Microsoft

AZ-500

Microsoft Azure Security Technologies

Agenda

1 Manage identity and access 

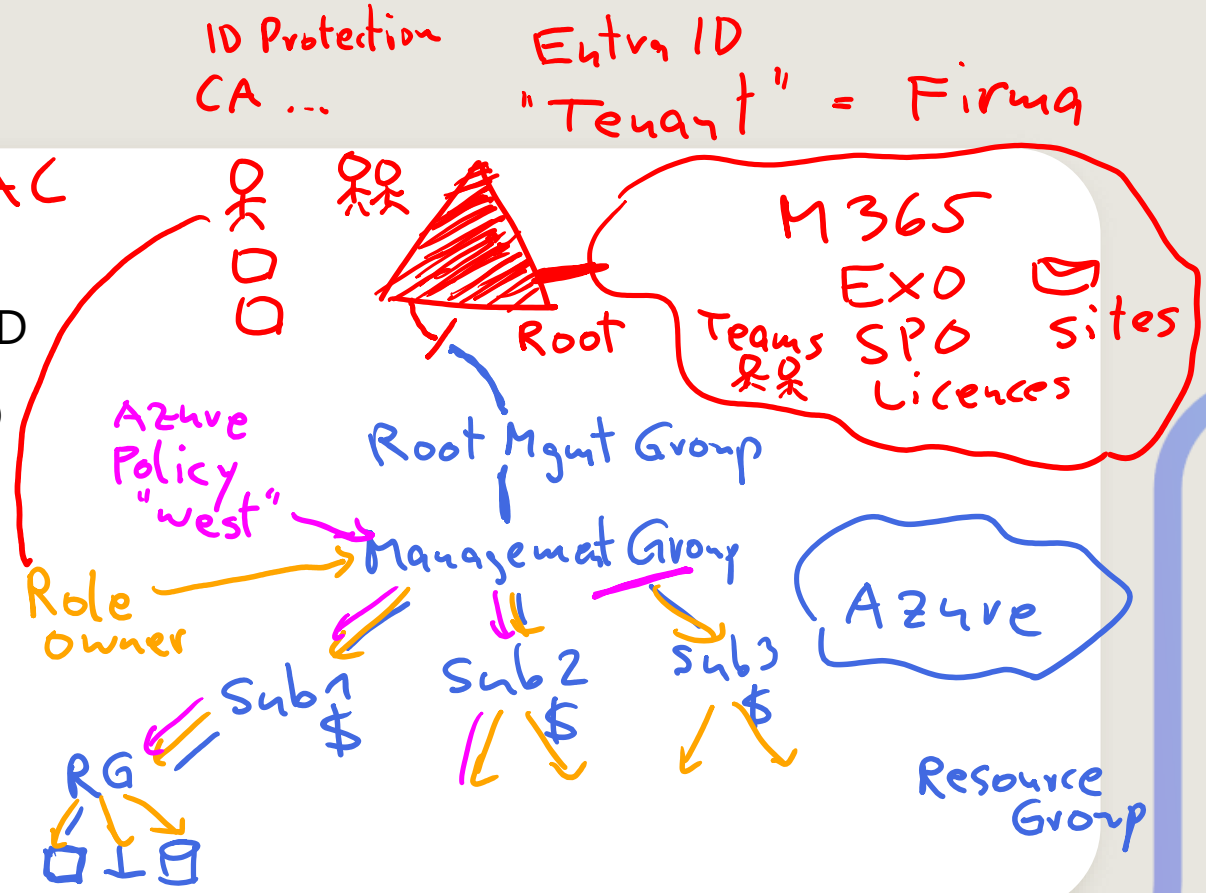
2 Secure networking

3 Secure compute, storage, and databases

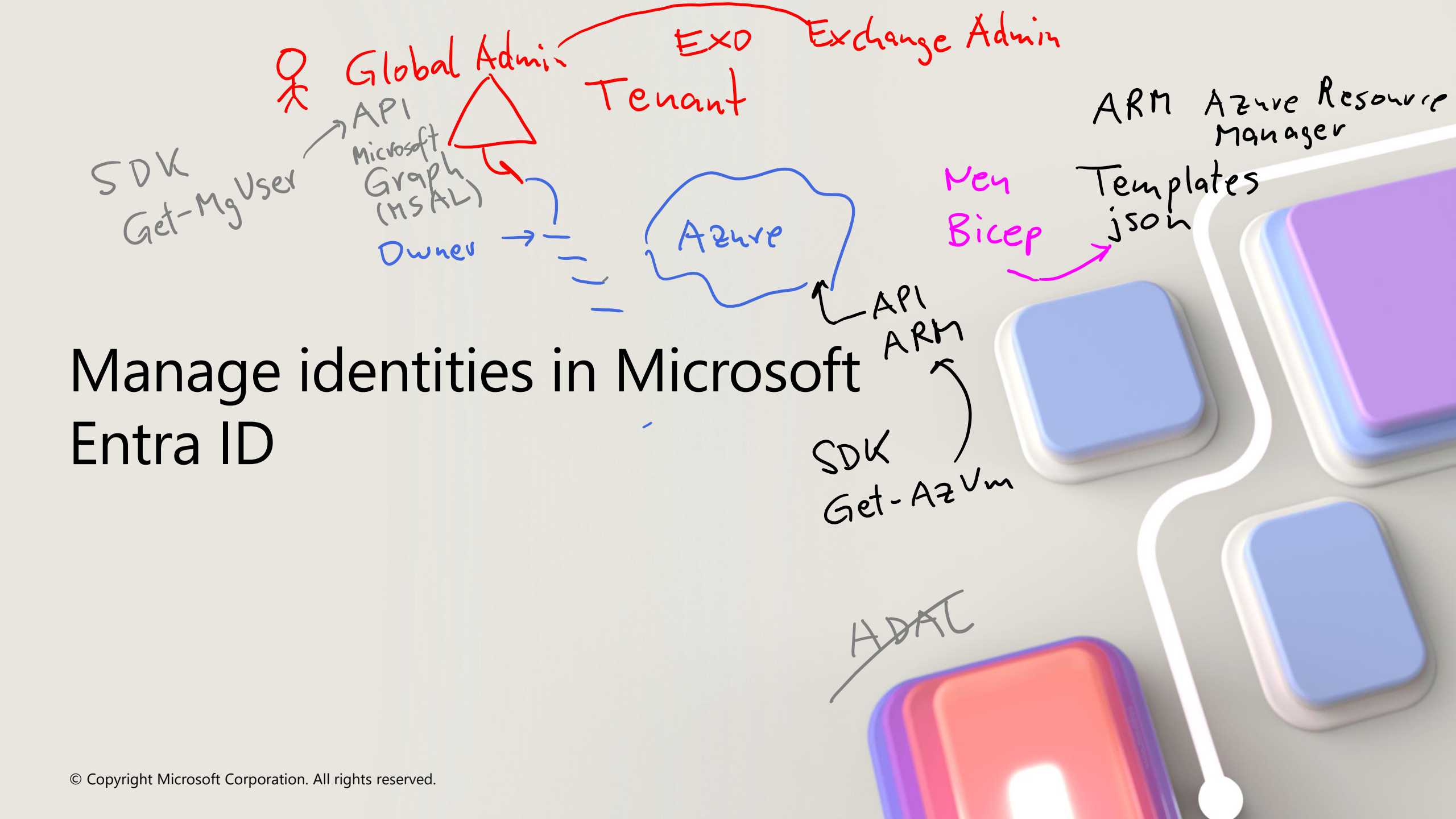
4 Manage security operations

Learning Path: Manage identity and access

- Manage identities in Microsoft Entra ID
- Manage authentication by using Microsoft Entra ID
- Manage authorization by using Microsoft Entra ID
- Manage application access in Microsoft Entra ID
- Module Lab



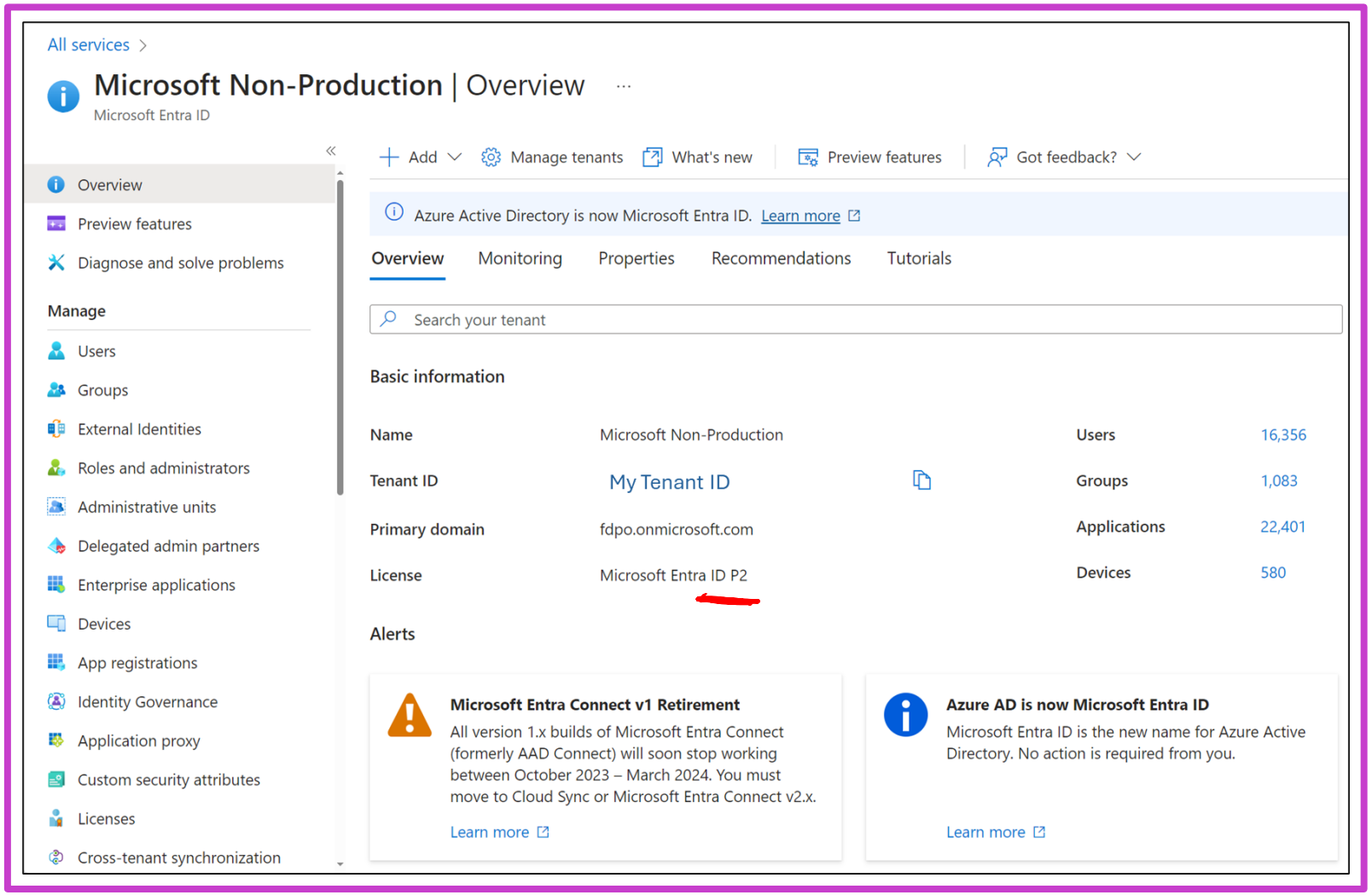
Managed ID



Manage identities in Microsoft Entra ID

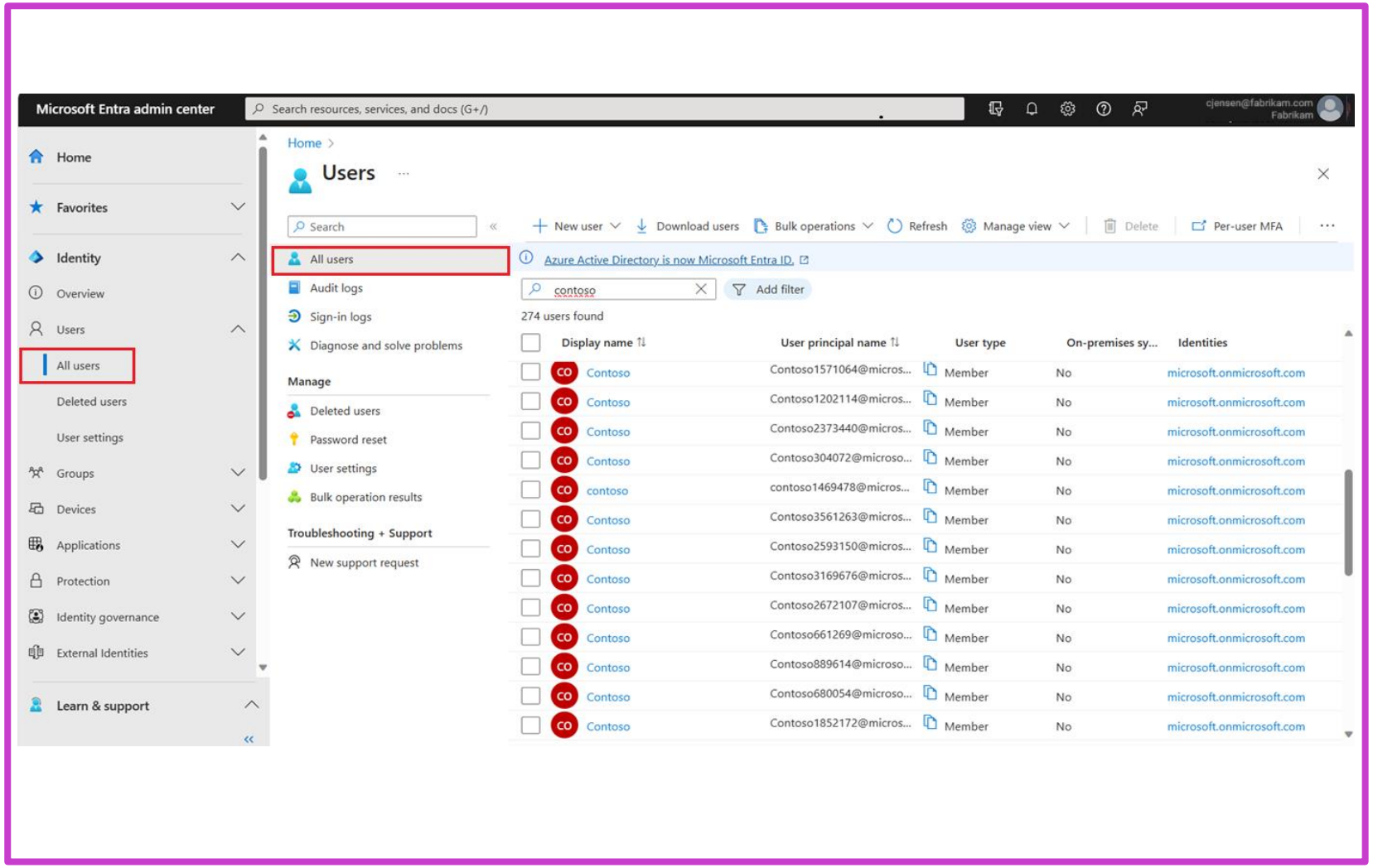
Microsoft Entra ID

- Microsoft Entra ID enables access to both external (e.g., Microsoft 365, Azure) and internal resources, offering role-based benefits for IT admins and app developers.
- Offers free and paid licenses (P1, P2) enhancing security, access management, and supports hybrid user access with advanced administration features.
- Supports a wide range of features including application management, authentication, B2B/B2C interactions, Conditional Access, and identity protection.



Microsoft Entra ID – users

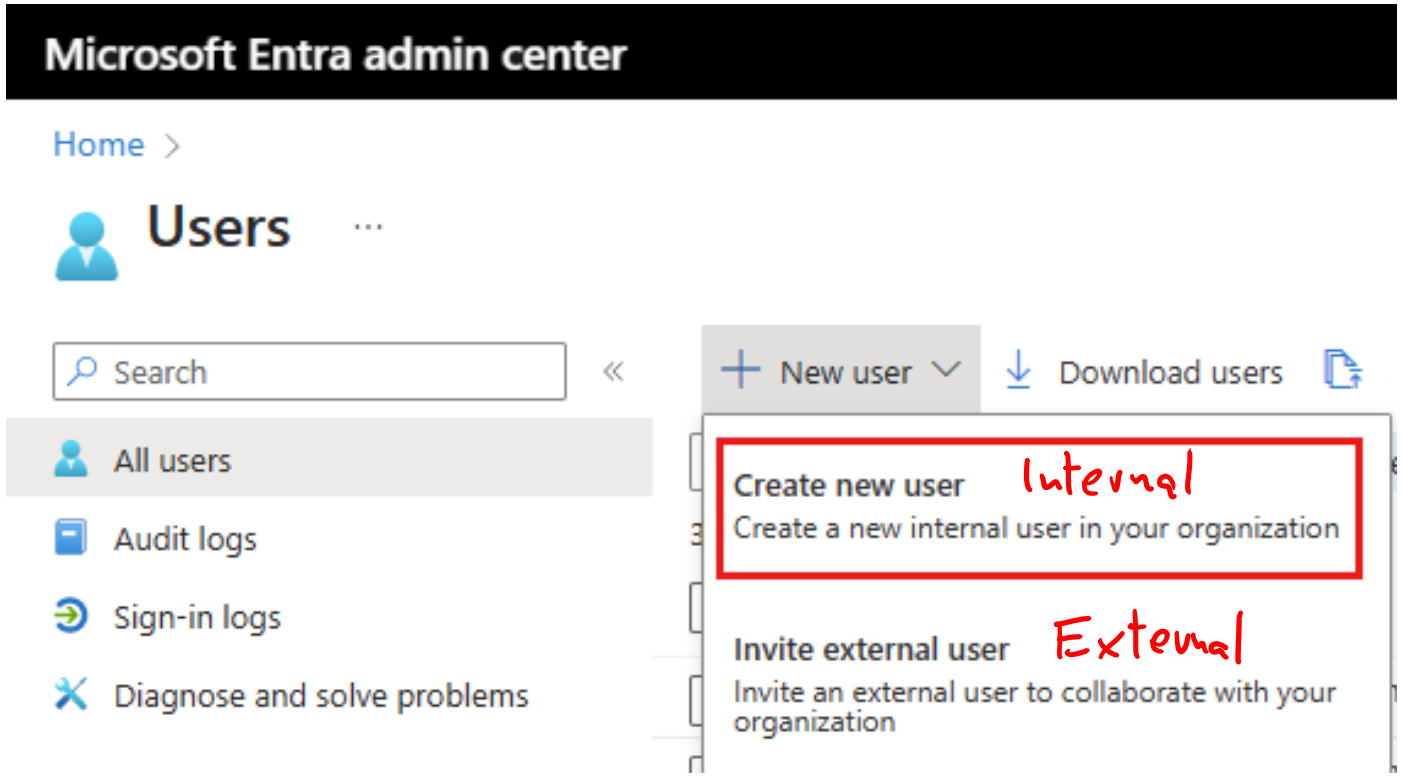
- Microsoft Entra ID supports creating internal members, internal guests, external members, and external guests, each with specific access levels.
- Authentication methods differ: internal users manage passwords within the tenant, while external users rely on their home tenant or self-setup.
- External member access is authenticated via federation, and password management is handled by their home tenant's administrators.



Microsoft Entra ID – Types of users

Type	Definition
Internal member	These users are most likely full-time employees in your organization.
Internal guest	These users have an account in your tenant but have guest-level privileges. It's possible they were created within your tenant prior to the availability of B2B collaboration.
External member	These users authenticate using an external account but have member access to your tenant. **Note:** These types of users are common in multitenant organizations.
External guest	These users are true guests of your tenant who authenticate using an external method and who have guest-level privileges.

