2.Entra ID

Cloud Advanced

Klaas Thys
klaas.thys@pxl.be

Microsoft Entra certification

[Microsoft Learn: SC-900]()

[Microsoft Learn: SC-300]()

2.Entra ID

1. **What is Entra ID?**
2. Securing identities
3. Entra for Microsoft 365

Microsoft Entra ID

Microsoft Entra ID is Microsoft Azure’s cloud-based identity and access management service.

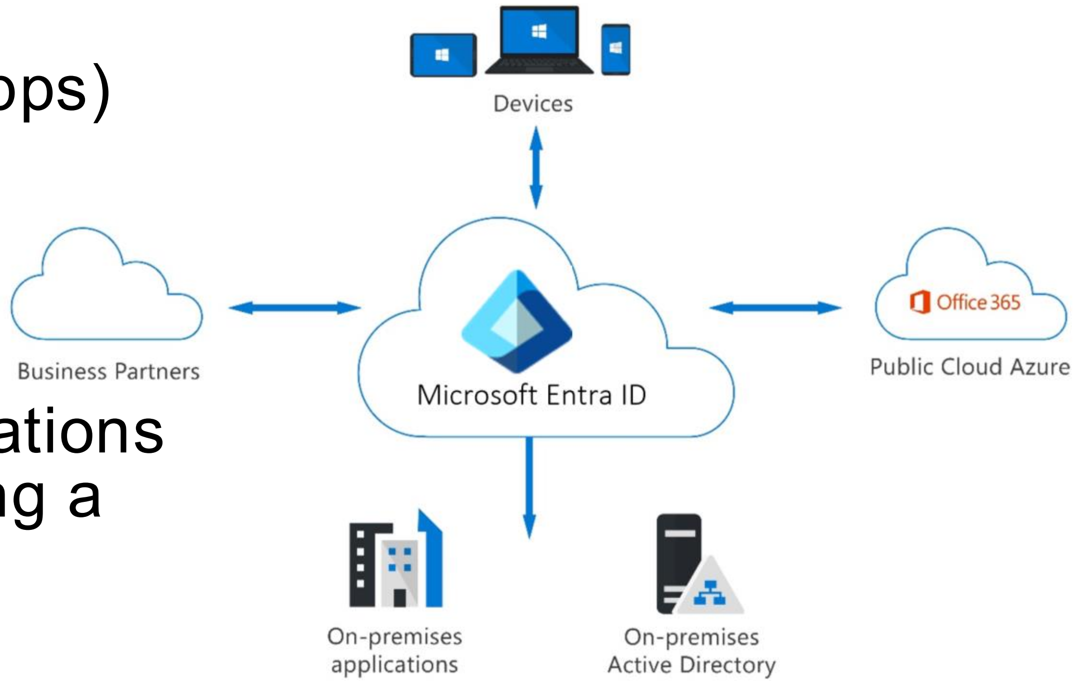
- Authentication (employees sign-in to access resources)
- Modern authentication
- Application management
- Business to Business (B2B)
- Device Management

Microsoft Entra ID

Entra ID enables employees, guests, and others to securely access:

- Internal resources
(corporate apps, intranet, custom cloud apps)
- External services
(Microsoft 365, Azure portal, SaaS apps)

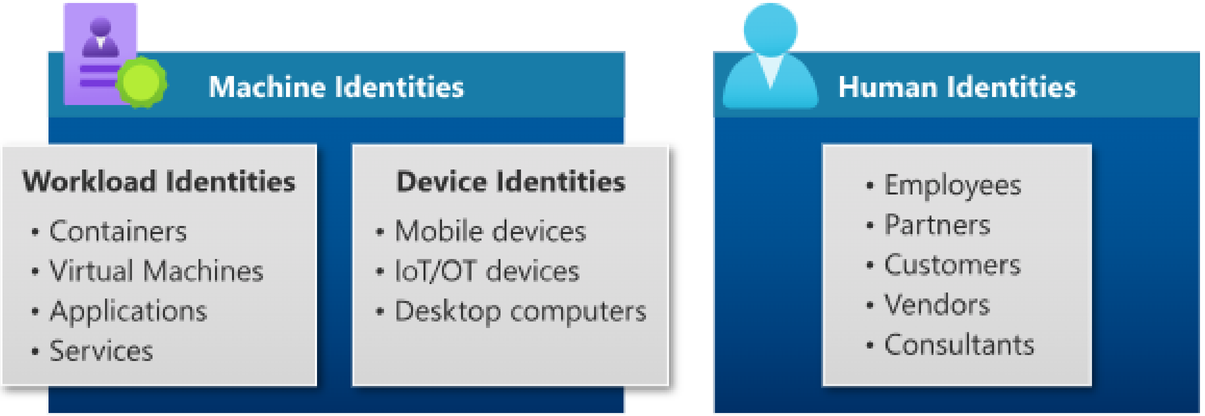
Microsoft Entra ID simplifies the way organizations manage authorization and access by providing a single identity system for their cloud and on-premises applications



