



SC-500 Domain 1: Entra Access, PIM and App Identities

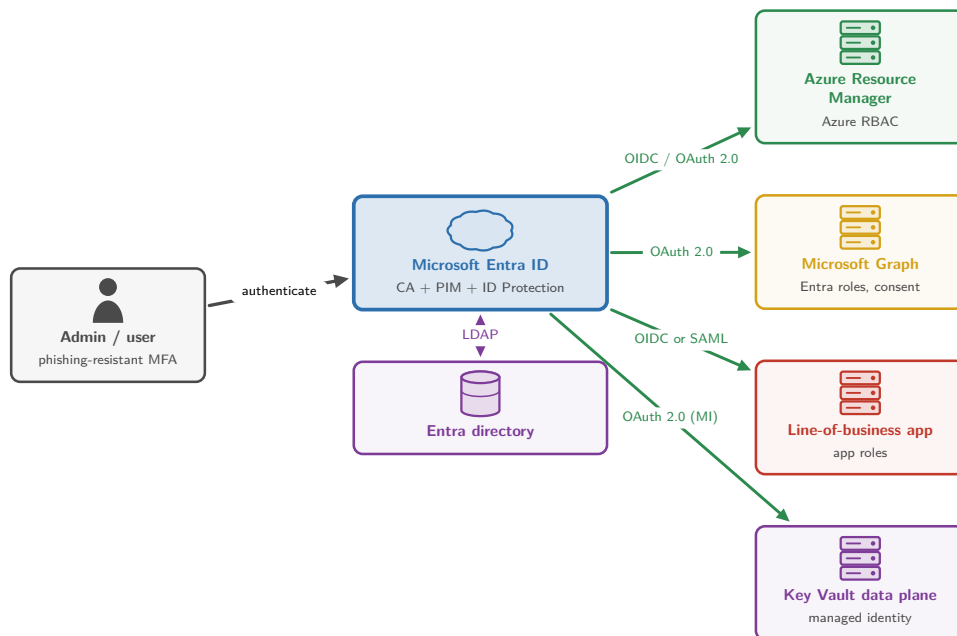
SC-500 skills measured: Secure access to resources by using Microsoft Entra ID | PIM, Conditional Access, MFA and passwordless, app registrations, OAuth consent, managed identities

SC-500 Domain 1 Entra ID PIM Conditional Access

Recall and scope

Recall (AZ-500 sheet 01, SC-300 for depth): **Entra roles** manage the directory and Microsoft 365, **Azure roles** manage Azure resources at a scope; both follow **least privilege at the smallest scope for the shortest time**. SC-500 tests six identity skills: **PIM, Conditional Access, authentication methods (MFA, passwordless), identity for applications, OAuth consent and managed identities**. Licence reminder: Conditional Access needs **Entra ID P1**, PIM and risk-based policies need **Entra ID P2** (or Entra ID Governance / Entra Suite).

Who issues tokens to whom



Privileged Identity Management (PIM)

PIM setting (role settings)	What it does	Exam-safe value
Activation maximum duration	how long an activation lasts (1-24 h)	short: 1-4 h for Global Admin, 8 h default
On activation, require	MFA or a Conditional Access authentication context	auth context → phishing-resistant strength
Require justification / ticket	free text and ticket number logged	on for every privileged role
Require approval to activate	named approvers approve or deny	on for Global Admin, Owner, User Access Admin
Allow permanent eligible / active	assignment expiry	eligible time-bound; never permanent active
Notifications	email on assignment and activation	send to SOC mailbox

- **Three scopes** Microsoft Entra roles, Azure resource roles (management group, subscription, RG, resource) and **PIM for Groups** (eligible membership or ownership of a security group, including role-assignable groups)
- **Access reviews** recurring reviews of eligible and active assignments; auto-apply 'remove access' when reviewers do not respond
- **Alerts** 'roles assigned outside PIM', 'too many Global Administrators' (more than 5 by default), 'roles do not require MFA for activation'
- **Break-glass** two cloud-only Global Admins, permanent active, FIDO2, excluded from CA, alert on every sign-in

How much standing privilege does PIM remove?

