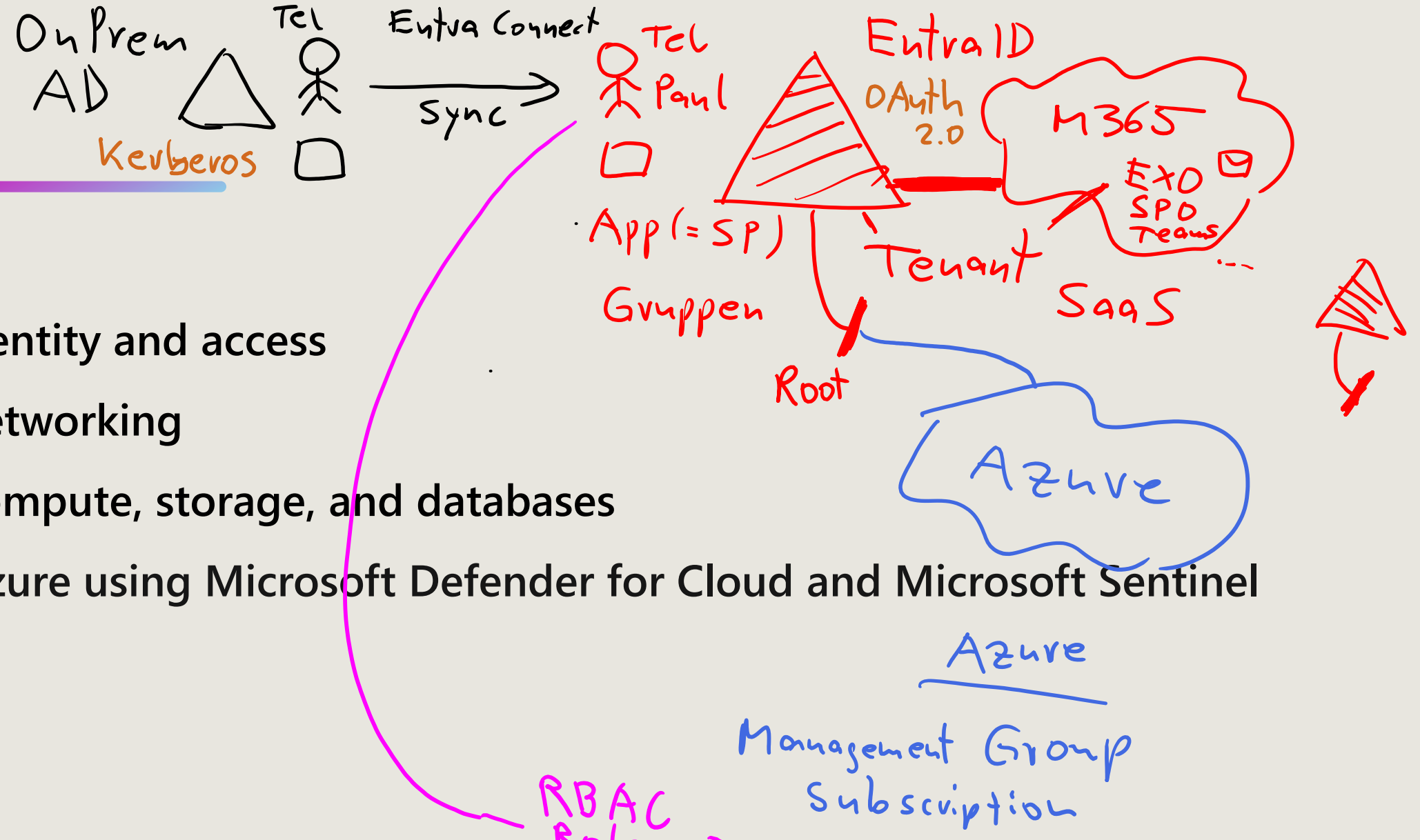
Microsoft

AZ-500

Secure cloud resources with Microsoft security technologies

Agenda



1 Secure identity and access

2 Secure networking

3 Secure compute, storage, and databases

4 Secure Azure using Microsoft Defender for Cloud and Microsoft Sentinel

Learning Path: Secure identity and access

Manage security controls for identity and access

Manage Microsoft Entra application access

Implement and manage enforcement of cloud governance policies

Module lab

Learning Objectives

After completing this learning path, you will be able to:

1. Effectively manage identities using Microsoft Entra ID to ensure secure access and identity governance.
2. Manage authentication processes effectively using Microsoft Entra ID to secure user access and verify identities.
3. Implement and manage authorization settings using Microsoft Entra ID to control access rights and permissions securely.
4. Manage and secure application access effectively using Microsoft Entra ID to ensure proper authorization and user authentication.

Manage security controls for identity and access

MCSB Security Controls: Identity Management and Privileged Access

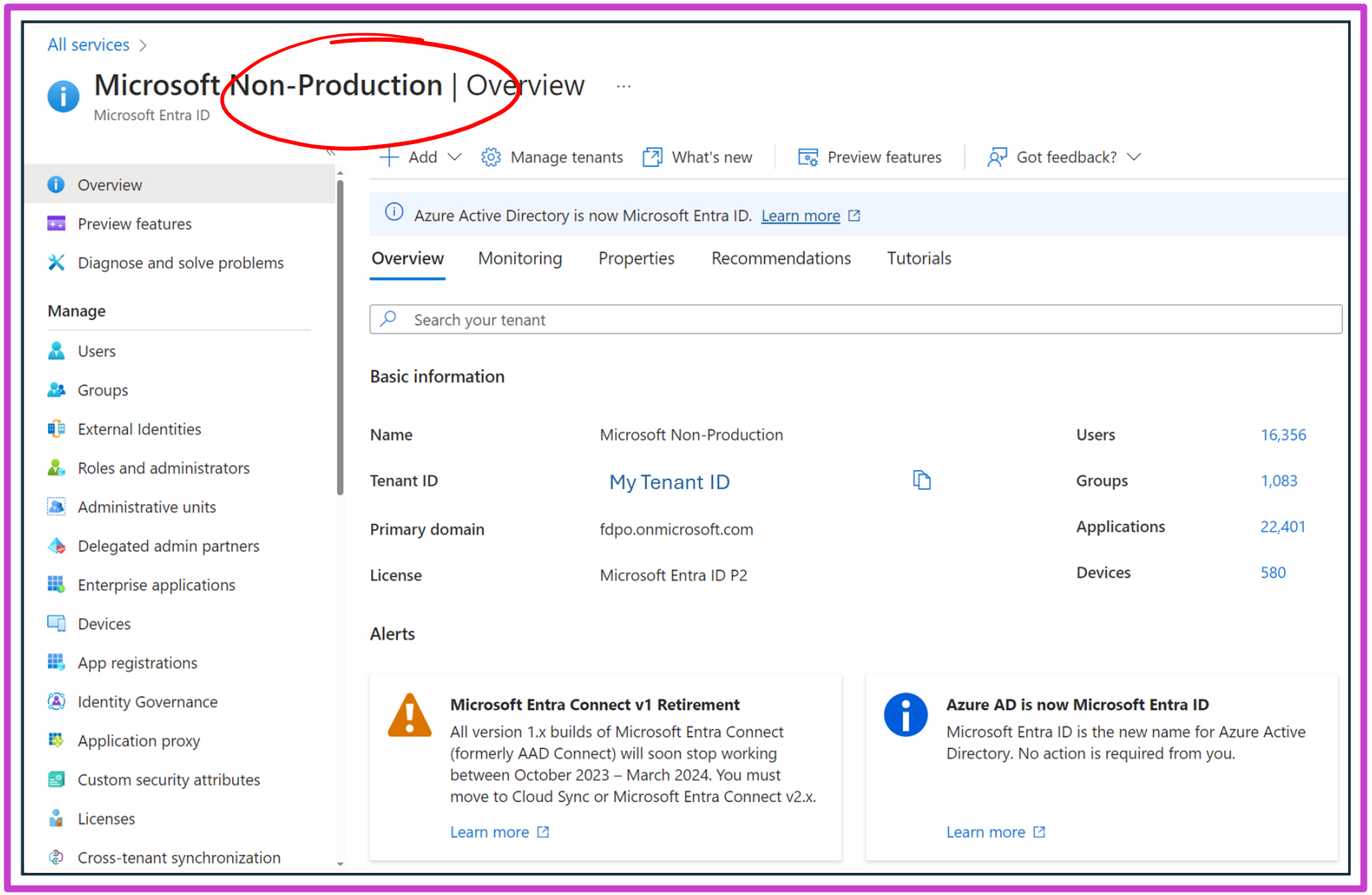
- Identity Security: Centralizes authentication, protects systems, manages app identities, and authenticates servers securely.
- Access Control: Restricts resource access with conditional policies and enforces secure authentication methods.
- Privileged Access: Limits admin roles, avoids standing access, and applies least privilege principles.
- Lifecycle and Reviews: Manages identity lifecycle, reviews access, ensures emergency access, and secures privileged operations.

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.

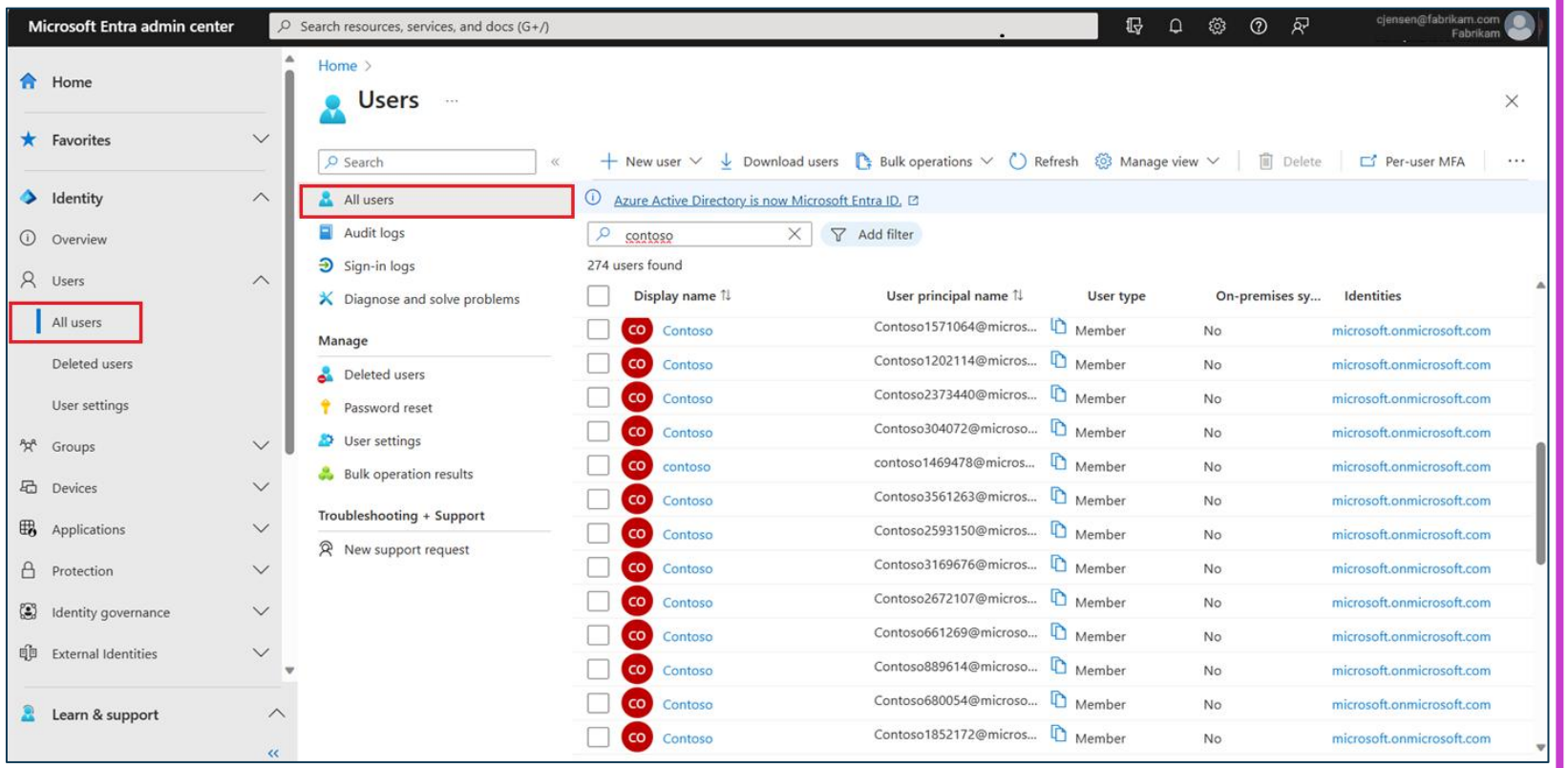
- Offers free and paid licenses (P1, P2) enhancing security, access management, and supports hybrid user access with advanced administration features.

- 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.

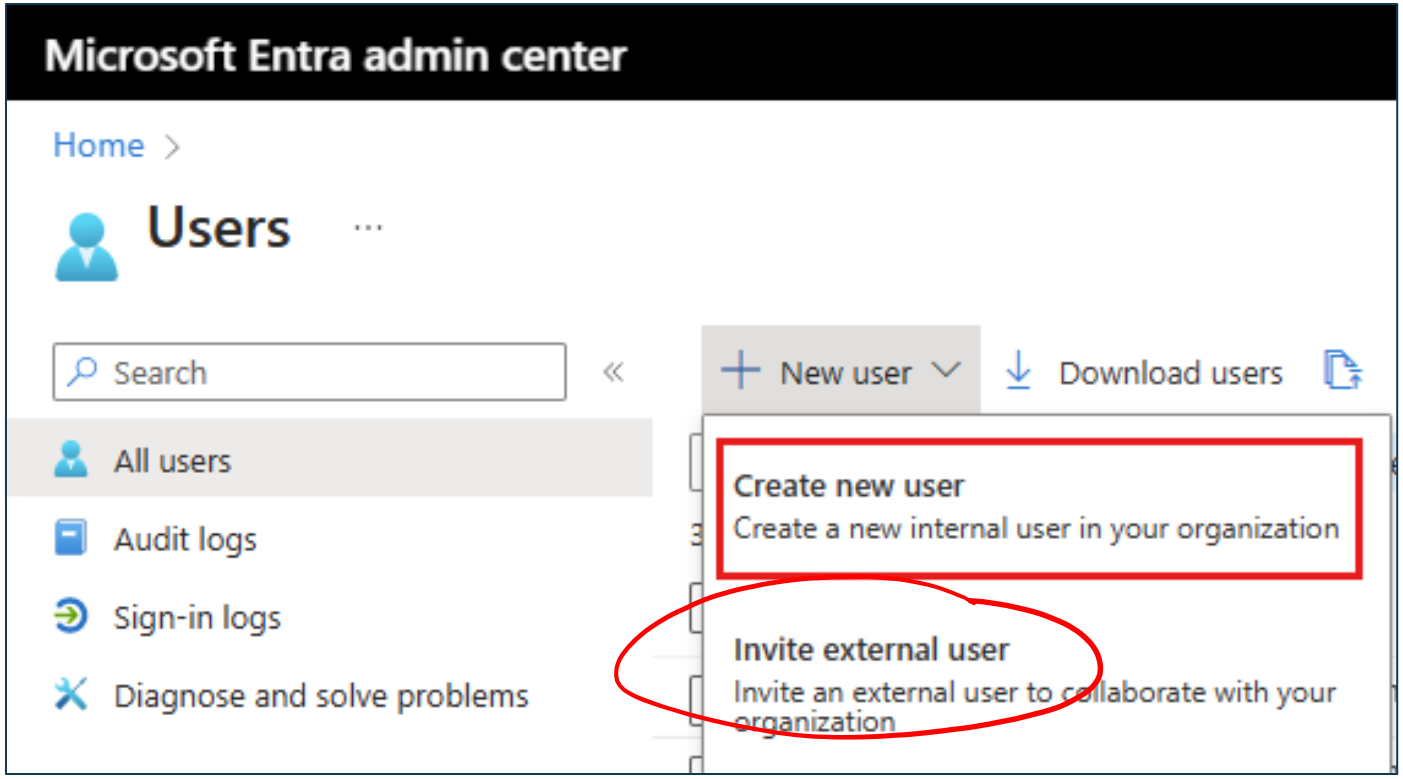


Microsoft Entra ID – Types of users

Standard User Perm in Entra:
Member: alle User Profiles
Guest: nur Basic Profiles

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.

