

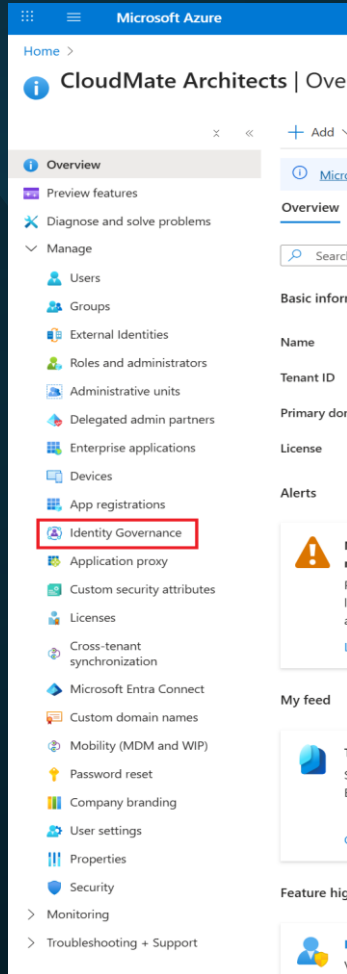


Build a Secure Access Catalog in Microsoft Entra

Implement governance foundation with Microsoft Entra Entitlement
Management

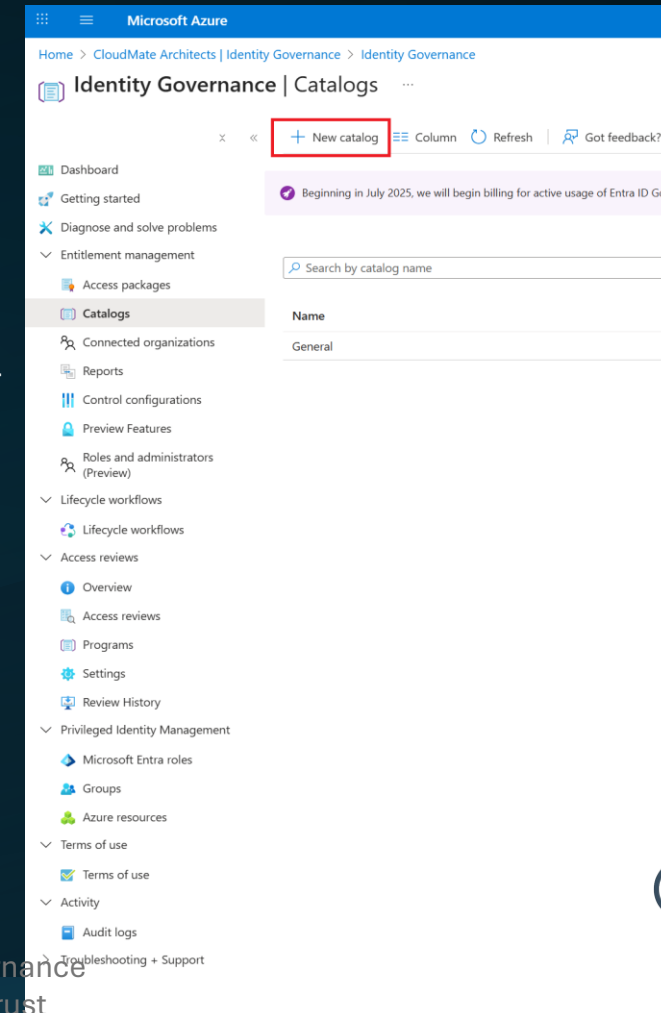
Open Microsoft Entra Admin Center

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



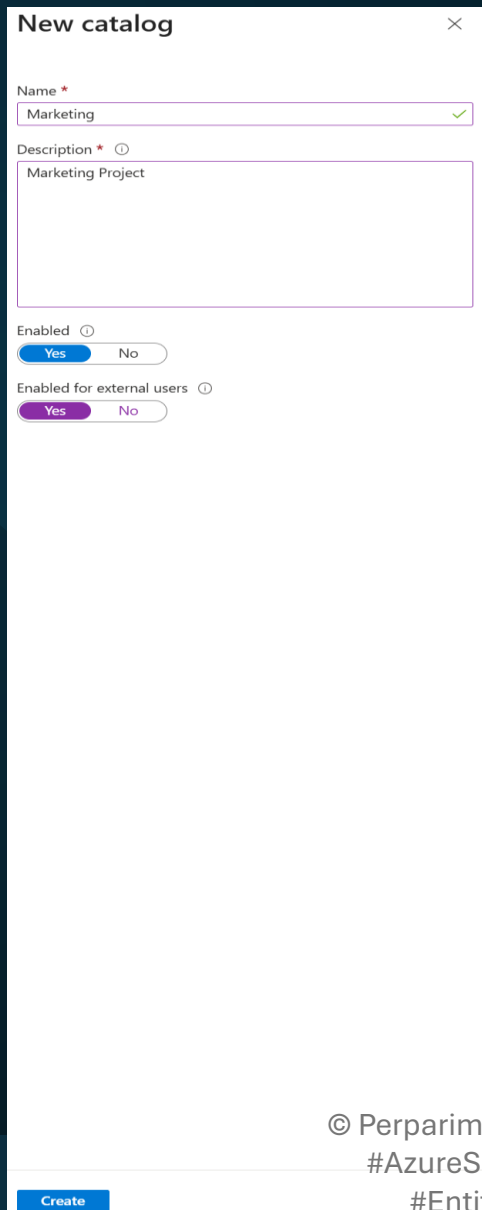
Architect Insight: Entitlement Management automates identity lifecycle governance — replacing static group membership with policy-based access that expires automatically.

