled by default. With this option, users can sign up with their email address and password. This creates a local account in the external tenant and the user's password is stored in the external tenant directory. The user clicks on the **No account? Create one** option on the login screen. They can enter any existing email address. They are then sent an OTP to confirm the email address. Once they enter the OTP, they are asked to choose a password. On subsequent logins, the user uses the password they selected during the sign-up process. The following screenshot shows the user's journey when signing up with email and password.



Figure 13.13: User flow using email and password

Later, if the user forgets their password, they can reset it using the **Forgot password?** link on the password page.

Email and OTP

Using this option, users can sign up using an email address and an OTP. They are not required to create a password. They receive an OTP each time they sign in.

Username or alias

In some scenarios, organizations want the users to be able to sign in using a username. This could be a frequent flyer number, loyalty number, student ID, etc. With this option, users can choose to log in using a username or their email address. To enable username as a sign-in identifier, it must be enabled in Microsoft Entra admin center. Following are the steps:

1. In the Microsoft Entra admin center, switch to your Entra External ID tenant and navigate to **Entra ID | External Identities | Sign-in identifiers**.
2. If this is the first time you have navigated to this page, click on **Enable now**.
3. Email and UPN are enabled by default. To enable sign-in using an alias, select the box next to **Username** and click **Save** as shown below.

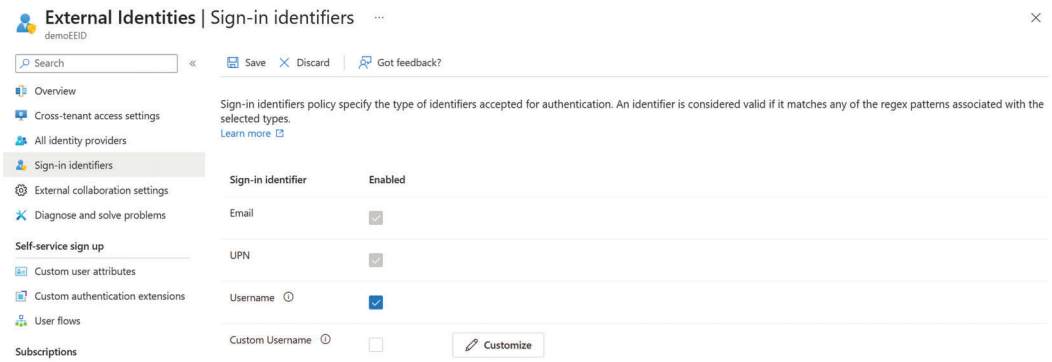


Figure 13.14: Enable username sign-in

4. You can also validate usernames against a custom regular expression (regex) by clicking on **Customize** next to the **Custom Username** option. In the flyout pane, click **Enable**. Up to two regex patterns can be specified. Click **Save**. Refer to *Figure 13.15*.

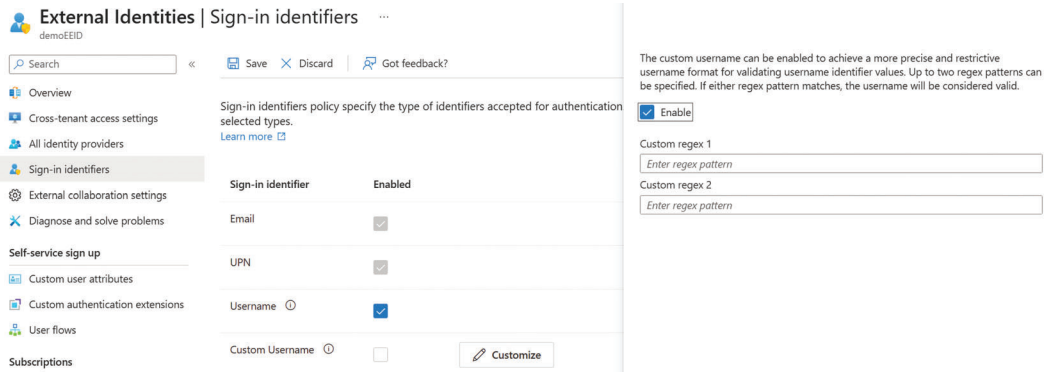


Figure 13.15: Enabling custom usernames

If the regex pattern is invalid or if the provided username does not match the regex pattern, the login will fail.

At the time of this writing, this option is only for signing in using the username and not signing up using the username. For sign-in using the username to succeed, a username must exist for the user in their user object in the directory. You must create users with both email and username as sign-in methods. For existing users, usernames can be added using the Microsoft Entra admin center or Microsoft Graph API.

The login experience for the users can be customized to provide them with a helpful hint indicating that they can sign in using email or username. This is explained in the section *Customizing neutral branding*. Refer to *Figure 13.29*.

Now when the users attempt to sign in, they will see the helpful hint on the sign-in page as shown below:

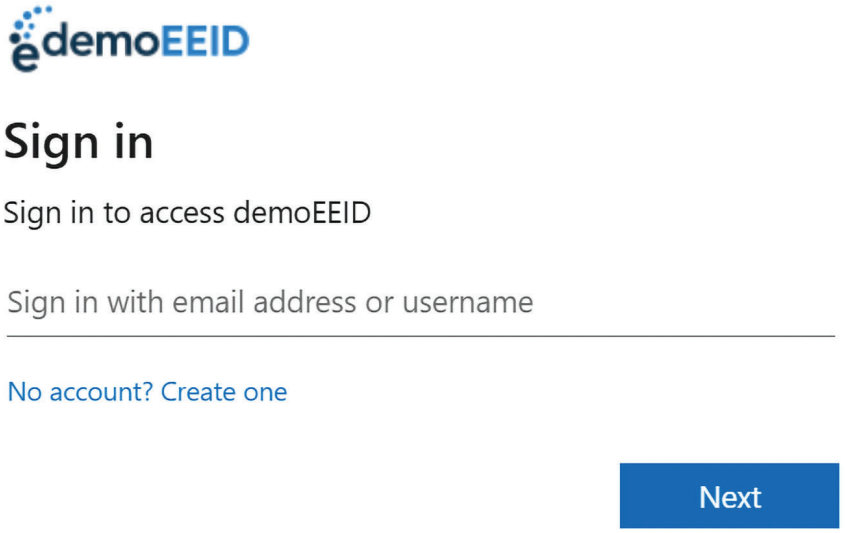


Figure 13.16: Customized sign-in hint

They will be able to sign in using either their username or email address.

Social identities

When users sign in to different applications, they must create user accounts specific to those applications. This leads to bad password practices like repeating passwords across applications. This is prone to credential stuffing attacks. Administrators also must maintain passwords for users, making them responsible for protecting identities from password spray and brute force attacks. Federation solves this problem by passing the responsibility of user authentication to an external IdP. External ID in external tenant supports federation with Google, Facebook, and Apple. When social identity federation is enabled, users get the option to sign-in using that identity on the sign-in and sign-up page as shown below:

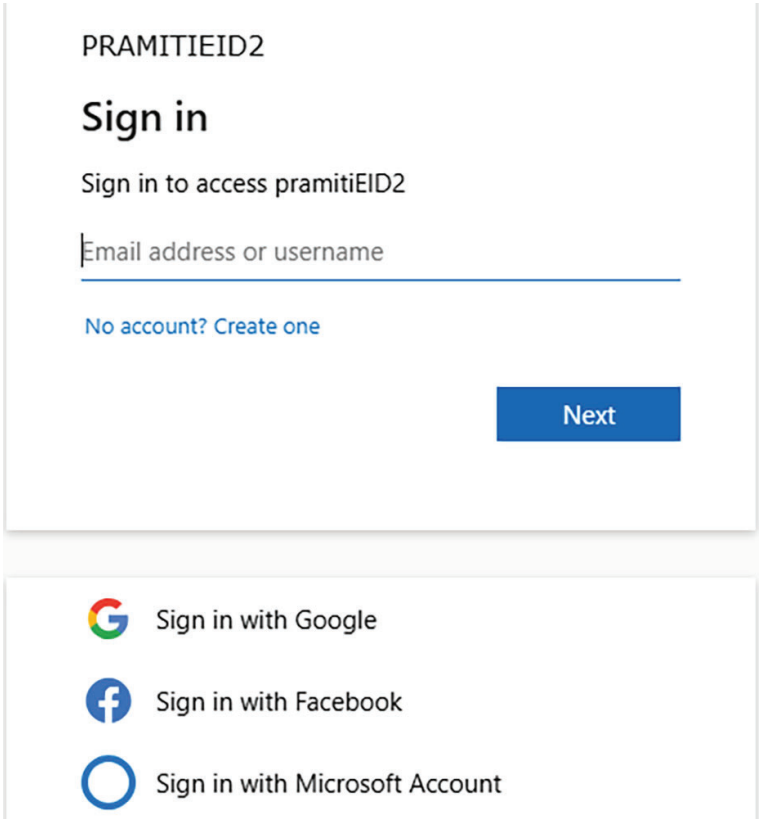


Figure 13.17: Social IdP sign-up

Users can click on the social identity of their choice, and they will be redirected to their IdP to complete authentication. Once the IdP authenticates the user, Entra External ID provides the user access to the application.

Note

Detailed steps to configure federation with each IdP are beyond the scope of this book.

Custom OIDC identity provider

Federation with a custom OpenID Connect IdP allows users to sign up and sign in using credentials from any federated external provider that adheres to the OpenID Connect protocol. This is done using the following steps.

1. In the Microsoft Entra admin center, switch to your Entra External ID tenant and navigate to **Entra ID | External Identities | All identity providers**.
2. In the right pane, click on **Custom | Add new | Open ID Connect**.
3. Enter the following details for your IdP.
    a. **Display name**: This is the name that will appear on the sign-in and sign-up screen like "*Sign in with IdP name*".
    b. **Well-known endpoint**: Also known as the metadata URI, this is the OIDC discovery URI for your IdP.
    c. **Issuer URI**: This is the entity of your IdP that issues access tokens for the applications.
    d. **Client ID**: This is the identifier your IdP uses to identify the registered application.
    e. **Client authentication**: This is the type of authentication method used to authenticate to your IdP using the token endpoint. The available options are
        1. `client_secret`: If this option is selected, the client secret must be provided.
        2. `private_key_jwt`: If this option is selected, the public key needs to be provided in the OpenID provider metadata.
    f. **Scope**: This is the information and permissions required from the IdP.
    g. **Response type**: This describes the information that is sent back in the initial call to your IdP. Only code response type is currently supported.

> **Note**
>
> Refer to the OpenID Connect documentation for more information on the above: `https://openid.net/specs/openid-connect-core-1_0.html`

The following example shows Microsoft Account configuration as an OIDC IdP. Click **Next: Claims mapping**.

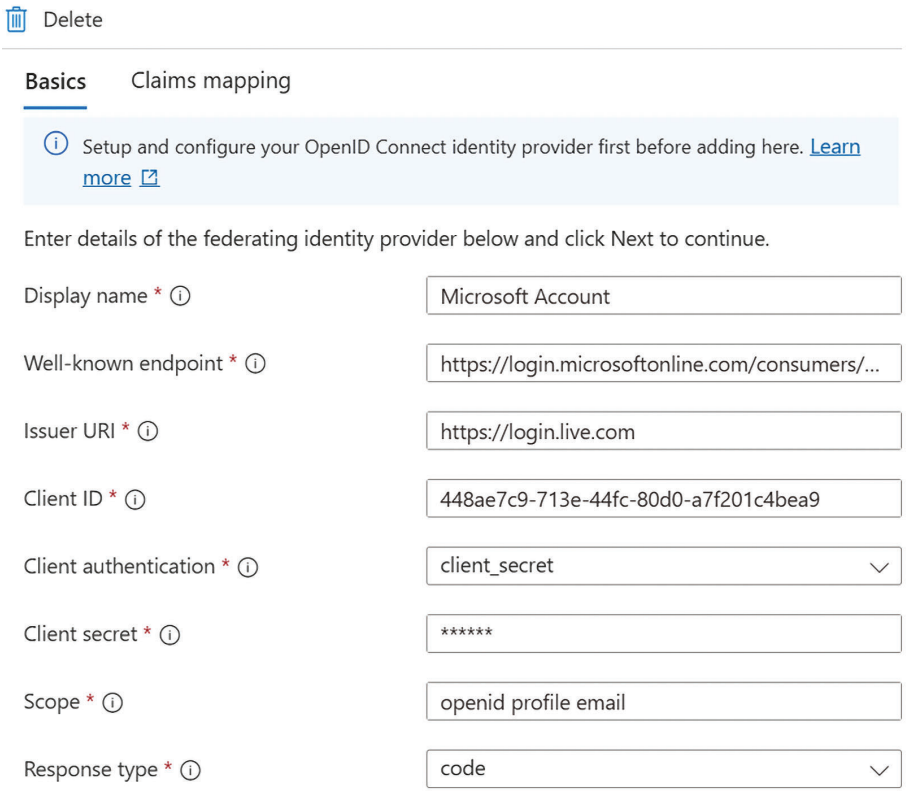


Figure 13.18: Configure custom OIDC provider

4. This is an optional step. OIDC claims are used to communicate information about the end user. They contain information that an IdP provides inside the ID token issued by the IdP. ID tokens uniquely identify a user and provide information about the user during sign-up. This information is stored in the user object in Entra ID. The following claims are available to be mapped. Once mapping is configured, MSA will send the mapped attributes to Entra ID during sign up. Entra ID will store those attributes in the user object. Click **Next: Review**.

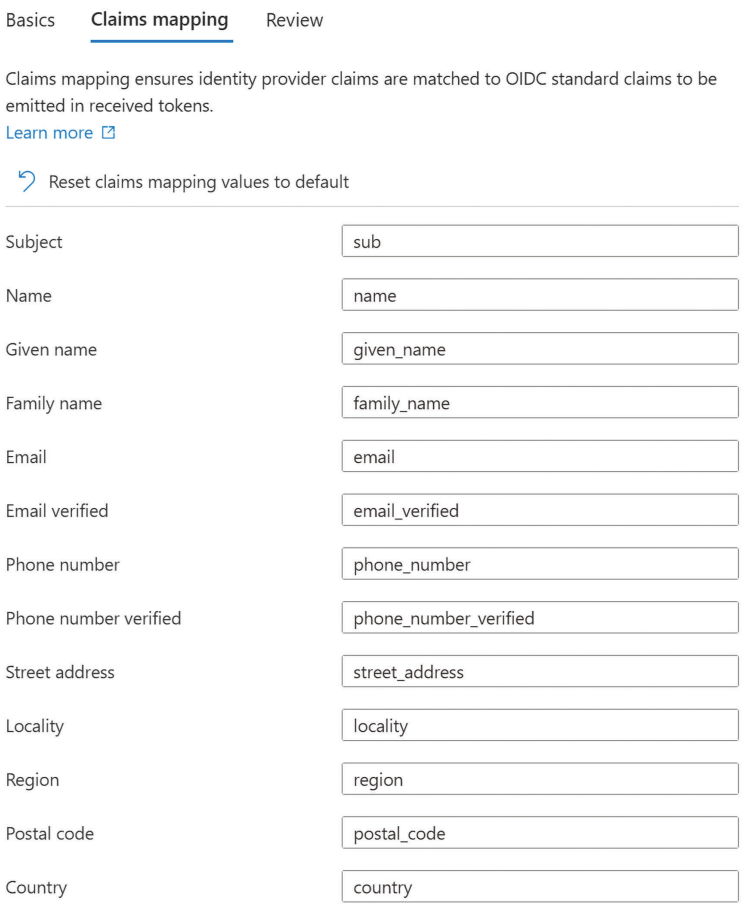


Figure 13.19: Claims mapping

5. On the **Review** page, review your selections and click **Create**.

When federating with external IdPs like social identities or custom OIDC providers, users see the Microsoft sign-in page and then select their IdP. Administrators can include the `domain_hint` parameter in the sign-in URL to send users directly to the sign-in page for the IdP associated with that domain. For example, you can use `domain_hint=facebook`, `domain_hint=Google` or `domain_hint=apple` to direct users to the respective sign-in pages. For custom OIDC IdPs, use the domain part of the **Issuer URI** as `domain_hint=<issuer_uri>`.

Custom SAML/WS-Fed

Entra External ID can federate directly with SAML or WS-Fed IdPs. This enables users from organizations using these IdPs to access applications registered in your external tenant using

their own credentials. They are redirected to their IdP and once authenticated, they are returned to Entra. Multiple domains can be associated with a single federation configuration. These domains can be **verified** or **unverified**.

- **Unverified**: These domains are not DNS-verified in Microsoft Entra ID.
- **Unmanaged**: Also called email-verified or viral, these domains are created when a user signs up using a domain that does not exist.
- **Verified**: These domains are DNS-verified in Microsoft Entra ID.

If an external user has already signed up, their authentication method does not change if federation is set up later. They continue using their original authentication method.

For SAML/WS-Fed IdP federation to work, it must be set up both in your organization and the organization using the SAML/WS-Fed IdP (partner organization).

Following are the steps to set up SAML/WS-Fed IdP federation:

1. **Determine if the partner organization needs to update their DNS text records**: This is required if the passive authentication URL does not match the target domain or a host within the target domain. For example, if you are federating with `tailspintoys.com` and their passive authentication URL is `https://www.tailspintoys.com` or `https://sts.tailspintoys.com`, no change is needed. However, if their passive authentication URL is `https://tailspingroup.com` or `https://tailspintoys.com.au`, then they must add a TXT record to their domain's DNS in the following format:

   ```
   tailspintoys.com.   IN    TXT DirectFedAuthUrl=https://
   tailspingroup.com
   ```

2. **Configure the partner's IdP**: For federation to work, Microsoft Entra ID requires that the partner sends certain attributes and claims, which must be configured at the partner IdP. Refer to `https://learn.microsoft.com/en-us/entra/external-id/direct-federation#to-configure-a-saml-20-identity-provider` for the required attributes for SAML and WS-Fed IdPs.
3. **Configure SAML/WS-Fed IdP federation at your organization**: To complete the configuration at your end you will require the Issuer URI of the partner IdP, the passive authentication endpoint of the partner IdP and the certificate. Follow the steps below:
   a. Login to the Microsoft Entra admin center and switch to the external tenant as an **External Identity Provider Administrator**.
   b. Navigate to **Entra ID | External Identities | All identity providers**.

c. Click **Custom | Add new | SAML/WS-Fed**.

d. In the flyout pane, enter a **Display name** and select the **Identity provider protocol** as **SAML** or **WS-Fed**. If you have a file that contains the metadata information, select **Parse metadata file** under **Select a method for populating metadata** and upload the metadata file. If not, select **Input metadata manually** and enter the details manually. Once done, click **Save**. Refer to the following screenshot.

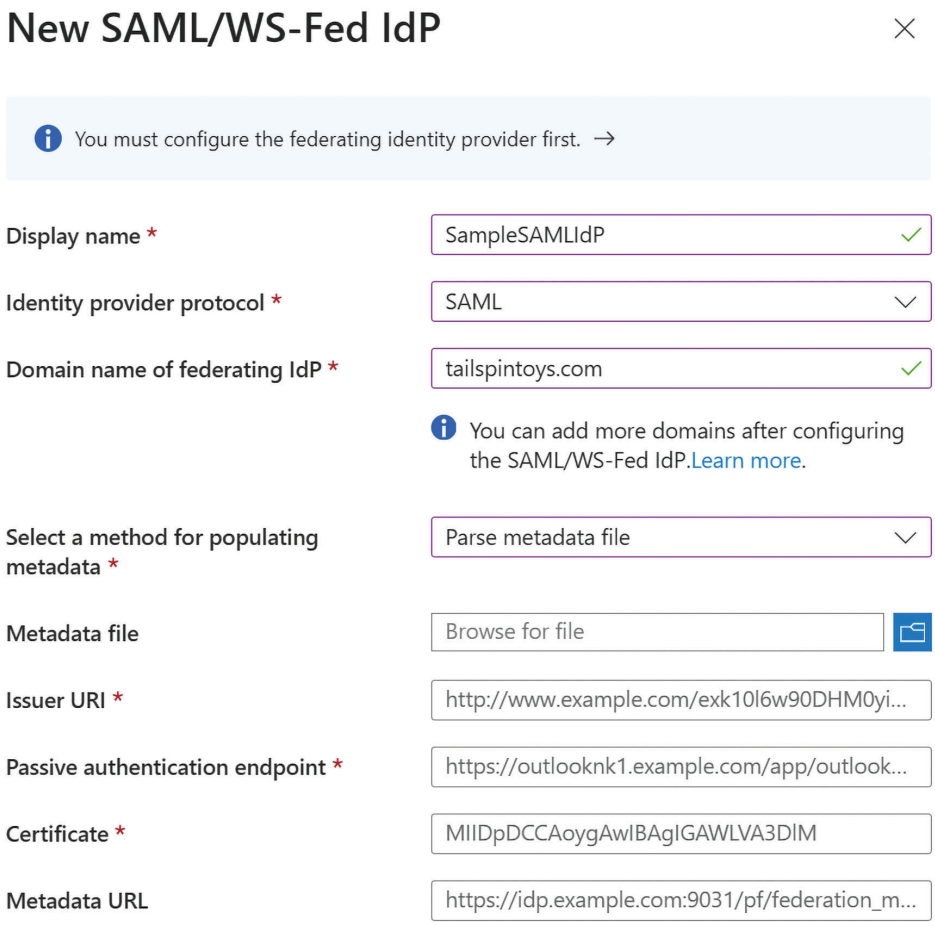


Figure 13.20: Configure SAML/WS-Fed IdP

The federation will be added. Additional domains can be added to this federation if required. Users will see the Microsoft sign-in page first and can then select their IdP. Include the `domain_hint` parameter to send the user to their IdP sign-in page directly. For SAML IdPs, use the syntax `domain_hint=<domain name of the federating IdP>`.

Registering applications in Entra External ID

For users to be able to access your application, you must register your application with Entra ID. Registering the application with Entra External ID creates a unidirectional trust relationship between your application and Entra External ID. The application trusts Entra External ID and not the other way around. Once the application object is created, it cannot be moved to another tenant.

Registering an OIDC application

Entra External ID supports registering applications that use the OIDC protocol. To register an OIDC application in the external tenant, follow the steps below:

1. In the Microsoft Entra admin center, switch to your Entra External ID tenant and navigate to **Entra ID | App registrations | New registration**.
2. Enter a name for the application. Under **Supported account types**, choose who can use the application. The following options are available.
    a. **Single tenant only - <tenant name>**: Select this option if you want your application to be accessed only by users and guests in your tenant.
    b. **Multiple Entra ID tenants**: This option is ideal for multitenant applications that you want to make available to users in any Microsoft Entra tenant.
    c. **Any Microsoft Entra ID tenant + Personal Microsoft accounts**: Using this option makes your multitenant app available for users in any Microsoft Entra tenant and Microsoft personal accounts.
    d. **Personal accounts only**: Use this option for applications that you want to make available to personal Microsoft accounts only.

3. Under Redirect URI select the type of application. The following options are available.
    a. **Public client/native (mobile & desktop)**: Use this option to register a mobile application.
    b. **Web**: Use this option to register a web application.
    c. **Single-page applications (SPA)**: Use this option to register a single-page application. SPA is a type of web application that loads one HTML page once, and then dynamically updates the content on that page without reloading the entire page.

    Click **Register** to create the app registration. Refer to the following screenshot.

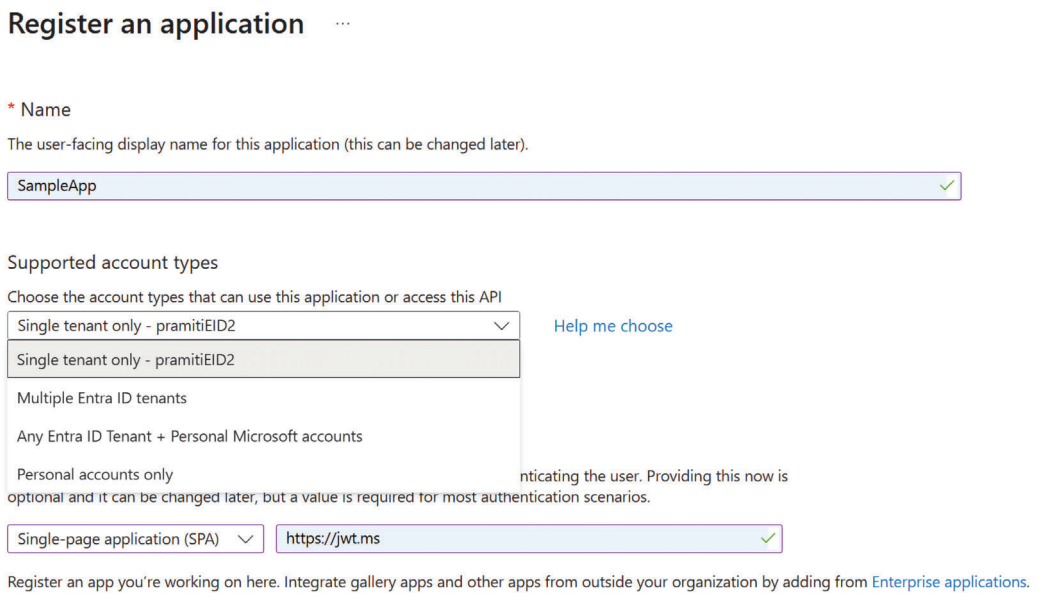


Figure 13.21: Register an app

The registered application gets `User.Read` API permission. However, customer users may not be able to grant permissions for the app. You must grant admin consent for the app on behalf of the users. Under **App registrations**, select the newly created app. Click on **API permissions** and click **Grant admin consent for <tenant name>**. In the box that pops up, click **Yes** to confirm. Once consent is granted, it will show up in the status column as shown in the following screenshot:

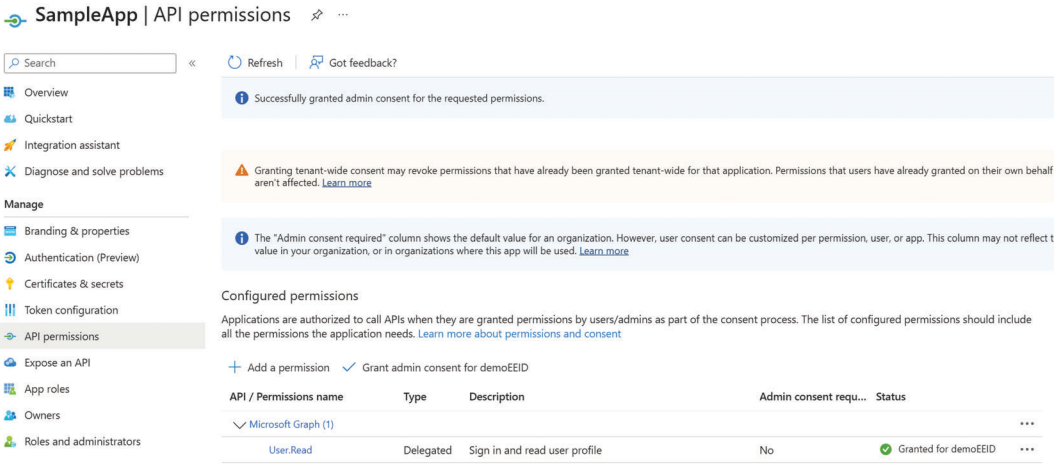


Figure 13.22: Admin consent granted

A trust relationship is now created between the app and Entra External ID.

Registering a SAML application

You can register a SAML application by using the Enterprise apps feature. The following are the steps.

1. In the Microsoft Entra admin center, switch to your Entra External ID tenant and navigate to **Entra ID | Enterprise apps | New application | Create your own application**.
2. Type a name for your application.
3. Select the option **Integrate any other application you don't find in the gallery (Non-gallery)** and click **Create**.
4. The application will be added, and the Overview page will open.
5. In the left pane, click on **Properties** and toggle the **Assignment required?** toggle to **No**. Now the users will be able to sign in using sign-in and sign-up flow. Click **Save**.
6. Click on **Single Sign-on** and select **SAML**. On this page you can either **Upload metadata file** containing configuration information for your app or manually make the required changes. Note that there is no download button next to Federation metadata XML. The download button is available only in workforce tenants and not in external tenants. To download this file, copy and paste the URL in a browser.

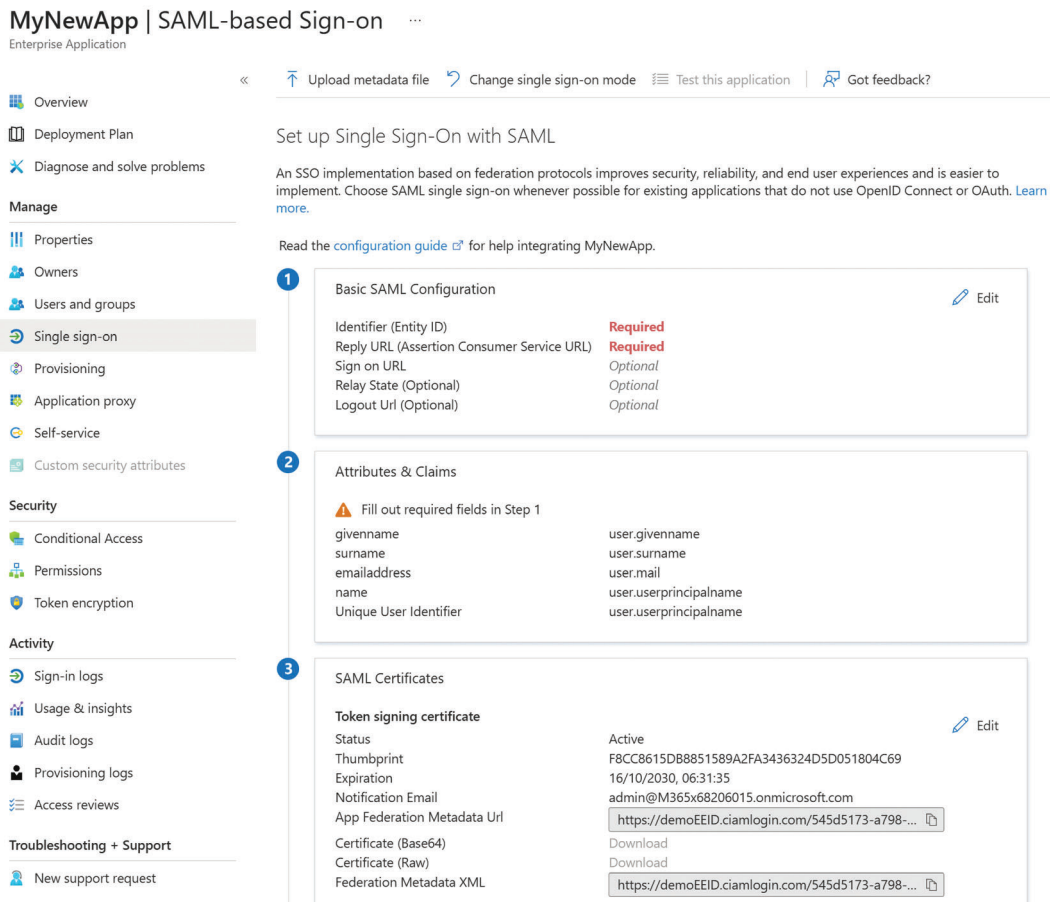


Figure 13.23: SSO for SAML app

Finally, you can test using the Test button. This will confirm that your currently logged in account is able to log in.

Adding an enterprise application

Enterprise applications are **Software-as-a-Service (SaaS)** applications that are integrated with Microsoft Entra ID. Microsoft Entra ID has a wide range of pre-integrated SaaS

applications. This enables support for SSO and authentication. Following are the steps to add an enterprise application to Entra External ID.

1. In the Microsoft Entra admin center, switch to your Entra External ID tenant and navigate to **Entra ID | Enterprise apps | New application | Create your own application**.
2. Start typing the name of the application you want to add, such as *Salesforce*. Select the application from the list and click **Create** as shown in the following screenshot:

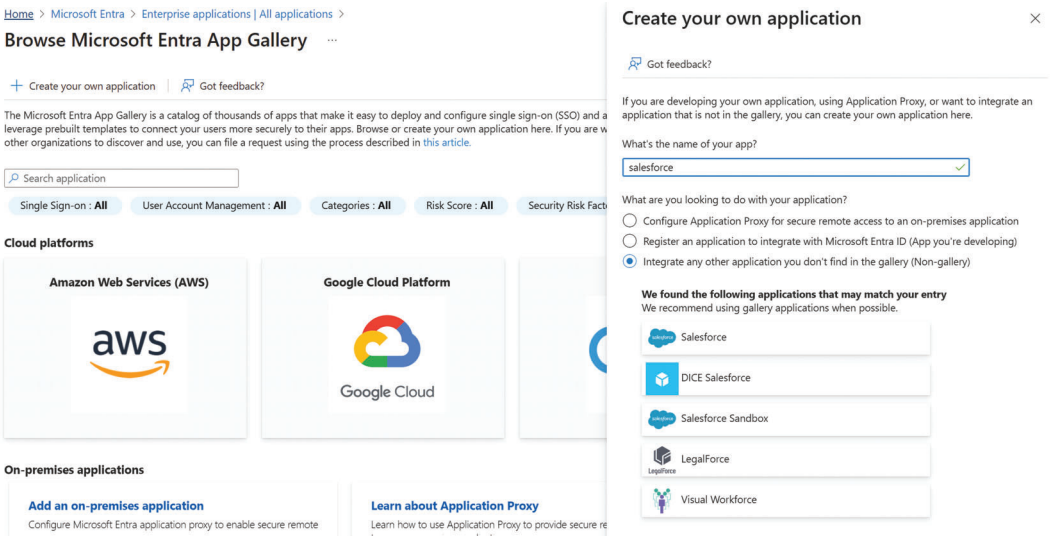


Figure 13.24: Register application

The application will be added to the Enterprise apps list. You will have to configure SSO settings in the application. These settings are different for each application and are beyond the scope of this book. As a best practice, it is also recommended to add owners to the application.

Creating a user flow

To enable self-service sign-up to applications, administrators can use user flows. These user flows define the user's journey, their sign-in methods, and the information they must provide to sign up to applications. Administrators can enable users to create a local account in Entra External ID or sign up using social identities or custom OIDC and SAML IdPs. Users can also be required to provide some information that can be stored in built-in or custom user profile attributes. Following are the steps to create a user flow.

1. In the Microsoft Entra admin center, switch to your Entra External ID tenant and navigate to **Entra ID | External identities | User flows | New user flow**.

2. Give the user flow a meaningful **Name** and select the **Identity providers** that you want to enable users to sign-in with as shown in *Figure 13.25*. By default, only the **Email Accounts** identity provider shows up. For Apple, Facebook and others to show up in this list, enable federation with the IdPs using the steps in the *Configuring identity providers* section.
3. Under **User attributes** click on **Show more...** to select the list of attributes you want to collect from the users at sign up. Select the appropriate attributes and click **Ok**. Refer to the following screenshot:

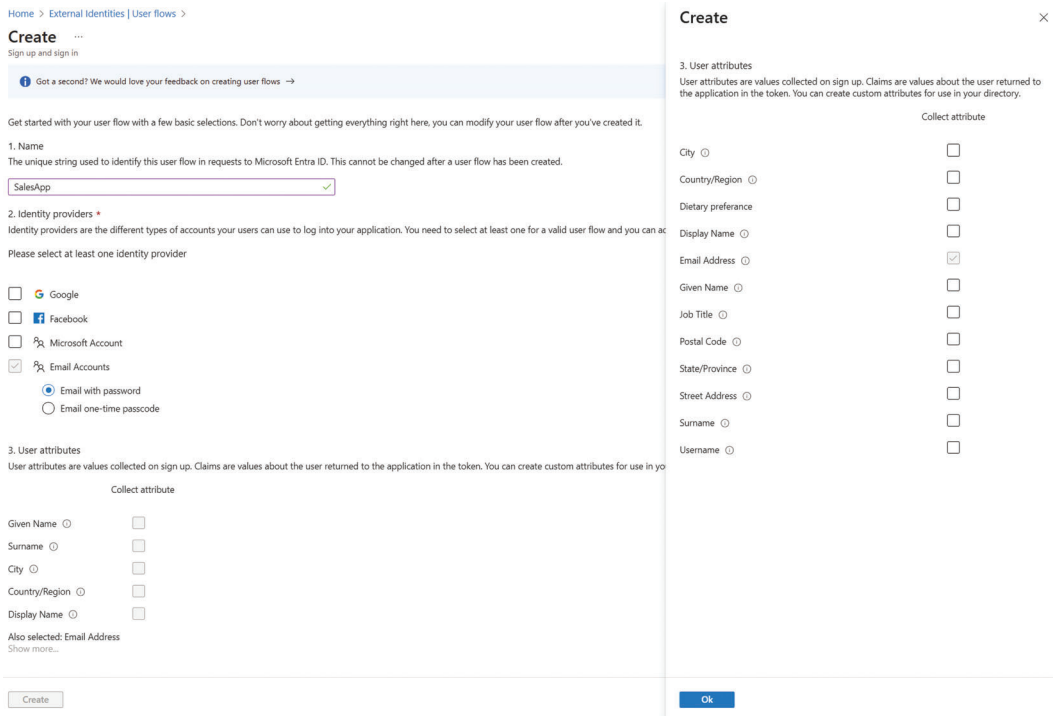


Figure 13.25: Create user flow

4. Click **Create** to create the user flow.

Once the flow is created, applications will need to be added to the user flow to enable self-service sign-up for users. One application can be added to only one user flow; however, one user flow can be associated with multiple applications. The following are the steps to add an application to a user flow.

1. In the Microsoft Entra admin center, switch to your Entra External ID tenant and navigate to **Entra ID | External identities | User flows**
2. Select the user flow. In the left pane, click on **Applications | Add application**.
3. Pick the application from the list and click **Select**.

You can test the user flow by clicking on **Run user flow**. If the user flow is associated with multiple applications, select the application for which you want to test from the **Application** drop-down as shown below.

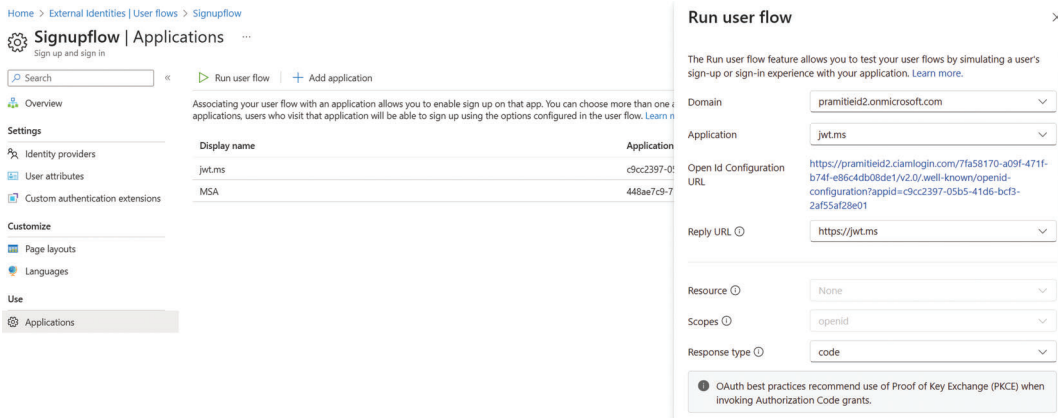


Figure 13.26: Run user flow

Click **Run user flow**. The application will open in a new tab. Use a test user account to test the user's sign-up experience.

Note

In Entra External ID, the same flow is used for both sign-up and sign-in experiences. In some scenarios, administrators may pre-create user accounts and may want to prevent users from self-service sign-up. Sign-up can be disabled from the user flow using Microsoft Graph API. Refer to `https://learn.microsoft.com/en-us/entra/external-id/customers/how-to-disable-sign-up-user-flow` for detailed steps.

Customization

Entra External ID enables organizations to customize the look and feel for users using your applications. This helps create brand stickiness and loyalty. By default, Microsoft creates neutral branding for all tenants. This does not include any Microsoft branding. Organizations can personalize this to suit their requirements.

Customizing neutral branding

Administrators can customize the neutral branding by adding a custom background image or color, favicon, header, and footer. If custom branding fails to load, the sign-in page automatically falls back to the neutral branding. To customize the neutral branding, follow the steps below.

1. In the Microsoft Entra admin center, switch to your Entra External ID tenant and navigate to **Entra ID | Custom branding**.
2. In the right-pane, click **Customize** under **Default sign-in experience**.
3. On the **Basics** page, select an image for **Favicon** and **Background image**. You can also change the **Page background color**. Click **Next: Layout**.
4. On the **Layout** page, you can choose between a **Full-screen background** or a **Partial-screen background**. You can also choose to show or hide **Header** and **Footer**. On this page you can also upload a custom CSS that replaces the default styling. Click **Next: Header**.

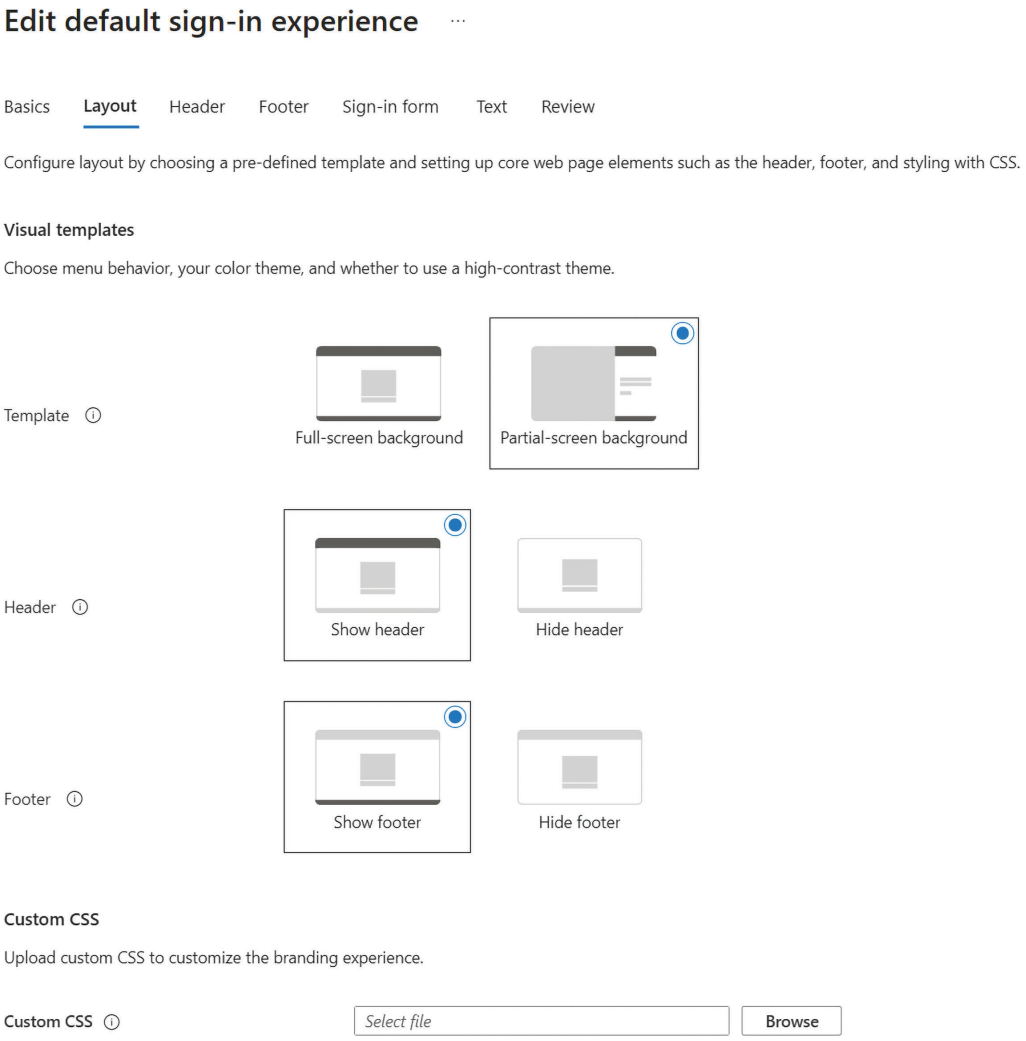


Figure 13.27: layout page

5. On the **Header** page upload a header image. Click **Next: Footer**.

6. On the **Footer** page you can choose to show **Privacy & Cookies** and **Terms of use**. You can enter a **Display text** and give a **URL** for both. Click **Next: Sign-in form**.

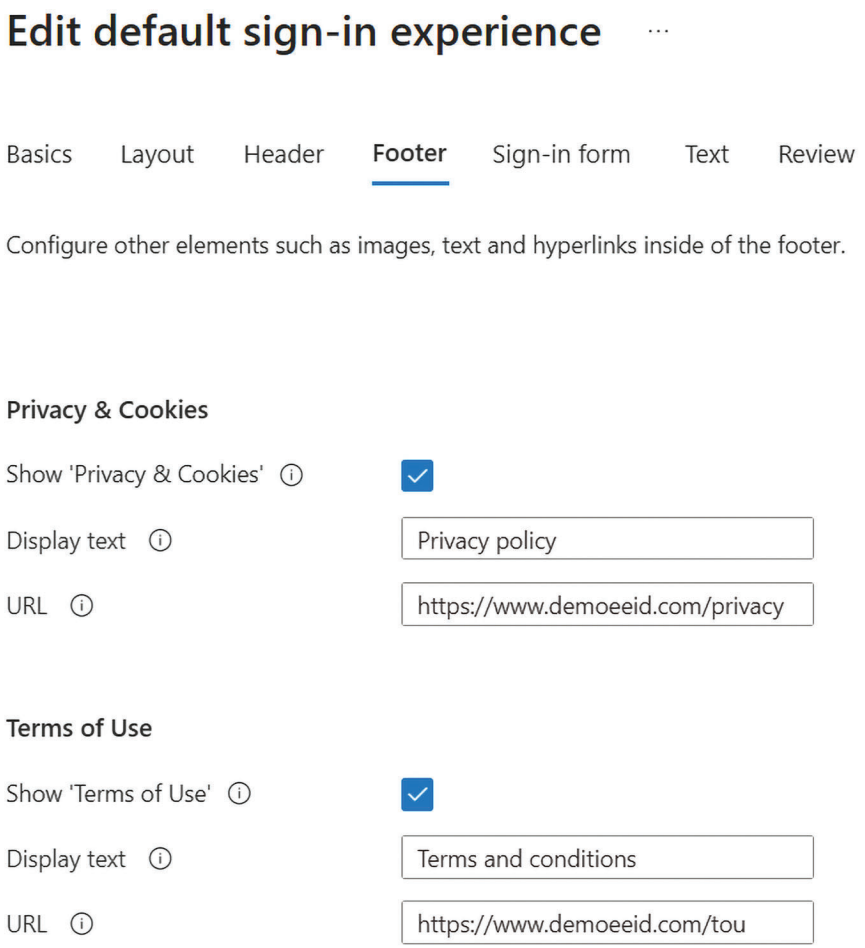


Figure 13.28: Footer page

7. There are several options on this page. You can add a **Banner logo**, customize the **Username hint text** and **Sign-in page** text. Check the box next to **Show self-service password reset** to show the **Forgot password?** link on the password page during sign-in. You can also provide a custom password reset URL instead of the default Microsoft link. **Under Account collection display text**, enter a text to replace the default "*Can't access your account*" text. Under **Password collection display text** enter a text to replace the default "*Forgot password*" text. Click **Next: Text**.

