



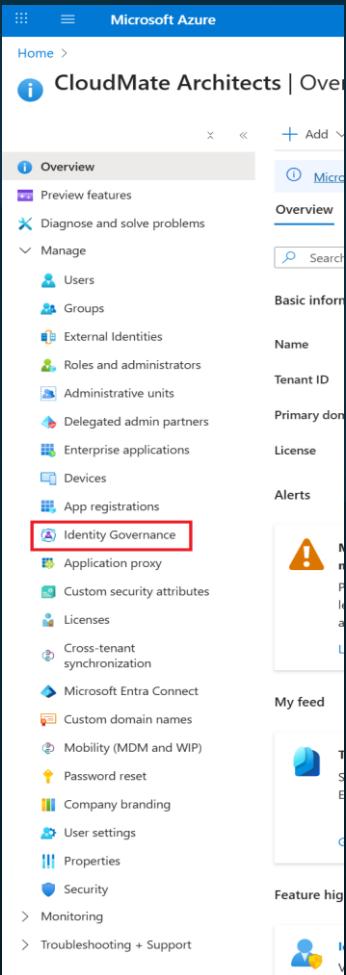
Build a Secure Access Catalog in Microsoft Entra

Implement governance foundation with Microsoft Entra Entitlement Management



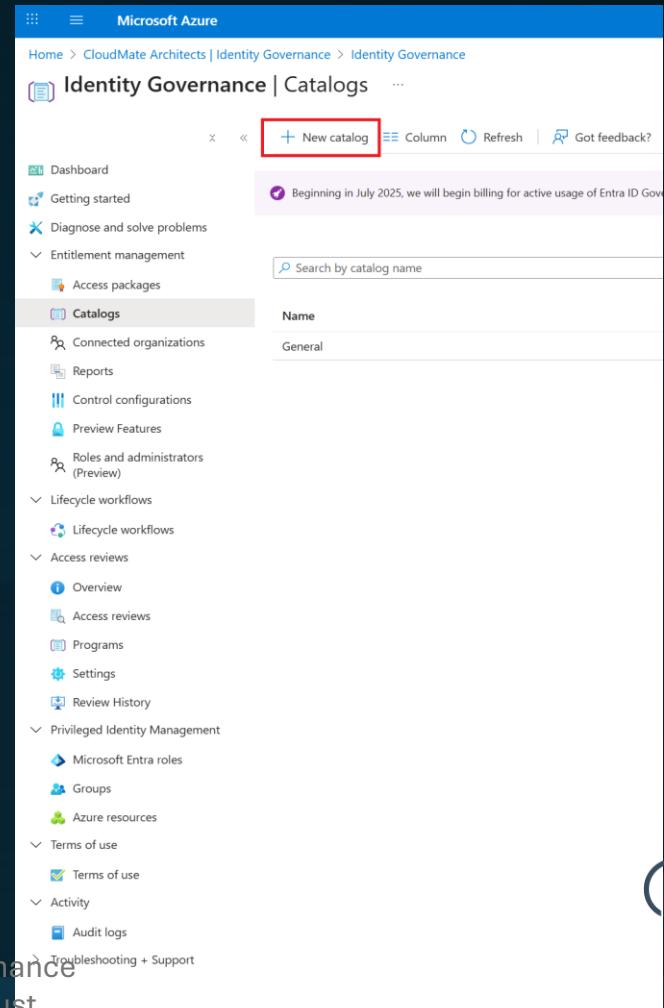
Open Microsoft Entra Admin Center

Navigate to **Identity Governance** → **Entitlement Management**



Architect Insight: Entitlement Management automates identity lifecycle governance — replacing static group membership with policy-based access that expires automatically.

Create New Catalog



Name the Catalog

Example:
Marketing Project
— describes
business scope

New catalog

Name *
Marketing

Description *
Marketing Project

Enabled
Yes No

Enabled for external users
Yes No

Why It Matters: Catalogs act as containers for resources and access packages.

They enforce governance boundaries — each catalog can have its own set of owners, policies, and connected resources.

Created the **Marketing** catalog that will host all project resources.

Microsoft Azure

Home > Identity Governance

Identity Governance | Catalogs

Dashboard Getting started Diagnose and solve problems Entitlement management Access packages Catalogs Connected organizations Reports Control configurations Preview Features Roles and administrators (Preview)

New catalog Column Refresh

Beginning in July 2025, we will begin billing for active usage of Entra ID Governance features for guest users. In July you will have the option to opt out.

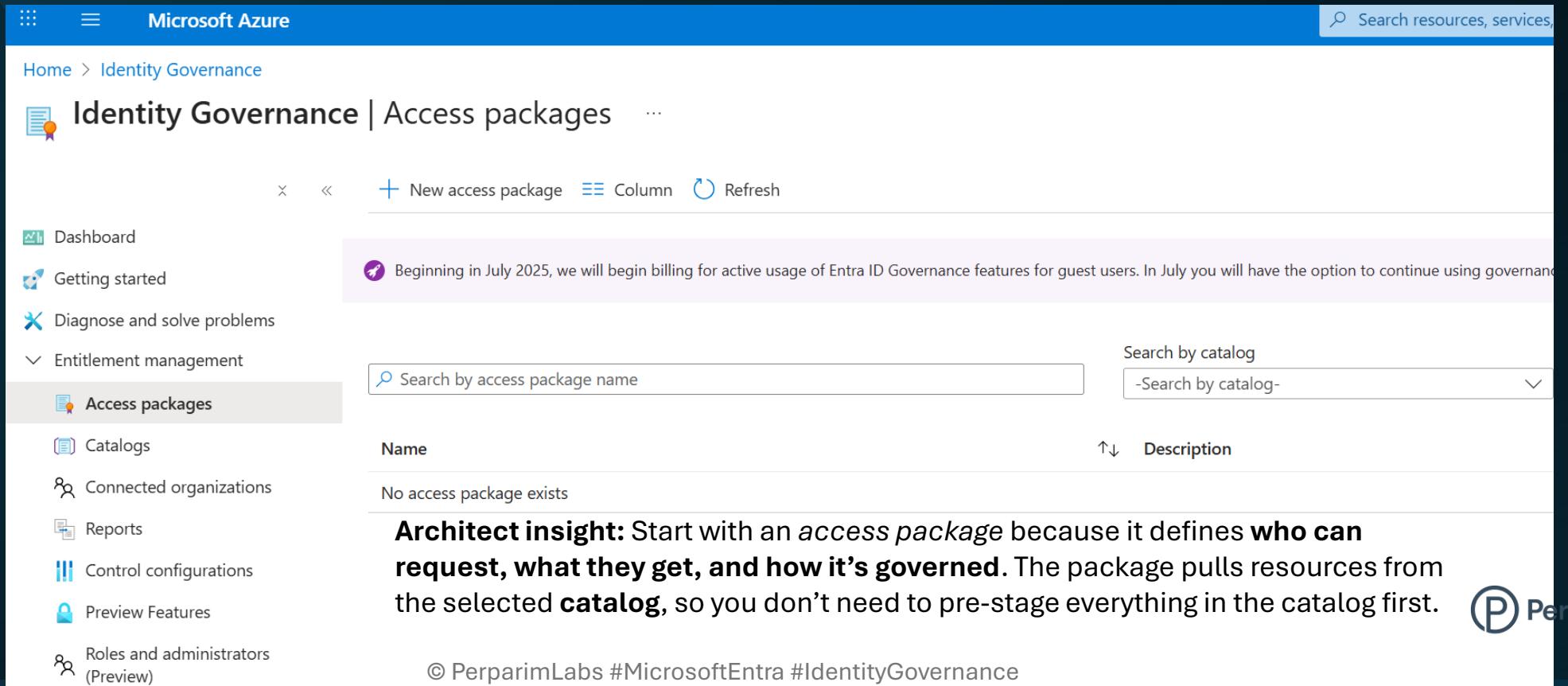
Name	Description
Marketing	Marketing Project
General	Built-in catalog.