PROBLEM

Six engineers hold Global Administrator permanently. You move them to eligible with 4-hour activations; each activates twice a week. What is the monthly exposure before and after, and the reduction?

1. Before: $E0 = n \times T$

$$\Rightarrow 6 \times 720 = 4\,320 \text{ privileged hours}$$

why: standing access is exposed every hour of the month

2. After: $E1 = n \times a \times d$

$$\Rightarrow 6 \times 8.66 \times 4 = 207.8 \text{ privileged hours}$$

why: rights exist only while activated

3. Reduction $R = 1 - E1 / E0$

$$\Rightarrow 1 - 207.8 / 4\,320 = 1 - 0.048 = 0.952$$

why: share of the exposure removed

GIVEN

- $n = 6$ privileged users
- $T = 720$ h in a 30-day month (24×30)
- $a =$ activations per user per month = 2 per week $\times$ 4.33 weeks = 8.66
- $d =$ activation duration = 4 h
- $E =$ exposure in privileged hours per month

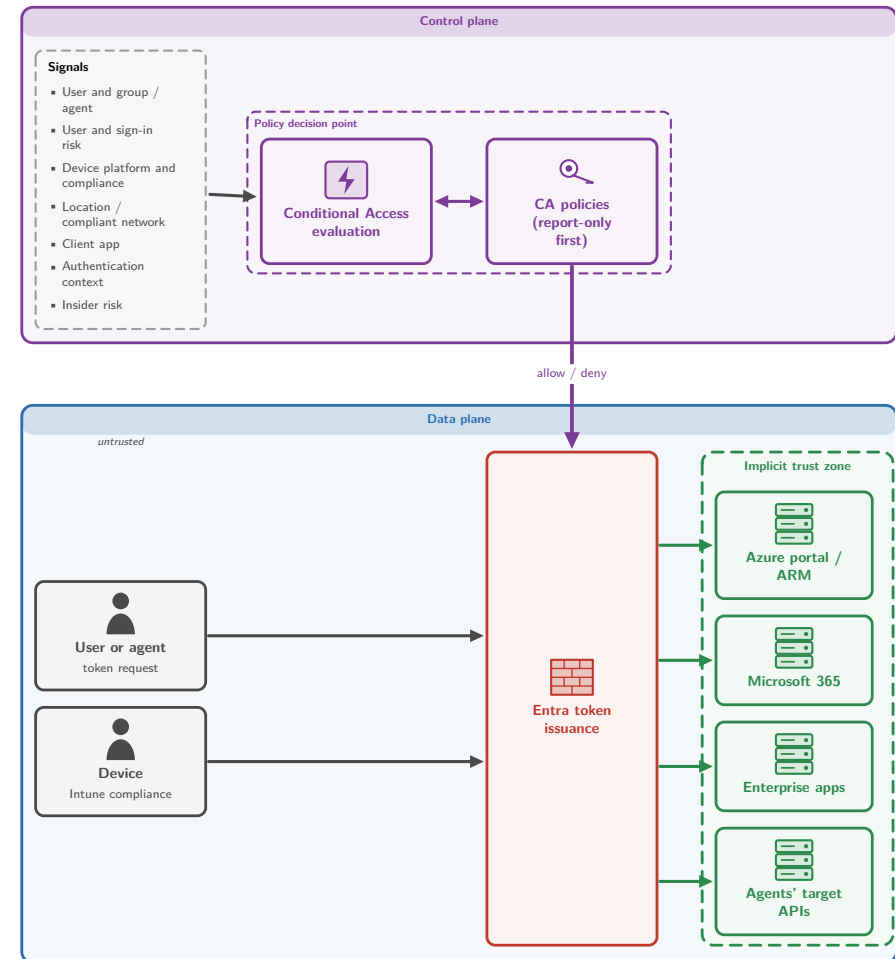
ANSWER

About 4 320 $\rightarrow$ 208 privileged hours per month: a 95 % reduction, plus an approval and MFA gate at each activation

Check: $208 \text{ h} \div 6 \text{ users} \approx 35 \text{ h each} \approx 8.66 \times 4 \text{ h} \checkmark$

Conditional Access and authentication methods

Conditional Access is the policy engine of Entra



Which grant or session control?