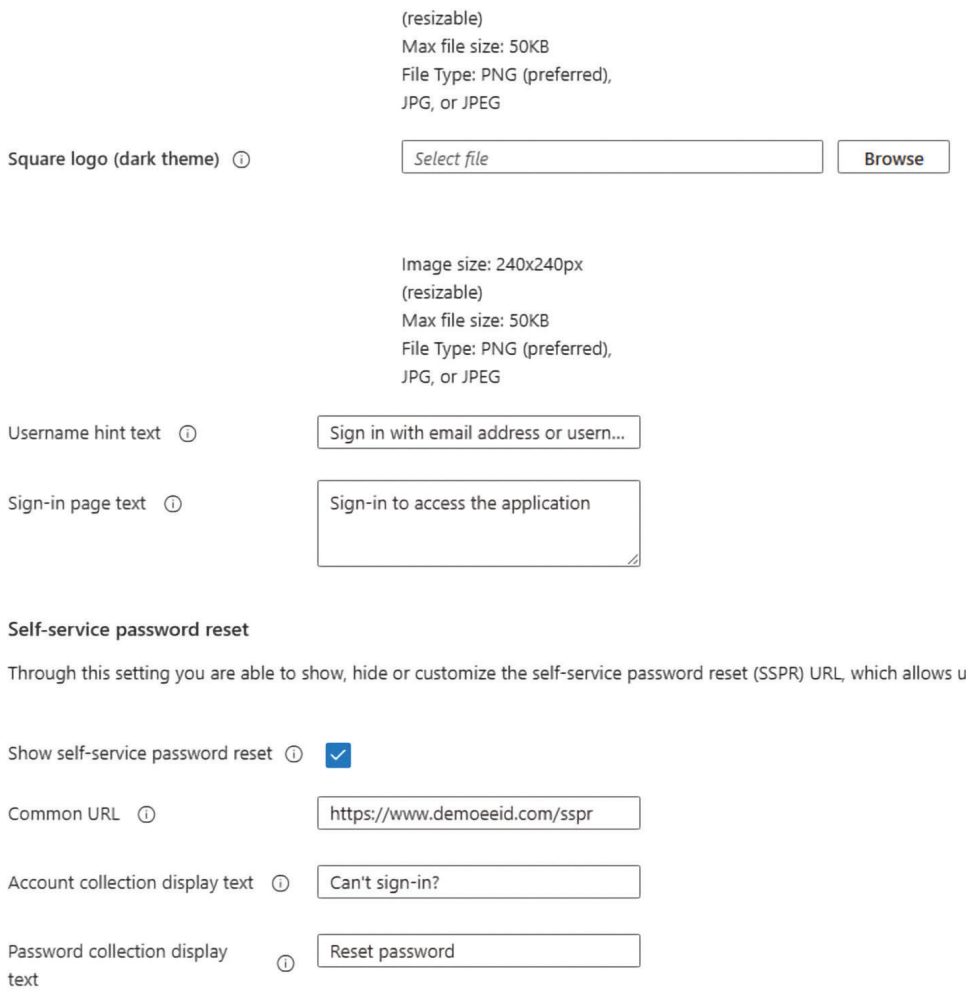


Figure 13.29: Sign-in form page

8. On the **Text** page, you can customize the labels of attributes you collect from users during sign-up. The following options are available.
    a. **Attributes**: Override the default values of attributes. For example, you can change the label "*Given name*" to "*First name*" and "*Surname*" to "*Last name*".
    b. **Attribute collection**: Add a new attribute to collect during sign-up.
    c. **Sign in**: Add a custom text for the sign-in page.
    d. **Sign up**: Add a custom text for the sign-up page.
    e. **Sign-in/up one time code**: Add a custom text for the title.
9. Click **Add Custom Text** and pick the relevant option from the **Text to customize** box. Make the necessary changes and click **Add**. The following figure shows text customization for **Attributes**. Make the changes for the others as required and click **Next: Review**.

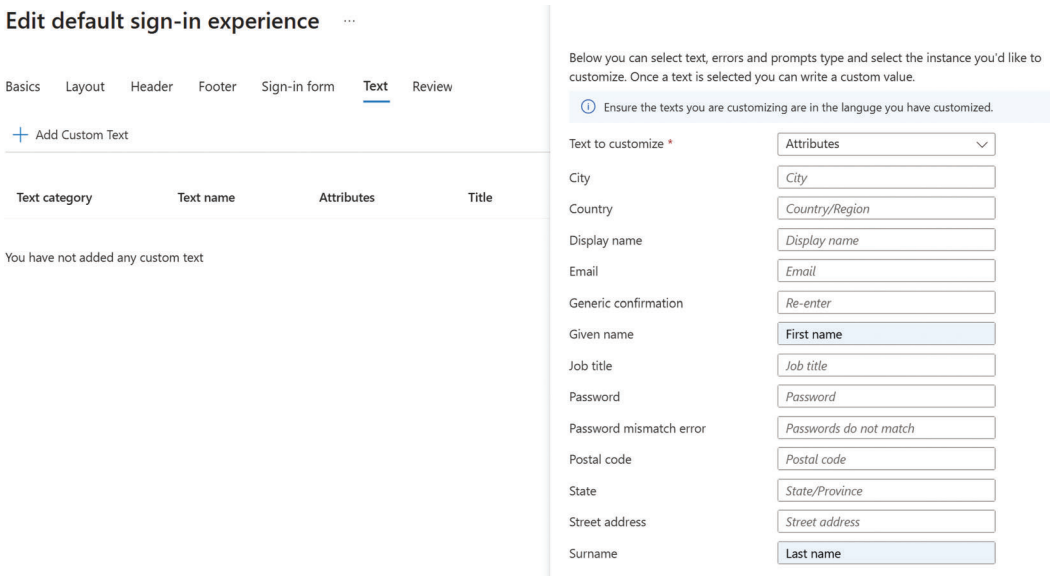


Figure 13.30: Add custom text

10. On the **Review** page, click **Save**.

These customizations will now apply to all applications registered with Entra External ID. The following page shows the customized elements.

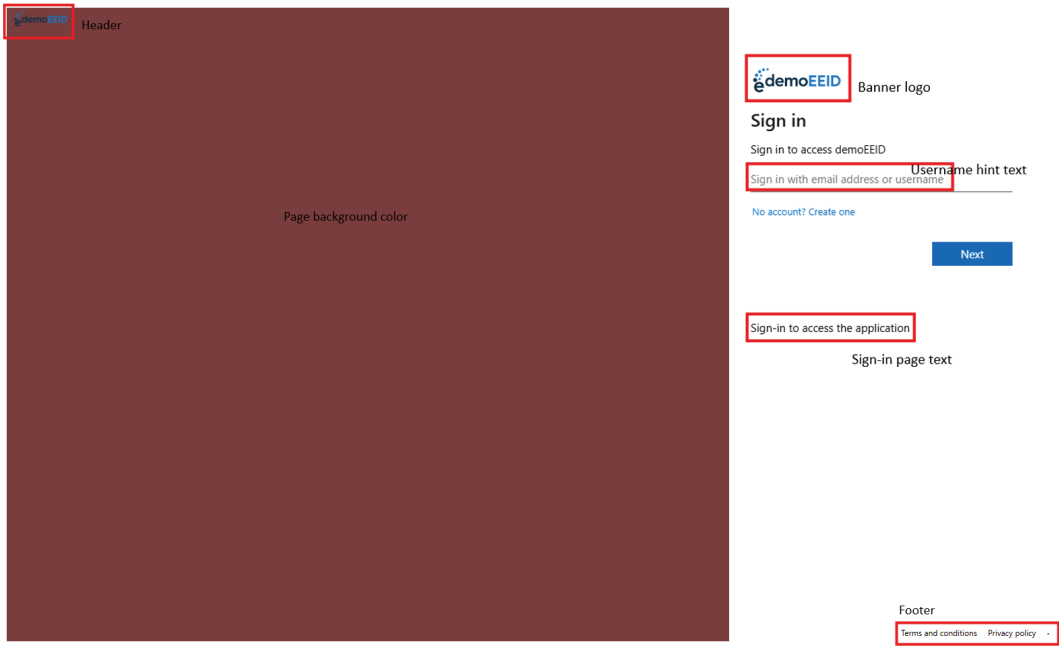


Figure 13.31: Customized sign-in page

Global organizations operating in multiple countries may want to provide more personalized experiences to their customers by customizing the browser language for them. This can be done by navigating to **Entra ID | Custom branding | Company branding | Browser language customizations | Add browser language**. Select the language you want and then customize the rest of the user experience as described in the above steps.

Configuring branding themes

Sometimes organizations want to create different sign-in experiences for different applications registered in the same Entra External ID tenant. Using themes, each application can have its own header, footer, page background color or picture, and favicon. Branding themes override any settings in the default branding or neutral branding. For elements not defined in the branding themes, default elements are displayed. Up to 5 branding themes can be created per tenant. Multiple applications can use a single theme. Follow the steps below to create a new theme.

1. In the Microsoft Entra admin center, switch to your Entra External ID tenant and navigate to **Entra ID | Custom branding | Branding themes**. In the right-pane click on **Get started**.
2. On the **Themes** page click on **Create new theme**.

3. Give a **Name** to the theme and click **Add applications** to select the applications that will use this theme. Click **Next: Layout**.
4. The rest of the steps will take you through configuring layout, header, footer, background image and color, favicon, logo and custom text. Make the necessary changes and create the theme.

More applications can be added to this theme after it is created.

Customizing tokens

Using built-in and custom user profile attributes, administrators can collect information from users during sign-up as described in the *User profile attributes* section. This information can be included in the token to be sent to the application. The application might use this information to function as designed or to present the relevant information to the users. The following are the steps to add attributes to a user token.

1. In the Microsoft Entra admin center, switch to your Entra External ID tenant and navigate to **Entra ID | Enterprise apps**.
2. Select the application from the list and click on **Single sign-on**. In the right pane, click on **Edit** next to **Attribute & Claims**.
3. Click on **Add new claim** and enter a **Name** for the claim.
    a. To add a built-in attribute, select **Attribute** under **Source**. Under **Source attribute**, select the built-in attribute from the list and click **Save**.
    b. To add a custom attribute, select **Directory schema extension** under **Source**. Select **b2c-extensions-app** from the **App registrations** list and click **Select**. From the list of attributes, select the required attribute and click **Add** as shown below.

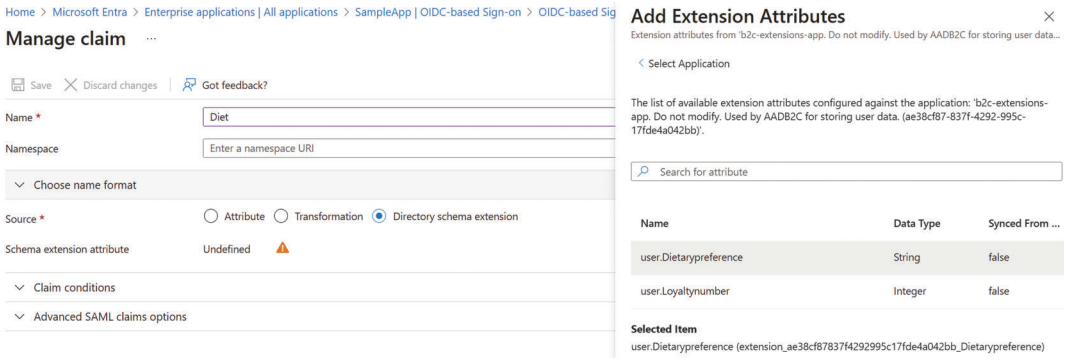


Figure 13.32: Add attributes to token

4. Click **Save**.

These attributes will now be included in the token that Entra ID sends to the application. The application can use this information in various ways. For example, your application might use the dietary preference attribute to present relevant food options to the customer.

Configuring optional claims

Tokens returned by Entra ID are intentionally kept small to ensure optimum performance by clients that request them. Due to this, several claims are no longer included by default in the tokens and must be added on a per-application basis if required. The following are the steps to add optional claims.

1. In the Microsoft Entra admin center, switch to your Entra External ID tenant and navigate to **Entra ID | App registrations**.
2. Select the application and click **Token configuration | Add optional claim**.
3. In the flyout pane, select the **Token type** and select the claims you want to add as shown below.

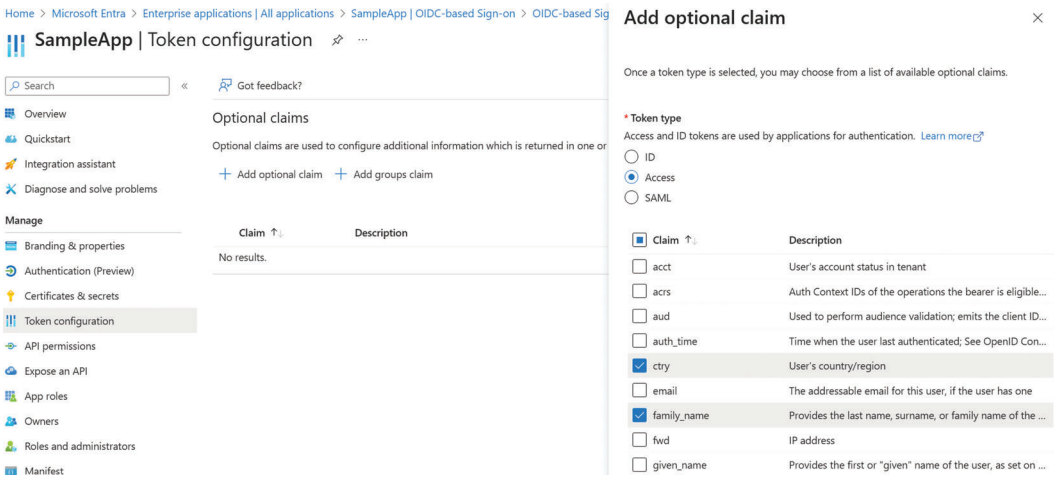


Figure 13.33: Add optional claims

4. Click **Add**.

In addition to the standard optional claims, tokens can also include Microsoft Graph extensions.

Optional claims include built-in and custom user profile attributes. They help in attaching more information to the token that can be used by the application.

Adding custom URL domains

When you create an Entra External ID external tenant, you get a default domain name like `<domainname>.onmicrosoft.com`. You can create a customized and branded experience for your users by adding custom URL domains. To do this, you must have a custom domain name added and verified in your external tenant. This is explained in *Chapter 3, Implementing Microsoft Entra ID*. You can also verify subdomains like `login.pramlabs.com` or `portal.pramlabs.com`.

Once you have the subdomain added and verified, you can associate it with a custom URL domain using the following steps.

1. In the Microsoft Entra admin center, switch to your Entra External ID tenant and navigate to **Entra ID | Domain names | Custom URL domains | Add Custom URL domain**.
2. Under **Add Custom URL domain** select the verified domain and click **Add**.

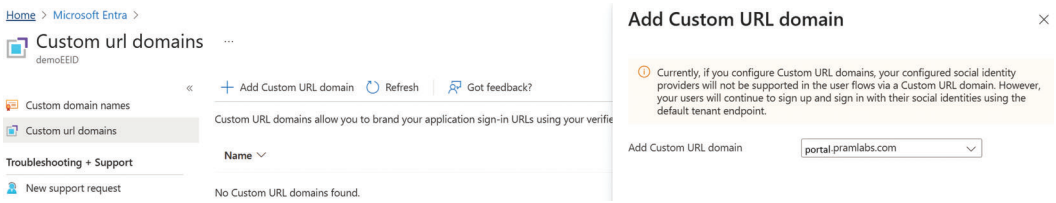


Figure 13.34: Add custom URL domain

Now a reverse proxy like **Azure Front Door (AFD)** can use the custom URL domain to direct sign-ins to your application. The following are the steps to configure Azure Front Door.

1. Sign in to `https://portal.azure.com` and select the subscription in which you would like to create the Azure Front Door instance. This could be the same subscription where you created your external tenant or another subscription.
2. Create an Azure Front Door profile with the following settings:
    a. **Subscription**: Select the subscription where you would like to create your Azure Front Door instance.
    b. **Resource group**: Select the resource group where you would like to create your Azure Front Door instance.
    c. **Name**: Give a unique name.
    d. **Tier**: Select the appropriate option depending on your requirements.
    e. **Endpoint name**: Give a globally unique name. The **Endpoint hostname** will be automatically generated.
    f. **Origin type**: Select **Custom**.
    g. **Origin host name**: Enter your tenant's name in the format `<tenant-name>.ciamlogin.com`.
    h. Leave the **Caching** and **WAF policy** empty.

    Refer to the following screenshot, for example.

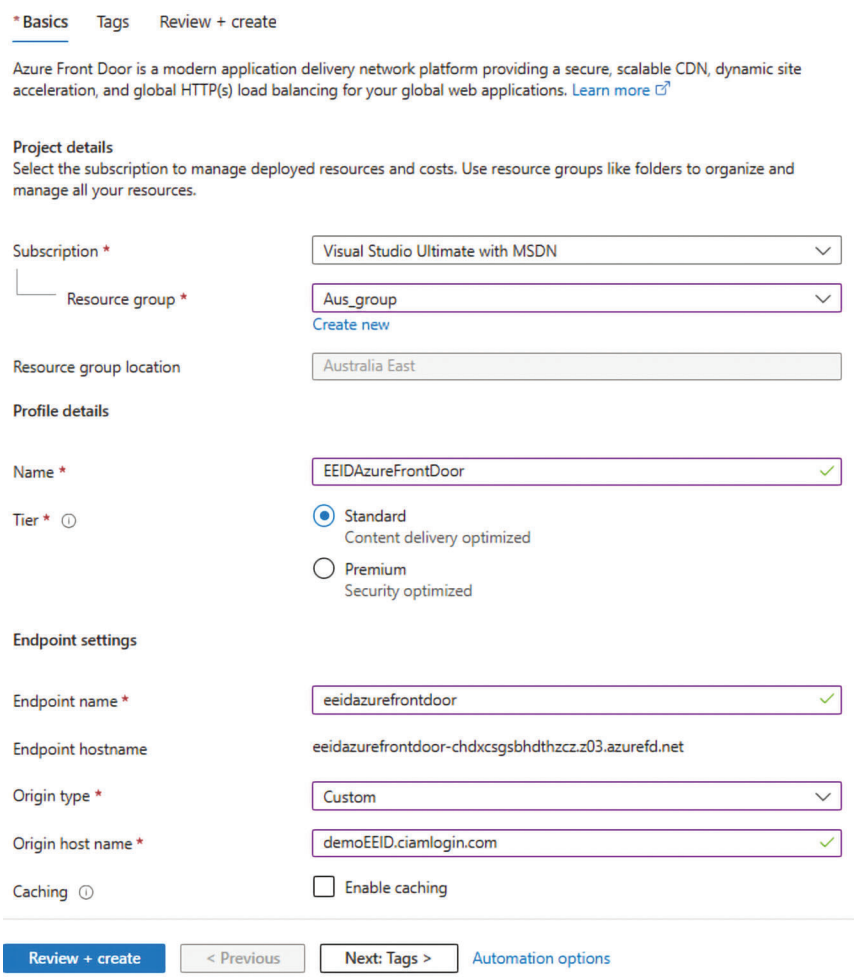


Figure 13.35: Create an AFD profile

3. Click **Review + create** to create the AFD profile.
4. Once created, click on **Go to resource** and in the left pane navigate to **Settings | Origin groups**.
5. Click on the name of the origin group and in the flyout pane click on the **Origin host name** as shown below:

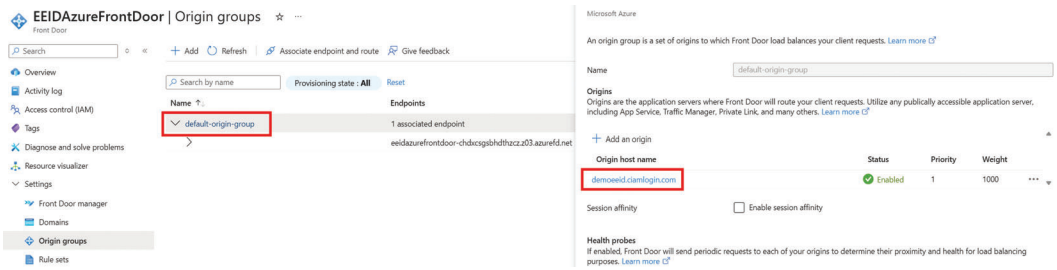


Figure 13.36: Configure AFD

6. Ensure that the **Host name** and **Origin host header** have the same value as shown below. Click **Apply** and **Update**.

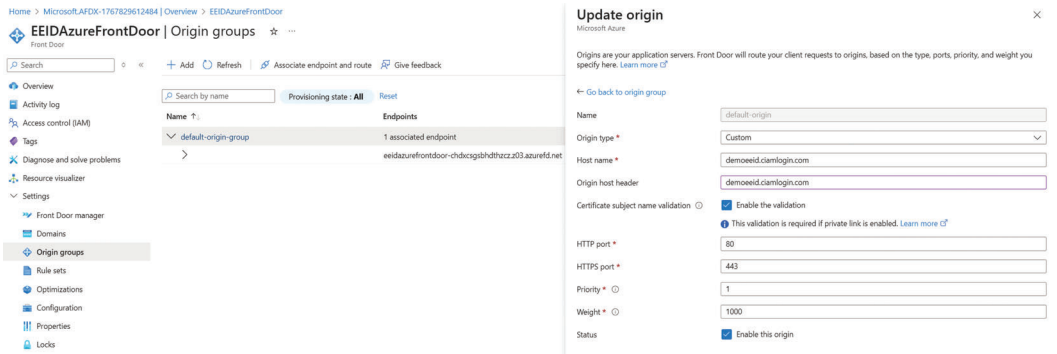


Figure 13.37: Update settings

When you create an AFD profile, Azure automatically generates a system-assigned endpoint with a name like `eeidazurefrontdoor-chdxcsgsbhdthzcz.z03.azurefd.net`. This is the public endpoint of your AFD instance. It is globally distributed and highly available. It is the entry point for all traffic before it reaches the backend. Although this is a fully functional endpoint, it is not suitable for production use because it is not branded and does not represent your organization. It is also not secure by default. To make it more user-friendly, it needs to be mapped to a simple URL like `portal.pramlabs.com` which can be easily remembered and represents your brand. Following are the steps to map the system-assigned endpoint to a user-friendly URL.

1. Create a CNAME record with your domain registrar that maps your URL (`portal.pramlabs.com`) to the system-assigned URL (`eeidazurefrontdoor-chdxcsgsbhdthzcz.z03.azurefd.net`). When a user enters `portal.pramlabs.com` in their browser, they are redirected to `eeidazurefrontdoor-chdxcsgsbhdthzcz.z03.azurefd.net`.

2. To prove ownership of your domain, create a CNAME record with your domain registrar that maps the special subdomain `adverify` (`adverify.portal`) to your AFD profile (`afdverify.eeidazurefrontdoor-chdxcsgsbhdthzcz.z03.azurefd.net`). Azure checks this special subdomain to verify that you have the authority to bind `portal.pramlabs.com` to your AFD profile. Once Azure sees this record, it knows the domain is legitimately yours.
3. Add the `portal.pramlabs.com` domain to your AFD profile.
    a. Sign in to `https://portal.azure.com` and go to your AFD instance.
    b. In the left pane navigate to **Settings | Domains**. In the right pane, click **Add**.
    c. In the **Add a domain** page, make the following selections and click **Add**.

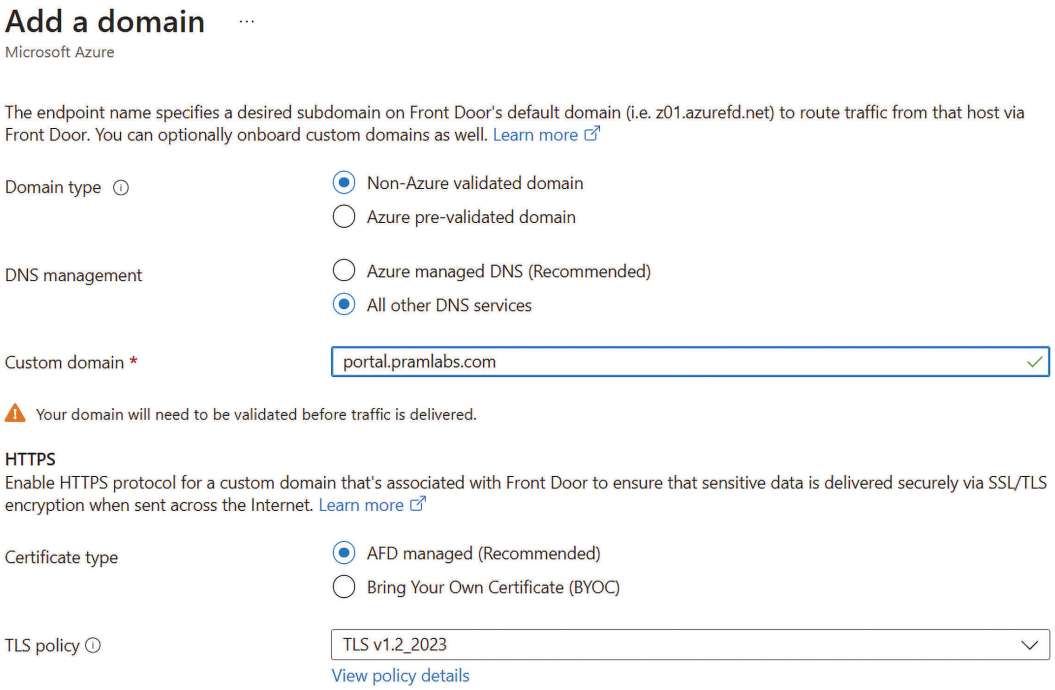


Figure 13.38: Add a domain in AFD

    d. Azure might ask you to create a TXT record with your domain registrar as additional proof of ownership. Get the details from the portal and create the TXT

record. This TXT record is like a signature—a cryptographic handshake between your DNS provider and Azure.

e. Soon your domain's **Validation state** will show **Approved** in the Azure portal as shown below:



Figure 13.39: Domain approved

4. The domain now needs to be associated with an endpoint and a route. Click on the three dots on the far right and click **Associate**. In the flyout pane, select the endpoint and route as shown below and click **Associate**.

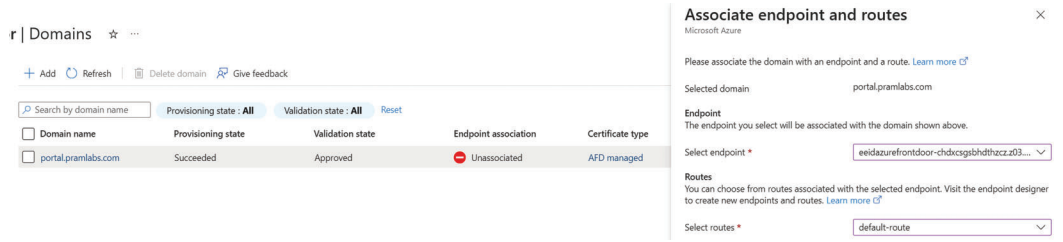


Figure 13.40: Associate endpoint

Once this association is created, all traffic for `portal.pramlabs.com` will be redirected to the AFD endpoint. You can test this by running the user flow for your application and replacing the `<tenant-name>.ciamlogin.com` of the **Run user flow endpoint** with the custom domain. The application page should load correctly, and you should be able to sign in.

It is also recommended to block the default domain `<tenant-name>.ciamlogin.com` so that attackers cannot use it to access your application or launch DDOS attacks. This can be done by submitting a support ticket to Microsoft.

Custom authentication extensions

Custom authentication extensions in Entra External ID allow organizations to tailor the authentication experience to meet unique business or security requirements. By leveraging these extensions, you can integrate external systems, apply advanced validation logic, or trigger custom workflows during the sign-in process. This flexibility is particularly useful for scenarios where out-of-the-box authentication methods are insufficient. Developers can create and register their own RESTful API endpoints to interact with Entra ID during authentication, enabling dynamic user validation, step-up authentication, or integration with third-party

services, thereby enhancing both security and user experience within your applications. Microsoft Entra External ID offers the following custom authentication extensions.

- `OnAttributeCollectionStart`: Using this extension developers can modify the sign-up experience for customers. The `OnAttributeCollectionStart` event occurs before the attribute collection page renders and allows developers to define actions before attributes are collected from the user. For example, users can be blocked from signing up based on their email or federated identity or some attribute values can be prefilled.
- `OnAttributeCollectionSubmit`: This event is triggered when the user submits the attributes collection form. It can be used to validate the user input. For example, you can validate a customer number or invitation code. You can show a validation error based on submitted values or block the user from signing up.
- `EmailOtpSend`: When users receive OTP during sign-up or when they reset their passwords, they receive emails in the default Microsoft format. Very little branding and customization is possible. It uses Microsoft gateway to send the emails. `EmailOtpSend` allows organizations to call a REST API and use their own email providers for sending OTPs.
- `TokenIssuanceStart`: This is a custom claims provider that allows developers to inject custom logic at the beginning of the token issuance process, right before the security token is generated and returned to the user after successful authentication. This extension can be used to perform additional validation, modify claims, or integrate with external systems to enforce custom policies. By leveraging `TokenIssuanceStart`, organizations can tailor the authentication and authorization experience, ensuring that issued tokens meet specific business or security requirements before users gain access to protected resources. You can call an external REST API to retrieve additional user attributes, such as a user's dietary preference or location, and then configure claims mapping to include those attributes as custom claims in the issued token. This allows your application to use information from external systems during authentication, ensuring tokens contain up-to-date and relevant user data.

These events can be created in the Microsoft Entra portal by navigating to **Entra ID | External identities | Custom authentication extensions | Create custom authentication extension**.

They can then be injected in the user flow by navigating to **Entra ID | External identities | User flows**. Select the user flow and click **Custom authentication extensions**. Choose if you would like to trigger the extension before collecting information from the user or after the user submits their information.

> **Note**
>
> The detailed setup of custom authentication extensions is beyond the scope of this book. Refer to `https://learn.microsoft.com/en-us/entra/identity-platform/custom-extension-overview`.

Enabling self-service password reset

Entra External ID gives users the option to reset their password in case they forget it. They do not need to call the helpdesk. This process uses email OTP authentication. To enable password reset, follow the steps below.

1. Create a user flow with **Email with password** as the authentication method. Refer *Figure 13.25*.
2. Ensure that **Email OTP** is enabled in **Entra ID | Authentication methods | Policies** as shown below:

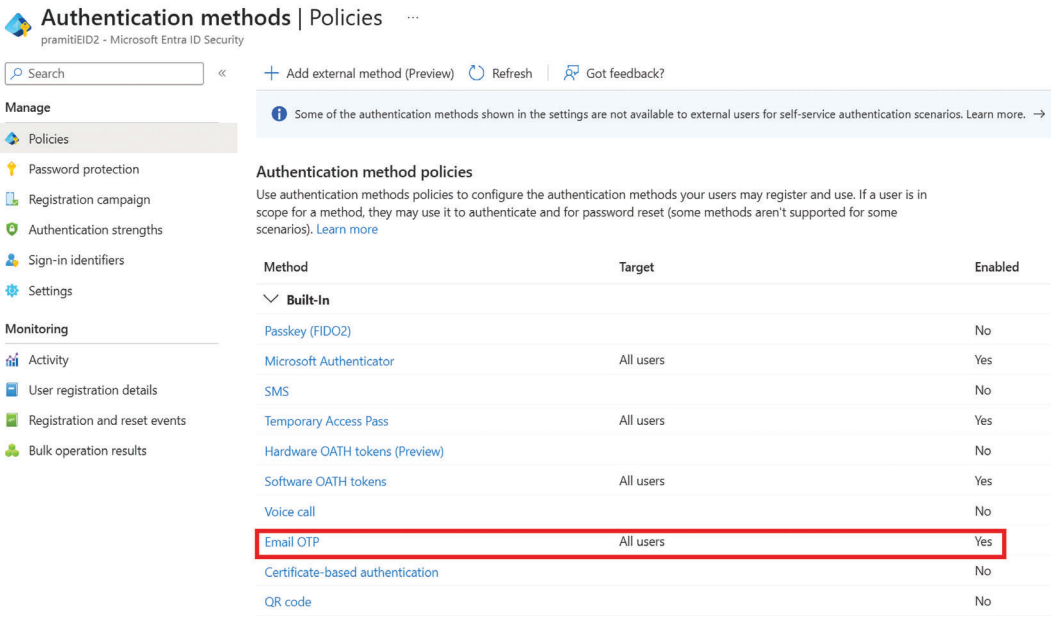


Figure 13.41: Email OTP enabled

3. Lastly, enable the forgot password link in custom branding. Refer to *Figure 13.29*.

Now, if the user forgets their password, they can click on the **Forgot password?** link on the **Enter password** page. This will send a code to their email ID. Once they enter the code, they will be asked to create a new password.

Securing external tenants

Microsoft Entra External ID provides some baseline features in external tenants to protect against threats like brute force and network layer attacks. These default settings provide a foundation for developing a security plan for your external identities. The following built-in security features are enabled by default in all external tenants to protect your applications from threats.

- **Brute force protection**: External tenants use Microsoft Entra ID's **smart lockout** feature to prevent unauthorized access through repeated password guessing. Smart lockout helps block out bad actors that try to guess a user's password or use brute-force mechanisms. It can recognize attempts from bad actors and block them, while letting legitimate users sign in.
- **Common networking HTTP Protection**: This provides protection against network-layer and timing-based attacks to protect against attempts to overwhelm resources and make them inaccessible to users.
- **Account protection**: Account protection helps safeguard user accounts from unauthorized access to protect user data and prevent account breaches. Microsoft offers integration with partner solutions like Akamai and Cloudflare for account protection. These solutions are available in the Microsoft Entra portal by navigating to **Entra ID | Security Store | Protect apps from DDOS with WAF**.
- **Access control**: External ID uses role-based access control to ensure that only authorized users get access to sensitive data. This is done using **App roles** and **Groups**. Microsoft Entra ID allows you to define roles for your applications and assign users to those roles. These roles then define the level of access users get in the application. Entra ID sends the role information to the application as a claim in the user's security token. Developers can also use Entra ID groups to define the level of access users have in the application or to define which group gets access to which application. The group claim is included in the user's security token.
- **Conditional Access policies**: Conditional Access policies can be created in the external tenant to trigger MFA, force a secure password reset or block access depending on conditions like location or device platform and the application being accessed.
- **Multifactor authentication**: MFA can be enforced to ensure that the legitimate user is accessing the application. External tenants support Email and SMS OTP MFA. SMS

MFA automatically checks for fraud and prompts users to complete a CAPTCHA if fraud is suspected. It also protects against telephony fraud. SMS is an add-on feature and charged per SMS sent. MFA is implemented using Conditional Access policies.

- **Fraud protection**: Consumer applications are prone to bot attacks and fake sign-ups. Microsoft offers partner solutions like HUMAN and Arkose Labs that help protect against these types of attacks. These solutions are available in the Microsoft Entra portal by navigating to **Entra ID | Security Store | Sign-up protection**.

Native authentication

The out of the box branding capabilities in Microsoft Entra ID offer limited customization capabilities. Sometimes, organizations need to provide fully customized user experiences and user journeys. Native authentication in Microsoft Entra External ID enables developers to build fully customized, in-app sign-in experiences for mobile and desktop applications. This approach allows applications to directly collect user credentials and interact with Entra's identity APIs, offering a seamless, branded experience that aligns with the app's native UI.

Native authentication supports two primary credential types: email with **one-time passcode** (**OTP**) and email with password (including self-service password reset). It is ideal for scenarios where redirecting to a browser is not feasible or desirable—such as mobile-first consumer apps, kiosk environments, or embedded systems—where maintaining a consistent, immersive user experience is critical.

Native authentication does not currently support social IdPs or federated identity providers. It supports **Single Sign-On** (**SSO**) for embedded web views and email and SMS OTP as MFA methods. It also requires developers to handle more of the authentication flow, including secure credential collection and token management. Microsoft strongly recommends using the **Microsoft Authentication Library** (**MSAL**) SDKs for supported platforms (Android, iOS/macOS, React, Angular) to simplify implementation and ensure best practices.

To enable native authentication, administrators must allow public client flows and explicitly enable native authentication in the app registration. Developers must also configure supported challenge types to inform Entra which authentication methods the app supports.

Use native authentication when you need full control over the sign-in UI, especially in mobile or desktop apps where browser redirects disrupt the user experience. It's best suited for consumer-facing apps where branding and flow consistency are paramount and where SSO or federated identity is not required. Native authentication offers a powerful option for crafting tailored identity experiences—provided the development team is equipped to manage the added complexity and evolving API surface.

Migrating to Entra External ID

Most organizations will have a CIAM solution that they are currently using. This could be Azure AD B2C or other solutions. Organizations wanting to adopt Entra External ID would like to do so without disrupting end user experience. Migration involves migrating user credentials and data. Migration consists of three main steps.

1. **Directory cleanup**: Moving to another system is a good opportunity to clean up data. Migrate only the data that is required. Identify stale accounts and exclude them from the migration. Identify required user attributes and don't migrate the ones not required. This makes the migration process smoother and ensures that the new system is clean.

   Note

   Do not store sensitive information like credit card numbers, medical records or passport numbers in Entra External ID.

2. **User data migration**: This is the step where user accounts are created in Entra External ID. This can be done manually or by importing the user accounts from the existing system to Entra External ID. Set a random password for now. Users' passwords will be updated as part of the password migration process.
3. **Password migration**: The next step is to migrate user passwords. There are two approaches to password migration.
   a. **Self-service password reset**: In this approach when the user accounts are migrated, a temporary password is created for the users. When the users log in, they are prompted to reset their passwords using the forgot password option. This approach is simple to implement; however, it does require users to reset their passwords which might be disruptive for some users and organizations may not like this.
   b. **Just-in-time (JIT) migration**: Organizations that don't want to make users reset their password can utilize JIT migration. This allows users to use their existing passwords once their accounts are migrated. JIT migration involves invoking a custom API during the sign-in process to validate the user's credentials against the legacy IdP using the `onPasswordSubmit` custom authentication extension. This extension allows defining custom logic that runs during the authentication process. From a user's perspective, this process is seamless. The user enters their password in the application login screen. Behind the scenes, their password is

validated against the legacy IdP. If the password is correct, it is securely migrated and stored in Entra External ID. On subsequent logins, the user authenticates directly against Entra External ID.

Monitoring External ID

Entra External ID offers the following tools to monitor user activity:

- **User activity insights**: This dashboard provides insights into user activity and their interaction with the applications registered in the external tenant. Using this dashboard you can track monthly active users, monitor new users added, analyze daily and monthly application sign-ins and assess MFA success and failures. This dashboard is available in your external tenant by navigating to Entra ID | Monitoring & health | Usage & insights.
- **Sign-up logs**: Entra External ID records all sign-ups, including successes and failures. Using these logs, organizations can gain insight into the sign-up process to enhance the sign-up experience and improve customer engagement. These logs show the percentage of sign-ups that led to successful account creation and drop-off rates.
- **Sign-in logs**: Using sign-in logs, administrators can find out how many users sign in and use applications, any failed sign-ins, and the browsers or devices from which users are signing in.
- **Audit logs**: Audit logs record information about any changes to the tenant, such as the creation of new users, applications or groups, password resets, and a lot more.
- **Provisioning logs**: These record the activities performed by the provisioning service. For example, users created or deleted in registered applications.
- **Azure Monitor**: Logs from the external tenant can be sent to Azure Monitor and a Log Analytics workspace from where they can be ingested in Microsoft Sentinel for security monitoring.

Summary

This chapter was a deep dive into Microsoft's CIAM solution. You learned how to create and customize an external tenant. You also learned how to configure different identity providers and register OIDC and SAML applications. Lastly, you learned the different security options available to secure your external tenant and the applications registered in it. This chapter also covered how developers can build pixel-perfect applications for end users using native authentication, migrating from an existing CIAM solution to External ID and how you can monitor your External ID tenant. In the next chapter, you will learn about Microsoft's Secure Services Edge solution.

Exercises

1. Which of the following is NOT supported by native authentication in Microsoft Entra External ID?
    a. Email and password sign-in
    b. One-time passcode (OTP) via email
    c. Social identity providers like Google or Facebook
    d. Self-service password reset (SSPR)
2. When registering an application in an Entra External ID tenant, which of the following is required to enable customer sign-in using a custom domain?
    a. Assigning the app to an Azure AD security group
    b. Verifying the custom domain in the External ID tenant
    c. Enabling multi-factor authentication (MFA)
    d. Creating a managed identity for the app
3. What is the primary purpose of a user flow in Microsoft Entra External ID?
    a. To define how internal employees access Microsoft 365 apps
    b. To configure DNS routing for custom domains
    c. To guide external users through sign-up, sign-in, and profile management experiences
    d. To assign roles and permissions to Azure AD B2B collaborators

Answers

1. c
2. b
3. c

Additional resources

- Entra External ID pricing: `https://learn.microsoft.com/en-us/entra/external-id/external-identities-pricing`
- Add Google as an identity provider: `https://learn.microsoft.com/en-us/entra/external-id/customers/how-to-google-federation-customers`

- Add Facebook as an identity provider: https://learn.microsoft.com/en-us/entra/external-id/customers/how-to-facebook-federation-customers
- Add Apple as an identity provider: https://learn.microsoft.com/en-us/entra/external-id/customers/how-to-apple-federation-customers
- Add Microsoft Account as an OIDC identity provider: https://learn.microsoft.com/en-us/entra/external-id/customers/how-to-microsoft-accounts-federation-customers
- Tokens and claims: https://docs.azure.cn/en-us/entra/identity-platform/security-tokens
- Entra external ID service limits: https://learn.microsoft.com/en-us/entra/external-id/customers/reference-service-limits
- Native authentication: https://learn.microsoft.com/en-us/entra/identity-platform/concept-native-authentication
- Just-in-time migration: https://learn.microsoft.com/en-us/entra/external-id/customers/how-to-migrate-passwords-just-in-time

Get this book's PDF version and more

Scan the QR code (or go to packtpub.com/unlock). Search for this book by name, confirm the edition, and then follow the steps on the page.





Note: Keep your invoice handy. Purchases made directly from Packt don't require an invoice.

14

Microsoft Entra Internet Access

Today's way of working has changed. People no longer work in traditional offices. They work from anywhere, using any device and network. As workloads move to the cloud, organizations need an identity-aware cloud-delivered network perimeter. This is called **Secure Service Edge (SSE)**. It is an advanced, cloud-delivered security framework designed to address the evolving needs of modern organizations. As businesses increasingly adopt remote work and cloud-based applications, traditional network perimeters become less effective. SSE responds to this shift by delivering security functions directly from the cloud, ensuring that users, devices, and data remain protected no matter where they are located or what network they use. At its core, SSE consolidates several critical security services—such as **secure web gateways (SWG)**, **cloud access security brokers (CASB)**, and **zero trust network access (ZTNA)**—into a unified, centrally managed platform. This consolidation not only reduces the complexity of managing multiple, disparate security tools but also enhances visibility and control for IT administrators. By enforcing policies at the network edge, SSE helps organizations defend against cyber threats, manage user access, prevent data loss, and maintain regulatory compliance. SSE empowers organizations to adopt flexible, hybrid work models without compromising security. Microsoft's implementation of SSE, known as **Global Secure Access (GSA)**, further extends these capabilities by integrating with **Microsoft Entra Internet Access** and **Microsoft Entra Private Access**, providing seamless protection for users and resources across distributed environments. This chapter will cover

- Overview of Global Secure Access
- Microsoft Entra Internet Access
- Microsoft Entra Internet Access for Microsoft Services

Overview of Global Secure Access

The solutions Microsoft Entra Internet Access and Microsoft Entra Private Access together comprise **Microsoft's Secure Service Edge (SSE)** solution. Microsoft uses the term **Global Secure Access (GSA)** to describe the SSE solution. Built on the principles of Zero Trust, GSA provides secure access to internet or private resources for any user or device from any network. The following figure is a graphical representation of GSA.

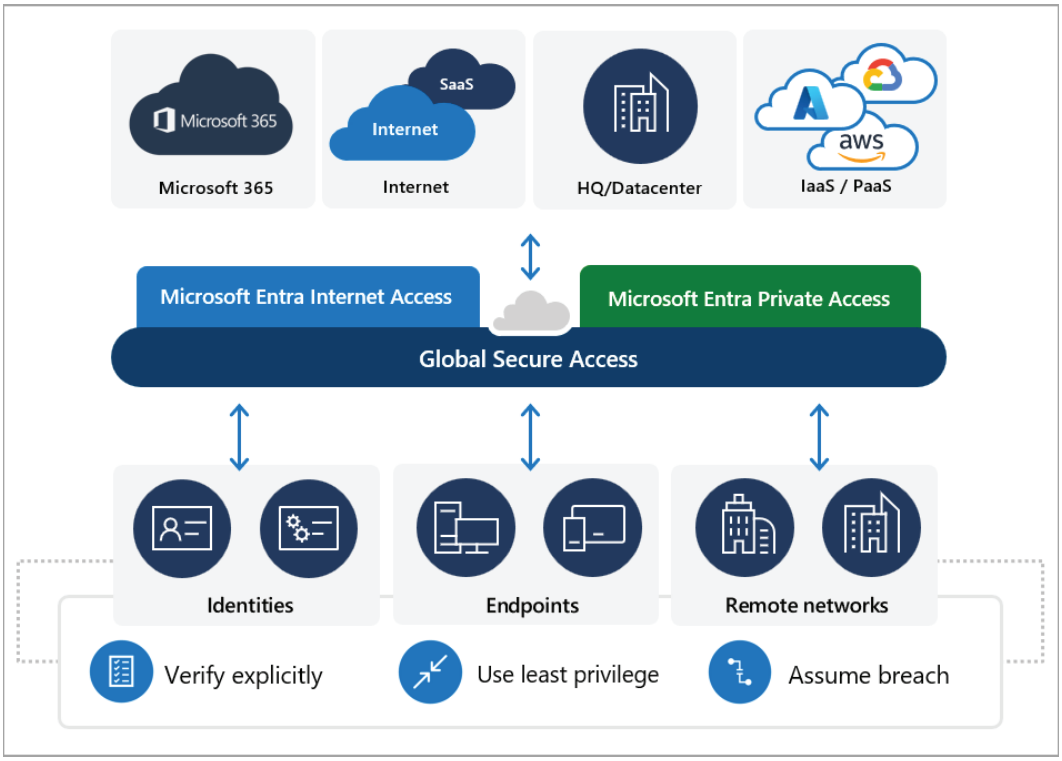


Figure 14.1: Global Secure Access

Microsoft Entra Internet Access and Private Access together with Microsoft Defender for Cloud Apps converge network, identity, and endpoint access to enable organizations to secure any app or resource from anywhere. Microsoft Entra ID provides simplified access policy management and orchestration for employees and business partners.

