Mastering Microsoft 365 Security Technologies

Design and implement Microsoft security, compliance, and identity

Pramiti Bhatnagar

www.bpbonline.com

First Edition 2025

ISBN: 978-93-65892-871

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true and correct to the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but the publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

www.bpbonline.com

Dedicated to

*My little twins **Aadi** and **Shiv***
and
My parents

About the Author

Pramiti Bhatnagar is a seasoned professional with over twenty years of deep technical experience in Microsoft technologies, including Microsoft Entra, Microsoft Purview, Microsoft Defender, Microsoft 365 Windows, and Microsoft Endpoint Manager. Pramiti holds an honours degree in applied psychology from the University of Delhi and has numerous technical certifications, such as Certified Information Privacy Manager, Microsoft Certified: Cybersecurity Architect Expert, and Project Management Professional (PMP).

Currently, Pramiti serves as a Principal Product Manager for Microsoft Entra, primarily focusing on Copilot for Security and Entra External Identities. Pramiti has also held various roles at Microsoft, including Global Black Belt, Cloud Solution Architect, and Partner Technology Strategist.

About the Reviewers

- **Mahesh Kohli** is a product manager at Microsoft, holding CISM certification and Microsoft Certified Trainer credentials, with over 18 years of experience in the IT industry. He is currently focused on enhancing Microsoft Defender solutions, managing roadmaps, overseeing customer expectations, conducting market research, and providing strategic advice to security leadership to help customers strengthen their overall security posture.

  Additionally, Mahesh specializes in delivering security-focused training sessions and webinars for both internal and external stakeholders. Before transitioning to a product management role, he served as a Premier Field Engineer, managing security and compliance solutions. In this role, he acted as a trusted advisor, conducting security assessments, health assessments, and workshops, while assisting customers with implementing security controls based on best practices. Outside of his professional role, Mahesh is an avid reader with a passion for classic novels, non-fiction and IT-related books.

- **Taresh Mehra** is a data protection and cyber security QA Engineer with over 18 years of experience in Edison, New Jersey. He specializes in backup and storage solutions, ransomware mitigation, and data indexing, ensuring data integrity in modern IT environments. His expertise spans AI/ML applications in data security, REST API testing, and cloud technologies.

  Taresh has also shaped industry standards through his leadership in the Cloud Security Alliance and extensive contributions as a cyber security publication reviewer. His work advancing the field through IEEE conference papers and technical evaluations at major hackathons earned him the prestigious 2024 SILVER GLOBEE® AWARD for Cyber Security Professional of the Year. As both an IEEE Senior Member and RSA Fellow, he continues to influence the direction of enterprise security, helping define best practices and innovation benchmarks across the industry.

Acknowledgement

I would like to express my sincere gratitude to all those who contributed to the completion of this book.

First and foremost, I want to extend my heartfelt thanks to my family who have offered their unwavering support during the development of this book.

I also want to thank my colleagues, managers and mentors at Microsoft who have provided me with numerous opportunities to learn and grow and become capable of writing a book.

I am immensely grateful to BPB Publications for offering me the opportunity to share my knowledge. Their guidance and expertise in bringing this book to fruition has been incredible. Their support and assistance were invaluable in navigating the complexities of the publishing process.

I would also like to acknowledge the reviewers, technical experts, and editors who provided valuable feedback and contributed to the refinement of this book. Their insights and suggestions have significantly enhanced the quality of the book.

Finally, I want to express my gratitude to the readers who have shown interest in this book. Your support and encouragement have been deeply appreciated.

Thank you to everyone who has played a part in making this book a reality.

Preface

Security is top of mind for most organizations today. With the increasing number of cyber-attacks and shortage of skilled professionals, organizations are struggling to protect themselves from bad actors. At the same time, data is exploding making it even tougher for organizations to keep themselves and their data safe. M365 Security technologies provide end-to-end solutions for protecting and organisation's data, identities and applications.

This book covers end-to-end Microsoft security solutions. Section 1 of this book focuses on Microsoft's identity and access management solution Microsoft Entra. The five chapters in this section introduce Microsoft Entra and then guide the reader through implementation of Microsoft Entra and managing, protecting and governing identities using Microsoft Entra ID Governance, Microsoft Entra Privileged Identity Management. It also introduces the reader to Microsoft Entra Secure Services Edge, Microsoft's Zero Trust network access solution.