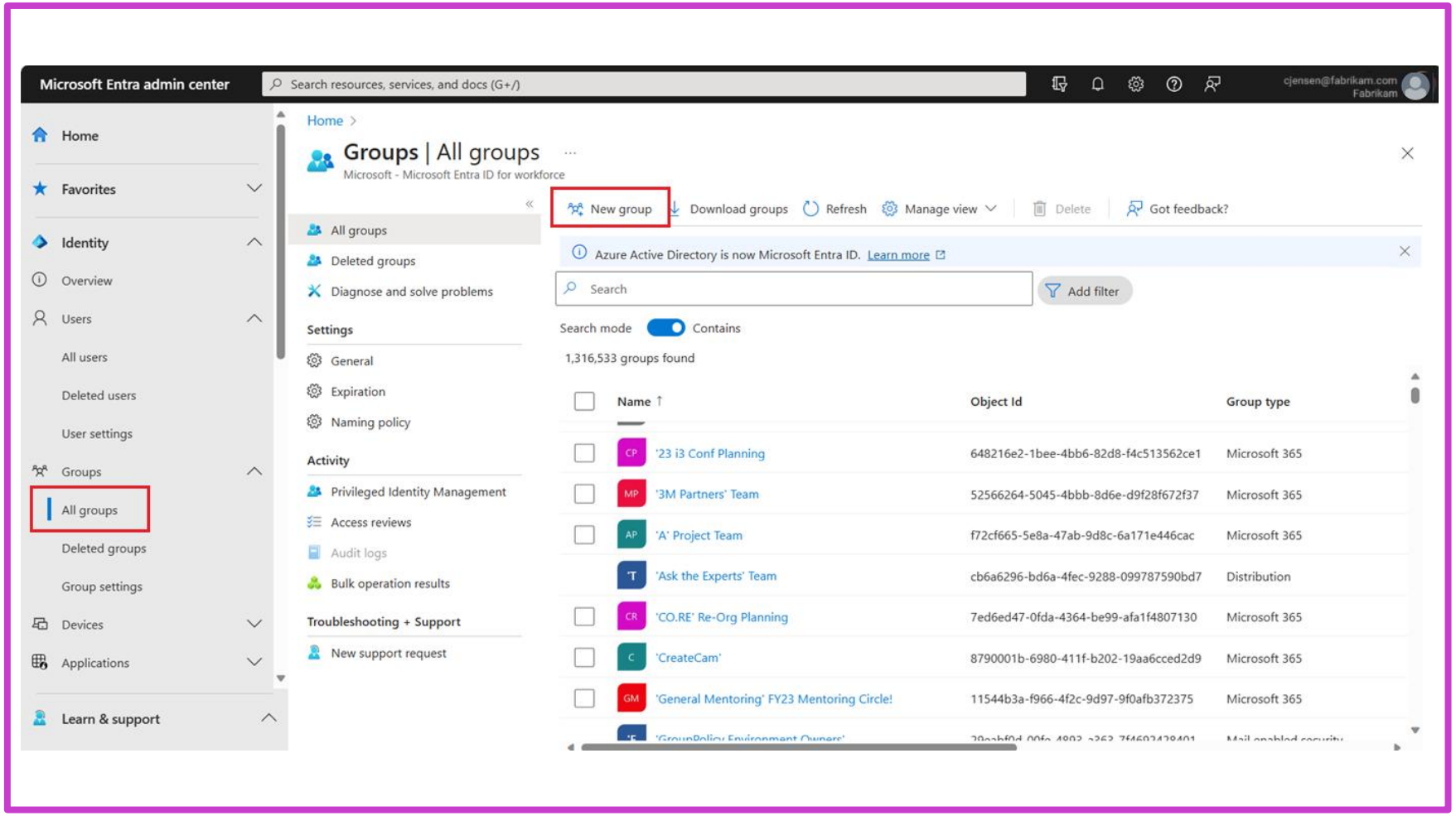
Microsoft Entra ID – Create a new user



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

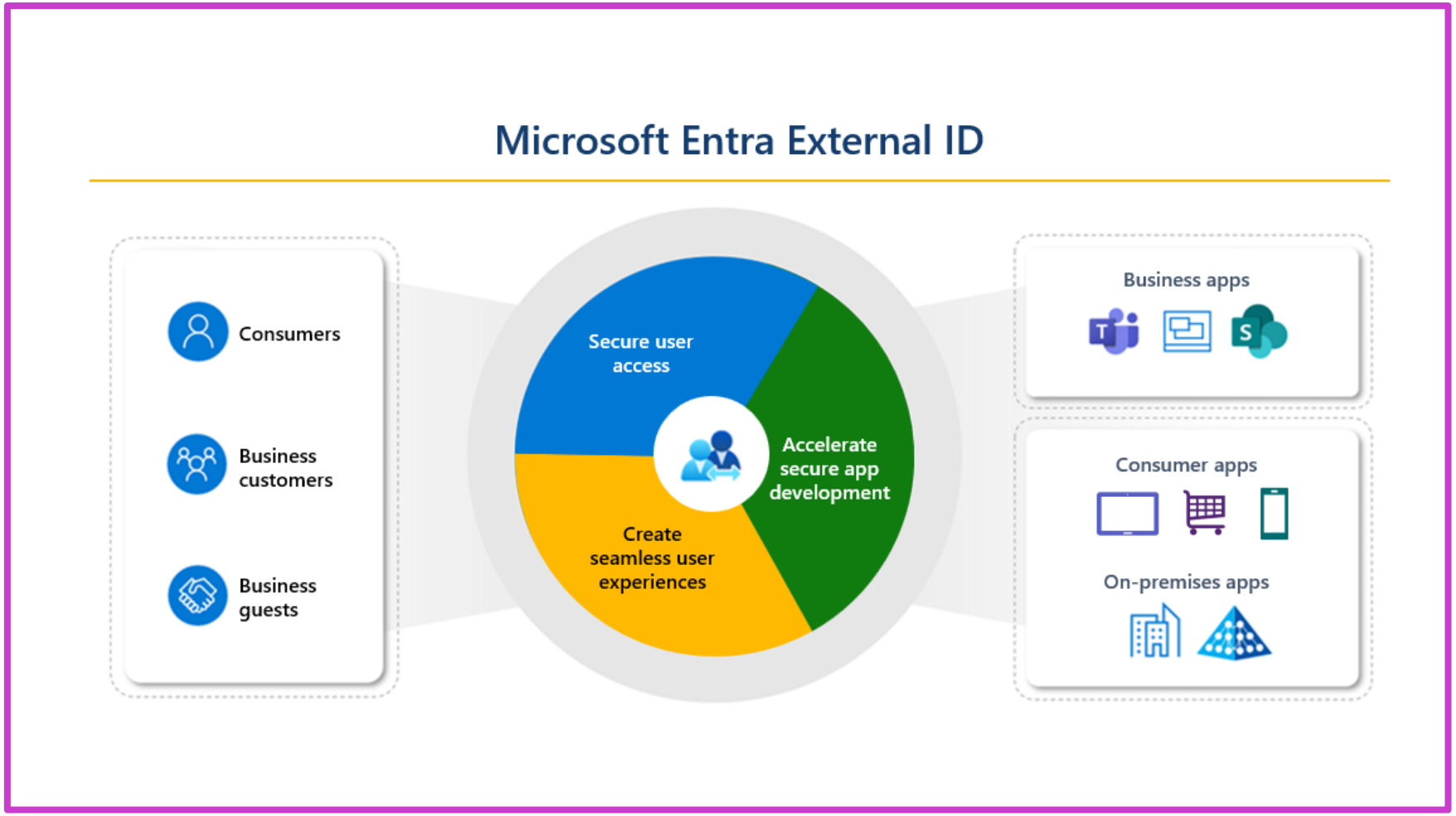
Microsoft Entra ID groups

- 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.



Microsoft Entra External ID

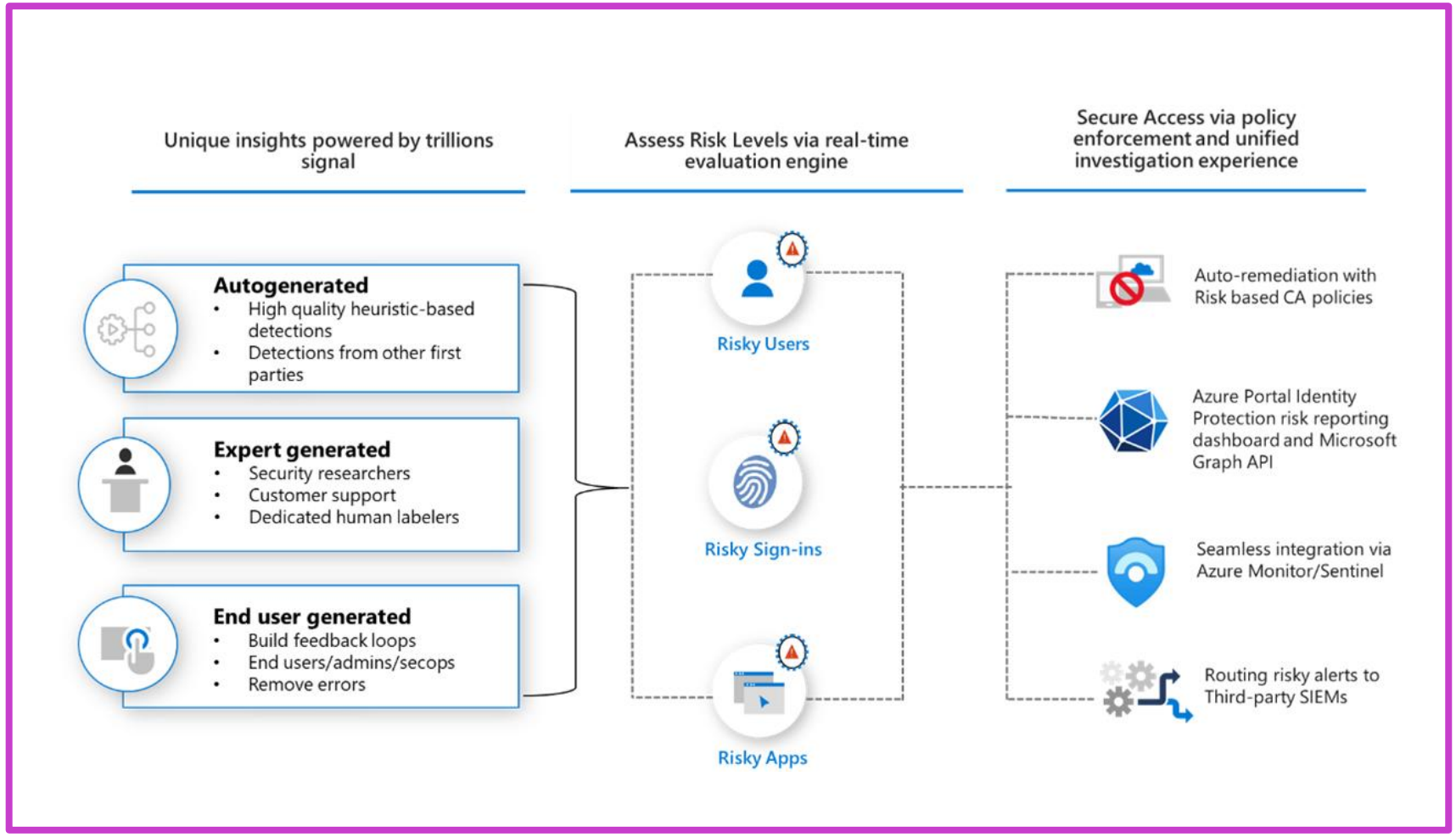
- Enable secure access for external users with social, corporate, or government-issued identities.
- Support both B2B collaboration and CIAM through workforce or external tenant configurations.
- Customize sign-in, branding, and access policies using Microsoft Entra features and APIs.



Microsoft Entra ID Protection

CA Policies

- Detects identity risks using trillions of daily signals from diverse Microsoft platforms.
- Federate on-premises with Microsoft Entra ID for robust access control, ensuring all authentication happens locally.
- Automates risk remediation via Conditional Access or manual actions through portal/API.
- Exports risk data to SIEMs; requires Entra ID P2 and relevant admin roles.

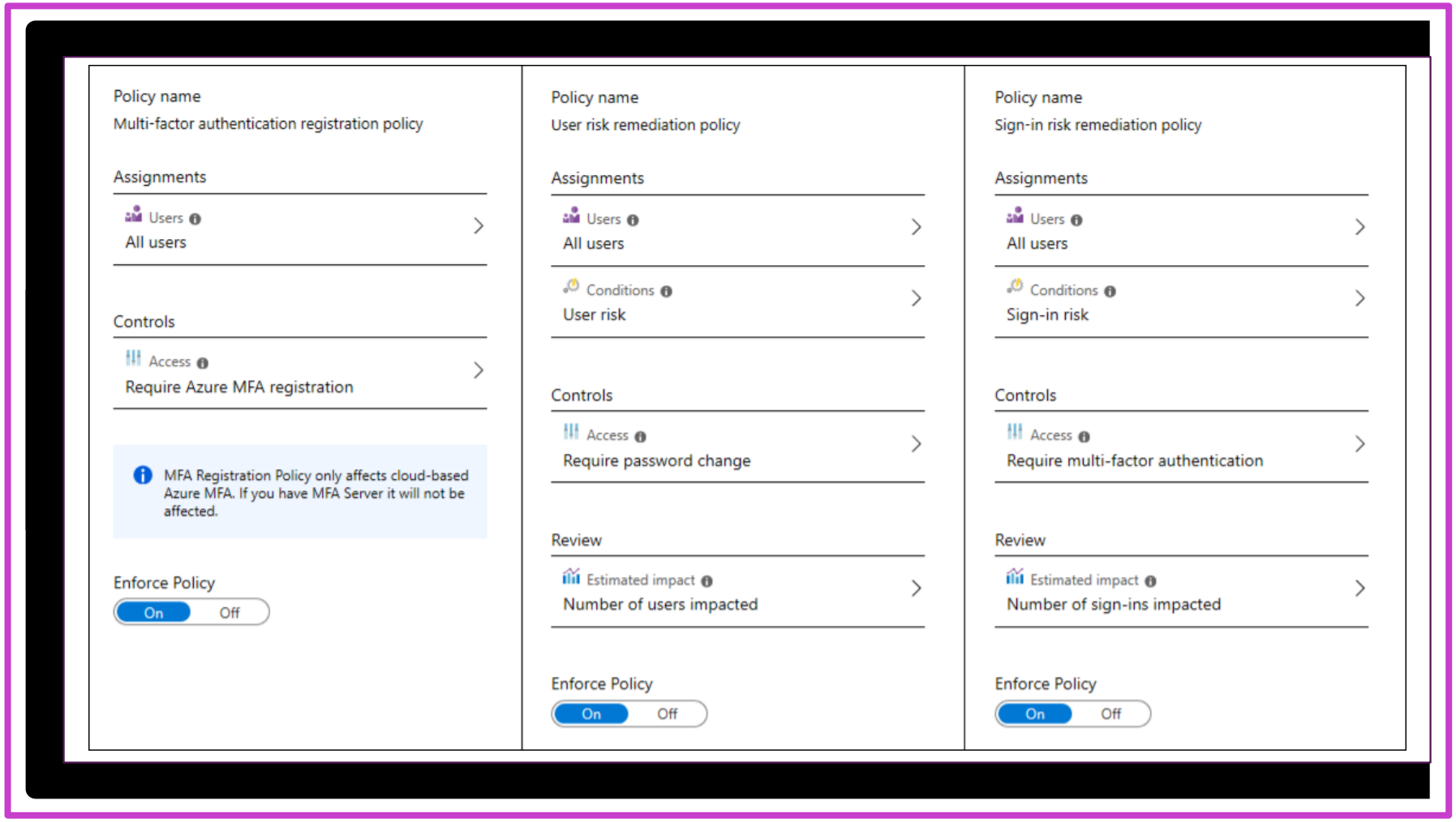


Implement Microsoft Entra ID protection

Automate the detection and remediation of identity-based risks

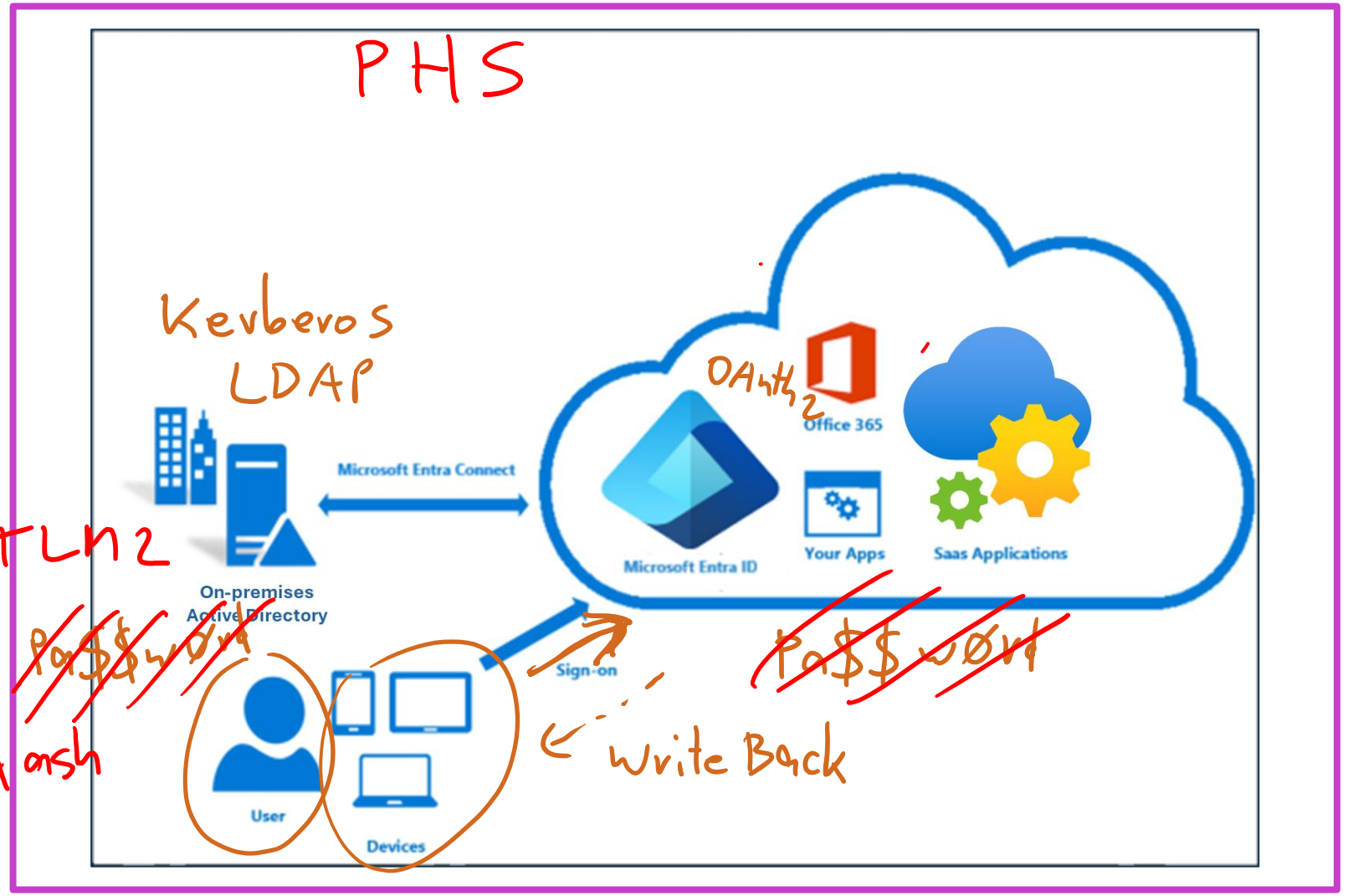
Investigate risks using data in the portal

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



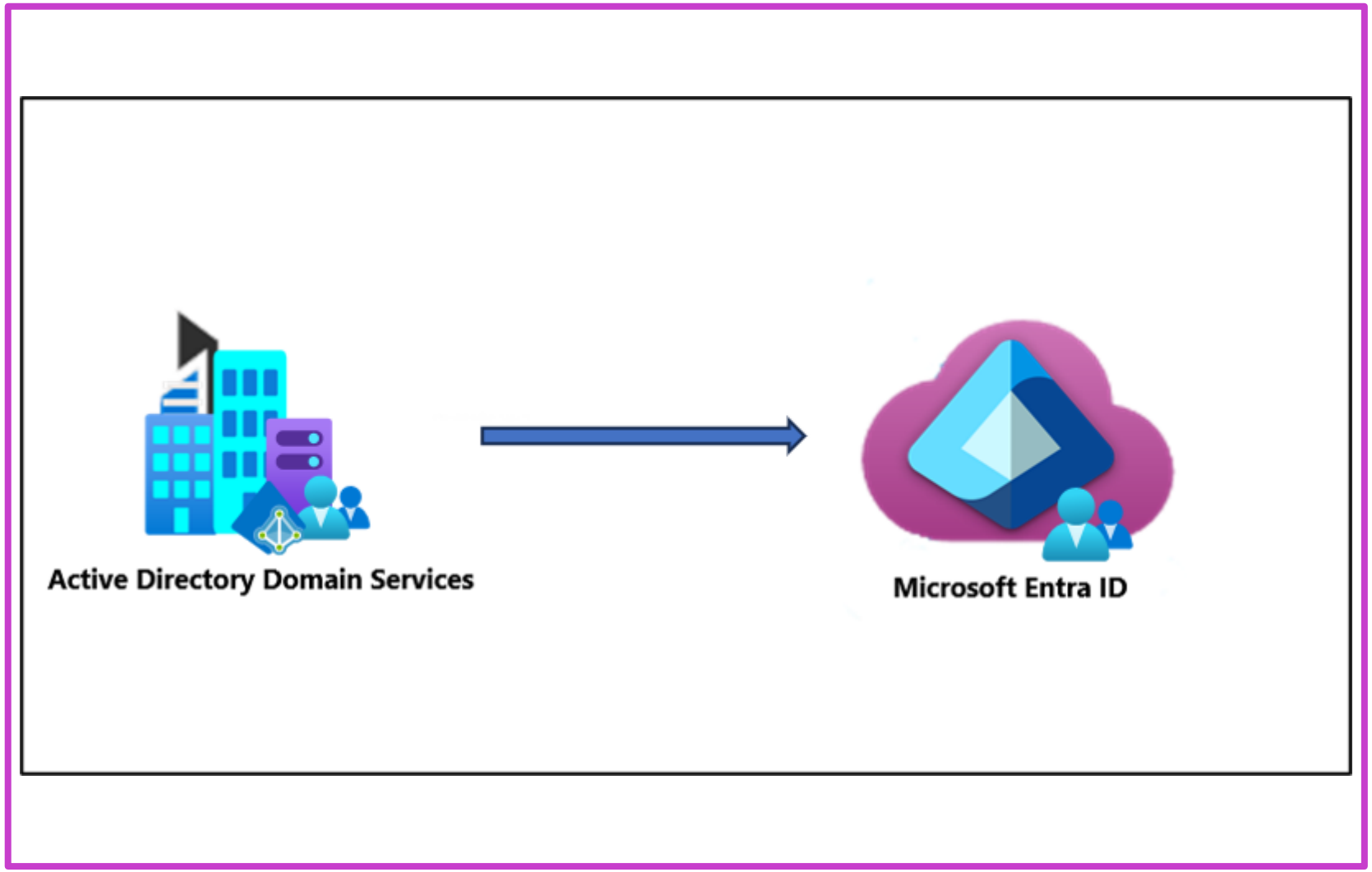
Microsoft Entra connect

- **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.