Search by catalog name

Enabled All

Open Access packages → New access package

Start a new package that will pull resources from the **Marketing** catalog.



Microsoft Azure

Home > Identity Governance

Identity Governance | Access packages

[New access package](#) [Column](#) [Refresh](#)

Beginning in July 2025, we will begin billing for active usage of Entra ID Governance features for guest users. In July you will have the option to continue using governance features for guest users.

Name	Description
No access package exists	

Search by access package name

Search by catalog

-Search by catalog-

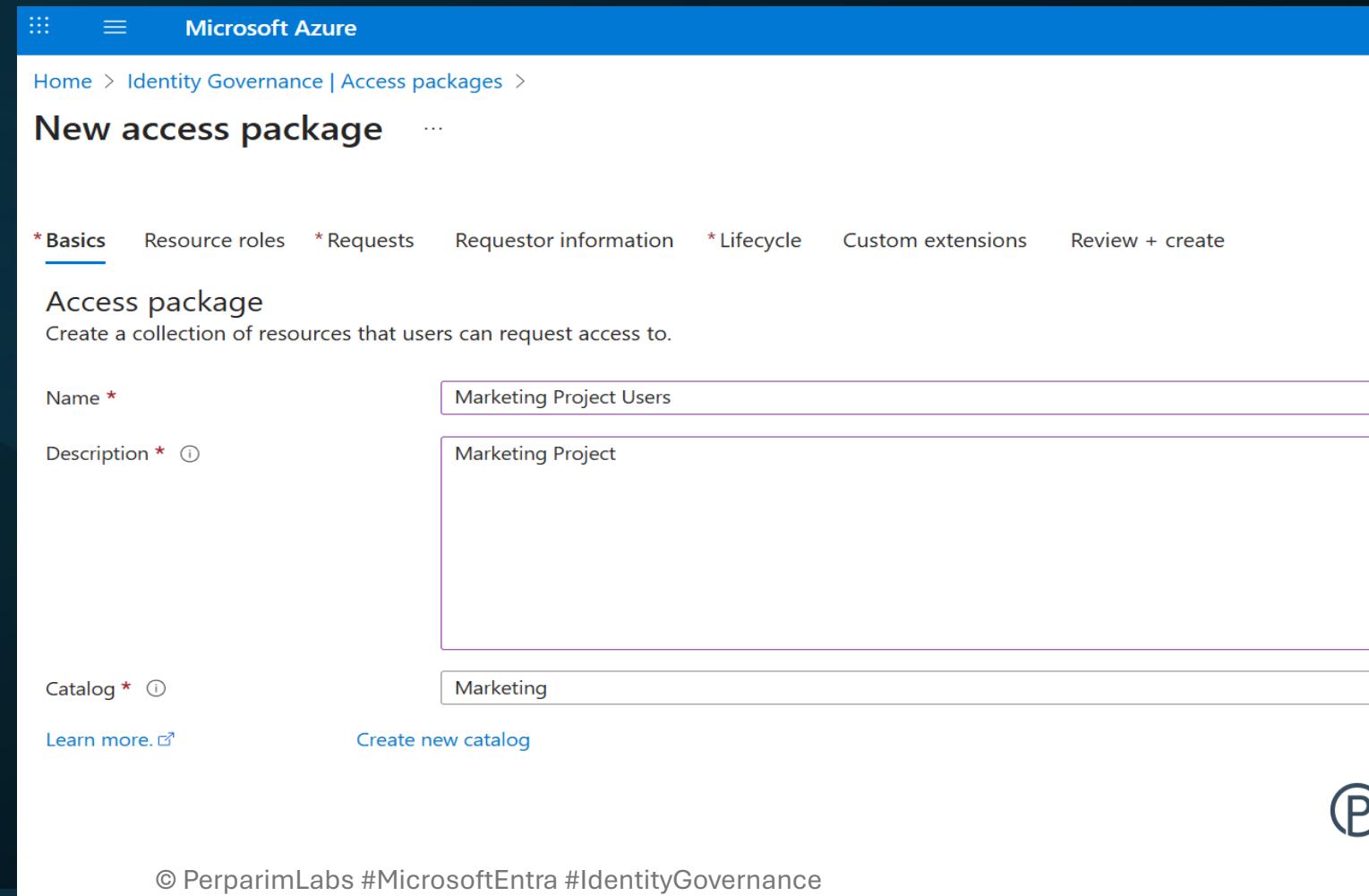
Architect insight: Start with an access package because it defines **who can request, what they get, and how it's governed**. The package pulls resources from the selected **catalog**, so you don't need to pre-stage everything in the catalog first.

© PerparimLabs #MicrosoftEntra #IdentityGovernance #AzureSecurity #AccessManagement #ZeroTrust #EntitlementManagement #CloudSecurity

PerparimLabs

Name, description, and select Marketing catalog

Package name **Marketing Project Users**; catalog **Marketing**.