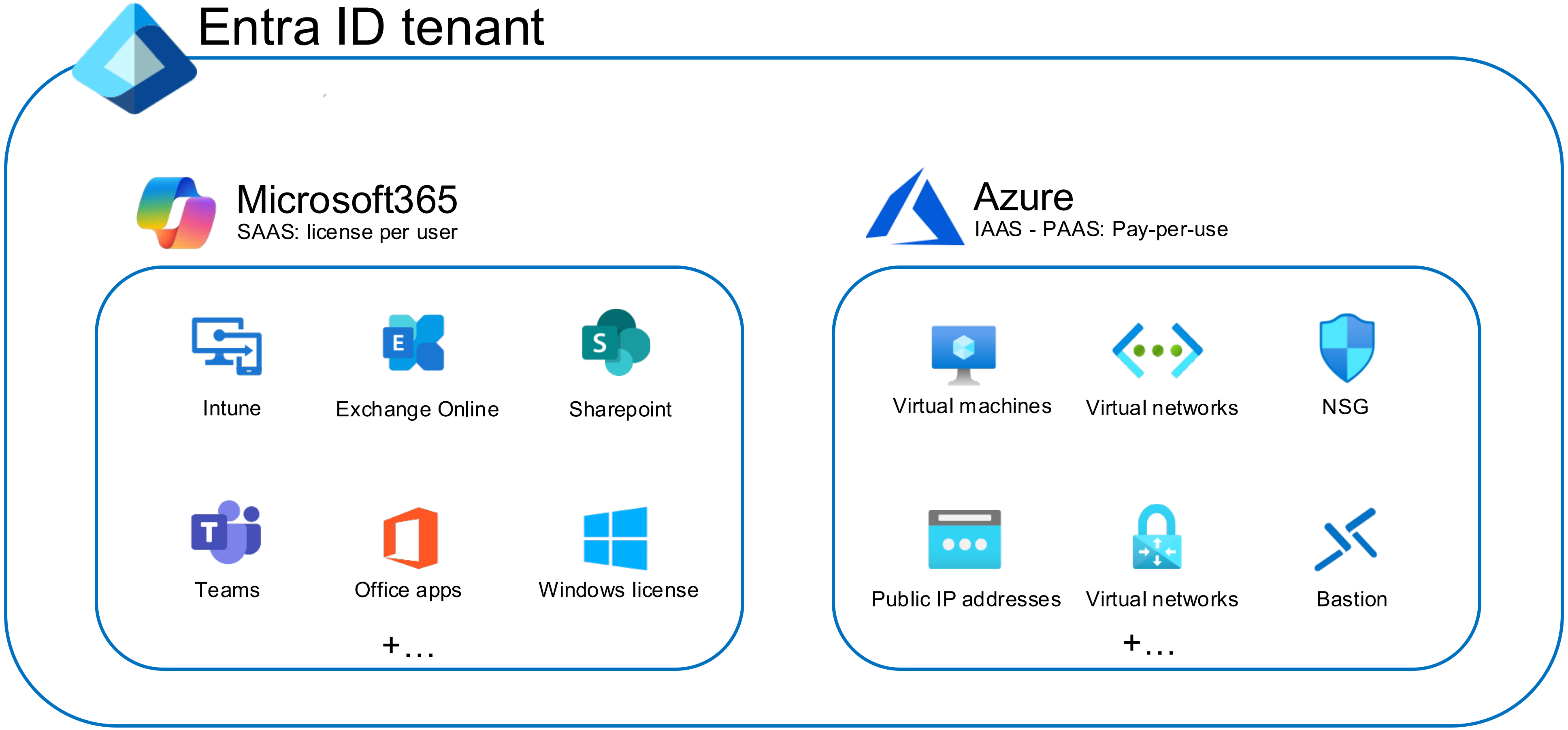
Entra ID: identities

Microsoft Entra ID supports various types of identities:

- **User identities:** Assigned to people (employees, external users like customers or partners).
- **Device identities:** Assigned to physical devices (mobile phones, desktops, IoT devices).
- **Workload identities:** Assigned to software objects (apps, virtual machines, services, containers).



Cloud Workplace IT infrastructure



Entra ID tenant

Microsoft365
SAAS: license per user

Intune

Exchange Online

Sharepoint

Teams

Office apps

Windows license

+...

Azure
IAAS - PAAS: Pay-per-use

Virtual machines

Virtual networks

NSG

Public IP addresses

Virtual networks

Bastion

+...

Terminology

- **UPN** each user is identified by a unique User Principal name (UPN)
- **Tenant:** A Microsoft Entra tenant is an instance of Entra ID for a single organization, storing data like users, groups, devices, and app registrations. Each tenant has a unique ID and domain name (e.g., contoso.onmicrosoft.com).

Terminology

- **Directory Service:** The Microsoft Entra directory is a logical container within a tenant, holding and organizing identity-related resources like users, groups, and devices. A tenant contains only one directory, acting as a catalog for identities and resources.
- **Multi-Tenant:** A multi-tenant organization has multiple Microsoft Entra ID instances, often due to reasons like subsidiaries, mergers, acquisitions, or geographical/regulatory requirements.

Identity Provider

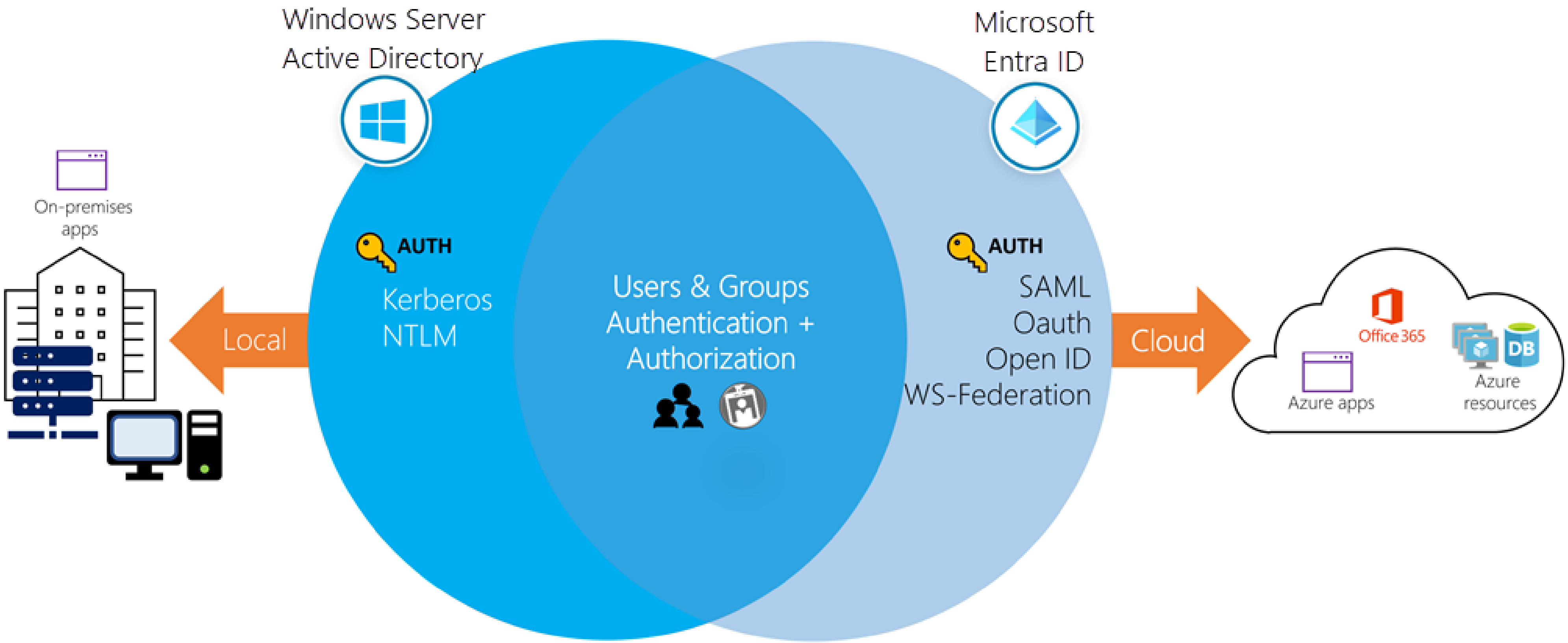
An **identity provider (IdP)** is a system that creates, manages and stores digital identities. The three most common components are:

- a repository of user identities
- an authentication system
- security protocols that defend against intrusion