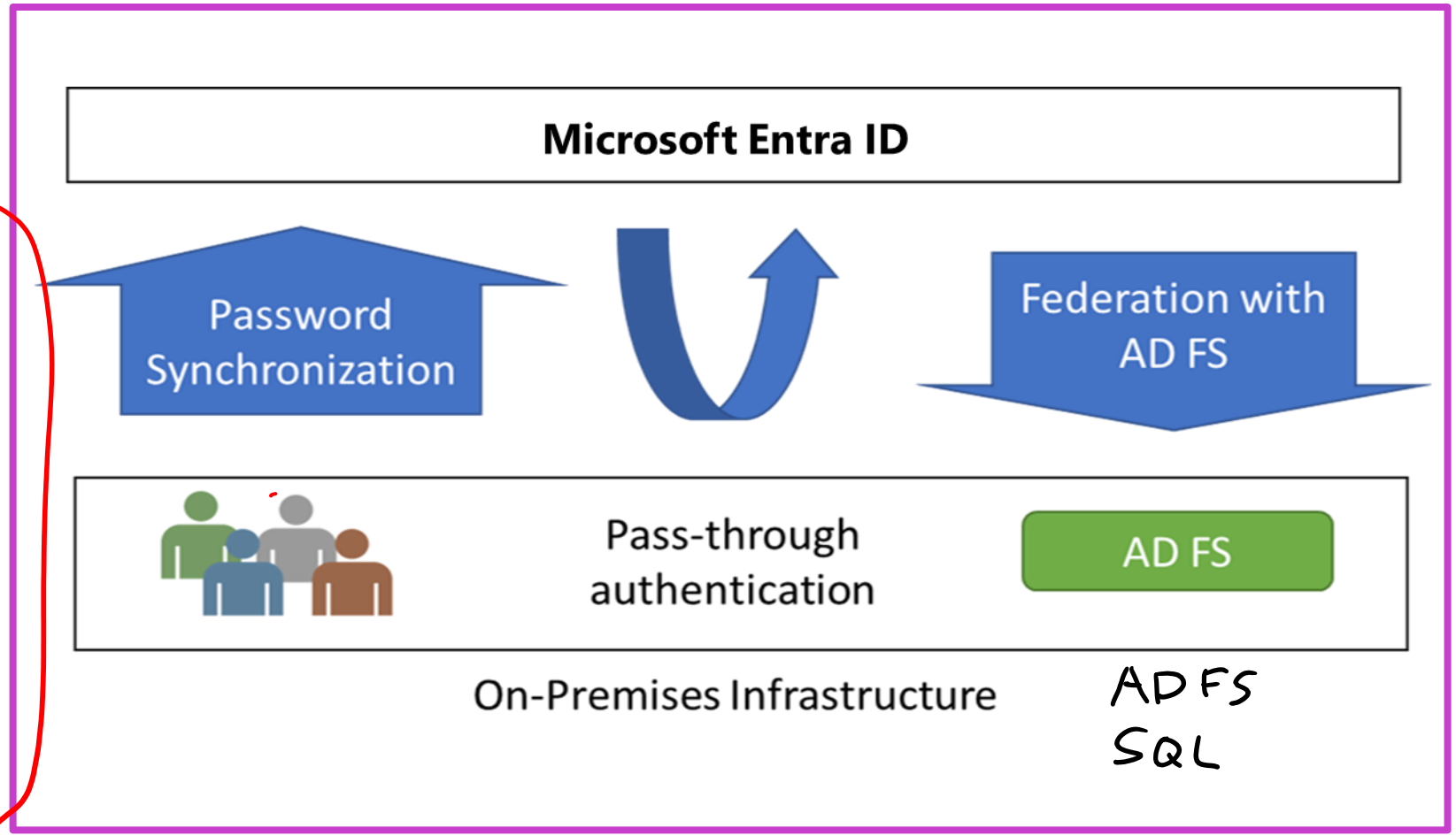
Microsoft Entra cloud sync

- **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.

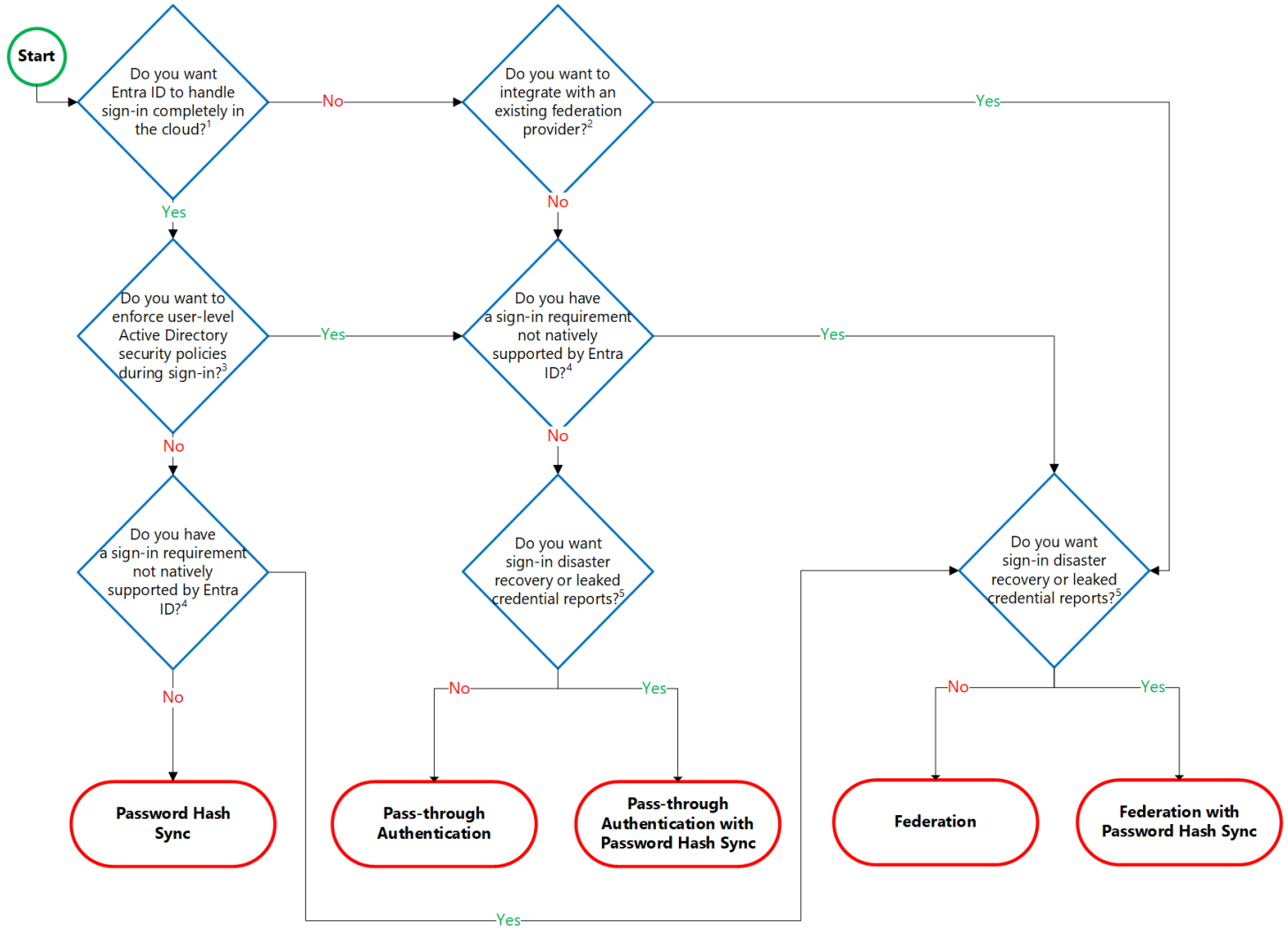


Authentication options

- **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.

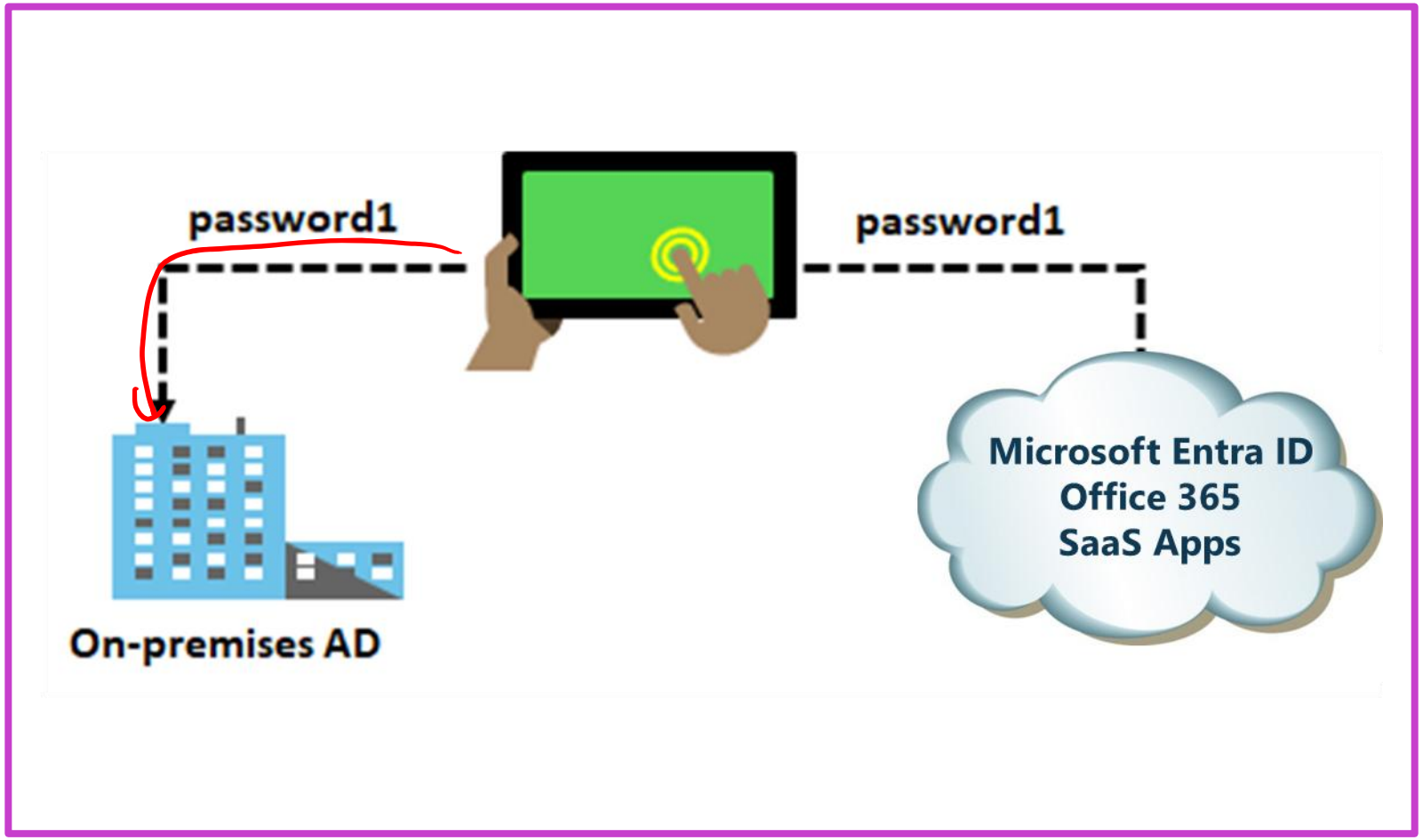


Authentication decision tree



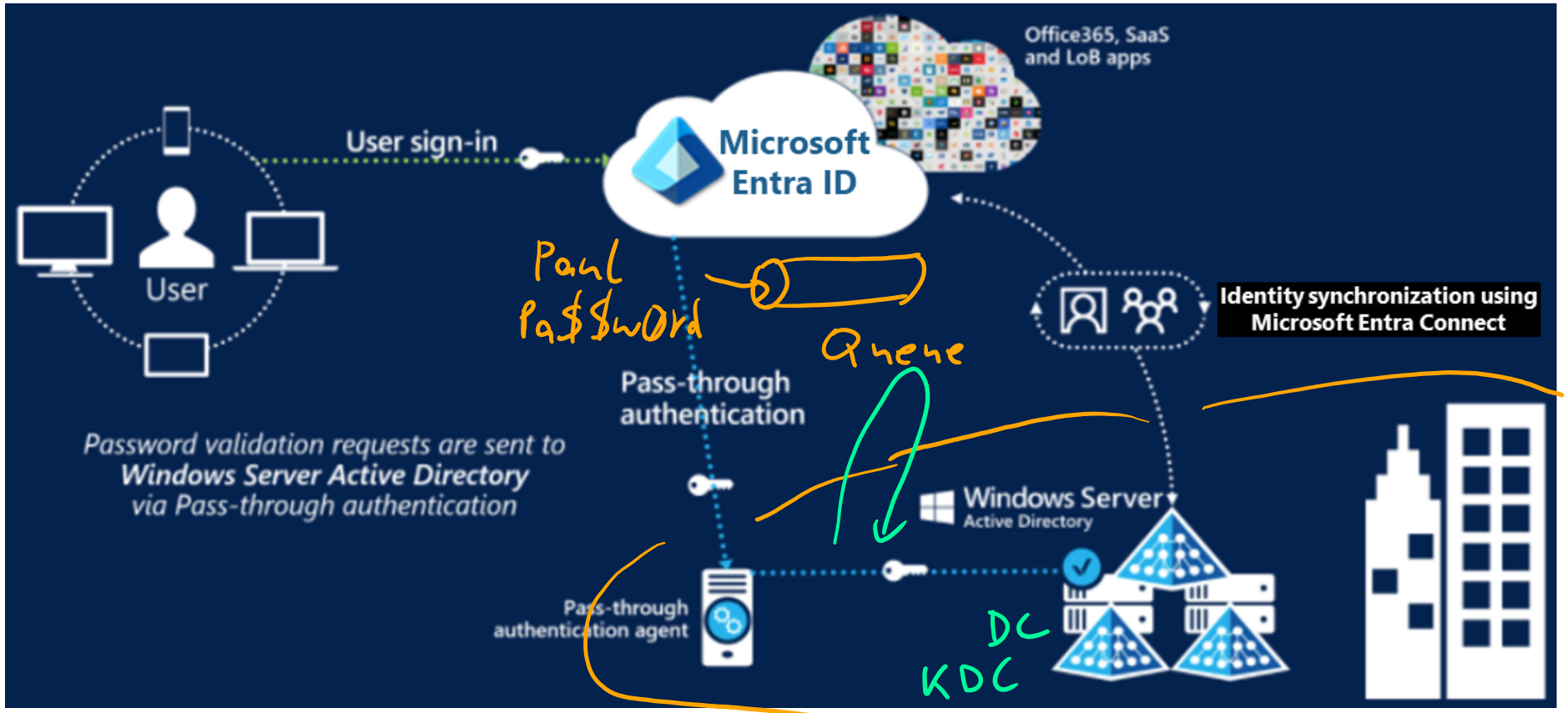
Password hash synchronization with Microsoft Entra ID

- 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

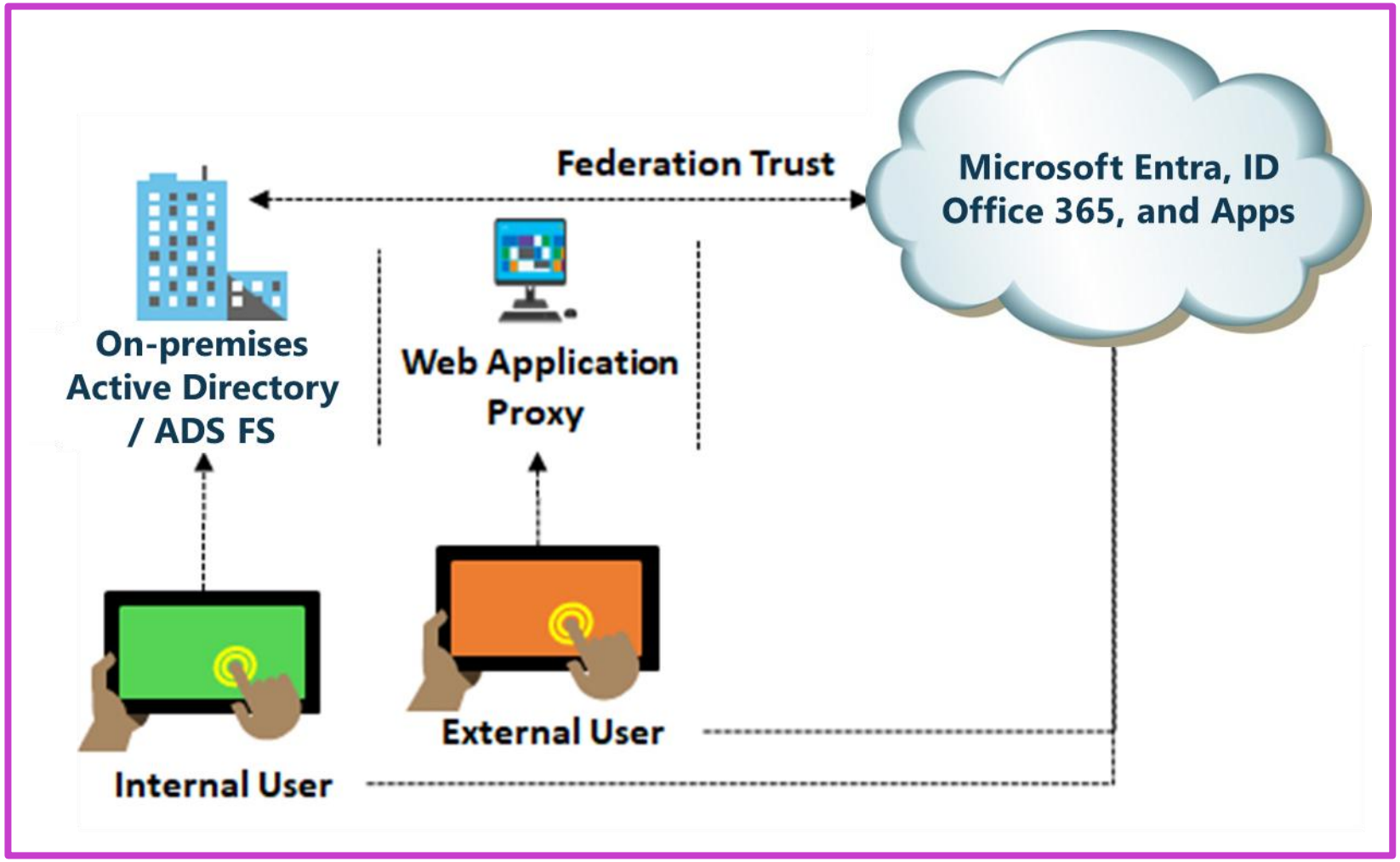
PTA



- Sign in to on-premises and cloud apps with the same password, improving user experience.
- Easy deployment with a lightweight agent, no complex setup.
- Secure with Conditional Access, high availability, and self-service password management.

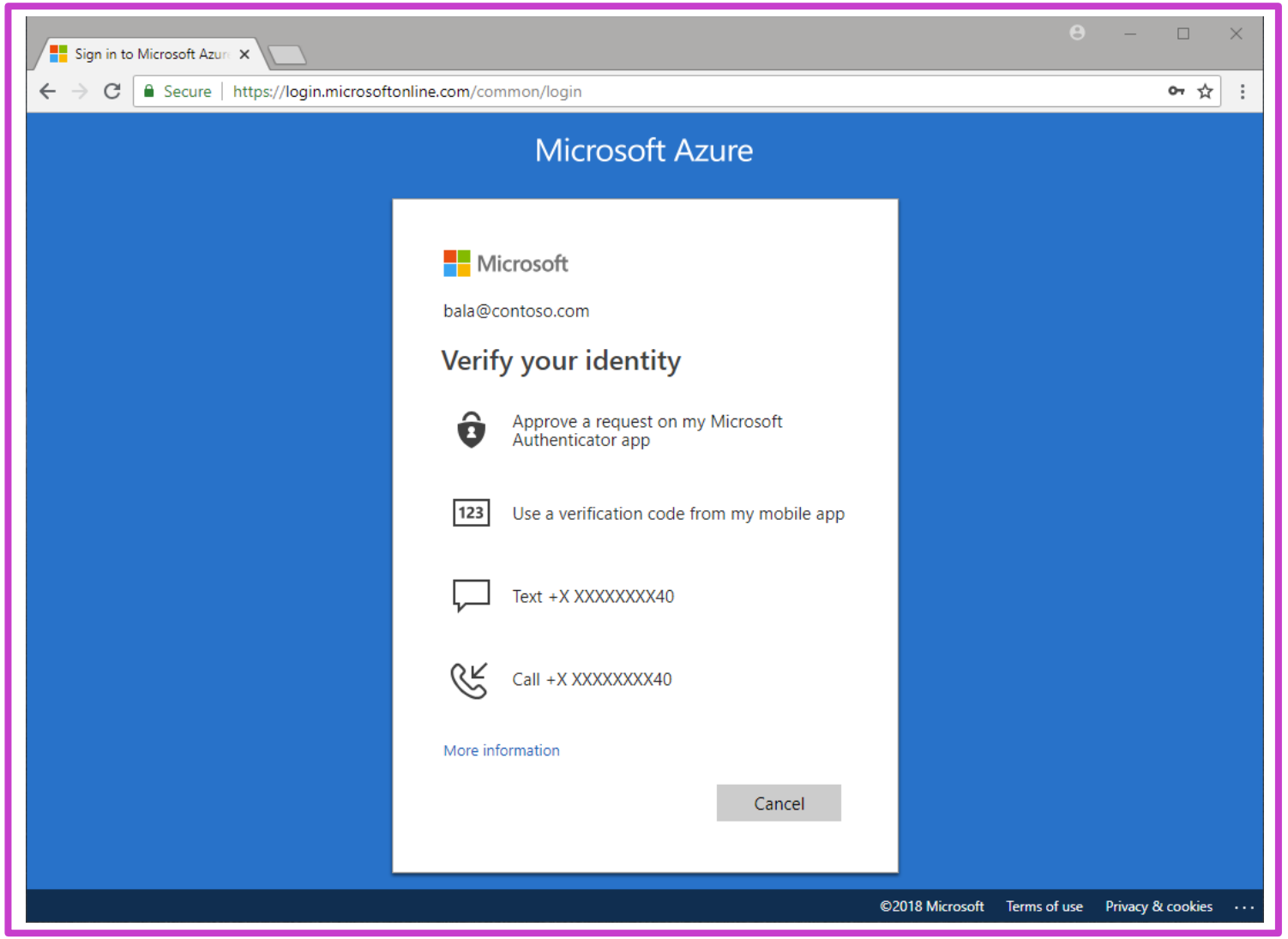
Federation with Microsoft Entra ID

- 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.