Conditions	R1	R2	R3	R4	R5
Admin roles or Azure management	Y	--	--	--	--
Sign-in risk medium or high	--	Y	--	--	--
Unmanaged device, browser	--	--	Y	--	--
Legacy authentication client	--	--	--	Y	--
Sensitive app action (auth context)	--	--	--	--	Y
Actions					
Require phishing-resistant MFA strength	X				X
Require MFA + risk remediation		X			
App-enforced restrictions / Defender for Cloud Apps session			X		
Block access				X	
Notes	Global Admin, Owner	ID Protection (P2)	SharePoint limited access	no MFA possible	step-up inside the app

Method	Phishing-resistant?	Use
FIDO2 security key / passkey (device-bound, incl. in Authenticator)	yes	admins, break-glass, shared workstations
Windows Hello for Business	yes	managed Windows devices
Certificate-based authentication (CBA)	yes	smart-card / PIV estates, no AD FS needed
Authenticator push with number matching	no	default MFA for users; number matching blocks fatigue attacks
Temporary Access Pass	n/a (bootstrap)	onboarding and recovery to register passwordless
SMS / voice / email OTP	no	last resort; SMS can be SIM-swapped

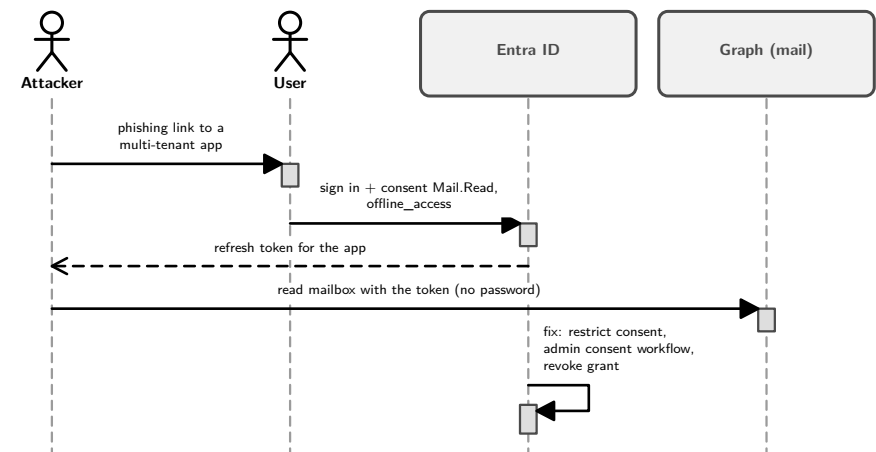
- **Authentication methods policy** the single place to enable methods per group (legacy per-user MFA and SSPR method settings were migrated here); enable **system-preferred MFA** so the strongest registered method is prompted
- **Roll out safely** report-only → review sign-in logs and the **What If** tool → On; exclude break-glass; never block all users from all apps without testing
- **Security defaults vs CA** mutually exclusive: turn security defaults off before creating CA policies
- **Agents CA** also targets agent identities and agent identity blueprints (sheet 06)

☀ Application identities, consent and managed identities

	App registration	Enterprise application	Managed identity Recommended
Object	application object	service principal	service principal (no app object you manage)
Where it lives	home tenant only	every tenant using the app	your tenant
Holds	credentials, redirect URLs, requested permissions, app roles	granted consent, assignments	nothing you can read
You configure here	secrets/certs/FIC, token config, expose an API	assignment required, SSO, CA target, owners, sign-in logs	role assignments only

User consent setting	Effect	When
Do not allow user consent	every app needs an admin; pair with the admin consent workflow	regulated tenants
Allow consent for apps from verified publishers, for low-impact permissions you classify	users can consent to e.g. User.Read, openid, profile	Microsoft-recommended balance
Allow user consent for all apps	any app, any delegated permission users hold	never: illicit consent risk