Identity Provider: ADDS vs Entra

	Active Directory Domain Services	**Entra ID**
Usage	Managing identities and devices within a local infrastructure	Cloud-based solution designed for modern, hybrid, and cloud environments.
Authentication	Uses Kerberos for authenticating Windows Machines. LDAP for local queries	Modern authentication methods like OAuth, OpenID Connect and SAML for cloud authentication
Device management	Managing devices on prem	Managing devices regardless of location
Applications	Focused on on-prem apps, supports LDAP & Kerberos	Cloud-based app access with SSO, integrates with SaaS apps
User Access	Relies on local network/domain	Accessible anywerhe with internet connectivity

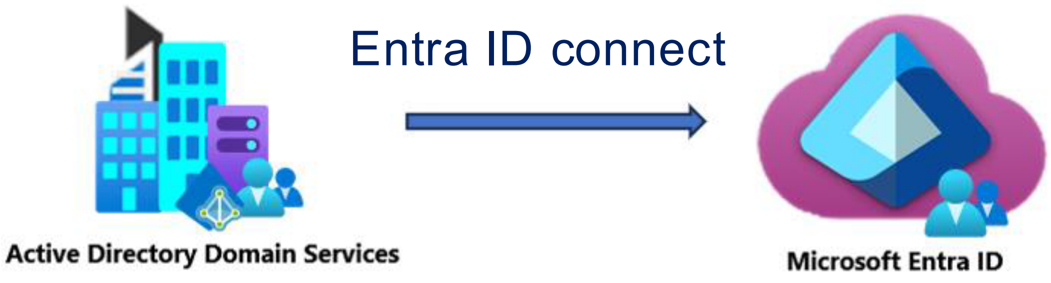
Identity Provider: ADDS vs Entra



Hybrid identity

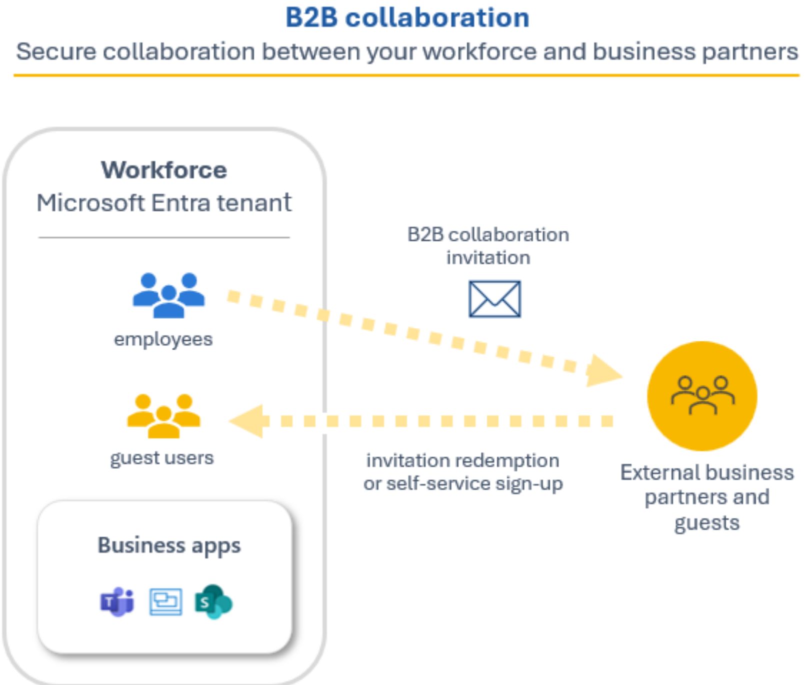
Sync users and or devices from Active Directory to Entra ID with ***Entra ID connect.*** Synchronization is responsible for making sure identity information for your on-premises users and groups is matching the cloud.

- Using Active Directory for on prem legacy applications
- Using Entra ID for modern web applications



External users: B2B Collaboration

B2B collaboration is a capability of Microsoft Entra External ID that lets you **collaborate with users and partners outside of your organization.** With B2B collaboration, an external user is invited to sign in to your Microsoft Entra workforce tenant using **their own credentials.**


B2B collaboration
Secure collaboration between your workforce and business partners
Workforce
Microsoft Entra tenant
employees
guest users
Business apps
B2B collaboration invitation
invitation redemption or self-service sign-up
External business partners and guests

2.Entra ID

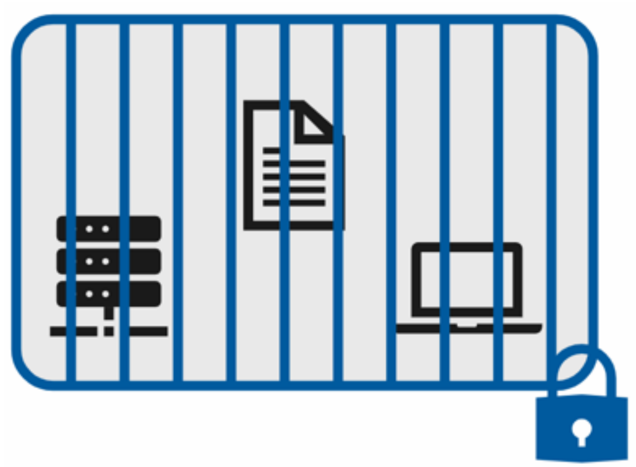
1.What is Entra ID?

2.Securing identities

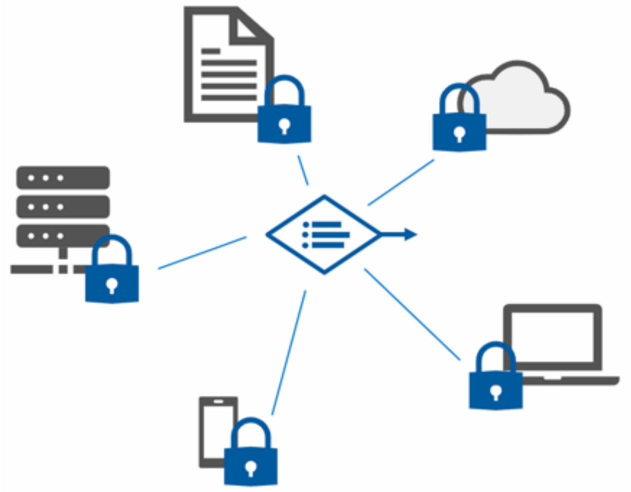
3.Entra for Microsoft 365

Classic identity to zero trust identity

Historically, identity provided full access via username and password behind a firewall. Today, one stolen credential can compromise everything. Zero Trust secures assets everywhere with policies.



Classic identity
Restrict everything to a secure network



Zero Trust Identity
Protect assets anywhere with central policy

Zero Trust model

“Trust no one, verify everything”

- **Verify explicitly:** Authenticate and authorize based on user, device, location, and anomalies.
- **Least privileged access:** Grant minimal access with JIT (Just In Time) ,JEA (Just Enough Access) and adaptive policies.
- **Assume breach:** Segment access, encrypt data, and use analytics for threat detection.