Microsoft Azure

Home > Identity Governance | Access packages >

New access package

[... Review + create](#)

[* Basics](#) [Resource roles](#) [* Requests](#) [Requestor information](#) [* Lifecycle](#) [Custom extensions](#)

Access package
Create a collection of resources that users can request access to.

Name * Marketing Project Users

Description * Marketing Project

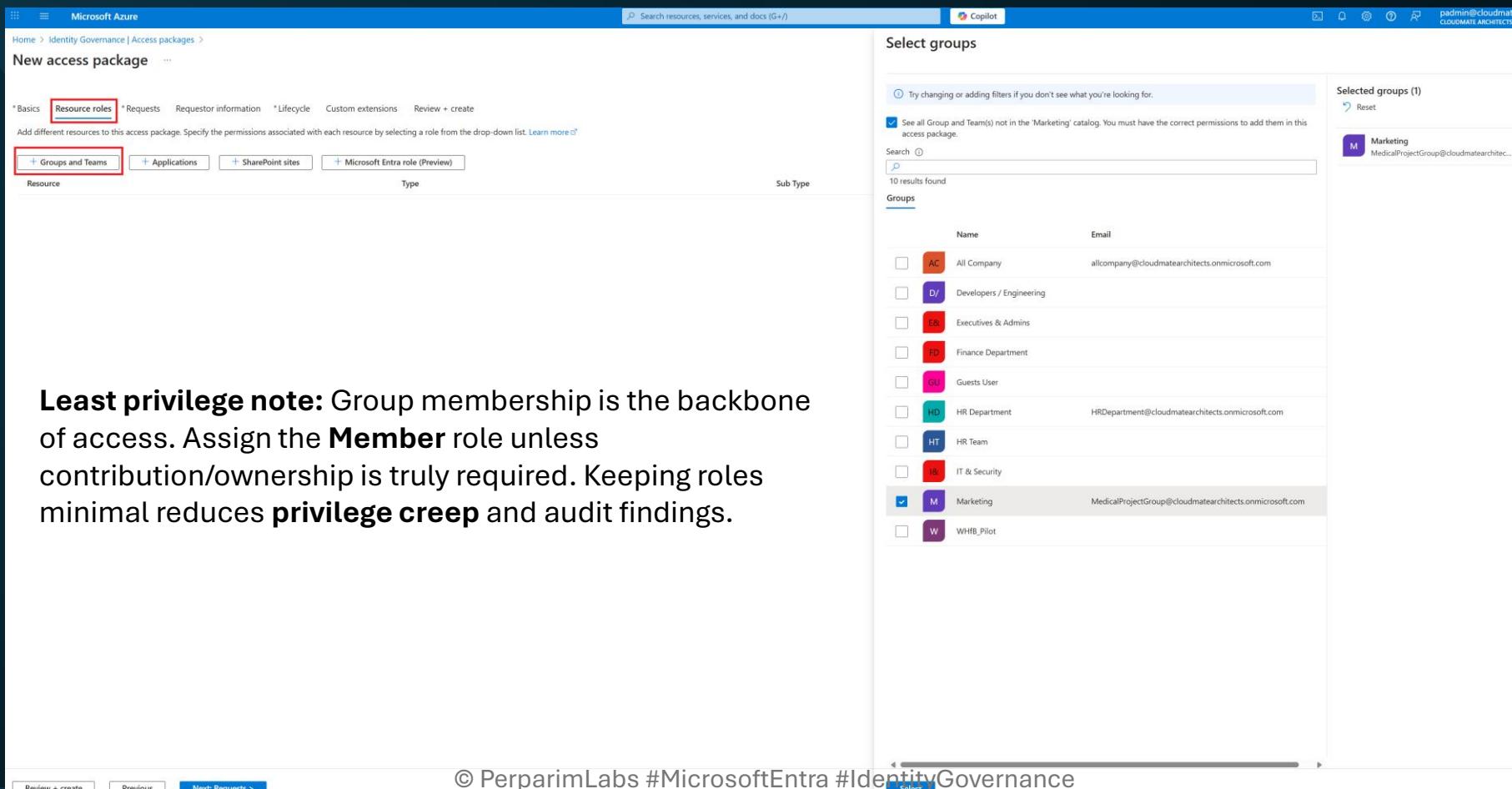
Catalog * Marketing

[Learn more.](#) [Create new catalog](#)

Why it matters: The **catalog** sets the governance boundary (owners, resources, policies). The package name/description should reflect **business purpose** so approvers/auditors instantly understand *why access exists*.

Add Group: Marketing (Member)

Added **Marketing** M365 Group, role **Member**.



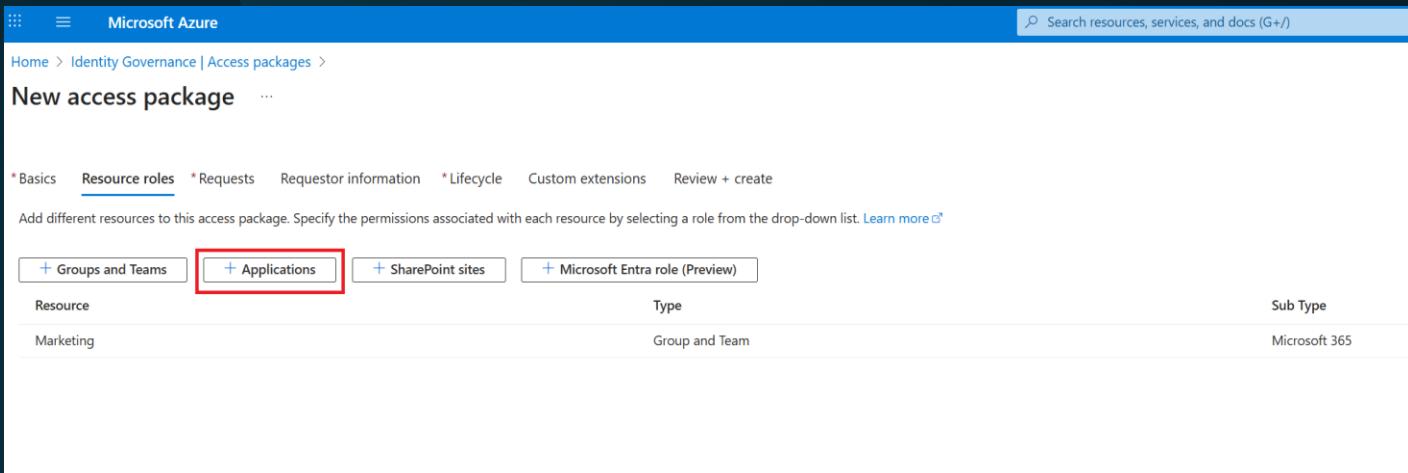
The screenshot shows the Microsoft Azure Identity Governance interface for creating a new access package. The 'Resource roles' tab is selected. A 'Groups and Teams' button is highlighted with a red box. The 'Marketing' group is selected in the 'Select groups' modal, also highlighted with a red box.