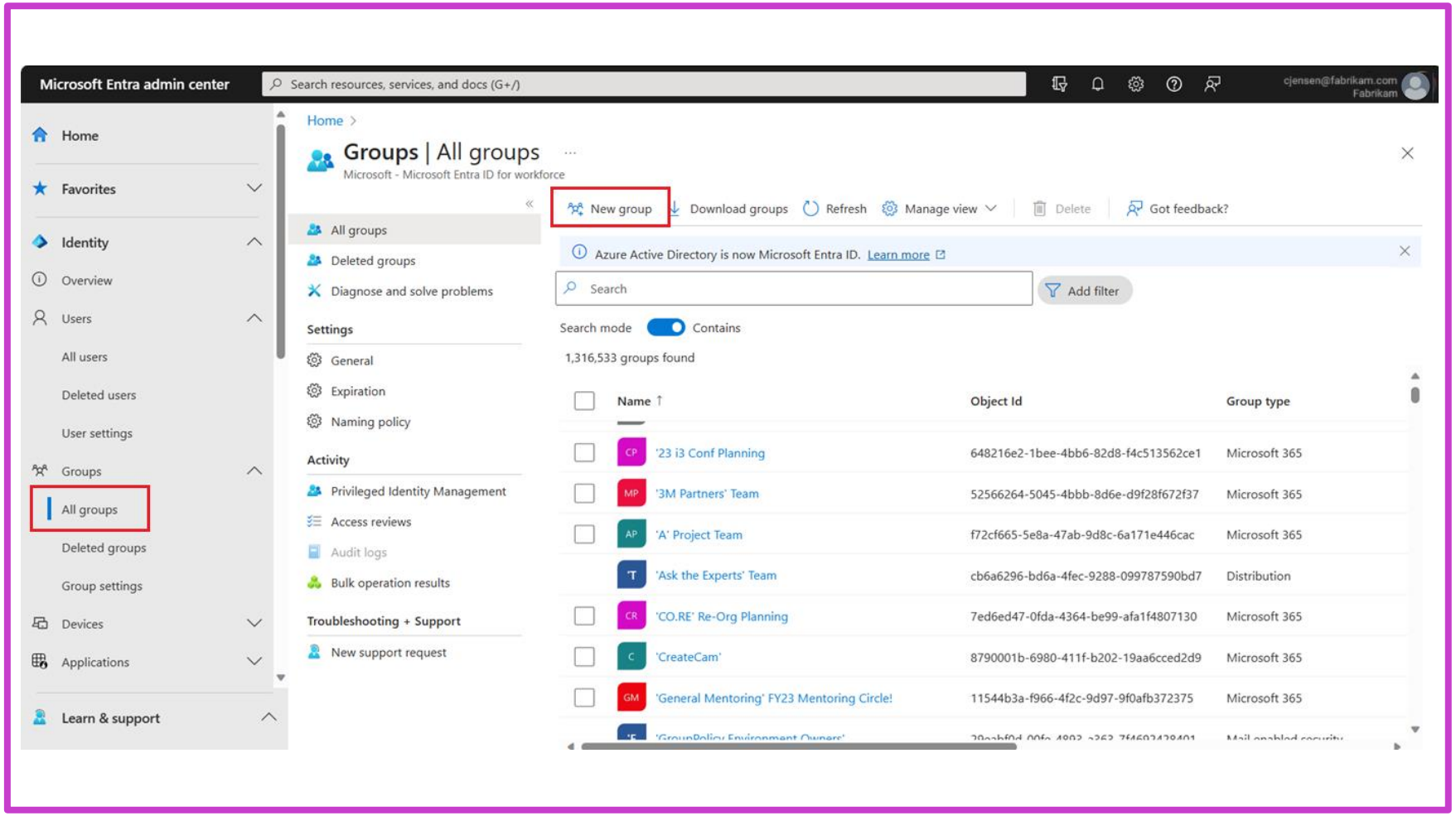
Microsoft Entra ID – Create a new user



Sign in to the Microsoft Entra admin center as at least a User Administrator.

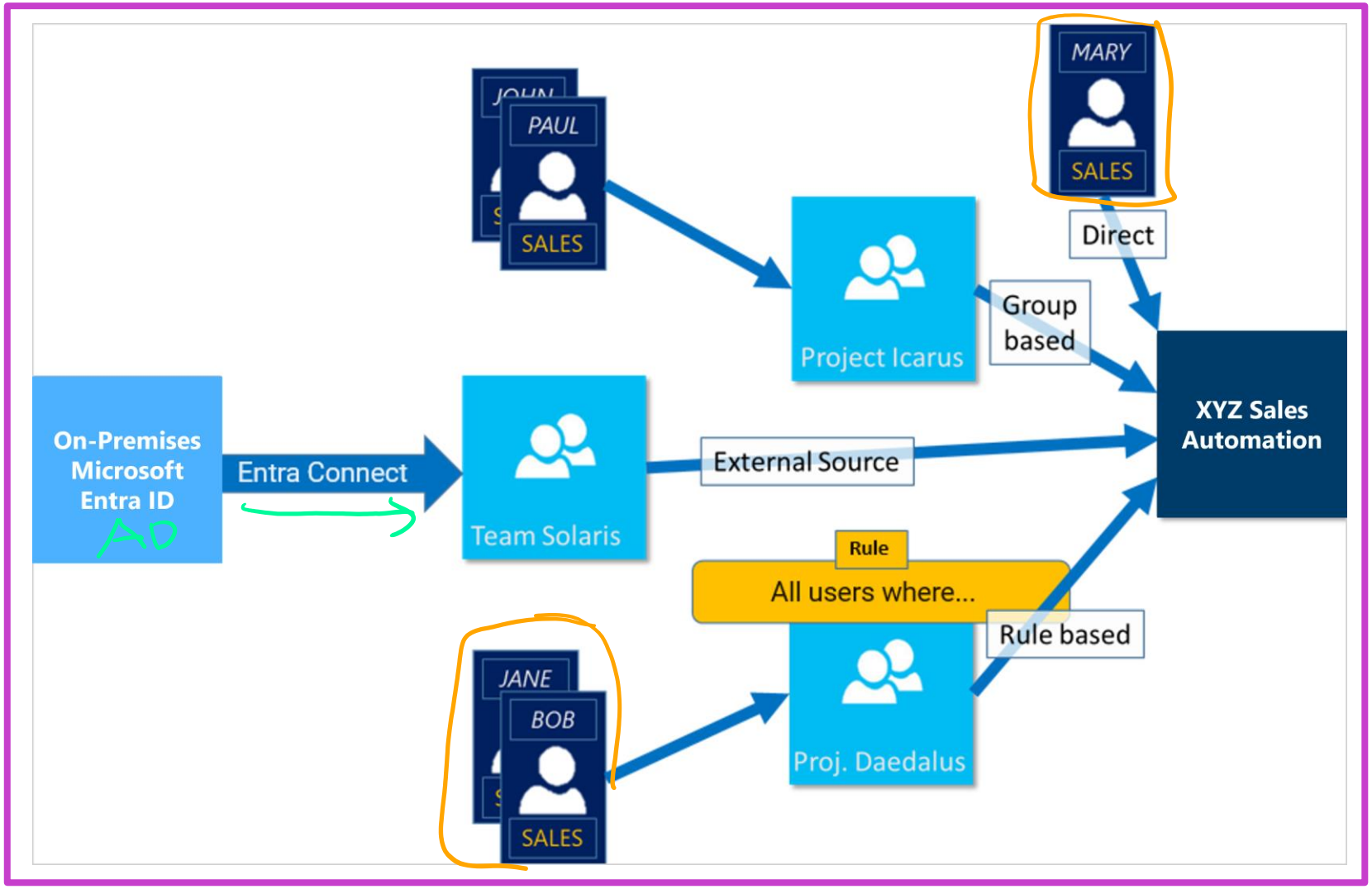
Microsoft Entra ID groups

- Microsoft Entra ID manages access with groups for applications, data, and tasks.
- Groups cater to both internal and external resources, with various management options.
- Access assignment includes direct, group, and rule-based methods, plus dynamic memberships.



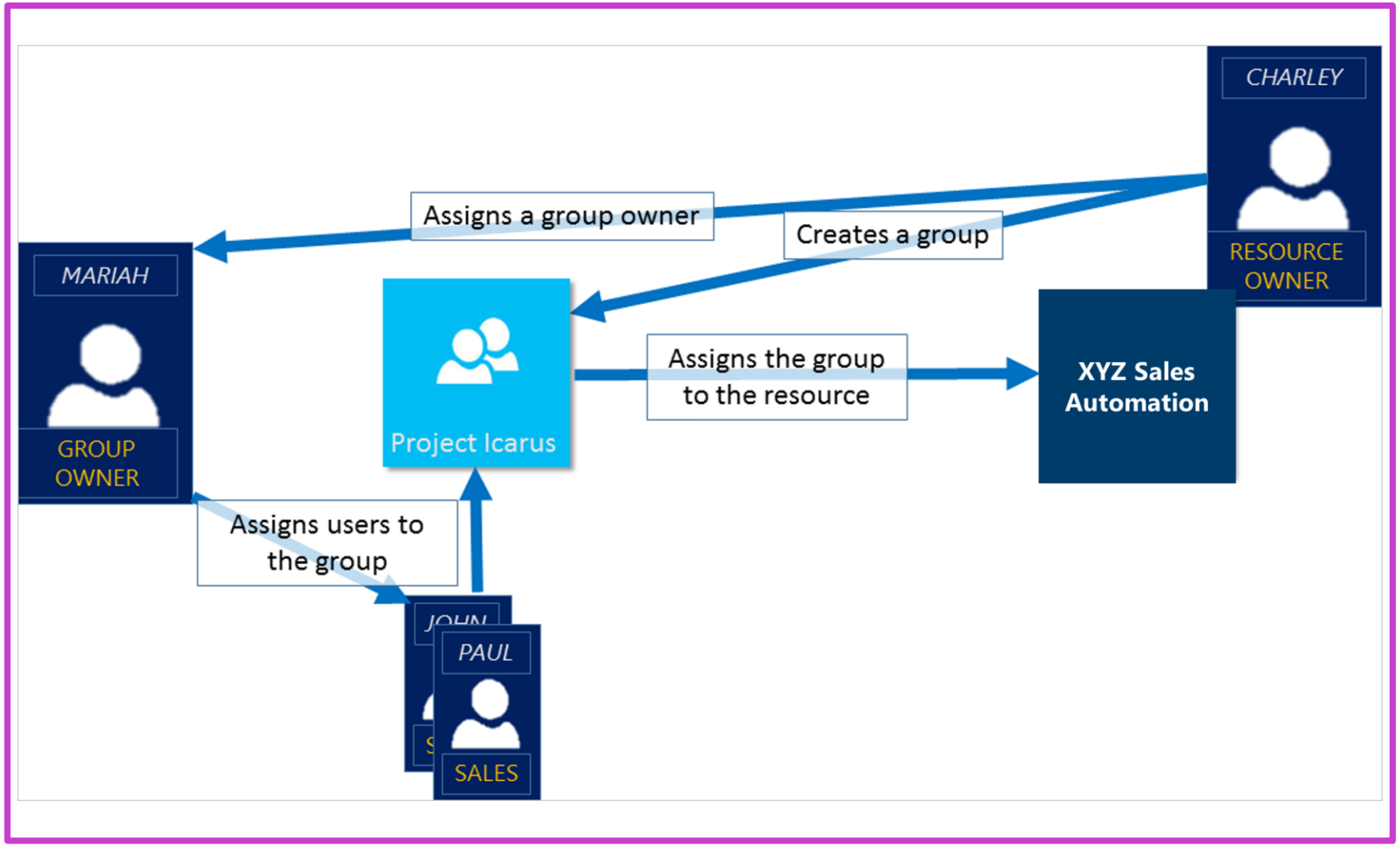
How access management in Microsoft Entra ID works

- Microsoft Entra ID facilitates access rights assignment to individual users or entire groups.
- Groups allow for bulk permission assignments by resource or directory owners.
- Management rights can be delegated for adding or removing group members.



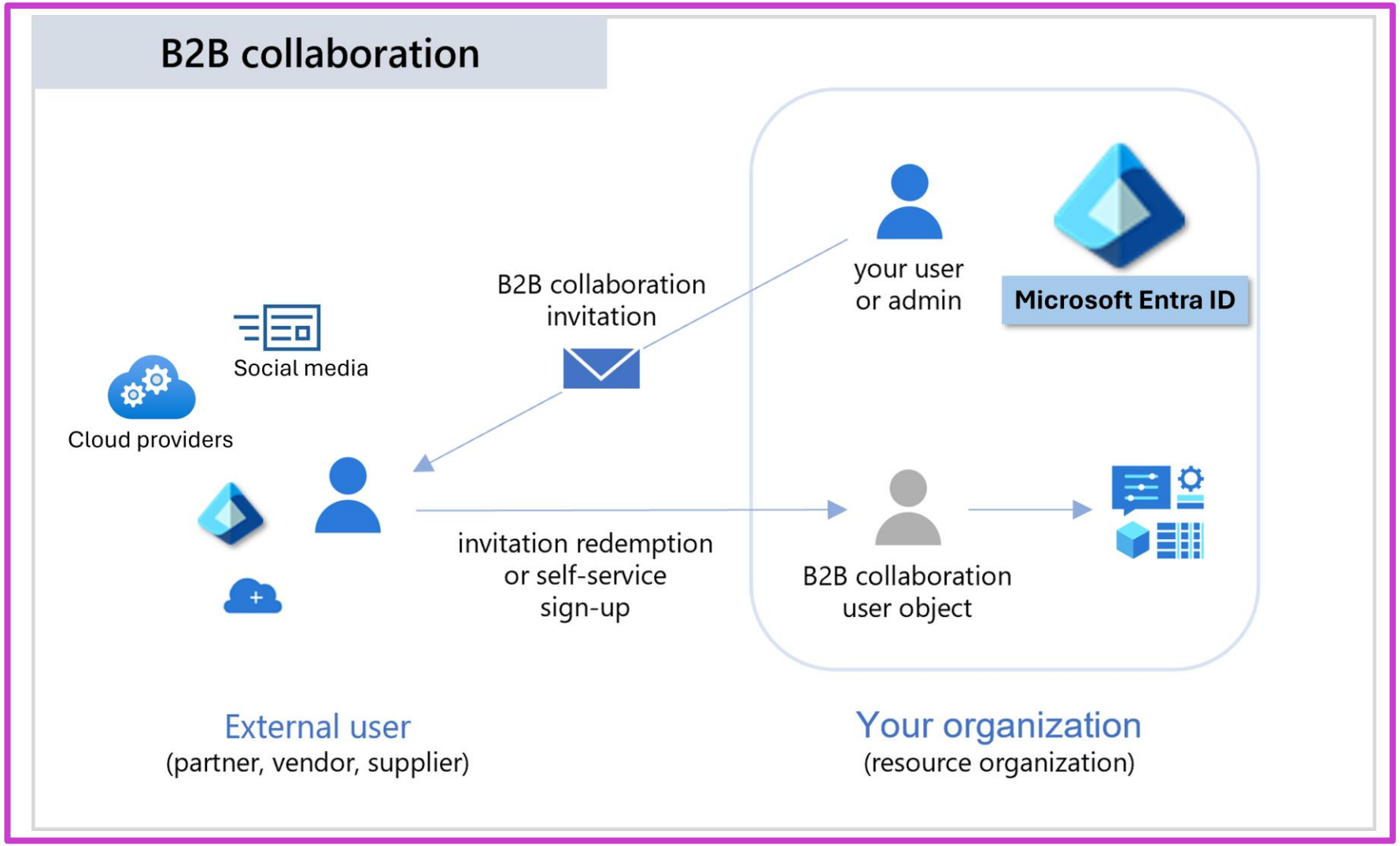
Ways to assign access rights

- Direct assignment allows resource owners to assign users individually to resources.
- Group assignment grants access to all members of a Microsoft Entra group, with managed membership.
- Rule-based and external authority assignments utilize user attributes and external sources for access control.



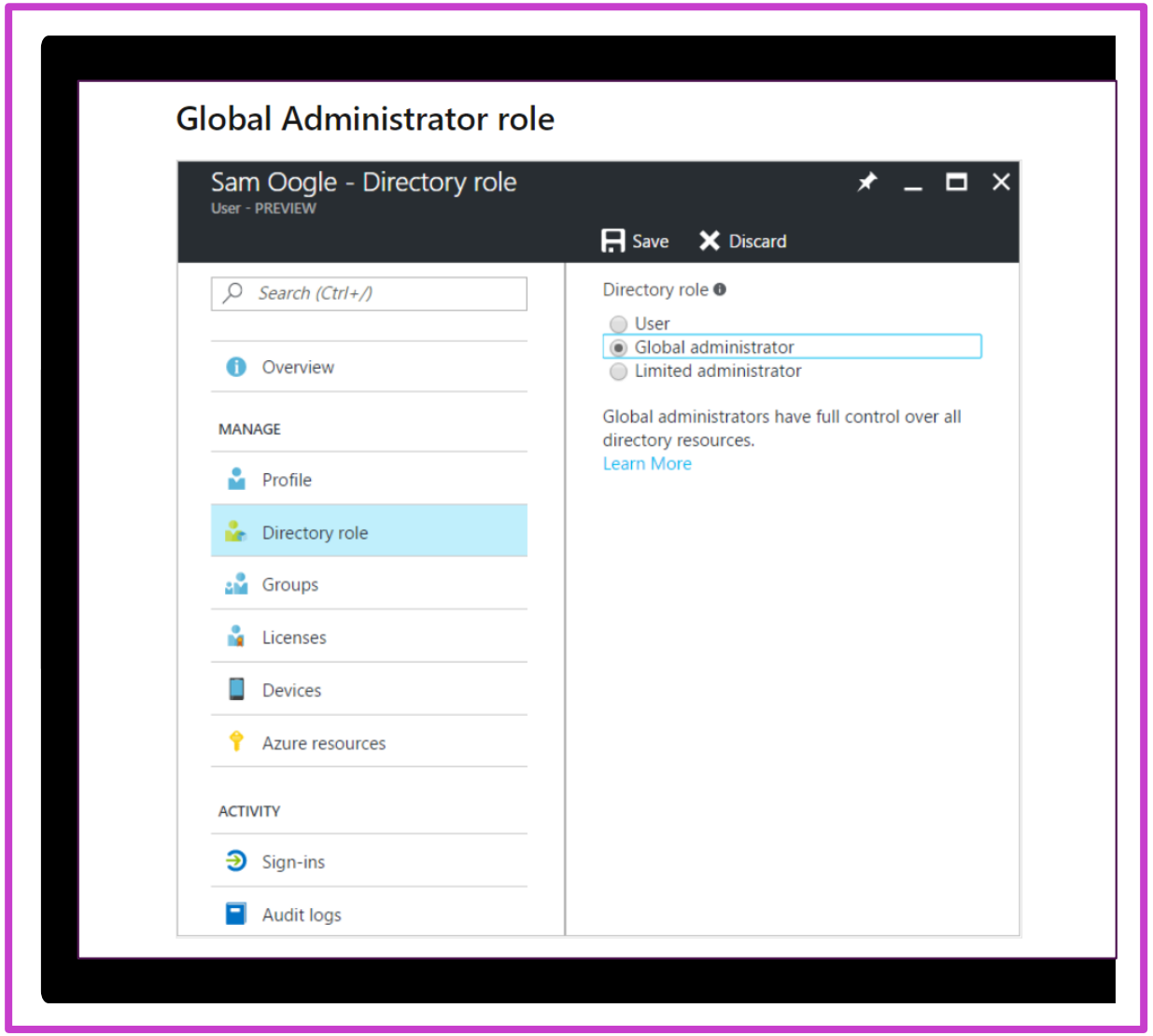
Microsoft Entra External ID

- Entra External ID allows secure interactions with external identities for resource access.
- Includes B2B collaboration/direct connect, Azure AD B2C, and cross-tenant sync.
- Managed in Azure, supports self-sign-up, and customizable access/collaboration settings.



Recommend when to use external identities

- Microsoft Entra ID B2B collaboration users are added as guest users to the directory, and guest permissions in the directory are restricted by default.
- Your business may need some guest users to fill higher-privilege roles in your organization.
- To support defining higher-privilege roles, guest users can be added to any roles you desire, based on your organization's needs.



Secure external identities

Remember the following security policy and compliance management aspects:

For B2B collaboration and B2B direct connect: Managed by the host/inviting organization, using features such as Conditional Access policies and cross-tenant access settings.

For Microsoft Entra ID B2C: Managed by the organization via Conditional Access and Identity Protection.