Section 2 focuses on protecting the organization against threats. It introduces Microsoft Defender XDR as Microsoft's extended detection and response solution. The chapters in this section shed light on how Microsoft Defender solutions can help protect devices, identities, M365 and non-M365 applications from external threats.

Section 3 shifts the focus on protecting data. This section explains how organizations can protect structured and unstructured data in Microsoft 365 and multi-cloud environments using Microsoft Purview Information Protection, prevent accidental or intentional data exfiltration using Microsoft Purview Data Loss Prevention, identify insider risks and manage regulatory compliance and privacy.

This book is designed to help experienced and novice security professionals become experts in administering and implementing Microsoft security solutions. Through practical examples, comprehensive explanations, hand-on labs, and a structured approach, this book aims to equip readers with a solid understanding of Microsoft security solutions. Whether you are a novice or an experienced learner, this book will serve as a valuable resource as you work towards advancing your cybersecurity career.

Chapter 1: Introduction to Microsoft Entra- This chapter introduces the Microsoft Entra product family. Microsoft Entra is a family of products that help organisations create and manage users and govern user access to applications and services. This chapter introduces the components of the Microsoft Entra and how they can help organisations address their identity and access management requirements. It touches on the licensing options for each capability. This chapter explains how to create users using Microsoft Entra, the external collaboration capabilities using Microsoft Entra External ID. It also introduces new capabilities like Microsoft Entra Permissions Management, Microsoft Entra Verified ID and Global Secure Access.

Chapter 2: Implementing Identity- Many organizations worldwide use on-premises Active Directory for managing their identities. When they decide to move to the cloud, they would want to provide their end users with seamless access to both cloud and on-premises applications and resources. This chapter describes how these organizations can sync their on-premises Active Directory identities to Microsoft Entra ID securely so that users can use the same credentials to access both on-premises and cloud resources. It goes on to explain the password synchronization methods like password hash sync and pass-through authentication. It explains the password protection capabilities available in Microsoft Entra ID and how these can be extended to on-premises Active Directory. It also talks about setting up single sign-on for applications and end user self-service in Microsoft Entra ID.

Chapter 3: Identity Management- One of the main tasks of an identity and access management administrator is to make sure that the right system resources are accessible to the right users. This can be a challenging task since there are thousands of user identities in any organisation. This chapter introduces the group management features in Microsoft Entra ID to handle these identities and protect your organisation's resources effectively. It also covers the key concept of role based access control, which aids in understanding the other Microsoft capabilities explained in this book.

Chapter 4: Identity Protection- Identity is the key to access. Hence, a secure cloud deployment relies on a secure identity. Identity attacks have increased dramatically in recent years. Organisations need to enforce rigorous identity protection strategies while also offering a smooth work experience to their end users. This chapter describes the different identity protection features in Microsoft Entra ID like multifactor authentication, passwordless sign-in, unphishable credentials like passkeys. It also explains how Microsoft Entra ID Protection feature like risk-based conditional access policies can help prevent identity-based attacks.

Chapter 5: Identity Governance- Each identity goes through a lifecycle that needs to be managed from when a user joins the organisation to when they leave. The user access must be kept up to date across the joiner-mover-leaver scenario and this must be done efficiently. This chapter shows how to use entitlement management to give the users the right access that they need to do their job. Access reviews can be used to check the user's access to data and applications regularly, making sure that they do not have more access than necessary to fulfil their job roles. Lastly, it explores how Privilege Identity Management can be used to give just in-time access to the users that have the most sensitive access.

Chapter 6: Microsoft Defender XDR- Organizations these days are exposed to a myriad of threats ranging from viruses, malware, phishing attacks, ransomware and more. They need to have effective threat protection strategies which include a combination of proactive prevention, real-time detection and rapid response. They need to deploy security solutions like firewalls, antivirus software, intrusion detection and protection systems to protect their networks, devices and data from potential harm. Microsoft Defender XDR is a suite of solutions that helps with detection, prevention, investigation and response of threats across endpoints, identities, email and applications. It provides integrated protection against sophisticated cyber-attacks.