Least privilege note: Group membership is the backbone of access. Assign the **Member** role unless contribution/ownership is truly required. Keeping roles minimal reduces **privilege creep** and audit findings.

Name	Email
AC	allcompany@cloudmatearchitects.onmicrosoft.com
D/	Developers / Engineering
EA	Executives & Admins
FD	Finance Department
GU	Guests User
HD	HR Department
HT	HR Team
IS	IT & Security
M	Marketing
W	WHFB_Pilot

Add Application: Adobe Identity Management (SAML)

Added SAML app with role User.

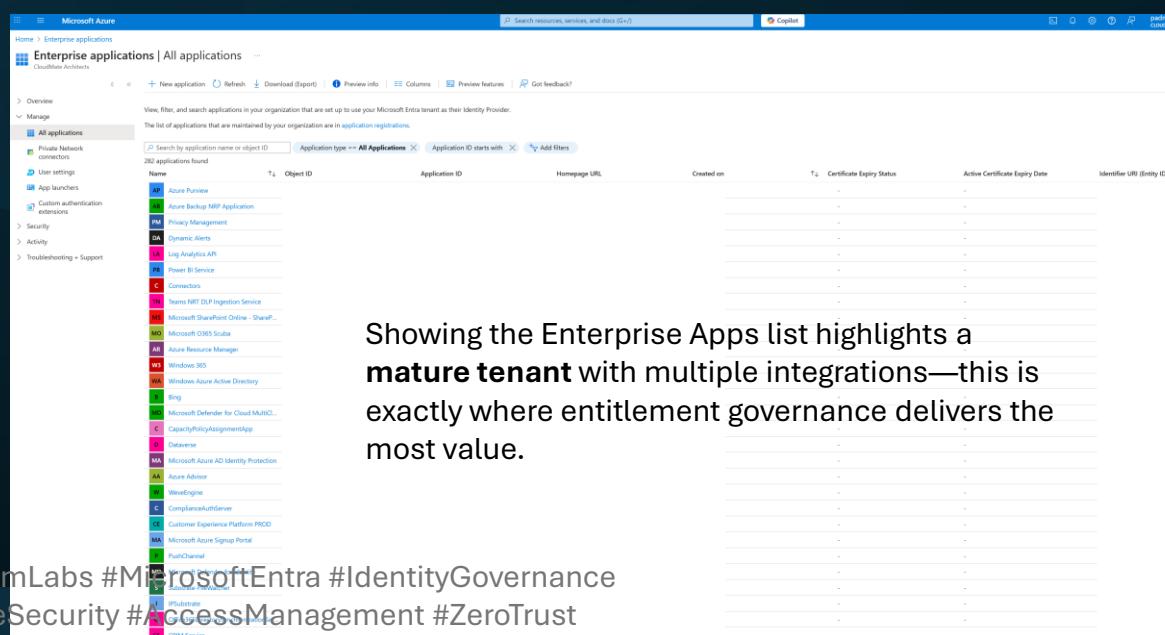


The screenshot shows the Microsoft Azure 'New access package' interface. The 'Applications' tab is highlighted with a red box. The table below shows a single entry for 'Marketing' as a 'Group and Team' type resource under 'Microsoft 365'.

Resource	Type	Sub Type
Marketing	Group and Team	Microsoft 365

On the right, a 'Select applications' sidebar shows the 'Enterprise applications' section with a single result: 'Adobe Identity Management (SAML)'.

Governance tip: Adding **enterprise apps** to the package brings **SSO + app roles** under the same lifecycle controls (expiration, reviews). If the app supports **SCIM**, user provisioning/de-provisioning can be fully automated.