GSA has a dedicated location within the Microsoft Entra admin center to simplify the management of access control capabilities. GSA is delivered from Microsoft's Wide Area Network that spans 70 regions and has more than 190 network edge locations. It is available in specific **points of presence (PoP)**, and new locations are added periodically. Based on the

customer's location, they are connected to the nearest PoP to enable quick access to the GSA service.

Following the Zero Trust principle of least privilege access, GSA uses **Role-Based Access Control (RBAC)** to manage administrative access. Microsoft Entra ID offers several built-in roles that can be assigned to administrators who manage GSA. They are as follows:

- **Security Administrator**: This role grants permissions to perform specific tasks like configuring remote networks, setting up security profiles, viewing traffic logs etc. This role cannot configure Private Access.
- **Global Secure Access Administrator**: This is also a limited role and can perform tasks such as configuring remote networks, managing traffic forwarding profiles, viewing traffic logs etc. This role cannot configure Private Access or create and manage Conditional Access policies. It also cannot manage user and group assignments.
- **Conditional Access Administrator**: This role is required to create and manage Conditional Access policies for GSA.
- **Application Administrator**: This role can configure Private Access, private network connectors, application segments and enterprise applications.
- **Global Secure Access Log Reader**: This role is intended for staff that need read-only access to traffic logs. They cannot make changes to the environment; however, they can view detailed GSA traffic logs including session, connection and transaction data. They can also review alerts and reports.
- **Security Reader and Global Reader**: These roles have read-only access to GSA except for traffic logs.

To perform tasks in Microsoft Entra, administrators need to have the **Global Secure Access Administrator** and the relevant role assigned. For example, if administrators need to create Conditional Access policies, they should be assigned both the Conditional Access Administrator and the Global Secure Access Administrator roles.

GSA offers useful dashboards that provide visualization of data across Microsoft Entra Internet Access and Private Access. This helps administrators understand the number of devices that are using GSA in the network, the usage patterns, most used destinations, cross-tenant activity patterns and more. Administrators with the Global Secure Access Administrator role can view this dashboard in the Microsoft Entra admin center by navigating to **Global Secure Access | Dashboard**.

Before proceeding with Microsoft Entra Internet Access, let's explore some key concepts of GSA.

GSA client

The GSA client routes traffic that needs to be secured by GSA to the cloud service. All other traffic goes over the internet. **Traffic forwarding profiles** are used to decide which traffic goes through the client and which over the internet. This client is available for Windows, macOS, iOS and Android and helps organizations manage and secure traffic on client devices. It can be downloaded from the Microsoft Entra admin center by navigating to **Global Secure Access | Connect | Client download**. From the right pane download the client for the operating system you want.

> **Note**
>
> Detailed instructions for installing the client on various operating systems are beyond the scope of this book. Refer to the following URLs:
>
> - `https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-install-windows-client`
> - `https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-install-macos-client`
> - `https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-install-android-client`
> - `https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-install-ios-client`

Running an antivirus solution along with the GSA client can degrade system performance. If you experience high CPU usage or performance degradation, exclude the GSA processes from the antivirus solution. For a list of the processes, refer to `https://learn.microsoft.com/en-us/entra/global-secure-access/concept-edr-antivirus-coexistence`.

Remote networks

Some organizations have small branch offices in remote locations that have a handful of employees. These employees need access to corporate applications and data. The security of these remote locations is crucial. These offices are usually connected to headquarters over a **Virtual Private Network (VPN)**. Over time, the number of devices that need access to corporate resources has grown exponentially. This puts a high load on traditional network connectivity. Applications like Microsoft 365 require low-latency and jitter-free communication. Traditional network technologies like **Wide Area Network (WAN)** and

Multi-Protocol Label Switching (MPLS) cannot meet these demands. Moreover, some branch offices have physical firewalls which require maintenance by an IT team. Placing an IT team in each branch office is expensive.

GSA helps connect these remote offices to the corporate network over an **Internet Protocol Security (IPSec)** tunnel. This tunnel is established between a **customer premises equipment (CPE)** and the nearest GSA PoP. This eliminates the need for each client in the remote office to have a VPN or GSA client installed. Once the IPSec tunnel is established, traffic forwarding profiles route designated traffic from the remote office over the tunnel, while other traffic is routed over the internet. GSA provides secure network connectivity for employees in remote offices without needing to route traffic to their headquarters.

Following are the prerequisites for setting up a remote network:

- A Global Secure Access Administrator role
- CPE must support the following:
    - IPSec
    - GCMEAES128, GCMAES192, or GCMAES256 algorithms for Internet Key Exchange (IKE) phase 2 negotiation
    - Internet Key Exchange Version 2 (IKEv2)
    - Border Gateway Protocol (BGP)
- CPE must use **RouteBased VPN** with **any-to-any** traffic selectors
- CPE must initiate the connection using **Responder** modes

Remote networks in GSA can be created in the Microsoft Entra admin center using the steps below.

1. Sign in to `https://entra.microsoft.com` as **a Global Secure Access Administrator**.
2. Navigate to **Global Secure Access | Connect | Remote networks**.
3. In the right pane, click **Create remote network**.
4. On the **Basics** page, enter the name of the remote network and select the region. This is the Microsoft PoP that your remote network will connect to. Select the region closest to your location. Click **Next: Connectivity**.
5. On the **Connectivity** page, enter the device links for the remote network. These can be added after the remote network has been created. Device type, IP address, and BGP address are required. Once done, click **Next: Traffic profiles**.
6. On the **Traffic profiles** page, choose if you want to route internet traffic or Microsoft 365 traffic. Click **Next: Review + create**.

7. On the last page, review your configuration and click **Create remote network**. The remote network will show up in the console as shown below:

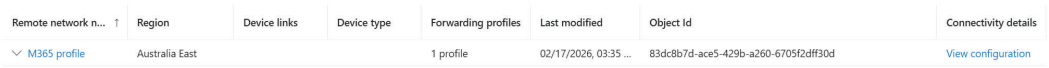


Figure 14.2: Remote network

8. Click on **View configuration** in the screenshot above. From the flyout pane, save Microsoft's public IP address `endpoint`.
9. IPSec is a bidirectional communication. For IKE negotiations to occur between the remote network and the Microsoft PoP, configuration must be completed on the CPE as well. In your CPE management console, enter the IP address saved in *Step 8*.

This completes the remote network configuration, and the IPSec tunnel is established.

Traffic forwarding profiles

Traffic forwarding enables organizations to configure the type of traffic to be routed over Microsoft Entra Internet Access and Microsoft Entra Private Access. This is done by configuring traffic forwarding profiles.

There are three traffic forwarding profiles pre-created in GSA. To view the profiles, navigate to **Global Secure Access | Connect | Traffic forwarding**. *Figure 14.3* shows the available profiles. Each profile can be enabled or disabled by switching the corresponding toggle on or off. For each profile you can also view the linked Conditional Access policies.

To scope a profile to specific users and groups, click on **View** under **User and group assignments** (*Figure 14.3*) and select the users and groups from the list. You must have the **Global Secure Access Administrator** and **Application Administrator** roles to enable a profile and scope it to specific users and groups. You can also use a dynamic group to automatically assign users to the profile. Following are some considerations for group assignments:

- Traffic profiles apply to the user who is logged into the device.
- If there is no user logged in, then a profile applies only if it is assigned to all users. For example, if you are logged into a device as a local user, you are a part of all users.
- Multiple users logging in to the same device simultaneously is not supported.
- Group-based assignments are only supported for Security groups and Microsoft 365 groups whose `SecurityEnabled` is set to `True`.
- Nested groups are not supported.

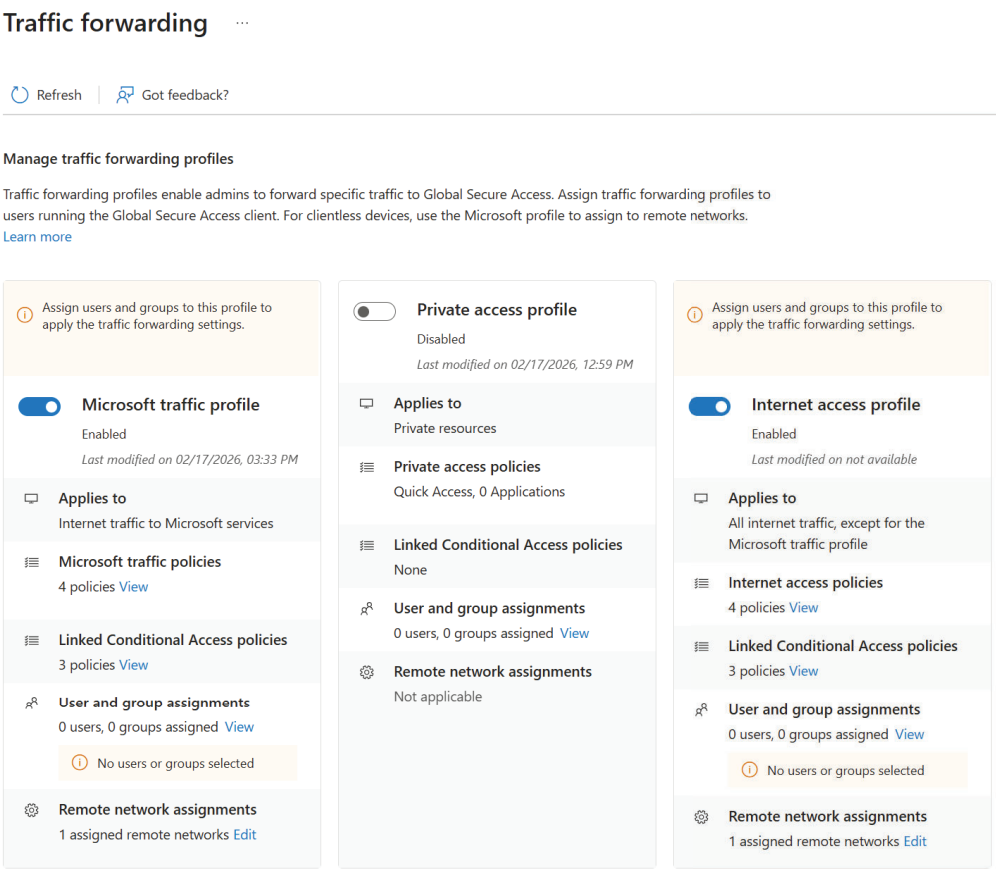


Figure 14.3: Traffic forwarding profiles

These profiles will be discussed in detail in the subsequent sections.

In addition to the above profiles, a **Microsoft Entra traffic profile** handles all authentication and identity-related traffic for Microsoft Entra services. This profile ensures that identity traffic is always acquired and protected regardless of license assignment. Following are the key features of this profile.

- **Always on**: This profile is automatically enabled whenever any of the other traffic forwarding profiles are active. It is independent of the others and cannot be enabled or disabled.
- **Highest priority**: Entra traffic is always processed first. It leverages **mutual Transport Layer Security (mTLS)** and certificate-based authentication.

- **No assignment requirement**: This profile is automatically included in any active traffic forwarding profile and does not require any explicit user or branch assignment.
- **Coverage**: This profile covers a defined set of **Fully Qualified Domain Names (FQDN)** and IP ranges of the Microsoft Entra services. All traffic for these destinations is automatically acquired by this profile and routed through the GSA service.

This profile is Microsoft-managed and is not visible in the portal.

Access controls

GSA can apply several access controls to the traffic being routed through it. Let's explore some of them.

Universal Conditional Access

GSA is integrated with Conditional Access policies and can apply policies to secure traffic profiles. Controls like MFA, compliant device or risk-level can be applied to network traffic. These policies can be applied to all traffic acquired by Microsoft Entra Private Access or Microsoft Entra Internet Access profiles. This functionality helps protect applications that don't support modern authentication. Conditional Access policies can be targeted to traffic profiles and not specific applications. This is done by selecting **All internet resources with Global Secure Access** under **Target resources** while creating the Conditional Access policy.

Compliant network check

The integration between GSA and Conditional Access can prevent malicious access to applications using several conditions, such as device compliance and location. GSA introduces the **compliant network check**, which ensures that users are connecting through the GSA client installed on their devices or through configured remote networks. This ensures that traffic for protected resources is flowing through the GSA service and that clients are compliant with the security policies enforced by the Conditional Access policies.

Compliant network check reduces the risk of token theft and token replay attacks. Authentication is provided by Entra ID. If a client's token is stolen and a bad actor attempts to replay it using a device that does not have the GSA client installed and connected to the organization's compliant network, Entra ID will block access. The compliant network check is specific to the tenant where the policy is configured. For example, if the compliant network policy is applied at *abc.com*, a user from *xyz.com* will not be able to pass the compliant network check.

To enable compliant network check, GSA signaling for Conditional Access must be configured using the following steps:

1. Sign in to `https://entra.microsoft.com` as a **Global Secure Access Administrator**.

2. Navigate to **Global Secure Access | Settings | Session management**.
3. In the right pane, click **Adaptive Access** and toggle the **Enable Conditional Access Signaling for Microsoft Entra ID** to on, as shown in the following figure:

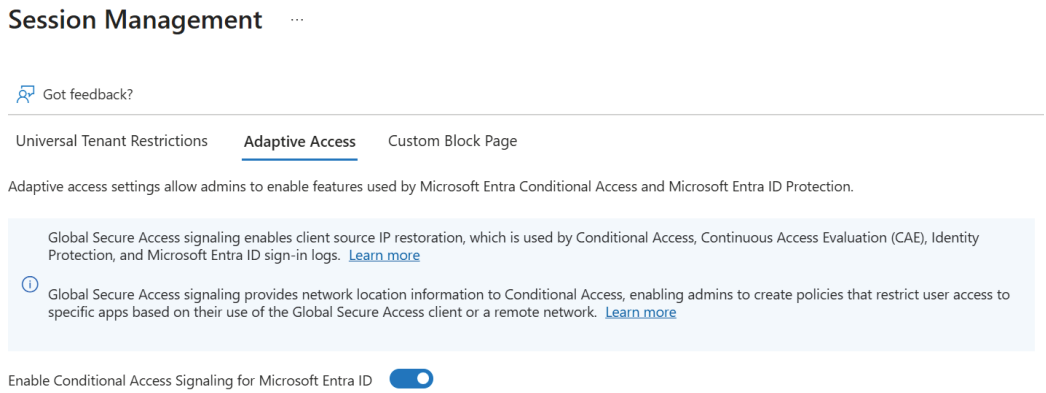


Figure 14.4: Enable CA signaling

4. Navigate to **Entra ID | Conditional Access | Named locations**. Confirm that a location exists with the name All Compliant Network locations, with location type as Network Access. Organizations can mark this location as trusted. Refer to the following figure.

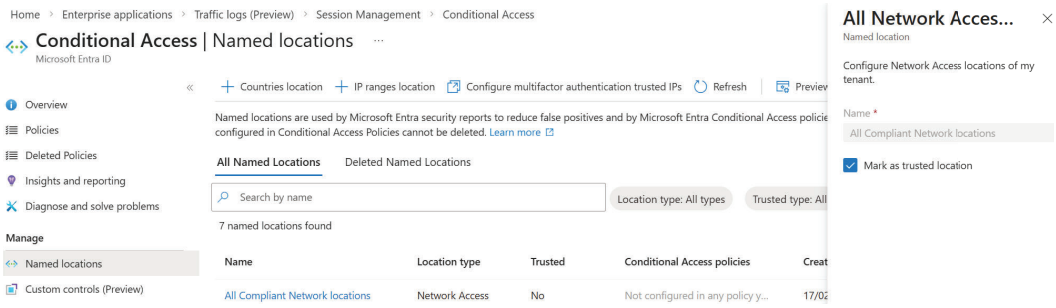


Figure 14.5: Named location in CA

Conditional Access policies can now be configured to ensure the compliant network check by selecting **All Compliant Network locations** under **Network**.

Tip

If you create a policy based on compliant network check and later turn off GSA signaling users may be blocked from accessing the target resource. If you need to turn off GSA signaling, ensure that any Conditional Access policy that uses the compliant network check is turned off.

Source IP restoration

Cloud security layers like SSE, SWG, ZTNA, CASB, etc. typically mask the user's true IP. The destination service sees only the cloud proxy's IP. This creates several problems, such as:

- Conditional Access based on trusted IPs fails because Entra ID cannot see the user's actual egress IP.
- Audit logs lose fidelity, showing the proxy's IP instead of the user's real location.
- Location-based risk signals degrade, making it harder to detect anomalies.
- Legacy apps relying on IP allowlists break, because the "source IP" is no longer the corporate or expected IP.

Source IP restoration in GSA restores the user's original client IP address when their traffic passes through a cloud-based network proxy or SSE service. This allows Microsoft Entra ID and Microsoft Graph to evaluate network-based policies and logs using the true client IP address.

Source IP restoration is enabled for all tenants created after June 2025. To explicitly enable or disable this feature, turn **Enable Conditional Access Signaling for Microsoft Entra ID** on or off as explained in the *Compliant network check* section.

This allows Entra ID to receive the public egress source IP address of the user.

Understanding Microsoft Entra Internet Access

Microsoft Entra Internet Access is a cloud-delivered identity-centric **Secure Web Gateway (SWG)** designed to safeguard organizational resources as users access the internet and cloud-based applications from any location or device. By leveraging identity-aware controls, it provides secure browsing, enforces access policies, and helps prevent data leaks at the network edge. Microsoft Entra Internet Access integrates seamlessly with Microsoft's SSE strategy, combining web protection, threat defense, and visibility into user activity. The solution empowers organizations to enable remote and hybrid work while maintaining robust security standards and centralized management, ensuring users stay protected no matter where or how they connect. The following are some key features of Microsoft Entra Internet Access.

- It can acquire network traffic using traffic forwarding profiles.
- It records detailed traffic logs for internet traffic and provides detailed dashboards that show relationships between users, devices and endpoints.
- It integrates with Conditional Access policies to apply network security policies using context-aware vectors like user, device, device compliance, location, and risk.
- It enables web content filtering to regulate user access to the internet based on web categories or FQDNs.

Let's understand a few important concepts before moving forward.

Internet Access profile

To use Microsoft Entra Internet Access, you must first enable the **Internet access profile**. Refer to *Figure 14.3*. Once enabled, traffic to the public internet, except for the Microsoft traffic profile, will be forwarded to the service through the GSA client or the remote network. This profile includes a list of regular expressions for FQDNs and IP Addresses representing the public internet. It includes the following Internet access policies:

- **Custom bypass**: Administrators can define traffic that must be excluded from being routed to the service. Traffic for the destinations listed under this policy will not be acquired by the profile. Organizations usually exclude traffic for their VPN endpoints, private IP ranges and networks that use a network **Access Control List (ACL)**. To add rules to this policy, click on **Add rule** as shown in *Figure 14.6*. You can add a FQDN, IP, IP Subnet or IP Range. Once a rule is added it takes 15-20 minutes to appear on the client computer.
- **Default bypass**: This policy contains predefined internet traffic that the profile does not acquire, like private IP ranges. The rules in this policy cannot be changed.
- **Microsoft traffic bypass**: This policy lists all traffic that can be acquired by the Microsoft traffic profile. This traffic is bypassed by the Internet access profile and is acquired by the Microsoft traffic profile when it is enabled. The rules in this policy cannot be changed.
- **Default acquire**: This policy defines traffic that is always acquired by the profile. All internet traffic on ports 80, 443 over **Transmission Control Protocol (TCP)** is included in this policy. This policy has the lowest priority and is processed after all bypass rules are processed. The rules in this policy cannot be changed.

To view a list of these policies, click on **View** under **Internet access policies**. Refer to *Figure 14.3*. The following figure shows the policies discussed above:

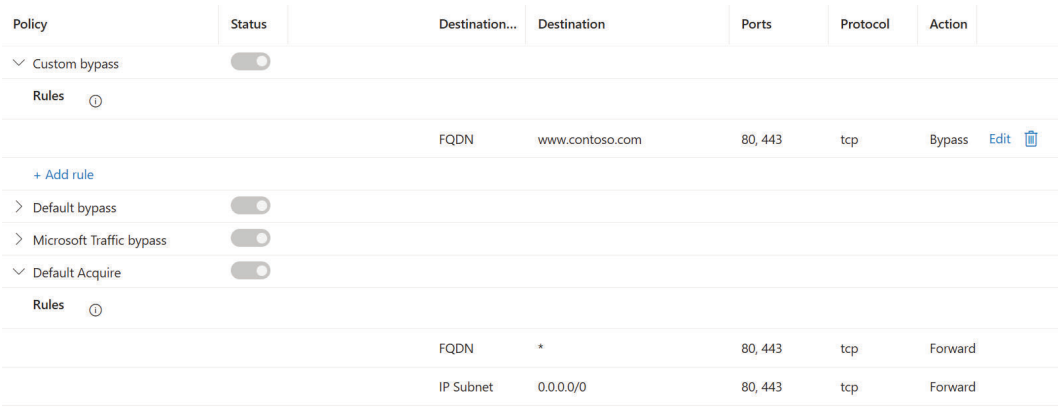


Figure 14.6: Internet access profile policies

Once the internet access profile is enabled and configured, you can use the other capabilities of Microsoft Entra Internet Access.

Security profiles

Security profiles help organize policies like web content filtering policy, TLS inspection policy, threat intelligence policy and more. They can be linked to Conditional Access policies to make them user and context aware. One security profile can have multiple web filtering policies, TLS inspection policies, threat protection policies, and more. One security profile can be linked to multiple Conditional Access policies. For example, you could have a security profile for the finance department containing all policies specific to the finance department. This security profile can then be applied to all users in the finance department using a Conditional Access policy. Within a security profile, policies are enforced based on priority of numbers: 100 is the highest priority and 65000 is the lowest priority. When a security profile is linked to a Conditional Access policy, if multiple Conditional Access policies match, all matching security profiles are processed as per priority ordering.

A **baseline security profile** exists with a priority of 65000. This policy applies to all internet traffic routed via the GSA client or remote network without being linked to a Conditional Access policy. It sits at the lowest priority in the policy stack and acts as a catch-all policy. It ensures that no internet traffic goes uninspected even if an administrator misconfigures the Conditional Access policies or forgets to link a profile. It acts as a safety net. While the baseline security profile provides basic security, it is recommended that organizations create additional security profiles as per their business needs and link them to Conditional Access policies to adequately protect the network.

The following figure shows the relationship between security profiles, Conditional Access policies and other policies in GSA:

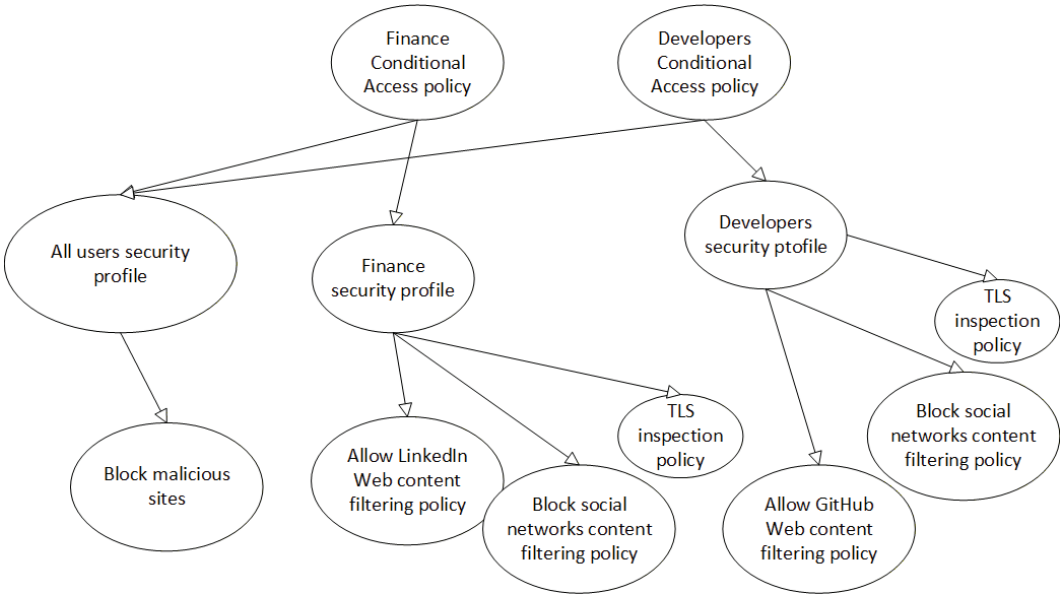


Figure 14.7: Relationship between security profiles, Conditional Access policies and other policies in GSA

Security profiles can be accessed using the following steps:

1. Sign in to `https://entra.microsoft.com`.
2. Navigate to **Global Secure Access | Secure | Security profiles**.
3. In the right pane, click on **Baseline profile** to view the baseline security profile.
4. Click on the ellipses and click on **Edit** to enable or disable the profile and link policies.
5. Click on **Link policies | Link a policy** to link a policy to the profile as shown in the screenshot below:

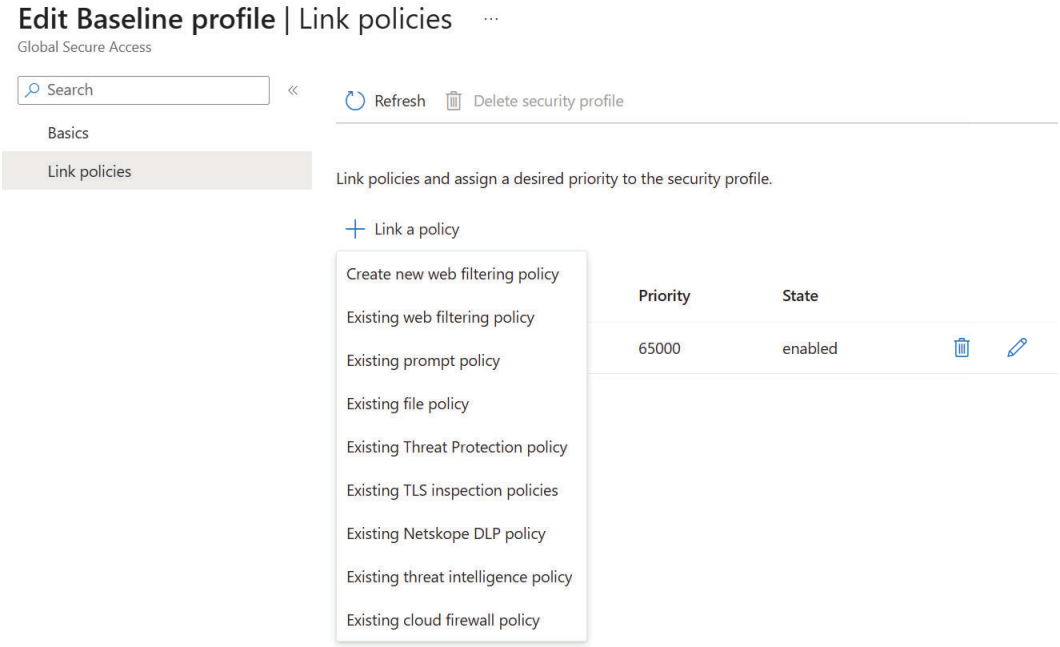


Figure 14.8: Link policies to the security baseline profile

Additional security profiles can be created by navigating to **Global Secure Access | Secure | Security profiles | Create profile**. These security profiles can then be linked to Conditional Access policies to make them user and context aware.

Prerequisites

Before configuring GSA policies, ensure that the Internet Access Profile is enabled and the GSA client is installed on the devices. The following are additional prerequisites:

- Administrators must have the **Global Secure Access Administrator** role to configure the GSA policies.
- Since GSA policies are delivered using Conditional Access policies, administrators require the **Conditional Access Administrator** role to create and configure the Conditional Access policies.
- **Domain Name System (DNS) over HTTPS (Secure DNS)** must be disabled.
- The built-in DNS client on Microsoft Edge and Chrome must be disabled.
- IPv6 traffic is not acquired by the GSA client, so the network adapter properties must be set to **IPv4 preferred**.
- **User Datagram Protocol (UDP)** traffic is not supported. You can deploy a Windows Firewall that blocks outbound UDP traffic.

Specific policies may have additional prerequisites which will be discussed in the relevant section below.

Configuring web content filtering

Web content filtering allows organizations to control user access to web resources. Administrators can block or allow sites based on categories, specific **FQDNs**, and URLs, promoting security and compliance by restricting access to harmful or inappropriate online content from any internet connection, whether remote or corporate.

Microsoft Entra Internet Access protects when the traffic reaches Microsoft's Secure Service Edge. For unencrypted HTTP traffic, **Uniform Resource Locator (URL)** is used. For HTTPS traffic encrypted using **Transport Layer Security (TLS), Server Name Indication (SNI)** is used.

Following are the steps to configure web content filtering. This includes creating a web content filtering policy, adding it to a security profile and linking the security profile to a Conditional Access policy.

1. Sign in to `https://entra.microsoft.com` as **a Global Secure Access Administrator**.
2. Navigate to **Global Secure Access | Secure | Web content filtering policies**.
3. In the right pane, click on **Create policy**.
4. On the Basics page give the policy a **Name** and **Description**. Select the **Action** as **Block** or **Allow**. This defines whether the policy will block or allow access to the defined destinations. Click **Next**. Refer to *Figure 14.9*.

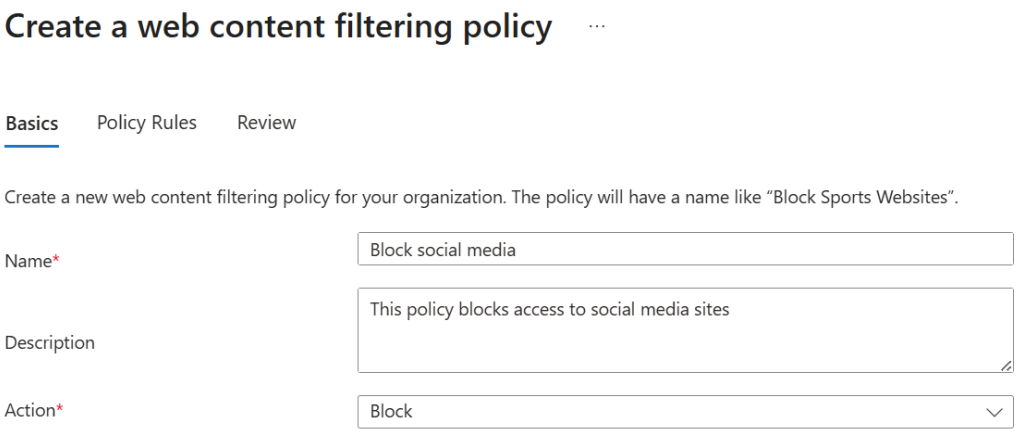


Figure 14.9: Web content filtering basics

5. On the **Policy rules** page, click **Add rule**. In the flyout pane, give the rule a **Name** and select the **Destination type** from the following options:
    a. `webCategory`: With this option selected you can pick from the available categories.
    b. `fqdn`: Enter the Fully Qualified Domain Names of websites you wish to include in the rule. For example, `www.facebook.com`
    c. `url`: Enter specific URLs that you would like to add to the rule. For example, `www.msn.com/sports`.

    Once done, click **Add** as shown in the following screenshot. Then click **Next**.

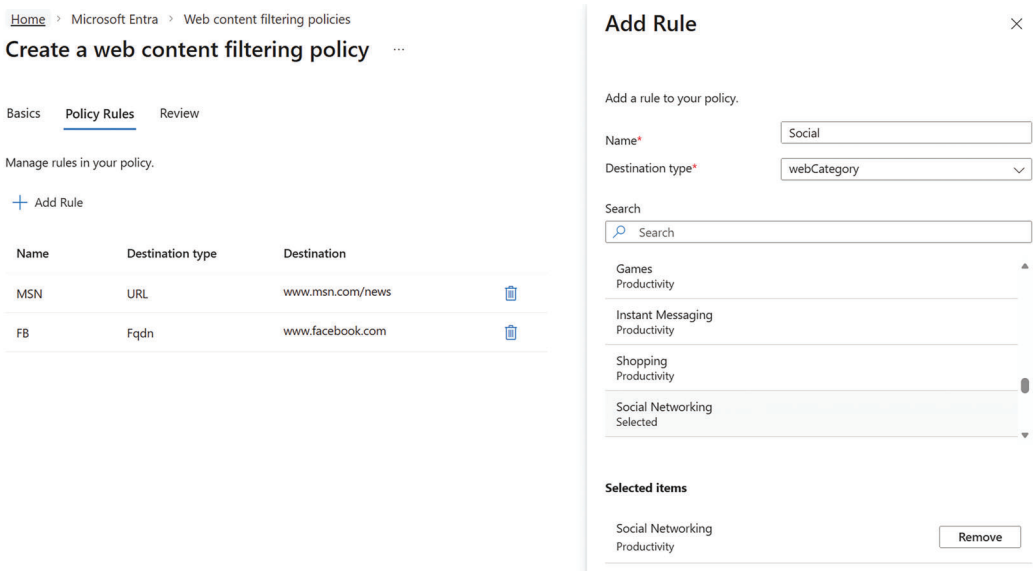


Figure 14.10: Define rules

6. On the **Review** page, review your selections and click **Create policy**.

As discussed above, web content filtering policies are delivered using security profiles. The following steps explain how to create a security profile:

1. In the left navigation menu, click on **Security profiles**.
2. In the right pane, click on **Create profile**.
3. On the **Basics** page, enter the **Profile name** and **Description**. Select state as **Enabled** and enter a **Priority** number. This number will determine the order in which the policies will be processed. Click **Next**.
4. On the **Link policy** page, click on **Link a policy** to link the web content filtering policies you would like to include in this profile. You can either link an existing web filtering policy or create a new one from here. From the flyout pane, choose the policy created earlier from the **Policy name** drop-down, select a **Priority** number between 100 and 65000, and select the **State** as **Enabled**. Once done, click **Add**. Refer to the following screenshot:

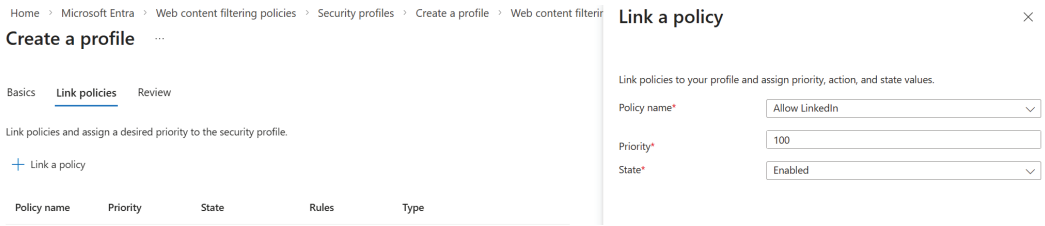


Figure 14.11: Link filtering policies

For example, if you want all social media content to be blocked but LinkedIn allowed, you can create two filtering policies: one policy blocking all social media based on web category and another allowing LinkedIn based on FQDN. Then add these two policies to a security profile with the allow LinkedIn profile having a higher priority than the blocking social media profile as shown in the following screenshot:

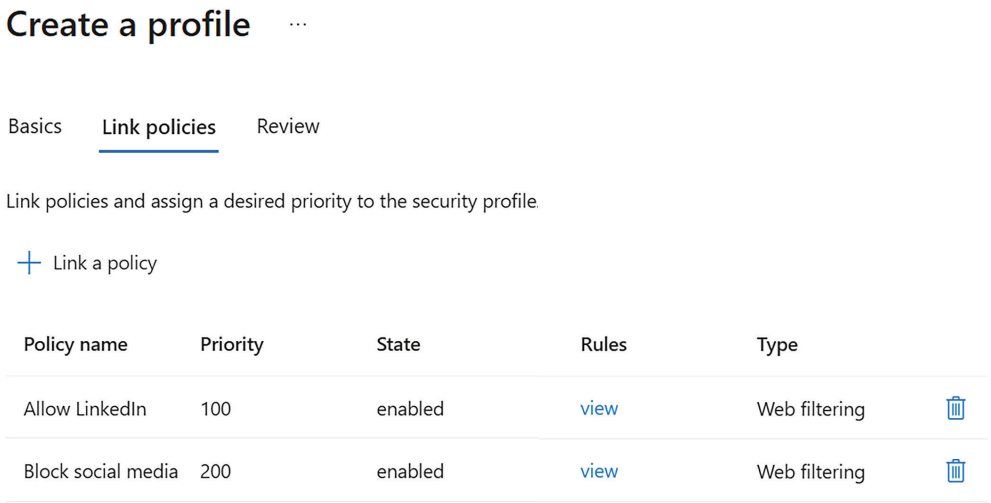


Figure 14.12: Policy order

5. On the **Review** page, review your settings and click **Create a profile**.

To enable this security profile for users it must be added to a Conditional Access policy. The following steps explain.

1. In the Entra Admin center navigate to **Entra ID | Conditional Access** as a Conditional Access Administrator.
2. In the right pane, click **Create new policy**. Enter a **Name** for the policy.
3. Under **Assignments**, click on **User, agents or workload identities** and select the users or group whom you want to cover with the policy.
4. Under **Target resources**, select **All internet resources with Global Secure Access**.
5. Under **Session**, select **Use Global Secure Access security profile** and select the profile created above and click **Select**.
6. Under **Enable policy**, switch the toggle to **On** and click **Create**. Refer to the following screenshot:

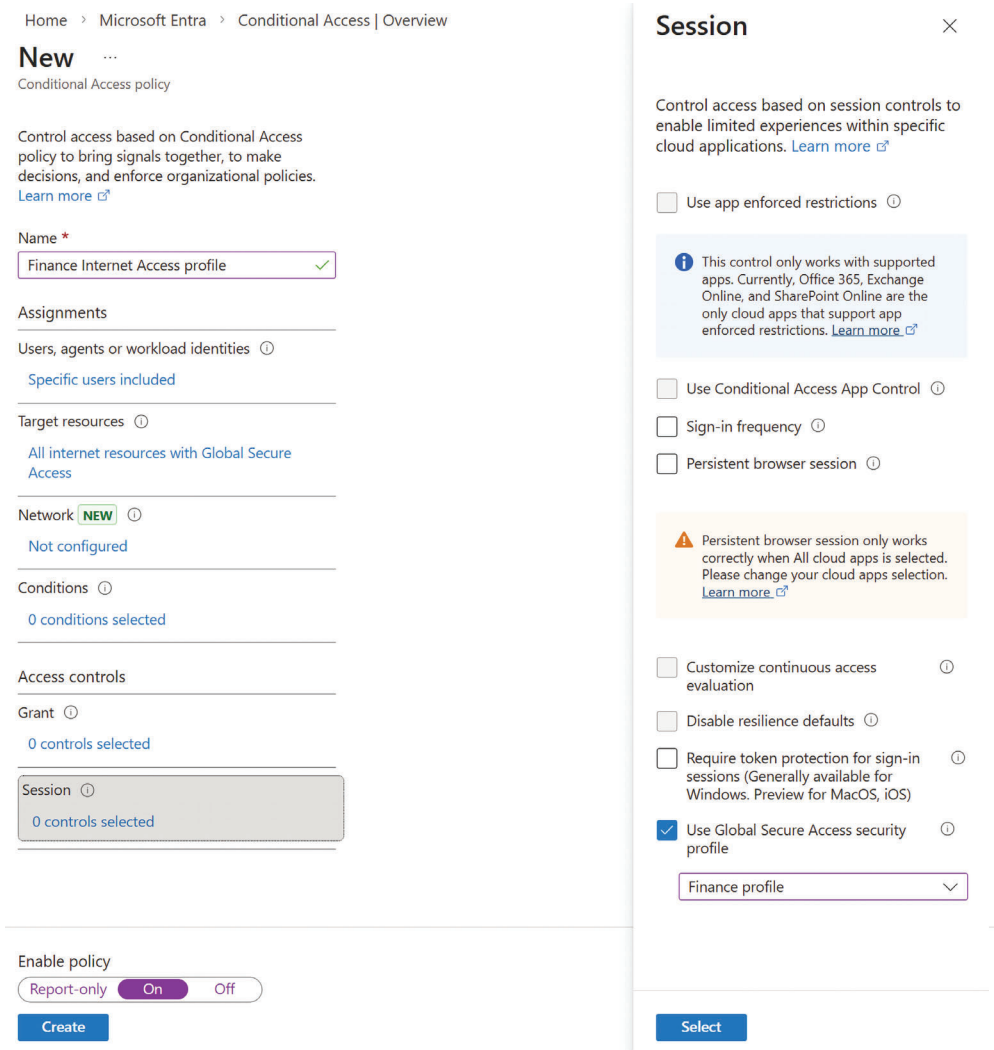


Figure 14.13: Conditional Access policy

Now whenever a user covered by this Conditional Access policy tries to access internet resources, the rules defined in the *Finance profile* will apply to them and they will be prevented from accessing social media sites. They will see a default block page instead. This block page can be customized as per the organization's branding requirements by navigating to **Global Secure Access | Settings | Session management | Custom block page**.

Configuring Transport Layer Security inspection

Transport Layer Security (TLS) protects privacy by encrypting the data transmitted between a user's device and the destination server. This means that even if someone intercepts the network traffic, they cannot read the contents without the proper decryption keys. TLS also ensures the authenticity of the server, helping users confirm they are communicating with the intended party and not an imposter. As a result, sensitive information such as login credentials, personal data, and business communications remains confidential during transit. However, this also enables malicious traffic to be hidden behind encryption. **TLS inspection** is the process of intercepting, decrypting, and analyzing encrypted internet traffic. This enables organizations to inspect data for threats or policy violations while maintaining security. After inspection, the data is re-encrypted and sent to its destination, ensuring privacy and compliance with security standards.

TLS inspection in GSA decrypts HTTPS traffic and applies security controls like web content filtering. It uses a two-tier intermediate certificate method to issue leaf certificates that are dynamically generated. These leaf certificates are used to decrypt traffic and protect against threats that hide behind encryption.

To configure TLS inspection in GSA, ensure that there is an existing **Public Key Infrastructure (PKI)** service available to sign the **Certificate Signing Request (CSR)** and to generate a certificate for TLS inspection. The following are the steps to create a CSR and upload a signed certificate:

1. Sign in to `https://entra.microsoft.com` as **a Global Secure Access Administrator**.
2. Navigate to **Global Secure Access | Secure | TLS inspection policies**.
3. In the right pane, click on **TLS inspection settings** and click **Create certificate**.
4. In the flyout pane, enter the following details and click **Create CSR** once done.
    a. **Certificate name**: This name appears in the browser when the certificate is viewed. It must be unique, with no spaces, and should not be more than 12 characters in length.
    b. **Common name**: Any name that identifies the certificate.
    c. **Organization name**: Any name that identifies the organization.
5. The CSR is created and saved to your default downloads folder. This CSR must be signed by your PKI service and saved in `.pem` format.
6. Click on **Upload certificate** and upload the `.pem` files and click **Upload signed certificate** as shown below.

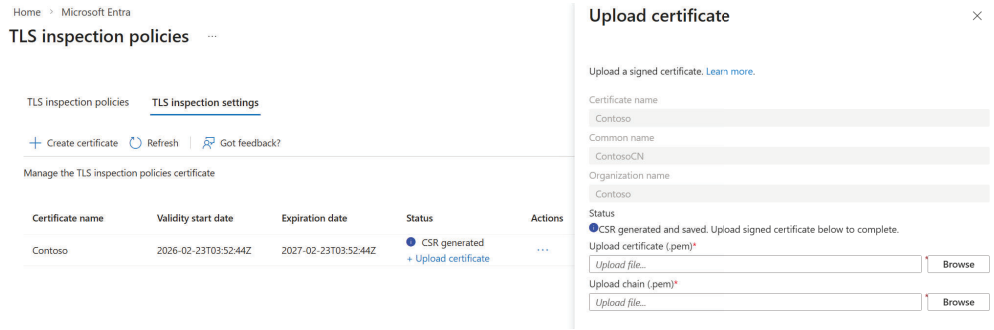


Figure 14.14: Upload signed certificate

7. By default, the certificate is **Disabled** when uploaded. Change the status to **Enabled**. At a time, only one enabled certificate is allowed.

Note

If you don't have a PKI and want to test TLS inspection, you can use a self-signed root certificate created using the **OpenSSL** utility.

Once you have an active enabled certificate, you can configure context-aware TLS inspection policies using the following steps:

1. Sign in to `https://entra.microsoft.com` as **a Global Secure Access Administrator**.
2. Navigate to **Global Secure Access | Secure | TLS inspection policies**.
3. In the right pane, click on **Create policy**. Enter a **Name** and **Description** for the policy. Select the **Default action** as **Inspect** or **Bypass** and click **Next**.
4. On the **Rules** page, click **Add rule**. Here you can define a rule by selecting a **FQDN** or **Web category**. Refer to the following screenshot. Click **Save** when done.