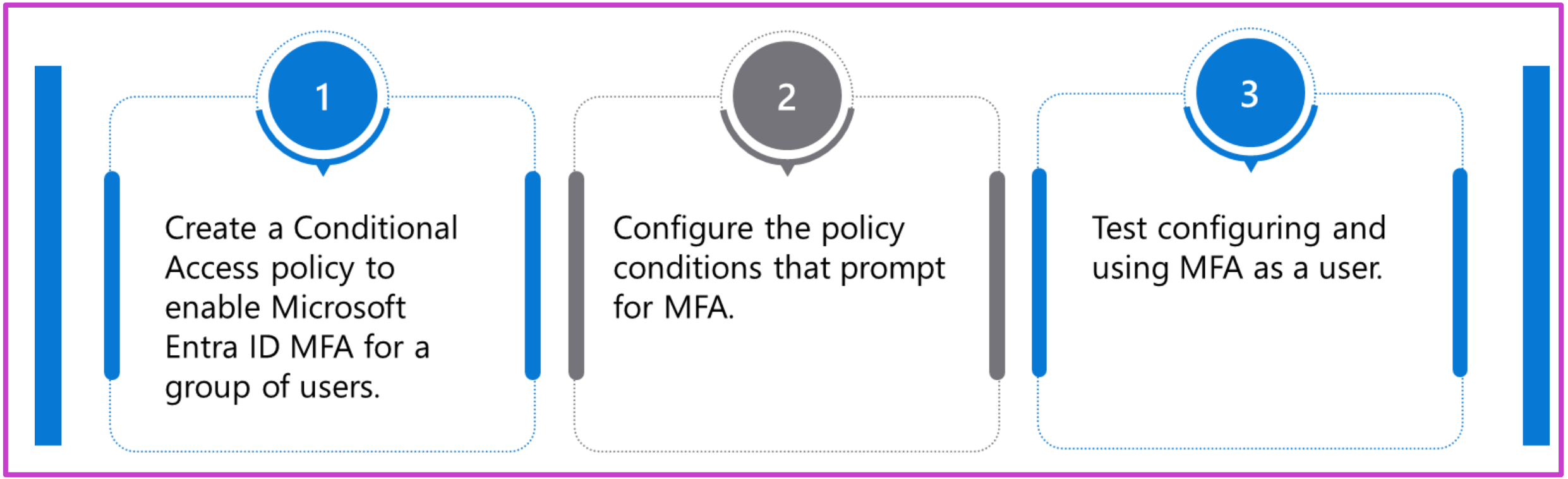
Microsoft Entra authentication

- 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) for Azure resources

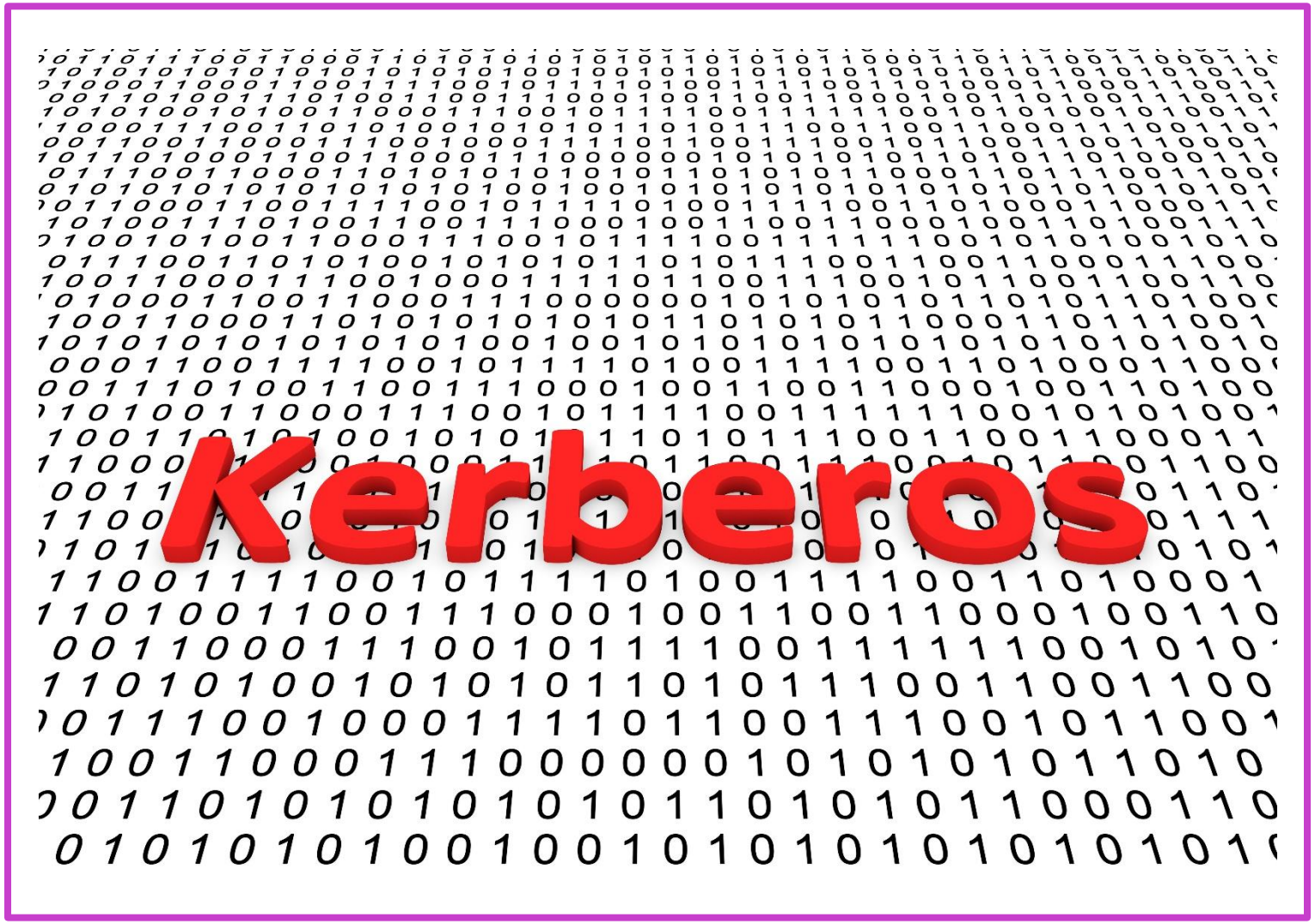
Perform the following tasks to implement MFA:



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

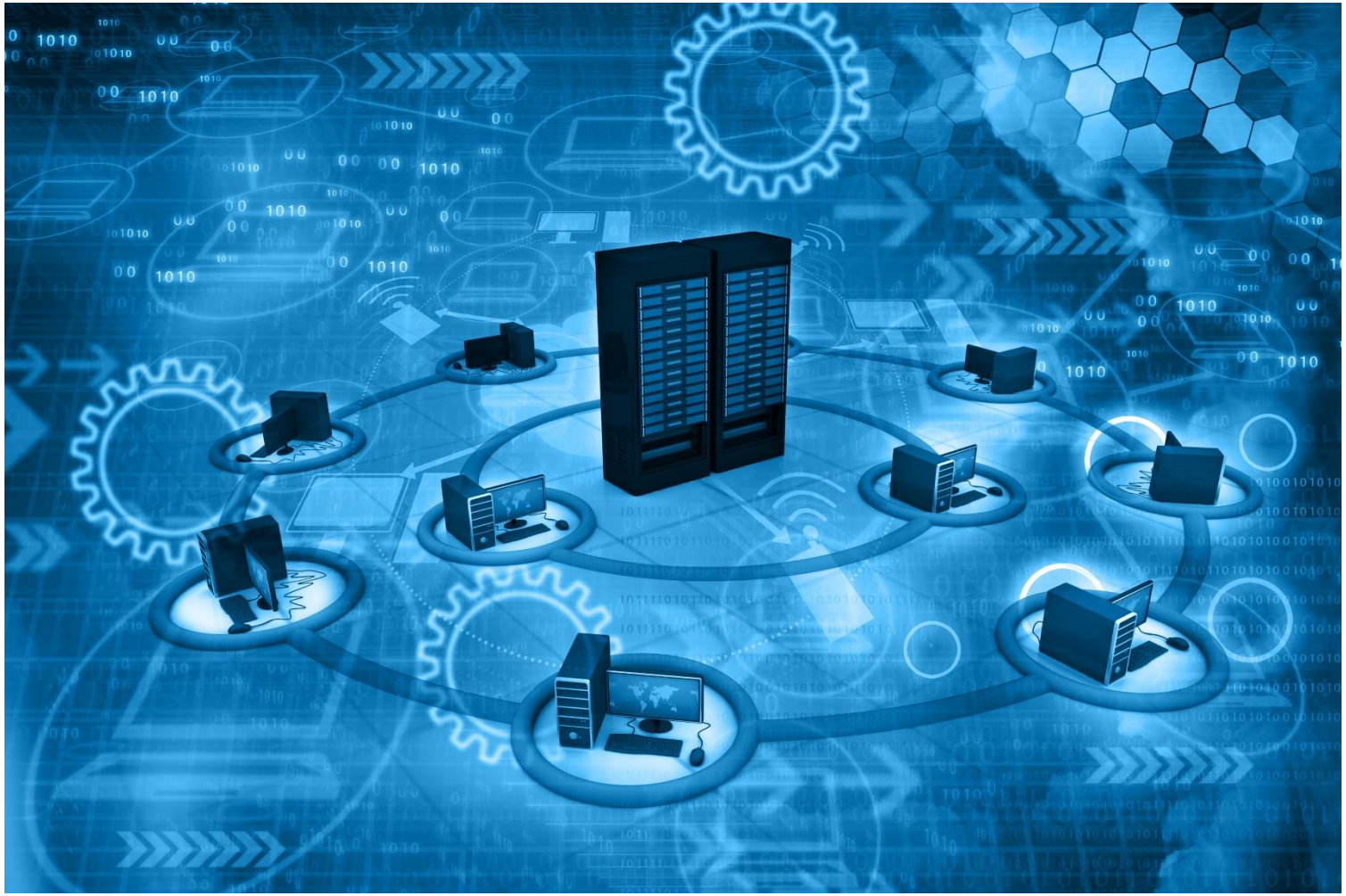
Kerberos Authentication

- Comprehensive Authentication: Kerberos provides secure, single sign-on, and delegated authentication for domain resources.
- Integrated with Active Directory: Kerberos uses AD for security accounts and supports efficient credential management.
- Interoperability & Efficiency: Kerberos ensures mutual authentication and seamless integration across networks with reusable session tickets.



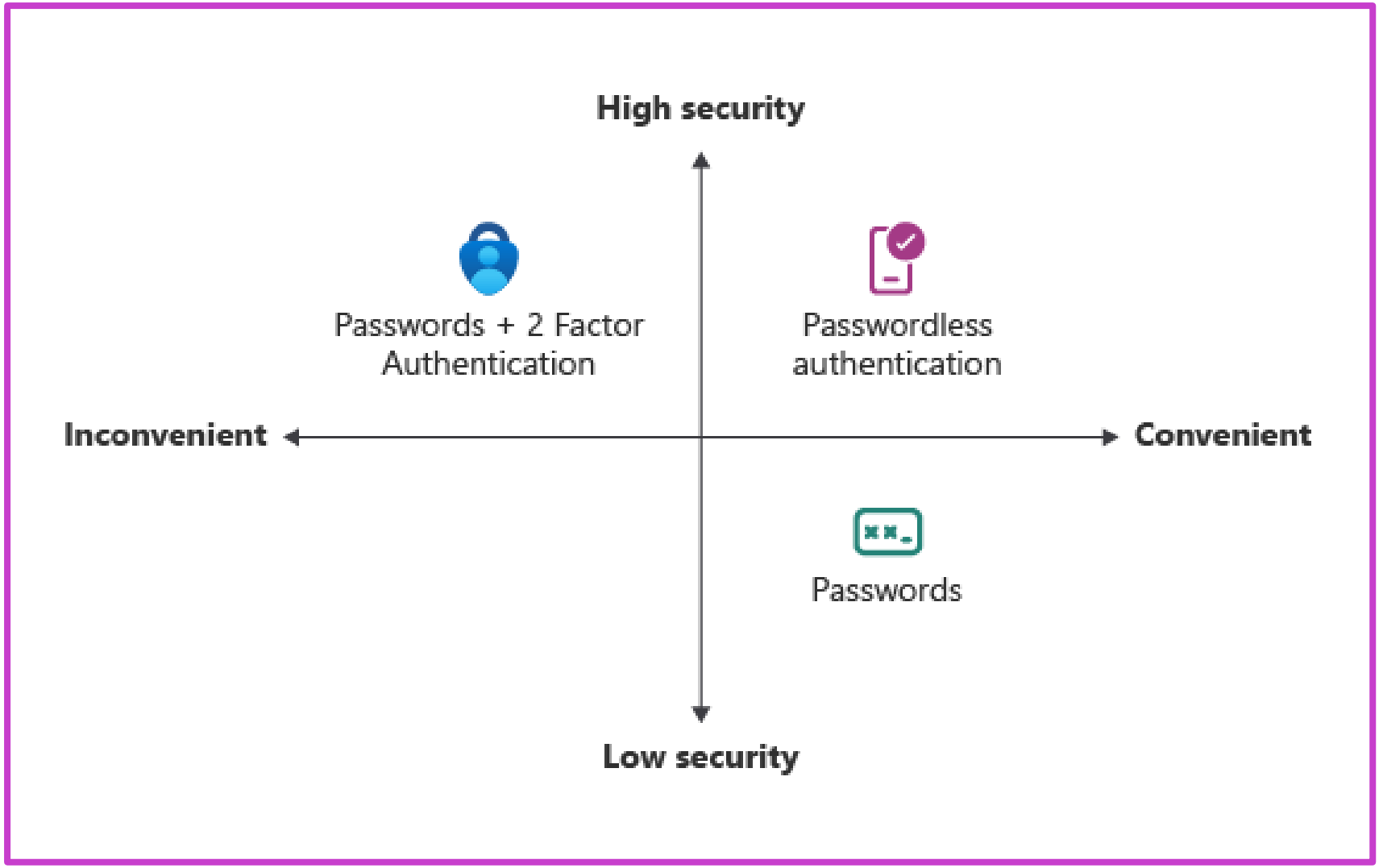
New Technology Local Area Network Manager (NTLM)

- Authentication Protocol: NTLM uses a challenge/response mechanism to authenticate users and computers.
- Workgroup Support: NTLM is essential for Windows authentication in workgroups and local logons.
- Legacy Protocol: While Kerberos is preferred, NTLM remains used in specific applications and environments.



Passwordless authentication options for Microsoft Entra ID

- Passwordless authentication replaces passwords with biometrics, PINs, or security keys for convenience.
- Microsoft Entra supports methods like Windows Hello, Authenticator, FIDO2, and certificate-based auth.
- Choose methods based on user roles, devices, and environments to enhance security and usability.

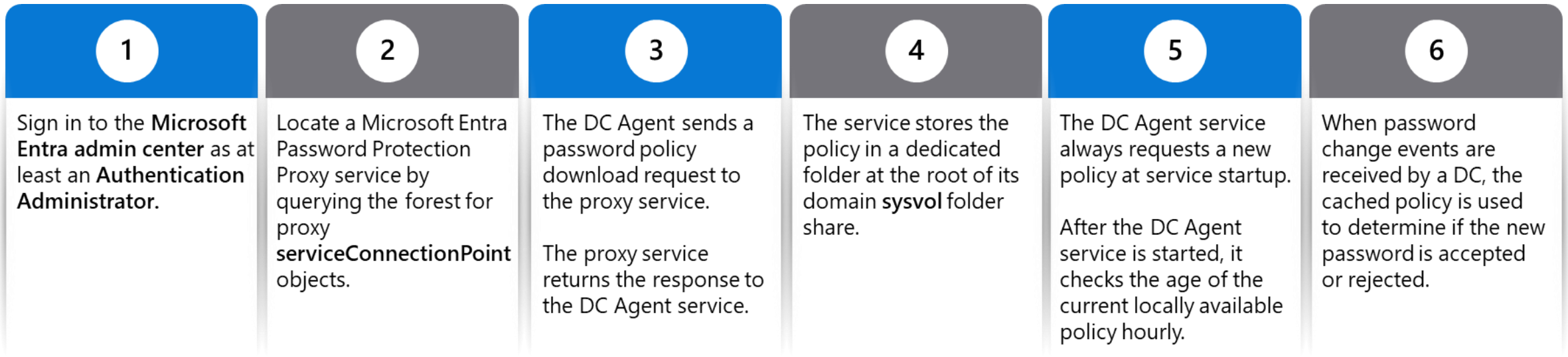


Implement passwordless authentication

- 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 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:

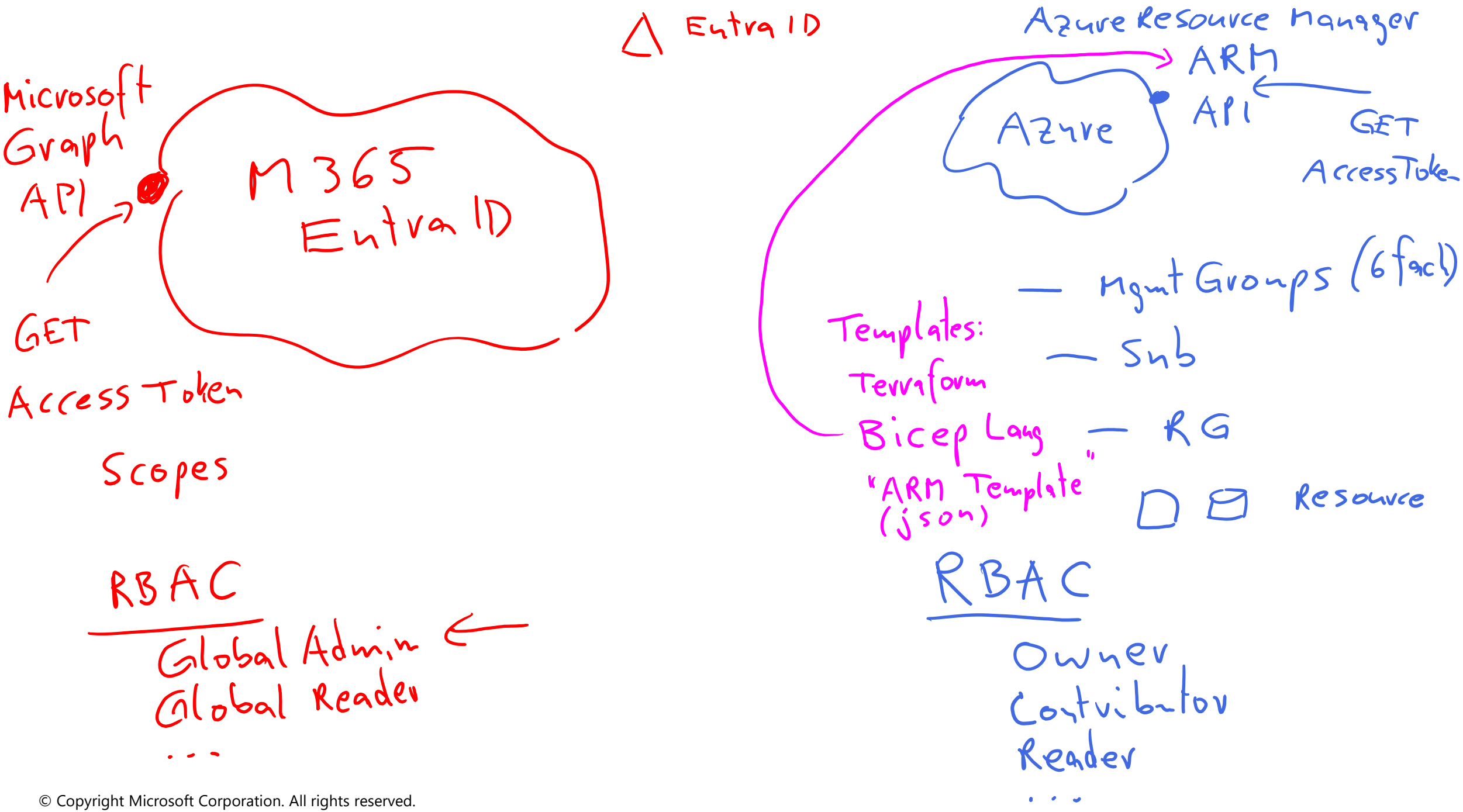
Roles: Opt for roles with the least permissions necessary and review periodically.