Modern Authentication

Modern authentication in Microsoft Entra ID enhances security and access control with advanced identity management, replacing traditional passwords with more secure, flexible methods.

- **Single Sign-On (SSO):** Users authenticate once and gain access to multiple applications without needing to log in again.
- **Multi-Factor Authentication (MFA):** Requires an additional verification step, such as a mobile notification, SMS code, or biometric authentication.
- **OAuth 2.0 & OpenID Connect (OIDC):** Secure, token-based authentication protocols for web, mobile, and API access.
- **Conditional Access:** Applies real-time policies based on user location, device compliance, risk level, and more.

Single Sign-On

Single Sign-On (SSO) allows users to log in once and access multiple applications without needing to re-enter credentials. The application is called the Service Provider

Modern authentication protocols enables SSO: OpenID Connect (OIDC), OAuth and Security Assertion Markup Language (SAML)

Single Sign-On: PXL examples

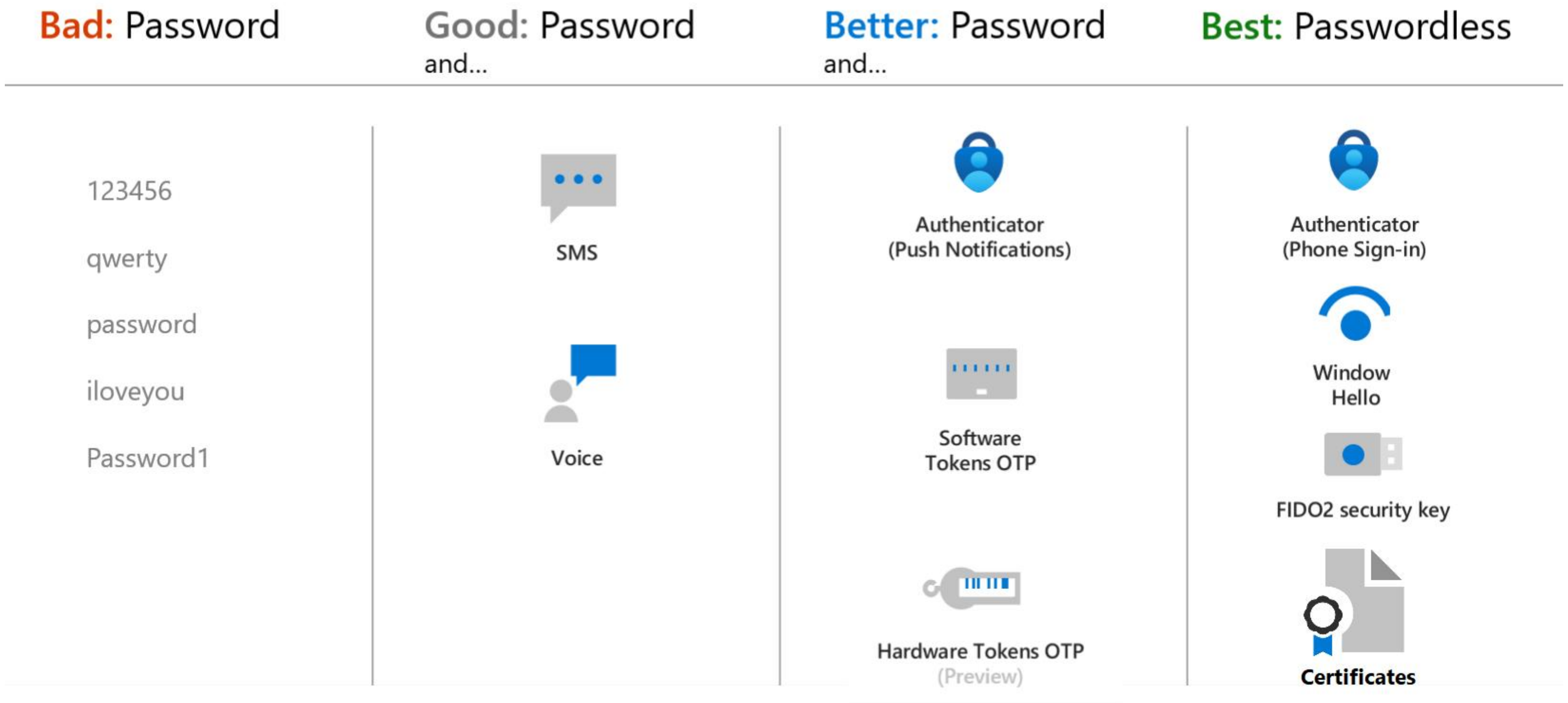
Learning Management System
https://pxl.blackboard.com

Wooclap - learning tool, with online quizzes, pols,…
www.wooclap.com

MijnPXL
mijnpxl.pxl.be

Multi Factor Authentication

Unlike authentication in Active Directory, Entra authentication supports multi-factor authentication.



Bad: Password	Good: Password and...	Better: Password and...	Best: Passwordless
123456	SMS	Authenticator (Push Notifications)	Authenticator (Phone Sign-in)
qwerty	Voice	Software Tokens OTP	Window Hello
password		Hardware Tokens OTP (Preview)	FIDO2 security key
iloveyou			Certificates
Password1			

Role Based Access

Manage permissions by assigning specific roles to users or groups, ensuring that individuals have only the access necessary to perform their job ***(least privilege access)***

Roles	**Description**	**Permissions**
Global Administrator	Full control over all settings and services in Microsoft 365	Can manage users, domains, subscriptions, and access to all admin centers.
User Administrator	Manages user accounts and groups.	Can reset passwords, create and delete users, and manage group memberships.
Helpdesk Administrator	Provides basic user support, primarily for password and account issues.	Can reset passwords, manage service requests, and assist with user sign-ins.
Exchange Administrator	Manages Exchange Online settings and mailboxes.	Can configure mail flow, manage mailbox permissions, and set up policies.
Billing Administrator	Manages subscriptions, licenses, and billing details.	Can view and manage subscription settings, invoices, and payment methods.