Illicit consent grant and its fixes



<code>az identity create -g rg-app -n uami-web</code>	user-assigned managed identity (lives on its own, shareable, pre-authorisable)
<code>az vm identity assign -g rg-app -n vm1 --identities uami-web</code>	attach it; <code>az vm identity assign</code> without <code>--identities</code> adds a system-assigned one
<code>az role assignment create --assignee <principalId> --role "Key Vault Secrets User" --scope <vaultId></code>	data-plane role at the narrowest scope
<code>Get-MgOauth2PermissionGrant -Filter "clientId eq '<spId>'"</code>	list delegated grants of an app; remove with <code>Remove-MgOauth2PermissionGrant</code>
<code>curl -H Metadata:true 'http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01&resource=https://vault.azure.net'</code>	token from IMDS inside the VM; no secret on disk

 **EXAM TIP**

'No secrets stored' + Azure resource → **managed identity**. 'Created before the resource / shared by many VMs / survives redeloys' → **user-assigned**. 'GitHub Actions without a secret' → **federated identity credential** (workload identity federation). 'Users keep granting mail access to unknown apps' → restrict **user consent** + **admin consent workflow**, then review and revoke grants.

🚩 **Myths, recap and self-test**

MYTH		FACT
❌ PIM removes the need for Conditional Access on admins	→	✅ PIM controls when a role is held; CA controls how the sign-in happens Combine them: require an authentication context with phishing-resistant strength on activation.
❌ Deleting the app registration removes access in every tenant	→	✅ Other tenants keep their service principal Disable or delete the enterprise app (service principal) in each tenant, and revoke its grants.
❌ A system-assigned identity can be reused by a second VM	→	✅ It is tied to one resource and deleted with it Use a user-assigned identity to share.
❌ Number matching makes push MFA phishing-resistant	→	✅ It stops MFA fatigue, not adversary-in-the-middle phishing Only FIDO2/passkeys, WHfB and CBA meet the phishing-resistant strength.

TOPIC

Entra access in one line each

HEADLINE 1

Standing admins become eligible ones

--- PIM

Why: time-bound, approved, MFA on activation

HEADLINE 2

Report-only before On

--- Conditional Access

Why: What If + sign-in logs, break-glass excluded

HEADLINE 3

Phishing-resistant for privileged access

--- Authentication strengths

Why: FIDO2, WHfB, CBA

HEADLINE 4

Users stop granting mail to strangers

--- Consent settings

Why: verified publishers + low impact + admin workflow

HEADLINE 5

No secret survives in code

--- Managed identities

Why: and federated credentials outside Azure

- Q1

Eligible vs active PIM assignment?

A

Eligible grants nothing until activated (MFA, justification, approval, limited hours); active grants the role immediately.
- Q2

Which licence do PIM and risk-based Conditional Access need?

A

Microsoft Entra ID P2 (or Entra ID Governance / Entra Suite); CA alone needs P1.
- Q3

Which methods satisfy the phishing-resistant authentication strength?

A

FIDO2 security keys and passkeys, Windows Hello for Business, certificate-based authentication.
- Q4

What should you do before turning a new CA policy On?

A

Run it in report-only mode, check the sign-in logs and What If, and exclude break-glass accounts.
- Q5

Where do you set 'assignment required' and see sign-ins for an app?

A

On the enterprise application (service principal), not the app registration.
- Q6

Which consent setting does Microsoft recommend for most tenants?

A

User consent only for verified publishers and permissions classified low impact, with the admin consent workflow for the rest.

Q7 System-assigned vs user-assigned managed identity?

A System-assigned lives and dies with one resource; user-assigned is a standalone resource you can share and authorise in advance.

Q8 How does a CI pipeline outside Azure get Entra tokens without a secret?

A A federated identity credential on an app registration or user-assigned identity (workload identity federation).

Q9 Can you use security defaults and Conditional Access together?

A No; disable security defaults before enabling CA policies.