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

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

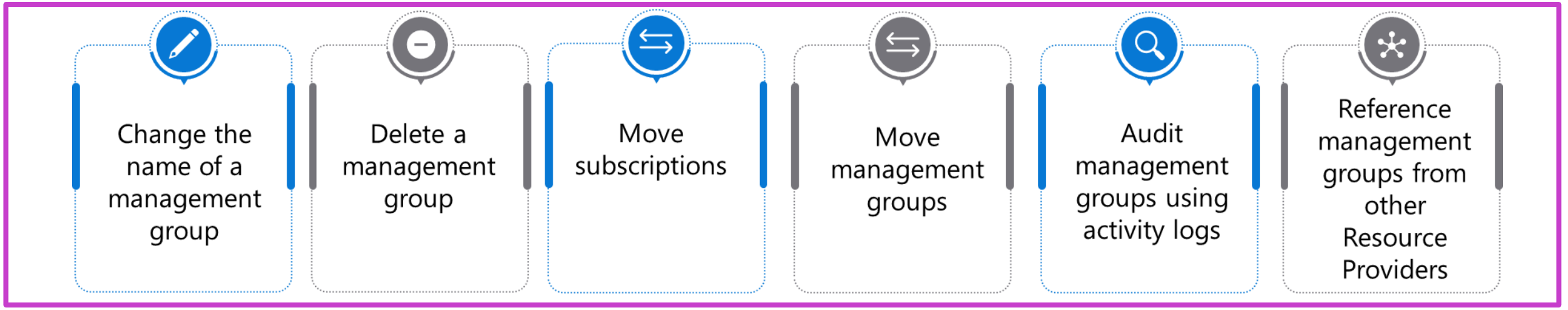
Licensing & Shared Accounts: Ensure proper licensing for Microsoft Entra ID and applications, and securely manage shared account passwords.

Understand modern authentication protocols



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

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



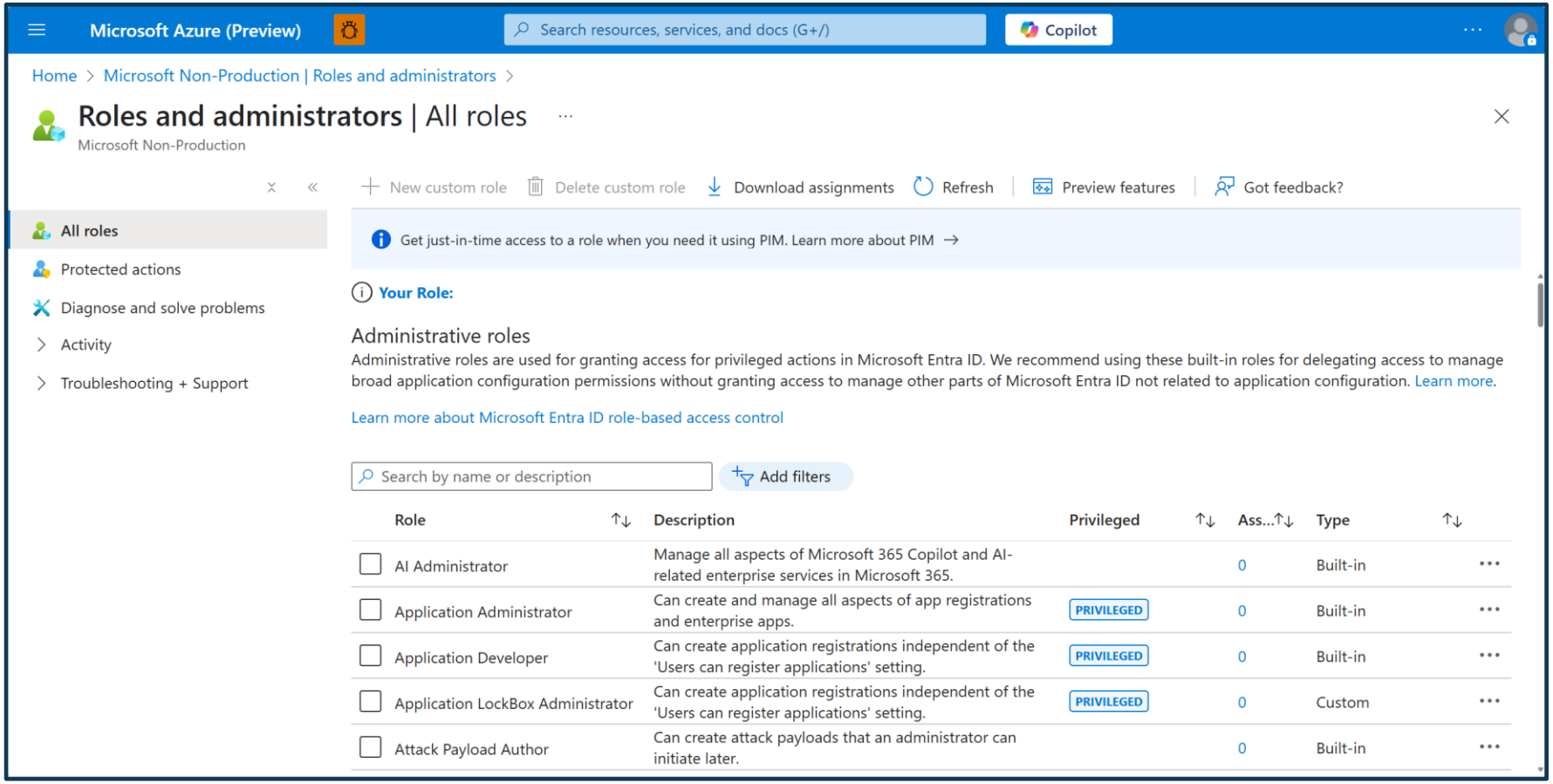
- Azure management groups organize subscriptions for centralized governance and automatic policy inheritance.
- Management groups can be renamed or deleted via portal, PowerShell, or Azure CLI with specific permissions.
- Subscriptions inherit access and policies when moved to a management group; audit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

Understand Microsoft Entra built-in role

- Assign Entra roles to delegate management of identity-related tasks and permissions.
- Roles cover actions like user management, license assignment, and domain configuration.
- Use Entra roles for identity; use Azure roles for resource management.



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.

Manage Azure built-in role assignments

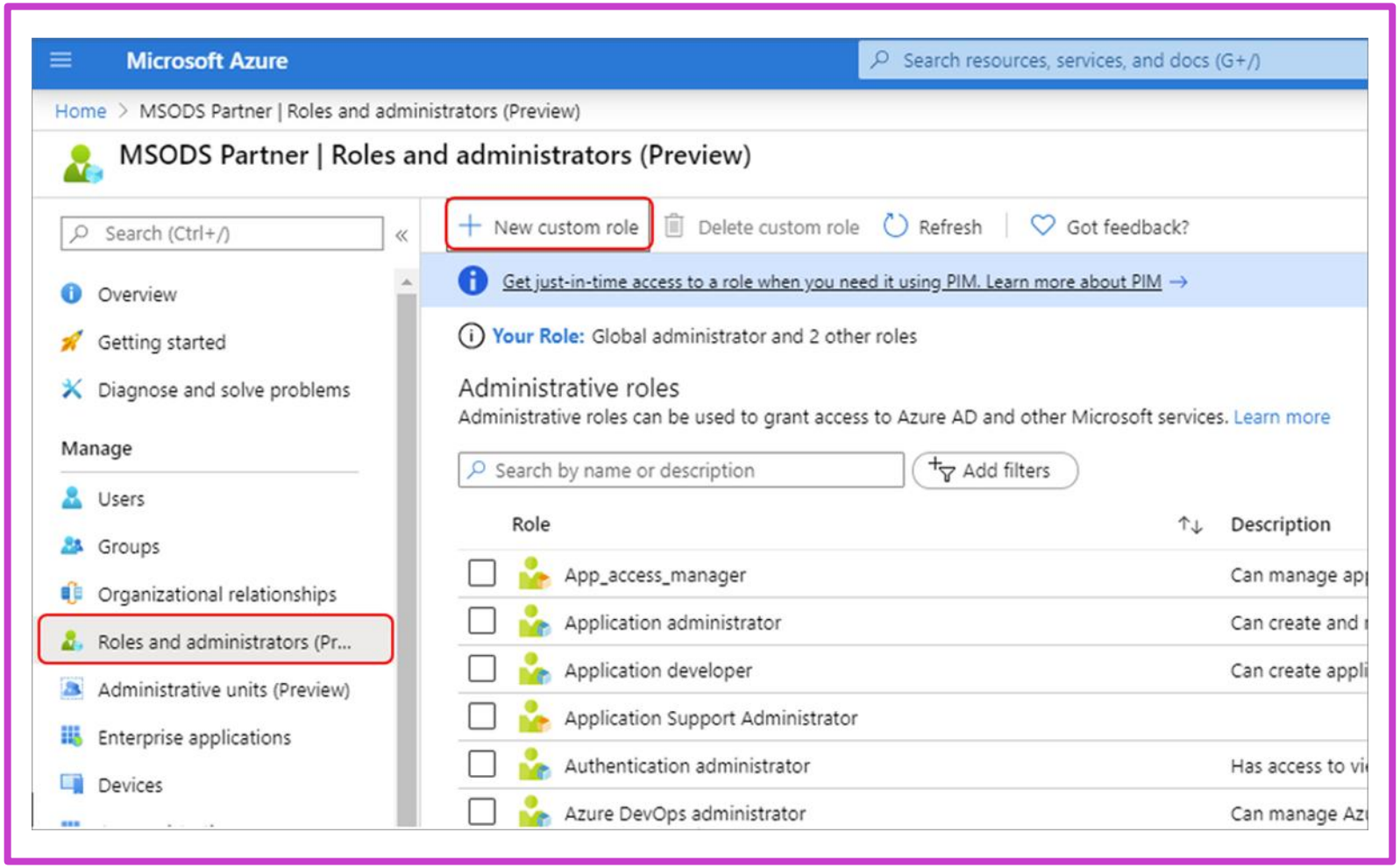
General	
Built-in role	**Description**
Contributor	Grants full access to manage all resources but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.
Owner	Grants full access to manage all resources, including the ability to assign roles 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.

- 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.

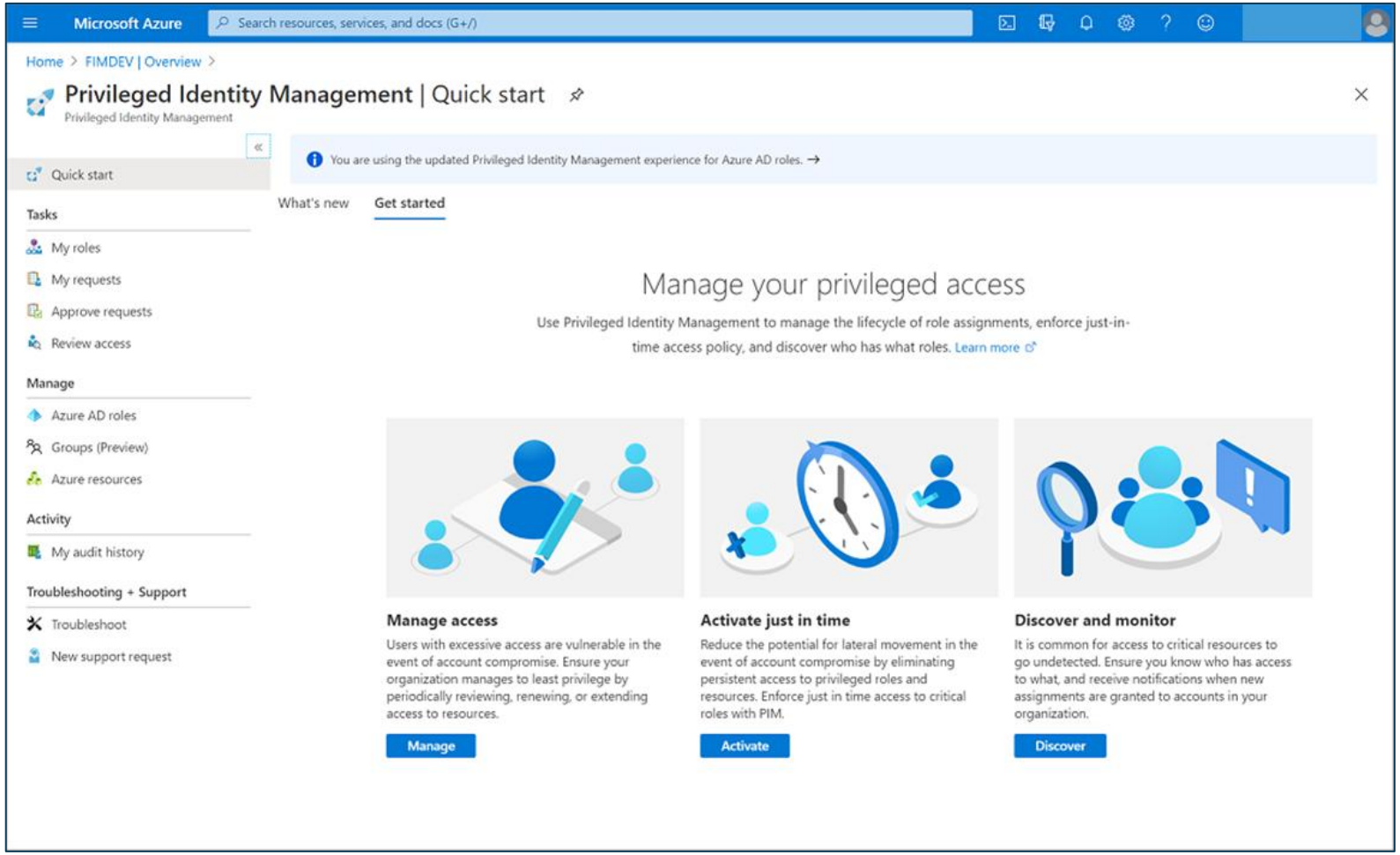
Manage custom roles, including Azure roles and Microsoft Entra ID roles

- 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 Privileged Identity Management

- 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.



Plan and manage Azure resources in Microsoft Entra Privileged Identity Management, including settings and assignments

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

Access reviews

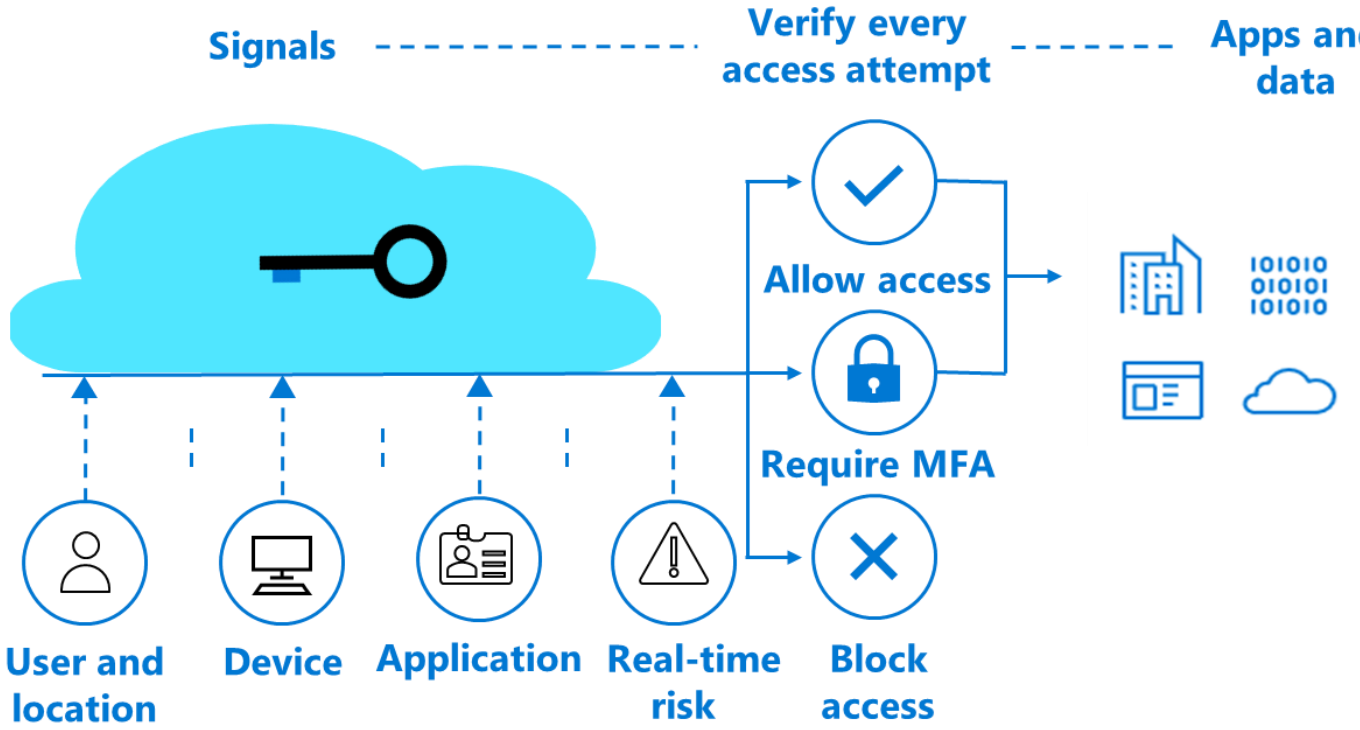
- Manage group memberships, app access, and roles with Microsoft Entra ID; ensure only authorized access.
- Review access for internal/external users, adjusting for roles changes or departures to maintain security.
- Use access reviews for over-privileged roles, automation limits, new group purposes, 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

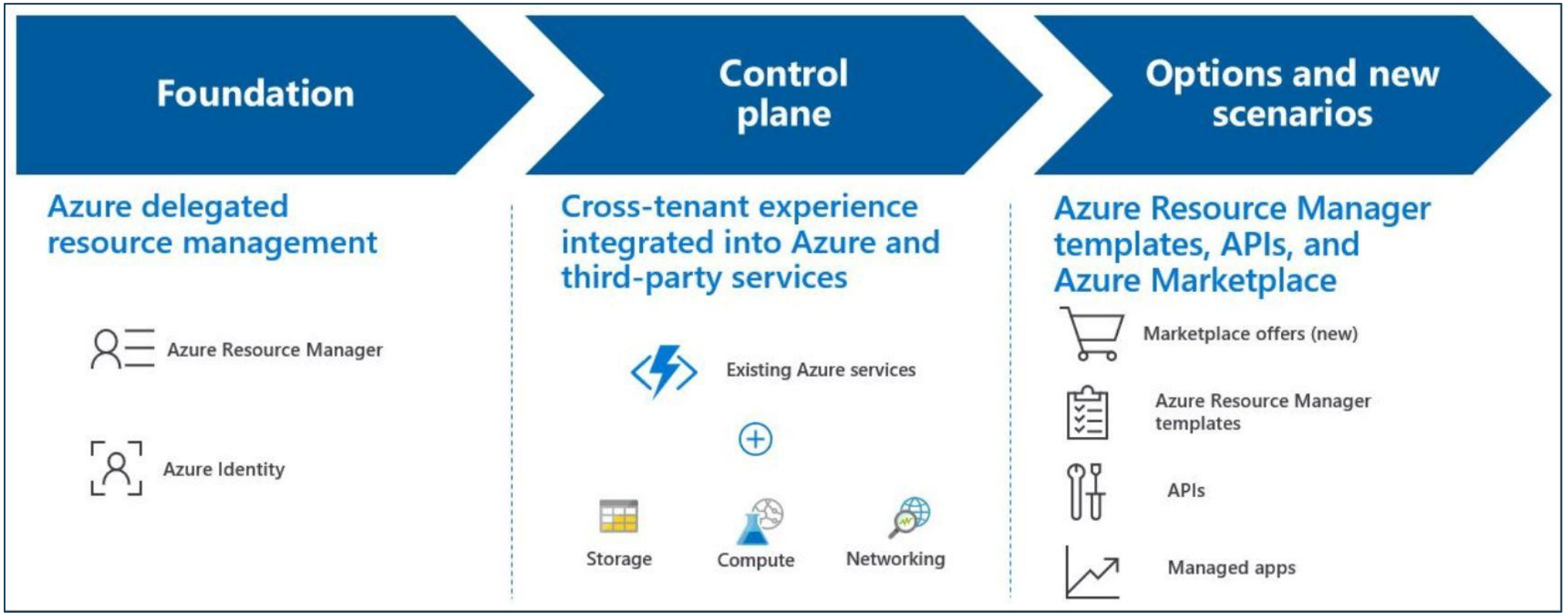
Access rights of users	Reviewers can be	Review created in	Reviewer experience
Security group members Office group members	Specified reviewers Group owners Self-review	access reviews Microsoft Entra groups	Access panel
Assigned to a connected app	Specified reviewers Self-review	access reviews Microsoft 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

Implement Conditional Access policies for Azure cloud resources



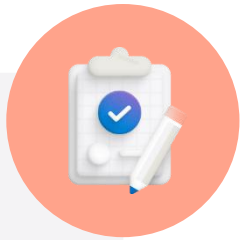
- Exclude emergency access and service accounts from MFA to prevent lockouts and ensure access.
- Administrators can exclude certain applications from MFA policies based on security needs.
- Option to deploy MFA policies via direct steps or Conditional Access templates for flexibility.