Chapter 7: Protecting Identities- Many organizations still have big on-premises Active Directory infrastructures that can be compromised by attackers. Organizations must have tools to identify attacks against these identities and protect them from being stolen or abused. This chapter explores how Microsoft Defender for Identity helps organizations avoid breaches by spotting threats, investigating and responding to incidents. Microsoft Defender for Identity is a cloud-based solution that helps your SecOps teams provide a modern identity and threat detection solution across hybrid environments. It helps stop breaches, identify threats, examine dubious activities and react to attacks.

Chapter 8: Protecting Endpoints- In today's hybrid working environment, users are using a multitude of devices from a multitude of locations. Gone are the days when users used to work only from their offices safe behind the corporate firewall. This exposes user endpoints to threats like never before. The attackers are also becoming very sophisticated. Organizations need modern and intelligent tools to protect their users' devices from bad actors. Microsoft Defender from Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats. Coupled with Microsoft Defender Vulnerability Management, it offers proactive protection and visibility into the vulnerabilities in the environment and provides recommendations to strengthen the security posture. Organizations today also use operational technology and Internet of Things devices. It is important for an organization to gain visibility into these devices and the threats surrounding them. Microsoft Defender for IoT provides device discovery and threat protection services for OT and IoT networks across cloud, on-premises and air-gapped infrastructure.

Chapter 9: Protecting M365 Apps- Many organisations are now shifting to cloud-based services. Microsoft is the world's top collaboration SaaS provider. Most organisations store a lot of data in the M365 cloud, Exchange Online, SharePoint Online, OneDrive for Business and Teams. Attackers try to compromise these applications using different methods like phishing and spoofing. This chapter explains Exchange Online Protection and Microsoft Defender for Office 365 and their roles in defending, detecting, investigating and responding to attacks aimed at your M365 environment.

Chapter 10: Protecting Non-Microsoft Cloud Apps- Today, end users have access to a wide variety of SaaS applications that help them work more efficiently. However, this poses a major challenge for Security Administrators as they might not have visibility of which applications are in use, their security posture and how they are being used. These applications introduce new threat vectors for an organization in terms of cyber-attacks and more avenues for data exfiltration. This chapter explores Microsoft Defender for Cloud Apps and how it can help identify the use of Shadow IT, approve and disapprove applications and ultimately track the usage of those applications to protect your organisation's data and assets.

Chapter 11: Security Management Using Microsoft Sentinel- This chapter introduces the concepts of **Security Incident and Event Monitoring** (**SIEM**) and **Security Orchestration Automation and Response** (**SOAR**). It then goes on to introduce Microsoft Sentinel as Microsoft's cloud-native SIEM and SOAR solution. It explains how Microsoft Sentinel helps SOC analysts manage hundreds of alerts daily, preventing critical security incidents. The chapter covers the setup of Microsoft Sentinel, connecting data sources, handling incidents, creating playbooks, and automating responses. It also highlights the integration with Microsoft solutions and non-Microsoft clouds, the use of Threat Intelligence, and the creation of visual reports.

Chapter 12: Protect and Govern Sensitive Data- Data is the most valuable resource that an organisation has. In today's world data is everywhere and organisations need tools to find the sensitive data, safeguard it from unauthorized access and manage it through its lifecycle. This chapter explores Microsoft Purview Information Protection and how it can be used to find and protect sensitive content; Microsoft Purview Data Loss Protection to prevent sensitive information from being shared with unauthorized parties. It also explains how Microsoft Purview Data Lifecycle Management and Records Management can be used to govern the life cycle of the data from the time it was created till when it is securely disposed of.

Chapter 13: Managing Insider Risks- Data does not move itself, people move data. To understand the user intent behind moving the data, we need to know not only how, but also why the data moved. This chapter explains Microsoft Purview Insider Risk Management and Microsoft Purview Communication Compliance solutions to set up policies that can track user behaviour over time and prevent insiders from leaking sensitive content. It also covers Adaptive Protection and how to gather forensic evidence for investigations.