Use the following features to secure external identities:

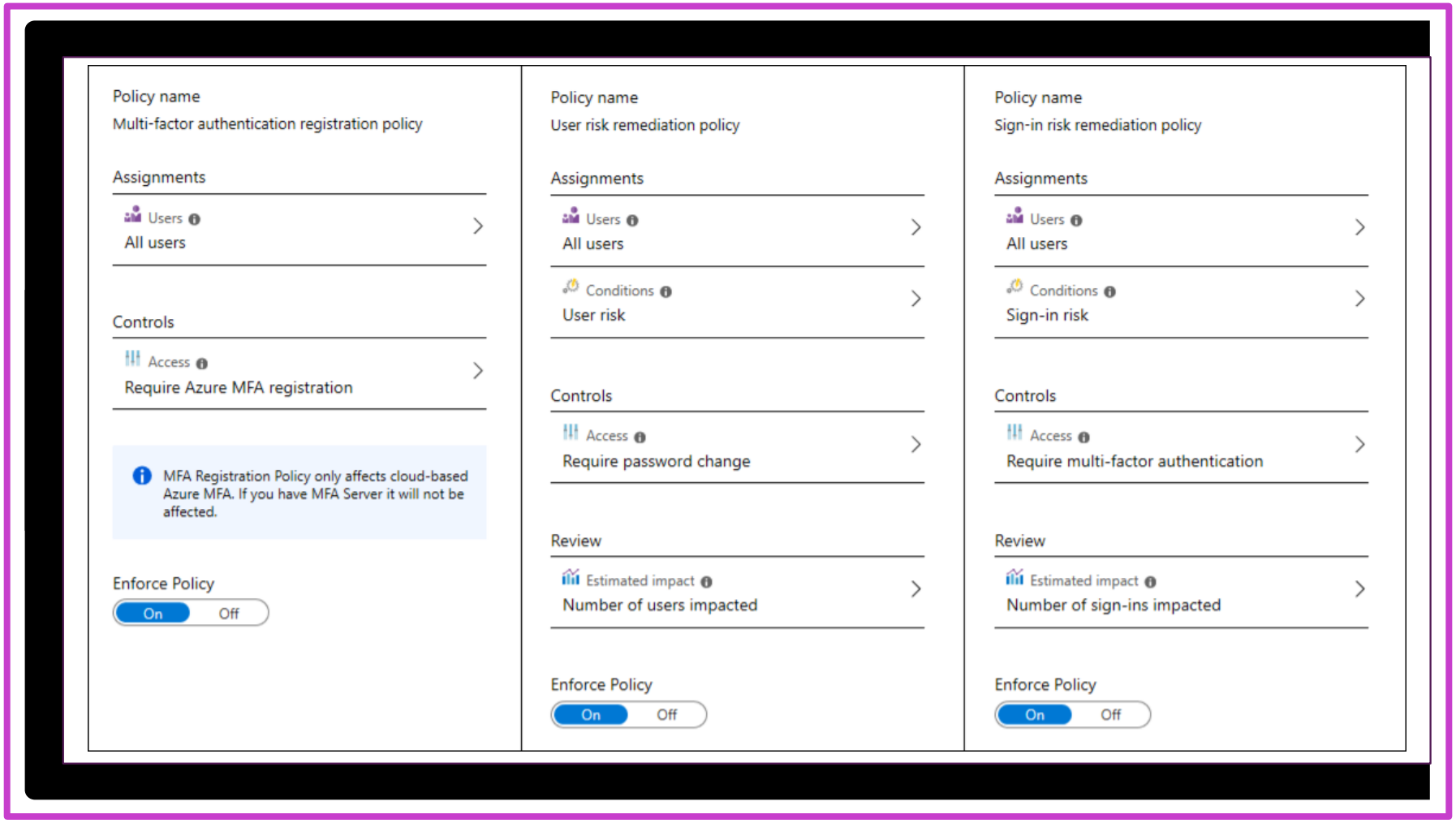
- Microsoft Entra ID entitlement management for B2B guest user sign-up
- Microsoft Entra ID Microsoft Graph API for B2B collaboration
- Conditional Access policies
- Multitenant applications

Implement Microsoft Entra ID identity protection

Automate the detection and remediation of identity-based risks

Investigate risks using data in the portal

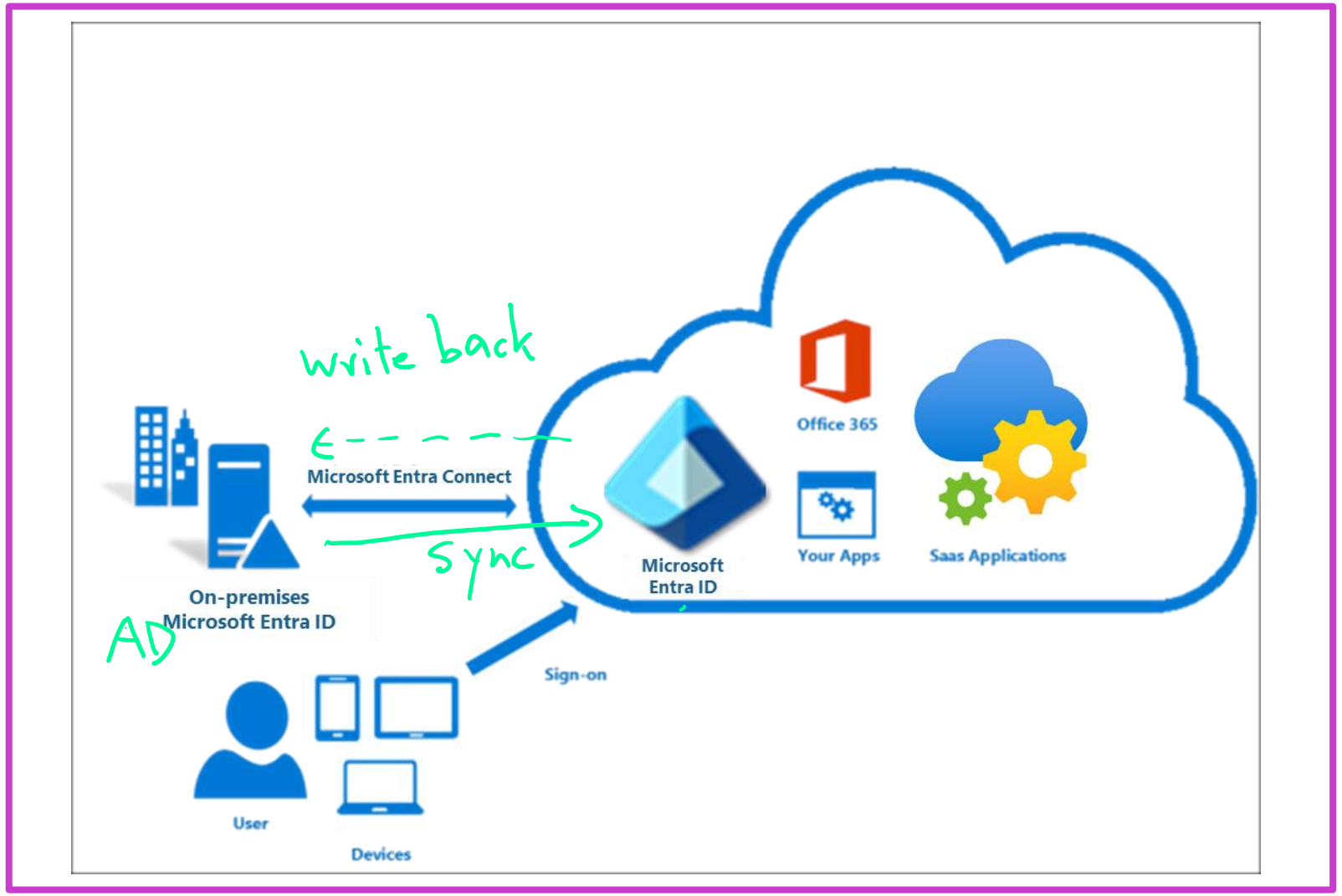
Export risk detection data to third-party utilities for further analysis



Manage authentication by using Microsoft Entra ID

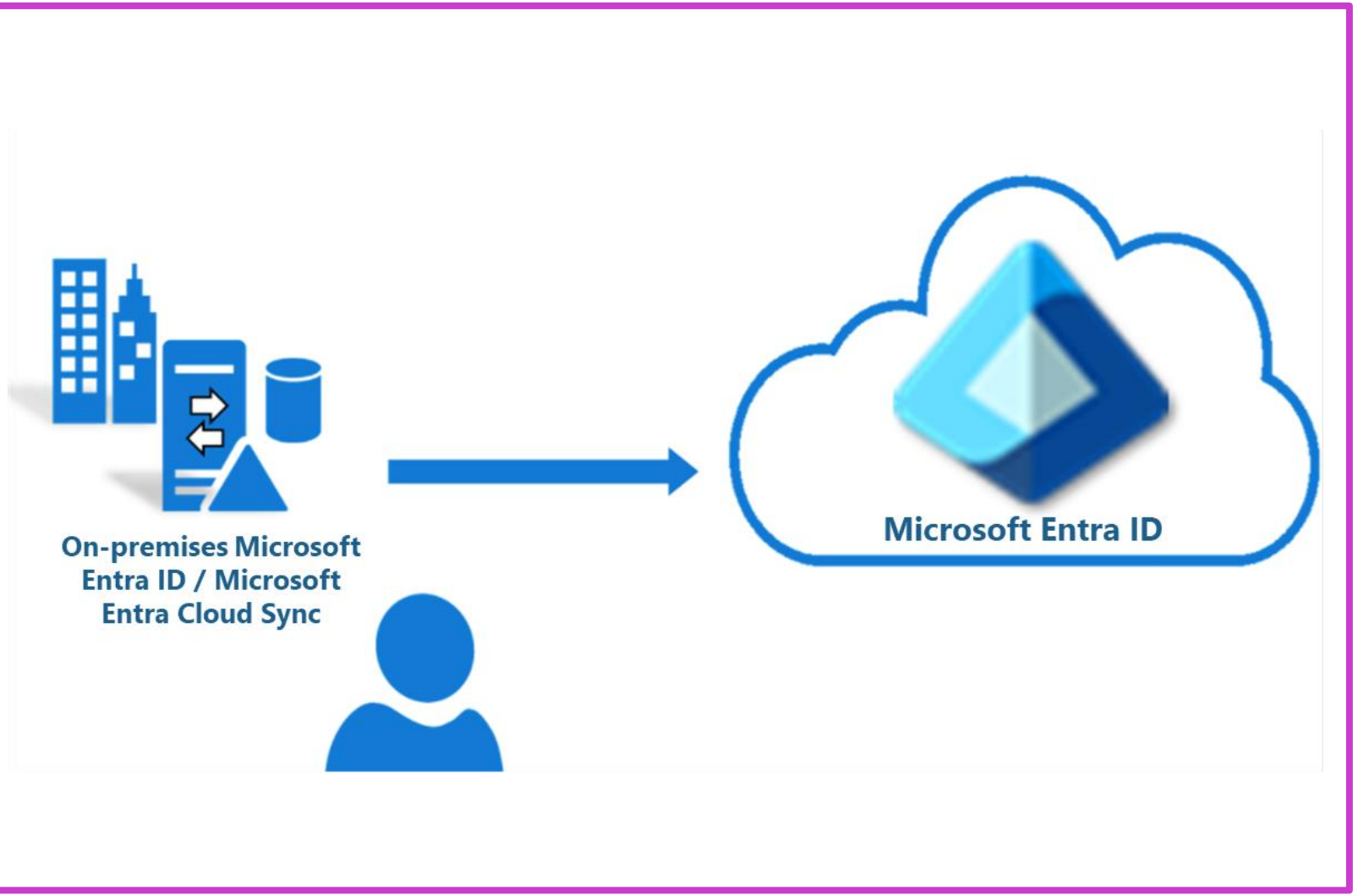
Microsoft Entra connect

- Microsoft Entra Connect: On-premises application for hybrid identity goals; consider cloud-managed solution Microsoft Entra Cloud Sync.
- Features: Password hash sync, pass-through auth, federation integration, synchronization, health monitoring.
- Microsoft Entra Connect Health: Robust monitoring for on-premises identity infrastructure, ensuring reliability for accessing Microsoft 365 and Online Services.



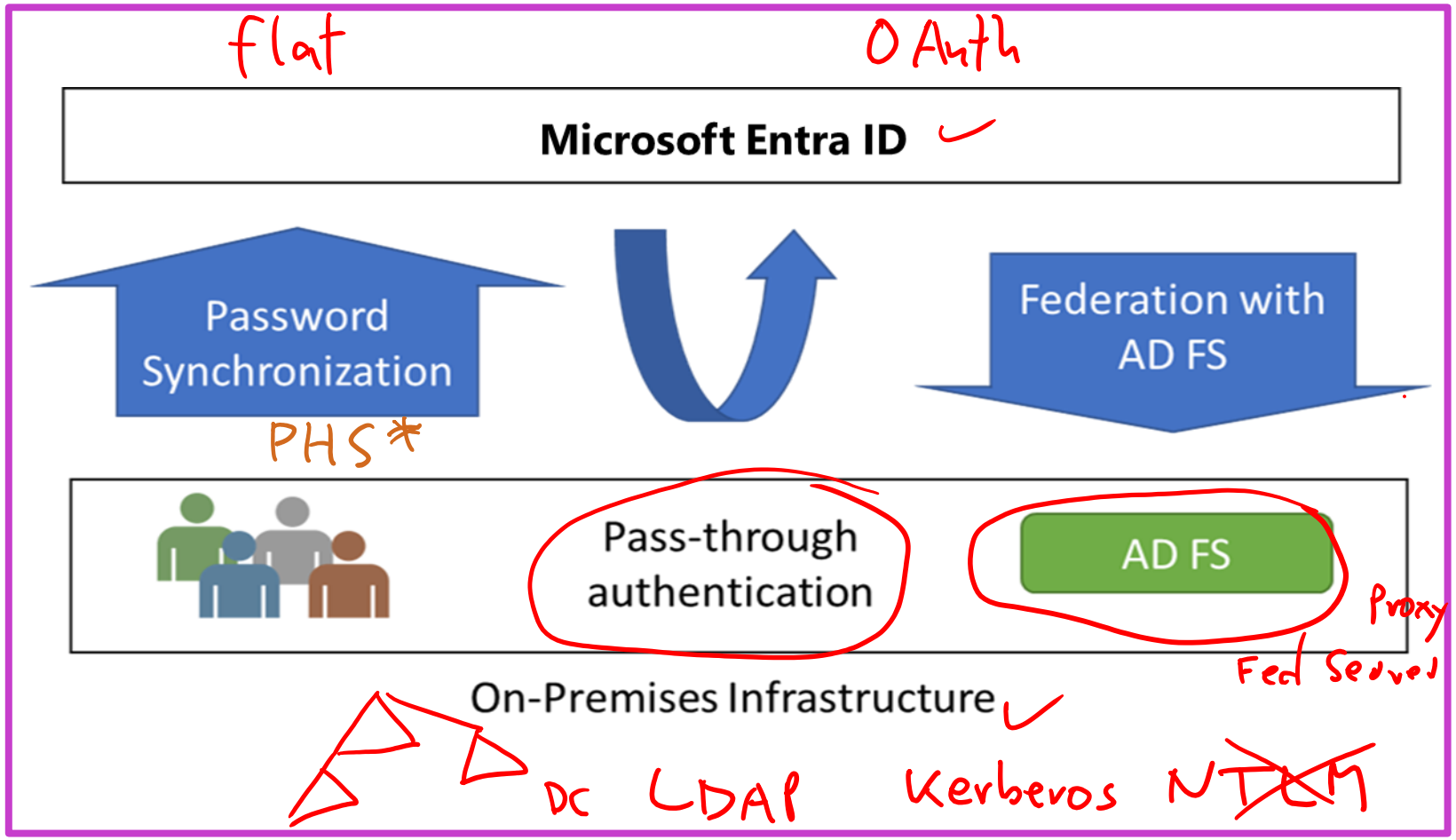
Microsoft Entra cloud sync

- Microsoft Entra Cloud Sync: Hybrid identity solution, synchronizes users, groups, and contacts to Microsoft Entra ID.
- Benefits: Supports multi-forest environments, simplified installation, multiple agents for high availability.
- Different from Entra Connect Sync: Orchestration in Online Services, lightweight agent deployment, configuration stored in Entra ID.

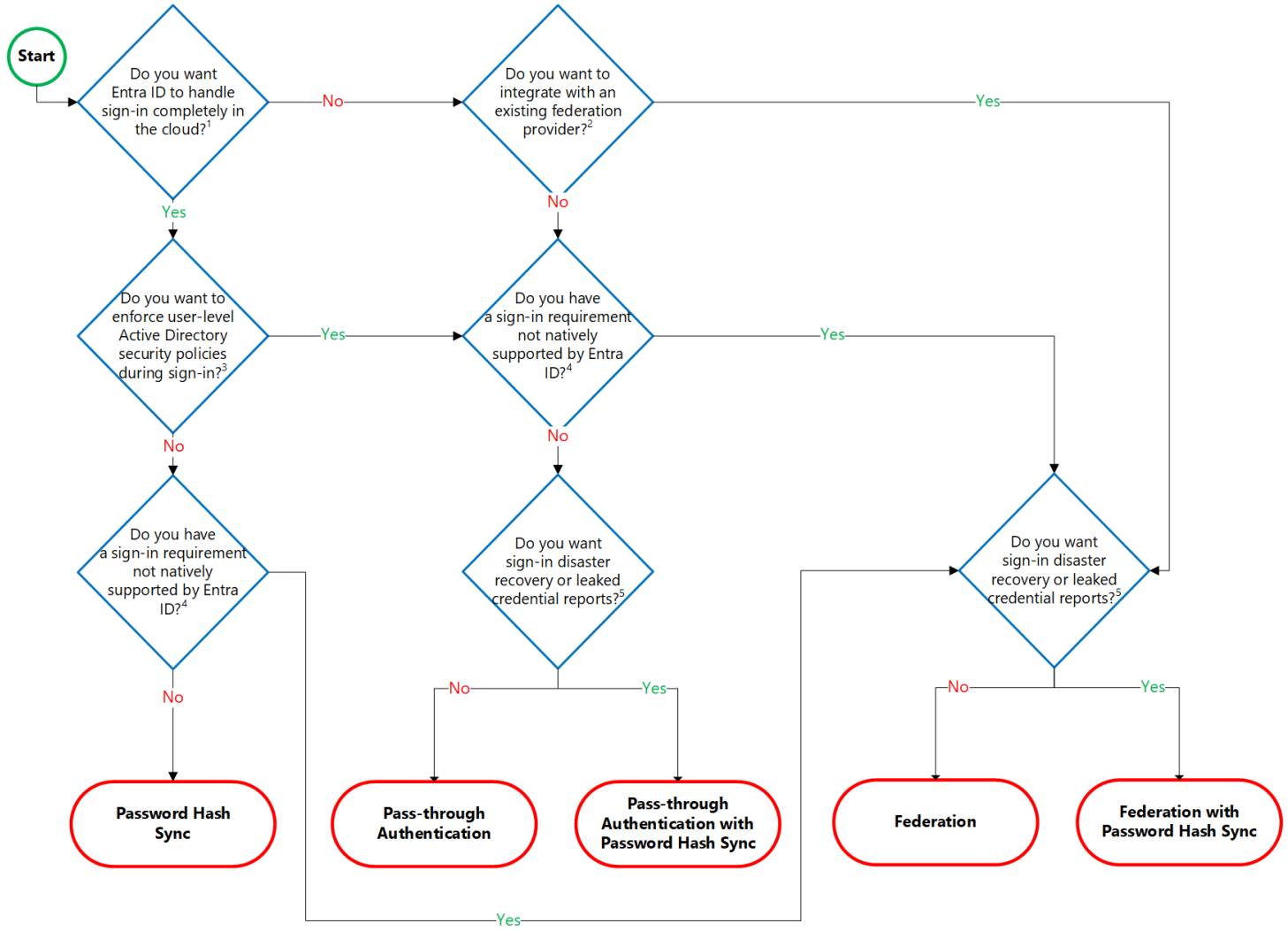


Authentication options

- **Password Hash Synchronization**:
  - Minimal effort, seamless sign-in.
  - Ensures business continuity.
  - Considerations for on-premises account states.
- **Pass-through Authentication**:
  - Lightweight agent deployment.
  - Enhanced user experience, enforced policies.
  - Backup authentication method recommended.
- **Federated Authentication**:
  - Requires external system, complex.
  - Flexible user experience, advanced scenarios.
  - High investment, single identity provider.