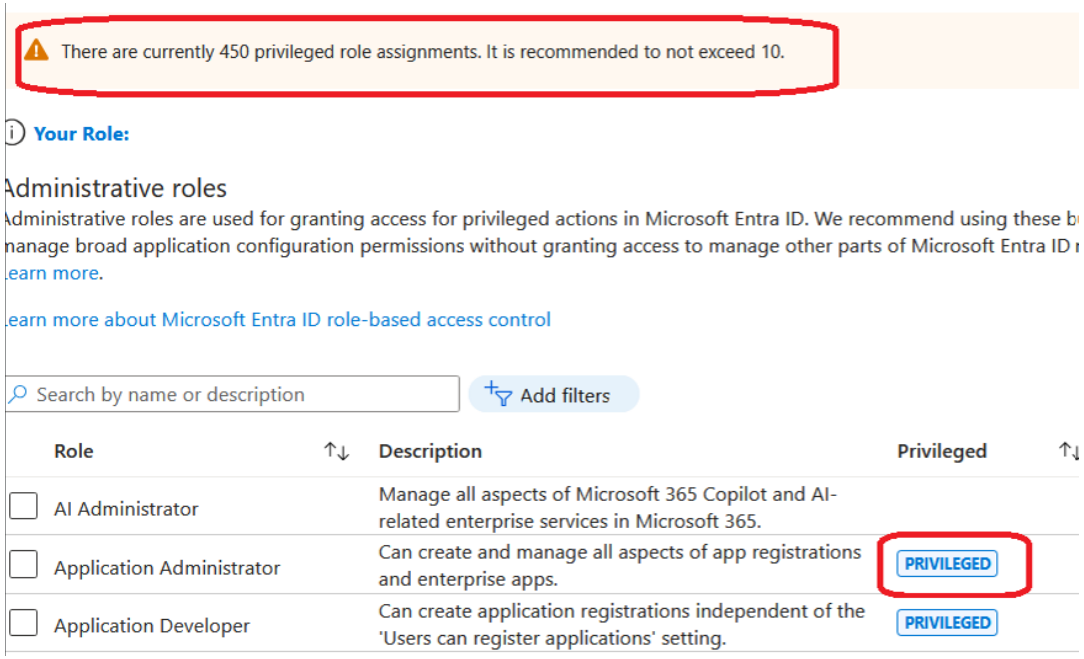
Role Based Access

Global Administrator

- Highest Privilege Role: Has full access to all management features in Entra ID and Microsoft services.
- Limit the number of Global Administrators to less than 5

Privileged role assignments

- Some role include privileged permissions, such as ability to update credentials
- These roles can potentially lead to elevation of privilege



There are currently 450 privileged role assignments. It is recommended to not exceed 10.

Your Role:

Administrative roles

dministrative roles are used for granting access for privileged actions in Microsoft Entra ID. We recommend using these b
nanage broad application configuration permissions without granting access to manage other parts of Microsoft Entra ID r
earn more.

earn more about Microsoft Entra ID role-based access control

	Role	Description	Privileged
□	AI Administrator	Manage all aspects of Microsoft 365 Copilot and AI-related enterprise services in Microsoft 365.	
□	Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	PRIVILEGED
□	Application Developer	Can create application registrations independent of the 'Users can register applications' setting.	PRIVILEGED

Privileged Identity Management

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about.

- Provide **just-in-time** privileged access to Microsoft Entra ID and Azure resources
- Assign **time-bound** access to resources using start and end dates
- Require **approval** to activate privileged roles

Privileged Identity Management

Privileged Identity Management workflow example: an IT support engineer, needs temporary Intune Administrator permissions to troubleshoot device compliance issues in Microsoft Intune.

Step 1

User Requests Elevated Access

- Selects a the intune admin role
- Provides a justification
- Selects the duration

Step 2

Approval

- Request is sent to Security admin or Global Administrator
- Reviews the request
- Approves the request

Step 3

Role activation & usage

- Requestor receives notification
- Requestor logs in the intune admin center
- Makes necessary intune configuration changes

Step 4

Automatic expiration

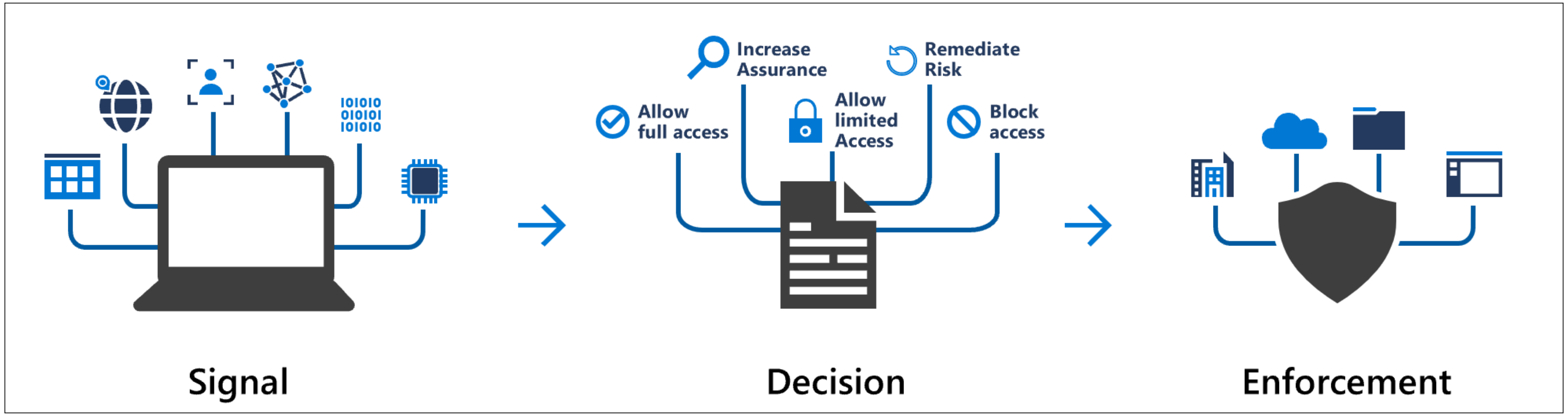
- Intune Administrator admin role is automatically revoked after the selected duration
- Security Team can review audit logs in Entra.

Conditional Access

Conditional Access policies at their simplest are if-then statements; if a user wants to access a resource, then they must complete an action.

Administrators are faced with two primary goals:

- Empower users to be productive wherever and whenever
- Protect the organization's assets



Conditional Access: Signals

- **User or Group Membership:** Policies can target specific users/groups, providing fine-grained access control.
- **IP Location Information:** Trusted IP ranges can be used to block/allow traffic based on geographic location.
- **Device:** Enforce policies based on device platform or state (e.g., privileged access workstations).
- **Application:** Policies can be triggered based on user access to specific applications.
- **Real-time & Calculated Risk Detection** Integration with Microsoft Entra ID Protection helps detect and remediate risky users and sign-ins.