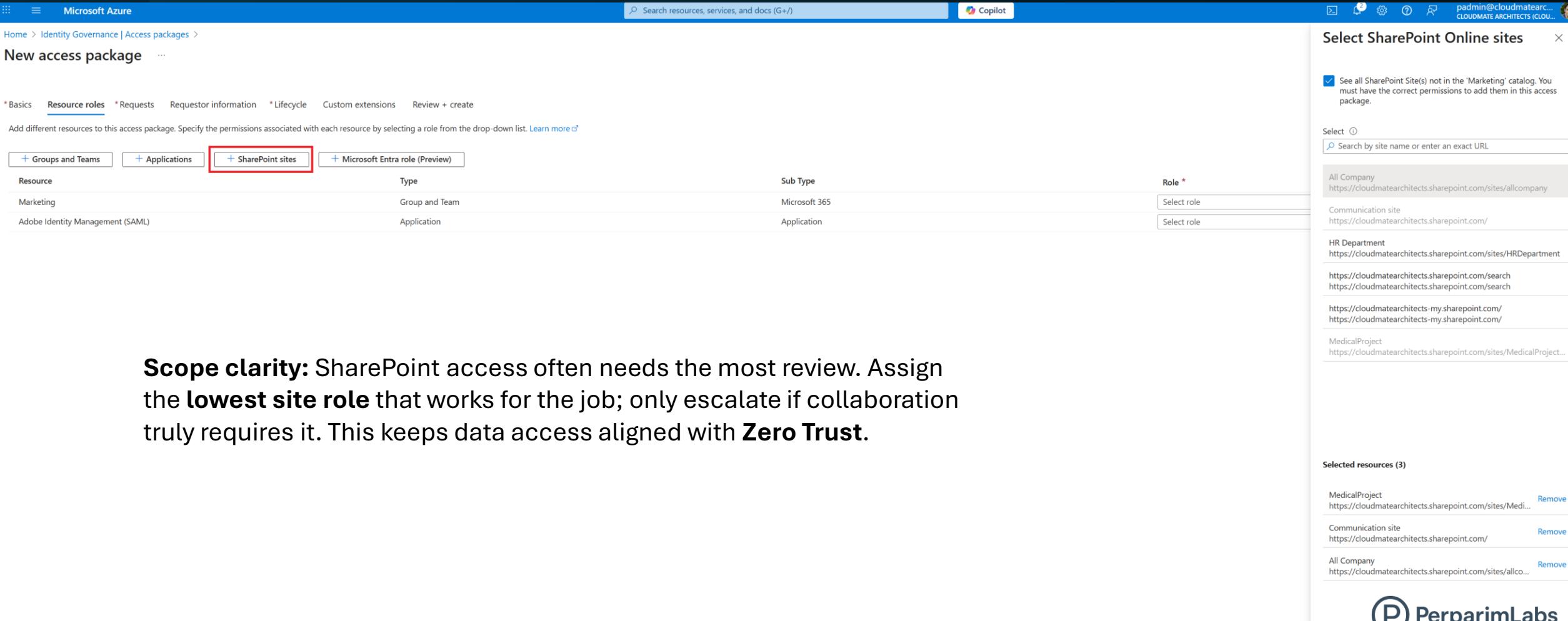


The screenshot shows the Microsoft Azure 'Enterprise applications' list. The sidebar indicates 282 applications found. The main table lists various Microsoft services and connectors, including Azure Purview, Azure Backup NRP Application, Privacy Management, Dynamic Alerts, Log Analytics API, Power BI Service, Connectors, Teams NRP DLP Ingestion Service, Microsoft SharePoint Online - Share..., Microsoft O365 Scobla, Azure Resource Manager, Windows 365, Windows Azure Active Directory, Microsoft Defender for Cloud Multi..., CapacityHybridAgreementApp, Database, Microsoft Azure AD Identity Protection, Azure Advisor, DevEngines, ComplianceAuthServer, Customer Experience Platform PROD, Microsoft Azure Signup Portal, PushChannel, Microsoft Power BI Service, Infobip, and CRM Service.

Showing the Enterprise Apps list highlights a **mature tenant** with multiple integrations—this is exactly where entitlement governance delivers the most value.

Add SharePoint sites

Added **MedicalProject**, **Communication site**, **All Company** with their default member roles.



The screenshot shows the Microsoft Azure Identity Governance 'New access package' interface. The 'Resource roles' tab is selected. A red box highlights the '+ SharePoint sites' button. The 'Selected resources (3)' section on the right lists 'MedicalProject', 'Communication site', and 'All Company', each with a 'Remove' link.

Selected resources (3)

- MedicalProject
<https://cloudmatearchitects.sharepoint.com/sites/MedicalProject...> Remove
- Communication site
<https://cloudmatearchitects.sharepoint.com/> Remove
- All Company
<https://cloudmatearchitects.sharepoint.com/sites/allcompany...> Remove

Who Can Request Access

- Defined users and groups allowed to request access to the package.
- Selected: **Perparim Abdullahu** and **Laura Johnson**
- Approval requirement: **No approval needed**
- This setup enables eligible users to self-request access while maintaining governance visibility.

Risk vs. friction: Limiting requestors (specific users/groups) maintains

Segregation of Duties. Skipping approvals is fine for **low-risk** packages; for sensitive apps/data, enable **manager or app owner approval**.

Microsoft Azure

Home > Identity Governance | Access packages > New access package

*Basics Resource roles *Requests Requestor information *Lifecycle Custom extensions Review + create

Create a policy to specify who can request an access package, who can approve requests, and when access expires. Additional request policies can be created. [Learn more](#)

Users who can request access

Users who can request access *

For users in your directory Allow users and groups in your directory to request this access package

For users not in your directory Allow users in connected organizations (other directories and domains) to request this access package

None (administrator direct assignments only) Allow administrators to directly assign specific users to this access package. Users cannot request this access package

Specific users and groups

All members (excluding guests)

All users (including guests)

Select users and groups ⓘ

Laura Johnson + 1 more

* + Add users and groups

Approval

Require approval * ⓘ

Yes No

Email Notifications

Disable assignment emails * ⓘ

Yes No

Enable

Enable new requests ⓘ

Enabling on-behalf-of requests requires a Microsoft Entra ID Governance subscription. [Learn more](#).

Allow managers to request on behalf of employees ⓘ

Yes No

Required Verified IDs

Choose whether or not you want users to show Verified IDs for this policy. First add the issuer's identifier and then add type of credential you want to check for. Users will need to present the selected credentials for this policy. [Learn more](#)

Require requestors to present a verified ID requires a Microsoft Entra ID Governance subscription. [Learn more](#).