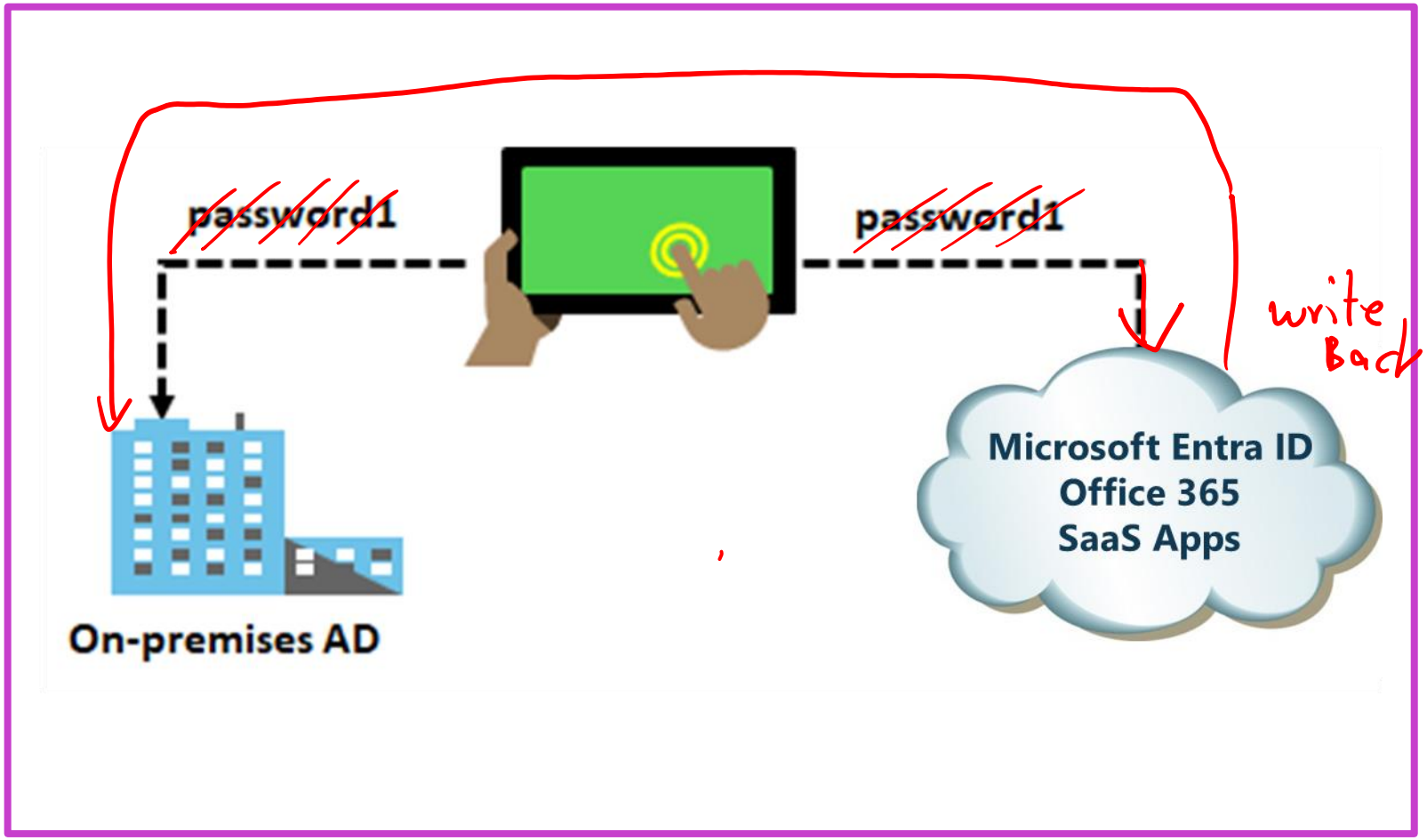


Authentication decision tree



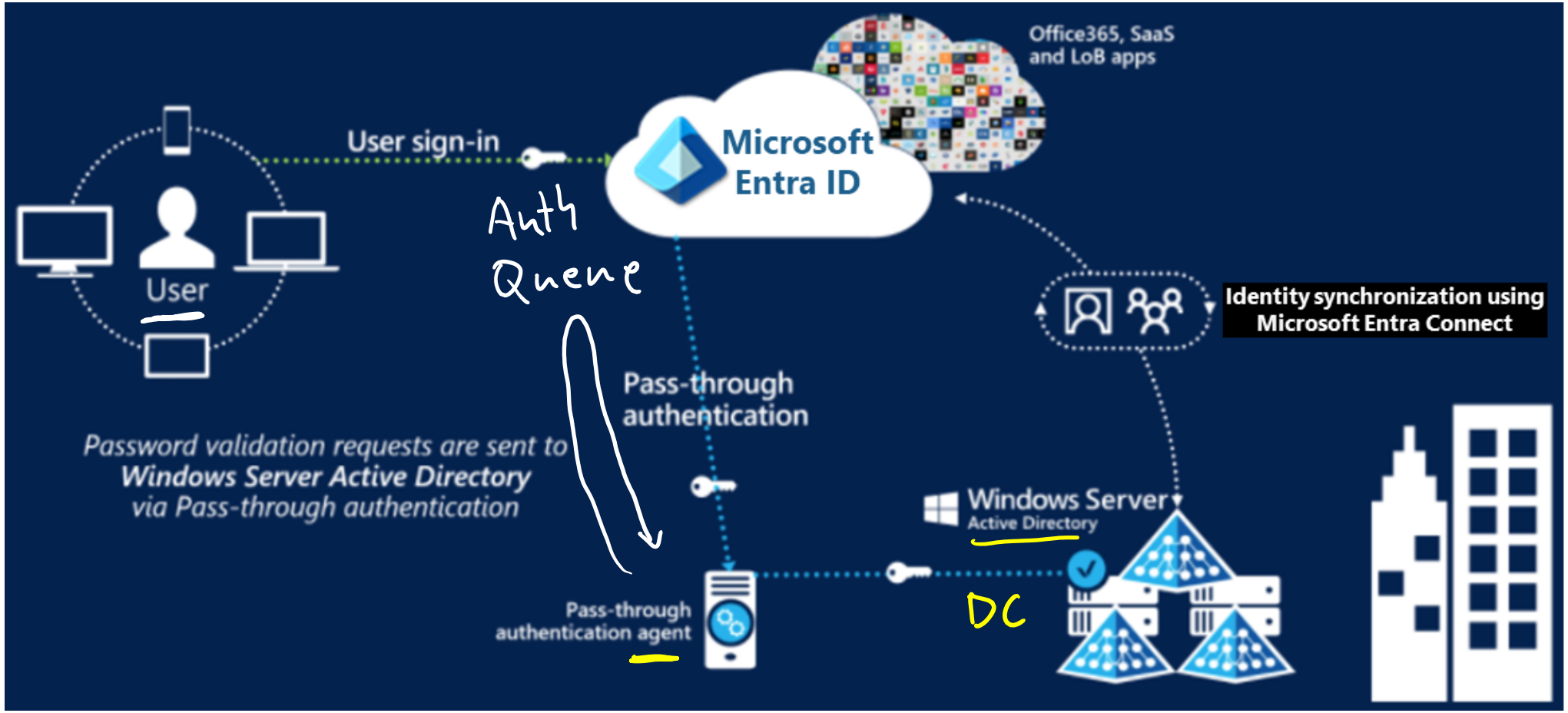
Password hash synchronization with Microsoft Entra ID

- Password hash synchronization simplifies sign-in for hybrid identity.
- Benefits include improved productivity, reduced helpdesk costs, and leaked credential detection.
- It requires setup with Microsoft Entra Connect and configuration of directory synchronization.



Pass-through authentication

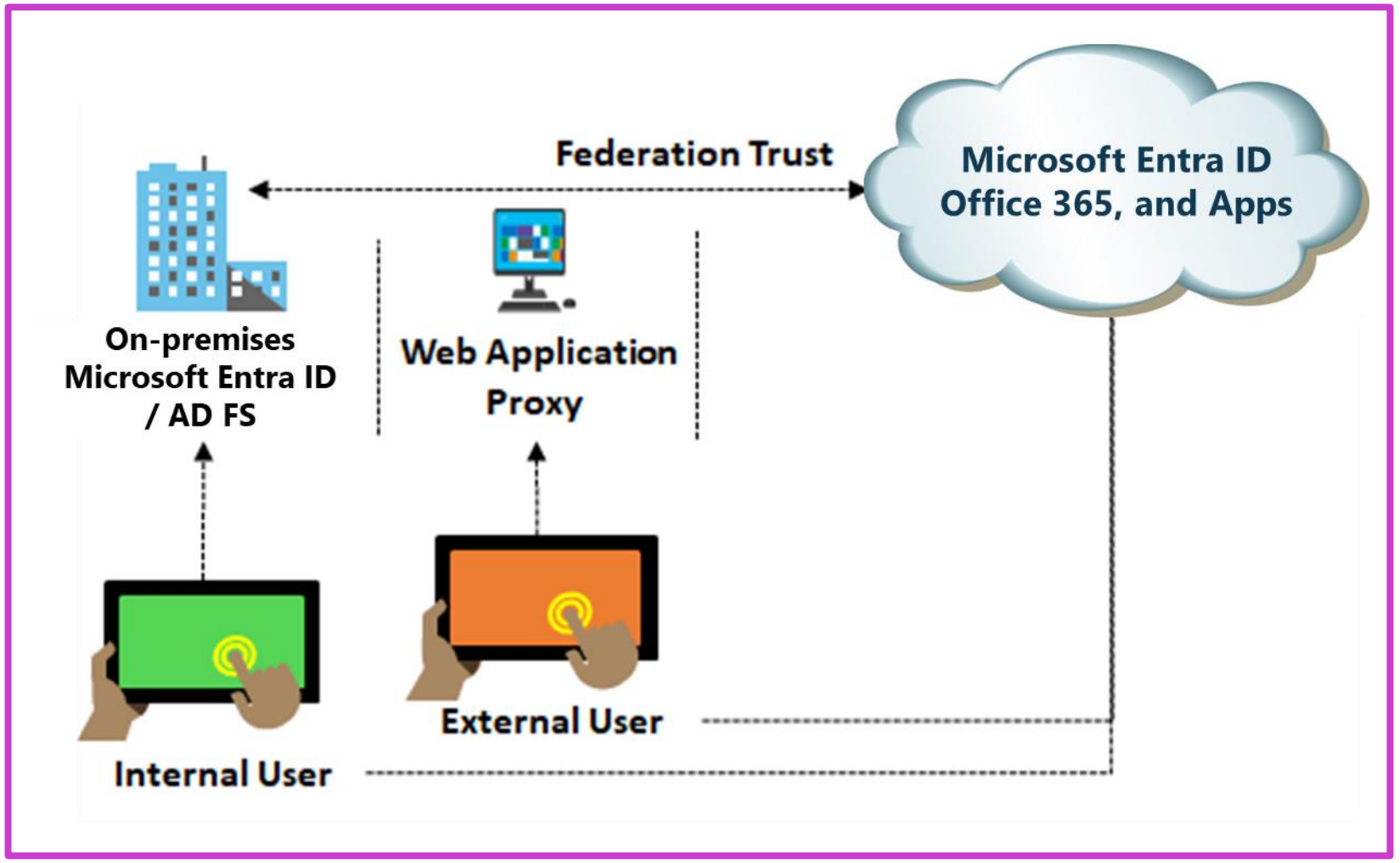
PTA



- Password hash synchronization: Hybrid identity sign-in method.
- Reduces passwords, boosts productivity, cuts helpdesk costs.
- Enables leaked credential detection, integrates with AD FS.

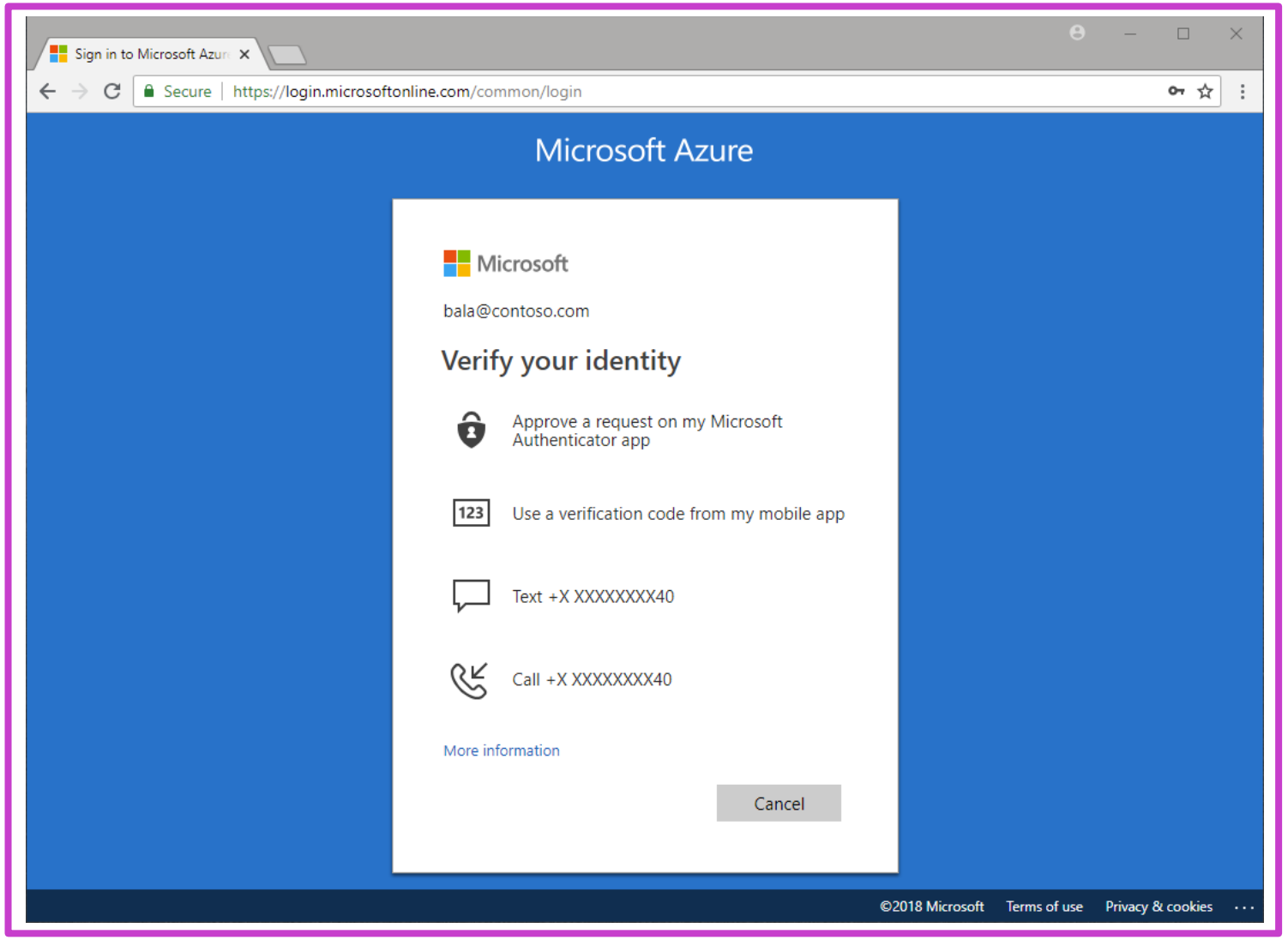
Federation with Microsoft Entra ID

- Federation: Trust between domains for authentication and authorization, vital for shared resource access across organizations.
- Federate on-premises with Microsoft Entra ID for robust access control, ensuring all authentication happens locally.
- Microsoft Entra Connect facilitates federation setup with AD FS, allowing seamless sign-in to Entra ID services without password re-entry.



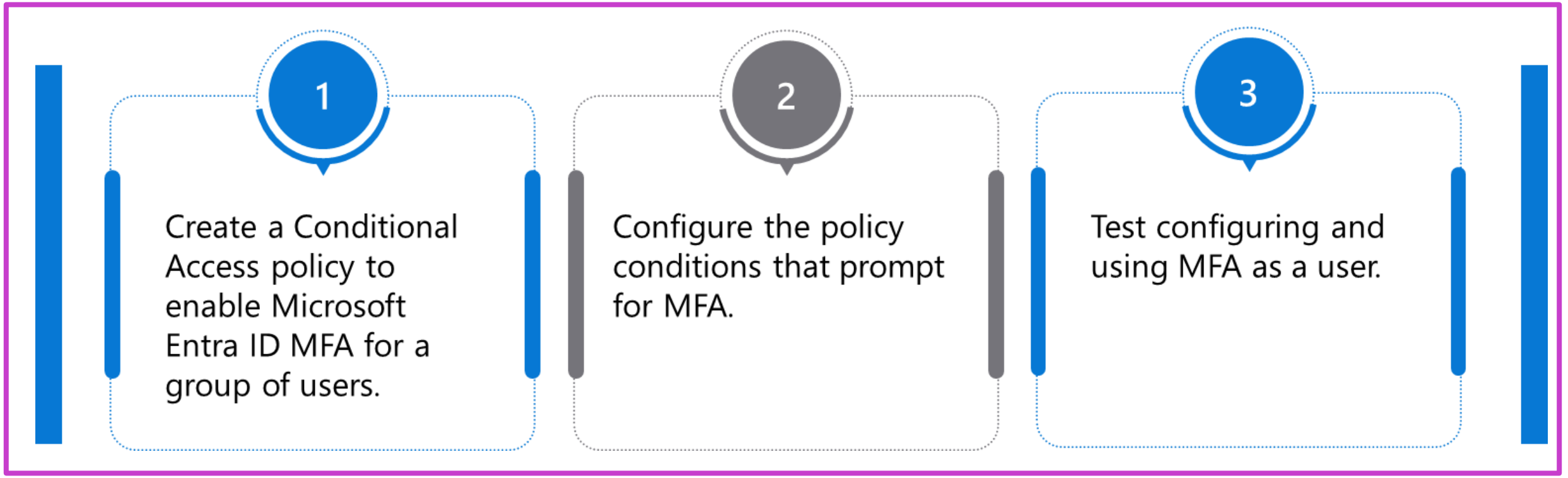
Microsoft Entra authentication

- Microsoft Entra ID enhances security through multifactor authentication, passwordless sign-in, and self-service password reset.
- Hybrid integration ensures password changes and protection policies are applied both on-premises and in the cloud.
- Aims to reduce help desk calls and improve user experience by enabling users to manage their credentials independently.



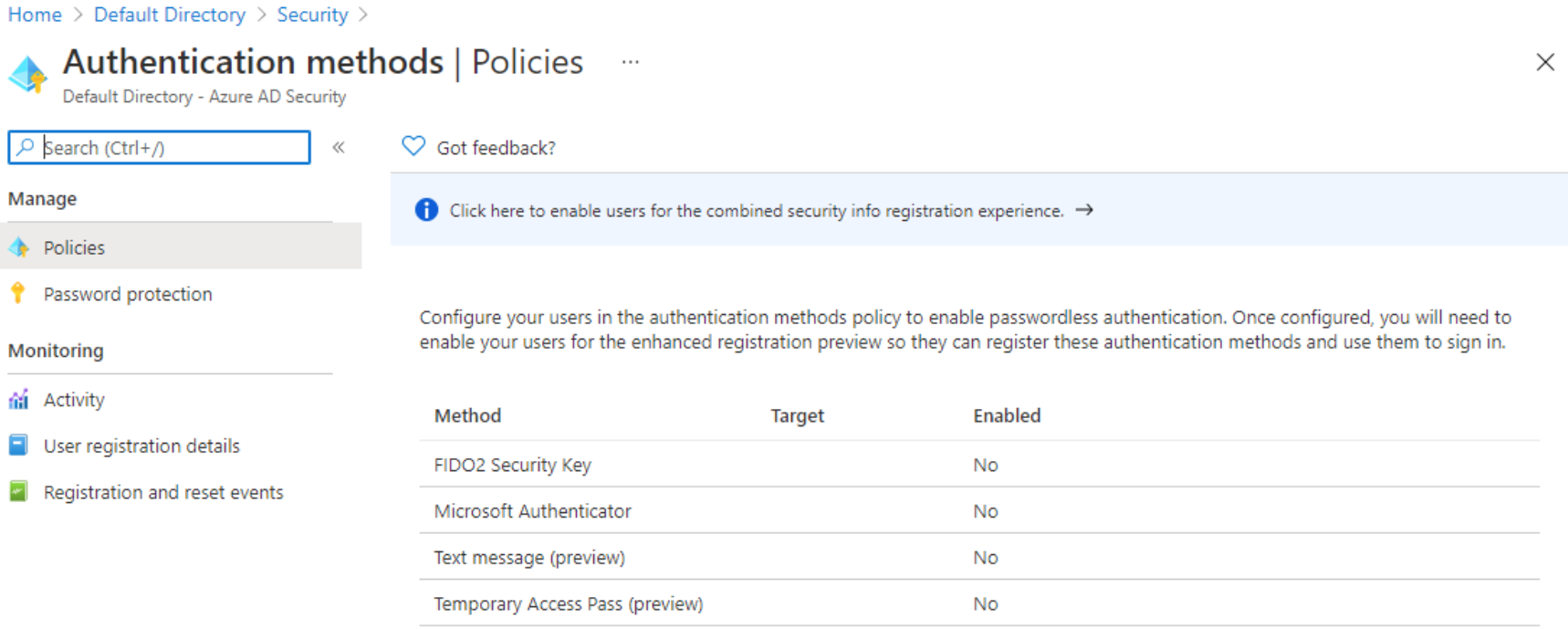
Implement multi-factor authentication (MFA)

Perform the following tasks to implement MFA:



Prioritize the requirement of MFA on sensitive accounts such as Global Admin and Microsoft Entra ID DC Admin.

Passwordless authentication options for Microsoft Entra ID



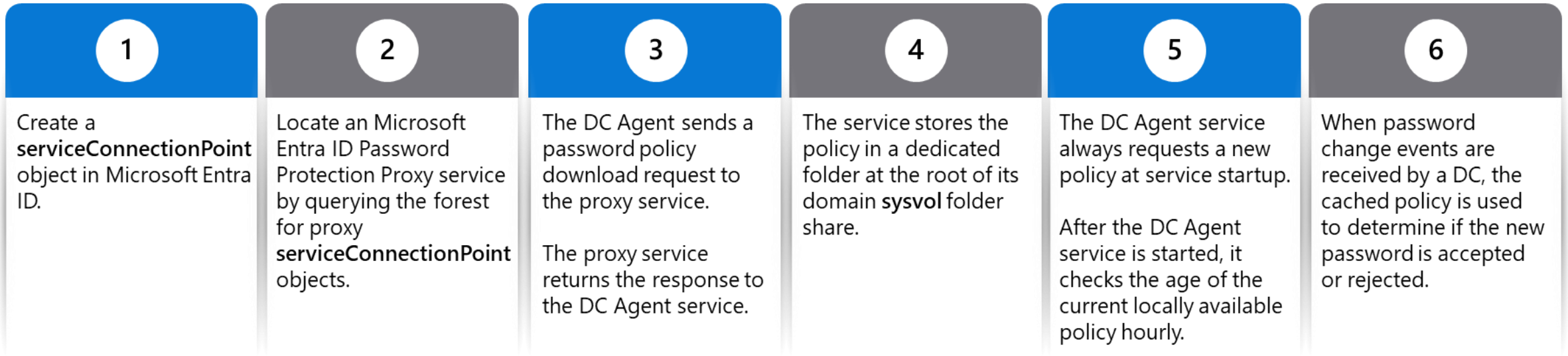
- MFA enhances security; passwordless options reduce user frustration.
- Microsoft Azure offers four passwordless methods: Hello, Authenticator, FIDO2 keys, Certificate-based authentication.
- Each method provides seamless, secure access without traditional passwords.

Implement passwordless authentication

- Microsoft offers passwordless options: Authenticator, Hello, FIDO2 keys, Certificate-based authentication.
- Passwordless methods enhance security, mitigate password attack risks.
- Deployment includes planning, pilot, user registration, and managing through Microsoft Entra admin center.