Conditional Access: Decision

Block access: most restrictive decision

Grant access: Less restrictive decision, can require one or more of the following options:

- Require multifactor authentication
- Require authentication strength
- Require device to be marked as compliant
- Require approved client app
- Require password change
- Require terms of use

Conditional Access: Example

1.Signal: User tries to sign in from a new device located outside the corporate network (detected by IP location).
Signals: unkown device - unknown IP

2.Decision: evaluates the signals

- User is in an untrusted location (outside corporate network)
- The device is not marked as compliant in Intune

➔ Require Multi-Factor Authentication (MFA)

3.Enforcement: The user is prompted for MFA before being granted access to the application

Entra Licensing

Entra ID license is included in the **Microsoft 365 licensing**

- **Microsoft Entra ID P1:** included in Microsoft 365 E3 licsense
- **Microsoft Entra ID P2:** included in Microsoft 365 E5 license

Most important difference: advanced security and identity protections features like Privileged Identity Management (PIM)

Microsoft Learn: Entra ID P1 vs Entra ID P2

2.Entra ID

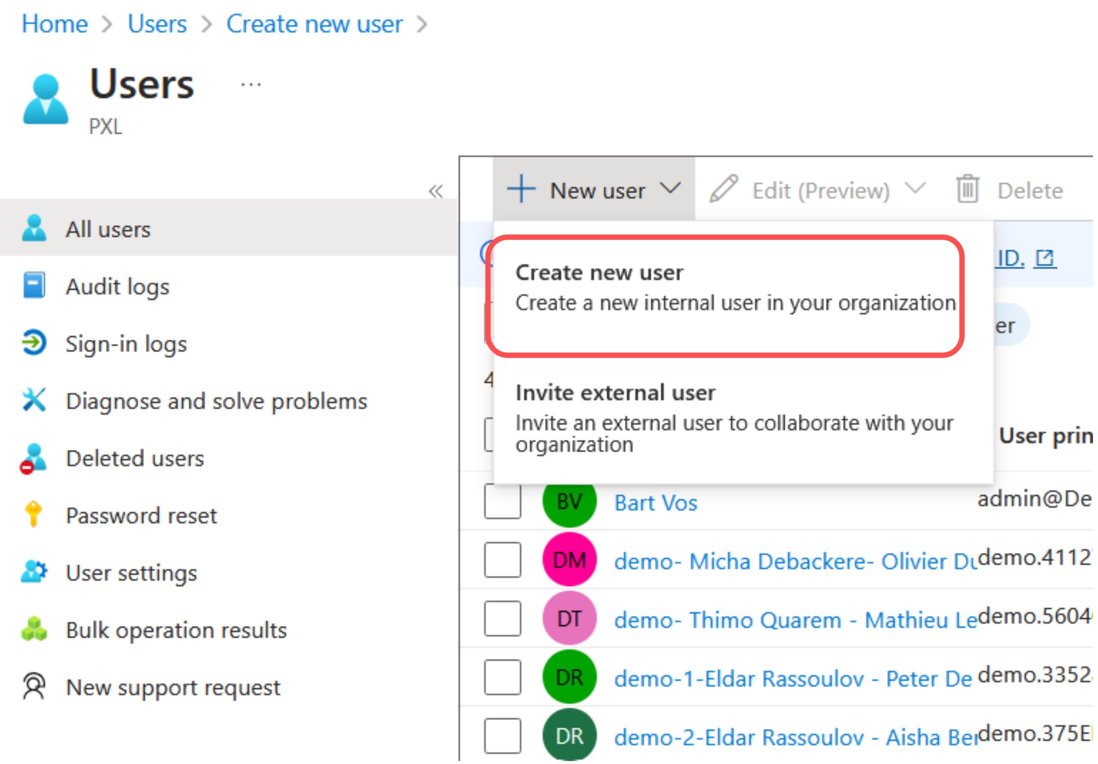
1.What is Entra ID?

2.Securing identities

3.Entra for Microsoft 365

Users: Internal

- Users within an organization (employees, students)
- Uses the organization's domain
- Access to internal resources (depending on role and permissions)



Home > Users > Create new user >

Users ···
PXL

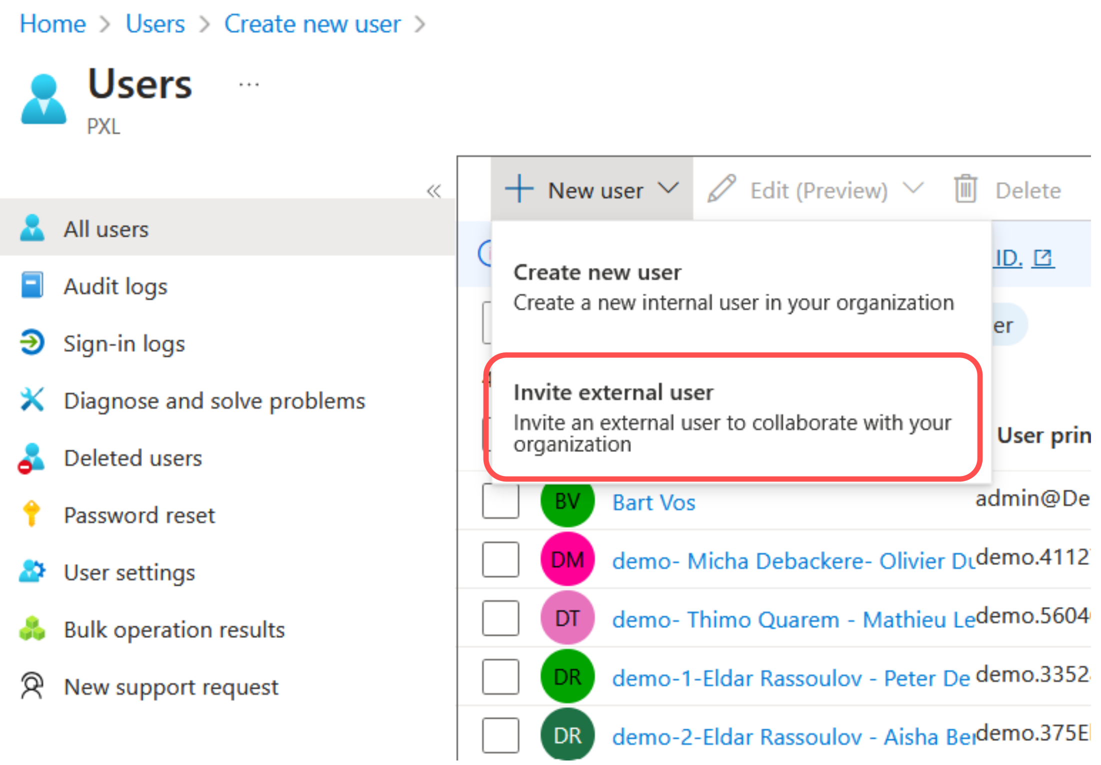
Create new user
Create a new internal user in your organization

Invite external user
Invite an external user to collaborate with your organization

	User prin
BV Bart Vos	admin@De
DM demo- Micha Debackere- Olivier Du	demo.4112
DT demo- Thimo Quarem - Mathieu Le	demo.5604
DR demo-1-Eldar Rassoulov - Peter De	demo.3352
DR demo-2-Eldar Rassoulov - Aisha Ber	demo.375E

Users: External

- External users from another organization, such as partners, vendors and customers
- Authenticate with another Entra ID account from another domain.
- Limited permissions, usually guest access only