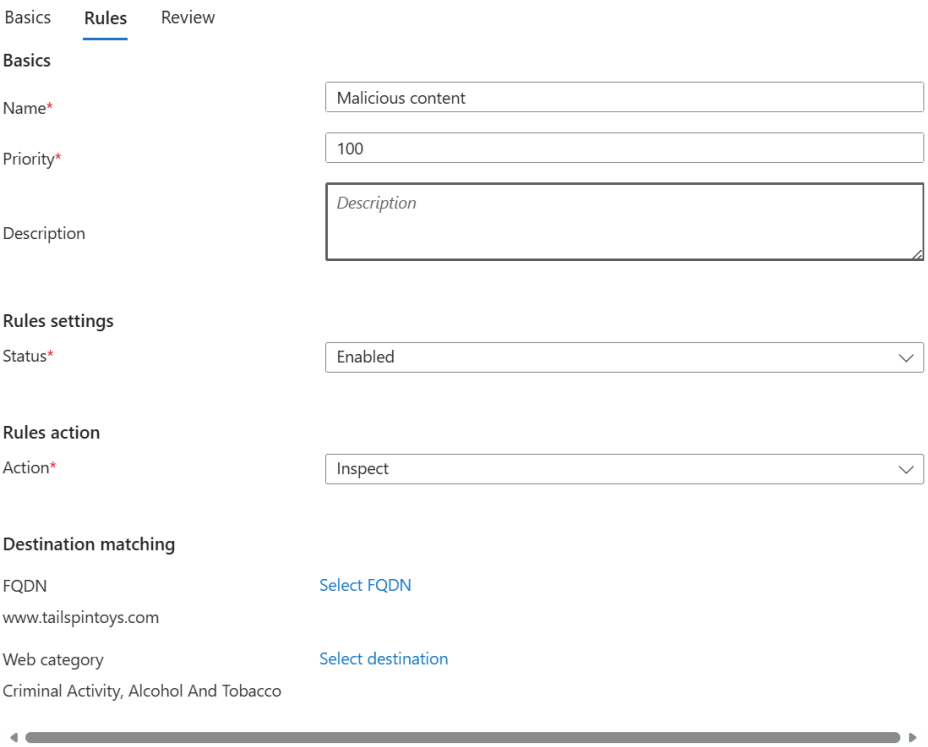


Figure 14.15: TLS inspection policy

5. Click **Next**. On the **Review** page, click **Submit** to create the policy.

A system rule is automatically created to bypass destinations that don't work with TLS inspection. This rule cannot be modified or deleted. An editable rule is also automatically created to exclude traffic for Education, Finance, Government, Health, and Medicine. This rule can be modified or deleted. Refer to the following screenshot:

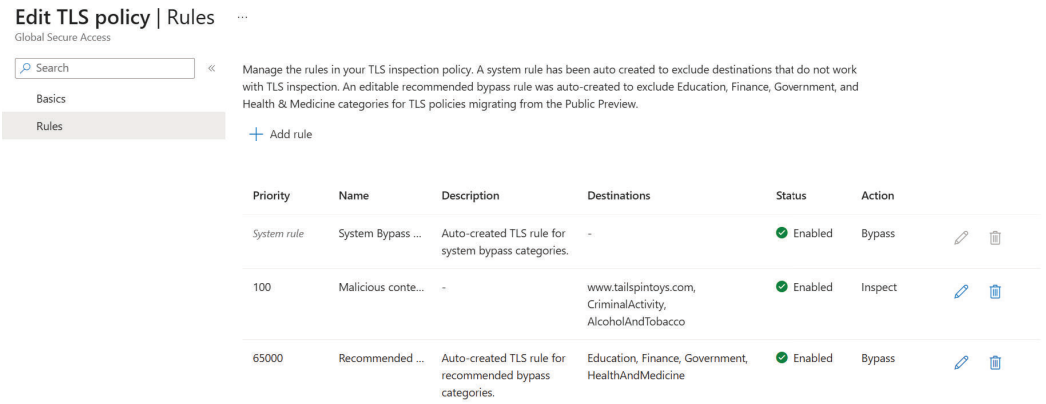


Figure 14.16: Rules in TLS inspection policy

Like web content filtering policies, TLS inspection policies are also delivered through security profiles. The TLS inspection policy must be linked to either the baseline security profile which will enable TLS inspection for all users, or to a security profile specific to users or groups using a Conditional Access policy. This has been explained in the section *Configuring web content filtering*.

Configuring threat intelligence

Threat intelligence refers to the process of collecting, analyzing, and applying information about current and emerging cyber threats. It helps organizations protect their users from accessing malicious websites based on real-time threat information, ultimately strengthening overall security posture. Threat intelligence in Microsoft Entra Internet Access enables organizations to block traffic based on domain and URL indicators. It uses Microsoft and non-Microsoft threat intelligence sources.

Following are the steps to configure threat intelligence in Internet Access:

1. Sign in to `https://entra.microsoft.com` as **a Global Secure Access Administrator**.
2. Navigate to **Global Secure Access | Secure | Threat intelligence policies**.
3. In the right pane, click **Create policy** and give the policy a **Name** and **Description**. Click **Next**.
4. The default action is set to **Allow**. If traffic does not match a rule in the policy, it will be sent to the next security control. Click **Next**.
5. On the **Review** page, click **Create** to create the policy.

The policy is created with a default rule that blocks access to high-risk destinations with a priority order of 65000. This rule cannot be deleted or modified. Administrators can create an

allow list of sites that are required by the business so that traffic to them is never blocked by this default rule even if they are risky. Following are the steps.

1. From the list of threat intelligence policies, select the policy to which you would like to add the rule.
2. Click on **Rules | Add rule**.
3. Enter a **Rule name** and **Rule description**.
4. Define a priority order between 100 and 64,900.
5. Set the **Status** to **Enabled**.
6. Under **Destination FQDNs**, add the sites that you would like to allow and click **Save**. Refer to the following screenshot.

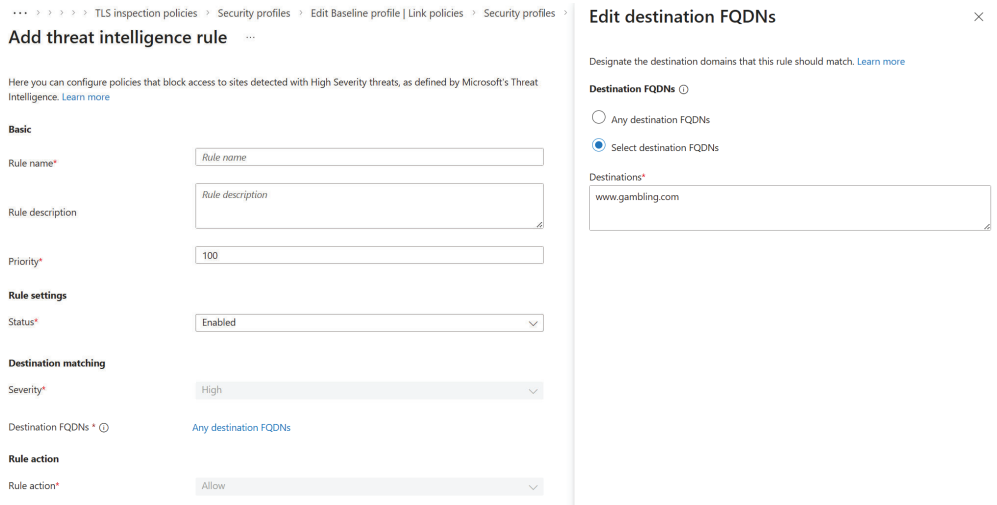


Figure 14.17: Create allowlist

7. Click **Add** to add the rule to the policy. The following figure shows the policy with the default rule and the allow rule.

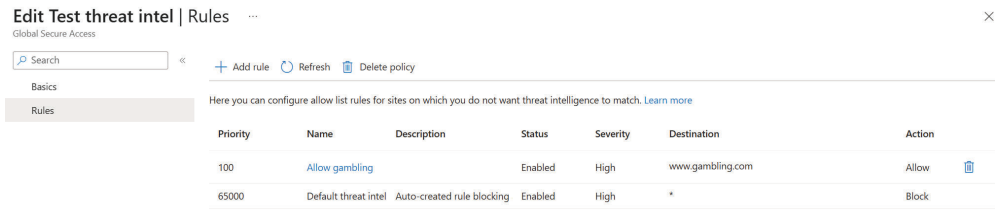


Figure 14.18: Threat intelligence policy

Additional rules can be added by clicking on **Add rule**, as shown in *Figure 14.18*.

Like other GSA policies, threat intelligence policies are also delivered through security profiles. The policy must be linked to either the baseline security profile which will enable threat intelligence for all users, or to a security profile specific to users or groups using a Conditional Access policy. This has been explained in the section *Configuring web content filtering*. Once this is enabled, users will be restricted from accessing high-risk sites and will receive a block message.

Configuring cloud firewall

The Cloud Firewall capability in Microsoft Entra Internet Access inspects outbound network traffic and enforces policies to prevent traffic from being sent to unapproved or risky destinations.

> **Note**
>
> This feature only applies to Remote Networks. GSA clients are not currently supported.

5-tuple rules based on IP, source port, destination IP, destination port and destination protocol (TCP, UDP) can be defined. Administrators can choose to block or allow access if traffic matches a defined rule.

Following are the steps to create a cloud firewall policy.

1. Sign in to `https://entra.microsoft.com` as **a Global Secure Access Administrator**.
2. Navigate to **Global Secure Access | Secure | Cloud firewall policies**.
3. In the right pane, click **Create firewall policy** and give the policy a **Name** and **Description**. Click **Next**.
4. The default action is set to **Allow**. Click **Next**.
5. On the **Review and create** page, click **Create** to create the policy.
6. Select the newly created policy and click on **Rules | Add rule**.
7. Give the rule a **Name** and **Description**. The **Priority** must be greater than or equal to 100 and unique within the policy.
8. Select the **Status** as **Enabled**.
9. Configure the source and destination IP ranges and ports.
10. Select the **Action** as **Allow** or **Block**. Click **Add** to add the rule. Refer to the following screenshot:

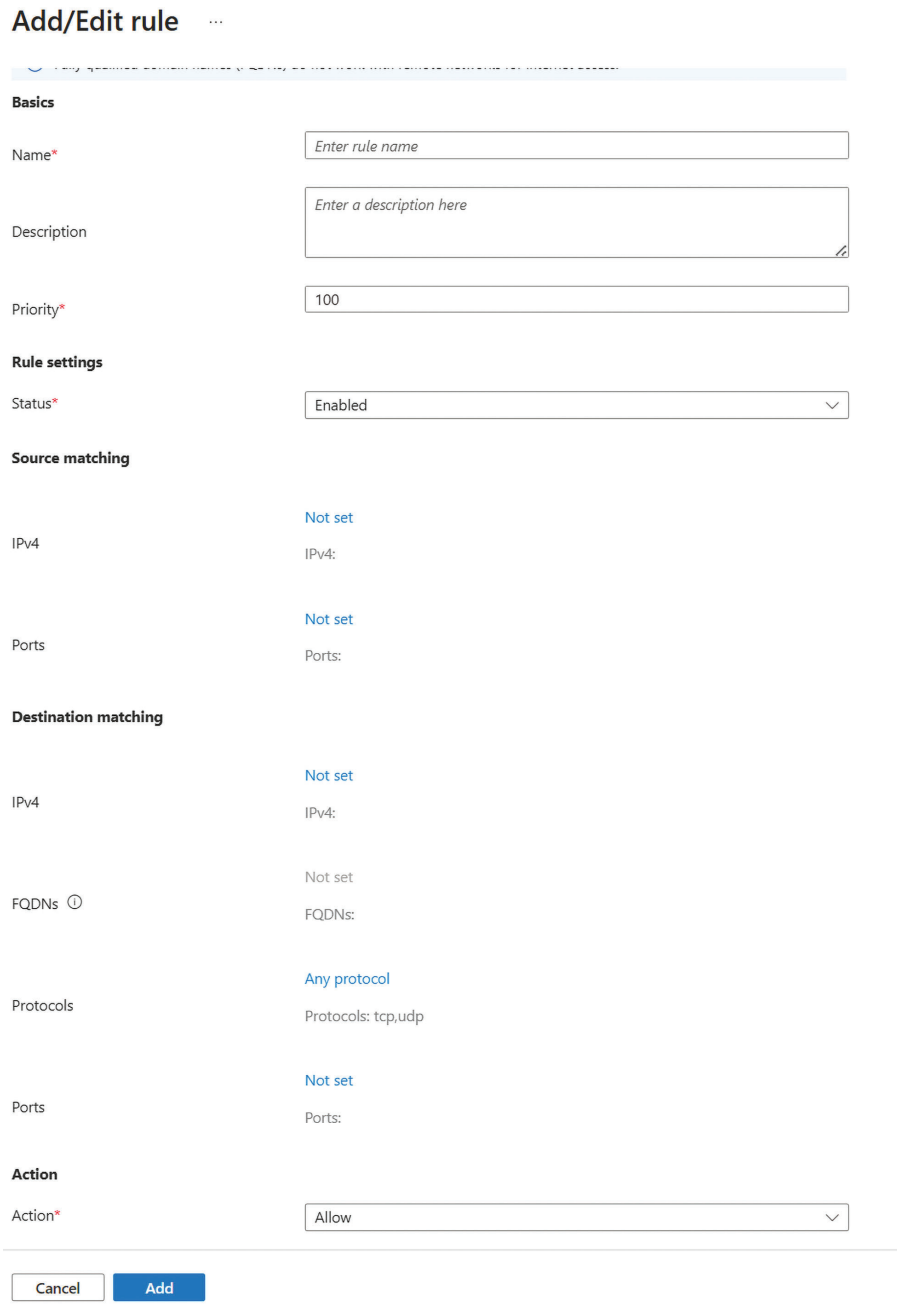


Figure 14.19: Cloud firewall rule

Cloud firewall policies are only delivered through the baseline profile. Only one cloud firewall policy can be linked to the baseline profile. Linking it to another security profile will have no effect.

It is recommended to create rules in the policy before linking it to the baseline profile. This ensures that all rules in the policy apply together. This is important if you want to create a block-all rule for the entire branch office and then add rules to allow certain traffic. Without this there is a risk of unintentionally blocking all branch traffic.

Network content filtering

File policies in GSA support network content filtering to help safeguard against data leakage into generative AI applications and other internet destinations. Using this, organizations can extend data protection capabilities to network traffic in real time. Administrators can discover whether protected files are being shared with unsanctioned destinations like generative AI and cloud applications from managed endpoints and browsers.

This solution integrates with Microsoft Purview's data classification service to provide **Data Loss Prevention (DLP)** at the network layer. This combination creates a DLP service at the network level that is identity-aware and policy-driven. Content is inspected in real-time and combined with user risk evaluation to enforce granular control over the movement of sensitive data.

> **Note**
>
> At the time of this writing, this feature supports filtering only for files over HTTP/1.1. Content filtering for text is currently not supported.

The following scenarios are supported:

- Block supported file types using the **Basic file policy**.
- Use the **Scan with Purview** feature to audit or block files based on Microsoft Purview sensitivity labels, sensitive information types and user risk levels.

Before configuring a file policy, ensure that the following prerequisites are met. These are in addition to the prerequisites described in the section *Prerequisites*:

- Internet Access traffic forwarding profile must be enabled.
- TLS inspection policy must be configured.
- GSA client must be installed.
- If you want to use the **Scan with Purview** feature, ensure you have a valid Microsoft Purview license and pay-as-you-go billing set up.

Following are the steps to configure a file policy:

1. Sign in to `https://entra.microsoft.com` as **a Global Secure Access Administrator**.
2. Navigate to **Global Secure Access | Secure | Content policies**.
3. In the right pane, click **Create policy** and give the policy a name and description. Click **Next**.
4. Click **Add rule**. Enter a **Rule name** and **Description**.
5. Configure a rule **Priority** and set the **Status** as **Enabled**.
6. Under **Action**:
    a. To configure a basic policy, select **Allow** or **Block**.
    b. To use data policies from Microsoft Purview, select **Scan with Purview**. If this option is selected, a corresponding data policy must be configured in Microsoft Purview.
7. Under **Activities**, select if you want to inspect content at **Upload** or **Download**.
8. Under **Content types**, select the file types that you want to inspect.
9. Click **Add destination** to add the Web Category, FQDN or URL destinations. Click **Save**. Refer to the screenshot below:

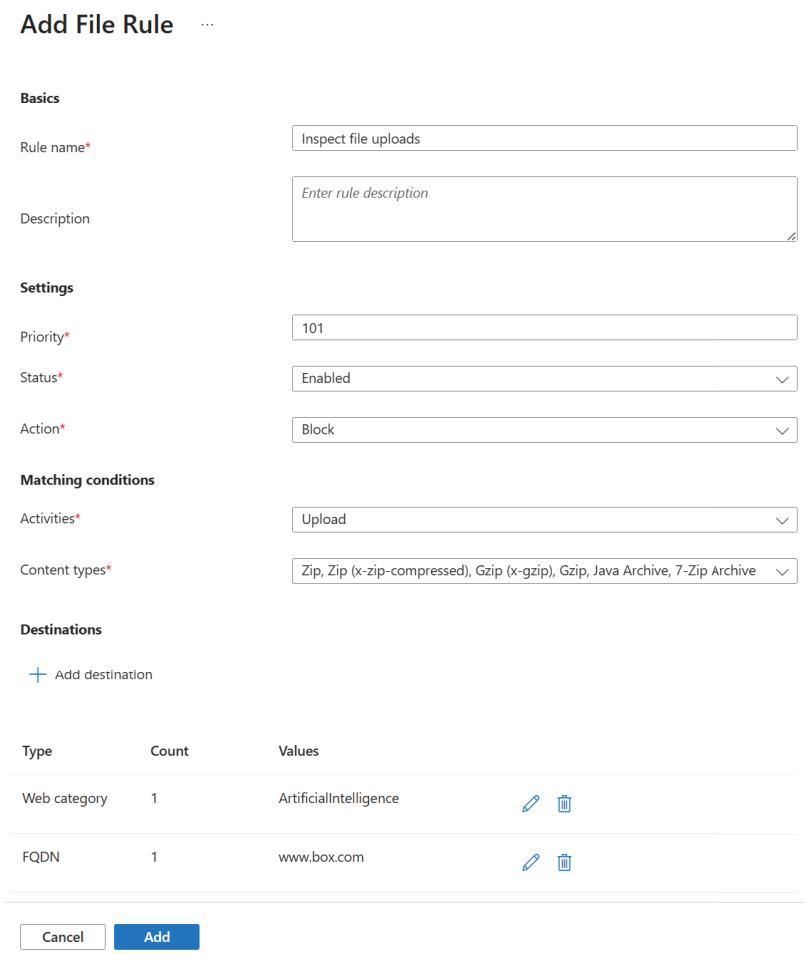


Figure 14.20: Create file policy

10. Click **Next**. On the **Review** page, click **Create** to create the policy.

Like other GSA policies, file policies are also delivered through security profiles. The policy must be linked to a security profile specific to users or groups using a Conditional Access policy. This has been explained in the section *Configuring web content filtering*.

Configuring the AI Gateway prompt injection protection

Generative AI apps are susceptible to prompt injection attacks. Bad actors try to enter malicious prompts in Generative AI apps which can make the **Large Language Model (LLM)** ignore previously given instructions, expose sensitive data, and perform unintended actions. The AI Gateway capability in GSA protects these generative AI applications and agents from

these kinds of attacks. Prompt injection protection provides real-time protection against prompt injection attacks by enforcing guardrails at the network level for all generative AI apps without requiring code change. It blocks adversarial prompts and jailbreak attempts and prevents unauthorized data exfiltration from any managed device or browser.

Before creating a prompt policy ensure that a TLS inspection policy is configured. Following are the steps to create a prompt policy:

1. Sign in to `https://entra.microsoft.com` as **a Global Secure Access Administrator**.
2. Navigate to **Global Secure Access | Secure | Prompt policies**.
3. In the right pane, click on **Create policy**. Enter a **Policy name** and **Description** and click **Next**.
4. On the **Rules** page, click **Add rule**. Enter a **Rule name**, **Description**, and **Priority**.
5. Select **Status** as **Enabled** and **Action** as **Block** to block malicious prompts.
6. Click **Conversation scheme** to choose the target LLM for your enterprise generative AI.
7. From the **Type** drop down box, select the required language model and click **Add** as shown below. Multiple schemes can be selected.

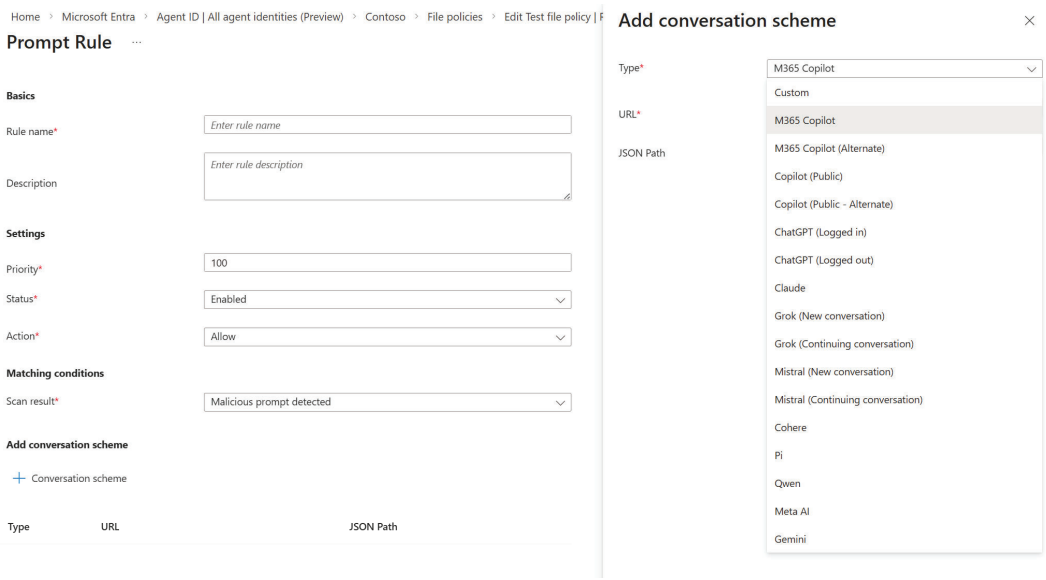


Figure 14.21: Create a prompt policy

8. Click **Add** to add the rule. Click **Next**.
9. On the **Review** page, click **Create** to create the rule.

Like other GSA policies, prompt policies are also delivered through security profiles. The policy must be linked to a security profile specific to users or groups using a Conditional Access policy. This has been explained in the section *Configuring web content filtering*.

Note

At the time of this writing, prompt injection protection only supports text prompts. Files are not yet supported.

Configuring Secure Web and AI Gateway for Microsoft Copilot Studio agents

Microsoft Copilot Studio is a platform that enables users to create, manage, and deploy AI-powered conversational agents. It integrates with Microsoft's ecosystem, allowing users to build custom workflows, automate tasks, and enhance productivity through natural language interactions and generative AI capabilities. GSA network controls now enable organizations to implement granular access controls to agents built using Microsoft Copilot Studio. Web content filtering, threat intelligence and network file filtering policies can be applied to agent traffic. Using these features organizations can extend similar security controls for agents that they use for other types of traffic enabling secure communication between agents and external resources.

Following are the prerequisites to enable security for Microsoft Copilot Studio agents:

- A **Global Secure Access Administrator** role.
- A **Power Platform Administrator** role to manage Microsoft Copilot Studio environment.
- A Power Platform environment with Dataverse added.

Following are the steps to enable network controls for Copilot Studio agents:

1. Log in to `https://admin.powerplatform.microsoft.com/` as a **Power Platform Administrator**.
2. Navigate to **Security | Identity & access | Global Secure Access for Agents**.
3. Select the Power Platform environment and click **Set up**.
4. Once the setup is complete, toggle the **Enable Global Secure Access for Agents** to on and click **Save**.

> **Note**
>
> Existing Copilot Studio custom connectors must be edited and saved after enabling GSA for agents to ensure that the traffic is routed through GSA.

This enables network controls so that GSA security policies can be enforced on agent traffic. You can now create web content filtering policies, threat intelligence policies or file policies to protect your agent and prevent unauthorized data exposure and data leaks.

Microsoft Entra Internet Access for Microsoft Services

This feature improves security and enhances performance for Microsoft 365 services. The following are some of the key features:

- It enables users to connect directly to Microsoft services using traffic forwarding profiles from any client or remote network.
- It can apply tenant restrictions to reduce risk of data exfiltration to foreign tenants or personal accounts.
- It can perform source IP restoration to help improve the accuracy of threat detections.
- It can leverage Conditional Access policies to require **Compliant Network check** for Entra ID applications integrated with Conditional Access.

To use Microsoft Entra Internet Access for Microsoft Services the Microsoft traffic profile must be enabled in Global Secure Access.

Microsoft traffic profile

This profile acquires traffic for Microsoft 365 services like Exchange Online, SharePoint Online, Microsoft Teams and other Microsoft apps. This profile ensures best performance for these services and simplifies configuration of the rules that govern traffic acquisition. **Microsoft traffic policies** (*Figure 14.3*) consists of rules that include the **Destination Type**, **Protocol**, **Ports**, **Category**, and **Action**. These are derived from the master Microsoft 365 IP and FQDN list. Rules are grouped by workload. You can use the **Enable/Disable** check box to indicate if the traffic for that group should be bypassed or acquired. When a group is enabled, the GSA client or remote network will acquire all traffic for that workload. Individual rules can be configured for an enabled group. For each rule, if **Action** is set to **Forward**, traffic for the specified destination will route through the GSA client or Remote network. Setting a rule to **Bypass** will send that traffic over the client's network routing path to egress to the internet. Refer to the following screenshot:

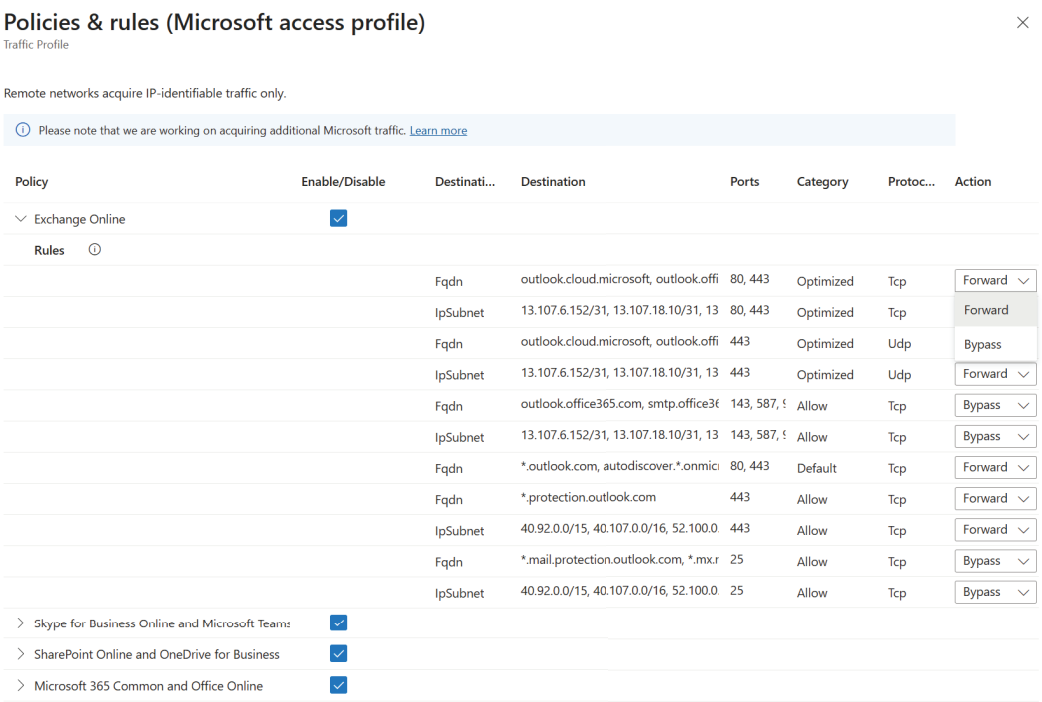


Figure 14.22: Policies in Microsoft traffic profile

When the Microsoft traffic profile is first enabled, the rule list is populated based on the supported traffic at the time. When Microsoft introduces new rules, they are added to the profile as enabled, with the action set to **Forward**.

Licensing

Microsoft Entra Internet Access is available as a standalone license or as part of the Microsoft Entra Suite license.

Microsoft Entra Internet Access for Microsoft Services is included in the Microsoft Entra ID P1 and P2 licenses.

Summary

This chapter introduced Microsoft's new identity-centric Secure Services Edge solution. It started with an introduction of Global Secure Access, the GSA client and the traffic forwarding profiles. It then went deep into explaining Microsoft Entra Internet Access. You learned the relationship between GSA policies, security profiles and Conditional Access policies. You then learned how to configure web content filtering, TLS inspection, threat intelligence, cloud

firewall and file policy. This chapter also explained how GSA can be used to protect information from being shared with generative AI applications using Prompt Shield and protect traffic to and from Microsoft Copilot Studio Agents. In the next chapter, we will learn how Microsoft Entra Private Access provides secure access to private applications from any device and any network.

Exercises

1. What is the primary purpose of Microsoft Entra Internet Access?
    a. To manage device compliance policies for Windows endpoints
    b. To host internal applications for remote access
    c. To synchronize on-premises directories with Microsoft Entra ID
    d. To provide secure, identity-aware access to internet destinations using Zero Trust principles
2. Which capability is unique to Microsoft Entra Internet Access compared to traditional secure web gateways?
    a. Blocking access to malicious URLs using static URL filtering
    b. Enforcing identity-aware access policies based on user, device, and session risk
    c. Providing basic firewall rules for outbound traffic
    d. Allowing administrators to configure DNS forwarding for internal domain
3. Which component is required for Microsoft Entra Internet Access to apply identity aware policies to outbound traffic?
    a. Microsoft Defender for Endpoint
    b. Global Secure Access client
    c. Azure Firewall Premium
    d. Microsoft Entra Connect Sync

Answers

1. d
2. b
3. b

Additional resources

- Global Secure Access points of presence: `https://learn.microsoft.com/en-us/entra/global-secure-access/reference-points-of-presence`
- Role-Based Access Control in GSA: `https://learn.microsoft.com/en-us/entra/global-secure-access/reference-role-based-permissions`
- Remote network connectivity: `https://learn.microsoft.com/en-us/entra/global-secure-access/concept-remote-network-connectivity`
- How to add remote device links: `https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-manage-remote-network-device-links?tabs=microsoft-entra-admin-center`
- Best practices for GSA network resilience: `https://learn.microsoft.com/en-us/entra/global-secure-access/remote-network-resilience`
- What is TLS inspection? `https://learn.microsoft.com/en-us/entra/global-secure-access/concept-transport-layer-security`

Join us on Discord

For discussions around the book and to connect with your peers, join us on Discord at `packt.link/discordcloud` or scan the QR code below:



15

Microsoft Entra Private Access

In today's increasingly hybrid and remote working environments, organizations face significant challenges in providing secure access to private, internal applications. Traditional **Virtual Private Network (VPN)** solutions, while widely used, are often complex to manage, may introduce vulnerabilities, and do not always provide granular, identity-based controls. Microsoft Entra Private Access addresses these modern security needs by enabling secure, seamless connectivity to private applications—regardless of whether users are working from a corporate office, home, or on the move.

The need for Microsoft Entra Private Access arises from the shift toward zero trust security principles. Rather than relying on a trusted network perimeter, organizations now require robust mechanisms to ensure that only authenticated and authorized users can access sensitive resources. With the proliferation of cloud adoption and **bring-your-own-device (BYOD)** policies, the risk of unauthorized access and data breaches increases. Microsoft Entra Private Access integrates with Microsoft's identity services, allowing for policy-driven access controls, real-time monitoring, and adaptive security responses based on user context and risk. Furthermore, it simplifies the user experience by eliminating the need for cumbersome VPN connections while offering IT teams centralized visibility and governance.

In this chapter, we will cover:

- Introduction to Microsoft Entra Private Access
- Private Access for domain controllers
- Application usage analysis
- Logs and monitoring

Understanding Microsoft Entra Private Access

Microsoft Entra Private Access is a modern solution designed to provide secure, seamless access to private, internal applications for users in any location. Built to support today's remote and hybrid work environments, it eliminates the complexity of traditional VPNs and enables organizations to adopt a Zero Trust security model. Users connect to internal applications and resources using the **Global Secure Access (GSA)** client installed on their devices. By integrating with Microsoft Entra's identity services, Private Access ensures that only authenticated and authorized users can reach sensitive resources, using adaptive policy controls and real-time monitoring. This approach simplifies remote access for end users while granting IT teams centralized visibility, governance, and the ability to enforce robust security measures across the enterprise.

The Private Access traffic profile determines the traffic to be routed through the GSA client. This profile is enabled in the Microsoft Entra Admin center by navigating to **Global Secure Access | Connect | Traffic forwarding** and switching the toggle to on as shown in the following screenshot:

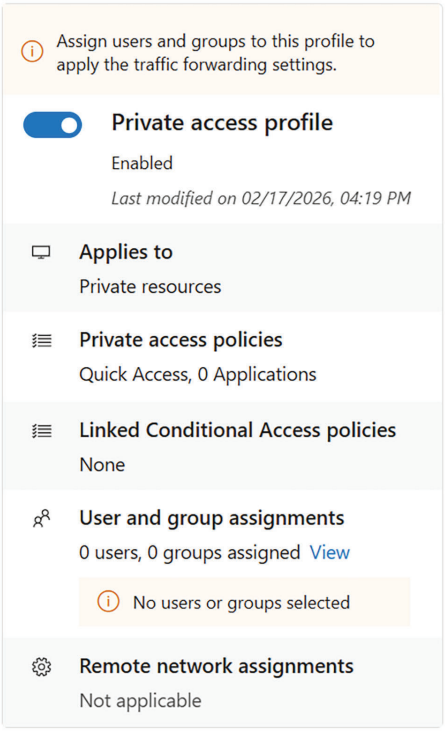


Figure 15.1: Private Access profile

Users and groups can be assigned to this profile by clicking on **View** and selecting either all users or specific users or groups. Administrators must be logged in using an account that has both the **Global Secure Access Administrator** and the **Application Administrator** roles assigned.

There are two ways to configure access to private resources that you want to make accessible through the GSA service.

Quick Access

Quick Access is a group of **Fully Qualified Domain Names (FQDNs)** and IP addresses that the organization wants to secure. When quick access is configured for the first time, a new enterprise application is created and is automatically configured to work with Private Access. Employees can then access the specified applications using the GSA client. The following figure shows a Quick Access configuration:

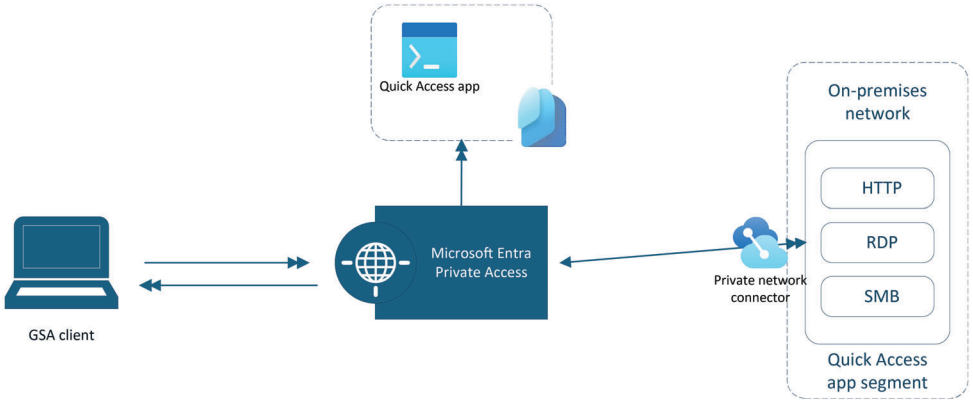


Figure 15.2: Quick Access architecture

Quick Access can be used as a transition state toward a Zero Trust posture.

Organizations looking to replace their VPN can start by using Quick Access to rapidly secure all private network traffic through Microsoft's global backbone with identity-based controls. Once traffic patterns are understood and apps are discovered, they can transition to per-app access, applying granular Zero Trust policies to each application, reducing lateral movement, and fully eliminating traditional VPN dependencies.

Creating a private network connector group

The first step is to configure a connector group with at least one active Microsoft Entra Private Access connector. Each connector group can handle traffic for specific applications. A connector group operates as a single unit. Therefore, it is recommended to configure at least two connectors in each connector group for high availability and load balancing. Connectors

can be added or removed at any time. Location based connector groups can reduce latency for large organizations that have applications in many regions by having each connector group serve local applications.

Connectors are lightweight agents installed on a Windows Server in a private network and facilitate outbound connection to the GSA service. This Windows Server must have access to the on-premises applications. Users connect to the GSA service which uses these connectors to route traffic to the on-premises applications.

Following are the prerequisites to configure a private network connector:

- An account with the **Application Administrator** role assigned.
- User identities must be either created directly in Microsoft Entra or synchronized from on-premises Active Directory. This allows Microsoft Entra to pre-authenticate users before granting access to the Private Access service.
- A server running Windows Server 2016 or later to install the connector with .NET version 4.7.2 or later and TLS 1.2 enabled. It is recommended to have more than one server for high availability.
- Open outbound ports 443 and 80.
- Allow access to the service URLs as listed in `https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-configure-connectors#allow-access-to-urls`.
- Minimum connector version 1.5.3417.0.

Following are the steps to install a connector and create a connector group:

1. Sign in to `https://entra.microsoft.com` as an **Application Administrator**.
2. Navigate to **Global Secure Access | Connect | Connectors and sensors**.
3. In the right pane, click **Download connector service**. In the flyout pane, click **Accept terms & Download**.
4. Install this connector on the Windows Server.
5. You will be prompted to register the connector with the service. Provide your **Application Administrator** credentials.
6. To verify that the connector installed correctly, navigate to **Global Secure Access | Connect | Connectors and sensors**. All installed connectors should appear on this page with status **Active**. Refer to the following screenshot.

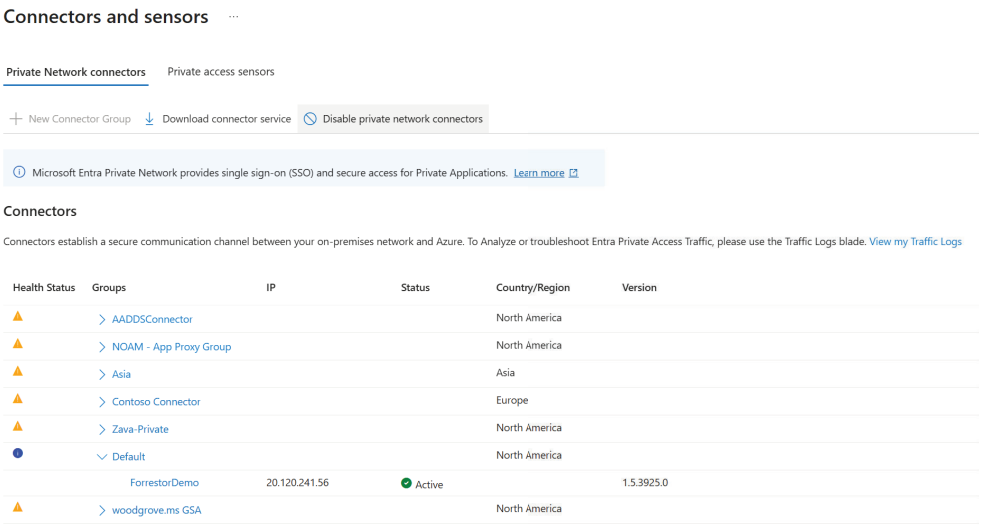


Figure 15.3: Installed connectors

7. To create a new connector group, click on **New Connector Group** on the **Connectors and sensors** page. Give the connector group a name and add the connectors that belong to this group.
8. By default, a tenant's default geo location determines how Microsoft Entra routes traffic for private access. If a tenant's geo location is North America, all connector groups will connect to the Microsoft Entra service in North America even if some applications are in different regions. Using **multi-geo capability**, organizations can optimize traffic flow by assigning connector groups according to their preferred geo locations instead of the default tenant location. This capability provides organizations with flexibility to direct connections to the GSA backend of their choice. To optimize traffic flow, select the country or region as shown in the following screenshot. Click **Save**.

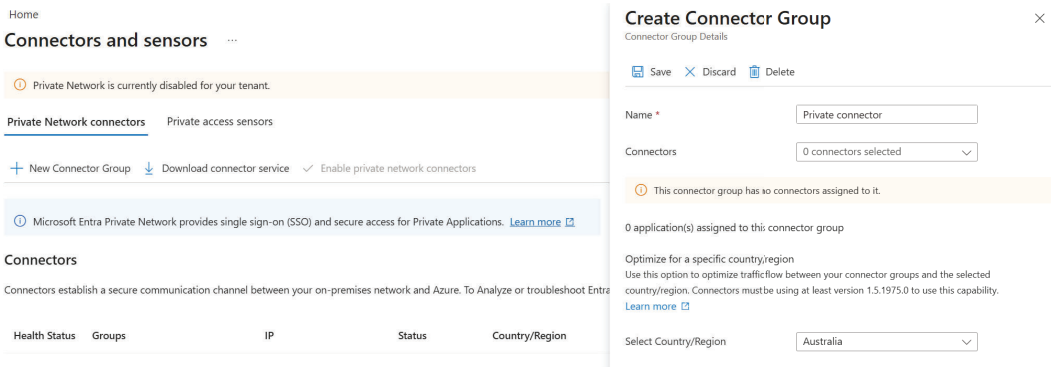


Figure 15.4: Creating a connector group

Once the connector group is created, you can proceed to configure Quick Access.

Configuring Quick Access

While configuring Quick Access, you select the connector group and specify the FQDNs and IP addresses. The following are the steps:

1. Sign in to `https://entra.microsoft.com` as a **Global Secure Access Administrator** and **Application Administrator**.
2. Navigate to **Global Secure Access | Applications | Quick Access**.
3. In the right pane, specify a name and select a connector group from the drop-down box. It is recommended to name this app *Quick Access*.
4. Click on **Add Quick Access application segment**. In the flyout pane, select the **Destination type** from the drop-down. You can select an IP address, FQDN or an IP address range.
5. Enter the other details and click **Apply**. Multiple destinations can be added in a single Quick Access configuration. Once done, click **Save**. Refer to the following screenshot.

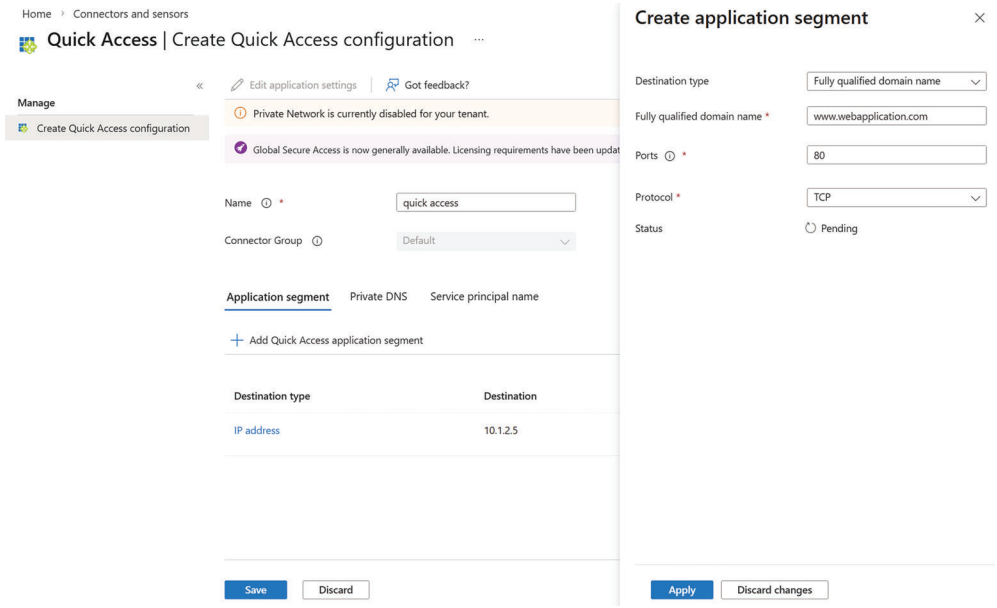


Figure 15.5: Configure Quick Access

Once Quick Access is configured, a new enterprise application is created. Access needs to be granted to the app by assigning users and groups to it. This can be done by clicking on **Edit application settings** in *Figure 15.5* and selecting user and groups from the flyout pane. Alternatively, you can do this directly in the application by navigating to **Global Secure Access | Applications | Enterprise applications**.

Applying Conditional Access policies

Using Conditional Access policies is a powerful way to enforce user-aware and context-aware security policies to on-premises resources. The following are the steps to apply Conditional Access policies to Quick Access and Private Access apps:

1. Sign in to `https://entra.microsoft.com` as a **Conditional Access Administrator**.
2. Navigate to **Global Secure Access | Applications | Enterprise applications**.
3. Select the Quick Access app from the list and click on **Conditional Access**.
4. In the right pane, click **New policy**. The **Target resource** will already be selected as the Quick Access app selected in *Step 3*.
5. Configure conditions, access control and assign users and groups as needed.

The Private Access profile will now start acquiring traffic, to forward to the GSA service.

Per-app access

Organizations often have varying security needs for private resources, such as different Conditional Access policies for specific users or limited-time access. Microsoft Entra Private Access enables per-app controls using Global Secure Access apps, allowing fine-grained access management for various private applications. Multiple Global Secure Access apps can be created to address distinct app segments. The following figure shows per-app access architecture:

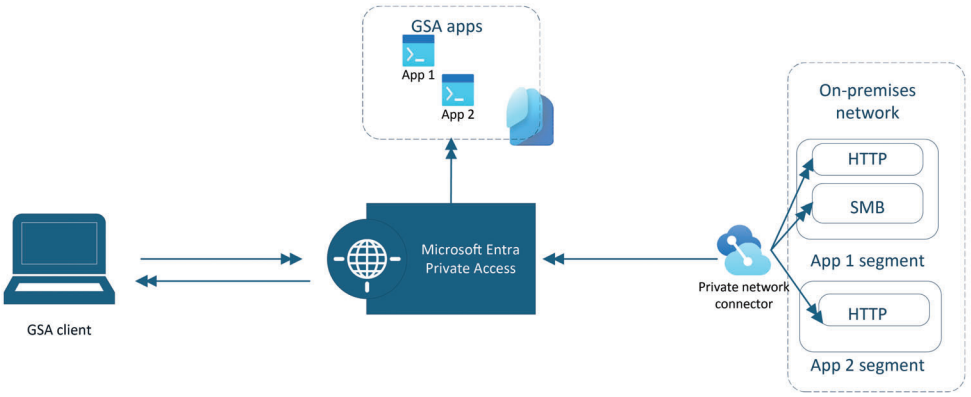


Figure 15.6: Per-app access architecture

Configuring per-app access involves creating the Global Secure Access apps and assigning users and groups to the app. Before continuing, ensure that the following prerequisites are met:

- You must have the **Global Secure Access Administrator** and the **Application Administrator** roles assigned.
- Create a connector group with at least one active private network connector. This is explained in the section, *Creating a private network connector group* earlier in this chapter.

Now you can proceed with creating the Global Secure Access app.

Creating a Global Secure Access app

Fine-grained access to private app segments is provided using Global Secure Access apps. Unlike Quick Access, where the enterprise application is automatically created when Quick Access is configured, for per-app access the application must be manually created. The following are the steps to create a Global Secure Access app:

1. Sign in to `https://entra.microsoft.com` as a **Global Secure Access Administrator** and **Application Administrator**.