Implement password protection

The on-premises Microsoft Entra ID Password Protection components work as follows:



Single sign-on

- SSO allows one set of credentials for multiple systems, simplifying user access across applications.
- Options for SSO include federation protocols, password-based, linked-based, or disabling SSO based on application needs.
- Planning SSO deployment is crucial, considering application hosting and access requirements for seamless integration.

Implement single sign-on (SSO)

Implementing single sign-on (SSO) in Microsoft Entra ID entails:

Roles: Opt for roles with the least permissions necessary and review periodically.

Certificates: Regularly renew and manage the SAML application certificate with a structured process.

Communications: Keep users informed about SSO changes and provide support guidelines.

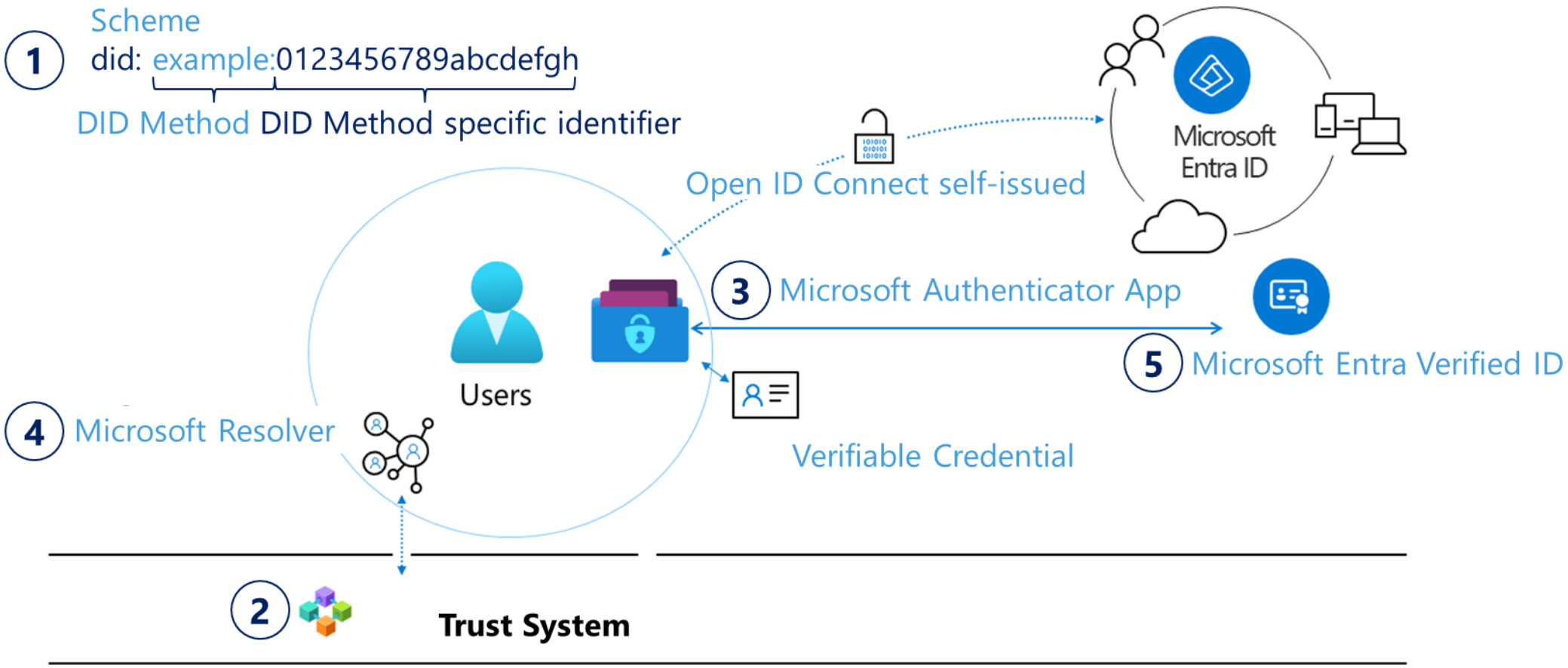
Licensing & Shared Accounts: Ensure proper licensing for Microsoft Entra ID and applications, and securely manage shared account passwords.

Integrate single sign-on and identity providers

- You can integrate your cloud-enabled software as service (SaaS) applications with Microsoft Entra ID.
- Refer to the Microsoft Entra ID Marketplace for a list of all SaaS apps that have been pre-integrated into Microsoft Entra ID.
- Use the application network portal to request:
  - A System for Cross-Domain Identity Management (SCIM) enabled application to be added to the gallery for automatic provisioning or
  - A Security Assertion Markup Language (SAML) / OpenID Connect (OIDC) enabled application to be added to the gallery for SSO.
- Once you add the application from the gallery, configure and test Microsoft Entra ID SSO for the application.

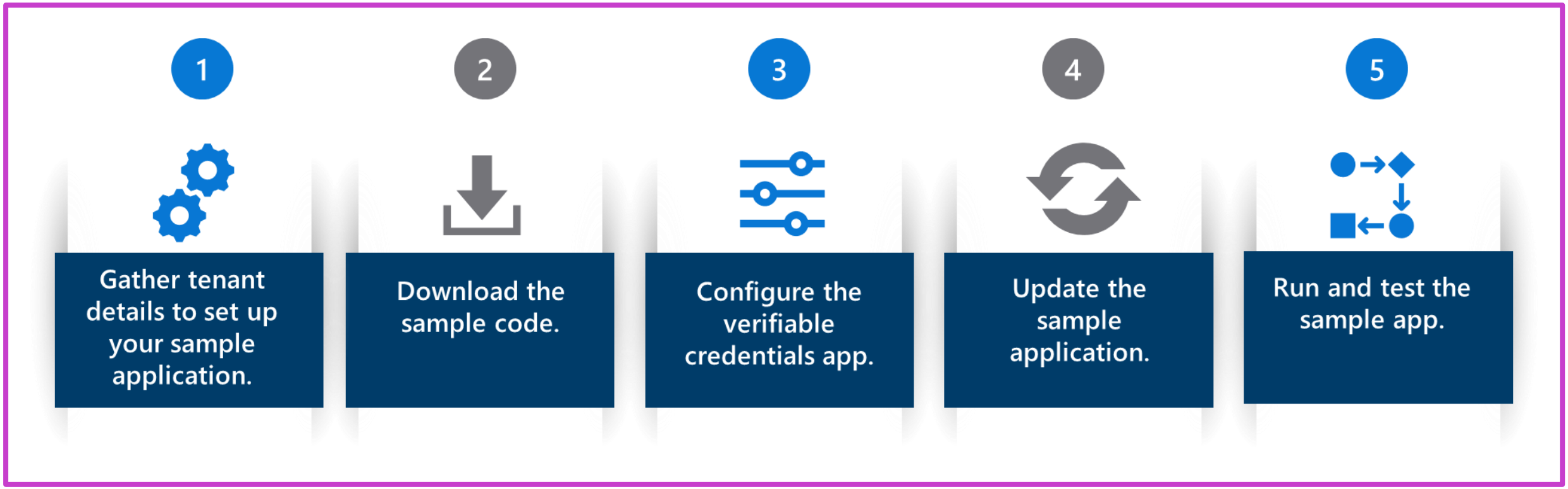
Introduction to Microsoft Entra Verified ID

Microsoft Entra Verified ID is a part of the Entra suite of identity and access management solutions. It's focused on establishing and managing decentralized identities.



Configure Microsoft Entra Verified ID verifier

Complete the following steps to present and verify your Microsoft Entra Verified ID for a sample application:

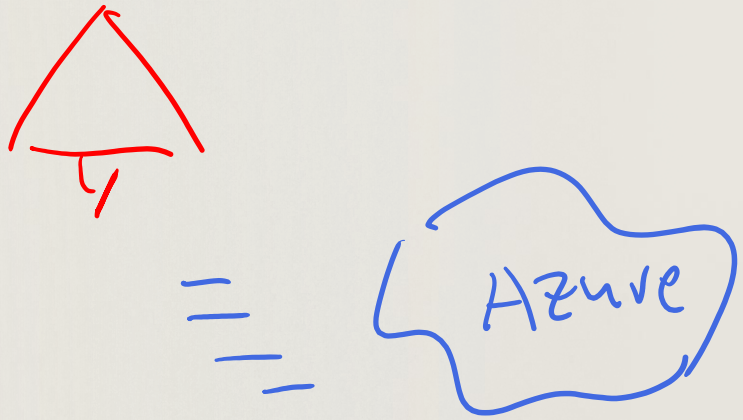


Recommend and enforce modern authentication protocols

Microsoft recommends the following passwordless authentication protocols.

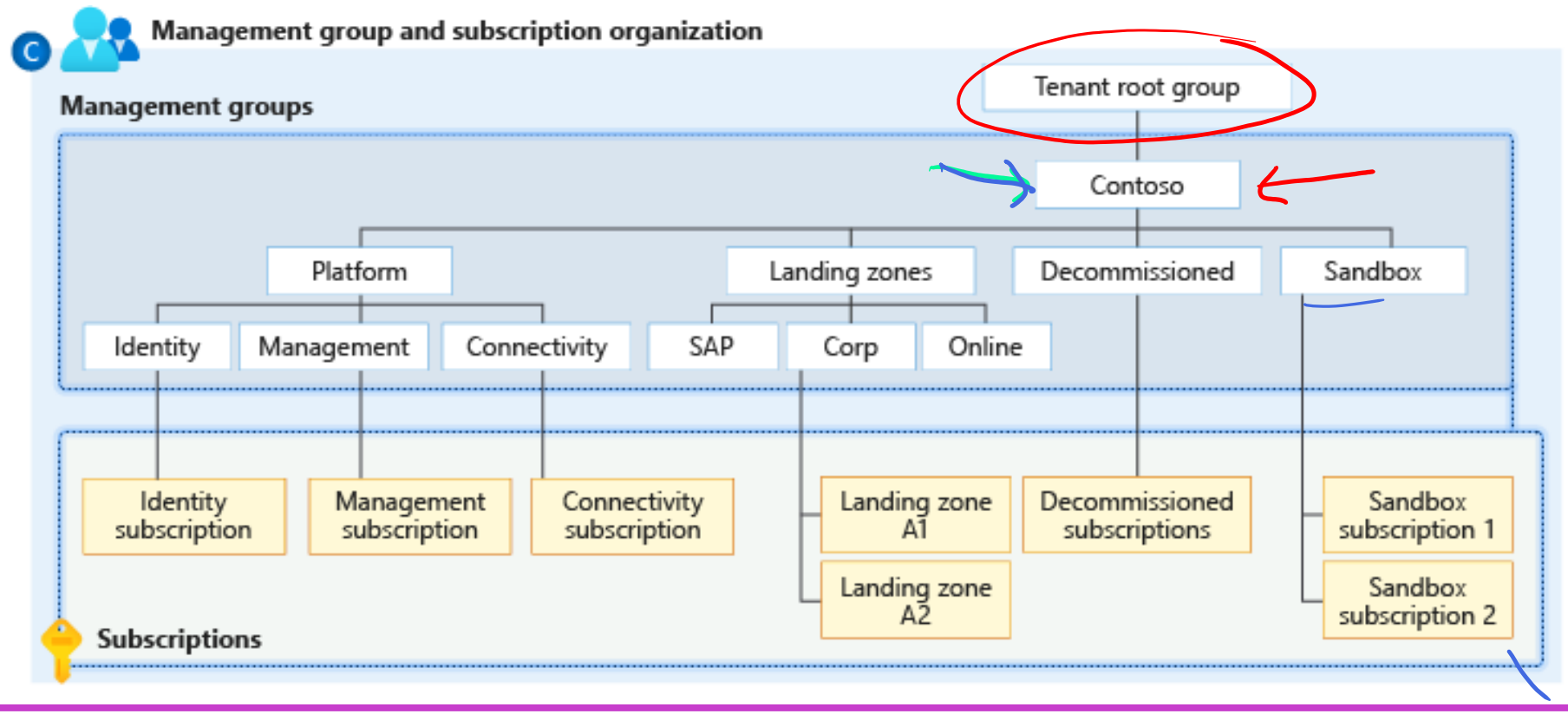
Method	Security	Usability	Availability	Primary authentication	Secondary authentication
Windows Hello for Business	High	High	High	Yes	MFA*
Microsoft Authenticator app	High	High	High	Yes	MFA and SSPR
FIDO2 security key	High	High	High	Yes	MFA

* Windows Hello for Business can serve as a step-up MFA credential by being used in FIDO2 authentication.



Manage authorization by using Microsoft Entra ID

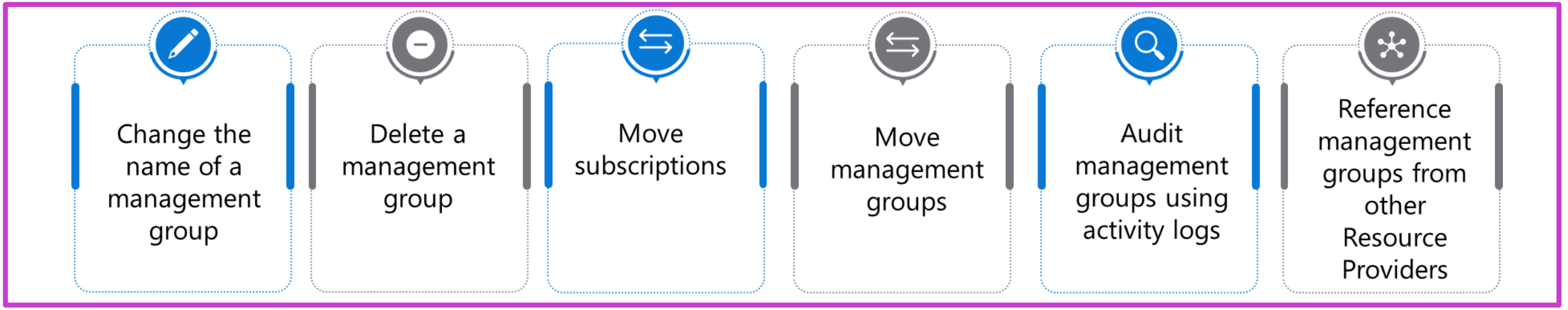
Azure management groups



- Management groups organize Azure subscriptions for scalable governance and policy compliance.
- Policies applied at management group level cascade to all subscriptions and resources within.
- Supports up to 10,000 groups, six levels deep hierarchy, ensuring centralized access and policy management.

Configure Azure role permissions for management groups, subscriptions, resource groups, and resources

To **configure Azure role permissions**, you have the following options:



- Azure management groups organize subscriptions for centralized governance and automatic policy inheritance.
- Management groups can be renamed or deleted via portal, PowerShell, or Azure CLI with specific permissions.
- Subscriptions inherit access and policies when moved to a management group; audit with Azure Activity Log.

Azure role-based access control

- Azure RBAC controls access to resources through role assignments based on security principal, role definition, and scope.
- Supports fine-grained access management, allowing specific permissions for users, groups, service principals, or managed identities.
- Role assignments and deny assignments determine access, globally stored to ensure resource accessibility regardless of region.

Azure built-in roles

General	
Built-in role	**Description**
Contributor	Grants full access to manage all resources but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.
Reader	View all resources but does not allow you to make any changes.
Role Based Access Control Administrator	Manage access to Azure resources by assigning roles using Azure RBAC. This role does not allow you to manage access using other ways, such as Azure Policy.
User Access Administrator	Enables you to manage user access to Azure resources.

Definition

self elevation

- Azure RBAC provides built-in roles for users, groups, and identities.
- Role assignments manage access to Azure resources.
- Custom roles cater to specific organizational requirements if built-in roles are insufficient.

The following is a general list of Azure built-in roles and is not an exhaustive representation.

Assign Azure role permissions for management groups, subscriptions, resource groups, and resources

To **assign Azure roles**, complete the following high-level steps:

- Identify who needs access: user, group, service principal, or managed identity.
- Select appropriate role; built-in or custom, based on specific actions required.
- Assign role at determined scope via Azure portal, PowerShell, CLI, SDKs, or REST APIs.

Microsoft Entra built-in roles

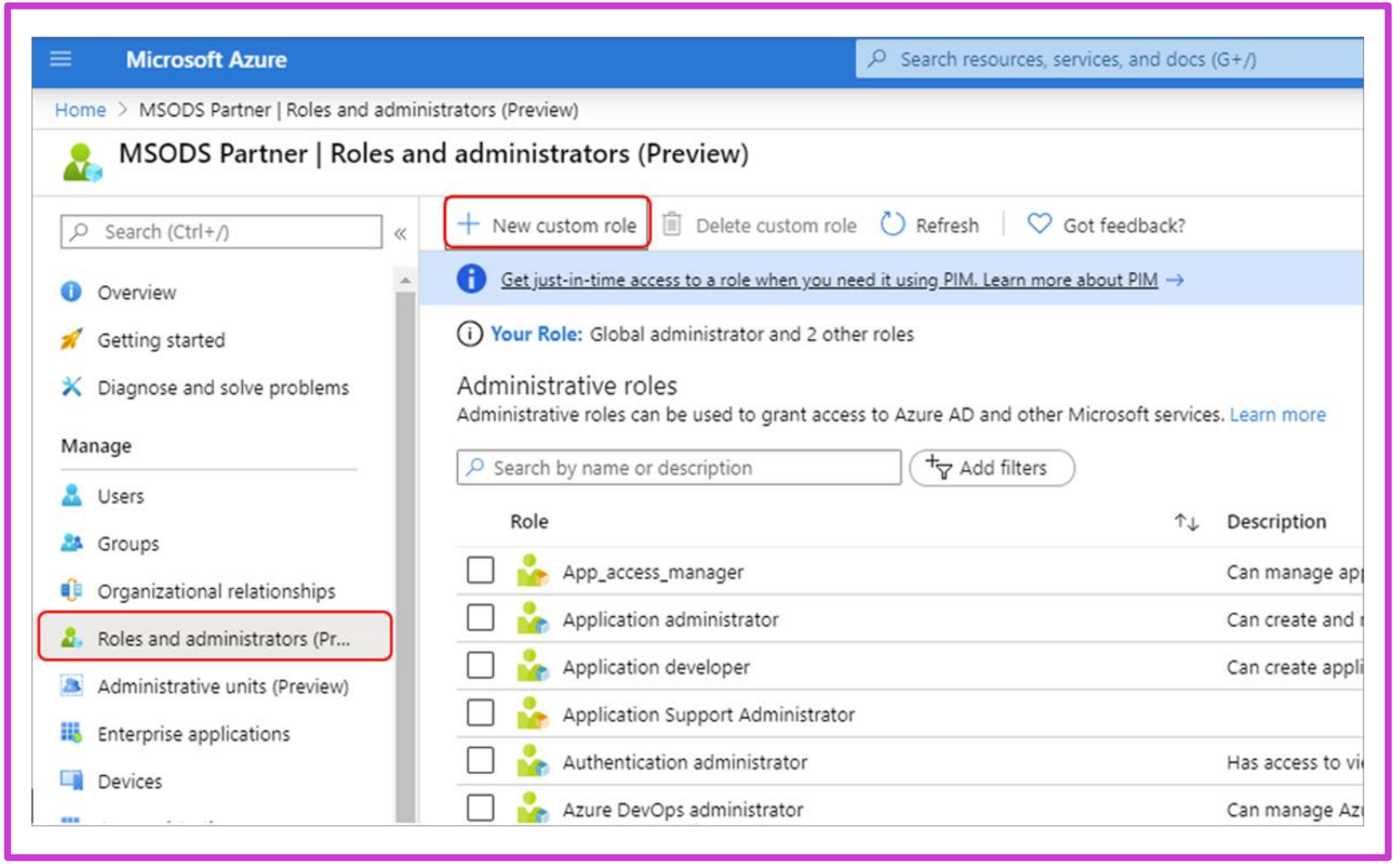
Built-in role	Description
Application Administrator	Privileged role allows application registration, consent, and owner status for assigned users.
Attribute Assignment Administrator	Role allows assigning custom security attributes to Microsoft Entra objects; not included in default admin roles.
Attribute Log Administrator	Attribute Log Reader role: access audit logs for custom security attributes; not granted in default admin roles.
Authentication Administrator	Authentication Administrator role: manage authentication methods, reset passwords, and perform sensitive actions; limitations apply.
Authentication Policy Administrator	Authentication Policy Administrator: configure policies, manage credentials, tickets; limitations apply.

- Assign Microsoft Entra roles for resource management.
- Roles grant permissions like user management.
- Permissions include password resets and license management.

The following is a list of Microsoft Entra built-in roles and is not an exhaustive representation.