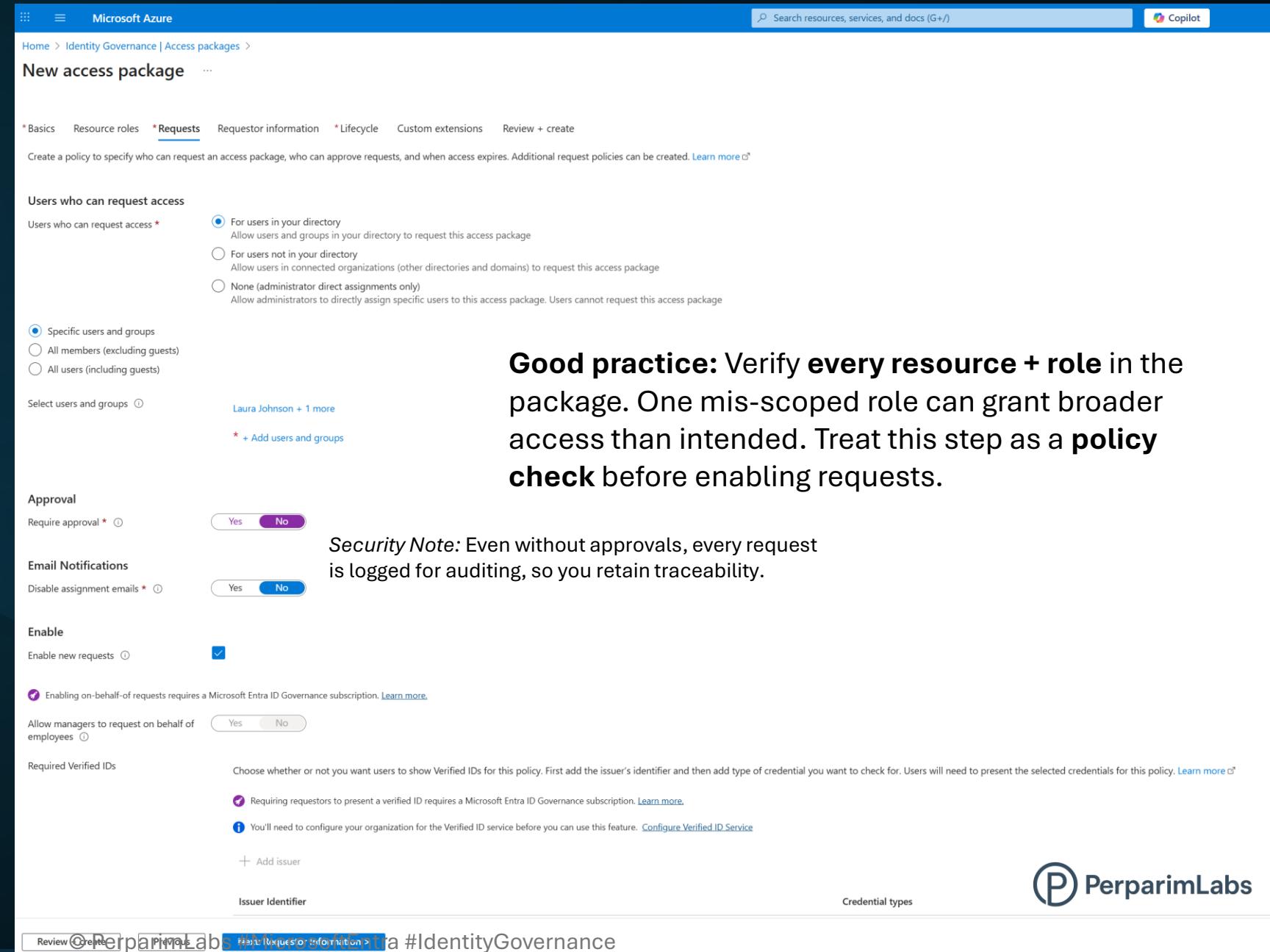
You'll need to configure your organization for the Verified ID service before you can use this feature. [Configure Verified ID Service](#)

+ Add issuer

Issuer Identifier

Credential types

Review Create Previous Requester information > #MicrosoftEntra #IdentityGovernance #AzureSecurity #AccessManagement #ZeroTrust #EntitlementManagement #CloudSecurity



Requestor Information (Optional Questions)

Here administrators can define additional attributes or custom questions to collect justification or business context from requesters.

In this demo, no custom questions were configured.

Microsoft Azure

Search resources, services, and docs (G/)

Home > Identity Governance | Access packages >

New access package

Use custom questions to capture **business justification, ticket IDs, or manager name**. This makes subsequent **access reviews** easier and strengthens audit trails.

* Basics Resource roles * Requests Requestor information * Lifecycle Custom extensions Review + create

Collect information and attributes from requestor. Go to Catalogs to add attributes for this access package's catalog resources. [Learn more](#)

Questions Attributes

Question	Add localization	Answer format
Enter question	add localization	Answer format

Lifecycle and Access Reviews

Configured lifecycle settings for ongoing access management.

Access reviews can be enabled to periodically verify if users still need access to the package — ensuring least-privilege and compliance. In this configuration, no access review policy was set.

Microsoft Azure

Home > Identity Governance | Access packages > New access package ...

* Basics Resource roles * Requests Requestor information *** Lifecycle** Custom extensions Review + create