2. Navigate to **Global Secure Access | Applications | Enterprise applications**.
3. In the right pane, click on **New application**.
4. Give the application a name and select the Connector Group.
5. Click on Add application segment and add the application segment based on IP address, IP range or FQDN. Click Apply.
6. Ensure that the box Enable access with Global Secure Access client is checked and then click Save. Refer to the following screenshot:

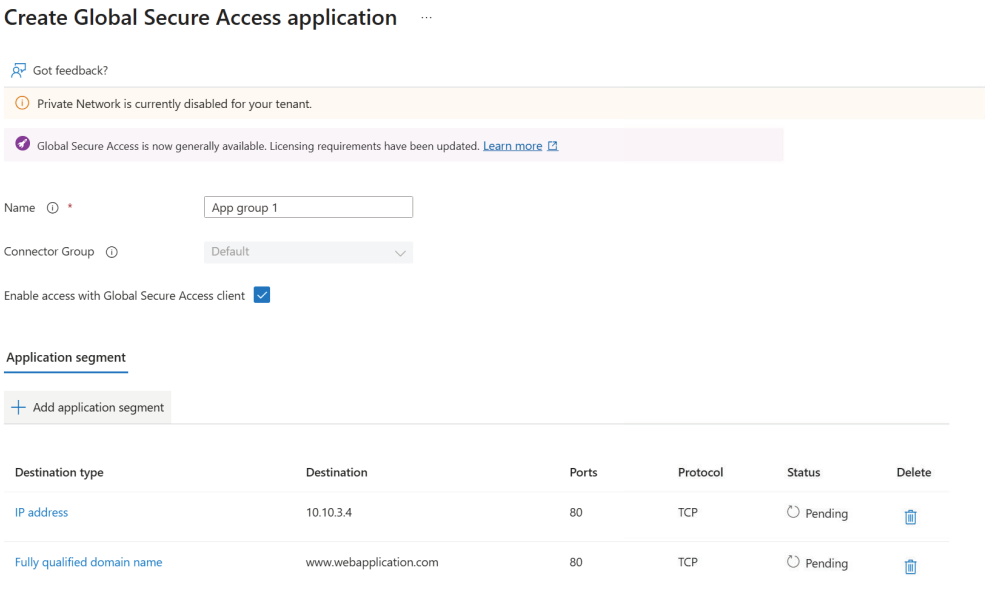


Figure 15.7: Global Secure Access application

Access needs to be granted to the app by assigning users and groups to it. In the **Global Secure Access | Applications | Enterprise applications** page, select the application just created and click on **Users and groups**. Add users and groups as needed.

Conditional Access policies can now be applied to the Global Secure Access app by following the steps explained in the section *Applying Conditional Access policies* above.

The Private Access profile will now start acquiring traffic, to forward to the GSA service.

Application discovery

The application discovery feature in GSA allows organizations to see which applications are used by users in their corporate network. This empowers organizations to create private applications with proper segmentation and least privilege access. Application discovery

leverages Quick Access, which can be configured with wide IP ranges and wildcard FQDNs to discover applications in use. This information can then be used to configure granular per-app access supporting **Zero Trust Network Access** (**ZTNA**) by replacing traditional VPN-style access with identity-based, app-level controls. This helps organizations move from not knowing which apps they have, to being able to enforce Zero Trust per application. It solves the common challenges of visibility gaps, over permissive VPN access, and complex migrations. By surfacing real usage data, Microsoft Entra helps prioritize which apps to onboard, define access policies, and tighten segmentation without breaking workflows.

To use application discovery, Quick Access must be configured, and the GSA client must be installed on devices.

To view a list of all applications accessed by users via Quick Access, follow the steps below:

1. Sign in to `https://entra.microsoft.com` as a **Global Secure Access Administrator**.
2. Navigate to **Global Secure Access | Applications | Application discovery**.

This view lists all application segments in descending order by the number of users. For each application segment, the destination FQDN, IP, protocol, port, number of users and devices and bytes sent and received are displayed as shown below:

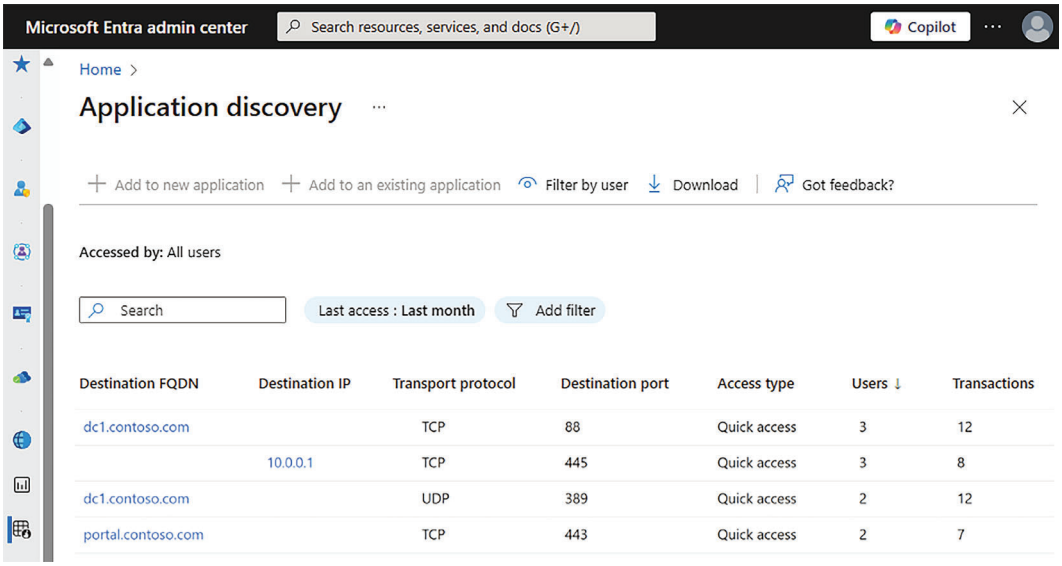


Figure 15.8: Application discovery

This raw network traffic data can be used to create actual, enforceable Zero Trust application boundaries. When application discovery identifies an internal app, it provides a blueprint of how that app behaves on the network. It groups related endpoints into possible applications.

For example, `hr.app01.corp.local:443`, `hr.api.corp.local:443`, and `10.1.20.15:443` may be grouped together. Administrators can decide if these endpoints belong to one private app or multiple. From within the application discovery page, they can create a new application containing these endpoints or add these endpoints to an already existing application. Refer *Figure 15.8*. These are not traditional enterprise applications. They are Global Secure Access apps. Creating an application involves naming the application, selecting the connector groups and defining the application segments (FQDN, IP addresses or IP ranges). Conditional access policies can then be applied to these Global Secure Access applications to make them user and context-aware. This way, application discovery helps organizations move from open VPN-like access to granular per-app access and achieve a Zero Trust posture.

Intelligent local access

Microsoft Entra Private Access routes all traffic between the GSA client and private applications through the GSA service regardless of the client location. Intelligent local access automatically detects when a device is on the corporate network and optimizes traffic flow by routing internal application requests directly, rather than through the GSA service. This reduces latency and improves performance while maintaining security and access controls for internal resources.

To enable Intelligent local access, define the private networks and add applications to it using the following steps:

1. Sign in to `https://entra.microsoft.com` as a **Global Secure Access Administrator**.
2. Navigate to **Global Secure Access** | **Connect** | **Private networks**.
3. In the right pane, click **Add Private network**.
4. In the flyout pane, give the network a **Name**, define the **DNS servers** for name resolution and enter the FQDN that needs to be resolved.
5. In the **Resolved to IP address type**, select an **IP address** or **IP address range (CIDR)** or **IP address range (IP to IP)**.
6. Under **Target Resource**, select the GSA applications you want to bypass when clients are connected to the defined network and click **Create**. Refer to the following screenshot:

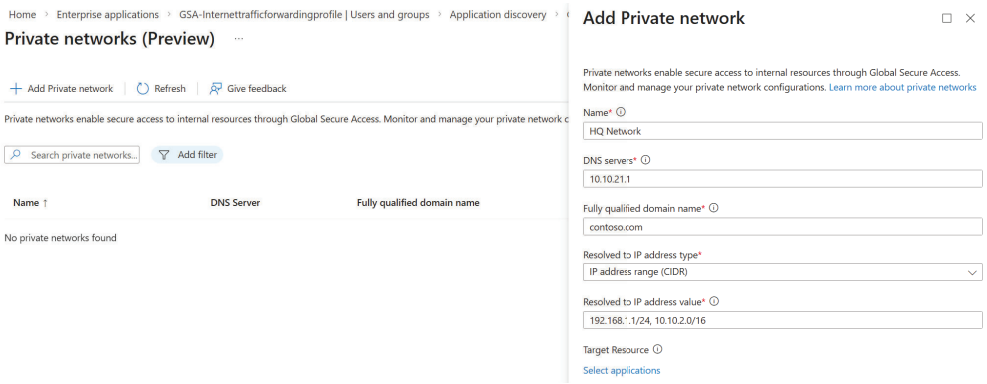


Figure 15.9: Intelligent local access

Traffic for the defined GSA apps will now bypass the GSA service when the GSA client is connected directly to the corporate network.

Securing access to private apps with Privileged Identity Management

Most organizations have high value servers and applications on their private networks. Microsoft Entra Private Access enables users to access these high value assets from anywhere. Microsoft Entra Private Access integrates with **Privileged Identity Management (PIM)** to add an extra layer of security by enforcing just-in-time access to critical resources. This also ensures that the organization meets compliance requirements by providing detailed logging and tracking of privileged access requests.

Following are the prerequisites for enabling PIM:

- Application Administrator, Global Secure Access Administrator, and Privileged Role Administrator roles.
- Private Access profile enabled with users and groups assigned.
- A connector group created with at least one active private network connector. This is explained in the section, *Creating a private network connector group* earlier in this chapter.
- A Microsoft Entra ID license that includes Privileged Identity Management.

Following are the steps to configure PIM:

1. Sign in to `https://entra.microsoft.com` as a **Global Secure Access Administrator**.
2. Navigate to **Global Secure Access | Applications | Quick Access**.
3. In the right pane, click on **Private DNS** and check the box **Enable Private DNS**.

4. Add a DNS suffix and click **Save**. Refer to the following screenshot.

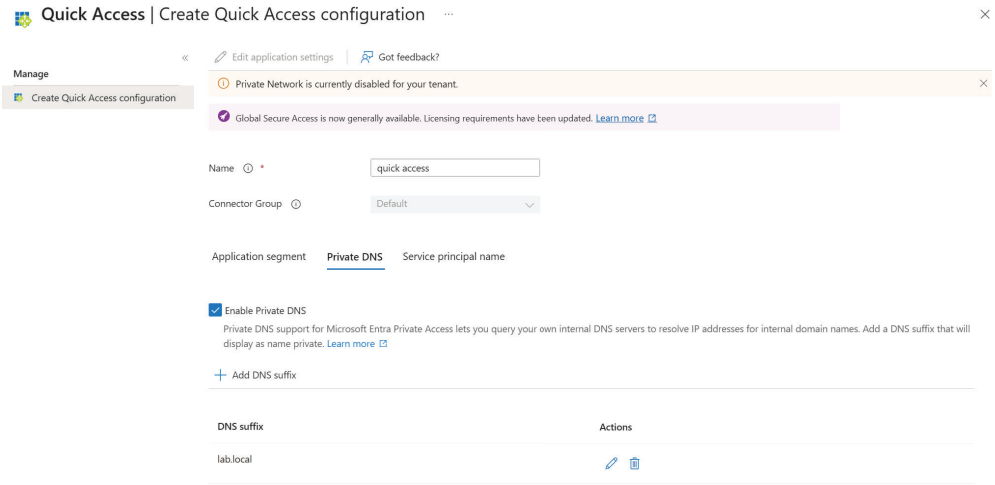


Figure 15.10: Enable Private DNS

5. Ensure users and groups are assigned to Quick Access.
6. Create a Global Secure Access app for the high value critical application you want to protect. The steps are explained in the section *Creating a Global Secure Access app* previously in this chapter. Ensure that a group is assigned to this application. This is the group that will be enabled for PIM.

Now that the GSA part is configured and the group assigned to the GSA application, it must be enabled for PIM. This is explained in detail in *Chapter 8, Microsoft Entra Privileged Identity Management*.

Users wanting to access the high-value critical application can now use PIM to activate their group membership and access the application using the GSA service.

Kerberos for Single Sign-On

Kerberos for **single sign-on (SSO)** is a secure authentication protocol that allows users to access multiple resources without repeatedly entering their credentials. When integrated with Microsoft Entra Private Access, Kerberos SSO streamlines access to on-premises applications and resources by using users' existing Active Directory credentials. This means that once a user signs in and is authenticated, a Kerberos ticket is issued, which can then be used to transparently access other resources within the organization's network that support Kerberos authentication.

With Microsoft Entra Private Access, organizations can enable Kerberos SSO for applications that are not directly exposed to the internet but require secure, seamless authentication. This

feature eliminates the need for users to remember multiple passwords and reduces the risk of credential theft or phishing, as authentication happens in the background. By leveraging Kerberos, Microsoft Entra Private Access ensures that users have a consistent and secure sign-on experience, whether they are working from the corporate network or remotely. Additionally, organizations can integrate with Windows Hello for Business cloud Kerberos trust to allow SSO for users.

Following are the prerequisites to get started with SSO:

- An Active Directory forest.
- Microsoft Entra Private Access traffic forwarding profile enabled.
- Microsoft Entra Private Access connector installed and running.
- GSA client installed on user devices.

To enable Kerberos for SSO, publish the resources that will be used with SSO. These are the on-premises resources that you want to enable SSO for, like, file shares. An enterprise application must be created in GSA with an app segment containing the on-premises resources and users and groups added to it.

If users are using passwords to sign in to Windows, no further configuration is required. Microsoft Entra ID joined devices use Active Directory domain and user information that is synchronized using Microsoft Entra ID Connect. Due to this synchronization, the domain controller locator can find domain controllers. Then the user's UPN is used to request a Kerberos **Ticket Granting Ticket (TGT)**.

If organizations would like to use **Windows Hello for Business (WHfB)** for SSO, it is recommended to deploy Hybrid Cloud Kerberos Trust. Devices using cloud Kerberos trust get a TGT that is used for SSO. To deploy cloud Kerberos trust with on-premises Active Directory, organizations need to create the Microsoft Entra ID Kerberos server object and enable WHfB Cloud Trust on devices.

For clients to obtain Kerberos tickets, domain controllers must be published. Kerberos tickets are used for SSO to on-premises resources. Publish all Domain Controllers in the Active Directory site where the Private Access connector is deployed. To publish a Domain Controller, create an enterprise application with an application segment containing all Domain Controllers. Add all users and groups synchronized from on-premises Active Directory to this application.

Private DNS will also have to be published to enable GSA clients to resolve private DNS names which are required for SSO. Clients use the DNS names to access published on-premises resources. This has been explained in the *Securing access to private apps with Privileged Identity Management* section.

Source IP anchoring

Source IP anchoring is a network-security technique that ensures your outbound traffic always appears to come from a specific, predictable public IP address, even when users are remote, mobile, or connecting through distributed cloud edges. This matters because many SaaS and line-of-business apps still rely on IP allowlists or location-based access controls to decide who can connect.

It forces selected traffic to egress through a fixed IP controlled by your organization. Even if a user is working from home, roaming, or connecting through a cloud security service, the application sees the same trusted IP.

This is used to:

- Maintain compatibility with legacy SaaS apps that require static IP allowlisting.
- Enforce network-based access policies without forcing all traffic through a physical office.
- Support Zero Trust transitions while keeping older controls intact.

Microsoft Entra Private Access routes specific application traffic through a private network connector, so the app always sees an organization-owned egress IP. This satisfies apps that enforce access based on known network locations. This is done by configuring an enterprise application in GSA. The GSA client on the device then acquires the traffic and routes it through the GSA service to a private network with a private network connector configured. The private network connector then passes the traffic through the egress point to the SaaS application. The following figure shows the traffic flow.

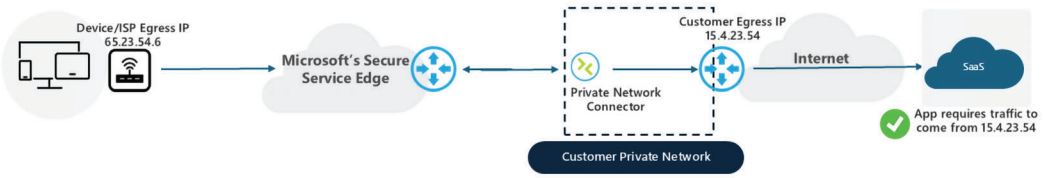


Figure 15.11: Source IP anchoring

In the above example, the SaaS application only accepts traffic from a predefined IP address which is the egress point of the organization's on-premises network. GSA routes traffic from all clients through the SSE tunnel where Conditional Access policies can be applied. The traffic is then sent to the on-premises network using the Private Network Connector and uses the egress point to connect to the SaaS application. The SaaS application recognizes the IP address and allows access.

Source IP anchoring is only required when SaaS applications enforce their own network-based controls. If the requirement is only limited to enforcing location, a compliant network check is sufficient.

Before configuring source IP anchoring, ensure that the following prerequisites are met:

- A private network with a private network connector configured.
- Provide the public IP of the connector to the SaaS application.

Following are the steps to configure source IP anchoring:

1. Create an enterprise application in GSA.
2. Select the connector group that will acquire the traffic for the SaaS application.
3. Add an application segment containing the SaaS application FQDN, ports (80/443), and protocol (TCP).
4. Add appropriate users and groups.

The GSA client on the users' devices should now start acquiring traffic for the SaaS application. This traffic will be routed through the GSA service to the on-premises private network connector and will egress to the internet through the organization's known egress IP address. The SaaS application will recognize the public IP and grant access.

Private Access for Domain Controllers

Ensuring private access for domain controllers is critical for safeguarding sensitive authentication and directory services within an organization. Exposing domain controllers to the public internet poses significant security risks, including unauthorized access and potential data breaches. Microsoft Entra Private Access provides a secure, identity-centric solution that enables users to connect to domain controllers from any device or network without exposing them to external threats. By leveraging Microsoft Entra Private Access, organizations can maintain strict control over who can access on-premises applications that use Kerberos authentication by enforcing Conditional Access policies and ensuring that only authenticated and authorized users are granted entry, significantly reducing the attack surface.

Prerequisites

Following are the prerequisites to configure Private Access for Domain Controllers:

- A **Global Secure Access Administrator** role.
- A Windows 10 machine that is Microsoft Entra joined or hybrid joined. The machine should have the GSA client installed and must have direct line of sight to the private resources and the domain controller.
- Private Access profile enabled.

- The user identity used to join the machine must be created in Active Directory and synchronized to Microsoft Entra ID using Microsoft Entra Connect.
- Latest version of Microsoft Entra Private network connector with direct line of sight to the domain controller.
- Open inbound TCP port 1337 in the firewall on the domain controllers.
- The firewall or proxy must allow outbound connections to `*.msappproxy.net:443`. The Private Access Sensor uses this channel to register and fetch policies from the Microsoft Entra cloud service.
- **Service Principal Names (SPNs)** of the private apps to be protected. These will be added to the policy for Private Access Sensors installed on the DCs. The SPNs are case insensitive.
- If you use **NT LAN Manager (NTLM) v1/v2**, you might need to restrict NTLM and use only Kerberos authentication in the domain.
- Install the private network connector as explained in the section *Creating a private network connector group*. Refer to *steps 1-6*.

It is recommended to test this functionality with a small set of private apps with sensors installed on a few domain controllers first.

Once the prerequisites are met, proceed with the configuration.

Creating an application

Create a Quick Access or enterprise application to publish the domain controllers using their IP addresses or FQDN. This allows the GSA clients to obtain Kerberos tickets.

1. Navigate to **Global Secure Access | Applications | Quick Access**. Specify the **Port** as 88 and **Protocol** as TCP.
2. Click on **Service Principal Name** and specify the SPNs of the applications to be secured. These SPNs are delivered to the Private Access Sensors installed on the domain controllers.
3. Add users and groups synchronized from Active Directory to the Quick Access application.

An enterprise application can also be used instead of Quick Access.

Installing the Private Access Sensor

Microsoft Entra Private Access Sensor extends Microsoft Entra Private Access and Conditional Access controls to enforce MFA for on-premises users and resources. It must be installed on the

domain controllers. It is recommended to test the setup by installing the sensor on a few domain controllers.

1. Download the Private Access Sensor from `https://entra.microsoft.com`, **Global Secure Access** | **Connect** | **Connectors and sensors** | **Private access sensors**.
2. Install this sensor on the domain controller. You will be prompted to sign in to Microsoft Entra during installation.
3. Once installed, ensure that the sensor status shows **Active** in the Entra portal.

Two JSON files are created at the sensor installation path. These files are called `cloudpolicy` and `localpolicy`. The `cloudpolicy` file contains the SPNs configured above. This file should not be modified. Add the IP address of the connector noted earlier to the `localpolicy` file under `SourceIPAllowList`. This allows only Kerberos requests from the connector. Others are blocked.

This sensor is installed in **Audit** mode by default. To enforce Conditional Access policies for domain controllers, change the status of the sensor to **Enforce** mode in the Entra portal by navigating to **Global Secure Access** | **Connect** | **Connectors and sensors** | **Private access sensors**.

Creating Conditional Access policy

You can now configure a Conditional Access policy that requires strong authentication for users and groups added to the Quick Access application.

Inclusions and exclusions

If you have devices in your environment that don't have the GSA client installed, these devices will be blocked from accessing the applications whose SPNs are specified in the Quick Access application. To enable these devices to access the applications, configure exclusions for each SPN in the Microsoft Entra Admin center. This will allow the client devices to access the applications without having the GSA client installed. Exclusions can be added by client IP addresses, IP address ranges or on-premises **User Principal Names (UPNs)**.

Alternatively, if there are many users that need to access the on-premises applications without the GSA client, you can configure inclusions for each SPN. Only the included users will need to have the GSA client installed. The remaining users will be able to access without the client.

The following considerations must be kept in mind when configuring inclusions and exclusions:

- A SPN can either have UPNs in the inclusion list or the exclusion list, not both
- UPN inclusion and IP exclusion can be configured for the same SPN

- UPN exclusion and IP inclusion can be configured for the same SPN
- If a policy matches a UPN inclusion and an IP exclusion, access to SPN is allowed

Inclusion and exclusion lists can be used to fine tune the Private Access Sensor policy if you have devices that don't run the GSA client.

Break glass mode

In case of emergency, the Private Access Sensor supports a break glass mode that allows all network traffic. This can be enabled in the Microsoft Entra Admin center by navigating to **Global Secure Access | Connect | Connectors and sensors | Private access sensors** and selecting the required Private Access Sensor. Under **Settings**, select **Enable break glass mode**.

Application usage analytics

Application usage analytics in GSA provide critical insights into how users are engaging with both on-premises and cloud-based applications within your organization. By leveraging these analytics, administrators can monitor user access patterns, identify frequently accessed applications, and detect anomalies or potential security risks. The analytics dashboard typically presents data such as the number of unique users per application, session durations, peak usage times, and trends in application adoption over time.

These insights help IT teams make informed decisions about resource allocation, policy adjustments, and access controls. For example, applications that show unusually high or unexpected access patterns can be investigated for potential misuse or security concerns. Conversely, underutilized applications can be reviewed for relevance or decommissioning. Application usage analytics also support compliance initiatives by providing an auditable trail of who accessed what applications, when, and from where.

In the context of Global Secure Access, usage analytics are further enhanced by integrating with identity-centric controls. This ensures that visibility extends across hybrid environments, supporting Zero Trust principles. Ultimately, robust analytics empower organizations to optimize application portfolios, improve user productivity, and strengthen overall security posture.

The dashboard is available in the Microsoft Entra Admin center by navigating to **Global Secure Access | Applications | Insights and analytics**. The **Global Secure Access Log Reader** is the minimum role required to access this dashboard.

> **Note**
>
> At the time of this writing this feature is in Public Preview.

Logs and monitoring

Logs and monitoring form the operational backbone of GSA. They provide the visibility needed to understand how traffic flows through the network, how policies are being applied, and where risks or performance issues may be emerging. Because GSA sits at the intersection of identity, network access, and Zero Trust enforcement, its logging model brings together signals from multiple layers—identity, device posture, network edges, and application access.

GSA integrates with **Microsoft Sentinel** so all the logs and alerts can be streamed directly into it, where logs from GSA can be correlated with logs from other systems to improve threat detection and response.

GSA Dashboard

The Global Secure Access dashboard provides a consolidated, real-time view of how identity-aware network access is performing across the environment. It surfaces key metrics such as connector health, session volumes, policy outcomes, and traffic patterns, allowing teams to quickly spot anomalies or degradation. Visual summaries highlight trends in access requests, blocked sessions, device posture, and user experience signals. Because the dashboard unifies identity, network, and device telemetry, it becomes a central command surface for monitoring Zero Trust enforcement. It also links directly to deeper analytics and logs, helping administrators move from high-level insights to detailed investigation with minimal friction. The GSA Dashboard is accessible in the Microsoft Entra Admin center by navigating to **Global Secure Access | Dashboard**.

Traffic logs

Traffic logs in Global Secure Access provide detailed visibility into how users, devices, and applications interact across the identity-aware network fabric. They capture information such as source and destination, protocols used, session duration, data volume, and policy outcomes. This telemetry helps administrators understand access patterns, validate segmentation, and troubleshoot performance or connectivity issues. Traffic logs also reveal anomalies like unexpected destinations or unusual data transfers, supporting threat detection, and forensic investigations. Because they correlate identity, device posture, and network behavior, traffic logs become a critical component of Zero Trust monitoring, enabling continuous verification, and informed policy refinement.

Traffic logs are retained in the system for 30 days. To view these logs, administrators must have the **Global Secure Access Administrator** or the **Global Secure Access Log Reader** role.

To view the traffic logs, navigate to **Global Secure Access | Monitor | Traffic logs** in the Microsoft Entra Admin center.

Audit logs

Audit logs in Global Secure Access capture the administrative actions that shape how the service operates, providing a traceable record of configuration changes, policy updates, connector management, and role assignments. These logs help establish accountability by showing who performed an action, when it occurred, and what settings were modified. Because GSA spans identity, network access, and device posture, audit logs become essential for compliance and operational governance. They support investigations by linking administrative activity to downstream effects such as policy enforcement outcomes or traffic shifts. Consistent review of audit logs strengthens change control and ensures the access fabric remains secure and predictable.

To access the audit logs, you must have the **Reports Reader**, **Security Reader**, or **Security Administrator** role.

To view the audit logs, navigate to **Global Secure Access | Monitor | Audit logs** in the Microsoft Entra Admin center.

Remote network health logs

Remote network health logs provide continuous insight into the operational state of the office connected using remote networks. Remote offices depend on the **customer premises equipment (CPE)** to function correctly. To ensure everyone remains connected, the health of the IPSec tunnel and the Border Gateway Protocol route needs to be monitored. To view these logs, administrators must have the **Global Secure Access Administrator** or the **Security Administrator** role.

To view the remote network health logs, navigate to **Global Secure Access | Monitor | Remote network health logs** in the Microsoft Entra Admin center.

Deployment logs

Deployment logs in Global Secure Access provide a detailed record of how the service is provisioned, updated, and expanded across an environment. They capture events such as connector installation, registration, version updates, policy package deployment, and configuration propagation to remote networks. These logs help administrators verify that new components have been deployed correctly, identify failures during rollout, and ensure that changes have reached all required endpoints. Because GSA relies on distributed connectors and cloud-managed policies, deployment logs become essential for validating consistency, troubleshooting onboarding issues, and maintaining a predictable, well-governed access fabric.

To view these logs, administrators must have the **Global Secure Access Administrator** or the **Security Administrator** role.

To view the deployment logs, navigate to **Global Secure Access | Monitor | Deployment logs** in the Microsoft Entra Admin center.

Alerts

GSA alerts notify administrators of important security events or operational issues within the environment. These alerts are generated in real time when anomalies, policy violations, or infrastructure problems are detected, such as failed connector health checks, suspicious access attempts, or misconfigurations. GSA alerts help teams respond quickly to incidents by providing actionable information, including event details, severity, and impacted resources. Administrators can use these alerts to prioritize investigations, mitigate risks, and ensure compliance with organizational policies. Regular monitoring and prompt response to GSA alerts are essential for maintaining a secure and resilient access infrastructure.

Licensing

Microsoft Entra Private Access is available as a standalone license or as part of the Microsoft Entra Suite.

Summary

This chapter built on the knowledge of the previous chapter and explained the Private Access part of Global Secure Access. It went in depth into setting up Microsoft Entra Private Access. It further explained how Microsoft Entra Private Access can be used to configure Quick Access for a quick VPN replacement to provide per-app access to achieve granular security. You also learned how to configure application discovery and use the intelligent local access feature to bypass the GSA client when the client is directly connected to the corporate network. Lastly, it explained how to configure Private Access for domain controllers. The chapter ended with covering the application usage dashboard and logs available in Global Secure Access.

Exercises

1. What is the primary purpose of Microsoft Entra Private Access?
    a. Managing user identities across multiple SaaS applications.
    b. Providing secure, identity-based access to private network resources.
    c. Encrypting all outbound internet traffic from corporate devices.
    d. Monitoring cloud workload for anomalous behavior.
2. When configuring Microsoft Entra Private Access, which component is responsible for establishing the outbound connection from your network to the GSA service?
    a. Global Secure Access Client

   b. Microsoft Entra Application Proxy Connector
   c. Conditional Access policy engine
   d. Private Network Connector

3. Which prerequisite must be in place before onboarding Windows devices to Microsoft Entra Private Access?
   a. Devices must have a static public IP assigned.
   b. Devices must be connected through an on-premises VPN gateway.
   c. Devices must be joined to Microsoft Entra ID, hybrid joined, or Microsoft Entra ID registered.
   d. Devices must be enrolled in Microsoft Defender for Endpoint.

Answers

1. b
2. d
3. c

Additional resources

- Global Secure Access deployment guide: `https://learn.microsoft.com/en-us/entra/architecture/gsa-deployment-guide-intro?toc=/entra/global-secure-access/toc.json&bc=/entra/global-secure-access/breadcrumb/toc.json`
- Microsoft's SASE partner ecosystem: `https://learn.microsoft.com/en-us/entra/global-secure-access/partner-ecosystems-overview`

Get this book's PDF version and more

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.



UNLOCK NOW

Note: Keep your invoice handy. Purchases made directly from Packt don't require an invoice.

Part 5

Optimizing, Modernizing, and Growing with Microsoft Entra

Part 5 focuses on sustaining operational excellence, modernizing identity infrastructure, and advancing your professional journey with Microsoft Entra. It begins with Microsoft Entra health, threats, and trust, offering insights into monitoring, diagnostics, and proactive threat detection to maintain a resilient identity environment. The section then explores strategies for migrating to Microsoft Entra ID, guiding organizations through modernization with clarity and confidence. Finally, it highlights the growing career landscape around Microsoft Entra skills, outlining the roles, opportunities, and competencies that define the future of identity. Together, these chapters prepare readers to operate, evolve, and thrive in the Microsoft Entra ecosystem.

This part of the book includes the following chapters:

- *Chapter 16*, *Microsoft Entra Health, Threats, and Trust*
- *Chapter 17*, *Migrating to Microsoft Entra ID*
- *Chapter 18*, *Career Opportunities with Microsoft Entra Skills*

16

Microsoft Entra Health, Threats, and Trust

Microsoft Entra Health, Threats, and Trust sets the stage for understanding Entra as the modern identity control plane—one that must stay healthy, resilient, and continuously verified in a world where identity has become the primary attack surface. This chapter introduces how Entra's monitoring and health capabilities provide the operational visibility needed to maintain identity integrity at scale, ensuring that signals, anomalies, and service posture are understood before they become business-impacting issues. It also explores the evolving identity threat landscape, where credential attacks, token theft, and adversary-in-the-middle techniques increasingly target identity systems directly. Against this backdrop, Zero Trust becomes not just a philosophy but a practical enforcement model, with Entra acting as the engine for continuous evaluation of user, device, and workload trust. Finally, the chapter connects these elements to the rise of mesh and distributed identity architectures, where trust must be brokered across systems, clouds, and boundaries. Together, these themes frame Entra as both a defensive shield and an architectural foundation for secure, interconnected digital ecosystems.

In this chapter, we will cover:

- Microsoft Entra Monitoring and health
- Microsoft Entra threat landscape
- Microsoft Entra and Zero Trust
- Microsoft Entra and Mesh Architecture

Introduction

Monitoring and maintaining the health of Microsoft Entra ID is essential for ensuring the security, compliance, and operational stability of an organization's identity infrastructure. As organizations increasingly adopt cloud services and support remote work, Microsoft Entra becomes a crucial hub for managing identities and controlling access to resources. Effective monitoring provides real-time visibility into user activities, configuration changes, and potential security threats, enabling administrators to detect unusual patterns, respond to incidents quickly, and enforce compliance requirements. By leveraging Entra's built-in monitoring and health tools, IT teams can proactively identify and resolve issues before they impact users, ensure high availability, and support ongoing digital transformation efforts. Ultimately, robust monitoring safeguards sensitive resources, helps maintain business continuity, and fosters trust in the organization's identity management processes.

Microsoft Entra activity logs

Microsoft Entra activity logs provide a view of the identity-related activity in the tenant. This enables organizations to understand how users are using applications and services, detect risks that affect the health of the tenant, troubleshoot problems that can impact users and gain insights into the changes made to the tenant. Microsoft Entra provides activity logs that help organizations understand the user behavior in their environment. Entries in the activity logs are immutable and cannot be changed or deleted.

The following types of activity logs are available:

Audit logs

Microsoft Entra audit logs provide a comprehensive record of all changes and activities performed within the Microsoft Entra environment. These logs capture detailed information about actions such as user and group management, application assignments, directory role changes, policy updates, and other administrative operations. Each audit log entry includes crucial details like the timestamp of the event, the initiator (who performed the action), the target object (such as a user or application), the type of operation (For example, add, update, delete), and the status of the action (success or failure). This level of detail enables organizations to trace modifications, investigate security incidents, and ensure compliance with regulatory requirements.

Administrators can access the audit logs from the Microsoft Entra admin center by navigating to **Entra ID | Monitoring and health | Audit logs**. Following is an example of audit logs:

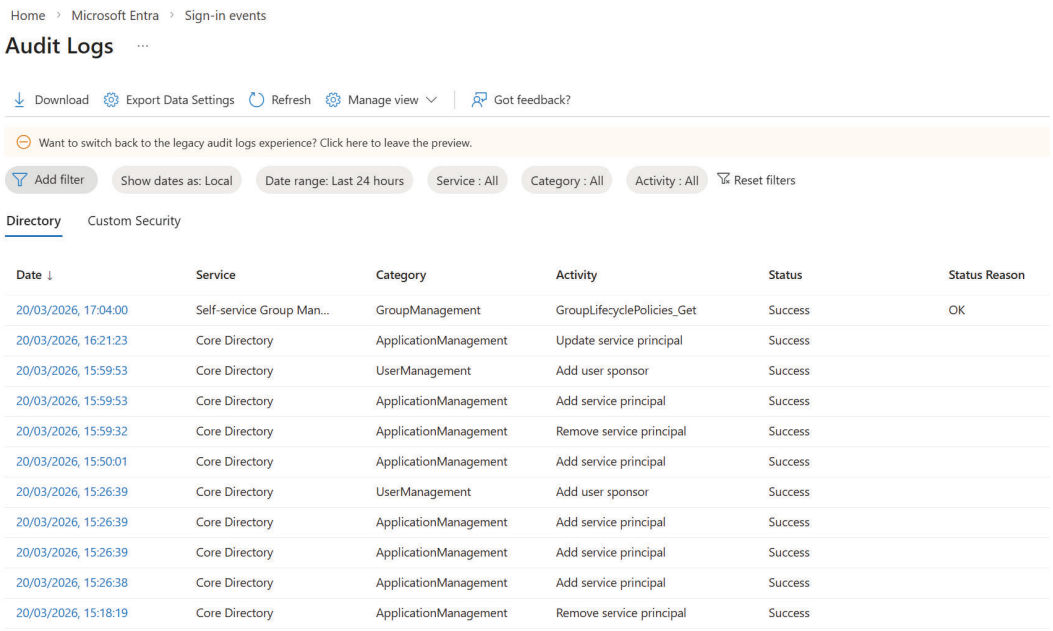


Figure 16.1: Microsoft Entra audit logs

For automation and advanced reporting, the logs are also accessible via the Microsoft Graph API, allowing organizations to incorporate log data into custom dashboards or monitoring workflows. Audit logs can also be downloaded as CSV or JSON by clicking the **Download** button.

Reports Reader is the minimum role required to access audit logs, and it is available with all licenses of Microsoft Entra ID.

Sign-in logs

Microsoft Entra sign-in logs provide a detailed record of user authentication attempts within an organization's environment. These logs are essential for monitoring access patterns, detecting suspicious sign-in activity, and supporting security investigations. There are four types of sign-in logs.

- **Interactive user sign-ins**: These are sign-ins that are performed by a user by providing an authentication factor like a password or MFA response to Entra ID. This log also includes sign-ins from IdPs that are federated with Microsoft Entra ID.
- **Non interactive user sign-ins**: These are sign-ins that are performed on behalf of a user. These could be delegated sign-ins performed by a client application. These don't

require the presentation of an authentication factor. Microsoft Entra ID refreshes the user's token without interrupting the session.

- **Service principal sign-in**: These are sign-ins from a non-user account. These are sign-ins performed by an application or service by providing an authentication factor such as a certificate or client secret.
- **Managed identity sign-ins**: These are sign-ins performed by managed identities for Azure resources. These identities have their credentials managed in Azure.

Administrators can access sign-in logs through the Microsoft Entra admin center by navigating to **Entra ID | Monitoring and health | Sign-in logs**. This centralized location allows for a comprehensive view of all sign-in events in the tenant. The following screenshot shows an example of the sign-in logs.

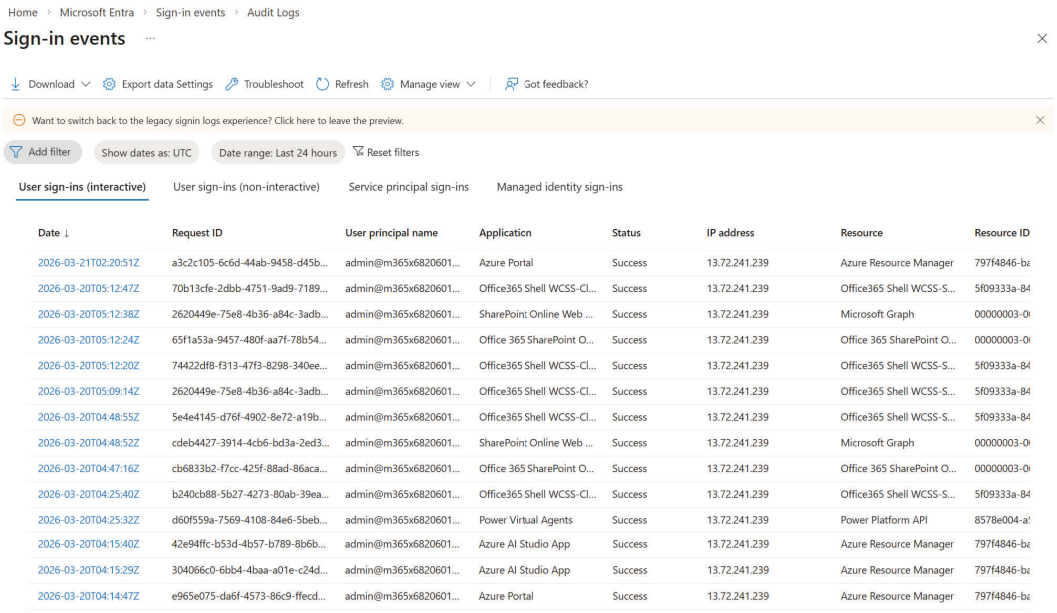


Figure 16.2: Microsoft Entra Sign-in logs

Each entry in the sign-in logs contains crucial information such as the timestamp of the sign-in attempt, the user's identity, application accessed, status of the attempt (success or failure), and the conditional access policies applied. Additional details captured include the IP address, device information, location of the user, client app used (for example, browser or mobile app), and any associated risk detections or sign-in errors. This level of detail enables organizations to trace authentication events, identify possible threats such as unauthorized access or brute-force attacks, and fulfill compliance or auditing requirements.

For advanced analysis, sign-in logs can be exported or integrated with SIEM tools, as well as accessed via Microsoft Graph API for custom reporting and automation. Sign-in logs can also be downloaded as CSV or JSON by clicking on the **Download** button.

Reports Reader is the minimum role required to access sign-in logs, and it is available with all licenses of Microsoft Entra ID.

Provisioning logs

Microsoft Entra can integrate with several non-Microsoft tools like ServiceNow and Workday to provision users into the tenant. Provisioning logs help in troubleshooting issues related to a provisioned user. The provisioning logs give details about the identity, the source system, and the status of provisioning. The following screenshot shows an example of provisioning logs:

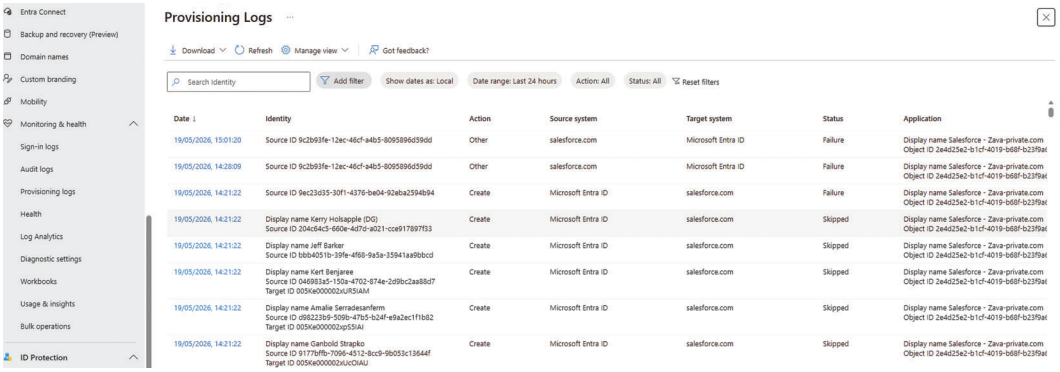


Figure 16.3: Microsoft Entra provisioning logs

Clicking on any item in the provisioning log provides more information about the item.

For advanced analysis, provisioning logs can be exported or integrated with SIEM tools, as well as accessed via Microsoft Graph API for custom reporting and automation. Provisioning logs can also be downloaded as CSV or JSON by clicking on the **Download** button.

Reports Reader is the minimum role required to access provisioning logs, and Microsoft Entra ID P1 is the minimum license required.

Diagnostic settings

For Microsoft Entra activity logs to be integrated with **Azure Monitor**, streamed to an event hub, or archived to a storage account, diagnostic settings need to be configured using the following steps:

1. Sign in to `https://entra.microsoft.com` as a **Security Administrator**.
2. Navigate to **Entra ID | Monitoring and health | Diagnostic settings**.

3. In the right pane click on **Add diagnostic setting**. Give the diagnostic setting a name and select the log categories that you would like to send.
4. Select the destination under **Destination details** and click **Save** as shown in the following screenshot:

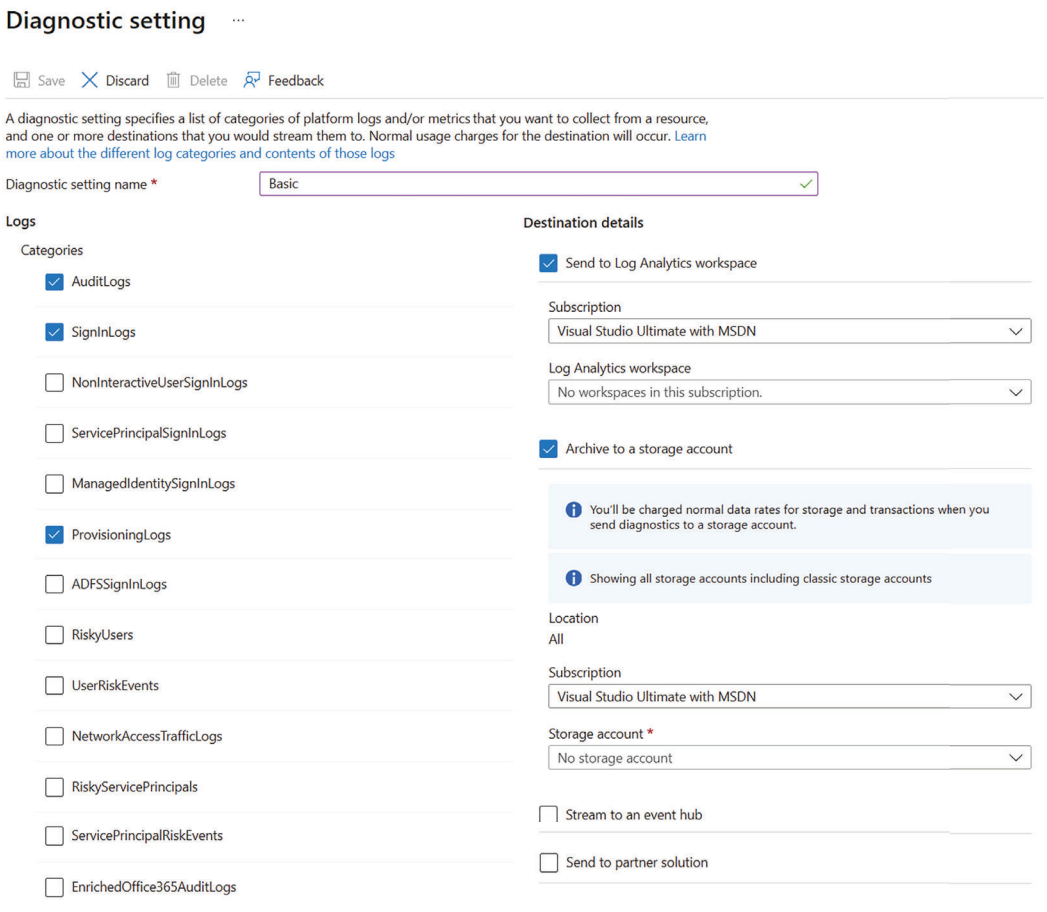


Figure 16.4: Diagnostic settings

Usage and insights reports

Microsoft Entra ID provides several reports that administrators can use to monitor application activity, authentication methods activity, and more. These reports are accessible in the

Microsoft Entra admin center by navigating to **Entra ID | Monitoring & health | Usage and insights**. The following reports are available:

- **Microsoft Entra application activity**: This report shows applications that have signed in to Microsoft Entra in the last 30 days. Administrators can see the number of successful and failed sign-ins for each application. The following is an example of this report:

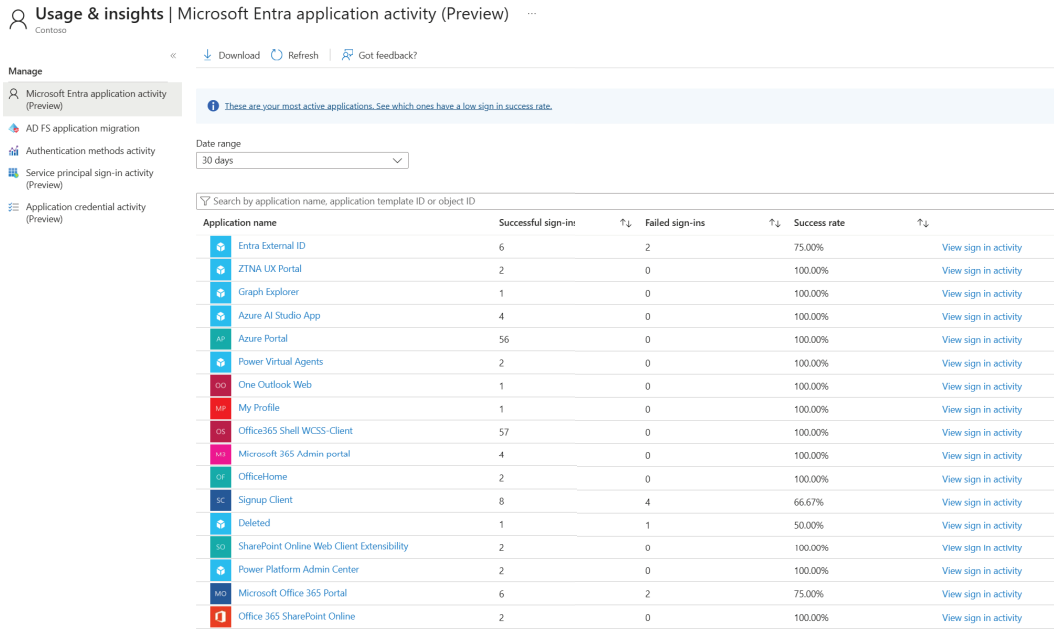


Figure 16.5: Application activity report

You can see more details about each application by clicking on **View sign in activity**.