Create and assign custom roles, including Azure roles and Microsoft Entra ID roles

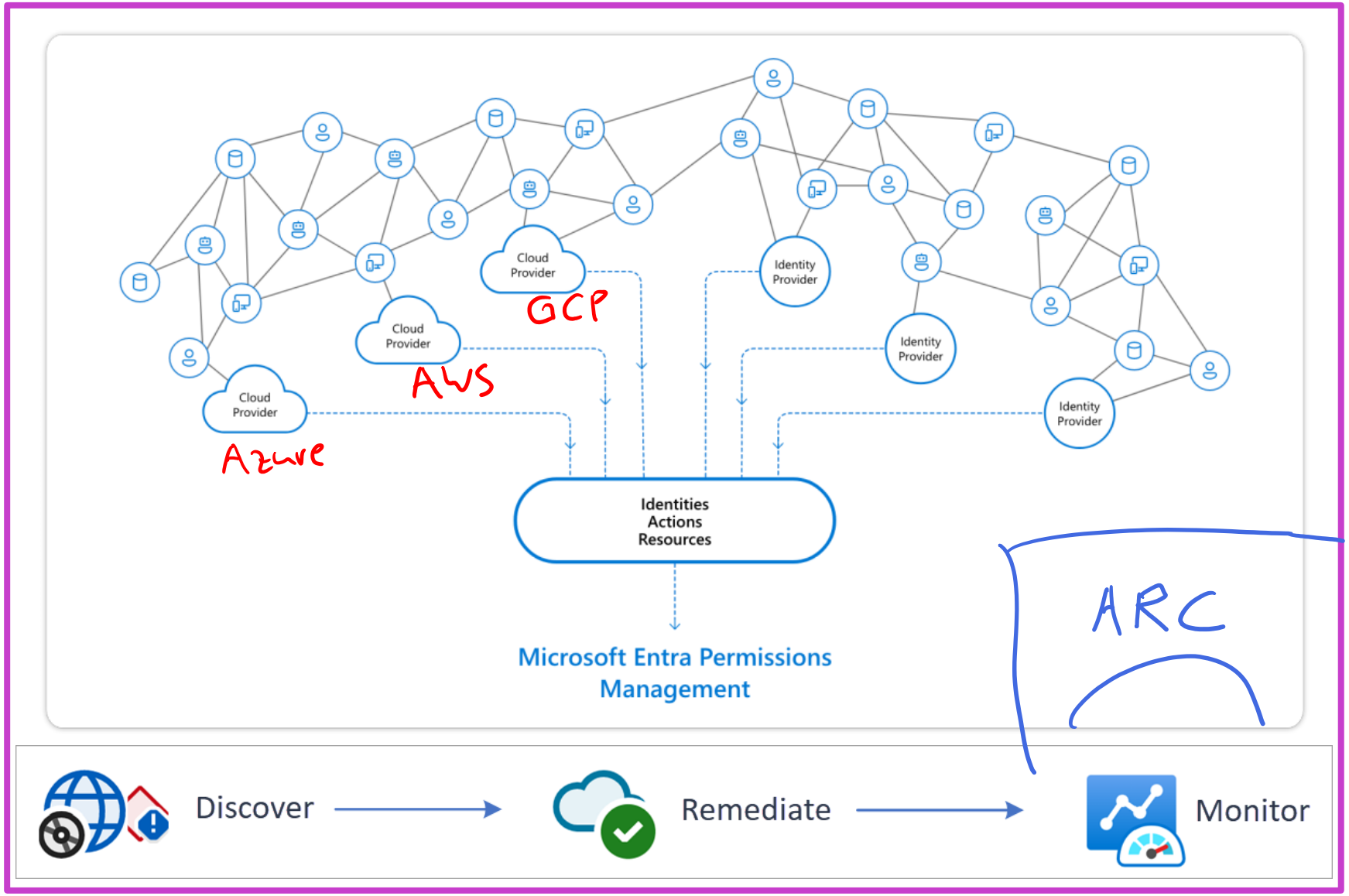
- Access Azure's RBAC settings via Azure portal or Azure CLI.
- Assign appropriate roles (e.g., Owner, Contributor, Reader) to management groups, subscriptions, and resource groups.
- Fine-tune permissions for specific resources within resource groups as required, ensuring comprehensive access control across the Azure environment.



Microsoft Entra permissions management

Entra Portal

- Entra permissions management enhances cloud security across Azure, AWS, GCP with visibility and control.
- Automates permission right-sizing, addresses over-privileged identities, supports Zero Trust with least privilege access.
- Offers discovery, remediation, monitoring phases to manage permissions, reduce attack surface, ensure compliance.



Implement and manage Microsoft Entra Permissions Management

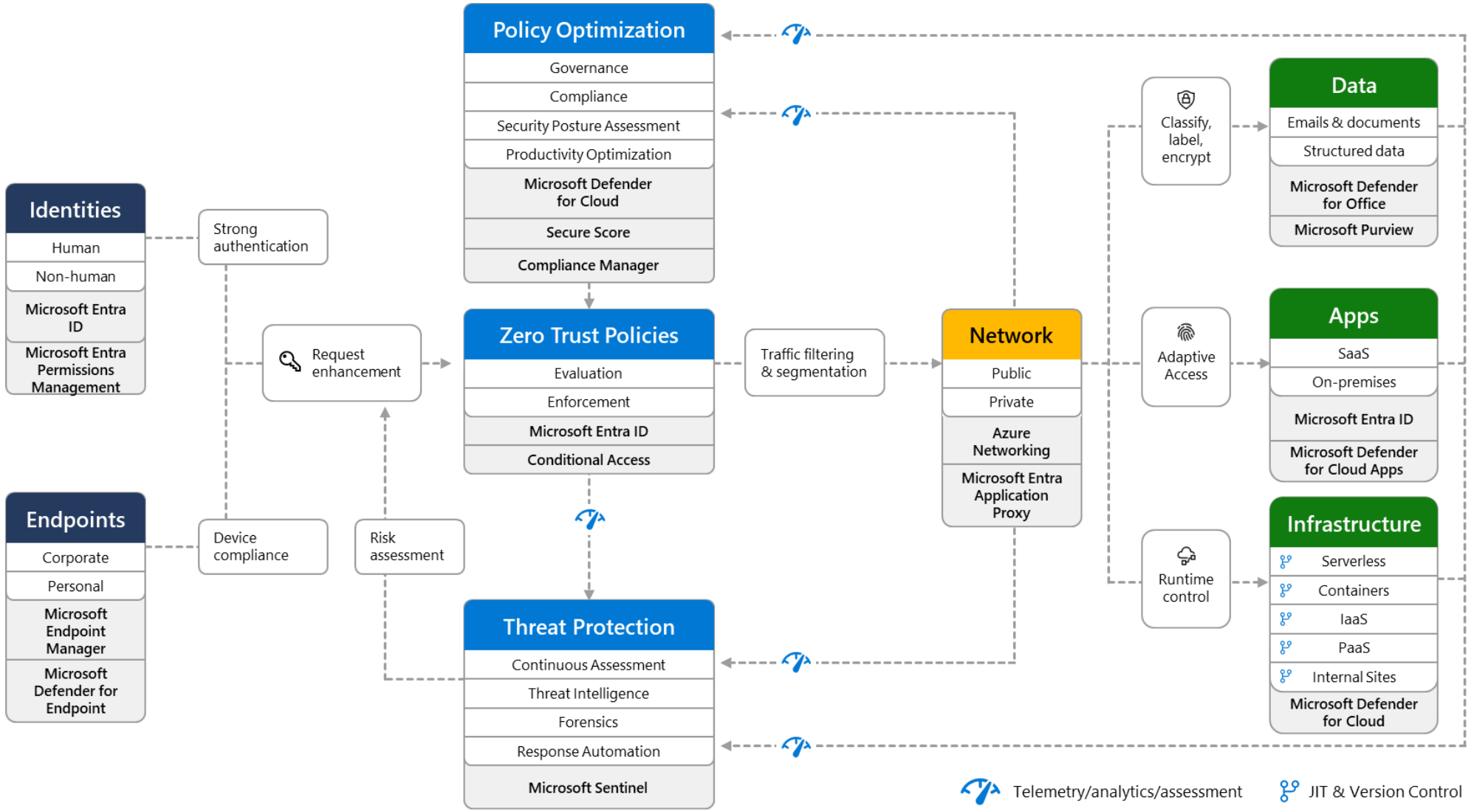
Enable Microsoft Entra Permissions Management on Microsoft Entra ID tenant

- In your browser, go to **Entra services** and sign into Microsoft Entra ID.
- In the Microsoft Entra ID portal, select **Permissions Management**, and then purchase a license or begin a trial.
- Permissions Management launches with the **Data Collectors** dashboard.

Configure data collection settings

- Use the **Data Collectors** dashboard in **Permissions Management** to configure data collection settings for your authorization system.
- Select the authorization system: **Amazon Web Services** (**AWS**), **Azure**, or **Google Cloud Platform** (**GCP**).

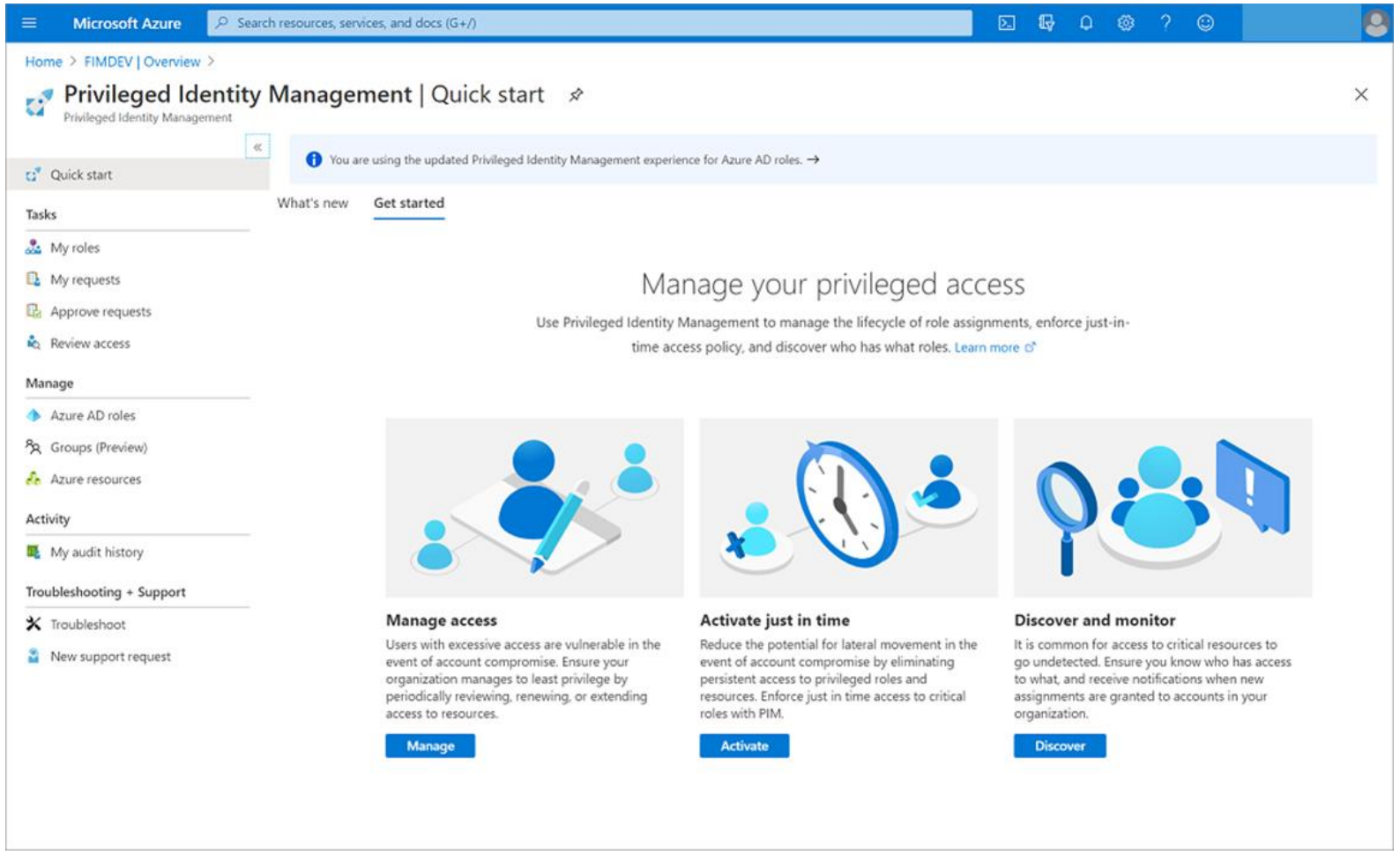
Zero Trust security



Microsoft Entra Privileged Identity Management

PIM

- PIM **manages**, **controls**, and **monitors access** to key resources across Microsoft services, requiring licenses.
- Enables **just-in-time privileged access** and oversight for user operations in Azure and Microsoft services.
- Offers **role management**, **activation**, and **approval processes**, with email notifications for assignment changes.



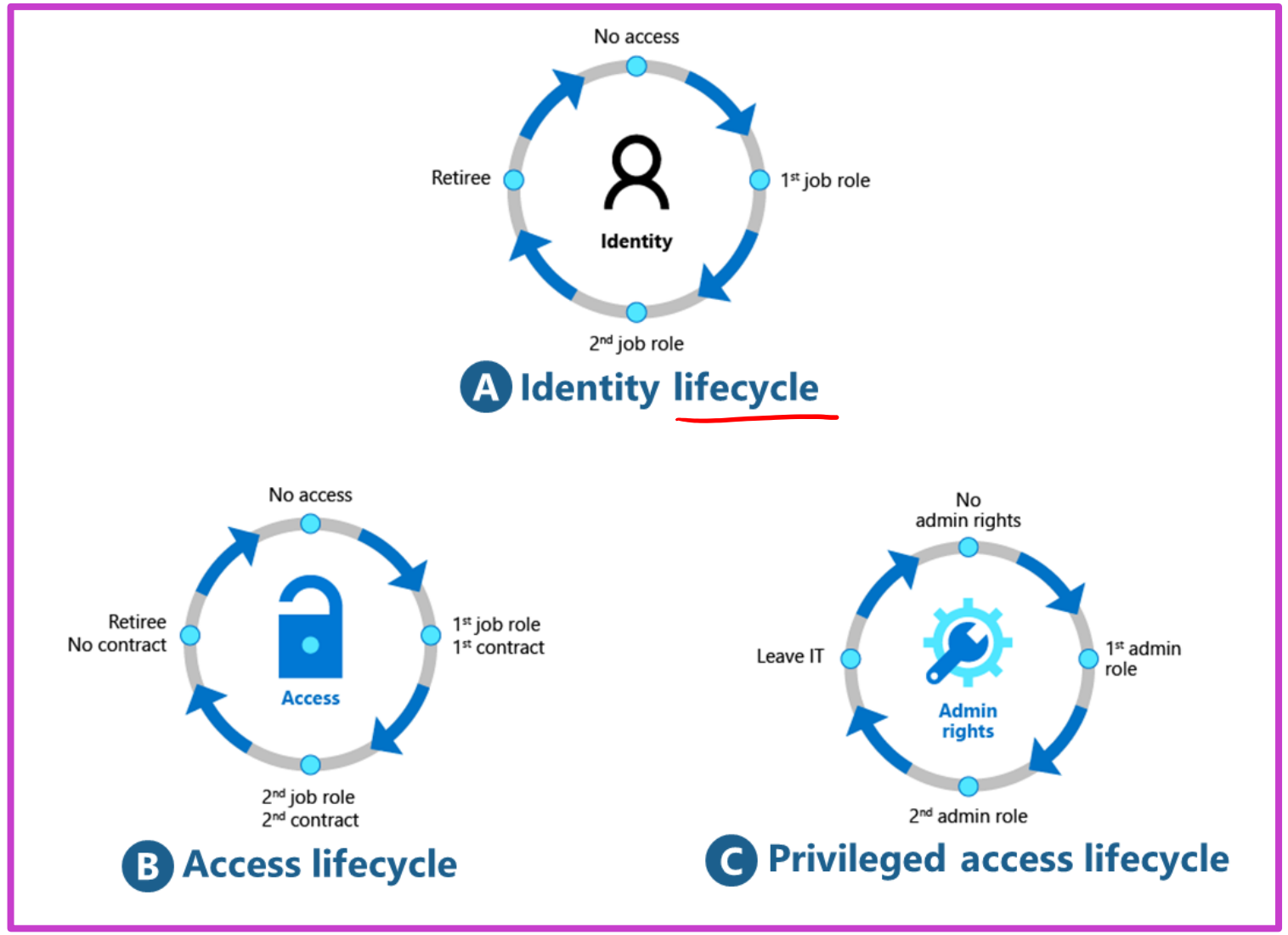
Configure Microsoft Entra Privileged Identity Management (PIM)

Time-based and approval-based role activation for privileged users

- Just-in-time privileged access to Azure
- Time-bound access to resources
- Approval to activate privileged roles
- Multi-factor authentication to activate any role
- Justification to understand why users activate
- Notifications when privileged roles are activated
- Access reviews to ensure users still need roles
- Audit history for internal or external audit

Microsoft Entra ID governance

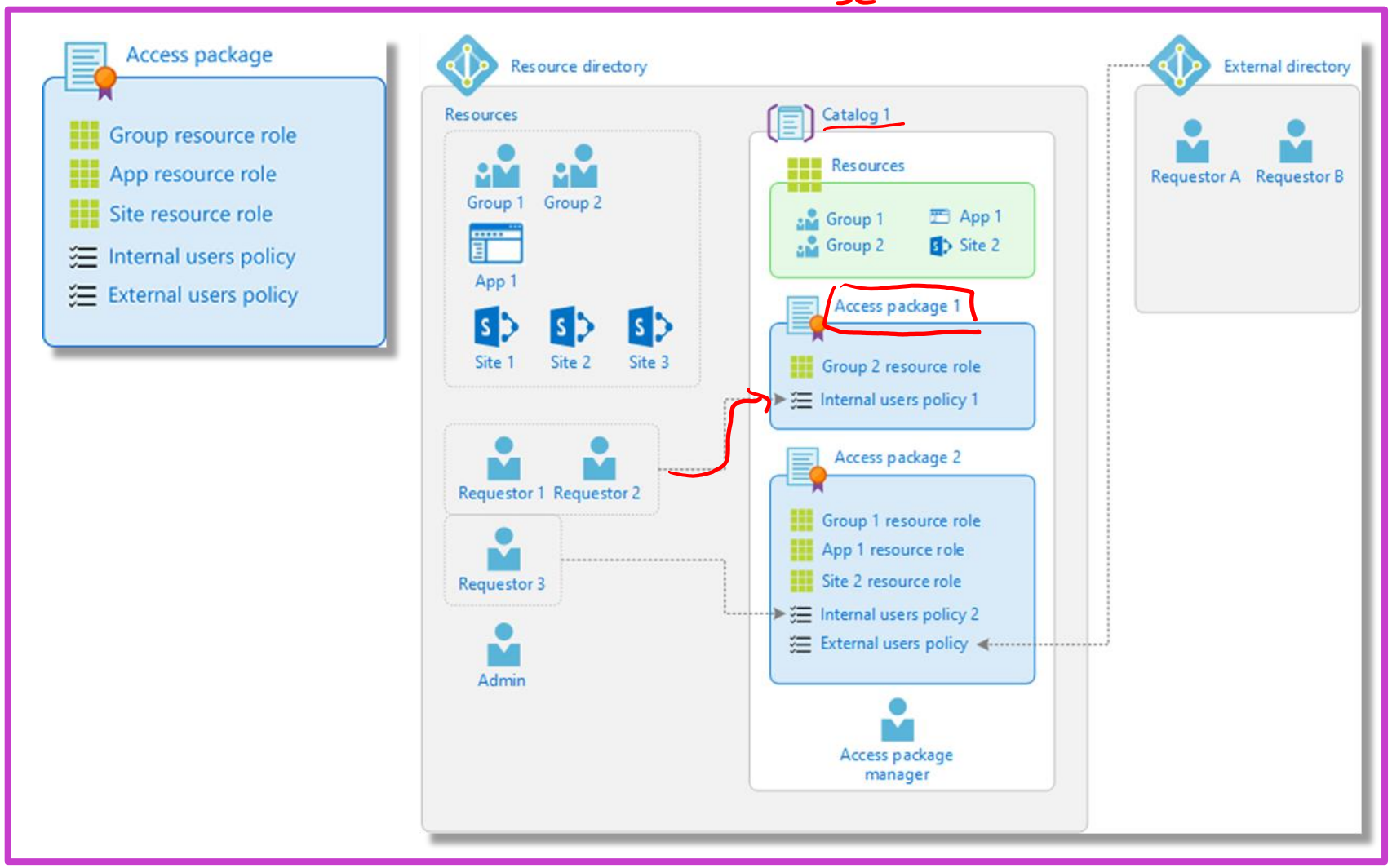
- Boosts productivity, security, and compliance with automated identity/access management and governance.
- Addresses critical access questions, automates identity/access lifecycle, and secures privileged administration
- Automates provisioning from HR sources, manages identity changes, and controls guest access.
- Enforces policies, integrates applications, and ensures continuous access review and privileged access governance.



Entitlement management

AZ-500 SC-400 SC-300 SC-200 SC-100

- Automates management of identity/access across organizations, improving efficiency and security.
- Eases access for internal/external users, addressing dynamic requirements and collaboration challenges.
- Offers control via access packages, multi-stage approvals, and automatic role assignments based on user properties.
- Facilitates delegated management, enabling non-admins to create access packages and policies for resource access.



Access reviews

- Manage group memberships, app access, and roles with Microsoft Entra ID; ensure only authorized access.
- Review access for internal/external users, adjusting for roles changes or departures to maintain security.
- Use access reviews for over-privileged roles, automation limits, new group purposes, and critical data access compliance.
- Create reviews in access reviews, Microsoft Entra apps, PIM, or entitlement management, depending on the resource.