Expiration

Access package assignments expire ⓘ

On date Number of days Number of hours Never

Assignments expire after (number of days) *

365

Users can request specific timeline *

Yes No

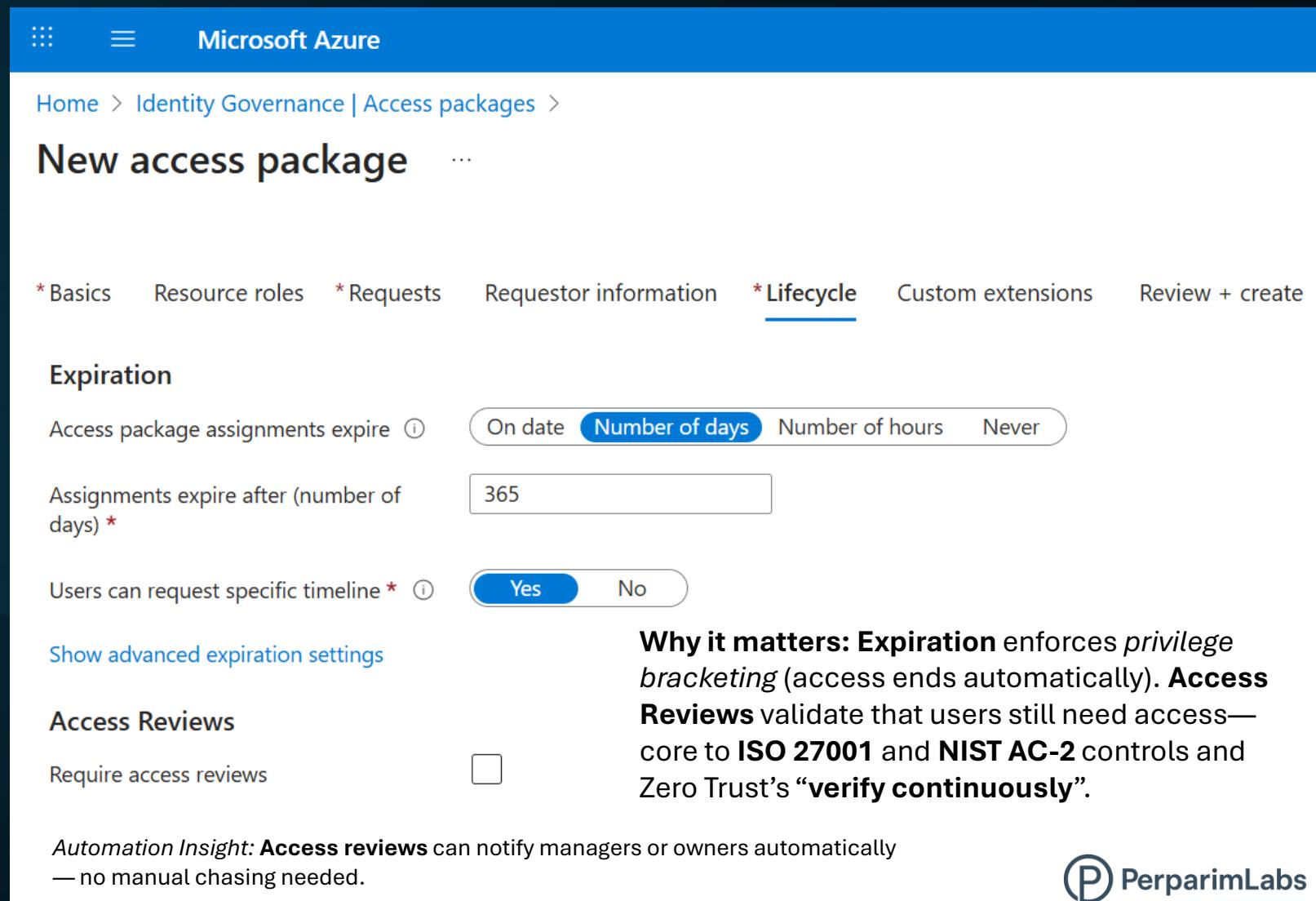
Show advanced expiration settings

Access Reviews

Require access reviews

Automation Insight: Access reviews can notify managers or owners automatically — no manual chasing needed.

Why it matters: **Expiration** enforces privilege bracketing (access ends automatically). **Access Reviews** validate that users still need access—core to **ISO 27001** and **NIST AC-2** controls and Zero Trust's "verify continuously".



Custom Extensions

Custom extensions allow administrators to automate external workflows such as ServiceNow approvals or ticket generation.
This step was skipped in this demo.

Microsoft Azure

Search resources, services, and docs (G/)

Home > Identity Governance | Access packages >

New access package

...

* Basics Resource roles * Requests Requestor information * Lifecycle **Custom extensions** Review + create

Configure a rule: If <event>, then do <flow>. A rule contains an event that/and triggers a previously defined custom flow

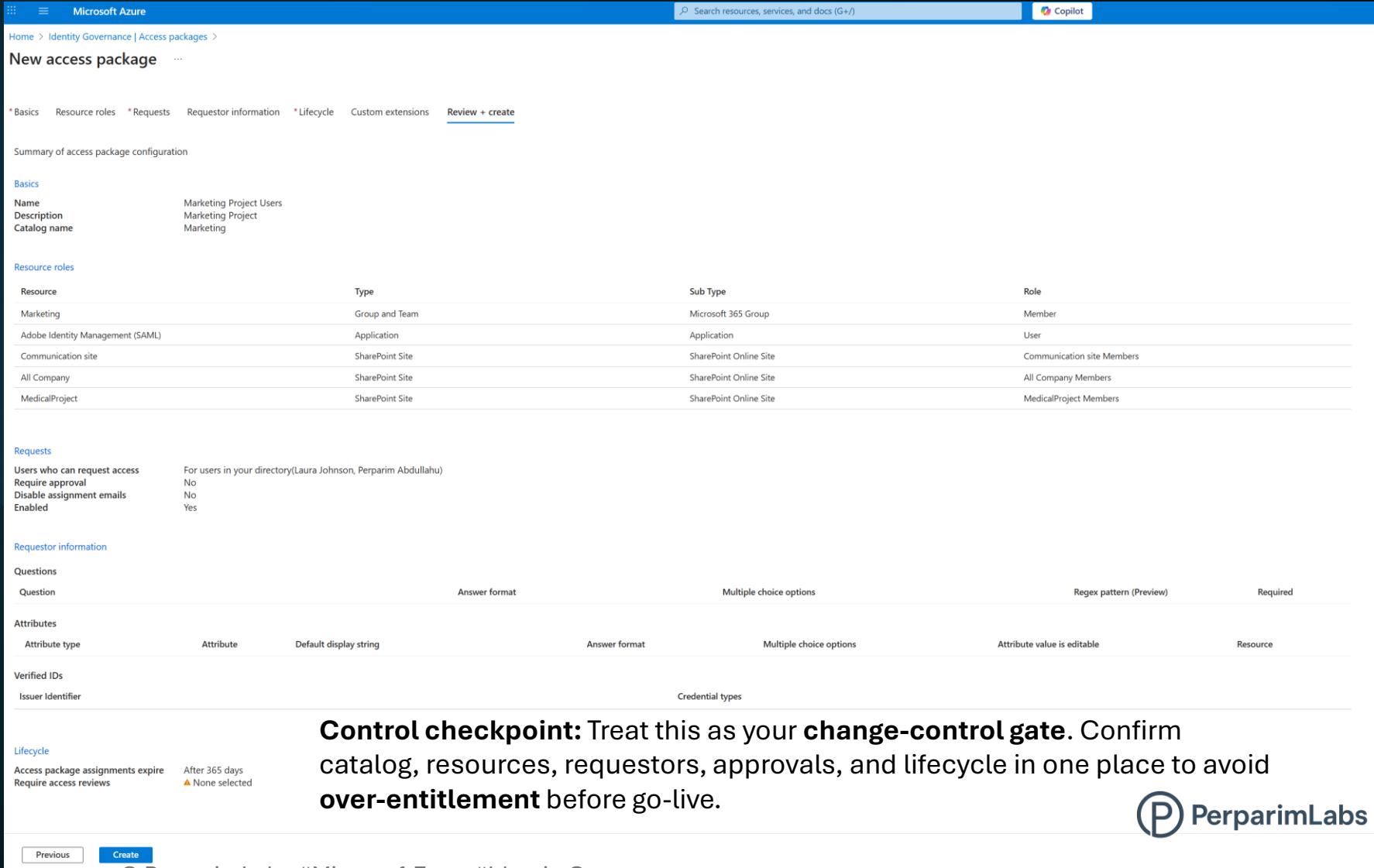
Custom extensions require a Microsoft Entra ID Governance subscription. [Learn more.](#)

Stage	Custom Extension
Select stage	Select custom extension

Extensions can trigger **ServiceNow/Jira tickets, Logic Apps, or Graph automations** during request/assignment events—useful for high-control environments.

Review and Confirm Configuration

Reviewed all configuration details for the *Marketing Project Users* access package, including catalog, resources, request settings, and lifecycle. Confirmed settings and created the package successfully.