- **AD FS application activity**: This report shows all **Active Directory Federation Services (AD FS)** applications that users have signed in to in the last 30 days. This helps organizations identify applications that have not yet been migrated to Microsoft Entra ID for authentication.
- **Authentication methods activity**: This report shows the different authentication methods used in the organization. The following is an example of this report:

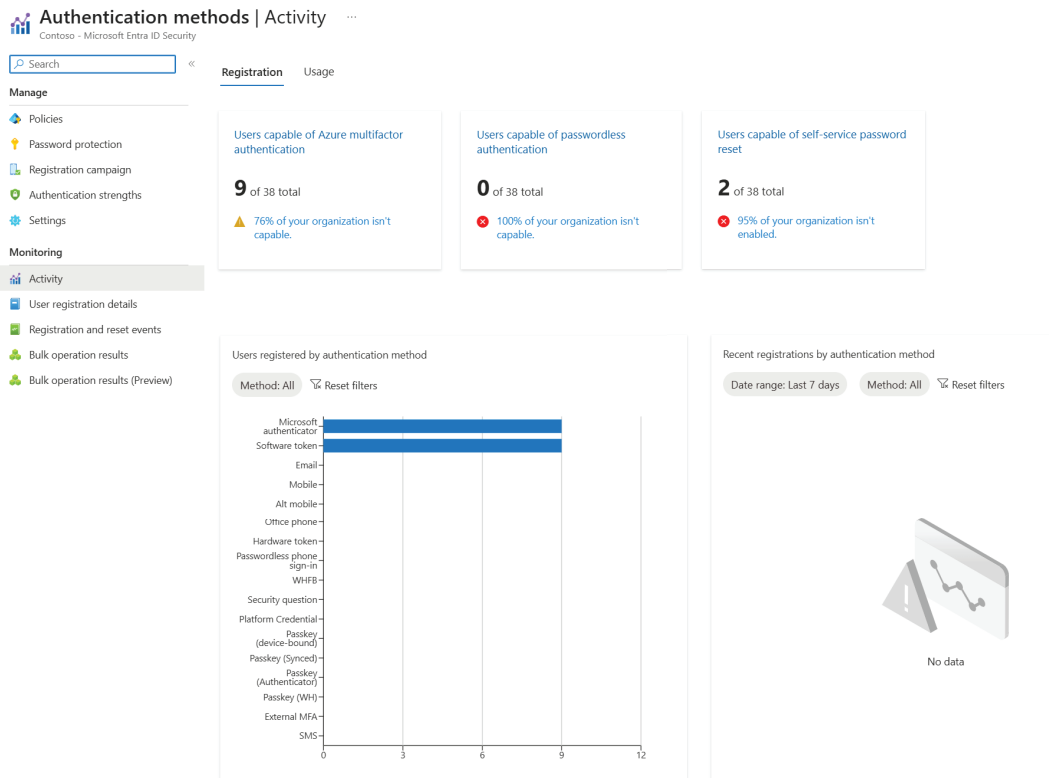


Figure 16.6: Authentication activity report

This report provides several useful insights into the authentication methods used in the organization and highlights gaps like the number of users not configured for passwordless authentication or self-service password reset. This can help organizations design campaigns for users to set up authentication methods like the Microsoft Authenticator app or passkeys.

- **Service principal sign-in activity**: This report shows information about the usage of service principals. It shows if the service principal was a client or resource application and when the service principal was last used.
- **Application credential activity**: This report provides the last activity date for application credentials like certificates or client secrets. It also shows the expiration date of application credentials.

These reports can also be viewed and managed using Microsoft Graph.

Microsoft Entra recommendations

Microsoft Entra recommendations provide actionable guidance to help organizations strengthen their identity security posture and optimize their configurations. These recommendations are generated by analyzing your current settings, usage patterns, and security signals within the Entra environment. Common suggestions may include enabling multi-factor authentication, reviewing risky user sign-ins, updating conditional access policies, or addressing legacy authentication protocols. By following these tailored recommendations, organizations can proactively reduce vulnerabilities, ensure compliance, and enhance operational efficiency. Regularly reviewing and implementing Entra recommendations supports continuous improvement, helping your organization adapt to evolving security threats and best practices in identity and access management.

Microsoft Entra recommendations include the **Identity Secure Score** recommendations. Identity Secure Score is a percentage indicator of the tenant's alignment with Microsoft's recommendation for security. Every day Microsoft Entra ID analyzes the configuration of the tenant by comparing the configuration with security best practices and recommendation data, and a new percentage is calculated. Following is a screenshot of Microsoft Entra recommendations. It includes the identity secure score. You can also see how the score changes over time.

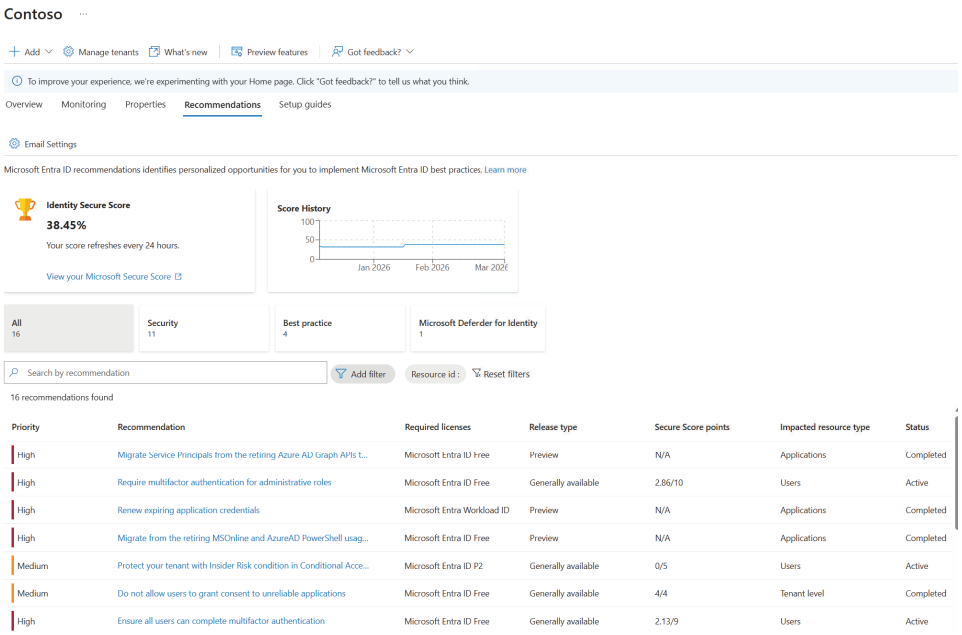


Figure 16.7: Microsoft Entra recommendations

The recommendation page shows the license required to implement the recommendation, its impact on the identity secure score and the impacted resource. Clicking on a recommendation provides a detailed description of the recommendation along with an action plan to implement it. The following screenshot shows a recommendation:

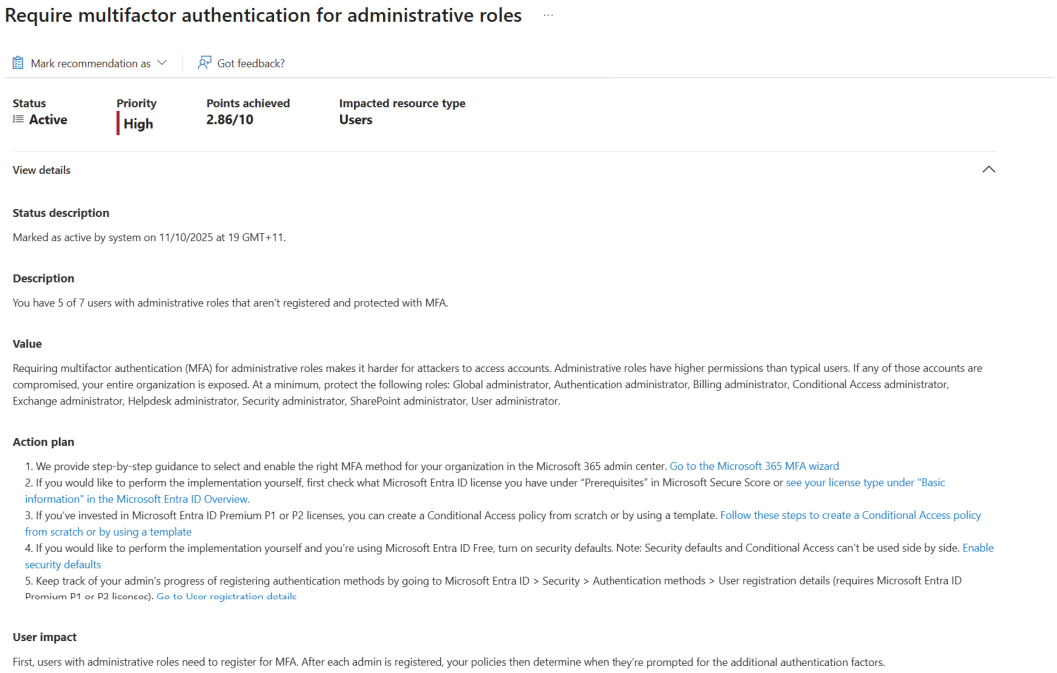


Figure 16.8: Recommendation details

Administrators with the **Reports Reader**, **Security Reader**, and **Global Reader** roles can read a recommendation. To modify and update a recommendation, administrators must have the **Authentication Policy Administrator**, **Exchange Administrator** or **Security Administrator** role.

The **Status** of a recommendation can have the following values:

- **Active**: The recommendation needs attention.
- **Completed**: The recommended actions have been addressed. Microsoft Entra automatically marks a recommendation as Completed once the recommendation has been implemented on all affected resources. A recommendation cannot be manually changed to Completed.

- **Dismissed**: Administrators can mark a recommendation as Dismissed, if they feel it is irrelevant for their environment. A reason must be provided.
- **Postponed**: Administrators can mark a recommendation as Postponed if they want to address it later. A date must be provided. The recommendation becomes active on that date. A recommendation can be postponed for up to a year.

The **Priority** of a recommendation can be Low, Medium or High depending on several factors. Priority is automatically assigned by Microsoft and cannot be manually set.

The Points achieved section is automatically updated by Microsoft depending on the implementation. If a recommendation is completely implemented, full points are given. If it is partially implemented (For example, on 5 out of 7 resources), partial points are given.

Email notifications can be sent if a new recommendation is generated by clicking on **Email Settings** (refer to *Figure 16.7*). Depending on the nature of the recommendation, specific admin roles are notified. For example, to enable a Conditional Access policy, the Conditional Access Administrator will be notified. To update email notification settings for Microsoft Entra recommendations, the **Security Administrator** role is required.

Microsoft Entra workbooks

Microsoft Entra workbooks are interactive dashboards that help administrators visualize, analyze, and monitor identity and access-related data within their organization. These workbooks provide a customizable way to track key metrics like sign-in activity, authentication patterns, policy compliance, and security recommendations. By leveraging built-in templates or creating custom views, admins can quickly identify trends, detect anomalies, and make informed decisions to enhance security posture. Workbooks integrate with other Microsoft Entra features, allowing for deep-dive analysis across various identity resources. This powerful reporting tool supports proactive identity management and helps organizations maintain compliance and operational efficiency.

Microsoft Entra workbooks are built on **Azure Monitor Workbooks**. Using these workbooks, administrators can query data from multiple Azure sources, visualize data for reporting and combine several data sources into a single experience. Microsoft offers workbook templates that organizations can customize and use. The following workbook templates are available.

- **Authentication prompt analysis**: This workbook helps analyze and visualize authentication prompts so that administrators can detect unexpected authentication prompts.
- **Conditional Access gap analyzer**: This workbook helps detect gaps in Conditional Access policies to ensure that he resources are properly protected.

- **Cross-tenant access activity**: This workbook helps you understand how users in your tenant are collaborating and interacting with users from other tenants and which external users are accessing resources in your tenant.
- **Multifactor authentication gaps**: This helps identify users and applications that are not protected by MFA requirements.
- **Provisioning insights**: This workbook helps you analyze and visualize the provisioning logs.
- **Identity Protection Risk Analysis**: This workbook helps understand risk trends by visualizing data from Microsoft Entra ID Protection.
- **Sensitive Operations Report**: This workbook helps identify suspicious application and service principal activity.
- **Sign-ins using legacy authentication**: This workbook shows whether legacy authentication is still being used in the organization.

Additional workbooks can be created by organizations as per their requirements.

To use Microsoft Entra workbooks the following prerequisites must be met.

- Microsoft Entra ID P1 license
- A Log Analytics workspace created in Azure

Administrators require roles in both Azure Monitor and Microsoft Entra to work with workbooks.

To view data in **Azure Monitor**, administrators must have the **Monitoring Reader** and **Log Analytics Reader** roles. To modify settings, the **Monitoring Contributor** and **Log Analytics Contributor** roles are required.

To read data in a **Microsoft Entra** workbook, query data from Log Analytics and read logs in Microsoft Entra administrators require the **Reports Reader**, **Security Reader**, or **Global Reader** role in Microsoft Entra. To update a workbook with additional diagnostic settings, the **Security Administrator** role is required.

Workbooks are accessible in the Microsoft Entra admin center by navigating to **Entra ID | Monitoring & health | Workbooks**.

Microsoft Entra threat landscape

Microsoft Entra serves as a cornerstone for identity and access management in modern organizations. As enterprises increasingly adopt cloud services and remote access paradigms, the importance of securing identity platforms like Microsoft Entra cannot be overstated. The evolving cybersecurity landscape introduces a wide variety of threats targeting IAM systems,

making it essential for IT professionals and administrators to understand not only the nature of these threats but also the robust protection mechanisms available within Entra. This section provides a comprehensive examination of the threats facing Microsoft Entra, offers strategies for mitigation, and details the built-in security features designed to protect against both internal and external risks.

Types of threats facing Microsoft Entra

The threat landscape for identity and access management platforms is dynamic and complex. Microsoft Entra, as a central authentication authority, is a high-value target for attackers seeking to compromise organizational security. The most common threats include:

- **Credential theft:** Attackers employ tactics such as keylogging, credential stuffing, and harvesting credentials via malware or insecure endpoints to gain unauthorized access.
- **Phishing attacks:** Social engineering campaigns trick users into revealing login credentials or approving malicious authentication requests, often bypassing basic security controls.
- **Brute force attacks:** Automated attempts to guess passwords or authentication tokens through repeated login attempts, exploiting weak credentials.
- **Token theft**: Cybercriminals may steal authentication tokens from compromised devices or sessions, enabling them to bypass password requirements and impersonate legitimate users.
- **Social engineering**: Attackers often use deceptive tactics such as impersonation, pretexting, or manipulation to trick users into disclosing sensitive information or performing actions that compromise their identities.
- **Privilege escalation:** Exploiting misconfigured permissions to elevate access rights, allowing attackers to gain administrative privileges within Entra.
- **Insider threats:** Malicious or negligent actions by users with legitimate access, including data exfiltration or policy circumvention.
- **External attacks:** Targeted campaigns by advanced persistent threats (APTs), organized cybercriminals, or state-sponsored actors aiming to compromise Entra for broader network access.
- **Misconfiguration Risks:** Poorly implemented settings, such as overly permissive access or unmonitored legacy authentication, can expose Entra to exploitation.

Protecting Microsoft Entra from threats

Securing Microsoft Entra requires a multi-layered approach that combines technical controls, administrative best practices, and continuous monitoring. Key protection strategies include:

- **Multi-Factor authentication:** Enforcing MFA significantly reduces the risk of unauthorized access by requiring additional verification beyond passwords. Administrators should mandate MFA for all users, particularly those with high-privilege roles.
- **Conditional Access policies:** Leveraging Entra's conditional access capabilities allows organizations to define granular access controls based on user risk, device compliance, location, and other contextual signals. This approach ensures that only trusted entities can access sensitive resources.
- **Principle of least privilege:** Assigning users the minimum level of access necessary to perform their roles limits the potential impact of compromised accounts or insider misuse.
- **Regular review of roles and permissions:** Periodic audits of Entra roles and permissions help identify and remediate excessive or outdated access rights.
- **Disabling legacy authentication:** As highlighted in the context, monitoring and eliminating legacy authentication methods reduces exposure to credential-based attacks that bypass modern security controls.
- **Security awareness training:** Educating users about phishing, social engineering, and secure authentication practices strengthens the human layer of defense.

Built-in security features in Microsoft Entra

Microsoft Entra incorporates an array of built-in security features designed to protect identities and ensure secure access management. These features offer both proactive and reactive defense mechanisms:

- **Role-Based Access Control (RBAC):** Entra's RBAC model enables precise assignment of permissions through predefined and custom roles. Correct role assignment ensures that only authorized personnel can view or modify sensitive configurations.
- **Monitoring and Health workbooks:** Entra offers integrated workbooks that provide visualizations and analytics on sign-in activity, authentication methods, and potential anomalies, enabling administrators to detect suspicious patterns and legacy authentication usage.

- **Security logs and auditing:** Comprehensive logging of authentication events, permission changes, and administrative actions enable detailed auditing and forensic analysis.
- **Threat detection and response tools:** Entra leverages built-in detection mechanisms to identify brute force attempts, impossible travel, and other indicators of compromise, triggering alerts or automated responses as appropriate.

Advanced protection mechanisms

For organizations seeking enhanced security and operational insight, Microsoft Entra integrates seamlessly with advanced monitoring and analytics tools:

- **Azure Monitor and Log Analytics integration:** By connecting Entra to Azure Monitor and Log Analytics workspaces, administrators gain access to real-time data aggregation, customizable queries, and advanced alerting. This facilitates rapid detection of anomalies and supports proactive threat hunting.
- **Automated incident response:** Entra integrates with Microsoft Sentinel by exporting logs thereby supporting automation through playbooks that can respond to detected threats by revoking sessions, resetting credentials, or notifying incident response teams.
- **Threat intelligence integration:** Entra's security ecosystem can ingest threat intelligence feeds, correlating signals across Microsoft Defender and third-party sources to improve detection fidelity and response accuracy.

Example scenarios

To illustrate the practical application of Entra's security features, consider the following scenarios:

- **Phishing attack mitigation:** An attacker sends phishing emails to employees, attempting to harvest credentials. Entra's conditional access and enforced MFA prevent unauthorized access even if credentials are compromised. Security logs and workbooks quickly surface anomalous sign-ins, allowing rapid investigation.
- **Insider threat containment:** A user with elevated privileges attempts to export sensitive data. RBAC and least privilege principles ensure the user's access is limited, while audit logs capture the event for review and potential escalation.
- **Legacy authentication exploitation:** Attackers use outdated protocols to bypass modern security controls. Monitoring workbooks highlight legacy authentication attempts, prompting administrators to disable unsupported protocols and remediate affected accounts.

Continuous monitoring and improvement

Security is not a one-time exercise but a continuous process. Microsoft Entra's workbooks, analytics, and reporting capabilities empower organizations to maintain a robust security posture. Administrators should regularly review workbook insights, audit logs, and access patterns to identify trends, baseline normal behavior, and detect deviations that could signal emerging threats. Periodic assessments and updates to conditional access policies, user roles, and authentication requirements help adapt to the evolving threat landscape.

Responding to security incidents

Timely and effective incident response is critical for minimizing the impact of security breaches. Microsoft Entra supports administrators through the following steps:

- **Detection:** Continuous monitoring, security workbooks, and automated alerts facilitate early identification of suspicious activity.
- **Investigation:** Detailed audit logs and analytics enable root cause analysis, helping teams understand the scope and method of an attack.
- **Remediation:** Administrators can take immediate actions such as revoking sessions, resetting compromised credentials, and modifying conditional access policies to contain threats.
- **Post-Incident review:** Lessons learned from incidents should inform future security controls, policy adjustments, and user education initiatives.

Microsoft Entra is a critical asset in any organization's security architecture, and its protection requires diligence, expertise, and the strategic use of built-in features and integrations. By understanding the threat landscape, implementing layered security controls, and leveraging Entra's monitoring and response capabilities, IT professionals can safeguard their environments against current and emerging threats. As identity-based attacks continue to evolve, ongoing vigilance, regular policy updates, and proactive monitoring will remain essential for maintaining a secure and resilient Microsoft Entra deployment.

Recoverability

Today, identity is the backbone of modern security. When identity systems fail, user access breaks and productivity stops. Microsoft invests deeply in building resilient systems, and Microsoft Entra is designed to meet a 99.99% availability SLA. However, unintended changes or misconfigurations inside the tenant can also cause user impact. The key is to be able to recover from such incidents to minimize the impact to end users. Recoverability is the process that enables you to return your tenant to the state prior to the unintended change. Unintended

changes could be accidental deletion or misconfiguration of users, groups, policies or applications.

Recoverability is a shared responsibility between Microsoft and your organization. The following table explains the responsibility of Microsoft and the customer:

	Customer	**Microsoft**
Preparation	Business continuity and disaster planning	Identity and access management functionality
	Documentation of known good states	Tools for documentation
	Monitoring and data retention	Log availability and consistency
	Operational security	Platform security
Recovery	Restoring soft-deleted resources	Availability of soft-deleted resources
	Restoring prior configurations	Availability of APIs

Table 16.1: Recoverability responsibility

Microsoft Entra offers a built-in backup and recovery solution that helps organizations recover directory objects after accidental deletion or security compromises.

Soft deletion

Soft deletion is a concept in Microsoft Entra to enable quick recovery from accidental deletions or misconfigurations. Users, Microsoft 365 groups, cloud security groups, applications, and Conditional Access policies can be soft deleted.

The following table summarizes the items that can be soft deleted:

Object type	**Properties maintained**	**Recovered from**
Users	All properties maintained	Entra portal by navigating to **Entra ID** | **Users** | **Deleted users** Microsoft Graph API

Object type	Properties maintained	Recovered from
Groups	All properties maintained	Entra portal by navigating to **Entra ID** | **Groups** | **Deleted groups** Microsoft Graph API
Applications	All properties maintained	Entra portal by navigating to **Entra ID** | **App registrations** | **Deleted applications** Microsoft Graph API
Admin units	All properties maintained	Microsoft Graph API
Conditional Access policies	All properties maintained	Entra portal by navigating to **Entra ID** | **Conditional Access policies** | **Deleted policies**
Named locations	All properties maintained	Entra portal by navigating to **Entra ID** | **Conditional Access** | **Named locations** | **Deleted Named Locations**

Table 16.2: Soft deletion recovery

When deleted, these items must be restored within 30 days after which they are permanently deleted and cannot be recovered.

It is recommended that organizations regularly document the state of their tenant. The following tools are available to document the state:

- Microsoft Graph APIs help export the current state of many Microsoft Entra configurations.
- Microsoft Entra Exporter is a GitHub tool that can be used to export Microsoft Entra configuration settings.
- Microsoft 365 Desired State Configuration is a PowerShell module and can be used to export configurations for reference and to revert to the prior state of many settings.
- Conditional Access APIs can be used to manage Conditional Access policies as code.

In the absence of tools to export configuration settings, it is recommended to take screenshots of the settings to aid manual recovery.

Microsoft Entra Backup and Recovery

Microsoft Entra Backup and Recovery performs a backup of supported objects every day and retains the backup for up to five days. These backups are created automatically and are available to administrators to restore the objects to a previously known good state. These backups cannot be turned off, deleted or modified. They reside in the same geo location as the Microsoft Entra tenant. Supported objects are users, groups, applications, service principals, Conditional Access policies, Named location policies, Authentication method policy, Authorization policy, and Organization. Agent IDs are also supported because they consist of user and service principal objects.

> **Note**
>
> At the time of this writing, this feature was in Public Preview.

Prerequisites

Microsoft Entra ID P1 licenses are required to use this feature. To adhere to the principles of Zero Trust, administrators working with backups can be assigned one of the following roles depending on their tasks.

- **Microsoft Entra Backup Reader**: Can view backups and compare object changes between the backup and current state. They can also view recovery history.
- **Microsoft Entra Backup Administrator**: In addition to the permissions of the Microsoft Entra Backup Reader role, they can also initiate difference reports and trigger recovery.

Getting started

Backup and recovery can be accessed in the Microsoft Entra admin center by navigating to **Microsoft Entra | Backup and recovery**. To view the available backups, click on **Backups** in the right pane. The following screenshot shows the available backups in the tenant:

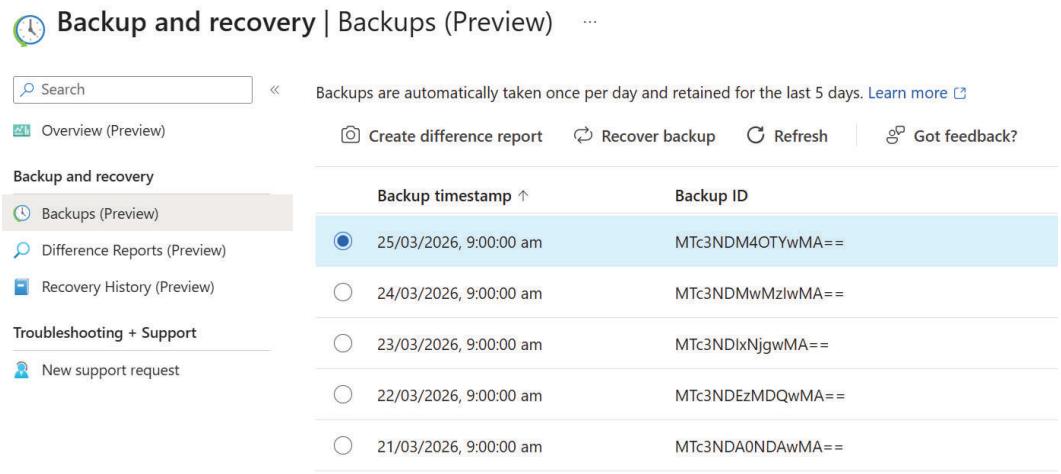


Figure 16.9: Microsoft Entra backups

Notice that from this screen you can recover a backup and create a difference report.

Difference report

A **difference report** is a comparison of the current state of objects in the tenant to the state of objects in the backup. Only changed objects appear in the report. It shows objects that were created, modified, soft-deleted or restored after the selected backup was taken. It gives details about object attributes that changed since the backup was taken and changes to object relationships to other objects like group membership changes. Difference reports are retained for five days after completion.

To create a difference report, select the backup and click on **Create difference report**. Select the required option and click **Create difference report**. Refer *Figure 16.10*.

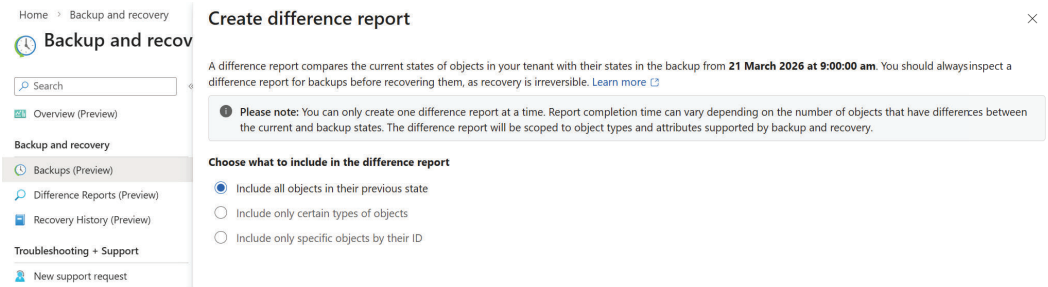


Figure 16.10: Create difference report

A difference report moves through the following statuses as it is created:

- **Loading data**: Data from the selected backup is being loaded for comparison.
- **In progress**: The difference between the objects in the loaded backup and the current state is being calculated.
- **Completed**: The report is ready for review.
- **Failed**: The report could not be generated due to an error.
- **Canceled**: The report generation was canceled by the administrator.

Tip

It is not possible to restore another backup or create a new difference report while a difference report is being processed.

To review a difference report go to **Entra ID | Backup and recovery | Difference Reports**.

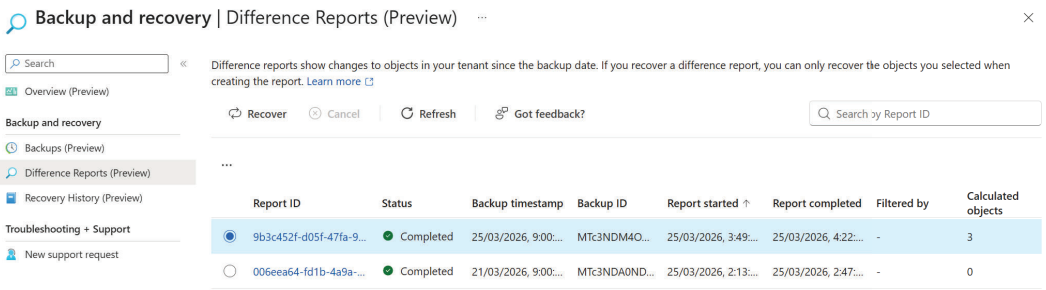


Figure 16.11: Completed difference report

Select a completed report to see the details. The report includes objects that changed and the recovery actions that apply during recovery.

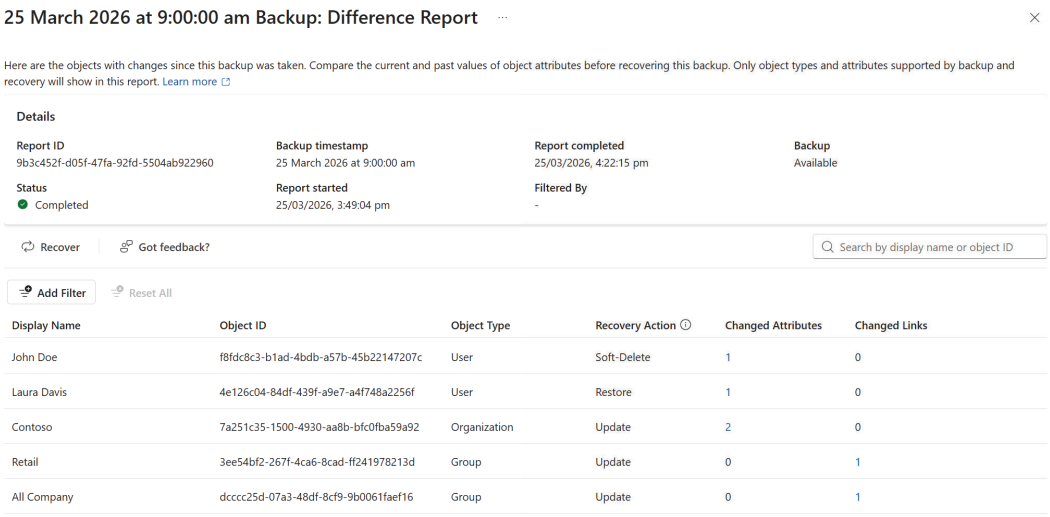


Figure 16.12: Difference report details

You can click on the numbers under **Changed Attributes** and **Changed Links** to view more details. The following screenshot shows changed details of the item *Retail*:

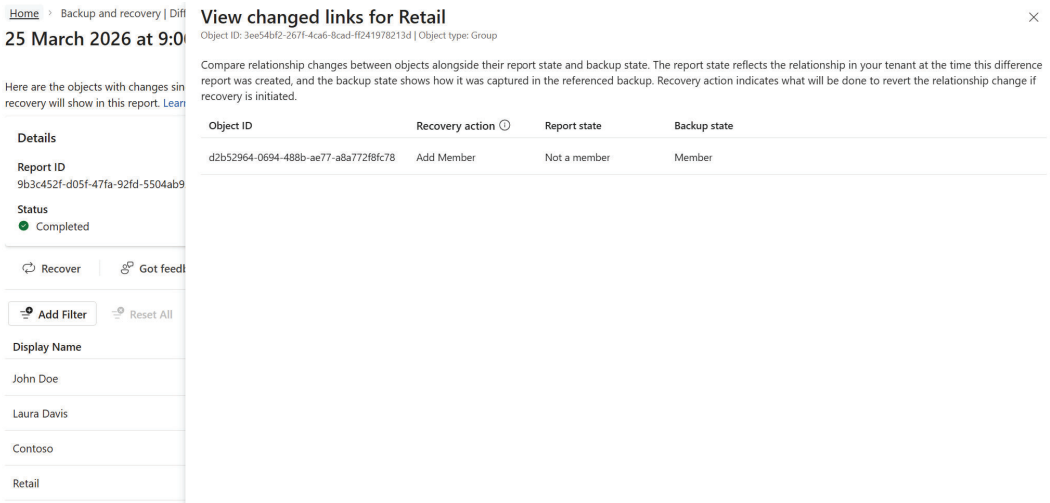


Figure 16.13: Recovery action details

Recovery actions can be one of the following:

- **Update**: When the backup is restored, changed attributes or links will be applied to the object in the directory. In the above example, a user was removed from the group *Retail*

after the last backup. When this backup is restored, the user will be added back to the group.

- **Restore**: The object was soft-deleted after the backup was taken and will be restored to the directory when the backup is restored.
- **Soft delete**: A new object was created after the backup was taken and will be soft-deleted when the backup is restored.

Recovery

Recovery can be performed directly from backups or from difference reports.

> **Tip**
>
> It is possible to recover directly from backups without creating a difference report. However, it is highly recommended to create a difference report to ensure that the correct backup is being restored.

Recover from difference report

To recover from a difference report, select the difference report and click on **Recover**. Refer to *Figure 16.12*.

It is also possible to recover only a single object by opening the object's changed attributes and clicking **Recover this object**.

Recover from backup

To recover directly from a backup, select the required backup and click **Recover backup**. Refer *Figure 16.14*. If a difference report is created for the backup, you will be prompted to view the difference report before recovery. If a difference report has not been created, you will be prompted to create a difference report. It is possible to recover a backup without creating or viewing the difference report. In the pop-up box click on **Recover backup**.

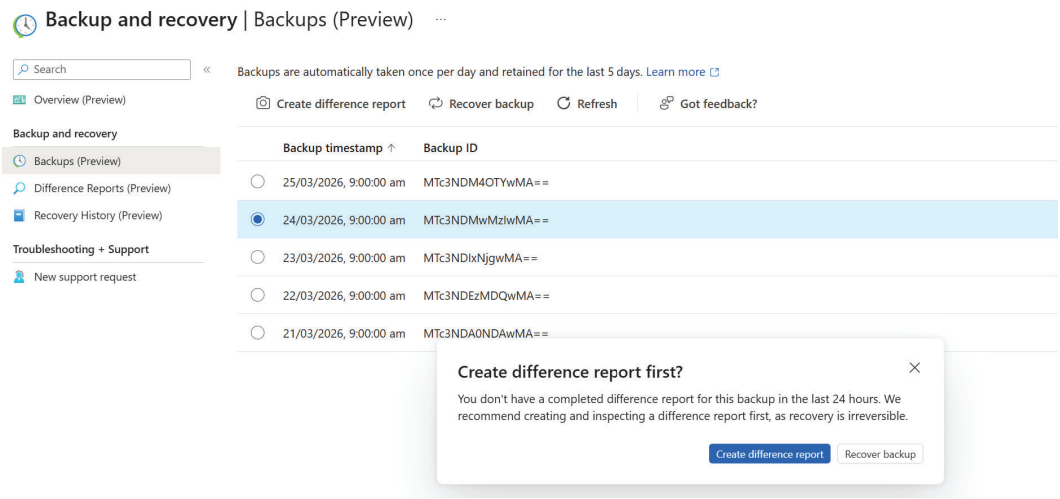


Figure 16.14: Recover from backup

Make the appropriate selection and click **Recover**.

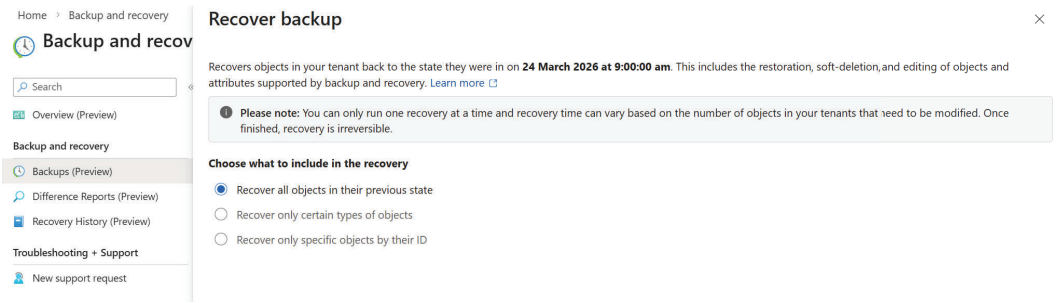


Figure 16.15: Recover objects

Once the recovery job starts it shows up on the **Recovery History** page. A recovery job goes through the following stages.

- **Loading data**: Data from the selected backup is being loaded for recovery.
- **In progress**: Data is being recovered from the loaded backup.
- **Completed**: The recovery has been completed successfully.
- **Completed with warnings**: The recovery was completed but some changes could not be applied. Failed changes can be reviewed for reasons.
- **Failed**: The recovery job failed due to an error. Some changes may have been applied.
- **Canceled**: The recovery job was canceled by the user.

Microsoft Entra Backup and Recovery leverages soft deletion. It continuously monitors and records changes to supported directory objects. If an object is soft-deleted, the backup restores that object when recovery is initiated. During a recovery operation, Microsoft Entra uses backups to determine the current object state and restores soft-deleted objects instead of recreating them. If a new object was created after the backup was taken, it is soft-deleted if the backup is restored. Objects are never hard-deleted as a part of the recovery process.

Together, Microsoft Entra Backup and Recovery and soft deletion enable organizations to quickly and confidently recover from unintended or accidental changes.

Microsoft Entra and Zero Trust

As organizations face an increasingly complex threat landscape and expanding digital environments, the Zero Trust security model has emerged as a leading framework for protecting sensitive resources and maintaining operational resilience. Microsoft Entra, as a comprehensive identity and access management solution, is purpose-built to help organizations realize the core tenets of Zero Trust. Through its robust capabilities—ranging from identity-centric controls to advanced analytics and seamless integrations—Entra empowers IT professionals, administrators, and security architects to implement Zero Trust principles at scale. This section provides a detailed examination of how Microsoft Entra aligns with and operationalizes Zero Trust, mapping foundational concepts to specific Entra features and illustrating their practical application in enterprise environments.

Zero Trust is predicated on the philosophy of "never trust, always verify." Rather than assuming implicit trust based on network location or prior authentication, Zero Trust demands continuous evaluation of user and device identities, contextual risk, and explicit policy enforcement for every access request. The foundational principles of Zero Trust include:

- **Verify Explicitly:** Authenticate and authorize every access attempt using all available data points, including user identity, device health, location, and behavior.
- **Use Least Privilege Access:** Limit user and application permissions to only what is necessary, reducing the attack surface and mitigating potential damage from a compromise.
- **Assume Breach:** Design security controls and monitoring under the assumption that attackers may already be present, enabling rapid detection, response, and containment of threats.

Let's explore how Microsoft Entra helps achieve Zero Trust.

Identity as the new security perimeter

In the modern digital enterprise, identity supplants the traditional network perimeter as the primary control point for access management. Microsoft Entra serves as the authoritative source for user, device, and workload identities, enabling organizations to enforce Zero Trust by validating every interaction based on identity context. By centralizing identity management, Entra ensures that only verified entities—regardless of network location—can access protected resources, thereby reducing reliance on legacy perimeter-based security and supporting hybrid and remote work scenarios.

Conditional Access in Microsoft Entra

Conditional Access is the cornerstone of Zero Trust implementation in Microsoft Entra. These policies enable organizations to define granular access requirements based on a rich set of signals, such as user risk, device compliance, location, application sensitivity, and real-time threat intelligence. For example, administrators can require multi-factor authentication when users access sensitive applications from unfamiliar locations or block access entirely from high-risk countries. Conditional Access policies are dynamic and adaptive, ensuring that security requirements align with the risk profile of each request. This contextual enforcement not only strengthens defenses but also enhances user experience by applying controls only when necessary.

Multi-Factor Authentication

Multi-factor authentication is a critical Zero Trust capability within Microsoft Entra, significantly reducing the risk of credential-based attacks. Entra supports a variety of MFA methods—including push notifications, biometrics, hardware, and software tokens—allowing organizations to tailor authentication mechanisms to their risk tolerance and user needs. By requiring users to provide multiple forms of verification, Entra ensures that even if one authentication factor is compromised, unauthorized access is prevented. MFA can be enforced universally or triggered by Conditional Access policies in response to detected anomalies or elevated risk scenarios.

Least privilege and role-based access control in Microsoft Entra

The principle of least privilege is operationalized in Microsoft Entra through robust role-based access control. Administrators can assign built-in or custom roles to users, groups, and service principals, ensuring that permissions are precisely scoped to the tasks required. **Just-in-time (JIT)** access and **Privileged Identity Management (PIM)** further refine this model by enabling temporary elevation of privileges for critical tasks, with full audit trails and approval workflows. By minimizing standing privileges and tightly controlling administrative access,

Entra substantially reduces the risk of lateral movement and privilege escalation in the event of compromise.

Continuous monitoring and risk-based access

Continuous monitoring is essential for maintaining a Zero Trust posture. Microsoft Entra integrates real-time risk assessment into its access control decisions, leveraging signals such as atypical sign-in behavior, impossible travel, suspicious device patterns, and threat intelligence feeds. Risk-based Conditional Access policies can automatically prompt additional authentication, restrict access, or trigger security workflows in response to detected anomalies. This continuous evaluation ensures that access decisions are always informed by the latest security context, enabling rapid containment of threats without disrupting legitimate business operations.

Device compliance and health integration

Device compliance is a key pillar of Zero Trust, recognizing that secure access requires both verified identities and trusted endpoints. Microsoft Entra integrates with Microsoft Intune and other mobile device management (MDM) solutions to assess device health, compliance status, and security posture before granting access to corporate resources. Conditional Access policies can enforce requirements such as up-to-date antivirus, encryption, or approved operating system versions, ensuring that only trusted and compliant devices can connect. This integration protects against compromised or unmanaged devices being used as entry points for attackers.

Real-time analytics and threat intelligence in Microsoft Entra

Microsoft Entra leverages the Microsoft security ecosystem to provide advanced analytics and threat intelligence for proactive risk management. Features such as Identity Protection analyze billions of signals daily to detect compromised accounts, risky sign-ins, and emerging attack patterns. Administrators receive actionable insights through dashboards, alerts, and reports, enabling rapid investigation and remediation of security incidents. Integration with Microsoft Sentinel and Azure Monitor further enhances visibility, allowing organizations to correlate identity events with broader security telemetry for comprehensive threat detection and response.

Automated threat detection and response

Automation is fundamental to Zero Trust, enabling organizations to respond to threats at machine speed. Microsoft Entra supports automated workflows for responding to identity-based risks, such as disabling compromised accounts, enforcing password resets, or escalating incidents to security operations teams. Integration with security orchestration, automation, and response (SOAR) platforms allows for end-to-end automation of detection, investigation,

and remediation processes. By reducing manual intervention and accelerating incident response, Entra helps organizations contain threats quickly and minimize potential damage.

Integration with Microsoft security solutions

Microsoft Entra is deeply integrated with the broader Microsoft security portfolio, including Microsoft Defender, Microsoft Sentinel, Microsoft Purview, and Intune. This interoperability enables unified policy enforcement, centralized monitoring, and coordinated incident response across identities, devices, applications, and data. For example, a risky sign-in detected by Entra can trigger automated device quarantine in Intune or initiate investigation in Sentinel. Such integrations amplify the effectiveness of Zero Trust strategies by eliminating silos and providing end-to-end visibility across the digital estate.

Practical scenarios: Microsoft Entra enforcing Zero Trust

Here are a few real-world scenarios to help understand this concept better.

- **Remote Workforce Access:** A user attempts to access sensitive financial data from an unmanaged device while traveling. Entra evaluates the risk based on device compliance, geolocation, and sign-in behavior. Conditional Access policies require MFA and block access unless the device meets compliance standards, ensuring that only trusted users and endpoints gain entry.
- **Privileged Role Activation:** An administrator requests temporary elevation to a Global Administrator role. Entra PIM enforces approval workflows and limits the duration of elevated access, while logging all activities for audit purposes. If suspicious activity is detected during the session, automated remediation actions are triggered.
- **Suspicious Sign-In Detection:** Entra's Identity Protection flags a user's sign-in as high-risk due to impossible travel and unusual device fingerprinting. Access is immediately restricted, and the user is prompted to reset their credentials, preventing potential account takeover.
- **Third-Party Application Integration:** A partner organization requests access to a shared app. Entra enforces B2B collaboration policies, requiring external users to authenticate using their own enterprise credentials and comply with organization-defined security standards.

These are just a few ways in which Microsoft Entra helps organizations achieve a Zero Trust posture.

Best practices for achieving Zero Trust with Microsoft Entra

Following are some best practices for achieving Zero Trust with Microsoft Entra:

- Implement Conditional Access policies based on risk, device compliance, and user context.
- Mandate multi-factor authentication for all users, especially for privileged roles and sensitive resources.
- Enforce least privilege through RBAC and PIM, minimizing standing administrative access.
- Continuously monitor identity activity and configure automated responses to suspicious behavior.
- Integrate Entra with other Microsoft security solutions for unified protection and visibility.
- Educate users on secure authentication practices and regularly review access policies for alignment with evolving threats.