Home > Users > Create new user >

Users ···
PXL

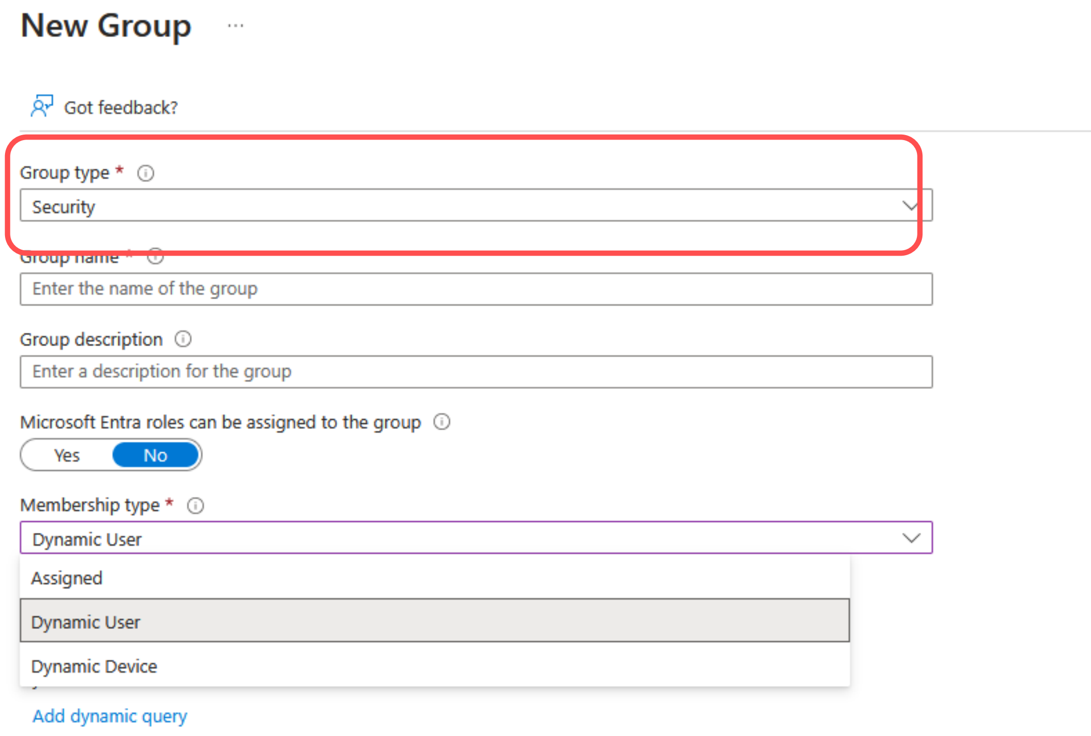
Create new user
Create a new internal user in your organization

Invite external user
Invite an external user to collaborate with your organization

	User prin
BV Bart Vos	admin@De
DM demo- Micha Debackere- Olivier Du	demo.4112
DT demo- Thimo Quarem - Mathieu Le	demo.5604
DR demo-1-Eldar Rassoulov - Peter De	demo.3352
DR demo-2-Eldar Rassoulov - Aisha Ber	demo.375E

Groups: Group Types

- **Security:** Used to manage the access of users and computers to resources. It is used to apply the same settings and permissions.
- **Microsoft 365 Groups: (***Members of a Microsoft 365 group can only be users, not devices)* Provides collaboration features by granting group members access to a:
  - Shared mailbox
  - Calendar
  - SharePoint site.



New Group ···

Got feedback?

Group type *

Security

Group name *

Enter the name of the group

Group description

Enter a description for the group

Microsoft Entra roles can be assigned to the group

Yes [✓ No]

Membership type *

Dynamic User

Assigned

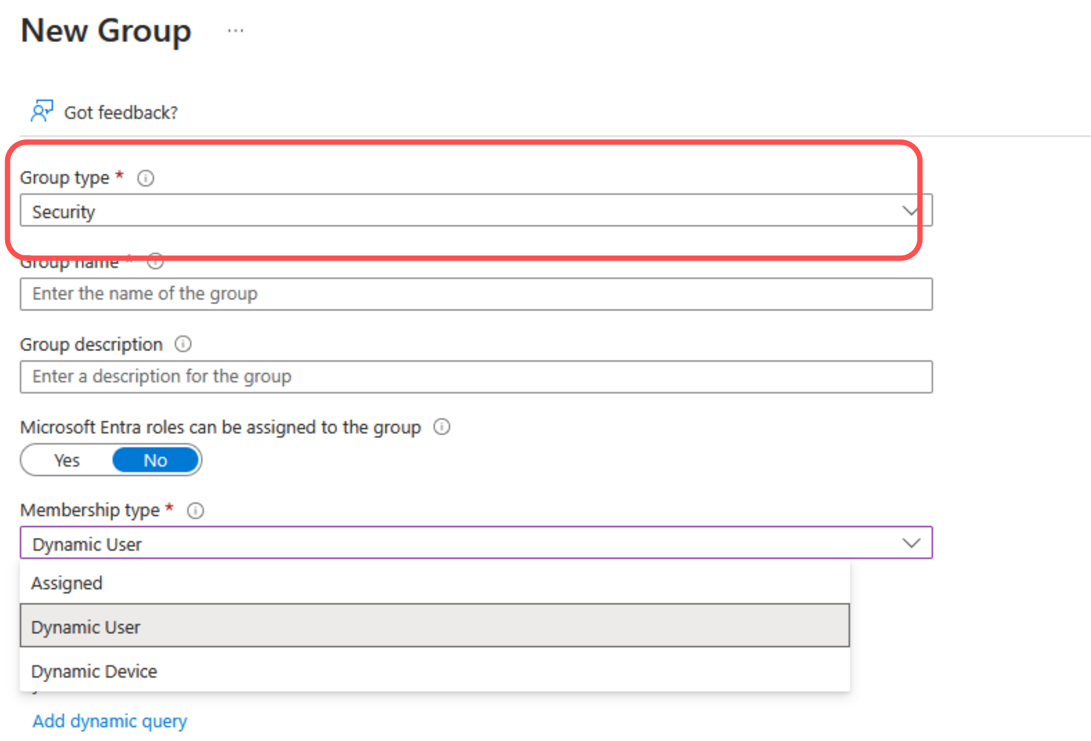
Dynamic User

Dynamic Device

Add dynamic query

Groups: Membership types

- **Assigned Groups:** Assigning users to a group.
- **Dynamic Membership Group for Users:** Allows you to set rules for automatically adding and removing users as members.
- **Dynamic Membership Group for Devices:** Allows you to set rules for automatically adding and removing devices as members.



New Group ···

Got feedback?