Access reviews (continued)

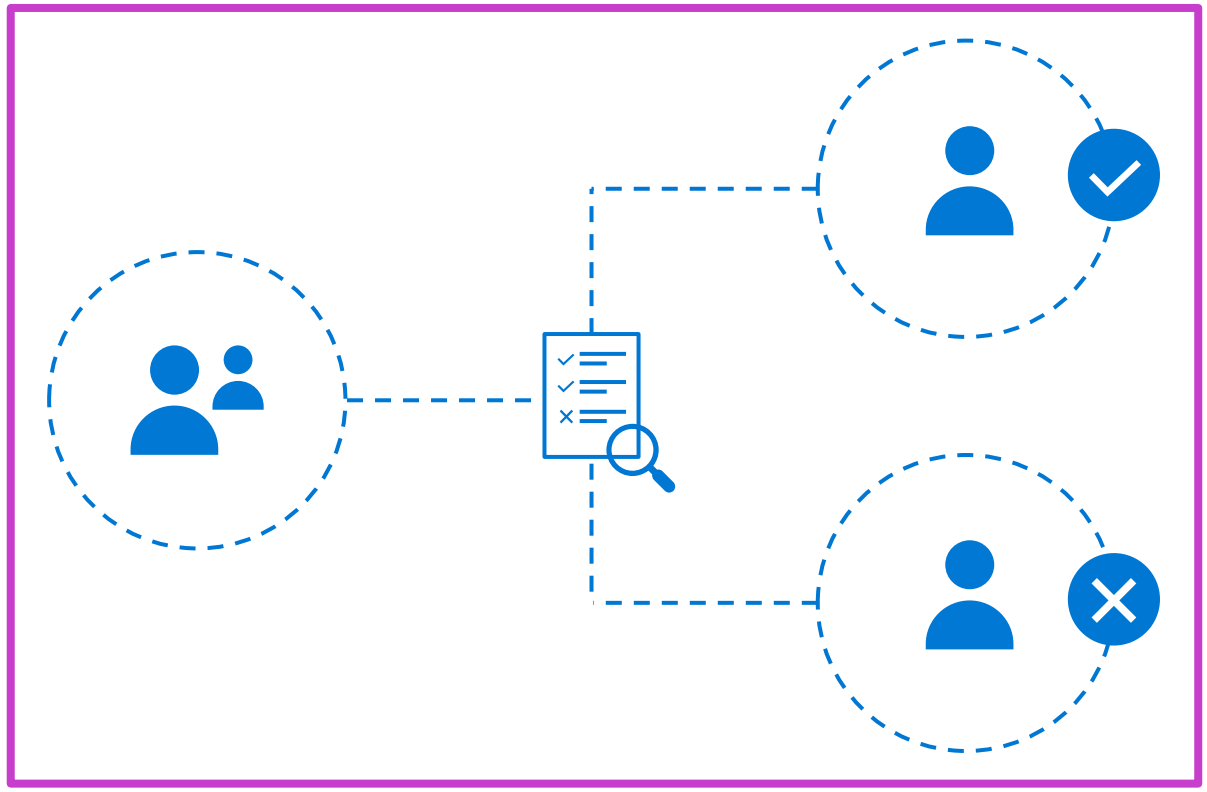
- Create access reviews in **access reviews**, **Microsoft Entra**, **PIM**, or **entitlement management** based on review needs

Access rights of users	Reviewers can be	Review created in	Reviewer experience
Security group members Office group members	Specified reviewers Group owners Self-review	access reviews Microsoft Entra groups	Access panel
Assigned to a connected app	Specified reviewers Self-review	access reviews Microsoft Entra enterprise apps	Access panel
Microsoft Entra role	Specified reviewers Self-review	Privileged Identity Management	Microsoft Entra Admin Center
Azure resource role	Specified reviewers Self-review	Privileged Identity Management	Microsoft Entra Admin Center
Access package assignments	Specified reviewers Group members Self-review	entitlement management	Access panel

Configure role management and access reviews by using Microsoft Entra ID Governance

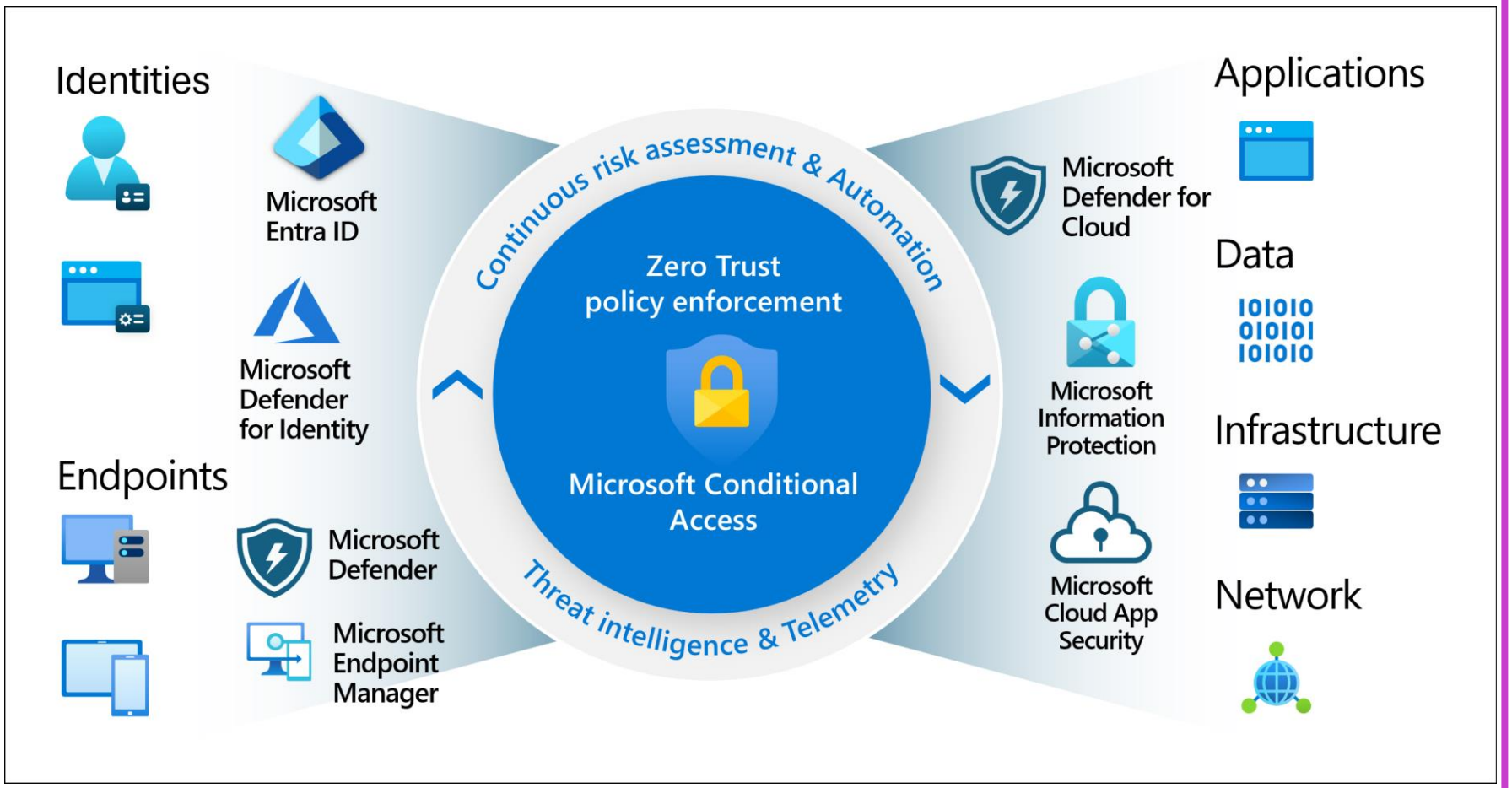
Enable organizations to re-certify group memberships, application access, and privileged role assignments.

- Included with Microsoft cloud subscriptions (Azure, 365)
- Entra ID P1 available standalone or with 365 E3/Business Premium
- Entra ID P2 available standalone or with 365 E5
- Entra ID Governance enhances P1/P2 with advanced identity governance

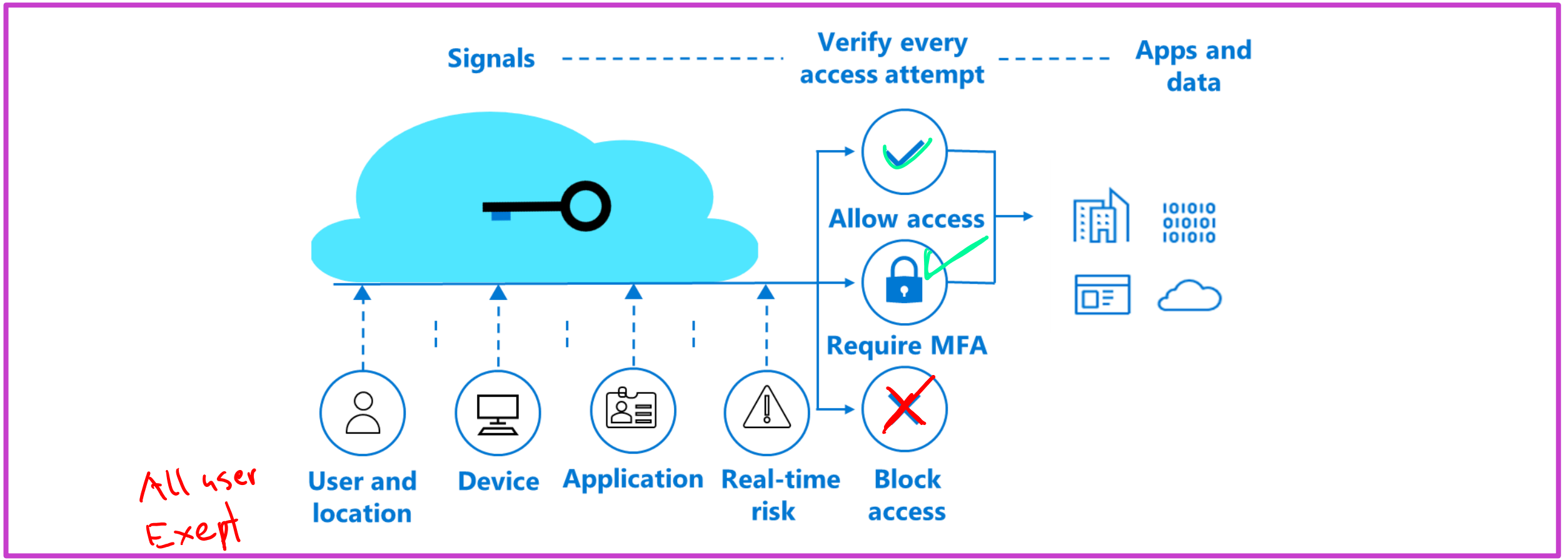


Microsoft Entra conditional access

- Security now includes user/device identity; Microsoft Entra integrates signals for access control.
- Conditional Access enforces policies based on user, device, application signals for resource access.
- Aims: empower productivity, protect assets, using multifactor authentication and specific access controls.



Implement Conditional Access policies



- Exclude emergency access and service accounts from MFA to prevent lockouts and ensure access.
- Administrators can exclude certain applications from MFA policies based on security needs.
- Option to deploy MFA policies via direct steps or Conditional Access templates for flexibility.

Manage application access in Microsoft Entra ID

Manage access to enterprise applications in Microsoft Entra ID, including OAuth permission grants

Assign users and groups to an app

There are two primary assignment modes:

- Individual assignment
- Group-based assignment

Require user assignment for an app

Enable this to ensure only those users you assign to the application can sign in.

Determine experience for app access

Microsoft Entra ID provides many customizable ways to deploy applications to end users, such as Microsoft Entra ID My Apps.

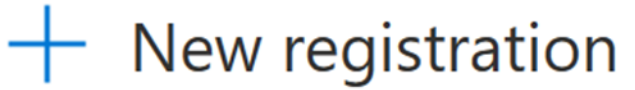
Main ways to access a Microsoft-published application:

- For applications in the Microsoft 365 or other paid suites, access is granted through **license assignment**.
- For applications that Microsoft or a third party publishes freely for anyone to use, users may be granted access through:
  - User consent
  - Administrator consent
- Some applications combine both these methods.

Manage app registrations in Microsoft Entra ID

Creating a Microsoft Entra application and service principal that can access resources entails the following steps:

1. **App Registration:** Sign into Microsoft Entra admin, navigate to Identity > Applications > App registrations, and register a new app.



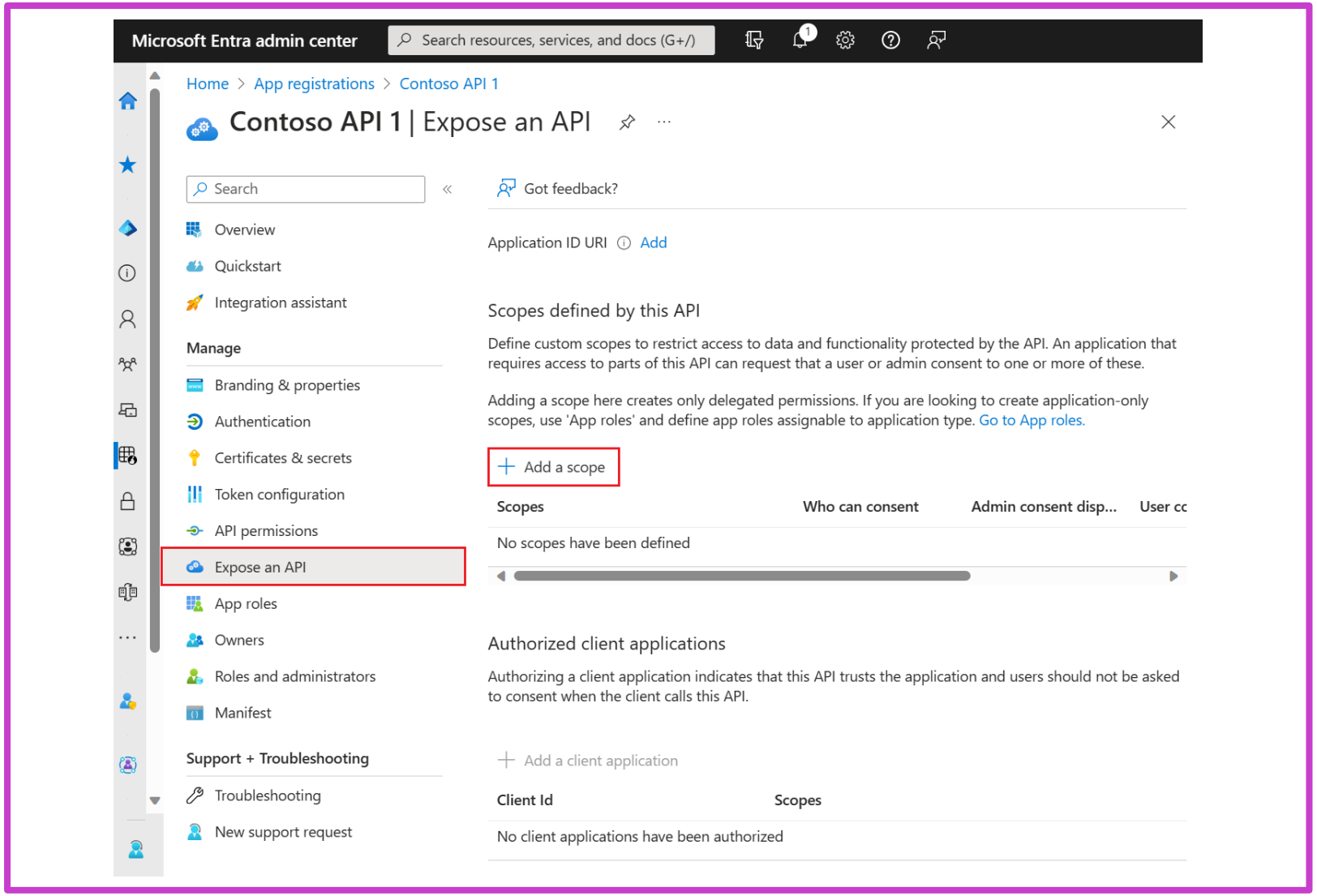
2. **Setting Up:** Name the app, select account type, and set a Redirect URI.

3. **Assigning Role:** In Azure portal, define the role and its scope for the app, ensuring it has adequate permissions.

4. **Access Control:** Assign roles at chosen scope, find and select the registered app, and finalize role assignment.

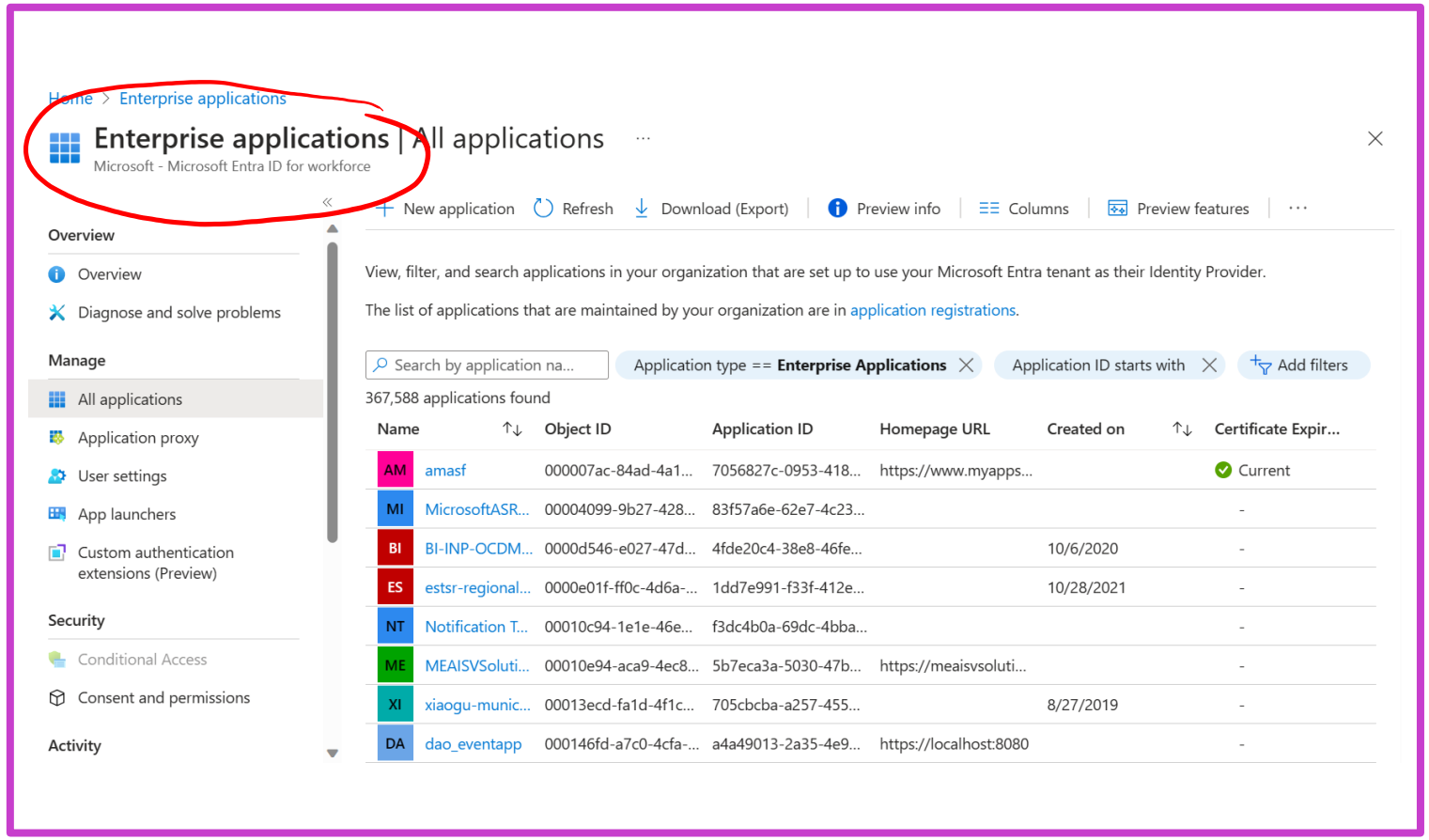
Configure app registration permission scopes

- Microsoft identity platform manages access for registered apps only, including web/mobile apps and web APIs.
- Registration creates a one-way trust where your app trusts the platform, not vice versa.
- Once registered, the application object is fixed to its tenant and cannot be moved.