Azure Lighthouse



- Azure Lighthouse enables scalable, automated, and secure multitenant management across Azure resources.
- It provides delegated resource management, cross-tenant visibility, and unified platform tooling.
- No additional cost, supports multiple licensing models, and integrates with Azure services.

Additional study – Manage security controls for identity and access



Module Review Questions

- Manage Azure Built-in Roles:
  Assign roles to users, groups, or service principals for resource access.
- Create and Manage Custom Roles:
  Define custom permissions in Azure and Microsoft Entra.
- Use Microsoft Entra Permissions Management:
  Discover, remediate, and monitor cloud permissions.
- Manage Azure Resources with PIM:
  Enable just-in-time access and secure privileged roles.
- Implement MFA and Conditional Access:
  Strengthen identity security with MFA and access policies.

Microsoft Learn Modules (docs.microsoft.com/Learn)

Manage Microsoft Entra application access

Manage access to enterprise applications in Microsoft Entra ID

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.

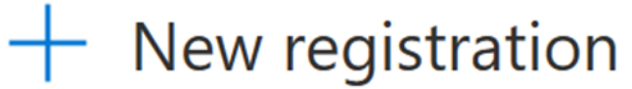
Main ways to access a Microsoft-published application:

- 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.



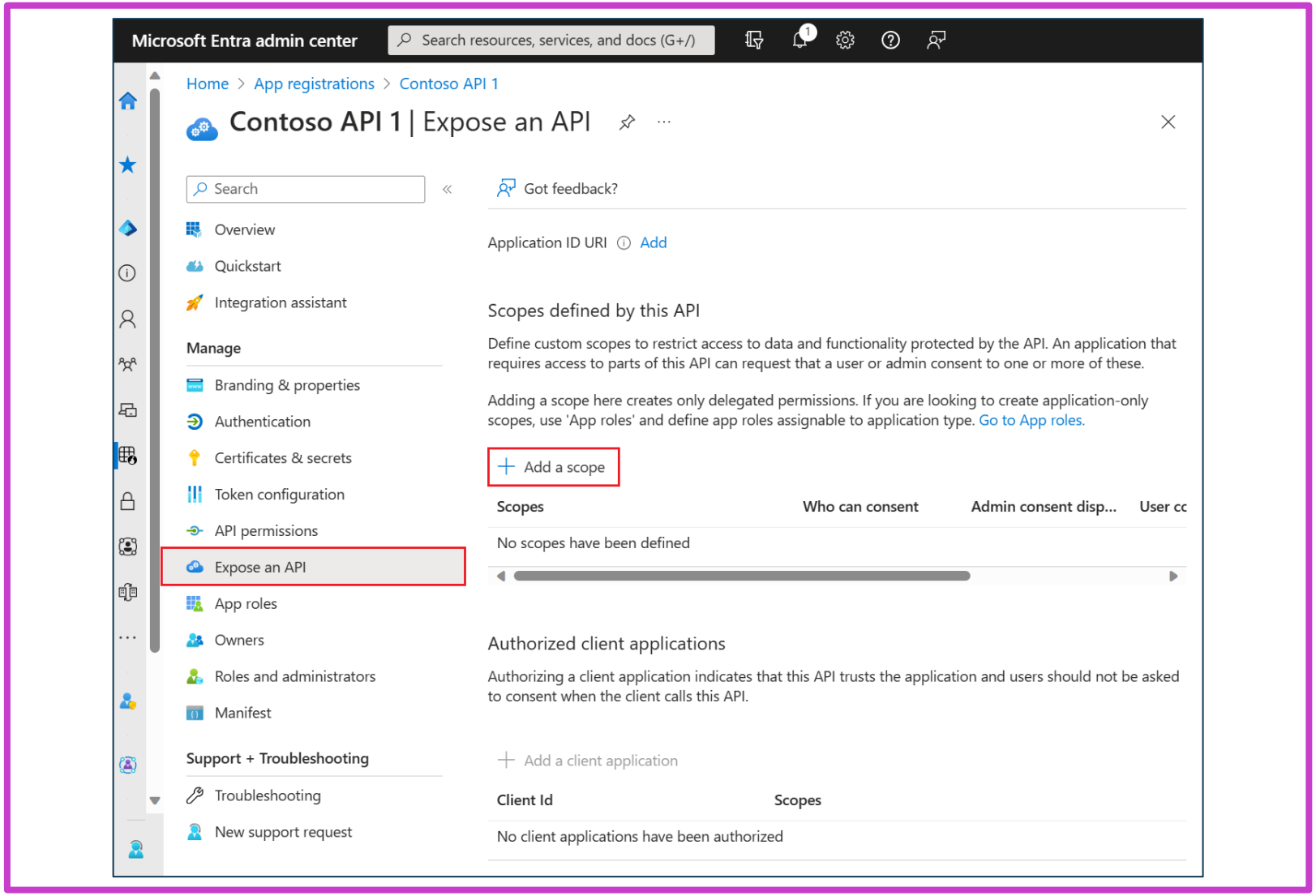
2. **Setting Up:** Name the app, select account type, and set a Redirect URI.

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.

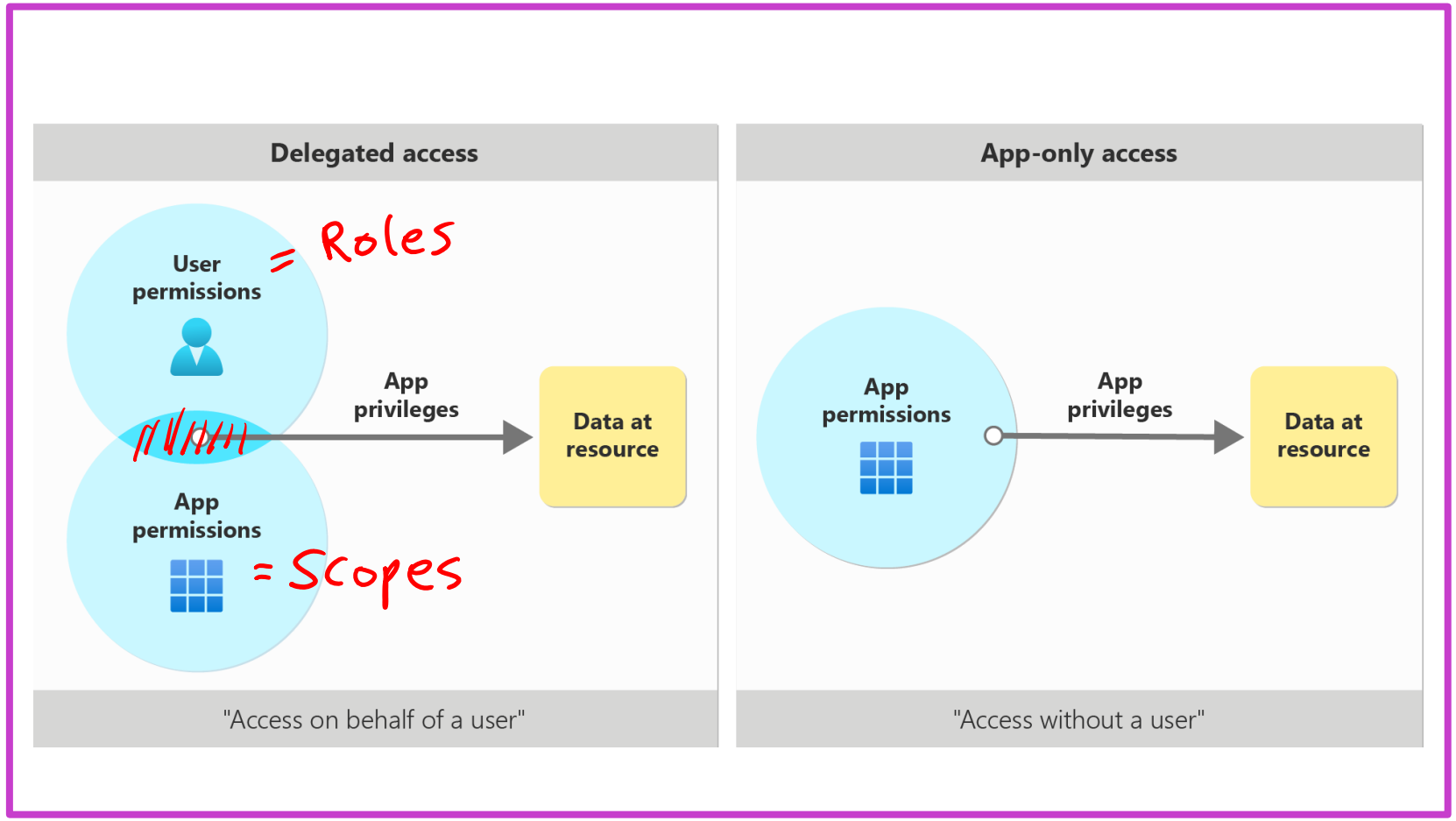
Configure app registration permission scopes

- 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.



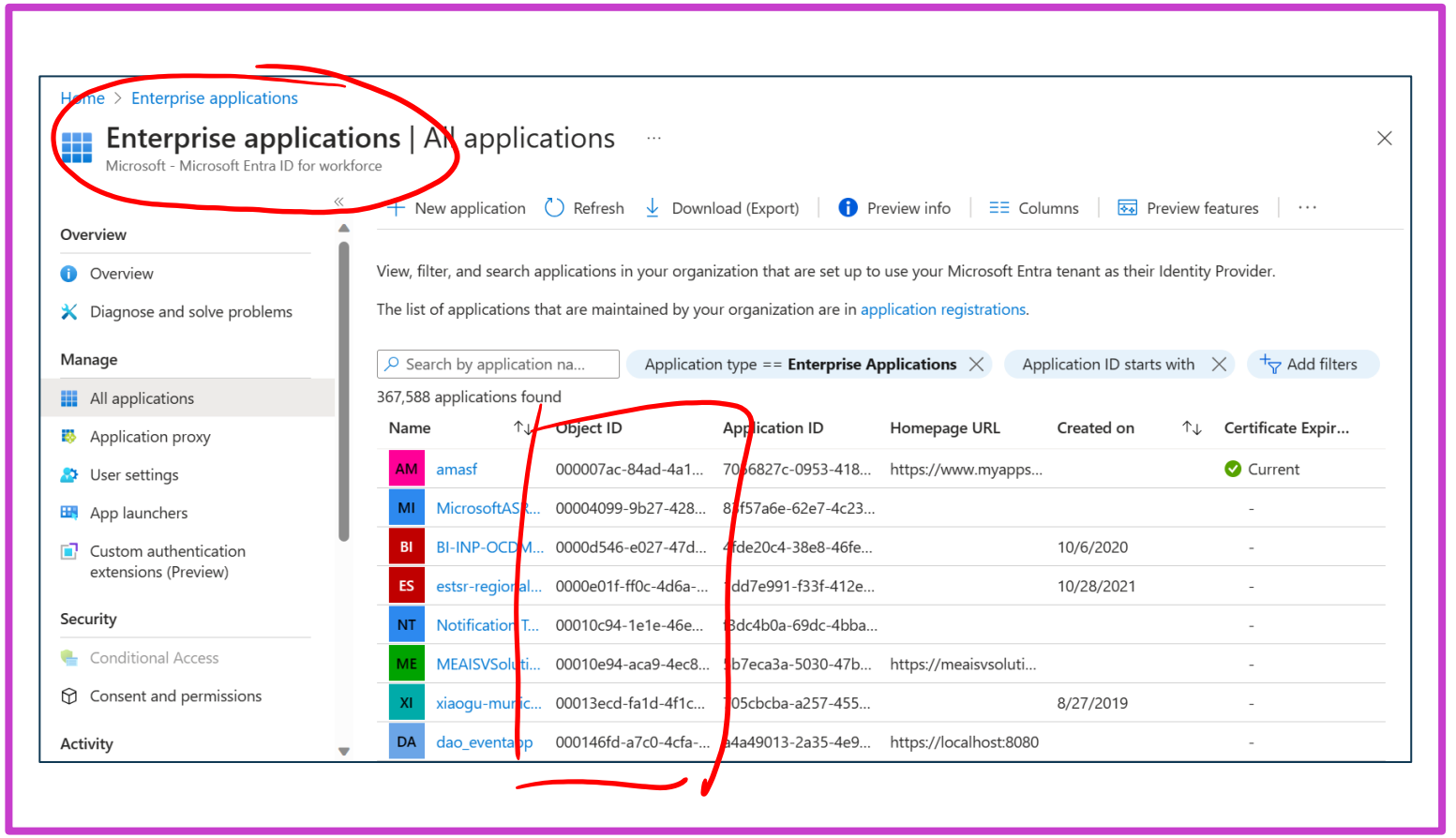
Manage app registration permission consent

- Two permission types: delegated (user-based) and application (app-only, admin consent required).
- Consent allows apps to access protected data via user or admin approval.
- Preauthorization avoids prompts; roles like Azure RBAC also control access.



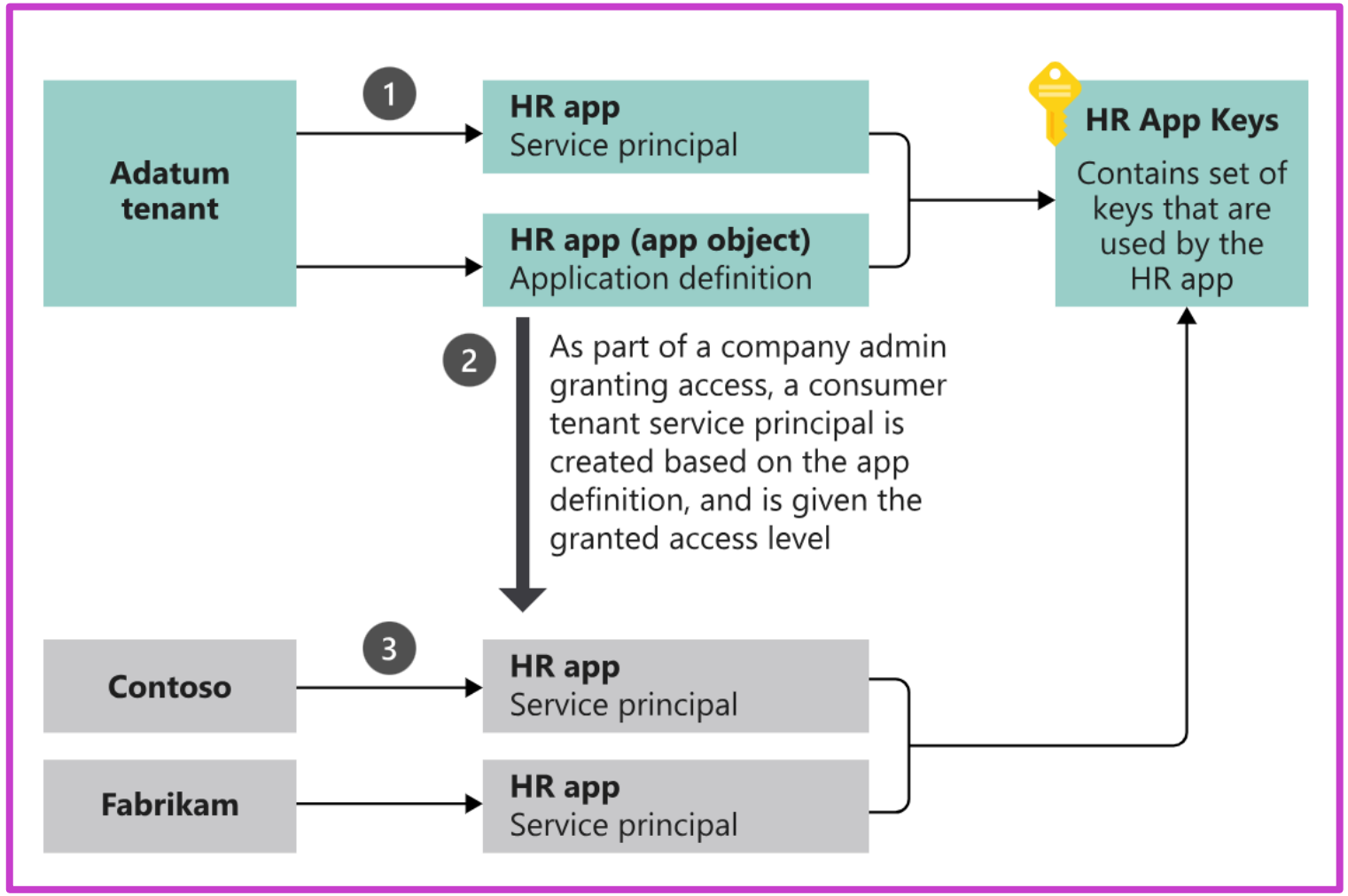
Manage and use service principals

- 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.



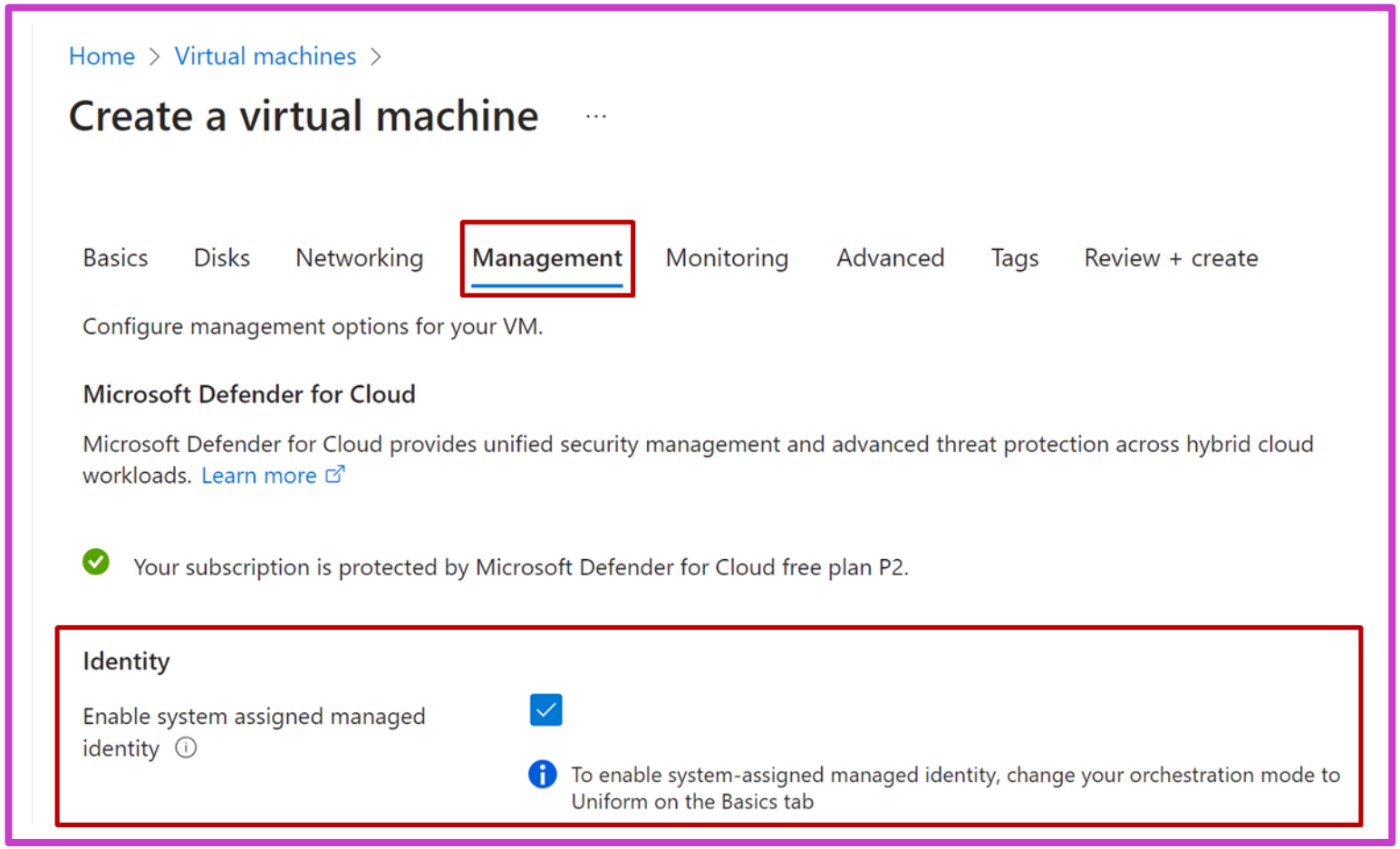
Relationship between application objects and service principals