Group type *: Security

Group name *: Enter the name of the group

Group description: Enter a description for the group

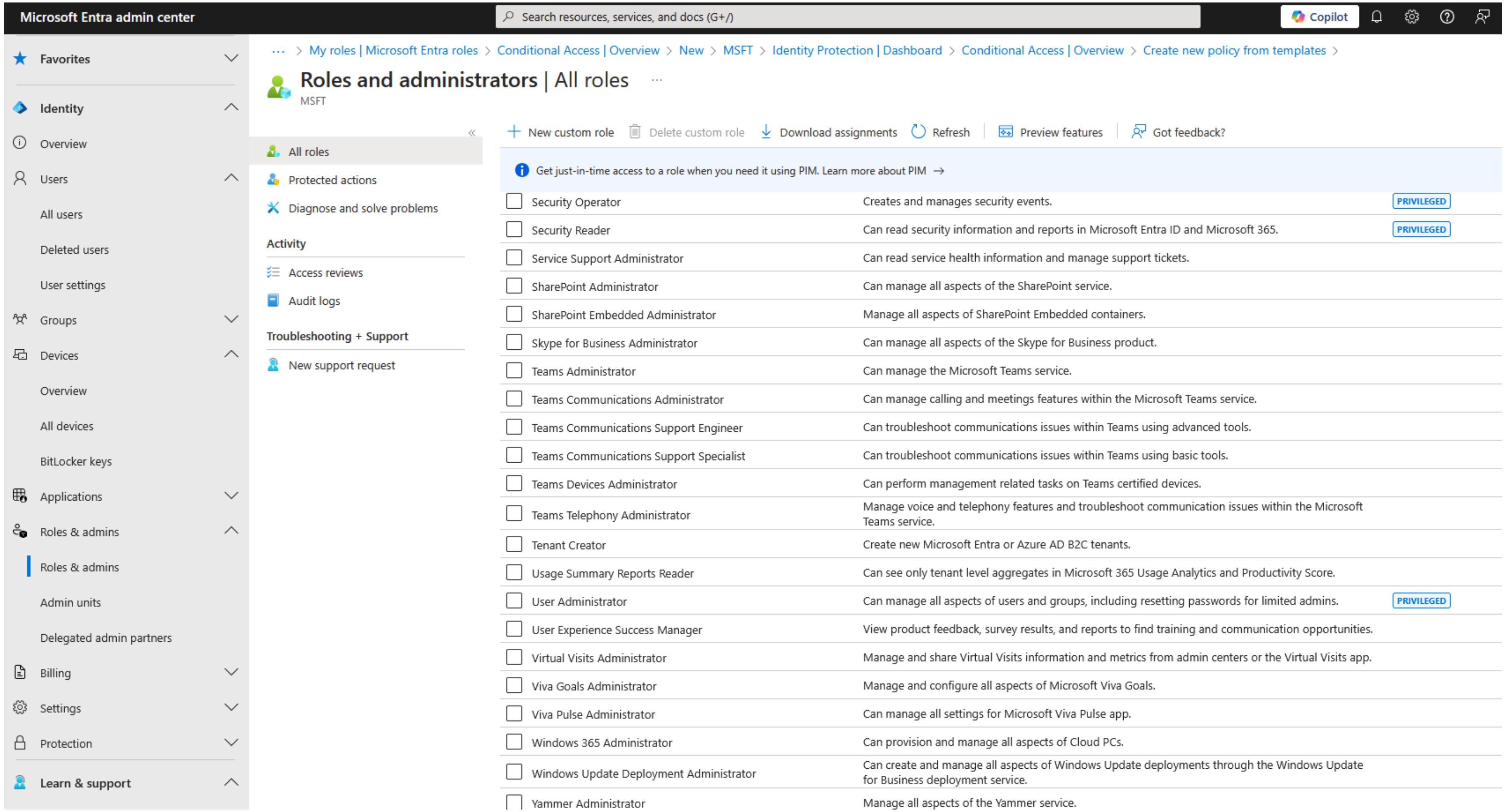
Microsoft Entra roles can be assigned to the group: Yes [✓ No]

Membership type *: Dynamic User

Entra ID: Dynamic groups examples

- **Department:** A group for the marketing department. Automatically adds users who have "Department: Marketing" assigned in their user profile.
- **Location:** A group for employees in Brussels. The group can include users who have the "Location" attribute set to "Brussels," ensuring only those users have access to specific resources or applications.
- **Role:** A group for all managers within the organization. The group can automatically add users who have the "Role" attribute set to "Manager" or a similar title.
- **Device:** group devices of a specific model or OS. Automatically add all HP ProBook 650 G8 to a group. Automatically add all Windows 11 with specific build to a group.

Entra: Microsoft365 roles



Roles and administrators | All roles

MSFT

Get just-in-time access to a role when you need it using PIM. Learn more about PIM →

☐	Security Operator	Creates and manages security events.	PRIVILEGED
☐	Security Reader	Can read security information and reports in Microsoft Entra ID and Microsoft 365.	PRIVILEGED
☐	Service Support Administrator	Can read service health information and manage support tickets.	
☐	SharePoint Administrator	Can manage all aspects of the SharePoint service.	
☐	SharePoint Embedded Administrator	Manage all aspects of SharePoint Embedded containers.	
☐	Skype for Business Administrator	Can manage all aspects of the Skype for Business product.	
☐	Teams Administrator	Can manage the Microsoft Teams service.	
☐	Teams Communications Administrator	Can manage calling and meetings features within the Microsoft Teams service.	
☐	Teams Communications Support Engineer	Can troubleshoot communications issues within Teams using advanced tools.	
☐	Teams Communications Support Specialist	Can troubleshoot communications issues within Teams using basic tools.	
☐	Teams Devices Administrator	Can perform management related tasks on Teams certified devices.	
☐	Teams Telephony Administrator	Manage voice and telephony features and troubleshoot communication issues within the Microsoft Teams service.	
☐	Tenant Creator	Create new Microsoft Entra or Azure AD B2C tenants.	
☐	Usage Summary Reports Reader	Can see only tenant level aggregates in Microsoft 365 Usage Analytics and Productivity Score.	
☐	User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.	PRIVILEGED
☐	User Experience Success Manager	View product feedback, survey results, and reports to find training and communication opportunities.	
☐	Virtual Visits Administrator	Manage and share Virtual Visits information and metrics from admin centers or the Virtual Visits app.	
☐	Viva Goals Administrator	Manage and configure all aspects of Microsoft Viva Goals.	
☐	Viva Pulse Administrator	Can manage all settings for Microsoft Viva Pulse app.	
☐	Windows 365 Administrator	Can provision and manage all aspects of Cloud PCs.	
☐	Windows Update Deployment Administrator	Can create and manage all aspects of Windows Update deployments through the Windows Update for Business deployment service.	
☐	Yammer Administrator	Manage all aspects of the Yammer service.	