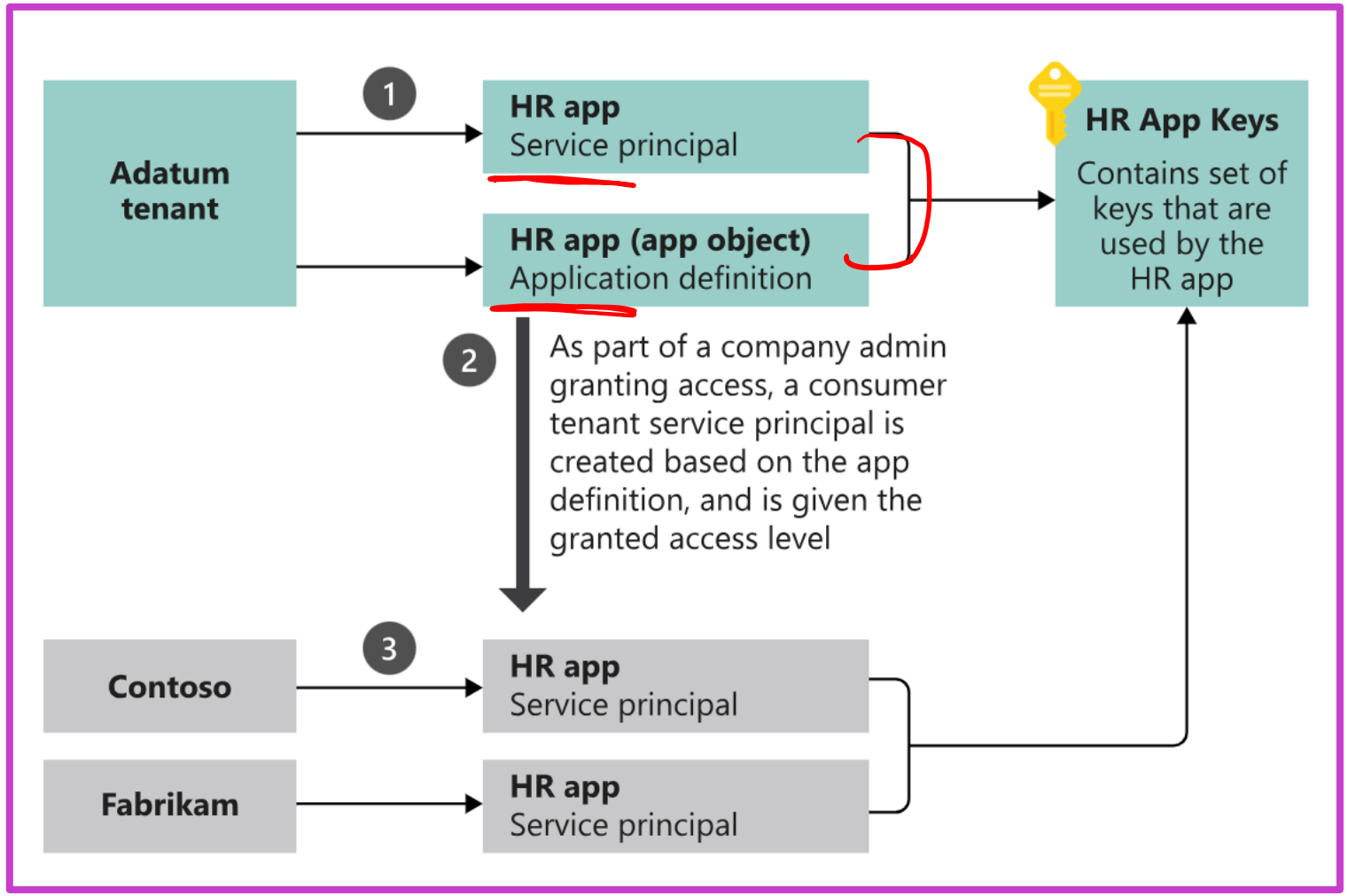
Manage and use service principals

- Registering an app with Microsoft Entra ID creates an identity configuration, enabling integration and choosing between single or multi-tenant setups.
- Completed registrations yield a unique app instance and ID, allowing for secrets, certificates, scopes, and customized branding.
- Registration automatically generates an application object and a service principal in your home tenant, with service principal creation being separate when using Microsoft Graph APIs.



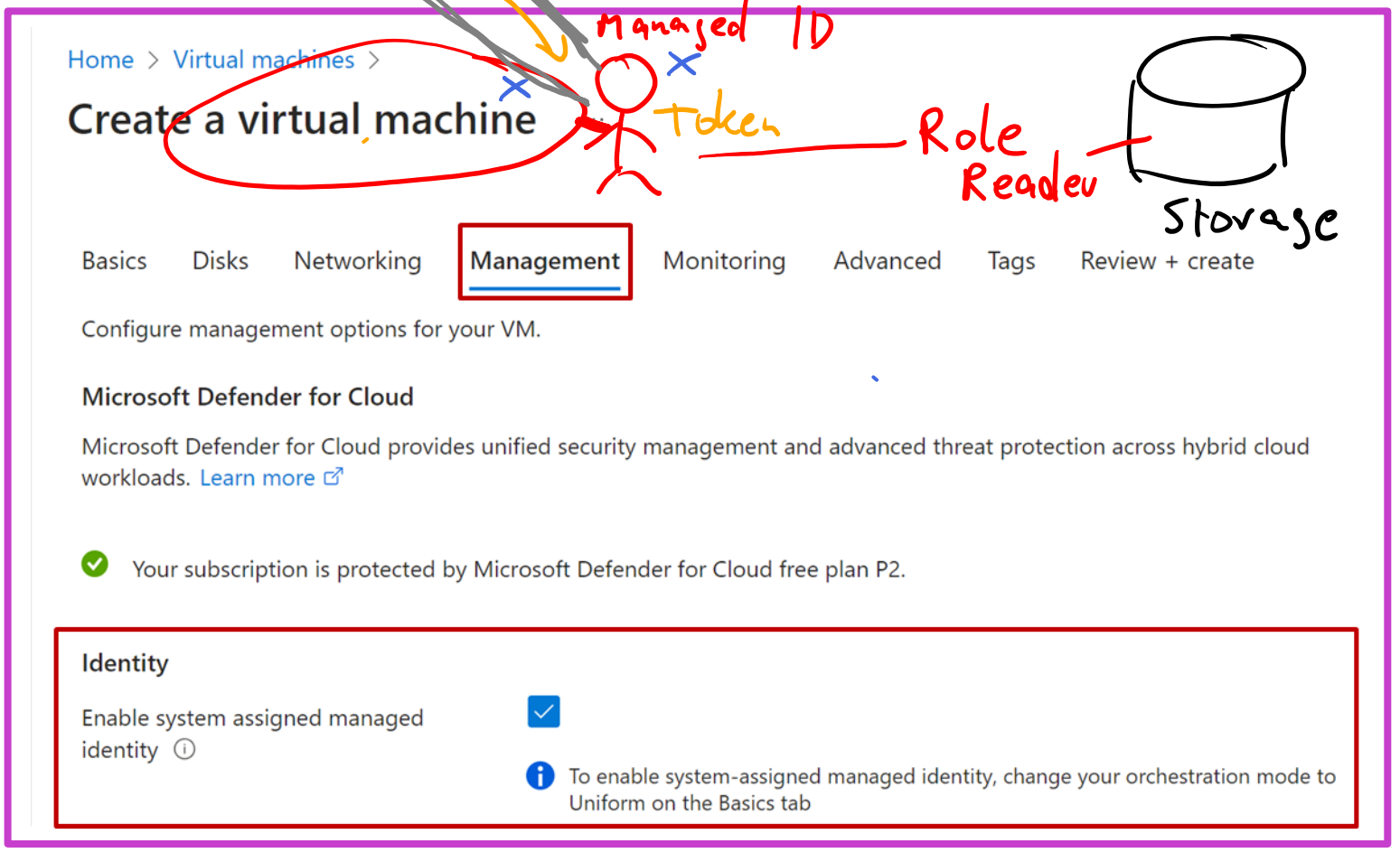
Relationship between application objects and service principals

- The application object is a global template for an app across all tenants, while service principals are its tenant-specific instances.
- Service principals are needed in each tenant for app sign-in/access, with single-tenant apps having one, and multi-tenant apps having multiple.
- Modifying or deleting the application object affects its service principal in the home tenant; deletion is permanent without restoring service principal.



Managed identities for Azure resources – system assigned

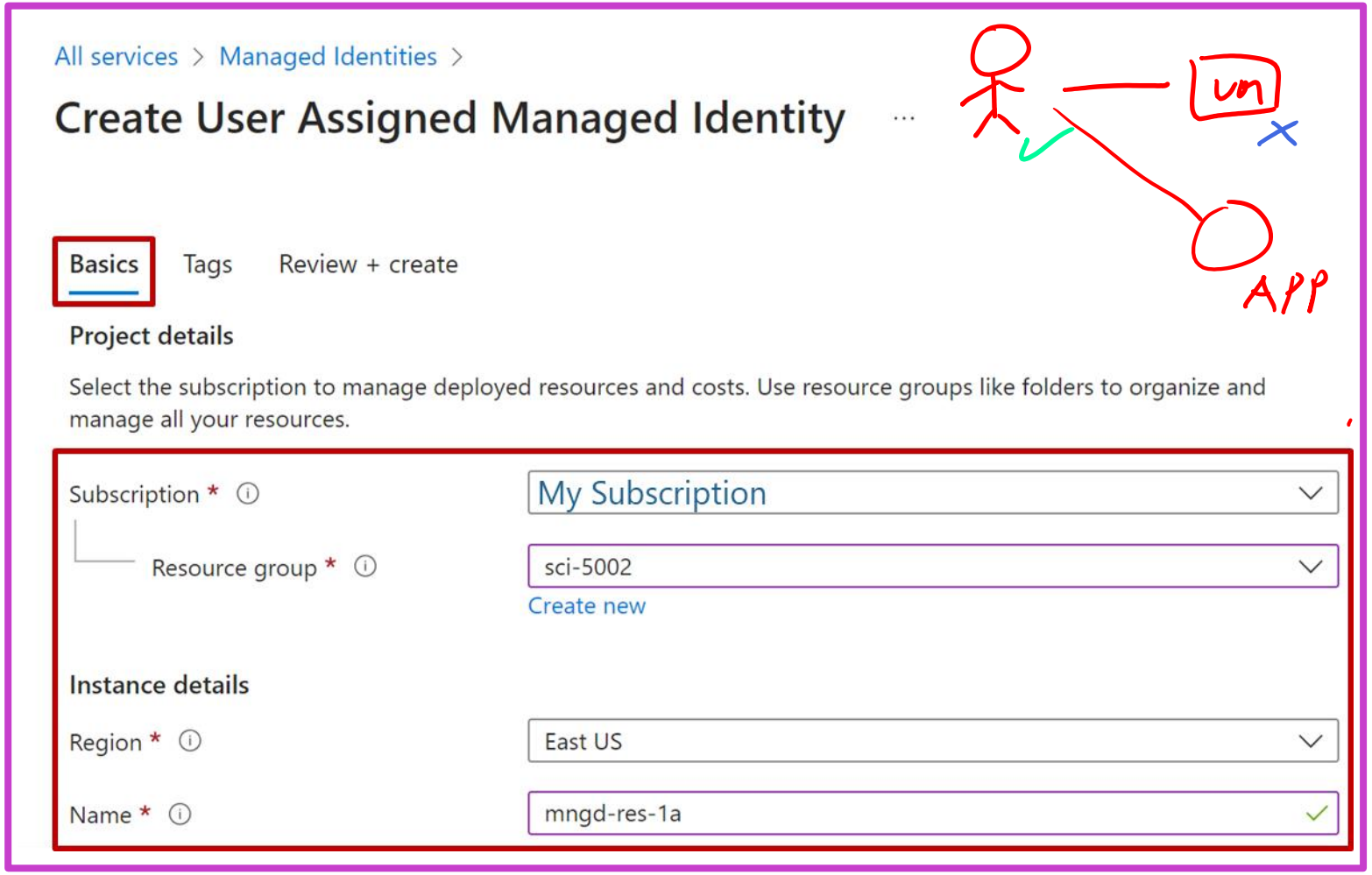
- Managed identities simplify authentication by eliminating code-based credentials, using Microsoft Entra tokens for Azure resource access.
- Azure automatically manages these identities, freeing users from manual identity management tasks.
- Two variants are available: **system-assigned identities**, linked to resource lifecycles, and **user-assigned identities**, adaptable across multiple resources.



Example: Creating a system-assigned managed identity for a virtual machine.

Managed identities for Azure resources – user assigned

- User-assigned managed identities are **standalone Azure resources** assignable to multiple Azure resources.
- A special type of service principal is created in Microsoft Entra ID, managed separately from its associated resources.
- These identities enable **authorization for access** to one or more services, enhancing flexibility and security.



Example: Creating a user-assigned managed identity resource.

Recommend when to use and configure authentication for a Microsoft Entra Application Proxy

Remember these key considerations to use and configure authentication for Microsoft Entra application proxy:

It is not recommended to use Microsoft Entra application proxy for intranet access because this adds latency that will impact the user.

Enable pre-authentication to challenge users first for authentication.

If SSO is configured, the backend application will also verify the user.

Change the pre-authentication mode from **Passthrough** to Microsoft Entra ID to configure the external URL with HTTPS.

Once a user has pre-authenticated, SSO is performed by the Microsoft Entra application proxy connector authenticating to the on-premises application.

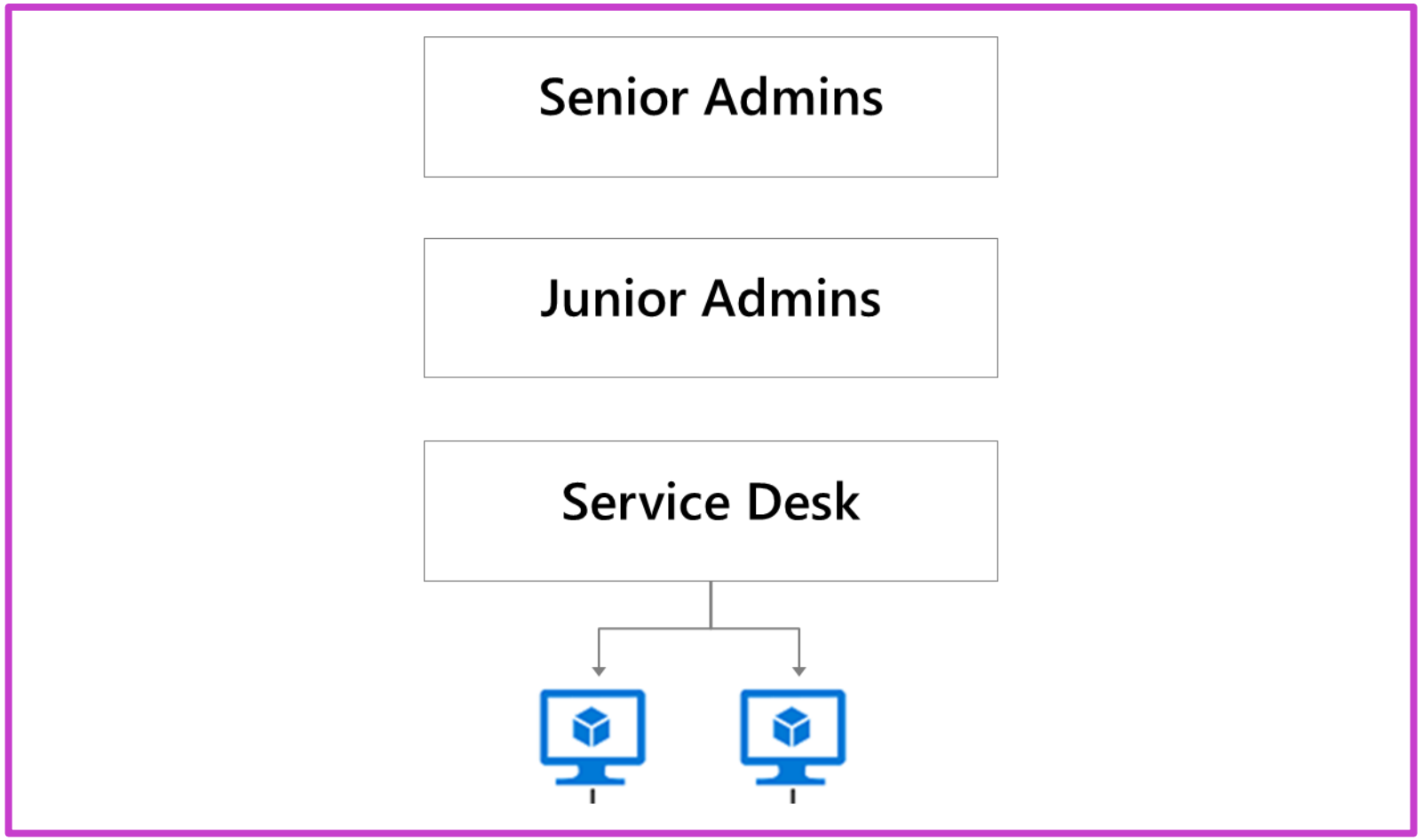
Choose the **Passthrough** option to allow access to the published application without ever having to authenticate to Microsoft Entra ID.

Microsoft Entra Application Proxy can also support applications that use the Microsoft Authentication Library (MSAL).

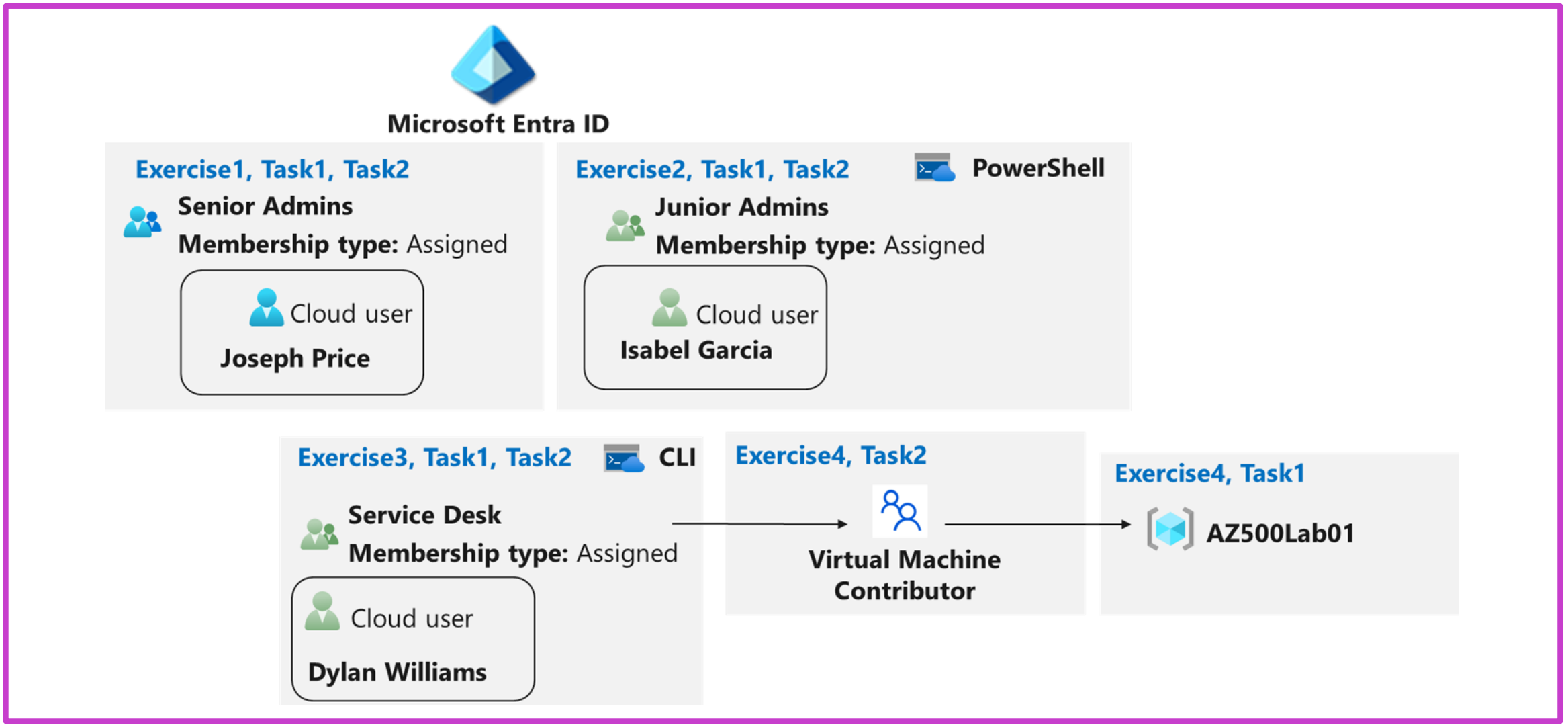
Module – Lab

Lab 01 – Role-based Access Control

- Use the Portal to create a Senior Admins group with member Joseph Price.
- Use PowerShell to create a Junior Admins group with member Isabel Garcia.
- Use the CLI to create a Service Desk group with member Dylan Williams.
- Assign the Service Desk group Virtual Machine Contributor permissions.



Lab 01 – Role-based Access Control



Knowledge check

1 **Your organization is considering multifactor authentication in Azure. Your manager asks about secondary verification methods. Which of the following options could serve as secondary verification method?**

- ☑ Automated phone call.
- ☐ Emailed link to verification website.
- ☐ Microsoft account verification code.

2 **Your organization has implemented multifactor authentication in Azure. Your goal is to provide a status report by user account. Which of the following values could be used to provide a valid MFA status?**

- ☐ Enrolled
- ☑ Enforced
- ☐ Required

3 **Which of the following options can be used when configuring multifactor authentication in Azure?**

- ☐ Block a user if stolen password is suspected.
- ☐ Configure IP addresses outside the company intranet that should be blocked.
- ☑ Configure a one-time bypass to allow a user to authenticate a single time without performing MFA.

Learning Path Recap

In this learning path, we:

We have mastered managing identities, ensuring optimal user and group control within Microsoft Entra ID.

We now skillfully navigate through Microsoft Entra ID, employing advanced authentication and authorization methods to reinforce security.

We have acquired expertise in managing application access, enabling streamlined and secure user interactions within Microsoft Entra ID applications.

End of presentation