Create New Catalog



Name the Catalog

Example:
Marketing Project
— describes
business scope



New catalog

Name *

Description *

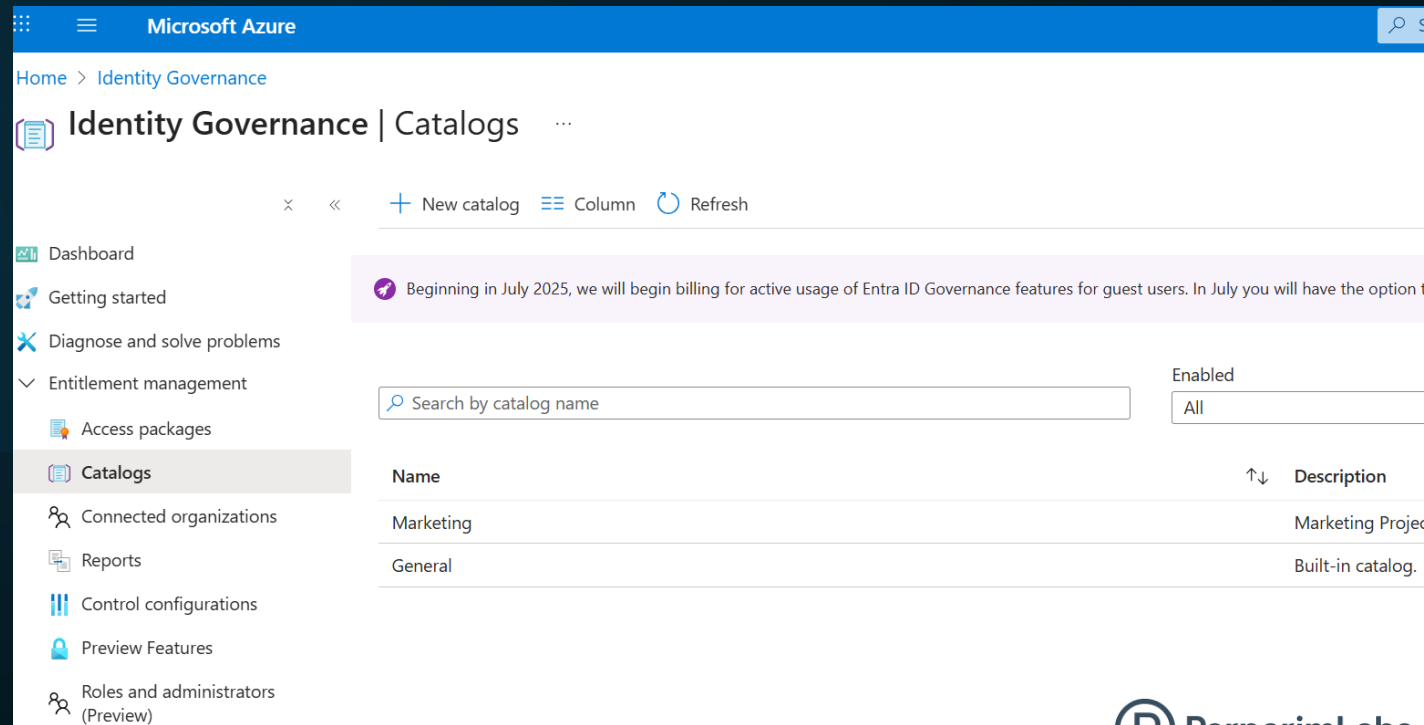
Enabled ☒ Yes ☐ No

Enabled for external users ☒ Yes ☐ No

[Create](#)

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

+ New catalog Column Refresh

Dashboard

Getting started

Diagnose and solve problems

Entitlement management

Access packages

Catalogs

Connected organizations

Reports

Control configurations

Preview Features

Roles and administrators (Preview)

Search by catalog name

Enabled All

Name	Description	Enabled
Marketing	Marketing Project	
General	Built-in catalog.	

Open Access packages → New access package

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