Chapter 14: Managing eDiscovery Cases- When something goes wrong, an organization might need to show proof to regulators, legal authorities or their own investigators. This chapter introduces Microsoft Purview eDiscovery as the tool investigate such incidents by creating cases, assigning custodians and conducting searches across the organization to find the data that is most important for the investigation. It can examine and filter the data in-place to save time and money when doing an eDiscovery investigation.

It is also important for organizations to be aware of user and admin activity happening in their environment. Microsoft Purview Audit serves as a comprehensive record of system activities, user actions, and changes to data. This chapter explains it can aid in investigating and resolving incidents of unauthorized access, data breaches, or other security violations.

Chapter 15: Managing Regulatory Compliance- Most organizations are subject to more than one industry or government regulation that they must adhere to. Remaining compliant with these regulations is an arduous task. Organizations invest a lot of time and money to achieve this. Microsoft Purview Compliance Manager is a simple SaaS based solution that helps organizations remain compliant with the regulations by providing easy to use templates and step-by-step guidance to meet the regulation requirements.

Chapter 16: Managing Privacy- Many organizations have a lot of PII stored in unstructured data in different locations. This PII can be mishandled and lead to serious consequences like loss of customer trust and reputation. Microsoft Priva helps a privacy officer to find out where PII is stored, how it moves within the organization and how old it is. It also empowers the user to make smart data handling decisions by providing timely trainings. Microsoft Priva Subject Rights Request is the tool that helps organizations to quickly answer Data Subject Requests. This chapter also introduces Preview capabilities of Consent management, Tracker scanning and Privacy assessments.

Chapter 17: Best Practices- The concluding chapter of this book takes the reader through identity, security and compliance best practices that further enhance the understanding of the concepts. This also enables administrators to take best decisions based on their organization business use cases and requirements.

Code Bundle and Coloured Images

Please follow the link to download the
Code Bundle and the *Coloured Images* of the book:

https://rebrand.ly/am8kms4

The code bundle for the book is also hosted on GitHub at **https://github.com/bpbpublications/Mastering-Microsoft-365-Security-Technologies**. In case there's an update to the code, it will be updated on the existing GitHub repository.

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

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 **business@bpbonline.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 **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights 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.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Table of Contents

CHAPTER 1

Introduction to Microsoft Entra

Introduction

This chapter introduces you to Microsoft Entra. Microsoft Entra is a family of products that help organisations create, manage, and govern user access to enterprise applications and services. In this chapter, we will learn the components of the Microsoft Entra and how they can help organisations address their identity and access management requirements. We will also explore the licensing options for each capability. This chapter will demonstrate how to create users using Microsoft Entra, the external collaboration capabilities using Microsoft Entra External ID. It will also introduce new capabilities like Microsoft Entra Permissions Management, Microsoft Entra Verified ID and Global Secure Access.

Structure

The chapter covers the following topics:

- Microsoft Entra ID
- Microsoft Entra ID Governance
- Microsoft Entra External ID
- Microsoft Entra Permissions Management
- Microsoft Entra Workload ID

- Microsoft Entra Verified ID
- Global Secure Access

Objectives

By the end of this chapters, readers will be able to explain the different components of the Microsoft Entra product family. You will be able to understand the different licensing options available to organisations when they buy Microsoft Entra ID and the identity governance capabilities in Microsoft Entra ID. This chapter also explains how Microsoft Entra enables secure collaboration with external vendors, partners and customers using Microsoft Entra External ID. Finally, you will understand the new capabilities Microsoft Entra Permissions Management, Microsoft Entra Workload ID, Microsoft Entra Verified ID and Global Secure Access.

The future chapters in this book build on the concepts covered in this chapter.

Microsoft Entra ID

Microsoft Entra ID, previously known as Azure Active Directory, is Microsoft's cloud-based service for identity and access management. This allows users in the organisation to access internal and external resources like Microsoft 365, Azure and many other third-party cloud applications.

Microsoft Entra ID serves many purposes for users in an organisation depending on their role:

- **IT admins**: They can use Microsoft Entra ID to create and manage user accounts and control access to applications and other resources.
- **Application developers**: They can use Microsoft Entra ID to authenticate users and provide **single sign-on** (**SSO**) for their applications. This allows users to access applications with their Entra ID login information.
- **Microsoft 365, Office 365, Azure or Dynamics CRM online users**: Microsoft Entra ID enables users to authenticate and gain access to resources required to do their job.