Microsoft Entra provides a comprehensive platform for operationalizing Zero Trust principles, combining identity-centric controls, adaptive policies, and deep integrations with the Microsoft security ecosystem. By leveraging Entra's capabilities—such as Conditional Access, MFA, RBAC, device compliance, real-time analytics, and automated response—organizations can systematically reduce risk, prevent unauthorized access, and respond swiftly to emerging threats. As the security landscape continues to evolve, Microsoft Entra stands as a critical foundation for building a resilient, adaptive, and Zero Trust-aligned enterprise.

Microsoft Entra and Mesh architecture

Mesh architecture represents a significant evolution in the design and management of modern IT environments. Unlike traditional hub-and-spoke models, Mesh is characterized by its decentralized, interconnected approach, where each node (such as users, devices, applications, and services) can communicate securely and directly with others. This model eliminates single points of failure, enhances scalability, and increases resilience by distributing control and connectivity across the organization.

Core principles of Mesh architecture include:

- **Decentralization:** Authority and access control are distributed, reducing reliance on central gateways.
- **Direct Connectivity:** Nodes can authenticate and interact with each other without routing through a centralized broker.

- **Dynamic Trust:** Trust relationships are established contextually and adaptively, based on real-time risk assessments and policy evaluations.
- **Scalability and Flexibility:** Mesh architectures support rapid scaling and flexible deployment across hybrid and multi-cloud environments.

Organizations are adopting Mesh to address the growing complexity of cloud-native applications, remote workforces, and the need for seamless, secure interconnectivity across distributed resources. Mesh provides the agility and resilience required to support digital transformation initiatives while maintaining robust security postures.

Let's explore how Microsoft Entra supports the Mesh architecture.

Technical integration points

In a Mesh environment, seamless and secure connectivity between nodes requires robust identity management.

- **Identity Federation:** Entra enables federated authentication across disparate domains, allowing users and services from different parts of the Mesh to trust each other based on standardized protocols (such as SAML, OAuth, and OpenID Connect).
- **Policy Enforcement:** Conditional Access policies can be dynamically applied to every access request, ensuring that context-driven controls (such as device compliance, user risk, and location) are enforced throughout the Mesh.
- **Integration with Service Mesh Technologies:** Entra can be integrated with service mesh platforms (e.g., Azure Service Mesh, Istio) to provide identity-aware routing, mutual TLS authentication, and fine-grained authorization at the service-to-service level.
- **Automated Provisioning and Deprovisioning:** Entra's identity lifecycle management automates the provisioning and removal of access as nodes join or leave the Mesh, reducing administrative overhead and minimizing risk.

Microsoft Entra serves as the identity backbone, enabling authentication, authorization, and policy enforcement at every interaction point.

Identity management integration

Identity management in a Mesh environment must be adaptive, context-aware, and resilient. Entra provides:

- **Unified Identity Store:** Centralized directory services with support for hybrid and multi-cloud scenarios.
- **Delegated Administration:** Granular delegation of administrative rights facilitates distributed management while maintaining oversight.

- **Single Sign-On (SSO):** Streamlined user experience across Mesh-connected applications and services.
- **API Security:** Entra supports securing APIs within the Mesh using OAuth 2.0, ensuring that only authorized entities can access sensitive resources.

Security and compliance in Mesh with Microsoft Entra

Security and compliance are critical in a distributed Mesh architecture. Microsoft Entra enhances the security posture and compliance readiness of organizations by:

- **Zero Trust enforcement**: Entra operationalizes Zero Trust by requiring authentication and authorization at every node-to-node interaction, continuously validating trust based on real-time risk signals.
- **Threat detection and automated response**: Entra monitors identity activity across the Mesh, detects anomalous behavior, and triggers automated responses to mitigate threats.
- **Regulatory compliance**: Entra provides audit trails, access reviews, and policy enforcement to support compliance with standards such as GDPR, HIPAA, and ISO 27001.
- **Data protection**: Entra integrates with Microsoft Purview Information Protection to classify and safeguard data as it moves throughout the Mesh.
- **Resilience and redundancy**: Decentralized identity and access controls reduce single points of failure, enhancing organizational resilience.

Implementation best practices

Successfully integrating Microsoft Entra with Mesh architecture requires careful planning and execution. Key best practices include:

- **Assess Identity Requirements:** Map out all nodes, users, services, and applications that will participate in the Mesh. Identify trust boundaries and integration points.
- **Design Conditional Access Policies:** Develop granular policies that account for user risk, device compliance, location, and application sensitivity. Test policies in pilot environments before broad deployment.
- **Leverage Federation and SSO:** Integrate external identities and enable SSO to reduce friction and improve security across Mesh-connected resources.
- **Automate Lifecycle Management:** Use Entra's provisioning tools to automate onboarding and offboarding processes, ensuring access is granted and revoked promptly as nodes join or leave the Mesh.

- **Monitor and Respond:** Continuously monitor identity activity using Entra's analytics and configure automated responses to suspicious behavior.
- **Document and Review:** Regularly review access policies, audit logs, and compliance reports to ensure alignment with organizational goals and regulatory requirements.
- **Integrate with Service Mesh Platforms:** Where applicable, integrate Entra with service mesh tools to extend identity-aware controls to microservices and APIs.

Common pitfalls to avoid include over-reliance on default policies, insufficient monitoring, and lack of coordination between IT and security teams. Collaboration and iterative policy refinement are essential for maintaining a secure and agile Mesh environment.

Real-world use cases

Let's explore a few real-world use cases to better understand this concept.

- **Global retailer:** A multinational retailer adopted Mesh architecture to connect its distributed stores, warehouses, and e-commerce systems. By integrating Entra for identity management, the organization enabled secure, direct communication between locations while enforcing strict access policies. Automated provisioning ensured that seasonal staff received appropriate access, and real-time monitoring detected and responded to credential misuse.
- **Healthcare provider:** A healthcare network leveraged Mesh and Entra to securely connect clinics, remote practitioners, and third-party service providers. Entra's Conditional Access and MFA protected sensitive patient data, while delegated administration allowed local IT teams to manage access without compromising central oversight. Compliance with HIPAA and other regulations was streamlined through Entra's audit and reporting capabilities.
- **Financial services firm:** A financial institution implemented Mesh to support secure, low-latency interactions between trading platforms, analytics engines, and compliance tools. Entra's identity federation enabled seamless integration of third-party applications, while RBAC and PIM minimized standing privileges and reduced insider risk. Automated threat detection rapidly contained suspicious activity, preserving trust and uptime.

Integrating Microsoft Entra with Mesh architecture empowers organizations to achieve secure, scalable, and resilient connectivity across distributed resources. Entra's robust identity management, adaptive policy enforcement, and deep integration capabilities align perfectly with the core principles of Mesh. By following best practices and leveraging Entra's advanced features, organizations can operationalize Zero Trust, enhance security and compliance, and support dynamic business needs in the era of digital transformation. As Mesh architecture

continues to gain traction, the partnership between Microsoft Entra and Mesh will be instrumental in building the next generation of secure, connected enterprises.

Summary

This chapter began by discussing the various activity logs available in Microsoft Entra that help organizations gain an understanding of user behavior in their tenant and analyze and troubleshoot access issues. It outlined the reports available in Microsoft Entra and how they help administrators gain insights into how their tenant is being used. Next, it explained how Microsoft recommendations guide administrators to improve the identity security posture of their tenant by aligning with Microsoft-recommended best practices. This chapter also covered the Microsoft Entra threat landscape, the types of threats faced by Microsoft Entra and how administrators can protect their tenants using the tools available in Microsoft Entra. It concluded by explaining the important concepts of Zero Trust and Mesh and how Microsoft Entra helps align with and implement these in the real world. In the next chapter, we will discuss how organizations can migrate to Microsoft Entra.

Exercises

1. You are an IT administrator for your organization. You are investigating why users were blocked from signing into an application. Which logs would you investigate?
    a. Audit logs
    b. Provisioning logs
    c. Microsoft Graph logs
    d. Sign-in logs
2. You are an IT administrator tasked with reducing dependency on the on-premises environment. You know that there are still applications that use AD FS authentication. What is the best way to identify these applications?
    a. Check the application activity logs.
    b. Check the AD FS application migration report.
    c. Check the service principal sign-in activity.
    d. Check the audit logs.
3. You are an IT administrator. Your organization has asked you to work toward improving the security posture of your organization. You want to first understand your current security posture. What should you do first?
    a. Look at Entra ID recommendations and identify the ones to complete.
    b. Perform a complete analysis of the current Entra ID configuration.

c. Check the identity secure score.

d. Export logs to Azure Monitor.

Answers

1. d
2. b
3. c

Additional resources

- Activity log schema: `https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-activity-log-schemas`
- What is Zero Trust?`https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview`
- Microsoft Entra Exporter`https://github.com/microsoft/entraexporter`
- Microsoft 365 Desired State Configuration: `https://github.com/microsoft/Microsoft365DSC`
- Conditional Access APIs: `https://learn.microsoft.com/en-us/graph/api/resources/conditionalaccesspolicy?view=graph-rest-1.0`

Join us on Discord

For discussions around the book and to connect with your peers, join us on Discord at `packt.link/discordcloud` or scan the QR code below:



17

Migrating to Microsoft Entra ID

Migrating from an on-premises **Active Directory** (**AD**) environment to Microsoft Entra represents a significant shift in how organizations manage identity and access. This transition is driven by the need for greater flexibility, enhanced security, and improved support for remote and hybrid working models. However, the migration process is not without its challenges. Organizations often encounter roadblocks such as complex legacy infrastructure, dependencies on on-premises applications, and the need to ensure seamless integration with existing systems. Data consistency, user authentication methods, and compatibility with older applications can also complicate the migration journey.

Another common challenge is managing user expectations and change resistance, especially when familiar workflows are altered. Security concerns, such as safeguarding sensitive information during the transition and maintaining compliance, are paramount. Despite these hurdles, the advantages of migrating to Microsoft Entra are compelling. Organizations gain access to advanced cloud-based security features, streamlined identity management, and improved scalability. Microsoft Entra also simplifies access for users, enabling secure single sign-on across a wide range of cloud and on-premises applications. Ultimately, a well-planned migration can reduce operational overhead, enhance security posture, and position organizations to better support future digital transformation initiatives.

In this chapter, we will cover:

- Understanding the migration landscape
- States of transformation
- Migration strategies
- Journey to the cloud

Understanding the migration landscape

For more than two decades, on-premises **Active Directory Domain Services (AD DS)** has served as the backbone of enterprise identity and access management. Organizations worldwide have built complex ecosystems around AD DS, including **Group Policy Objects** (**GPOs**), Kerberos and NTLM authentication, LDAP-based application integrations, and multi-forest trust relationships. However, as cloud computing, remote work, and Zero Trust security models have become standard, the limitations of a perimeter-based identity system have become increasingly apparent.

Microsoft Entra ID represents the modern, cloud-native evolution of identity management. It provides a comprehensive identity platform supporting modern authentication protocols such as OAuth 2.0, OpenID Connect, and SAML 2.0, along with advanced security features including Conditional Access, Identity Protection, and **Privileged Identity Management** (**PIM**).

Before diving into specific migration steps, it is essential to understand why organizations migrate, what changes fundamentally between AD DS and Microsoft Entra ID, and what the scope of a typical migration entails.

Organizations pursue this migration for several compelling reasons:

- **Cloud-first strategy:** As organizations adopt Microsoft 365, Azure, and SaaS applications, Entra ID becomes the natural identity backbone for cloud resources.
- **Enhanced security:** Entra ID provides Multi-Factor Authentication (MFA), Conditional Access, risk-based Identity Protection, and passwordless authentication capabilities that far exceed what on-premises AD DS offers natively.
- **Reduced infrastructure costs:** Eliminating or reducing on-premises domain controllers, **Active Directory Federation Services (AD FS)** farms, and VPN infrastructure lowers operational expenditure and administrative overhead.
- **Modern workforce support:** Remote and hybrid work models require identity solutions that work seamlessly regardless of network location, device type, or geographic boundary.
- **Governance and compliance:** Entra ID delivers advanced identity governance features including Access Reviews, Entitlement Management, Lifecycle Workflows, and dynamic group membership that help meet regulatory and compliance requirements.

Understanding the fundamental architectural differences between AD DS and Microsoft Entra ID is critical for planning a successful migration.

Capability	Active Directory (AD DS)	Microsoft Entra ID
Architecture	Hierarchical (forests, domains, OUs)	Flat tenant-based structure
Authentication Protocols	Kerberos, NTLM, LDAP	OAuth 2.0, OpenID Connect, SAML 2.0
Device Management	Group Policy Objects (GPOs)	Microsoft Intune, Configuration Manager, Windows Autopilot
Application Integration	LDAP binds, Kerberos auth	SSO via SAML/OIDC, App Proxy
Network Dependency	Requires line-of-sight to DCs	Internet-based, works anywhere
Security Model	Network perimeter-based	Zero Trust, identity-driven

Table 17.1: AD DS vs Microsoft Entra ID

The recommended approach is to first halt the growth of Active Directory and then systematically move existing on-premises workloads to Microsoft Entra ID through structured migration workstreams.

States of transformation

Most organizations today have existed for many years and have a significant on-premises footprint, such as on-premises file servers, mainframes, domain controllers, print servers, and applications running on legacy software. As a part of modernization and adoption of Zero Trust, organizations are shifting from on-premises to using solutions built in the cloud and for the cloud. More than 90 percent of organizations worldwide run Active Directory. For these organizations, Microsoft Entra plays a key role. Moving from Active Directory to Microsoft Entra is not a single-step process. It requires significant investment in terms of time and resources. Organizations go through several stages of transformation. These are described below.

Cloud-attached

This is the first stage where organizations have created a Microsoft Entra tenant to enable user productivity tools like Microsoft Teams, SharePoint Online and OneDrive for Business. However, most of the management still remains on-premises. Devices are joined to Active Directory and managed using Group Policy. Users are created and managed on-premises and synchronized to Microsoft Entra. Applications authenticate to Active Directory or AD FS.

Hybrid

In this stage, organizations begin to add cloud capabilities to their on-premises environment to reduce complexity, improve security, and reduce their on-premises footprint. Organizations start upskilling on using Microsoft Entra ID for Identity and Access Management, usually starting with user and device management. In this stage, devices are usually Microsoft Entra hybrid joined, and non-Microsoft applications start being integrated with Microsoft Entra to provide users with a Single Sign-On experience. Organizations may consider using Microsoft Entra Private Access to provide access to on-premises legacy applications.

Cloud-first

Once organizations are comfortable operating in a hybrid environment, they start moving more workloads to the cloud. Most organizations spend years at this stage. In the cloud first stage, devices are managed using Microsoft Intune and are Microsoft Entra joined. Users and groups are created and managed in Microsoft Entra ID.

Active Directory minimized

Most organizations have a significant on-premises footprint and minimizing Active Directory is challenging. There may be some use cases that still require on-premises infrastructure. In this stage organizations start looking at ways to move applications to Microsoft Entra and modernize applications and services that cannot be moved.

Cloud-only

In this stage, organizations have moved all workloads to the cloud and removed all on-premises domain controllers. Most organizations aspire to be in this stage in the long-term. In this stage, there are no on-premises domain controllers and users, groups and devices are created and managed directly in Microsoft Entra ID. All applications and services that used to depend on Active Directory have been modernized.

Migration strategies

There is no one-size-fits-all approach to migrating from Active Directory to Microsoft Entra ID. The optimal strategy depends on your organization's size, complexity, legacy dependencies, risk tolerance, and timeline. The four primary strategies are outlined below.

Phased migration

A phased migration is the most common and lowest-risk approach. It involves migrating workloads, users, and applications to Microsoft Entra ID incrementally over a planned timeline, typically spanning months to years depending on organizational complexity.

Key characteristics:

- Identity synchronization is established via Microsoft Entra Connect.
- Users and groups are migrated in defined waves, often by department, region, or business unit.
- Applications are modernized or migrated to cloud authentication iteratively.
- On-premises AD DS remains operational throughout the transition period.
- Each phase includes its own pilot, validation, and rollback plan.

This strategy is best for large enterprises with complex AD environments, multiple forests, and extensive application dependencies.

Hybrid coexistence

Hybrid coexistence is the most widely adopted approach and is often the first step toward a full cloud migration. In this model, on-premises AD DS and Microsoft Entra ID operate side by side, with identity synchronization maintaining consistency between the two directories.

Key characteristics:

- Microsoft Entra Connect or Microsoft Entra Cloud Sync bridges on-premises AD with Entra ID.
- Users maintain a single identity across both environments.
- Cloud authentication is configured for cloud resource access.
- Legacy applications continue to use on-premises AD for authentication.
- Gradual reduction of on-premises dependencies over time.

This strategy is ideal for organizations that must maintain on-premises infrastructure for specific workloads while progressively adopting cloud services.

Lift-and-Shift migration

A lift-and-shift approach moves existing AD DS domain controllers into Azure Infrastructure-as-a-Service (IaaS) virtual machines while simultaneously establishing Entra ID as the primary identity provider for cloud workloads.

Key characteristics:

- AD DS domain controllers are deployed as Azure VMs.
- Entra ID is used for cloud application authentication.
- Microsoft Entra Domain Services may be used for legacy applications requiring NTLM or Kerberos.
- Reduces physical data center footprint without re-architecting applications.

This strategy suits organizations with significant investment in legacy applications that cannot be immediately modernized but who want to eliminate physical on-premises infrastructure.

Greenfield (Cloud-Native) approach

A greenfield approach establishes Microsoft Entra ID as the sole identity provider from the start, with no dependency on on-premises Active Directory.

Key characteristics:

- No on-premises AD DS infrastructure is deployed or maintained.
- All devices are Entra ID joined.
- Device management is handled entirely through Microsoft Intune and Autopilot.
- All applications use modern authentication protocols like SAML, OIDC, and OAuth.
- Group Policy is replaced entirely by Intune configuration profiles and compliance policies.

This is most viable for new organizations, divisions, or post-merger scenarios where no legacy AD footprint exists.

Journey to the cloud

Transformation to the cloud is not just the responsibility of the identity team. Organizations need to coordinate efforts from all teams, including infrastructure, devices, networks, security, operations, human resources, and applications, to define policies that include people, processes, and technology. Support staff must be trained to operate in the new environment. Effective communication with employees must be planned to ensure that they are aware of any changes in their way of working. Careful planning must be done before beginning the journey to ensure a smooth experience for the IT teams and end users.

Prerequisites and planning

Thorough planning is the single most important factor for successful migration. Rushing into technical implementation without adequate preparation is the most common cause of migration failures, user disruption, and security gaps.

Organizational readiness

Before technical work begins, ensure the following organizational elements are in place:

- **Executive sponsorship:** Secure buy-in from IT leadership and business stakeholders. Migration affects every user and every application.
- **Project governance:** Establish a cross-functional migration team with representation from identity, security, networking, application, and end-user support teams.
- **Communication plan:** Develop a comprehensive communication strategy to keep users informed of changes, timelines, and any actions required on their part.
- **Change management:** Create training materials and support resources, especially for self-service password reset (SSPR), MFA enrolment, and new sign-in experiences.
- **Rollback procedures:** Document rollback plans for every phase of migration to ensure rapid recovery in the event of issues.

Once a proper plan has been implemented, it is time to work on the technical details.

Technical prerequisites

The following technical prerequisites must be satisfied before migration begins.

- Verify that all user UPN suffixes match a verified custom domain in Entra ID.
- Clean up the on-premises Active Directory by removing stale accounts, standardizing naming conventions and resolving duplicate or conflicting attributes.
- Create emergency break-glass accounts in Entra ID with Global Administrator privileges, using the `*.onmicrosoft.com` domain, and exclude them from all Conditional Access policies.
- Deploy Microsoft Entra Connect or Microsoft Entra Cloud Sync on a supported Windows Server.
- Configure Microsoft Entra ID audit logging and diagnostic settings to stream sign-in and audit logs to a Log Analytics workspace.
- Establish a dedicated pilot group of representative users to test each migration phase.

Planning a phased migration from AD to Microsoft Entra ID helps ensure a smooth transition with minimal downtime.

Licensing requirements

Microsoft Entra ID is available in multiple tiers. Migration typically requires at least Microsoft Entra ID P1 for Conditional Access. Microsoft Entra ID P2 is recommended for organizations that require Identity Protection, PIM, and Access Reviews. Organizations requiring ID Governance may need the Microsoft Entra ID Governance or the Microsoft Entra Suite license.

Assessing the current Active Directory environment

A thorough assessment of the existing AD environment is critical for identifying risks, dependencies, and the scope of work required. This phase should be completed before any synchronization or authentication changes are implemented.

Inventory and discovery

Conduct a comprehensive inventory of the following:

- **Users and groups:** Total count, naming conventions, nesting depth, distribution vs. security groups, mail-enabled groups, and dynamic membership rules.
- **Organizational Units (OUs):** Structure, GPO linkages, and delegation of control configurations.
- **Service accounts:** Identify all service accounts, their purposes, password rotation policies, and the applications or services that depend on them.
- **Applications:** Catalog every application that authenticates against AD DS, noting the authentication method used (Kerberos, NTLM, LDAP bind, ADFS/SAML, forms-based, etc.).
- **Domain controllers:** Number, geographic distribution, FSMO role holders, replication topology, and OS versions.
- **Trust relationships:** Forest trusts, external trusts, and shortcut trusts with partner organizations.
- **Custom schema extensions:** Any custom attributes or schema modifications that may require special handling during synchronization.

Creating this kind of inventory helps in mapping out dependencies and understanding the scale of the migration.

Dependency mapping

Map dependencies across the following critical areas.

- Group Policy Objects (GPOs) and their linked Organizational Units (OUs).
- LDAP queries from applications, scripts, and automation tools.
- NTLM and Kerberos authentication dependencies.

- File shares with NTFS permissions based on AD security groups.
- Print servers and RADIUS-based network access.
- VPN and remote access solutions that rely on AD authentication.
- Custom scripts and PowerShell automation that query AD directly.

Tip

Use Microsoft Defender for Identity to gain visibility into on-premises AD activity, identify risky configurations, and detect lateral movement paths before migration begins.

Identity synchronization

Identity synchronization is the foundational step in most migration strategies. It creates a bridge between on-premises AD and Microsoft Entra ID, ensuring that user identities, group memberships, and attributes are consistent across both directories. Depending on the organization's requirements, you can use Microsoft Entra Connect Sync or Microsoft Entra Cloud Sync. These have been discussed in detail in *Chapter 3, Implementing Microsoft Entra ID*.

Migrating authentication

Selecting and implementing the correct authentication method is one of the most consequential decisions in migration. Microsoft Entra ID supports three primary authentication methods for hybrid environments, each with distinct characteristics, security profiles, and infrastructure requirements. These are password hash sync, pass-through authentication, and federation using AD FS. These have been discussed in detail in *Chapter 3, Implementing Microsoft Entra ID*. Review each method carefully before choosing the right method for your organization, as this decision is difficult to change later.

If your organization is using AD FS, migration to cloud authentication is a key step involving several dependencies like removing applications that depend on AD authentication. It is recommended to follow a staged rollout capability that enables selective testing of cloud authentication methods with specific user groups before performing a full domain cutover.

Migrating applications

Application migration is often the most complex and time-consuming aspect of the journey to Microsoft Entra ID. Legacy applications built with dependencies on Kerberos, NTLM, and LDAP authentication do not natively integrate with modern cloud identity. Application migration involves the following steps:

Application discovery and classification

Begin by classifying all applications into categories based on their authentication method and cloud readiness. The following categories could be used:

- **Cloud ready**: Modern applications that already support SAML, OIDC, or OAuth 2.0.
- **Migration candidates**: Applications using AD FS for federated authentication.
- **Legacy applications**: Applications that use LDAP, Kerberos or NTLM. These applications may require Microsoft Entra Private Access or Microsoft Entra Domain Services.

Once you have this inventory, you can plan to modernize or re-architect applications or implement services like Microsoft Entra Private Access and Microsoft Entra Domain Services. This also helps identify stale applications that are no longer required and don't need to be migrated. These can be retired.

Migration approaches by application type

Depending on the type of application, different methods of migration will apply. The following approaches can be used based on application classification:

- **SaaS applications**: Configure SSO in the Entra ID Enterprise Applications gallery. Most major SaaS applications have pre-built integrations.
- **AD FS relying parties**: Migrate to Entra ID by reconfiguring the SAML trust relationship. The AD FS application activity report helps identify migration-ready applications.
- **On-premises web applications**: Use Microsoft Entra Private Access to publish on-premises web applications securely without VPN, enabling the use of cloud-based SSO and Conditional Access.
- **Legacy Kerberos/NTLM applications**: Deploy Microsoft Entra Domain Services in Azure, which provides managed domain services compatible with legacy applications that rely on LDAP, NTLM, and Kerberos. Domain services has been discussed in *Chapter 4, Microsoft Entra Domain Services.*
- **Custom applications**: Modernize by integrating with the Microsoft Identity Platform using MSAL libraries for native OIDC/OAuth support.

Classifying applications based on types helps you understand the time and effort required to migrate each application.

Conditional Access policies

Conditional Access is the Zero Trust policy engine in Microsoft Entra ID. It evaluates real-time signals (user, device, location, application, risk level) at sign-in time and enforces granular

access controls. Designing a robust Conditional Access framework during migration is essential for maintaining security without disrupting user productivity.

Follow these design principles when building your Conditional Access policies:

- Adopt a structured naming convention with sequence numbers.
- Ensure every application has at least one policy applied.
- Assign policies through groups rather than individual users.
- Always exclude break-glass emergency accounts from all policies.
- Use report-only mode extensively before enforcing new policies.
- Implement disabled backup policies as resilient access controls for outage scenarios.

The following baseline policies form the foundation of a secure Conditional Access deployment:

Policy	Target	Control
Require MFA for all users	All users, all cloud apps	Require authentication strength
Require phishing-resistant MFA for admins	Administrative roles	Require phishing-resistant methods
Block legacy authentication	All users, all cloud apps	Block access for legacy client apps
Require compliant devices	All users, all cloud apps	Require device compliance or hybrid join
Risk-based sign-in policy	All users (Entra ID P2)	Require MFA for medium/high risk sign-ins
Risk-based user policy	All users (Entra ID P2)	Require password change for high-risk users

Table 17.2: Suggested Conditional Access policies

These policies must be evaluated and adapted by each organization before deployment.

Device migration and management

Device management is a critical component of migration. The target state determines how devices authenticate, receive policies, and access corporate resources.

Devices can be joined to Microsoft Entra in one of the following ways:

- **Microsoft Entra joined**: The recommended state for new devices. Devices are registered directly in Entra ID with no on-premises AD dependency. Managed entirely through Microsoft Intune.
- **Hybrid Microsoft Entra joined**: A transitional state for devices that must remain joined to on-premises AD while also being registered in Entra ID. Useful during the migration period.
- **Microsoft Entra registered**: For personal devices that need to access corporate resources without full device management.

Identify the types of devices in use in your organization and decide the best domain join option for them.

Following are some recommendations for migrating devices:

- Configure Windows Autopilot to provision all new devices as Entra ID joined with Intune management.
- Migrate Group Policy settings to Intune configuration profiles and compliance policies.
- Identify and resolve application compatibility issues on Entra ID-joined devices.
- Plan the transition for existing devices by either re-imaging them as Entra ID joined during a hardware refresh cycle or reprovisioning existing hybrid joined devices as Entra ID joined.
- Validate device-based Conditional Access policies with Entra ID-joined devices.

These are best practices and organizations can choose different methods as per their requirements.

Security considerations

Security must be embedded into every phase of migration, not treated as an afterthought. The transition from a perimeter-based security model to an identity-driven Zero Trust model requires a fundamental shift in security architecture and operations.

Zero Trust alignment

The migration to Microsoft Entra ID is an opportunity to implement Zero Trust principles across the identity infrastructure. The following are the core Zero Trust principles to implement during migration:

- **Verify explicitly**: Always authenticate and authorize based on all available data points (user identity, device health, location, application sensitivity, risk level).

- **Use least privileged access**: Limit user access with **just-in-time (JIT)** through Privileged Identity Management. Use Entra ID RBAC to ensure **just-enough-access (JEA)**.
- **Assume breach**: Minimize blast radius through network segmentation, encryption, and continuous monitoring.

Microsoft Entra offers tools like Microsoft Entra ID Protection and Microsoft Entra Privileged Identity Management to achieve the Zero Trust principles.

Privileged Access Management

Protecting privileged accounts is paramount during and after migration:

- Implement Microsoft Entra Privileged Identity Management for all administrative roles.
- Use time-bound, approval-required role activations instead of permanent role assignments.
- Require phishing-resistant MFA for all privileged operations.
- Create dedicated cloud-only administrative accounts that are separate from synchronized on-premises accounts.
- Monitor privileged role activations through PIM alerts and Entra ID audit logs.

PIM has been discussed in detail in *Chapter 8, Microsoft Entra Privileged Identity Management.*

Identity protection

Microsoft Entra ID Protection provides automated risk detection and remediation:

- **User risk detection:** Identifies compromised user accounts through leaked credential detection, threat intelligence, and anomalous behavior analysis.
- **Sign-in risk detection:** Evaluates individual sign-in attempts for anomalies such as atypical travel, anonymous IP addresses, password spray attacks, and malware-linked IP addresses.
- **Automated remediation:** Configure Conditional Access policies to automatically require MFA, password changes, or block access based on detected risk levels.

Identity protection has been discussed in detail in *Chapter 9, Microsoft Entra ID Protection.*

On-premises decommissioning

Once you verify that identity, device management, authentication, networking, and legacy workloads no longer depend on domain controllers, you can start decommissioning on-prem AD. The safest path is a staged shutdown. Below is some guidance on how to approach this.

Confirm no service depends on on-premises domain controllers

The first step in beginning to decommission on-premises domain controllers is to ensure that no service depends on them. Below is a checklist:

- Identity dependencies: Ensure that no applications require Kerberos/NTLM, LDAP, or AD DS lookups.
- Authentication flows: Ensure that authentication has moved completely to the cloud and that there are no AD FS servers, no PTA agents, and no password hash sync dependencies.
- Device join state: All devices must be Entra--oined or Entra-registered. No domain joined or hybrid joined devices should exist.
- Group Policy usage: Ensure that all GPOs have been migrated to the cloud.
- File/print services: Migrate on-premises file servers to SharePoint and move printing to the cloud. There should be no SMB shares requiring AD authentication.
- DNS dependencies: No internal DNS zones are tied to domain controllers.
- Certificate services: No AD CS templates, auto-enrollment, or domain-joined PKI.
- SCCM/ConfigMgr: Ensure no devices are managed using ConfigMgr or co-managed.
- RADIUS/NPS: Move Wi-Fi authentication to Entra ID.

Performing these checks prevents surprises later.

Validate Entra ID is the authoritative source

The next step is to make Entra ID authoritative for users, groups and devices. The following is a useful checklist.

- User lifecycle: Ensure that users are created and managed directly in the cloud.
- Group lifecycle: Ensure that groups are created and managed directly in the cloud.
- Access policies: Configure appropriate Conditional Access and identity protection policies.
- App authentication: Confirm that all applications use OIDC/SAML and no application depends on Kerberos.
- Device compliance: All devices should be managed using Intune.

Once it is confirmed that Entra ID is the source of authority, you can begin removing on-prem components.

Remove hybrid identity components

If you used hybrid identity, remove these in order:

- Microsoft Entra Connect: This involves disabling synchronization to Microsoft Entra and uninstalling Microsoft Entra Connect from the server it was installed on.
- PTA agents: If you had configured Pass-Through Authentication, remove all agents.
- AD FS: Migrate all relying parties to Entra and decommission the AD FS farm.

Once the hybrid dependencies are removed, ensure that there are no on-premises services depending on Active Directory.

Clean up the domain

Once dependencies are gone, ensure that there are no more servers that are joined to the Active Directory domain. Once done, remove all forest and domain trusts and remove entries from Active Directory sites and services entries.

Decommission domain controllers

The last step is to start decommissioning domain controllers. Depending on the number of domain controllers this activity could take several days or weeks. The following steps should be taken in order:

1. Transfer all FSMO roles to a single DC
2. Demote secondary DCs
3. Demote the final DC
4. Remove AD DS role
5. Power off

As a final cleanup step after decommissioning domain controllers, ensure that all AD DNS zones, DNS records, DHCP scopes, and client references to domain controllers are removed.

Summary

Migrating from on-premises Active Directory to Microsoft Entra ID is one of the most significant infrastructure transformations an organization can undertake. It touches every user, every device, and every application in the environment. Success requires a methodical approach that combines thorough planning, the right migration strategy, robust security practices, and continuous validation. This chapter discussed the states of migration and migration strategies and provided detailed guidance to migrate from Active Directory to Microsoft Entra ID. The journey from Active Directory to Microsoft Entra ID is not a single event but an ongoing transformation. Organizations that approach it with discipline, patience,

and a focus on security will emerge with a modern identity infrastructure that is more resilient, more secure, and better positioned to support the demands of the cloud-first era.

Exercises

1. In which of the following scenarios would you recommend a lift-and-shift migration from AD to Microsoft Entra ID?
    a. The organization wants to modernize identity immediately, has no on-premises dependencies left, and is ready to retire Active Directory with minimal redesign of apps or policies.
    b. The organization relies heavily on complex Group Policy Objects, multi-tiered domain trusts, and custom Kerberos extensions that must remain unchanged.
    c. The organization needs to redesign its identity architecture to support Zero Trust, implement new Conditional Access policies, and restructure its OU model before moving to the cloud.
    d. The organization has dozens of legacy LDAP-bound applications that cannot authenticate with modern protocols and require significant refactoring before cloud migration.
2. What are the advantages of discovering applications during migration from AD to Microsoft Entra ID?
    a. It automatically converts all legacy applications to support modern authentication without any developer involvement.
    b. It eliminates the need for Conditional Access design because discovered apps inherit cloud policies by default.
    c. It helps identify which applications can be modernized, retired, or re-platformed, reducing migration risk and improving planning accuracy.
    d. It guarantees that every application will function identically in Entra ID without requiring configuration changes.
3. Your organization is migrating from Active Directory to Microsoft Entra ID and wants to manage new devices directly in the cloud. Which device join method should you use?
    a. Hybrid Microsoft Entra joined
    b. Domain joined
    c. Microsoft Entra registered
    d. Microsoft Entra joined

Answers

1. a
2. c
3. d

Additional resources

- AD minimization case studies: `https://learn.microsoft.com/en-us/entra/architecture/road-to-the-cloud-ad-minimization`
- Migration best practices: `https://learn.microsoft.com/en-us/entra/architecture/migration-best-practices`

Get this book's PDF version and more

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.





Note: Keep your invoice handy. Purchases made directly from Packt don't require an invoice.

18

Career Opportunities with Microsoft Entra Skills

A career built on Microsoft Entra expertise is becoming one of the most dynamic and future-proof paths in the technology landscape. As organizations accelerate their move to cloud-first, Zero Trust architectures, they increasingly rely on professionals who can design, secure, and govern identity at scale. Entra sits at the center of this shift: it is no longer just an identity platform, but the control plane for access, trust, and digital safety across hybrid and multi-cloud environments. This chapter explores how Entra skills open doors to roles that blend technical depth with strategic influence, from identity engineering and access governance to AI-driven security operations and cross-cloud compliance.

The demand for Entra-literate talent is rising because identity has become the new perimeter. Companies need people who can translate business risk into policy, automate lifecycle management, integrate diverse applications, and build resilient access strategies that support both human and machine identities. These capabilities are now essential in cybersecurity, cloud architecture, DevOps, and emerging AI governance roles. Whether you are early in your career or looking to pivot into a high-impact domain, mastering Entra positions you at the intersection of security, innovation, and organizational trust.

This chapter maps Microsoft Entra skills to real job roles and career paths, showing where identity fits in modern security and cloud programs, and how to translate hands-on Entra experience into job-ready capability. It is intended for:

Early-career IT pros who want a clear set of identity-focused entry points and portfolio projects.

- **Experienced IT pros** who want to pivot into identity, improve seniority, or broaden scope into Zero Trust and cloud security programs.

The Entra leverage

The market signals are unambiguous. According to MarketsandMarkets, the global identity and access management market was valued at approximately $25 billion in 2025 and is projected to reach $42 billion by 2030, growing at a compound annual rate of 10.4 percent. According to Seeknay's State of IAM Job Market 2026 report, security roles are tracking salary increases of 4 percent annually, more than double the 1.6 percent growth seen across general technology positions, and 52 percent of technology leaders report they will increase starting offers for candidates with security skills. Within this landscape, Microsoft holds a position as a recognized leader in IAM and the Entra platform's deep integration with Microsoft 365 and Azure means that professionals who master these tools find themselves at the intersection of the two largest enterprise software ecosystems in the world. For professionals considering where to build a durable, rewarding career in technology, few domains offer the combination of growing demand, competitive compensation, and meaningful impact that identity and access management provides.

Professionals with Entra knowledge have strengths that come from its unique position as the identity fabric that connects people, devices, workloads, and AI systems across an organization. Because identity now anchors every access decision, professionals who understand Entra can influence security, productivity, and governance in ways few other skill sets allow. This leverage shows up in three powerful ways: the ability to design Zero Trust foundations, the capability to automate and simplify complex access workflows, and the insight to govern human and machine identities at scale.

Identity is the control plane for modern access: Apps, data, devices, and APIs increasingly gate access through Entra-based policies rather than network location.

- **Every major change program touches identity**: Cloud migrations, SaaS adoption, mergers/acquisitions, application modernization, and security uplift.
- **Regulatory and customer pressure** drives stronger authentication, least privilege, auditability, and lifecycle governance.

Automation is expected at scale: Organizations need role assignments, access reviews, and onboarding/offboarding to be policy-driven and API-enabled.

As organizations adopt more cloud services and AI agents, Entra skills become a multiplier turning identity expertise into strategic impact.

Job roles for identity professionals

Each role below includes what the job does, the Entra capabilities most relevant to it, adjacent skills that employers often expect, and guidance for both early-career entry and experienced-career pivots.

Identity administrator / identity operations (identity ops)

An identity administrator manages and maintains user identities and access within an organization. Responsibilities include user provisioning, troubleshooting access issues, maintaining tenant configurations, and enforcing security controls. They ensure smooth daily operations, monitor authentication activities, and support incident response, helping keep organizational systems secure and compliant.

What you do: Run day-to-day identity services like user lifecycle tasks, access troubleshooting, tenant hygiene, and operational change control.

Entra focus: Entra ID user and group management; authentication methods; Conditional Access basics; tenant settings; monitoring/sign-in logs; break-glass accounts.

- **Adjacent skills employers expect:** Basic networking and DNS; Microsoft 365 fundamentals; ticketing/ITIL; documentation; incident handling.

Early-career entry points: Professionals often move from service desk to identity. They start with account provisioning and MFA rollout support. Build a lab tenant to practice policy changes safely.

- **Experienced pivot angle:** Sysadmins can position themselves as the person who operationalizes security controls (MFA, CA baselines) and stabilizes identity during migrations.

Portfolio projects: Document an MFA rollout plan; implement a Conditional Access policy set for common scenarios (admin roles, risky sign-ins, legacy auth block).

The identity administrator role is suitable for both early-career professionals and experienced IT staff. Entry-level candidates often start with service desk tasks or account provisioning, while seasoned sysadmins can transition by leveraging operational expertise in security controls and identity management during organizational migrations and system upgrades.

Identity engineer (Microsoft Entra / IAM engineer)

An identity engineer designs, implements, and maintains secure identity and access solutions across cloud and hybrid environments. They manage authentication, authorization, lifecycle

automation, and directory integrations, ensuring the right users and workloads have the right access at the right time while strengthening an organization's Zero Trust security posture.

- **What you do:** Design and implement identity solutions like policies, integrations, and automation. Work across security, cloud, and app teams.
- **Entra focus:** Conditional Access design; identity protection concepts; app registrations; enterprise apps; SSO (SAML/OIDC); SCIM provisioning; hybrid identity considerations (directory sync); privileged role operations.
- **Adjacent skills employers expect:** Authentication protocols (SAML, OAuth2/OIDC); scripting (PowerShell); APIs/Graph basics; change management; troubleshooting distributed auth flows.

Early-career entry points: Move from Identity Ops by taking ownership of one capability (e.g., SSO onboarding for SaaS apps) and building repeatable patterns/runbooks.

- **Experienced pivot angle:** Security engineers can lead with "policy as code" thinking. Cloud engineers can emphasize app integration and automation across tenants and subscriptions.
- **Portfolio projects:** A reference design for onboarding an app to SSO and provisioning; a scripted joiner/mover/leaver workflow in a lab environment.

An identity engineer role typically requires mid-level to advanced experience in cloud identity platforms, especially Microsoft Entra. Candidates are expected to understand authentication protocols, access governance, automation, and security principles. Hands-on experience integrating applications, managing lifecycle workflows, and supporting zero-trust initiatives is essential for success in this role.

Security engineer (identity and access)

A security engineer specializing in identity and access management protects an organization's digital ecosystem by designing and enforcing secure authentication, authorization, and access controls. They manage identity platforms, monitor threats, implement Zero Trust policies, and ensure human and machine identities are governed, compliant, and resilient against evolving cyber risks.

What you do: Reduce identity-related risk by hardening authentication, improving access assurance, and detecting/responding to identity threats.

Entra focus: Conditional Access at scale; identity risk signals and response concepts; admin role separation; authentication strength strategy; legacy auth elimination; sign-in/anomaly investigation workflows.

- **Adjacent skills employers expect:** Threat modeling; incident response; log analysis; security baselines; basic understanding of endpoints and device posture signals.

Early-career entry points: Junior SOC/operations roles can specialize in identity-related investigations and become the *sign-in detective*.

Experienced pivot angle: Network security pros can shift from perimeter thinking to policy-driven access; GRC/assurance pros can operationalize controls into enforceable policies.

- **Portfolio projects:** A phased plan to block legacy authentication. Design a Conditional Access policy lifecycle from creation, testing, deployment to monitoring.

A security engineer specializing in identity and access management typically needs advanced, hands-on experience with Microsoft Entra. They should have a strong grasp of authentication protocols, conditional access, threat detection, and governance. Experience integrating applications, automating access workflows, and supporting zero-trust programs is essential for operating confidently in this role.

Identity governance specialist (access lifecycle and entitlement management)

An identity governance specialist ensures that the right users and workloads have the right access through well-designed policies, lifecycle processes, and compliance controls. They manage entitlement reviews, automate provisioning, enforce least-privilege principles, and maintain audit-ready governance frameworks that keep identity environments secure, efficient, and aligned with organizational risk and regulatory requirements.

What you do: Make access predictable, auditable, and reversible. Own processes like joiner/mover/leaver, access reviews, and time-bound access.

- **Entra focus:** Governance capabilities like access packages/entitlements, access reviews, lifecycle workflows. Guest user governance; privileged access processes; reporting for auditors.
- **Adjacent skills employers expect:** Process design; stakeholder management; role mining and RBAC concepts; documentation; comfort working with compliance/audit teams.

Early-career entry points: Analysts who like structured work can start by building role catalogs, defining approval workflows, and running access review campaigns.

- **Experienced pivot angle:** Business analysts, ITSM leads, and security governance professionals can step into a technical governance role by pairing process expertise with Entra implementation.
- **Portfolio projects:** Design an access package model for a fictional org. Build a quarterly access review plan with roles, owners, and evidence outputs.

An identity governance specialist typically needs mid-level to advanced experience with cloud identity platforms, especially Microsoft Entra. They should understand access lifecycle design, entitlement reviews, least-privilege models, and compliance requirements. Experience automating provisioning, integrating diverse applications, and maintaining audit-ready governance controls is essential to operate confidently and independently in this role.

Access governance analyst

An access governance analyst ensures that users and workloads have the correct access by monitoring entitlements, analyzing patterns, and supporting governance controls that keep identity environments compliant and low-risk. They review access assignments, validate policy alignment, support certification campaigns, and surface insights that help organizations enforce least-privilege and strengthen overall identity hygiene.

What you do: Analyze and validate user and workload access to keep entitlements accurate, compliant, least-privilege, and audit-ready.

Entra focus: Operate Entra ID Governance features like access reviews and entitlement management to maintain clean, well-controlled access across applications.

- **Adjacent skills employers expect**: Blend analytical skill, compliance awareness, technical fluency, and clear communication to interpret access patterns and drive remediation.

Early-career entry points: Enter from IAM support, service desk, junior analyst, or compliance roles that expose you to permissions and governance workflows.

- **Experienced pivot angle**: Transition from IAM operations, audit, risk, or security analysis roles seeking deeper involvement in preventative access controls.

Portfolio projects: Demonstrate capability through access review reports, role-mapping exercises, hygiene dashboards, and governance process guides that show measurable improvements.

An access governance analyst reviews, monitors, and validates user and workload entitlements to ensure access is accurate, compliant, and aligned with least-privilege principles. They

analyze patterns, support access reviews, identify anomalies, and partner with application and security teams to maintain clean, auditable access across the organization while strengthening overall identity hygiene.

Privileged access engineer (PAM / admin security)

A privileged access engineer safeguards an organization's most sensitive systems by designing, securing, and managing elevated access pathways. They implement just-in-time and just-enough-access models, maintain privileged identity tools, monitor high-risk activities, and enforce strict controls to prevent misuse. Their work ensures critical assets remain protected while enabling secure, auditable administrative operations.

What you do: Secure administrator and high-impact access by reducing standing privileges, enforcing approvals, and ensuring privileged actions are traceable.

Entra focus: Privileged role hygiene; privileged access processes (approval, time-bound elevation concepts); admin Conditional Access patterns; break-glass design and monitoring.

- **Adjacent skills employers expect:** Strong operational discipline; audit evidence; understanding of admin surfaces across Microsoft 365/Azure; incident response collaboration.

Early-career entry points: Start by documenting and cleaning up admin role assignments; implement a least-privilege model for a small set of roles in a lab.

- **Experienced pivot angle:** Senior sysadmins/architects can reframe their experience as *secure operations at the highest blast radius*.
- **Portfolio projects:** An admin role model (who gets what and why); a privileged access request workflow design with logging and review.

A privileged access engineer typically needs advanced experience securing administrative identities and high-risk access pathways across cloud and hybrid environments. They should be fluent in just-in-time and just-enough-access models, privileged identity tools, conditional access, monitoring, and threat response. Experience designing controls for sensitive systems and maintaining audit-ready governance is essential.

Identity architect / cloud security architect (identity)

An identity architect shapes the overall strategy, design, and governance of an organization's identity ecosystem. They create end-to-end architectures that unify authentication, authorization, lifecycle management, and privileged access across cloud and hybrid environments. Their work ensures scalability, resilience, and Zero Trust alignment while guiding engineering teams, influencing security posture, and integrating identity into broader business and technology roadmaps.