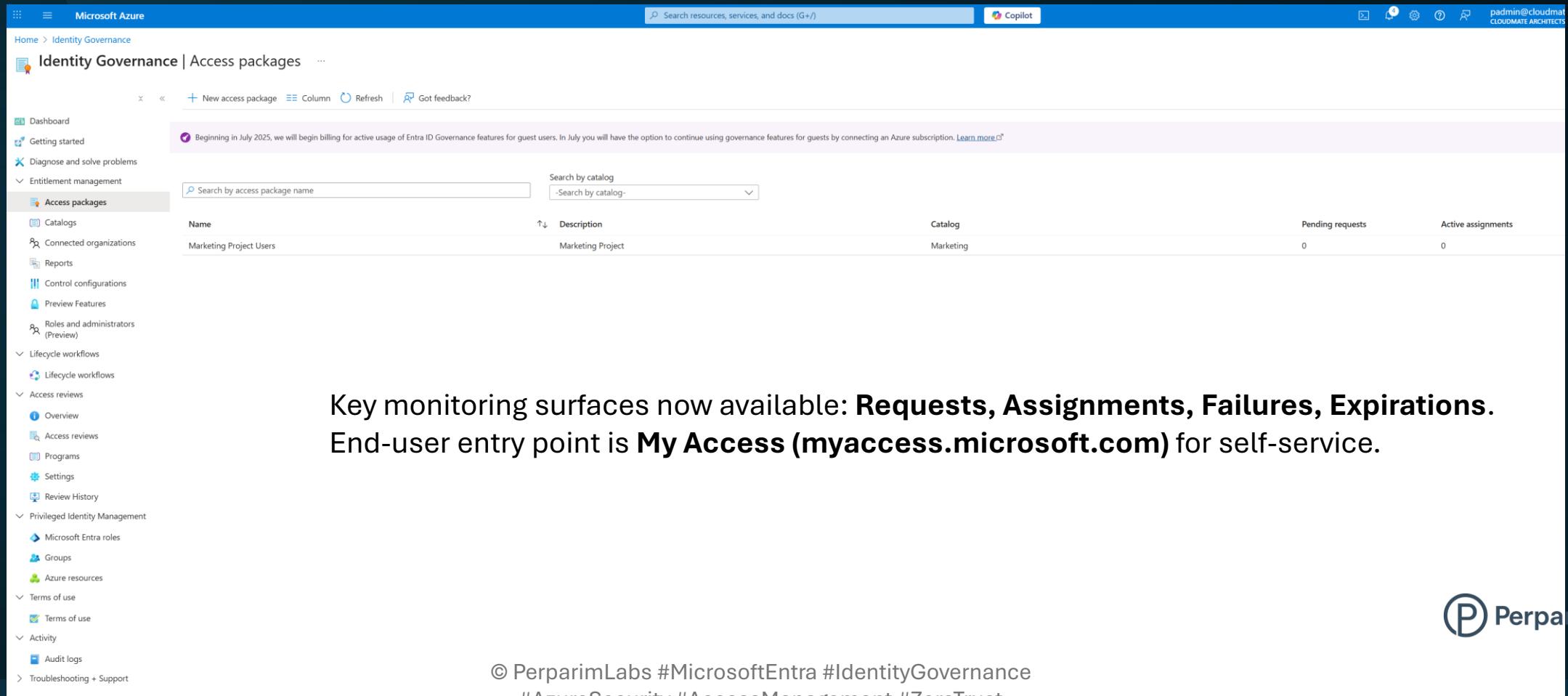
The screenshot shows the 'New access package' configuration page in Microsoft Azure. The page is titled 'New access package' and includes tabs for 'Basics', 'Resource roles', 'Requests', 'Requestor information', 'Lifecycle', 'Custom extensions', and 'Review + create'. The 'Review + create' tab is selected. The 'Basics' section shows a catalog named 'Marketing Project Users' with a description 'Marketing Project' and a catalog name 'Marketing'. The 'Resource roles' section lists resources and their types: Marketing (Group and Team, Microsoft 365 Group, Member), Adobe Identity Management (SAML) (Application, Application, User), Communication site (SharePoint Site, SharePoint Online Site, Communication site Members), All Company (SharePoint Site, SharePoint Online Site, All Company Members), and MedicalProject (SharePoint Site, SharePoint Online Site, MedicalProject Members). The 'Requests' section shows users can request access (Laura Johnson, Perparim Abdullahu), require approval (No), disable assignment emails (No), and enable requests (Yes). The 'Requestor information' section includes a table for questions, answer formats, multiple choice options, regex patterns, and required fields. The 'Attributes' section lists attribute types, attributes, default display strings, answer formats, multiple choice options, attribute value editability, and resource types. The 'Lifecycle' section shows access package assignments expire after 365 days and no reviews selected. The bottom of the page includes 'Previous' and 'Create' buttons.

Control checkpoint: Treat this as your **change-control gate**. Confirm catalog, resources, requestors, approvals, and lifecycle in one place to avoid **over-entitlement** before go-live.



Access Package Deployed Successfully

The *Marketing Project Users* access package now appears under the Access Packages list.
It's ready for users to request access through the *My Access Portal*.



The screenshot shows the Microsoft Azure Identity Governance Access packages list. The left sidebar shows various navigation options like Dashboard, Getting started, Diagnose and solve problems, Entitlement management, Access packages, Catalogs, Connected organizations, Reports, Control configurations, Preview Features, Roles and administrators (Preview), Lifecycle workflows, Access reviews, and Privileged Identity Management. The main content area shows a table with one row for the 'Marketing Project Users' access package. The table columns are Name, Description, Catalog, Pending requests, and Active assignments. The 'Marketing Project Users' row has 'Marketing Project' in the Description column and 'Marketing' in the Catalog column. Both Pending requests and Active assignments are 0. There are also two search bars: 'Search by access package name' and 'Search by catalog'. A message at the top states: 'Beginning in July 2025, we will begin billing for active usage of Entra ID Governance features for guest users. In July you will have the option to continue using governance features for guests by connecting an Azure subscription. [Learn more](#)'.

Name	Description	Catalog	Pending requests	Active assignments
Marketing Project Users	Marketing Project	Marketing	0	0

Key monitoring surfaces now available: **Requests, Assignments, Failures, Expirations.**
End-user entry point is **My Access (myaccess.microsoft.com)** for self-service.