- 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

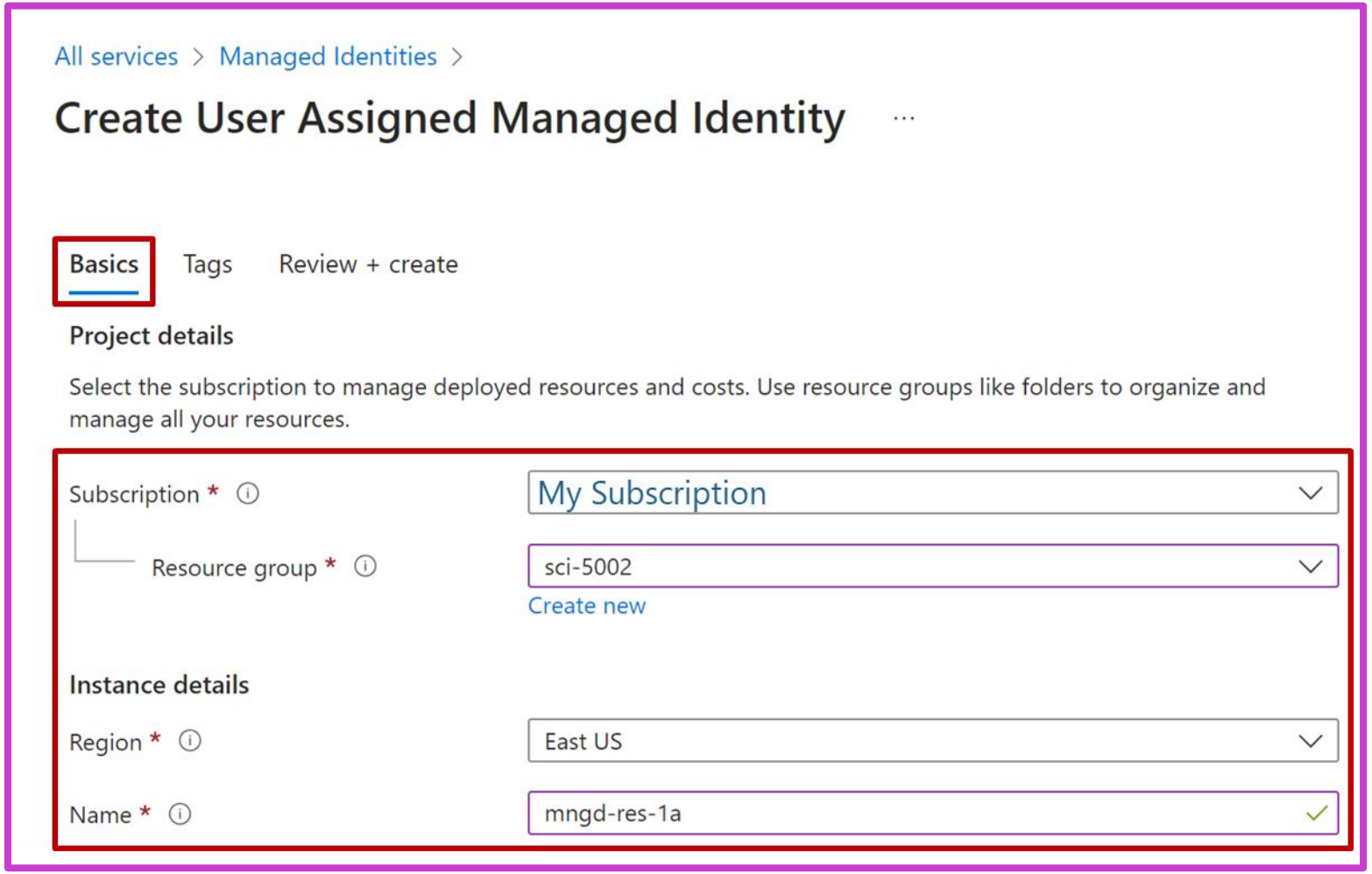
- Managed identities simplify authentication by eliminating code-based credentials, using Microsoft Entra tokens for Azure resource access.
- Azure automatically manages these identities, freeing users from manual identity management tasks.
- Two variants are available: **system-assigned identities**,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

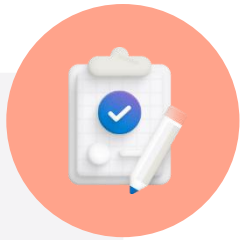
Once a user has pre-authenticated, SSO is performed by the Microsoft Entra application proxy connector authenticating to the on-premises application.

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).

Additional study – Manage Microsoft Entra application access

Microsoft Learn Modules (docs.microsoft.com/Learn)



Module Review Questions

- Manage Access to Enterprise Applications: Control access to enterprise apps in Microsoft Entra ID, including OAuth permission grants.
- Manage App Registrations:
  Register applications and configure authentication settings in Microsoft Entra.
- Configure Permission Scopes:
  Define and manage app registration permission scopes for secure access.
- Manage App Permission Consent:
  Control user and admin consent for app permissions.
- Manage Service Principals and Managed Identities:
  Securely authenticate apps using service principals and managed identities.

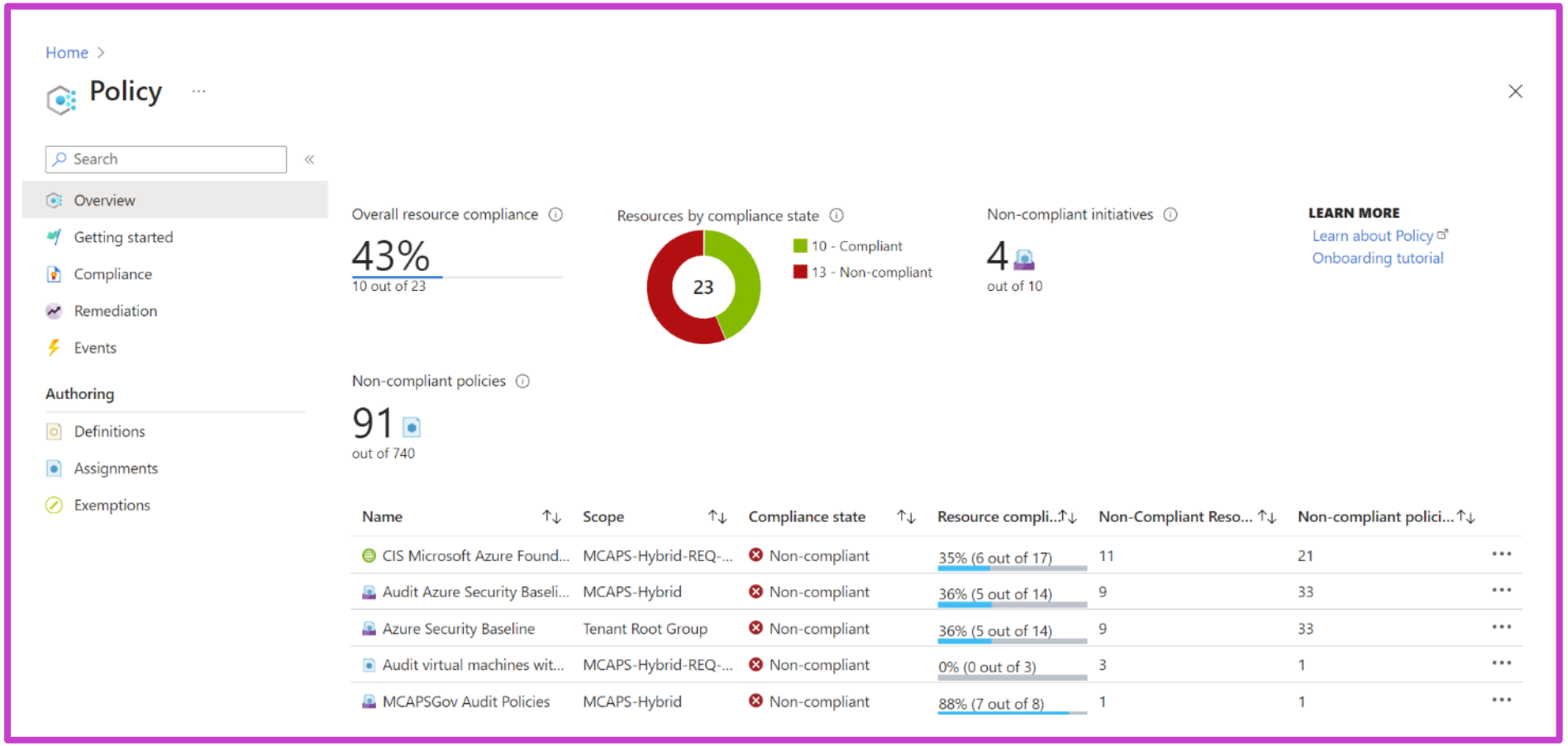
Implement and manage enforcement of cloud governance policies

MCSB Security Controls: Access, Data, Identity, Network, Endpoint, Governance, Recovery, Incident, and Vulnerability Management

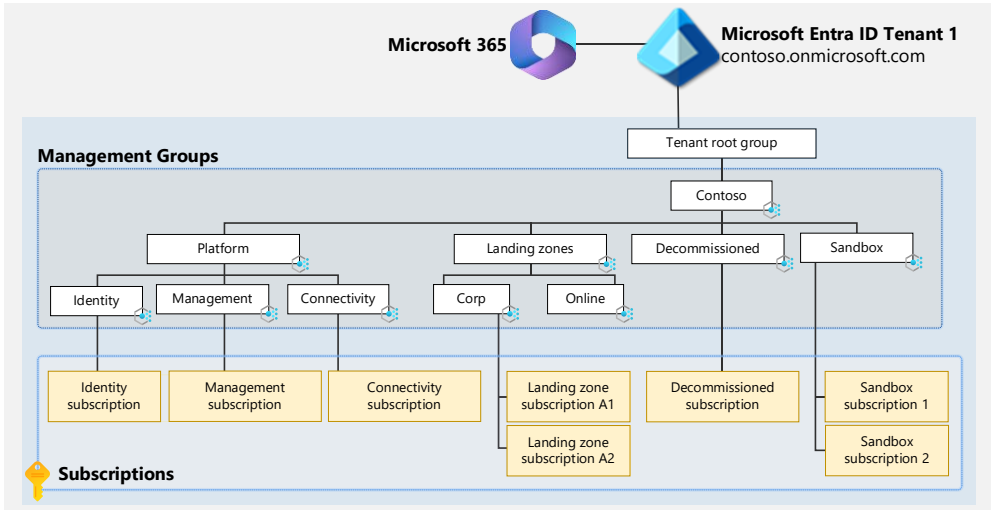
- Asset and Data Security: Track assets, enforce approved services, protect backups, and monitor sensitive data threats.
- Encryption and Key Management: Secure data in transit, manage keys/certificates, and protect storage repositories.
- Endpoint and Incident Response: Use EDR, anti-malware, automate incident handling, and enforce secure compute configurations.
- Logging and Strategy: Centralize logging, enable threat detection, and implement security posture and multi-cloud strategies.

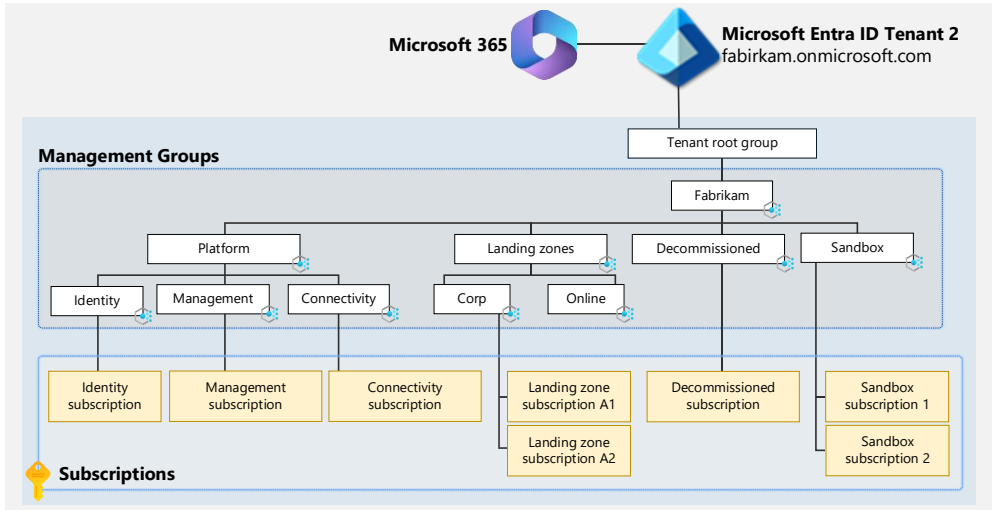
Create, assign, and interpret security policies and initiatives in Azure Policy

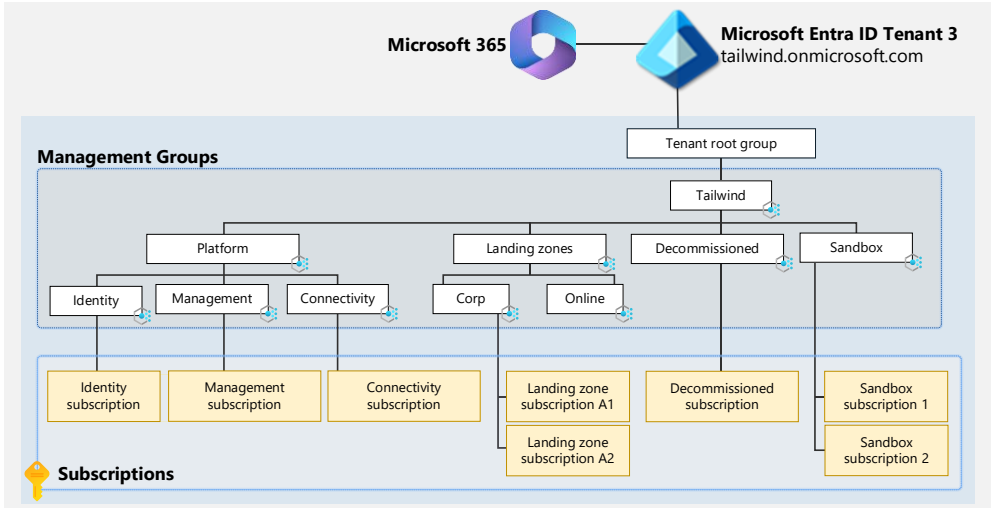
- Use Azure Policy for compliance with standards and SLAs.
- Assign policies and initiatives for future resources and compliance tracking.
- Resolve non-compliance and implement new policies organization-wide.

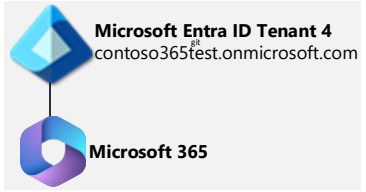


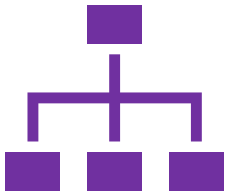
Deploy secure infrastructures by using a landing zone







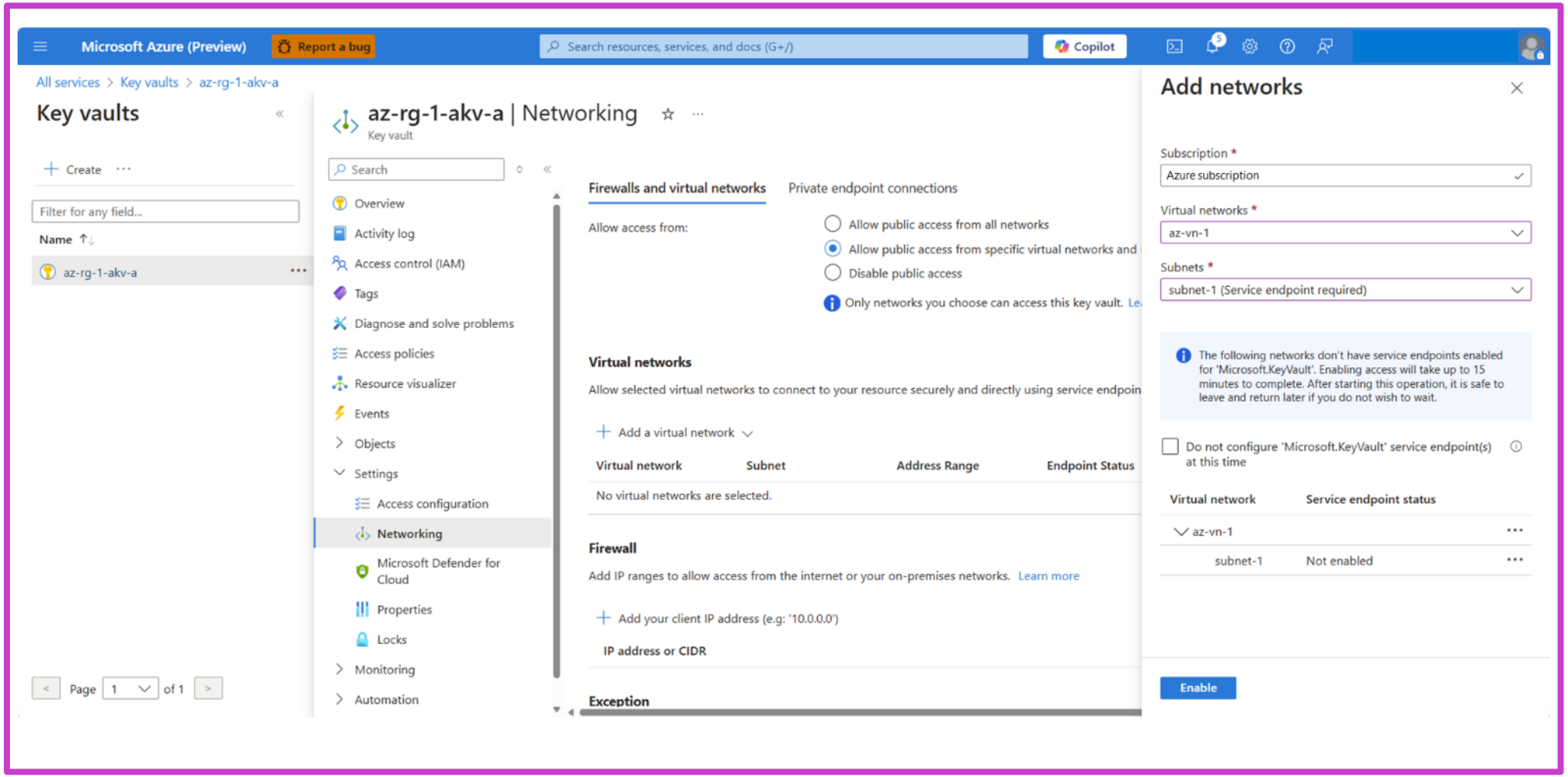




Contoso Corporation's Microsoft Entra ID Tenants

Configure Azure Key Vault networking settings

1. **Set Access:** Enable Selected networks under Firewalls and virtual networks.
2. **Add Rules:** Configure VNets, subnets, service endpoints, and IP ranges.
3. **Save Settings:** Allow Trusted Services and save the configuration changes.



Recommend when to use a Dedicated HSM

Use Azure Dedicated HSM when you need:

- Federal Information Processing Standard (FIPS) 140-2 Level-3 compliance
- Single tenancy of the cryptographic storage device
- Full administrative control and sole access to the device for administrative purposes
- High application performance
- Unique cloud-based offerings

Best fit for "**lift-and-shift**" scenarios that require direct and sole access to HSM devices.

Unfit for scenarios such as: Microsoft cloud services that support encryption with customer-managed keys that are not integrated with Azure Dedicated HSM.

Configure access to Key Vault including vault access policies and Azure Role Based Access Control

Configure vault access policies

You can use these options:

- Azure Portal: Under the **Principal** selection pane, configure the options.
- Azure CLI: Assign the access policy using the `az keyvault set-policy` command
- Azure PowerShell: Assign the access policy using the `Set-AzKeyVaultAccessPolicy` cmdlet

Configure Azure RBAC

With Azure RBAC, you can have

- One place to manage all permissions across all key vaults
- The ability to set permissions on different scope levels: management group, subscription, resource group, or individual resources
- Separate permissions on individual keys, secrets, and certificates with Azure RBAC for key vault

Manage certificates, secrets, and keys

Manage certificates

- Azure Key Vault assists in handling X.509 certificates.
- Ensures secure storage, management, and policy formulation.
- Users can input contact details for alerts.