What you do: Set the standards, patterns, and target-state architecture for authentication, authorization, and identity governance across the enterprise.

Entra focus: Reference architectures for Conditional Access; tenant and identity boundary strategy (multi-tenant, B2B); role and entitlement models; identity integration standards for apps and APIs.

- **Adjacent skills employers expect**: Enterprise architecture communication; security frameworks/Zero Trust; cloud landing zone concepts; ability to write standards and influence roadmaps.

Early-career entry points: It is uncommon for an entry-level person to move directly into this role. Aim first for engineer roles, then take on design ownership for a domain.

- **Experienced pivot angle**: Infrastructure and security architects can add identity as a specialization, then grow into "*identity is the north star*" architecture leadership.

Portfolio projects: Produce an identity target-state diagram and principles; a decision record set (for example, authentication strengths, guest access strategy, exception handling).

An identity architect role typically requires senior-level experience in designing and governing complex identity ecosystems across cloud and hybrid environments. They need deep expertise in authentication standards, authorization models, lifecycle architecture, privileged access patterns, and zero-trust design. Experience leading cross-functional teams, shaping enterprise identity strategy, and integrating large-scale applications is essential for operating confidently at this level.

Consultant / delivery engineer

An identity delivery engineer turns Entra designs into reliable, scalable, and secure implementations across an organization's environment. They build and configure identity solutions, integrate applications, automate lifecycle and access workflows, and ensure deployments follow architectural standards. Their work bridges strategy and execution, enabling smooth rollouts, stable operations, and continuous improvement of identity services.

What you do: Deliver identity projects across many customers: assessments, designs, migrations, app onboarding, governance rollouts, and post-incident remediation.

- **Entra focus:** Breadth matters. Understand tenant baselines, SSO patterns, migration playbooks, governance quick wins, and operational handover.
- **Adjacent skills employers expect:** Stakeholder management; scoping and estimates; documentation and training; troubleshooting under time pressure.

Early-career entry points: Join as a junior delivery engineer; become the person who can onboard many SaaS apps quickly and consistently.

Experienced pivot angle: Seasoned engineers can translate "battle-tested" migrations and incident lessons into repeatable delivery methods.

- **Portfolio projects:** A sample assessment report outline; an app onboarding factory checklist; a migration cutover runbook.

An identity delivery engineer typically needs mid-level experience implementing and operating Microsoft Entra solutions across cloud and hybrid environments. They should be confident configuring identity services, integrating applications, automating lifecycle workflows, and troubleshooting access issues. Experience translating architectural designs into stable deployments and supporting Zero Trust initiatives is essential for performing effectively in this role.

Identity product manager

An identity product manager defines the vision, strategy, and roadmap for an organization's identity services, ensuring they deliver secure, seamless, and scalable experiences for users and workloads. They translate business needs into identity capabilities, prioritize features, guide engineering teams, and align stakeholders. Their work shapes authentication, access, governance, and platform evolution across the enterprise.

- **What you do:** Shape the strategy, roadmap, and delivery of identity services to ensure secure, seamless, and scalable user and workload access across the organization.
- **Entra focus:** Prioritize and evolve Entra capabilities such as Conditional Access, lifecycle automation, governance, and privileged access to align with enterprise security and Zero Trust goals.
- **Adjacent skills employers expect**: Combine product thinking, security fundamentals, technical fluency, data literacy, and change leadership to guide identity capabilities from concept to adoption.

Early-career entry points: Enter through analyst, support, junior product, or cloud/security rotation roles that expose you to identity workflows and user needs.

- **Experienced pivot angle**: Transition from engineering, architecture, cybersecurity, service ownership, or adjacent product roles seeking broader strategic influence in identity.
- **Portfolio projects**: Demonstrate capability through roadmaps, governance improvements, feature prioritization exercises, metrics dashboards, and rollout communication plans that show real identity impact.

An identity product manager role typically requires mid-to senior-level experience working across identity, security, or cloud platforms, with strong fluency in Microsoft Entra capabilities, product strategy, and stakeholder management. Employers expect a track record

of shaping roadmaps, guiding engineering teams, improving user experience, and delivering measurable security and governance outcomes.

Identity platform owner / technical product owner

An identity platform owner provides strategic and operational leadership for an organization's entire identity ecosystem, ensuring Microsoft Entra services are reliable, secure, and aligned with business goals. They define the platform vision, set architectural and governance standards, prioritize roadmap investments, and oversee end-to-end service health. Their role spans stakeholder alignment, risk management, lifecycle automation, and continuous improvement of identity capabilities. They act as the accountable owner for performance, resilience, compliance, and user experience across all identity services, guiding engineering teams and influencing enterprise-wide security and access strategy.

- **What you do:** Run identity like a product. Own roadmap, standards, adoption, customer (internal) experience, and measurable outcomes.
- **Entra focus:** Platform governance. Focus on policy lifecycle, exception processes, onboarding patterns for apps/teams, and operational metrics.
- **Adjacent skills employers expect:** Product thinking; prioritization; communication; service management; ability to translate risk and compliance needs into backlog items.

Early-career entry points: Start as an operations lead or business analyst within identity/security; own a specific improvement program. For example, MFA adoption to 98%.

- **Experienced pivot angle:** Leads and managers can align identity work to business outcomes (reduced account compromise, faster onboarding, better audit results).
- **Portfolio projects:** Define 6–10 identity KPIs; create a roadmap with themes (hardening, governance, app onboarding, automation).

An identity platform owner role typically requires senior-level experience leading large-scale identity services across cloud and hybrid environments. They need deep expertise in Microsoft Entra architecture, governance, lifecycle automation, and privileged access patterns. Experience driving platform strategy, managing service health, aligning stakeholders, and guiding engineering teams is essential to operate confidently at this level.

Key skills and certifications by career level

Each stage of the IAM career demands a distinct combination of technical skills, certifications, and professional competencies. Understanding these requirements allows professionals to invest their development time strategically.

At the early-career level, the foundational certification is the **SC-900: Microsoft Security, Compliance, and Identity Fundamentals**. This entry-level credential validates

understanding of core identity concepts, authentication methods, and the Microsoft security portfolio. Professionals should also develop proficiency with the Entra admin center, basic PowerShell scripting, ticketing systems, and identity protocols including SAML and OAuth. Soft skills at this stage center on communication, documentation, and systematic troubleshooting.

Mid-career professionals should pursue the **SC-300: Microsoft Identity and Access Administrator Associate**, which validates the ability to design, implement, and operate identity and access management using Microsoft Entra. Complementary certifications include the **SC-100: Cybersecurity Architect Expert** for those moving toward architecture roles. Technical skills at this level expand to include infrastructure-as-code, API integration, identity governance platform administration, and Kusto Query Language for identity analytics.

Senior professionals benefit from the CISSP and CCSP for broad security leadership credibility, combined with deep platform expertise validated by other advanced certifications. The Certified Identity and Access Manager credential from the Identity Management Institute validates expertise in identity governance and access control at the strategic level. At this tier, the most critical skills are architectural thinking, vendor evaluation, regulatory compliance expertise, executive communication, and the ability to translate complex identity concepts into business value.

Career Level	Technical Skills	Recommended Certifications	Soft Skills
Early Career	Microsoft Entra ID administration, Active Directory Domain Services, PowerShell scripting, SAML and OAuth 2.0 fundamentals, MFA configuration, single sign-on concepts, identity lifecycle management	SC-900 Security, Compliance and Identity Fundamentals, CompTIA Security+	Communication, documentation, teamwork, attention to detail

Career Level	Technical Skills	Recommended Certifications	Soft Skills
Mid-Level	Advanced Conditional Access policy design, Privileged Identity Management, Zero Trust architecture implementation, Python/Java/Go automation, IAM-cloud security platform integration	Certified Identity and Access Manager (CIAM), SC-200 Security Operations Analyst, SC-300 Identity and Access Administrator Associate	Project leadership, cross-team collaboration, mentoring, stakeholder management
Senior	Enterprise architecture design, multi-cloud identity strategy, regulatory compliance frameworks, vendor evaluation, organizational change management	CISSP, CCSP, CISM, CIDPRO, and specialized identity governance certifications	Executive communication, strategic planning, organizational leadership, business value translation

Table 18.1: Certifications by career level

Career progression paths in identity management

The identity and access management career does not follow a single linear path. Instead, it branches into several distinct trajectories, each offering compelling opportunities for growth and specialization.

Technical architecture track

The Technical Architecture track progresses from Junior IAM Engineer to IAM Engineer to Senior IAM Engineer and ultimately to Principal Identity Architect. This path rewards deep technical expertise and the ability to design identity solutions that scale across complex, multi-cloud environments.

Operations and platform leadership track

The Operations and Platform Leadership track moves from Identity Support Analyst to Entra Administrator to IAM Operations Manager and into Director of Identity Services. Professionals on this path excel at running identity platforms reliably, managing teams, and ensuring compliance. This track emphasizes operational excellence, incident management, and the ability to maintain identity services at enterprise scale.

Security and strategy track

The Security and Strategy track evolves from Cloud Security Associate to Cloud Security Engineer to IAM Strategy Lead and into CISO or VP of Security. This path suits professionals who view identity as one dimension of a broader security mission and who aspire to shape organizational security strategy at the executive level.

Consulting and advisory track

The Consulting and Advisory track offers a parallel path through firms like Avanade, Deloitte, and Accenture, where professionals advise multiple organizations on identity transformation. Consulting roles often offer accelerated exposure to diverse environments and technologies.

The future of identity-focused careers

The identity profession is not merely growing; it is transforming in ways that will create entirely new categories of work over the coming decade. Three forces are reshaping the landscape, and professionals who position themselves at the intersection of these trends will find themselves in extraordinary demand.

The explosion of non-human identities

The first force is the explosion of non-human identities. AI agents, service principals, workload identities, IoT devices, and automated workflows now outnumber human identities. Microsoft has described this as the expanding identity perimeter, noting that non-human identities are often highly privileged, reducing the need for attackers to escalate their own access.

A specialist who understands how to secure AI agents using Workload Identity Federation, automate the rotation of secrets and certificates, and govern the lifecycle of machine identities is solving problems that keep CISOs awake at night. Recent industry focus on machine identity management signals that this is becoming a mainstream enterprise requirement.

Identity meets AI governance

The second force is the convergence of identity with AI governance. As organizations deploy AI agents that fetch data, make decisions, and interact with systems autonomously, every one of those actions requires an identity and an access decision. The professionals who can design identity architectures for agentic AI workflows, implement consent frameworks for AI-to-AI

interactions, and ensure that machine learning models operate within defined permission boundaries will define the next generation of identity leadership.

Decentralized identity and verifiable credentials

The third force is the maturation of decentralized identity and verifiable credentials. Microsoft Entra Verified ID represents an early implementation of this paradigm, enabling organizations to issue and verify digital credentials based on open standards. As these technologies mature, new roles will emerge around credential ecosystem design, trust framework governance, and privacy-preserving identity verification.

According to Precedence Research, the IAM market's projected growth from $22.99 billion in 2025 to approximately $65.70 billion by 2034 is not merely an expansion of existing roles. It represents the creation of new professional categories that do not yet have standardized titles. The professionals who enter and advance in identity management today are not simply joining a growing field; they are helping to define it.

Your place in the identity revolution

Whether you are a recent graduate exploring your first role in technology, a mid-career professional seeking a specialty with enduring demand, or a seasoned leader looking to shape the strategic direction of your organization, the identity and access management field offers a path that is both intellectually challenging and professionally rewarding.

The skills you develop in Microsoft Entra and the broader IAM ecosystem are not narrow technical competencies that risk becoming obsolete. They are foundational capabilities that grow more valuable as organizations become more digital, more distributed, and more reliant on automated and AI-driven systems. Every application needs authentication. Every user needs authorization. Every AI agent needs governance. And every organization needs professionals who can make these systems work securely, seamlessly, and at scale.

The identity perimeter is expanding, and the professionals who understand how to secure it are building careers that will matter for decades to come. The question is not whether the opportunity exists. The question is whether you are ready to step into it.

Summary

This chapter explored how emerging trends in identity, security, and cloud technology are driving increased demand for Entra skills. Key forces such as Zero Trust adoption, AI-driven governance, workload identity management, and regulatory pressures are highlighted, demonstrating how they create new career pathways for both newcomers and seasoned professionals. The chapter outlined the growing importance of areas like lifecycle automation, privileged access management, and operational excellence. It concluded by recommending

that early-career professionals focus on mastering identity operations, while experienced practitioners should leverage their expertise to lead impactful, measurable programs that enhance security and streamline access.

You've reached the end of Mastering Microsoft Entra ID. This is no small achievement. Identity is a living discipline, and your willingness to learn keeps it evolving. Thank you for investing your time and trust in this work. May your next steps be bold, thoughtful, and grounded in everything you've mastered.

Additional resources

- Identity Management Institute certification overview: `https://identitymanagementinstitute.org/certification/#cams`
- Certified Identity Professional: `https://idpro.org/cidpro/`

Join us on Discord

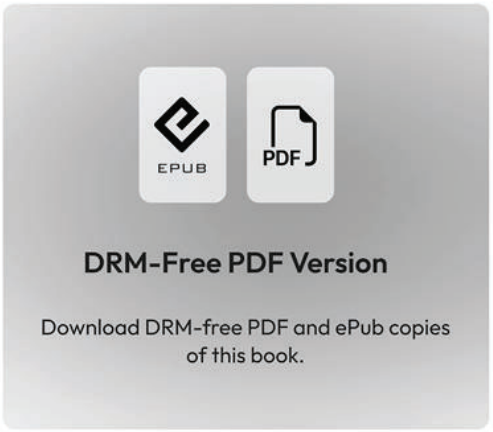
For discussions around the book and to connect with your peers, join us on Discord at `packt.link/discordcloud` or scan the QR code below:

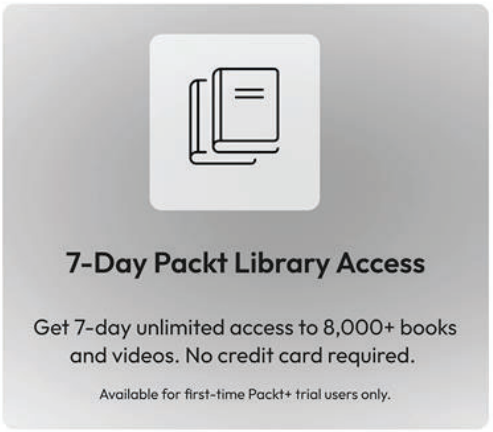


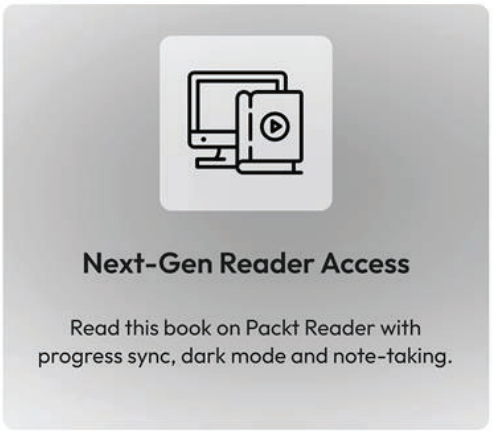
19

Unlock Your Exclusive Benefits

Your copy of this book includes the following exclusive benefits:







Follow the guide below to unlock them. The process takes only a few minutes and needs to be completed once.

Unlock this Book's Free Benefits in three Easy Steps

Step 1

Keep your purchase invoice ready for *Step 3*. If you have a physical copy, scan it using your phone and save it as a PDF, JPG, or PNG.

For more help on finding your invoice, visit `packtpub.com/en-us/unlock?step=1`.

> **Note**
>
> If you bought this book directly from Packt, no invoice is required. After *Step 2*, you can access your exclusive content right away.

Step 2

Scan the QR code or go to `packtpub.com/unlock`.

On the page that opens (similar to *Figure 19.1* on desktop), search for this book by name and select the correct edition.

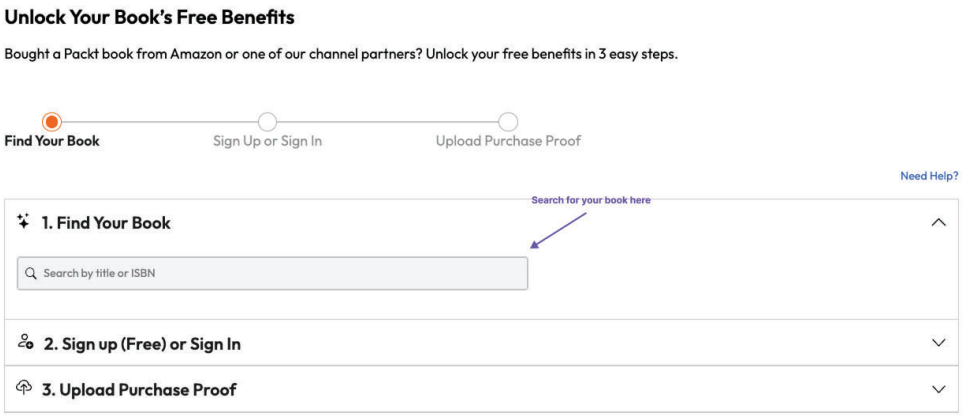


Figure 19.1: Packt unlock landing page on desktop

Step 3

After selecting your book, sign in to your Packt account or create one for free. Then upload your invoice (PDF, PNG, or JPG, up to 10 MB). Follow the on-screen instructions to finish the process.

Need Help

If you get stuck and need help, visit `packtpub.com/unlock-benefits/help` for a detailed FAQ on how to find your invoices and more. This QR code will take you to the help page.

Note

Note: If you are still facing issues, reach out to `customercare@packt.com`.



https://www.packtpub.com

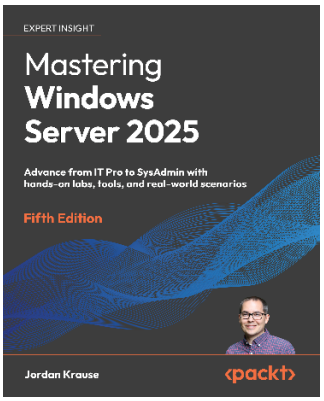
Subscribe to our online digital library for full access to over 7,000 books and videos, as well as industry leading tools to help you plan your personal development and advance your career. For more information, please visit our website.

Why subscribe?

- Spend less time learning and more time coding with practical eBooks and Videos from over 4,000 industry professionals
- Improve your learning with Skill Plans built especially for you
- Get a free eBook or video every month
- Fully searchable for easy access to vital information
- Copy and paste, print, and bookmark content

At https://www.packtpub.com, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on Packt books and eBooks.

Other Books You May Enjoy

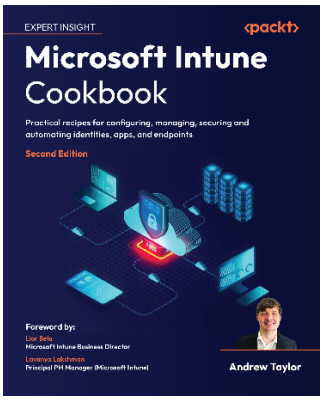


Mastering Windows Server 2025 – Fifth Edition

Jordan Krause

ISBN: 978-1-83702-991-4

- Create an entire lab of new servers and configure multiple roles
- Manage servers using Server Manager, PowerShell, and Windows Admin Center
- Close knowledge gaps in core infrastructure technologies such as Active Directory, DNS, DHCP, and Group Policy
- Virtualize your datacenter with Hyper-V
- Create redundancy through Failover Clustering services
- Deploy Remote Desktop Services
- Design and implement Distributed File System with Replication (DFSR) and Storage Replica
- Don the DevOps cap as you explore containers and Nano Server



Microsoft Intune Cookbook – Second Edition

Andrew Taylor

ISBN: 978-1-80580-723-0

- Set up and configure a Microsoft Intune tenant
- Manage Windows, macOS, iOS, Android, and Linux devices
- Secure endpoints using policies, compliance, and Microsoft Defender
- Deploy and manage applications across platforms
- Automate administration with PowerShell and Microsoft Graph
- Monitor devices using analytics, reporting, and logs
- Apply advanced endpoint capabilities such as Remote Help and EPM
- Use AI-assisted insights to troubleshoot and optimize operations

Packt is searching for authors like you

If you're interested in becoming an author for Packt, please visit `https://authors.packt.com` and apply today. We have worked with thousands of developers and tech professionals, just like you, to help them share their insight with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Share your thoughts

Now you've finished *Mastering Microsoft Entra ID*, *First Edition*, we'd love to hear your thoughts! Scan the QR code below to go straight to the Amazon review page for this book and share your feedback or leave a review on the site that you purchased it from.



https://packt.link/r/1-806-11601-4

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

Index

A

AI Gateway prompt injection protection
configuring 514 – 516
AI governance **611**
Access Control List (ACL) **495**
Active Directory Domain Services (AD DS)
versus Microsoft Entra ID 582
Active Directory (AD) **73, 581**
Active Directory Domain Services (AD DS) **117, 582**
Active Directory Federation Service (AD FS) **95, 553**
Adversary-in-the-Middle (AiTM) **304**
App/Client ID **380**
Apple Push Notification Service (APNS) **51**
Application Administrator **353**
Artificial Intelligence (AI) **149**
Authentication Policy Administrator **353**
Authenticator Attestation GUID (AAGUID) **53**
Azure AI Vision Face API **365**
Azure Active Directory **10**
Azure Front Door (AFD) **471**
Azure Monitor Workbooks **557**
Azure attribute-based access control (Azure ABAC) **285**
Azure resource roles **282**
permissions 282, 283
PIM role, assigning 284 – 286
PIM role, preparing 284
Azure resources
managed identities for 379
Azure roles **270**
access controls **492**
compliant network check 492, 493
source IP restoration 494
Universal Conditional Access 492
access package **190**
access reviews **209**
features 210
for access package 219
guest user reviews 213, 214
licensing requirements 223
multi-stage reviews 211, 212
reporting 222, 223
scenarios 209
workflow 210
access reviews for Microsoft Entra and Azure resource roles **220**
creating 220
reviewing 222
access reviews for access package
creating 219, 220
reviewing 220
access reviews for groups and applications **214**
creating 215 – 217
reviewing 218
administrative units **97**
administrative roles, assigning 103 – 106
creating 99
members, adding 100, 101
members, adding dynamically 101, 102
restricted management administrative units 97 – 99
alerts **291**
Azure roles 293
Microsoft Entra roles 291 – 293

app provisioning **81**
app registration **383**
application discovery **529 – 531**
application object **380, 381**
application usage analytics **539**
assigning roles
PIM, using 34
role-assignable groups, creating 30, 31
role-assignable groups, using 30
to groups 31 – 34
to users 30 – 34
attribute-based filtering **89**
audit logs **548, 549**
authentication and authorization standards, IAM
JSON Web Tokens (JWTs) 8
OAuth (Open Authorization) 7
OpenID Connect (OIDC) 8
Security Assertion Markup Language (SAML) 8
System for Cross-Domain Identity Management (SCIM) 8, 9
authentication methods **45, 89**
federated authentication 95
Microsoft Authenticator, in Push mode 57 – 62
OATH hardware token 62, 63
OATH software token 62
pass-through authentication 93
password hash sync 90, 91
passwordless authentication 49
QR code 64, 65
selecting 96
Temporary Access Pass (TAP) 45 – 49

B

B2B direct connect **428, 429**
B2B users
governance 429
Microsoft Entra ID Protection, using 430
Business-to-Business (B2B) **19, 397 – 399**
Business-to-Consumer (B2C) **19, 399**
branding themes
configuring 467, 468
break glass accounts **265**
bring-your-own-device (BYOD) **521**

C

Certificate Authority (CA) **57**
Certificate Revocation List (CRL) **57**
Certificate Signing Request (CSR) **505**
Cloud Authentication Provider (CloudAP) **50**
Conditional Access optimization agent **169**
limitations 171
onboarding 171
policy suggestions 169, 170
prerequisites 170
settings, adjusting 172 – 177
Conditional Access policy **66 – 68**
applying 527
for workload identities 387 – 390
Conditional Access policy evaluation **326**
Consulting and Advisory track **611**
Consumer Identity and Access Management (CIAM) **397, 435**
Continuous Access Evaluation (CAE) **325**
client capabilities 326
Conditional Access policy evaluation 326
critical event evaluation 325, 326
for workload identities 391
scenarios 325
Customer Identity and Access Management (CIAM) **18**

catalog **190**

certificate-based authentication (CBA) **51, 56, 57**

claim challenge **326**

client capabilities **326**

cloud access security brokers (CASB) **485**

cloud firewall
- configuring 510 – 512

cloud transformation **586**
- Active Directory environment, assessing 588
- application migration 589
- authentication, migrating 589
- conditional access policy 590, 591
- device migration and management 591, 592
- identity synchronization 589
- prerequisites and planning 587
- security considerations 592

cloud transformation, Active Directory environment
- dependency mapping 588
- inventory and discovery 588

cloud transformation, application migration
- application discovery and classification 590
- application type approach 590

cloud transformation, prerequisites and planning
- license requisites 588
- organizational readiness 587
- technical prerequisites 587

cloud transformation, security considerations
- identity protection 593
- Privileged Identity Management 593
- Zero Trust alignment 592, 593

cloud-only identity model **78**
- groups, creating 80
- users, creating 79

compliant network check **492, 493**

connected organization **191**
- adding 191 – 193

critical event evaluation **325, 326**

cross-tenant access settings **413**
- B2B direct connect 428, 429
- default settings 413, 414
- Microsoft cloud settings 423 – 428
- organization-specific settings 417, 418
- redemption order 415, 416
- tenant restrictions 419 – 423
- trust settings 415

custom URL domains
- adding 470 – 475

custom authentication extensions **475, 476**

custom credentials **357**
- issuing 357 – 360
- issuing app, creating 360, 361

custom task extension **254 – 256**

customer premises equipment (CPE) **489, 541**

D

Data Loss Prevention (DLP) **512**

Decentralized Identity Foundation (DIF) **344**

Decentralized Public Key Infrastructure (DPKI) **346**

Discovery and insights **295 – 297**

Domain Administrator **82**

Domain Controllers (DCs) **118**

Domain Services
- Kerberos Constrained Delegation (KCD), configuring 142, 143
- managed domain, securing 141, 142
- securing 141
- security audit events, enabling 144 – 146

data
- retention 154
- storage locations 154

decentralized identities (DIDs) **342, 343**

decentralized identity and verifiable credentials **612**

diagnostic settings **551, 552**

digital identity **4**
direct role assignment
versus Microsoft Entra Privileged Identity Management 268
directory provisioning **81**
domain-based filtering **89**

E

Enterprise Administrator **82**
Entra External ID
applications, registering 455
enterprise application, adding 458
migrating 480
monitoring 481
OIDC application, registering 455, 456
SAML application, registering 457
Entra knowledge **600**
External Health Monitoring **164**
External Multifactor Authentication (external MFA) **42**
end user self-service **107**
self-service application assignment 111, 112
self-service group management 109, 110
self-service password reset (SSPR) 107 – 109
entitlement management **189**
access package 190
access package manually, assigning 206, 207
access package, creating 199 – 203
access request 204
access, approving 205
additional roles, adding 196
catalog 190
catalog, creating 196
connected organization 191
delegating, to catalog creator 195
licensing requirements 194
Microsoft Entra portal access 195
resource attributes, adding to catalog 198, 199
resources, adding to catalog 197
roles 193
users, auto-assigning to access package 208
validating 206
external collaboration settings **410 – 412**
external tenants **19, 436**
creating 437, 438
securing 478, 479
versus workforce tenant 400

F

Fast Identity Online (FIDO) **53**
Firebase Cloud Messaging (FCM) **51**
Fully Qualified Domain Names (FQDNs) **21, 492, 523**
federated authentication **95**
federated identity credentials (FIC) **383 – 386**
forest trust
creating 134
prerequisites 134
fundamental security settings **113**
access control 113
application management 113
credential management 113
external collaboration 114
free security features 114
monitoring 114
privileged access 113

G

Global Administrator **239**
Global Secure Access (GSA) **20, 167, 485, 486, 522**
access controls 492
administrator 487
app, creating 528
client 488
licensing 22

Microsoft Entra Internet Access 21
Microsoft Entra Internet Access, for Microsoft Services 22
Microsoft Entra Private Access 22
overview 486, 487
remote networks 488 – 490
traffic forwarding profiles 490 – 492

Global Secure Access Administrator 536

Globally Unique Identifier (GUID) 359

Group Managed Service Accounts (gMSAs) 82

Group Policy Objects (GPOs) 582

get started guide
using 440 – 442

greenfield approach 586
characteristics 586

group-based filtering 88

guest user reviews 213, 214

guests 19

H

HR-driven provisioning 81

Human Capital Management (HCM) 14

Human Resource Management System (HRMS) 229

Hybrid Identity Administrator 82

human identities 380

hybrid coexistence 585
characteristics 585

hybrid identity model 80
Microsoft Entra Cloud Sync 81
Microsoft Entra Connect Sync 84, 85

I

Identity Governance (IG) 185

Identity Secure Score 555

Identity and Access Management (IAM) 3, 6, 7

Identity provider (IdP) 5, 378, 409

Internet Access profile 495

Internet Protocol Security (IPSec) 489

identity 4

identity and access management (IAM)
authentication and authorization standards 7
functionality 6

identity and access management career 610
AI governance 611
Consulting and Advisory track 611
decentralized identity and verifiable credentials 612
Operations and Platform Leadership track 611
Security and Strategy track 611
Technical Architecture track 610

identity establishment
accountability 5
authentication 4
authorization 5
identification 4
Identity provider (IdP) 5

identity model
determining 73

identity protection 593

identity providers
configuring 445
custom OIDC identity provider 450, 451
custom SAML/WS-Fed 452 – 454
email and OTP 446
email and password 445
social identities 448
username or alias 446, 447

identity providers (IdPs) 35

identity revolution 612

intelligent local access 531

J

JSON Web Tokens (JWTs) **8**

Just-in-time (JIT) **572, 593**

job roles for identity professionals **601**
- access governance analyst 604
- consultant/delivery engineer 606
- identity administrator/ identity operations 601
- identity architect/cloud security architect 605
- identity engineer 601, 602
- identity governance specialist 603, 604
- identity product manager 607
- identity product owner/ technical product owner 608
- privileged access engineer 605
- security engineer 602, 603
- skills and certifications 608 – 610

joiner-mover-leaver scenario **14**

just-enough-access (JEA) **593**

K

Kerberos Constrained Delegation (KCD) **142**
- configuring 142, 143

Kerberos SSO **533, 534**

Kerberos authentication. Microsoft Entra Domain Services **117**

Key Performance Indicators (KPIs) **257**

Kusto Query Language (KQL) **322**

L

LCW, Zero Trust security model **230, 231**
- joiner phase 231
- leaver phase 232
- mover phase 231, 232

Large Language Model (LLM) **514**

Lifecycle Workflows (LCW) **228**

Lifecycle Workflows Administrator **239**
- licensing requirements 239
- limits 239
- role requirements 239

Lightweight Directory Access Protocol (LDAP) **12, 117**

least privilege principle **188**
- concepts 189

lifecycle workflows components **233**
- scope 238
- tasks 233, 234
- triggers 235 – 238

lift-and-shift migration **586**
- characteristics 586

logs and monitoring **540**
- alerts 542
- audit logs 541
- deployment logs 541
- GSA dashboard 540
- remote network health logs 541
- traffic logs 540

M

MFA registration policy **319, 320**

MITRE ATT&CK
- reference link 309

Microsoft Authentication Library (MSAL) **9, 479**

Microsoft Authenticator **51, 52**
- in Push mode 57 – 62

Microsoft Defender for Cloud App **21**

Microsoft Entra **3, 10, 270**
- applications 377 – 379
- roles 385
- Security Copilot agents 167, 168

Microsoft Entra Agent ID **177 – 180**

Microsoft Entra Application Proxy **35**

Microsoft Entra Backup and Recovery **565**
- difference report 566 – 568

prerequisites 565
recovery 569
starting 565, 566

Microsoft Entra Cloud Sync **81**
deployment scenarios 81
installation, prerequisites 82
installation, verifying 84
installing 82, 83
key components 82

Microsoft Entra Connect Health **89**

Microsoft Entra Connect Sync **84, 85**
installation requisites 85, 86
installation steps 88
Microsoft Entra Connect Health 89
object filtering 88

Microsoft Entra Connect Sync, installation requisites
connect server requirements 86
SQL server requirements 87

Microsoft Entra Domain Services **12, 118, 119**
basic concepts 121
managed domain 120
pricing 12, 13

Microsoft Entra Domain Services, basic concepts
domain management 122
forests and trusts 121, 122
licensing 124, 125
password policy 124
replica sets 121
synchronization 122
user account creation 124

Microsoft Entra External ID **18, 19, 398 – 401**
best practices 431
Business-to-Business (B2B) 399
Business-to-Consumer (B2C) 399
external tenants 400
guest user, inviting 404 – 408
in workforce tenant 402, 403
organization process 430, 431
pricing 20, 432
workforce tenant 399

Microsoft Entra ID **10**
license types 11
licensing 11
versus Active Directory Domain Services (AD DS) 582

Microsoft Entra ID Account Recovery **369 – 371**

Microsoft Entra ID Governance **13, 186 – 188**
identity and access lifecycle 14
licensing 15
privileged access lifecycle 15
use cases 187

Microsoft Entra ID Protection **303 – 305**
dashboard 307 – 309
license requisites 306
role requisites 305, 306

Microsoft Entra ID credentials
revoking 371 – 373

Microsoft Entra ID tenant
setting up 74 – 78

Microsoft Entra Identity Protection **16**
licensing 16

Microsoft Entra Internet Access **20, 21, 485, 494**
AI Gateway prompt injection protection, configuring 514 – 516
cloud firewall, configuring 510 – 512
for Microsoft Services 517
Internet Access profile 495
license 518
network content filtering 512 – 514
prerequisites 499
Secure Web and AI Gateway for Microsoft Copilot Studio agents, configuring 516
security profiles 496 – 498
traffic profile 517, 518
Transport Layer Security (TLS) inspection, configuring 505 – 507
web content filtering, configuring 499 – 504

Microsoft Entra Lifecycle Workflows **228 – 230, 239**

attribute synchronization 240
creating 240 – 243
email customization 249 – 251
history reports 252
inactive users, managing 252 – 254
inbound provisioning 240
managing 245
prerequisites 240
properties, managing 245 – 247
reprocessing 251
running 243
scheduling 244
versioning 247, 248

Microsoft Entra Private Access **20, 485, 522**
application discovery 529, 530
Conditional Access policy, applying 527
intelligent local access 531
Kerberos SSO 533, 534
license 542
per-app access architecture 528
private apps access, securing with Privileged Identity Management (PIM) 532, 533
Quick Access architecture 523
Quick Access architecture, configuring 526, 527
source IP anchoring 535, 536

Microsoft Entra Privileged Identity Management **189, 263**
emergency access accounts 265, 266
licensing requisites 267
role assignment overview 266, 267
role requisites 264
terminology 264, 265
versus direct role assignment 268

Microsoft Entra Verified ID **16, 345 – 347**
advanced setup, using 353
credentials, verifying 361
custom credentials 357
end user experience 351, 352
license 347
licensing 17
quick setup, using 347 – 350

Microsoft Entra Verified ID, advanced setup
application, registering 355
DID, registering 356
domain ownership, verifying 356
key vault, creating 353
settings 354

Microsoft Entra Verified ID, credentials
Verified ID, setting up 361
verifier app, creating 362

Microsoft Entra Workload ID **17**
best practices 391, 392
licensing 18, 392
using 382, 383

Microsoft Entra activity logs **548**
audit logs 548, 549
diagnostic settings 551, 552
provisioning logs 551
sign-in logs 549, 550

Microsoft Entra admin center **11**

Microsoft Entra recommendations **555 – 557**

Microsoft Entra roles **26, 271**
assigning roles 29
assignments, approving 281
assignments, extending 281, 282
built-in roles 27, 28
custom roles 28, 29
PIM role, activating 279, 280
PIM role, assigning 275
PIM role, preparing 271 – 274

Microsoft Entra threat landscape **558**
advanced protection mechanisms 561
built-in security features 560
continuous monitoring and improvement 562
scenarios 561
security incidents 562
threat protection 560
threat types 559

Microsoft Entra workbooks **557, 558**

Microsoft Security Copilot **149 – 151**
authentication 157, 158
experiences 151
prerequisites 155
privacy and data security 153, 154
provisioning capacity 155 – 157
working with 154
Microsoft Security Copilot, experiences
embedded experience 152
standalone experience 152
Microsoft Security Store **347**
Microsoft Sentinel **305**
Microsoft cloud settings **423 – 428**
Microsoft identity platform **9**
components 9
Mobile Device Management (MDM) **51**
Monthly Active Users (MAU) **20, 432, 436**
Multi-Protocol Label Switching (MPLS) **489**
managed domain **119**
administering 136
administrator VM, creating 136
applications, enabling 128
creating 125 – 127
DNS, managing 138
forest trust, creating 134, 135
GPOs, administering 138
health status, checking 139 – 141
OU, creating 137
replica set, creating 132, 133
user accounts, enabling for Domain Services 128
virtual network, configuring 129
managed identities
for Azure resources 379
types 379
members **19**
mesh architecture **575**
best practices, implementing 577
core principles 575
identity management integration 576
security and compliance 577
technical integration points 576
use cases 578
migration **582**
migration strategy **585**
greenfield approach 586
hybrid coexistence 585
lift-and-shift migration 586
phased migration 585
multi-factor authentication (MFA) **4, 38, 303**
external MFA provider, configuring 42
rollout, configuring 43, 44
system-preferred MFA, configuring 41
multi-geo capability **525**
multi-stage reviews **211**
options 211
use cases 211
mutual Transport Layer Security (mTLS) **491**

N

NT LAN Managed (NTLM) **120**
NT LAN Manager (NTLM) v1/v2 **537**
Native authentication **479**
network content filtering **512 – 514**
neutral branding
customizing 462 – 467
non-human identities **380**
nonrepudiation **5**
notifications
configuring 328
email alert 328, 329
weekly email 330

O

OATH hardware token **62, 63**
OATH software token **62**
Open Authorization (OAuth) **8**
OpenID Connect (OIDC) **8, 436**
Operations and Platform Leadership track **611**

Organizational Units (OUs) **123**

object filtering
- attribute-based filtering 89
- domain-based filtering 89
- group-based filtering 88
- organizational Unit (OU)-based filtering 89

on-premises decommissioning **593**
- domain controllers 595
- domain, cleaning up 595
- Entra ID authoritative source, validating 594
- hybrid identity components, removing 595
- no service domain controllers 594

one-time passcode (OTP) **407, 479**

optional claims
- configuring 469

organization-specific settings **417, 418**
- automatic redemption 418, 419
- cross-tenant sync 419

organizational Unit (OU)-based filtering **89**

overage capacity **155**

P

PIM deployment
- Azure roles 270
- groups 270, 271
- Microsoft Entra 270
- planning 269

PIM role, to Microsoft Entra
- assigning 275
- assigning, with administrative unit scope 277 – 279
- assigning, with app registration scope 276
- assigning, with tenant scope 275

Passkey (FIDO2) **51**

PingFederate **95**

Platform Credential for macOS **51**

Platform SSO on macOS
- with SmartCard 51

Primary Refresh Token (PRT) **50**

Private Access for Domain Controllers **536**
- break glass mode 539
- Conditional Access policy, creating 538
- enterprise application, creating 537
- inclusions and exclusions 538
- prerequisites 536, 537
- Private Access Sensor, installing 537, 538

Privileged Identity Management (PIM) **15, 166, 261, 532, 572, 593**
- Azure resource roles 282
- best practices 297, 298
- configuring 532
- eligibility, assigning 290, 291
- features 263
- groups 287 – 289
- groups, preparing 289
- Microsoft Entra roles 271
- prerequisites 532
- using 271

Public Key Infrastructure (PKI) **57, 505**

pass-through authentication **93**
- benefits 93
- configuration prerequisites 94
- enabling 94
- testing 95

passkey (FIDO2) authentication **53**
- enabling 53, 54
- registering 55
- signing in 55

password hash sync **90, 91**
- advantages 90
- considerations 91, 92
- selective password hash synchronization 92
- setting up 92, 93

passwordless authentication **49**

certificate-based authentication (CBA) 56, 57
Microsoft Authenticator 51, 52
passkey (FIDO2) authentication 53
Platform Credential for macOS 51
Platform SSO on macOS, with SmartCard 51
Windows Hello for Business 49, 50

per-app access architecture **528**
Global Secure Access (GSA) app, creating 528

phased migration **585**
characteristics 585

points of presence (PoP) **486**

private apps access
securing, with Privileged Identity Management (PIM) 532, 533

private network connector group
connector, installing 524 – 526
creating 523, 524
prerequisites 524

privileged identities **262**

protected actions **68 – 70**

provisioned capacity **155**

provisioning **80**
app provisioning 81
directory provisioning 81
HR-driven provisioning 81

provisioning logs **551**

Q

QR code **64, 65**

Quick Access **22**

Quick Access architecture **523**
configuring 526, 527
private network connector group, creating 523, 524

R

Representational State Transfer (REST) **8**

Resource audit **294**

Risk-based Conditional Access (RBCA) **316**

Risk-based Conditional Access policy **305, 316**
impact analysis workbook 321 – 324
MFA registration policy 319, 320
prerequisites 317
Sign-in risk policy 317, 318
test risk policy 320, 321
user risk policy 318, 319

recoverability **562**
Microsoft Entra Backup and Recovery 565
soft deletion 563, 564

recovery
from backup 569 – 571
from difference report 569

replica set
creating 132, 133

restricted management administrative units **97 – 99**

risk assessment feedback **337**

risk data
exporting 336

risk detections **309, 335**
anonymous IP address 335
atypical travel 336
by Microsoft Entra ID Protection 312 – 315
detection types 311
leaked credentials for workload identities 336
risk levels 310
risk types 310
unfamiliar sign-in properties 335

risk levels **310**

risk types **310**

risks
detection report 334, 335
investigating 330
sign-ins report 333
user report 331, 332
workload identity 334

role-based access control (RBAC) **26, 487**

S

Secure Service Edge (SSE) **20, 485, 486**

Secure Web Gateway (SWG) **21, 494**

Secure Web and AI Gateway for Microsoft Copilot Studio agents
- configuring 516, 517

Security Assertion Markup Language (SAML) **8, 436**

Security Compute Units (SCUs) **155**

Security Copilot agents
- in Microsoft Entra 167, 168

Security Copilot, in Microsoft Entra **158**
- Access Reviews 165
- application risk 164, 165
- authentication methods 162
- Conditional Access 161, 162
- devices 161
- Domain Services support 161
- Entitlement Management 165
- Global Secure Access (GSA) 167
- group management 160
- health monitoring alerts 164
- license usage 167
- Lifecycle Workflows 166
- Privileged Identity Management (PIM) 166
- risky users 164
- roles and administrators 161
- Service Level Agreement (SLA) 164
- sign-in logs 162
- tenants 160
- users 160

Security Information and Event Management (SIEM) **16**

Security and Strategy track **611**

Security info
- reference link 64

Server Name Indication (SNI) **500**

Service Level Agreement (SLA) **164**

Service Principal Name (SPN) **82, 537**

Sign-in risk policy **317, 318**

Single Sign-On (SSO) **5, 35, 479, 533**
- administrative roles 36
- certificates 36
- communication 36
- deployment options 37
- licenses 36
- shared accounts 36, 37

Software Development Kits (SDKs) **10**

Software-as-a-Service (SaaS) **9, 458**

System for Cross-Domain Identity Management (SCIM) **8**

secure web gateways (SWG) **485**

security audit events
- enabling 144 – 146

security profiles **496 – 498**

selective password hash synchronization **92**

self-managed domain **118**

self-service application assignment **111, 112**

self-service group management **109, 110**

self-service password reset (SSPR) **38, 107 – 109, 317 – 319, 322**
- email 107
- enabling 477
- mobile application code 107
- mobile application notification 107
- mobile phone 107
- office phone 107
- prompts and session, configuring 39, 40
- security questions 107

self-sovereign identity (SSI) **342**

service principal object **381, 382**

sign-in logs **549, 550**

single sign-on (SSO)

prerequisites 534
source IP anchoring 535, 536
source IP restoration 494
synchronization 80
system-preferred MFA 41

T

Technical Architecture track 610
Temporary Access Pass (TAP) 45 – 49
Ticket Granting Ticket (TGT) 534
Transmission Control Protocol (TCP) 495
Transport Layer Security (TLS) 499, 505
inspection, configuring 505 – 507
Trusted Platform Module (TPM) 50
tenant 19
tenant restrictions 419 – 423
protection types 420
test risk policy 320, 321
threat intelligence
configuring 508, 509
time to live (TTL) 78
time-based one-time passcodes (TOTP) 62
tokens
customizing 468
transformation state 583
Active Directory 584
cloud-attached 584
cloud-first 584
cloud-only 584
hybrid 584

U

Uniform Resource Locator (URL) 499
Universal Conditional Access 492
Universal Tenant Restrictions 22
User Principal Names (UPNs) 538
User risk policy 318, 319
usage and insights reports 552 – 554
user flow
creating 459 – 461
user profile attributes 442 – 445
user-assigned managed identity 383

V

Verified ID Face Check 363
enabling 363 – 365
licensing 365
Verified ID service
opting out 374
Verified ID with Microsoft Entra entitlement management 365 – 369
licensing 369
Virtual Machines (VMs) 118
Virtual Private Network (VPN) 22, 120, 488, 521
verifiable credentials 343 – 345
virtual network
configuring, for managed domain 129
subnet, in Azure virtual network 130 – 132
subnet, in managed domain 129, 130

W

W3C Credentials Community Group 345
Web Services Federation (WS-Fed) 9
Wide Area Network (WAN) 488
Windows Hello for Business 49, 50
benefits 50
Windows Hello for Business (WHfB) 534
World Wide Web Consortium (W3C) 343
web content filtering
configuring 499 – 504

workflow insights **257**
workforce **19**
workforce tenant
versus external tenants 400
workload identities **17, 380**
application object 380
Conditional Access policy 387 – 390
Continuous Access Evaluation (CAE) for securing 391
386, 387
service principal object 381 – 383
types 380
workload identity **326**
securing 326 – 328
workload identity federation **383, 384**
federated identity credentials, configuring 385, 386

Z

Zero Trust **571**
automated threat detection and response 573
best practices 575
conditional access 572
continuous monitoring 573
device compliance and health integration 573
least privilege and role-based access control 572
Microsoft security solutions, integrating 574
multi-factor authentication 572
real-time analytics and threat intelligence 573
risk-based access 573
scenarios 574
security perimeter 572
Zero Trust alignment **592, 593**
principles 592
zero trust network access (ZTNA) **485, 530**