Licensing

Microsoft Online business services such as Microsoft 365 or Microsoft Azure rely on Microsoft Entra ID to enable sign-in for users and help secure their identities. If your organisation uses any of these services, you already have the free version of Microsoft Entra ID.

To access other advanced user management and identity governance features, you can purchase Entra ID P1 or Entra ID P2.

Following is a short description of these license types:

- **Microsoft Entra ID free**: It is included in Microsoft cloud subscriptions such as Microsoft 365 and Azure. It offers basic user and group administration, on-premises directory sync, SSO and basic reporting features.
- **Microsoft Entra ID P1**: This plan offers all the features of the free plan, plus it allows hybrid users to access applications both on-premises and in the cloud. It also gives advanced administration options like dynamic groups, self-service group management and self-service password reset for on-premises users. It can be purchased as a separate product. It is included in Microsoft 365 E3 and Microsoft 365 Business Premium.
- **Microsoft Entra ID P2**: P2 offers all the capabilities of free and P1 and adds identity protection features such as risk-based Conditional Access and Privileged Identity Management that give access to administrators only when needed. It can be purchased on its own or comes with Microsoft 365 E5.

Creating new Entra ID tenant

All administrative tasks related to Microsoft Entra ID are done using the Microsoft Entra admin centre. You will begin by creating a new tenant for your organisation.

Prerequisites

To get started with Microsoft Entra ID you need to create an Entra ID tenant. For this, you need the following:

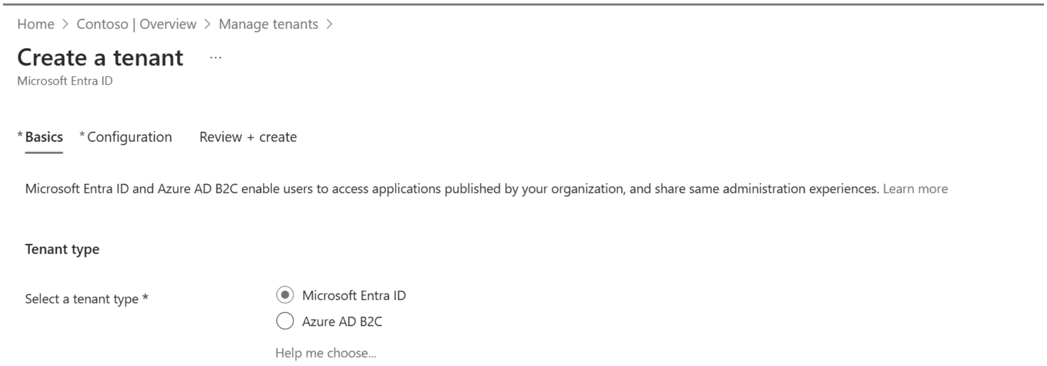
- An Azure subscription.
- An account with the Tenant Creator role assigned.

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

Steps

Following are the steps to create a new Microsoft Entra ID tenant:

1. Login to the Azure portal at **https://portal.azure.com** with an account that has the Tenant Creator role assigned.
2. Select **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 figure:



Home > Contoso | Overview > Manage tenants >

Create a tenant ...

Microsoft Entra ID

*Basics *Configuration Review + create

Microsoft Entra ID and Azure AD B2C enable users to access applications published by your organization, and share same administration experiences. Learn more