Manage secrets

- Granularly isolate secrets for enhanced application security.
- Store credentials in secret values; rotate bi-monthly.
- Oversee access using Key Vault logging.

Manage keys

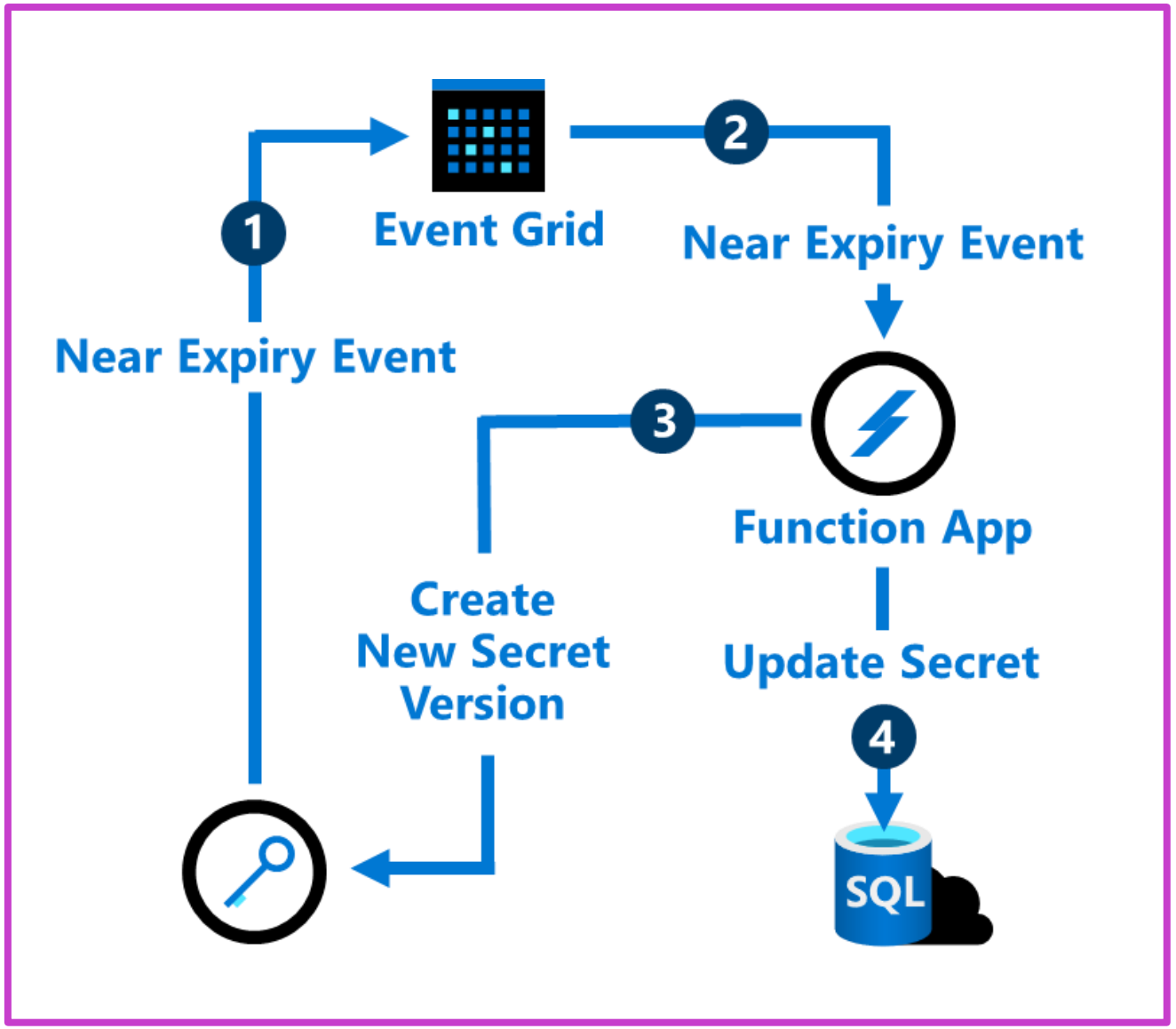
- Encryption keys: platform-managed or customer-managed.
- Storage options include Azure Key Vault and Dedicated HSM.
- Options vary by FIPS compliance, management overhead, and application suitability.

Configure key rotation

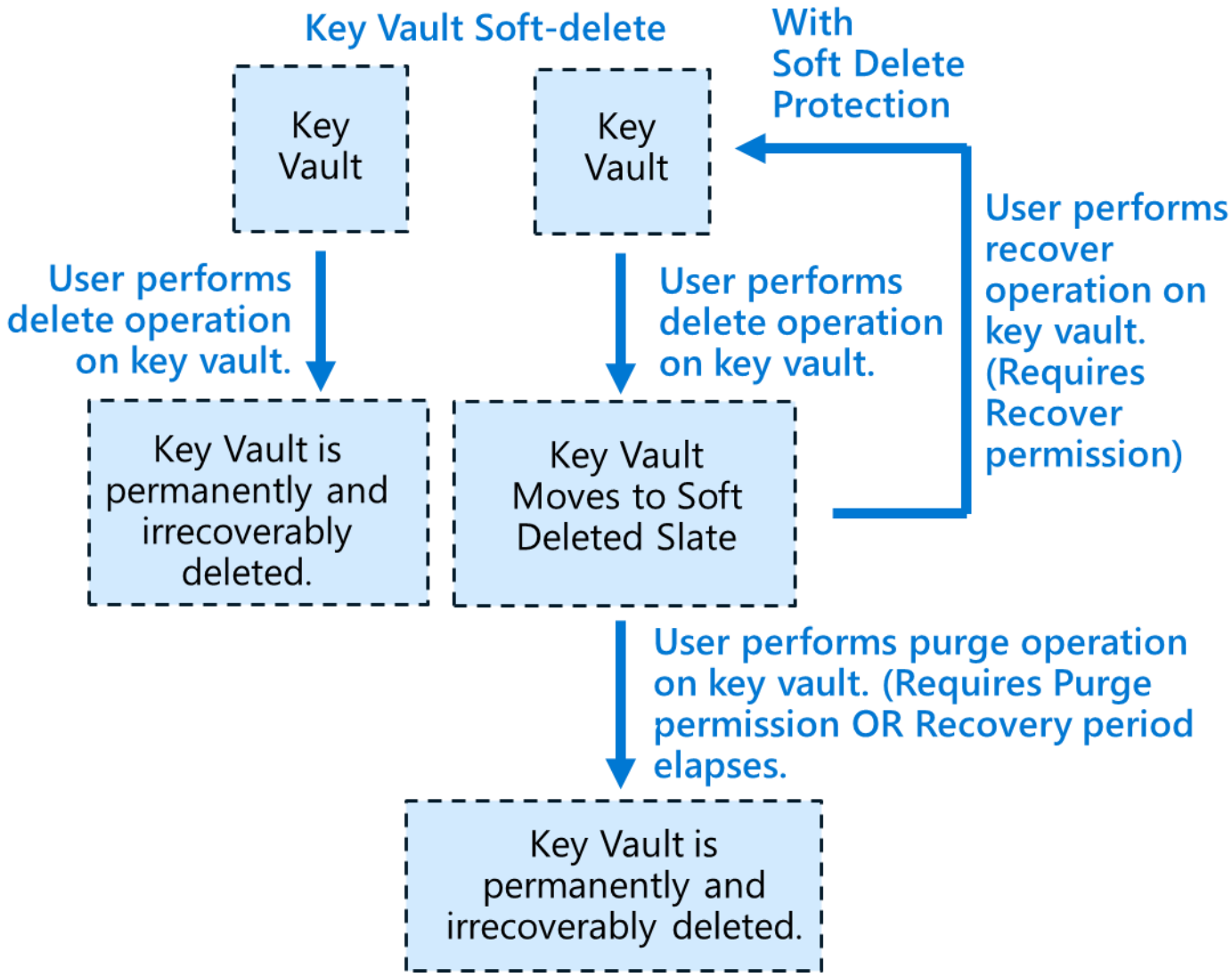
Update keys and secrets without affecting your application

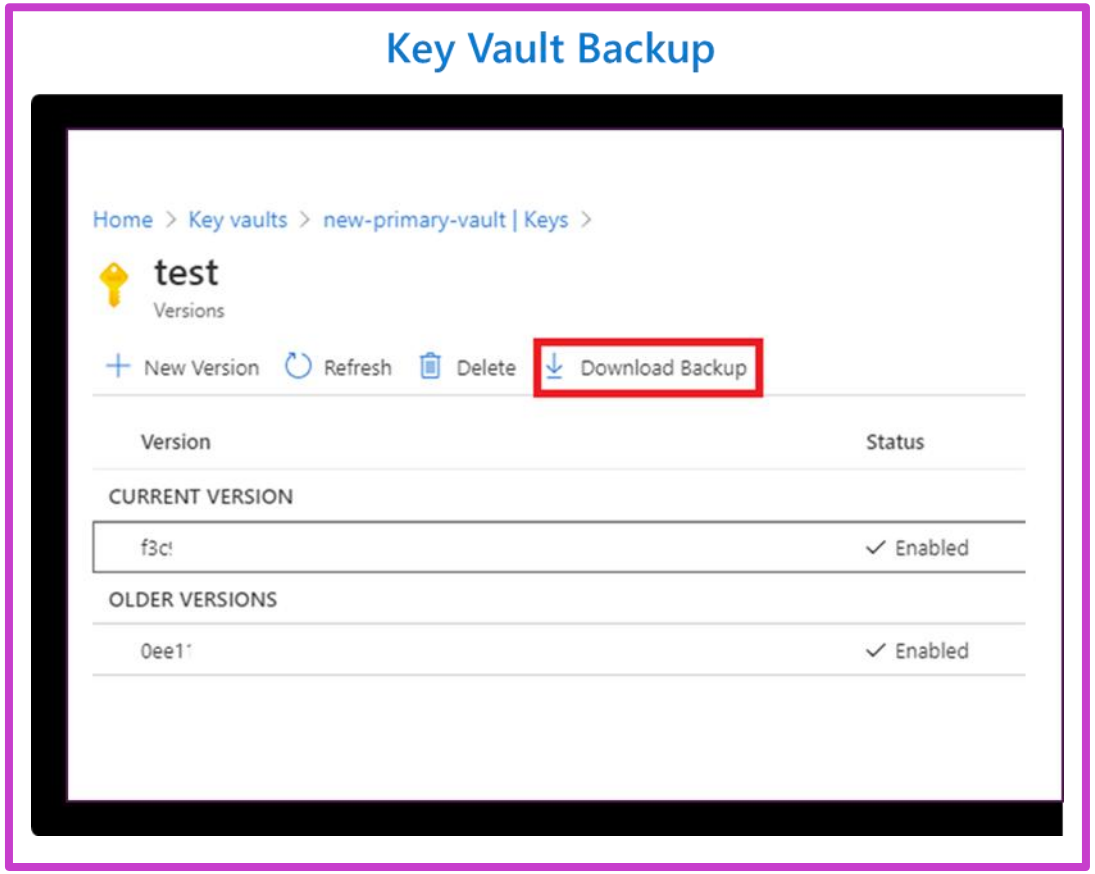
Rotate keys and secrets in several ways:

- As part of a manual process
- Programmatically with the REST API
- With an Azure Automation script



Perform backup and recovery of secrets, certificates, and keys





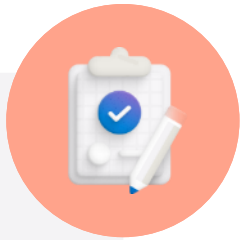
Implement security controls to protect backups

- Comprehensive Data Protection: Azure Backup secures data with encryption, isolation, soft delete, and immutable vaults.
- Advanced Access Management: Implements role-based access control (RBAC) and multi-user authorization for secure operations.
- Robust Monitoring and Compliance: Offers monitoring, alerts, and compliance with security standards for reliable data protection.

Implement security controls for asset management

- Asset Visibility and Governance: Track inventory, manage risks, and enforce approved services and applications.
- Lifecycle and Access Security: Secure asset lifecycle, restrict management access, and prevent unauthorized changes.
- Application Control: Enforce allow lists and block unauthorized software for compliance and integrity.

Additional Study – Implement and manage enforcement of cloud governance policies



Microsoft Learn Modules (docs.microsoft.com/Learn)

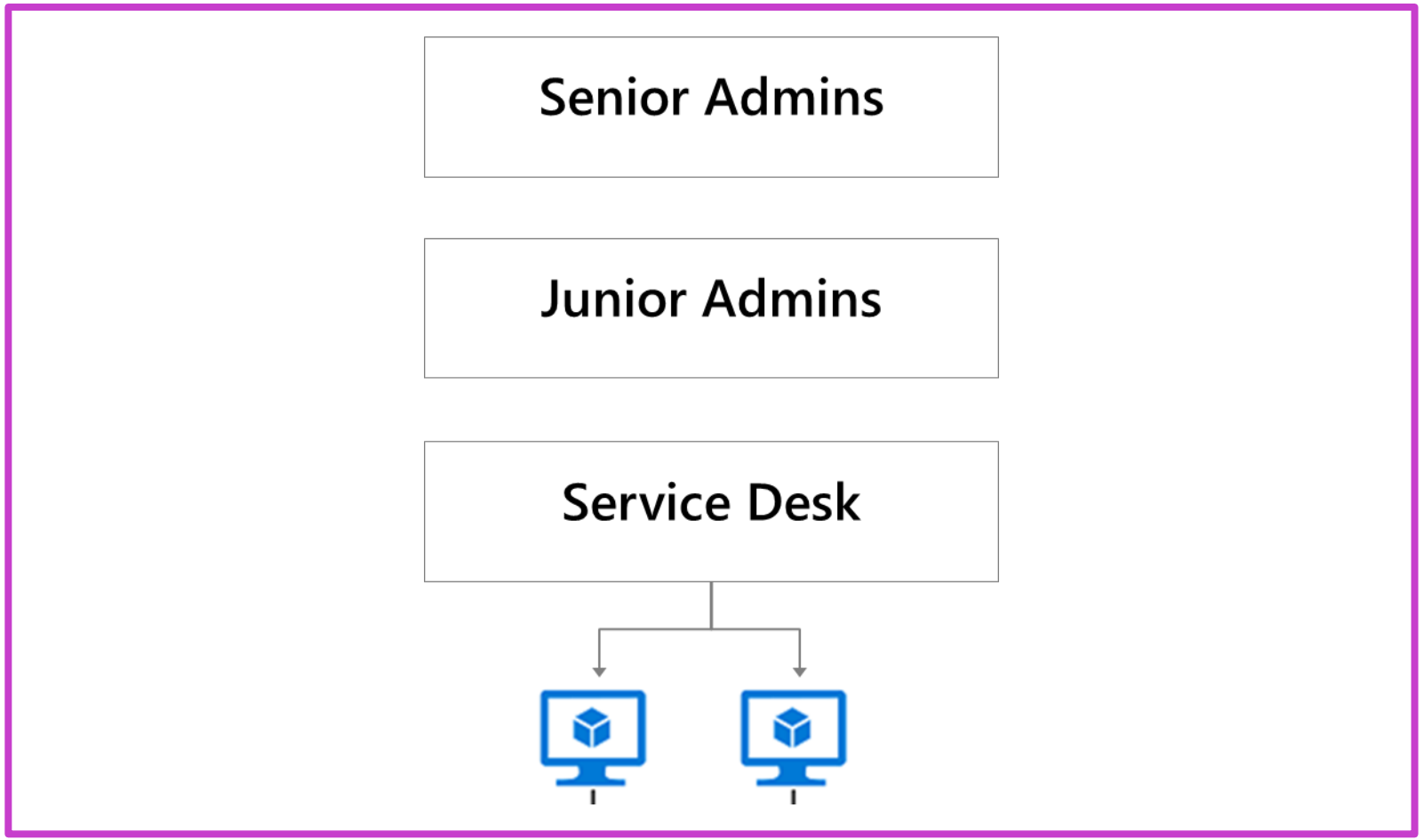
Module Review Questions

- Create and Assign Azure Policies: Define, assign, and interpret policies and initiatives in Azure Policy to enforce governance standards.
- Secure Azure Key Vault: Configure network settings and access policies, including Azure Role-Based Access Control (RBAC), for Key Vault.
- Manage Certificates, Secrets, and Keys:
  Store, manage, and control access to certificates, secrets, and encryption keys.
- Configure Key Rotation and Backup:
  Automate key rotation and implement secure backup and recovery practices for certificates, secrets, and keys.
- Implement Security for Backups and Assets:
  Apply security controls to protect backups and manage assets securely within Azure environments.

Module Lab

Lab 01 – Role-based Access Control

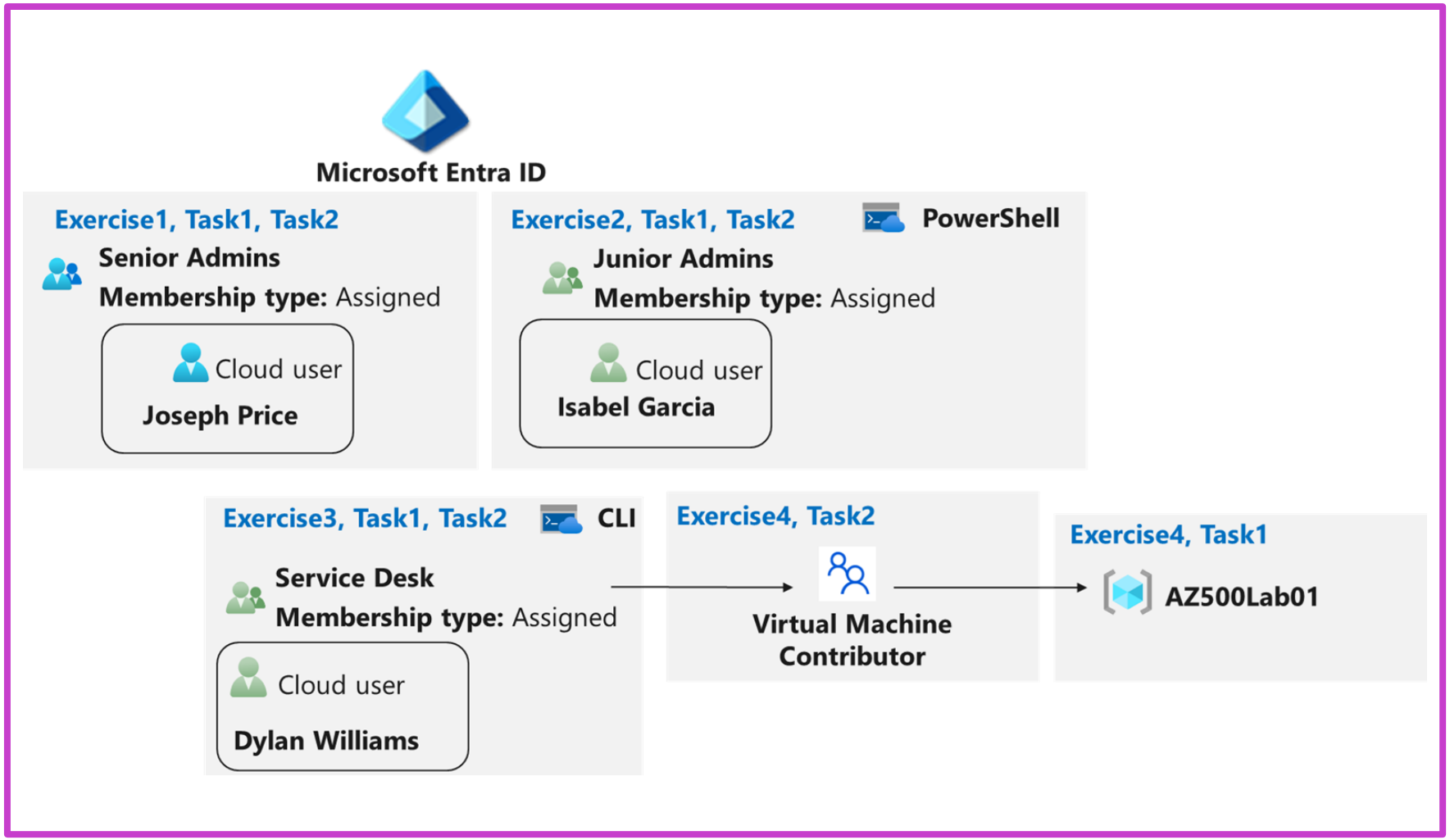
- Use the Portal to create a Senior Admins group with member Joseph Price.
- Use PowerShell to create a Junior Admins group with member Isabel Garcia.
- Use the CLI to create a Service Desk group with member Dylan Williams.
- Assign the Service Desk group Virtual Machine Contributor permissions.



Lab 01 - Role-Based Access Control

This exercise teaches students how Azure users and groups are created and how role-based access control is used to assign roles to groups.

[Launch this Exercise in GitHub]



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