Microsoft Azure

Search resources, services,...

Home > Identity Governance

Identity Governance | Access packages

+ New access package Column Refresh

Dashboard

Getting started

Diagnose and solve problems

Entitlement management

Access packages

Catalogs

Connected organizations

Reports

Control configurations

Preview Features

Roles and administrators (Preview)

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...

Search by access package name

Search by catalog
-Search by catalog-

Name	Description
No access package exists	

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.

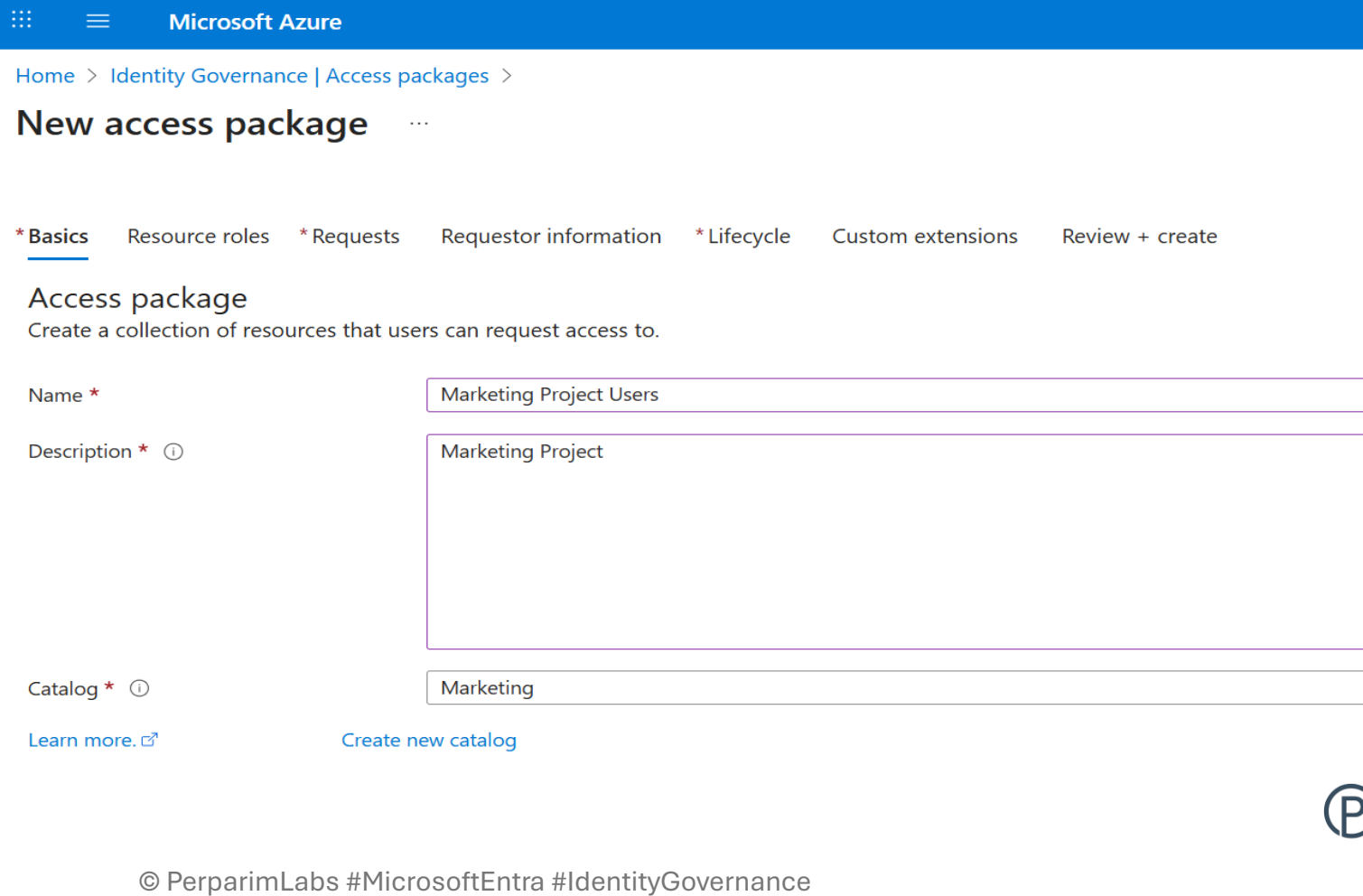
© PerparimLabs #MicrosoftEntra #IdentityGovernance
#AzureSecurity #AccessManagement #ZeroTrust
#EntitlementManagement #CloudSecurity

PerparimLabs

Name, description, and select **Marketing** catalog

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

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*.



Microsoft Azure

Home > Identity Governance | Access packages >

New access package ...

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

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](#)

Add Group: Marketing (Member)

Added Marketing M365 Group, role Member.

Microsoft Azure

Home > Identity Governance | Access packages >

New access package

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

Add different resources to this access package. Specify the permissions associated with each resource by selecting a role from the drop-down list. [Learn more](#)

+ Groups and Teams + Applications + SharePoint sites + Microsoft Entra role (Preview)

Resource	Type	Sub Type
----------	------	----------

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.

Select groups

Try changing or adding filters if you don't see what you're looking for.

☒ See all Group and Team(s) not in the 'Marketing' catalog. You must have the correct permissions to add them in this access package.

Search

10 results found

Groups

	Name	Email
<input type="checkbox"/>	AC All Company	allcompany@cloudmatearchitects.onmicrosoft.com
<input type="checkbox"/>	D/ Developers / Engineering	
<input type="checkbox"/>	EA Executives & Admins	
<input type="checkbox"/>	FD Finance Department	
<input type="checkbox"/>	GU Guests User	
<input type="checkbox"/>	HD HR Department	HRDepartment@cloudmatearchitects.onmicrosoft.com
<input type="checkbox"/>	HT HR Team	
<input type="checkbox"/>	IS IT & Security	
<input checked="" type="checkbox"/>	M Marketing	MedicalProjectGroup@cloudmatearchitects.onmicrosoft.com
<input type="checkbox"/>	W WHiB_Pilot	

Selected groups (1)

Reset

M Marketing
MedicalProjectGroup@cloudmatearchitects.onmicrosoft.com

Review + create Previous Next: Requests >

Add Application: Adobe Identity Management (SAML)

Added SAML app with role User.

The screenshot shows the 'New access package' page in the Microsoft Azure portal. The 'Resource roles' tab is active, and the 'Applications' button is highlighted with a red box. The 'Select applications' pane on the right shows 'Adobe Identity Management (SAML)' as the selected application.

Resource	Type	Sub Type
Marketing	Group and Team	Microsoft 365

Select applications

Try changing or adding filters if you don't see what you're looking for.

☒ See all Application(s) not in the 'Marketing' catalog. You must have the correct permissions to add them in this access package.

Search 1 result found

Enterprise applications

Name	Details
<input checked="" type="checkbox"/> Adobe Identity Management (SAML)	8fe30ae5-7d8d-4999-ac48-faec25862a09

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 'Enterprise applications' list in the Microsoft Azure portal. The list contains various applications, including Azure Purview, Azure Backup NRP Application, Privacy Management, Dynamic Alerts, Log Analytics API, Power BI Service, Connectors, Teams NRT DLP Ingestion Service, Microsoft SharePoint Online - ShareP..., Azure Resource Manager, Windows 365, Windows Azure Active Directory, Bing, Microsoft Defender for Cloud MACTI..., Capacity/Policy/AssignmentApp, Dataverse, Microsoft Azure AD Identity Protection, Azure Advisor, WeatherEngine, ComplianceAdvisor, Customer Experience Platform PROD, Microsoft Azure Signin Portal, PushChannel, and Microsoft Azure AD Identity Protection.

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry Status	Active Certificate Expiry Date	Identifier URI (Entity ID)
Azure Purview							
Azure Backup NRP Application							
Privacy Management							
Dynamic Alerts							
Log Analytics API							
Power BI Service							
Connectors							
Teams NRT DLP Ingestion Service							
Microsoft SharePoint Online - ShareP...							
Azure Resource Manager							
Windows 365							
Windows Azure Active Directory							
Bing							
Microsoft Defender for Cloud MACTI...							
Capacity/Policy/AssignmentApp							
Dataverse							
Microsoft Azure AD Identity Protection							
Azure Advisor							
WeatherEngine							
ComplianceAdvisor							
Customer Experience Platform PROD							
Microsoft Azure Signin Portal							
PushChannel							
Microsoft Azure AD Identity Protection							

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.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

padmin@cloudmatearc...
CLOUDMATE ARCHITECTS (CLOU...

Home > Identity Governance | Access packages >

New access package

* Basics

Resource roles

* Requests

Requestor information

* Lifecycle

Custom extensions

Review + create

Add different resources to this access package. Specify the permissions associated with each resource by selecting a role from the drop-down list. [Learn more](#)

+ Groups and Teams

+ Applications

+ SharePoint sites

+ Microsoft Entra role (Preview)

Resource	Type	Sub Type	Role *
Marketing	Group and Team	Microsoft 365	Select role
Adobe Identity Management (SAML)	Application	Application	Select role

Select SharePoint Online sites

☒ See all SharePoint Site(s) not in the 'Marketing' catalog. You must have the correct permissions to add them in this access package.

Select

Search by site name or enter an exact URL

All Company
https://cloudmatearchitects.sharepoint.com/sites/allcompany

Communication site
https://cloudmatearchitects.sharepoint.com/

HR Department
https://cloudmatearchitects.sharepoint.com/sites/HRDepartment

https://cloudmatearchitects.sharepoint.com/search
https://cloudmatearchitects.sharepoint.com/search

https://cloudmatearchitects-my.sharepoint.com/
https://cloudmatearchitects-my.sharepoint.com/


MedicalProject
https://cloudmatearchitects.sharepoint.com/sites/MedicalProject...

Selected resources (3)

MedicalProject
https://cloudmatearchitects.sharepoint.com/sites/Medi... Remove

Communication site
https://cloudmatearchitects.sharepoint.com/ Remove

All Company
https://cloudmatearchitects.sharepoint.com/sites/allco... Remove



Scope clarity: SharePoint access often needs the most review. Assign the **lowest site role** that works for the job; only escalate if collaboration truly requires it. This keeps data access aligned with **Zero Trust**.

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](#)

✓ Requiring 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 Next Requestor information > #IdentityGovernance

Good practice: Verify **every resource + role** in the package. One mis-scoped role can grant broader access than intended. Treat this step as a **policy check** before enabling requests.

Security Note: Even without approvals, every request is logged for auditing, so you retain traceability.

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](#)

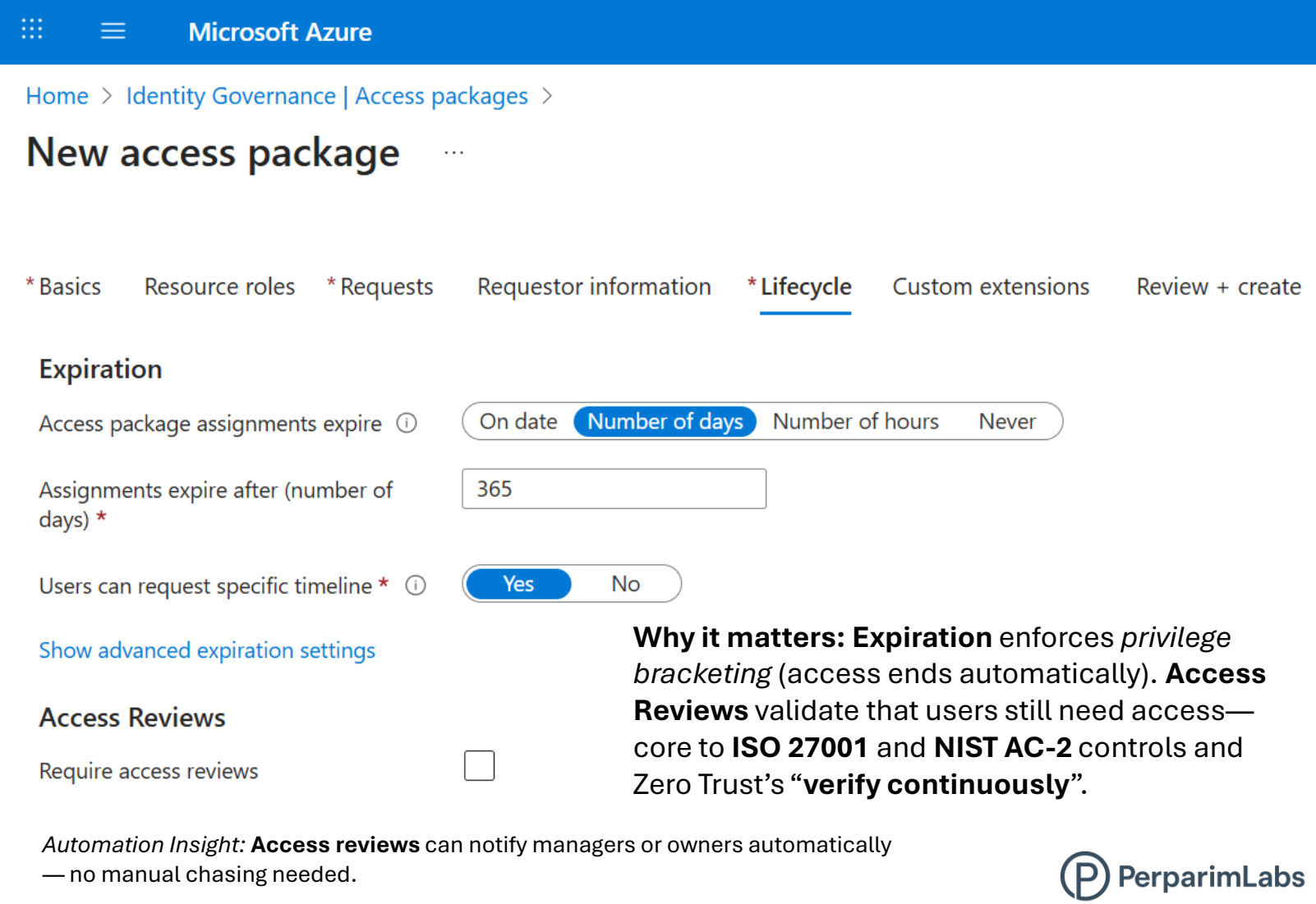
[Questions](#) [Attributes](#)

Question	Add localization	Answer format
<input type="text" value="Enter question"/>	add localization	<input type="text" value="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 ☐

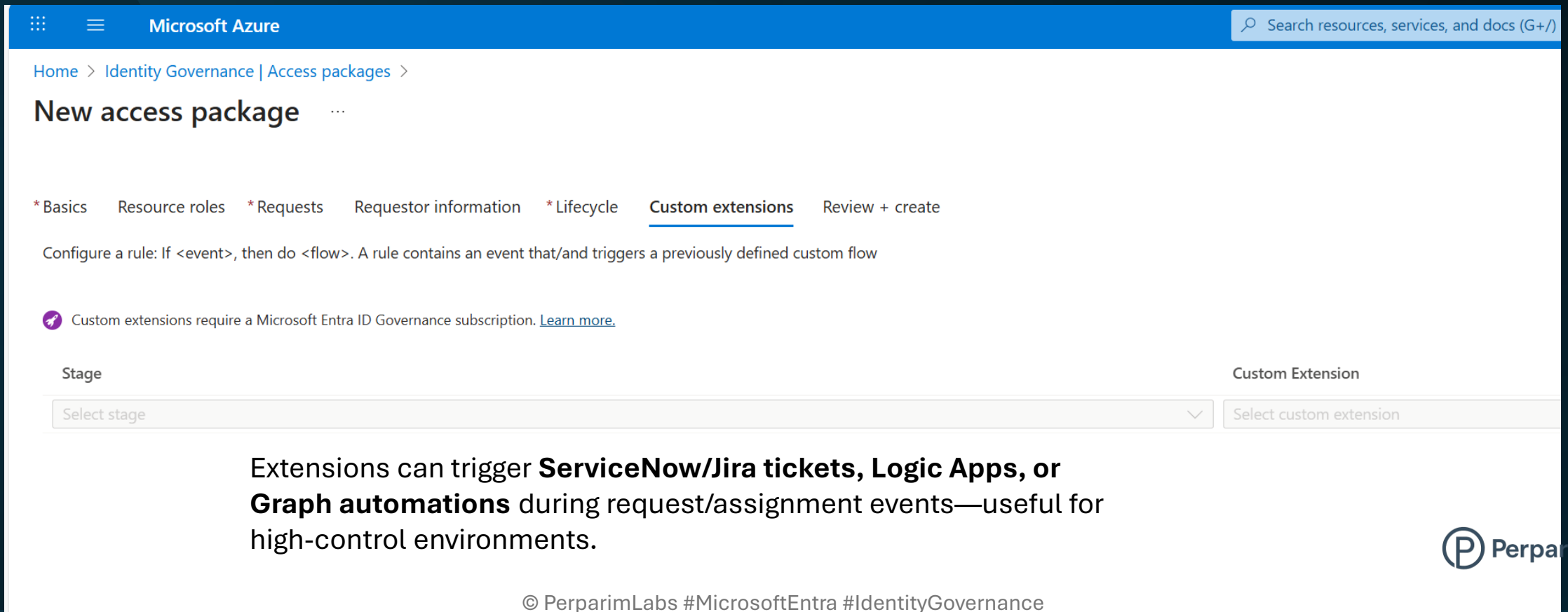
Automation Insight: **Access reviews** can notify managers or owners automatically — no manual chasing needed.

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**”.

 PerparimLabs

Custom Extensions

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



The screenshot shows the Microsoft Azure portal interface. At the top is a blue header with the Microsoft Azure logo and a search bar. Below the header, the breadcrumb trail reads 'Home > Identity Governance | Access packages >'. The main heading is 'New access package'. A series of tabs are visible: '* Basics', 'Resource roles', '* Requests', 'Requestor information', '* Lifecycle', 'Custom extensions' (which is underlined), and 'Review + create'. Below the tabs, a descriptive text states: 'Configure a rule: If <event>, then do <flow>. A rule contains an event that/and triggers a previously defined custom flow'. A purple icon with a lightning bolt is followed by the text: 'Custom extensions require a Microsoft Entra ID Governance subscription. [Learn more.](#)'. Below this, there are two dropdown menus. The first is labeled 'Stage' and has a placeholder 'Select stage'. The second is labeled 'Custom Extension' and has a placeholder 'Select custom extension'. At the bottom of the screenshot, there is a text block that reads: 'Extensions can trigger **ServiceNow/Jira tickets, Logic Apps, or Graph automations** during request/assignment events—useful for high-control environments.'

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.

Microsoft Azure

Search resources, services, and docs (G+/)

Copilot

Home > Identity Governance > Access packages >

New access package

* Basics

Resource roles

* Requests

Requestor information

* Lifecycle

Custom extensions

Review + create

Summary of access package configuration

Basics

Name

Description

Catalog name

Marketing Project Users

Marketing Project

Marketing

Resource roles

Resource	Type	Sub Type	Role
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
MedicalProject	SharePoint Site	SharePoint Online Site	MedicalProject Members

Requests

Users who can request access

Require approval

Disable assignment emails

Enabled

For users in your directory(Laura Johnson, Perparim Abdullahu)

No

No

Yes

Requestor information

Questions	Answer format	Multiple choice options	Regex pattern (Preview)	Required
Question				

Attributes

Attribute type	Attribute	Default display string	Answer format	Multiple choice options	Attribute value is editable	Resource

Verified IDs

Issuer Identifier	Credential types

Lifecycle

Access package assignments expire

Require access reviews

After 365 days

▲ None selected

Previous

Create

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.

Perparim Labs

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*.

Microsoft Azure Identity Governance | Access packages

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.