Tenant type

Select a tenant type *

● Microsoft Entra ID

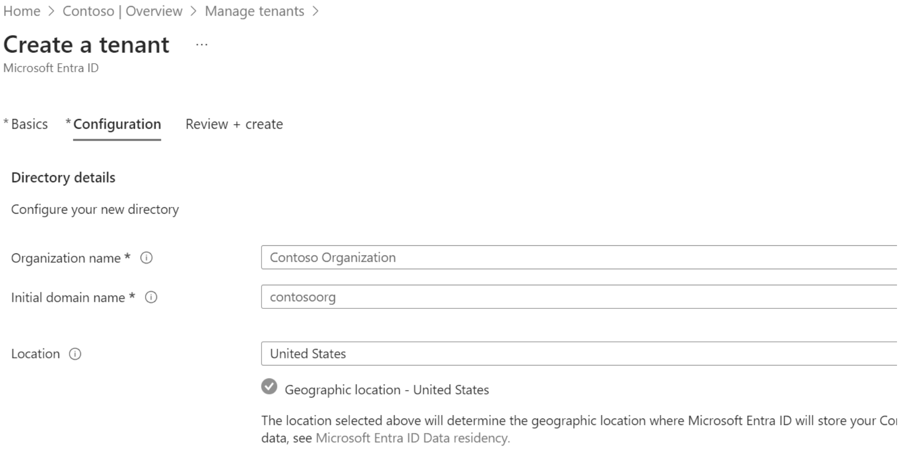
○ Azure AD B2C

Help me choose...

Figure 1.1: *Creating a new tenant*

5. On the **Configuration,** page enter the **Organisation name**, **Initial domain name** and **Location** and click **Next: Review + create**.

   Refer to the following figure:



Home > Contoso | Overview > Manage tenants >

Create a tenant ...

Microsoft Entra ID

*Basics *Configuration Review + create

Directory details

Configure your new directory

Organization name * ⓘ Contoso Organization

Initial domain name * ⓘ contosoorg

Location ⓘ United States

✓ Geographic location - United States

The location selected above will determine the geographic location where Microsoft Entra ID will store your Co
data, see Microsoft Entra ID Data residency.

Figure 1.2: *Enter organisation details*

The new tenant will be created with the domain **`domainname.onmicrosoft.com`**.

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.

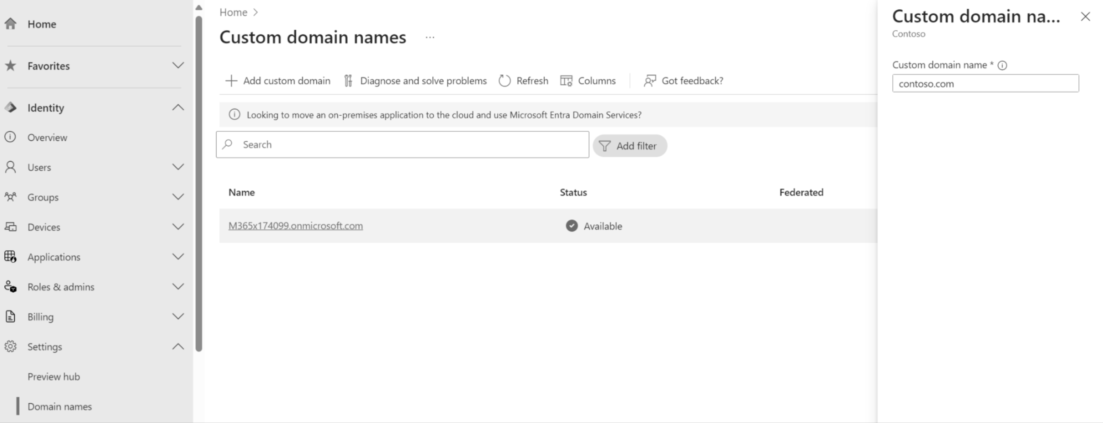
Adding custom domain name in Entra ID

Microsoft Entra tenants are created with an initial domain like **`youroganisationname.onmicrosoft.com.`** The user IDs are hence in the format **`user1@yourorganisationname.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@yourorganisationname.com`**.

Following are the steps to add a custom domain name:

1. Login to **https://entra.microsoft.com** with an ID that has the Domain Name Administrator role assigned.
2. Browse to **Identity | Settings | Domain names | Add custom domain.**
3. Click on **Add custom domain**. Enter your organisation's domain and click **Add domain**.

   Refer to the following figure:



Looking to move an on-premises application to the cloud and use Microsoft Entra Domain Services?

Name	Status	Federated
M365x174099.onmicrosoft.com	Available	

Custom domain name *: contoso.com

__Figure 1.3__: Adding a custom domain name

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 screen below. This will be required to validate your ownership of the domain. Save this information.

   Refer to the following figure: