

# Automating External User Onboarding, Collaboration, and Offboarding with Entra ID - Identity Governance: A Scenario Guide

By Kamran Astadabadi  
18<sup>th</sup> December 2024

## Disclaimer

This document is not an official Microsoft document. It provides insights and guidance based on practical experience and observations for automating external user onboarding and collaboration using Microsoft Entra ID Identity Governance. The scenarios and recommendations shared here are intended to complement official Microsoft guidance. For the latest and most accurate information, please refer to the relevant Microsoft documentation linked at the end of this guide.

**Collaboration** with external vendors, such as Vendor A, Vendor B, and Vendor C, often requires secure and streamlined access to resources like SharePoint folders. Without a structured approach, it can be challenging to manage access, especially when users frequently change, or multiple projects are involved.

Microsoft Entra ID Entitlement Management provides a solution to address these challenges. This guide explains how to use Entitlement Management to grant secure, governed, and automated access to external users while maintaining compliance.

## Common Challenges

1. **Varied Access Needs**  
External users often require different levels of access depending on their roles and projects.
2. **Governance Risks**  
Without a proper framework, users may retain access beyond their required period, creating potential security risks.
3. **Time-Consuming Processes**  
Manual onboarding and offboarding of external users can be inefficient and prone to errors.
4. **Limited Visibility**  
It can be difficult to track who has access to critical resources, leading to compliance concerns.

## Proposed Solution

Using Microsoft Entra ID Entitlement Management, you can create Access Packages tailored to specific projects or resources. These packages streamline external user access by defining:

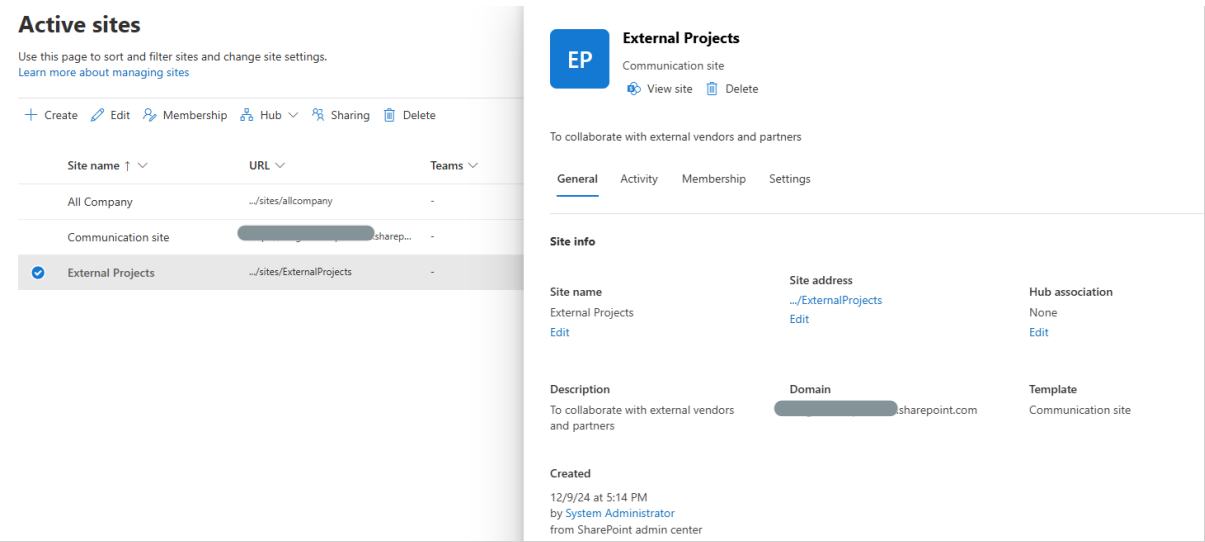
- Who can request access.
- Approval workflows.
- The duration of access, with automatic expiration.
- Periodic access reviews for compliance.

For example, Vendor A's team members can request access to Project A resources. Access is granted after approval by the designated approvers and will automatically expire unless explicitly extended.

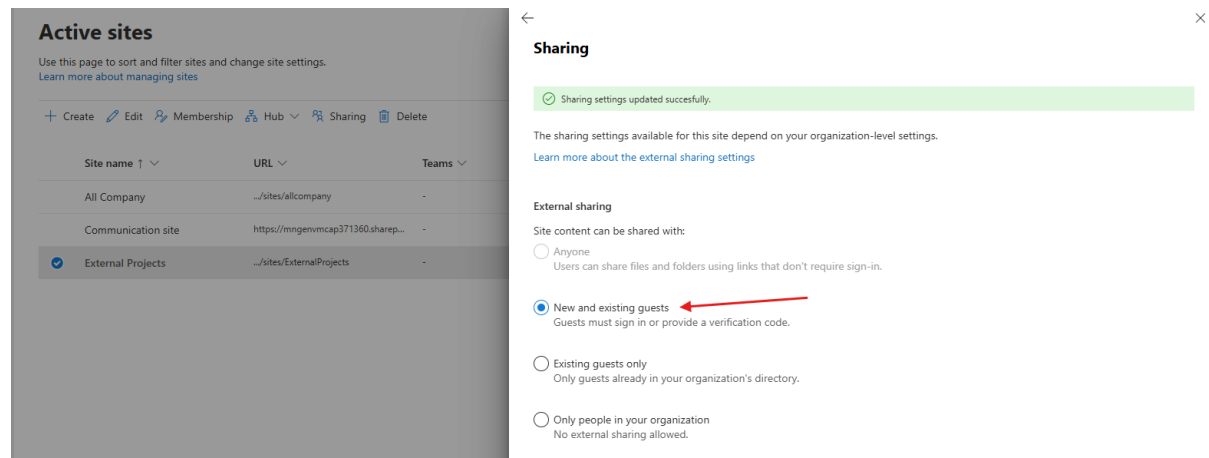
# Implementation Step-by-Step

## 1. Set Up a SharePoint Site for Collaboration

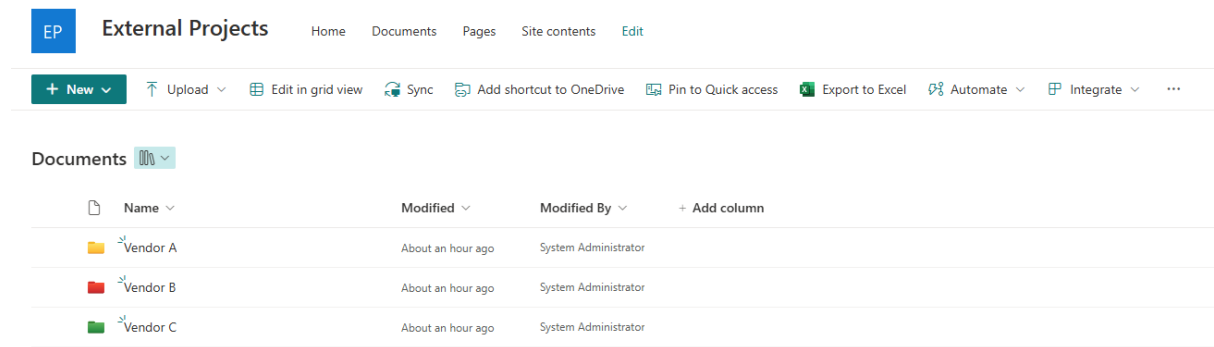
Start by creating e.g. a dedicated SharePoint Communication Site to manage external collaboration.



### a. Enable External Sharing Settings to allow external users access.



### b. Create a structured folder and subfolder hierarchy for organizing project files.



EP

External Projects

Home Documents Pages Site contents Edit

+ New

Upload

Edit in grid view

Share

Copy link

Sync

Add shortcut to OneDrive

Download

Export to Excel

Documents > Vendor A

	Name	Modified	Modified By	+ Add column
	Project A	48 minutes ago	System Administrator	
	Project B	48 minutes ago	System Administrator	

2. Create Security Groups

In the Microsoft Entra Admin Center, create security groups to manage access permissions. For example, use a naming convention like SG-EXT-<Vendor Name> to group users by vendor. These groups will be linked to Entitlement Management later.

	Name	Object Id	Group type	Membership type	Email
<input type="checkbox"/>	SG-EXT-Vendor-B	107ae506-3d5e-428f-bb82-43b35472ea6e	Security	Assigned	
<input type="checkbox"/>	SG-EXT-Vendor-C	8ba89263-19ca-4323-85f2-9fb17be19dcf	Security	Assigned	
<input type="checkbox"/>	SG-EXT-Vendor-A	f3326405-7c7f-40c8-b6ec-ce178a0c89d2	Security	Assigned	
<input type="checkbox"/>	SG-EXT-Vendor-A-PROJECT-B	17a48323-3700-4b34-97c5-a636cf97a85b	Security	Assigned	
<input type="checkbox"/>	SG-EXT-Vendor-B-PROJECT-A	33faf3a4-ab06-40e1-b385-9cee6b9ddc01	Security	Assigned	
<input type="checkbox"/>	SG-EXT-Vendor-C-PROJECT-B	ad4f92f0-17de-4039-833b-ffa2d69d666	Security	Assigned	

Structure your authorisation structure accordingly. The group you add here, will later enable your users to be added through Entitlement Management to access the appropriate Folder or Subfolder.

EP

External Projects

Home Documents Pages Site contents Edit

+ New

Edit in grid view

Share

Copy link

Delete

Pin to top

Favorites

Add shortcut to OneDrive

Download

Documents

	Name	Modified	Modified
	Vendor A	About an hour ago	System Adm
	Vendor B	About an hour ago	System Adm
	Vendor C	About an hour ago	System Adm

Manage Access

Vendor A

Share

Stop sharing

People • 1 Groups • 4 Links

External Projects Owners

SHAREPOINT GROUP

Owner

External Projects Visitors

SHAREPOINT GROUP

Can view

External Projects Members

SHAREPOINT GROUP

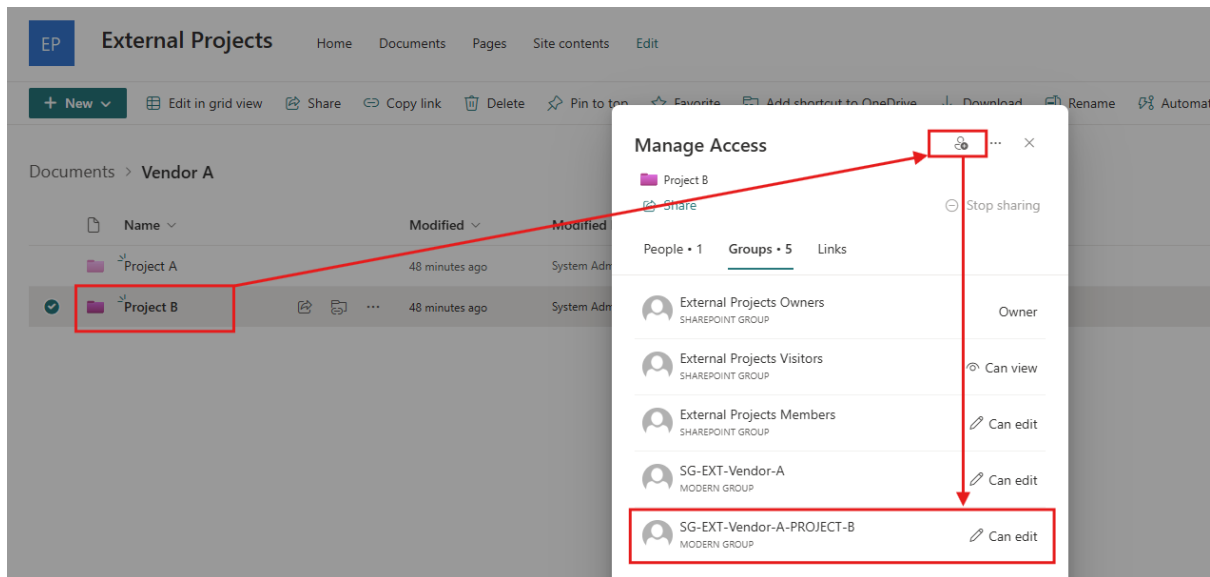
Can edit

SG-EXT-Vendor-A

MODERN GROUP

Can edit

**Pro-tip:** Consider reviewing folder inheritance settings in SPO for subfolder permissions (e.g., breaking inheritance for sensitive subfolders).

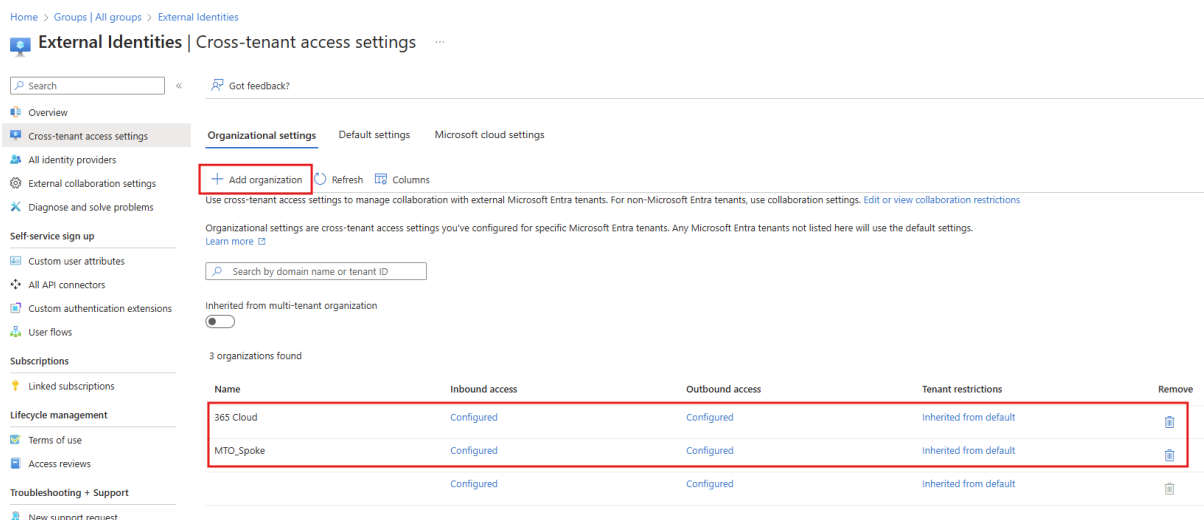


### 3. Configure Cross-Tenant Access Settings

Set up Cross-Tenant Access Settings to allow secure collaboration with external tenants. This ensures that users from Vendor A, B, or C can authenticate and access shared resources in your environment.

**Pro-tip:** Configure Conditional Access policies to accept claims from other Microsoft Entra tenants for external user access. By default, these settings apply to all external tenants unless customized for specific organizations.

Trust MFA from Microsoft Entra tenants to reduce MFA fatigue for external users, while maintaining secure access. To enforce additional requirements, such as compliant or hybrid-joined devices, ensure Conditional Access is configured for guest users across all cloud apps.



## 4. Configure Entitlement Management

### 4.1 Add Connected Organizations:

Adding Connected Organizations in Microsoft Entra ID facilitates secure and streamlined collaboration with external users. This setup allows external users from specified organizations to request access to your resources via Access Packages. Connected Organizations represent these external companies and provide a structured framework for managing access requests.

Sponsors play a key role in this process, serving as points of contact for governance and accountability:

- **External Sponsors:** Guest users from the connected organization, already present in your directory, who verify and validate access requests from their organization.
- **Internal Sponsors:** Member users within your organization who oversee and manage the relationship with the external organization.

Home > Identity Governance

Identity Governance | Connected organizations

Dashboard, Getting started, Diagnose and solve problems, Entitlement management, Access packages, Catalogs, **Connected organizations**, Reports, Settings

+ Add connected organization, Download, Refresh, Got feedback?

Search by name

Name	Description	Conn...	Internal sponsors	External sponsors	Connected date	State
Tenant A (365 Cloud)	365 Cloud Tenant   ETLM...	admin@...	1	1	12/6/2024	Configured
Tenant C (from MTO_SPOKE)	MTO_Spoke Tenant	admin@...	-	-	12/9/2024	Configured

### 4.2 Create a Catalog

Create a catalog, which is a container of resources and access packages. You can create a catalog when you want to group related resources and access packages. For instance, you may create a business partner catalog for organizations dealings with another organization. Inside this catalog, you can create access packages. An access package enables you to do a one-time setup of resources and policies that automatically administers access for the life of the access package. These access packages can be tailored to the various external users and partners within your organisation. You may have an access package for your vendors, and one for your contractors, and another for your internal users.

Home > Identity Governance

Identity Governance | Catalogs

Dashboard, Getting started, Diagnose and solve problems, Entitlement management, Access packages, **Catalogs**, Connected organizations, Reports, Settings

+ New catalog, Column, Refresh, Got feedback?

Search by catalog name, Enabled: All, Enabled for external users: All

Name	Description	Access packages	Resources	Enabled
General	Built-in catalog.	0	1	No
Vendor A	Company A	0	0	Yes
Vendor B	Company B	0	0	Yes
Vendor C	Company C	0	0	Yes

### 4.3 Create an Access Package

Within the catalog, create an Access package to define access and collaboration permissions. Scoping to the previously created catalog for Vendor A to this Access package.

[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 \*

Description \*

Catalog \*

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

Under Resource roles, add the Security Group which provides access through SharePoint Folder for Vendor A.

[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
SG-EXT-Vendor-A	Group and Team	Security	Member

For current requirements in this scenario there is no need to add any other resources like, Applications, SharePoint sites, etc.

### 4.4 Configure Policies

In the next step we will create a policy to specify who can request an access package, who can approve requests, and when access expires.

Implement multi-stage approvals if needed. For example:

## 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

 Learn more about setting up policies for users not yet in your directory

- ☒ Specific connected organizations
- ☐ All configured connected organizations
- ☐ All users (All connected organizations + any new external users)

Select connected organizations ⓘ

[Tenant A \(365 Cloud\)](#)

\* [+ Add directories](#)

Who can approve requests? In this scenario, we want to ensure having a 2-stage approval process. The first approver must be from the external Vendor, and once Vendor A approves the request it will move to the internal approver to allow access to SharePoint resources.

### Stage 1: Approval by the vendor's external sponsor.

#### Approval

Require approval \* ⓘ

☒ Yes ☐ No

Require requestor justification ⓘ

☒ Yes ☐ No

How many stages ⓘ

☐ 1 ☒ 2 ☐ 3

#### First Approver


External sponsor

Fallback ⓘ

Alex Wilber

\* [+ Add fallback](#)

Decision must be made in how many days? \* ⓘ

7 

Maximum 14

Require approver justification ⓘ

☒ Yes ☐ No

[Hide advanced request settings](#)

If no action taken, forward to alternate approvers? ⓘ

☒ Yes ☐ No

Alternate Approver

Choose specific alternate approvers

Select alternate approvers ⓘ

Adele Vance

\* [+ Add alternate approvers](#)

Forward to alternate approver(s) after how many days? \* ⓘ

5

(Allowed number of days is 0 - 6)

## Stage 2: Approval by an internal sponsor from your organization.

**Second Approver**

Internal sponsor ▼

Fallback ⓘ System Administrator

\* + Add fallback

Decision must be made in how many days? \* ⓘ  Maximum 14

Require approver justification ⓘ Yes No

[Hide advanced request settings](#)

If no action taken, forward to alternate approvers? ⓘ Yes No

**Enable**

Enable new requests \* ⓘ 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](#) ⓘ

1

## Lifecycle: Set expiration policies and enable periodic reviews to ensure compliance.

[\\* 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) \*  ✓

Users can request specific timeline \* ⓘ Yes No

[Hide advanced expiration settings](#)

Allow users to extend access \* ⓘ Yes No

Require approval to grant extension \* ⓘ Yes No

**Access Reviews**

Require access reviews \* Yes No

Starting on ⓘ  📅

Review frequency ⓘ Annually Bi-annually Quarterly Monthly Weekly

Duration (in days) \* ⓘ  Maximum 27

Reviewers ⓘ ☒ Self-review ☐ Specific reviewer(s) ☐ Manager

[Hide advanced access review settings](#)

If reviewers don't respond ⓘ Remove access ▼

Show reviewer decision helpers ⓘ Yes No

Require reviewer justification ⓘ Yes No



Once you completed the configuration, a summary of all settings will be displayed to be reviewed and submitted for creation of the Access Package.

Basics

Resource roles

Requests

Requestor information

Lifecycle

Custom extensions

Review + create

Summary of access package configuration

Basics

Name

Description

Catalog name

AP01-01-VENDOR-A-FULL-ACCESS

With this Access Package you will gain access to the External Collaboration SharePoint folder.

Vendor A

Resource roles

Resource

Type

Sub Type

Role

SG-EXT-Vendor-A

Group and Team

Security Group

Member

Requests

Users who can request access

Require approval

Enabled

Require requestor justification

How many stages

For users not in your directory(Tenant A (365 Cloud))

Yes

Yes

Yes

2

First Approver

Approvers

Decision must be made in how many days?

Require approver justification

If no action taken, forward to alternate approvers?

Forward to alternate approver(s) after how many days?

External sponsor ; Fallback(Alex Wilber)

7

Yes

Yes

5

Previous

Create

With this, you just created your first Access Package.

External users must use a directory hint link provided by e.g. the project manager or administrator. **Alternatively**, external users must **switch organisations** from the My Access portal to see eligible Access Packages.

Home > Identity Governance | Access packages >

AP01-01-VENDOR-A-FULL-ACCESS

Access package

« Edit Delete

Overview

Manage

Resource roles

Policies

Separation of Duties

Assignments

Requests

Access reviews

AP01-01-VENDOR-A-FULL-ACCESS

With this Access Package you will gain access to the External Collaboration SharePoint folder.

Properties

Created by

Created on

Object Id

Catalog

Hidden

My Access portal link

Vendor A

No

19952cfe-ddca-4acd-ac16-c71f112aa83b

https://myaccess.microsoft.com/@

Copy to clipboard

Contents

Resource roles

Policies

Activity

Incompatible assignments

1 Groups and Teams 0 Apps 0 SPO 0 Microsoft Entra role

1 Enabled 0 Disabled

0 Assignments 0 Pending Requests

0

N/A Change Propagation Sync

# User Experience

External users interact with Access Packages differently than internal users. Here's how they can request and gain access:

Requesting access through Access Packages in Microsoft Entra ID involves a slightly different experience for external users, such as those from **Tenant A**, compared to internal users. External users will not see Access Packages directly in their own tenant's My Access portal. Instead, they need to use a specific link to access the appropriate Access Package.

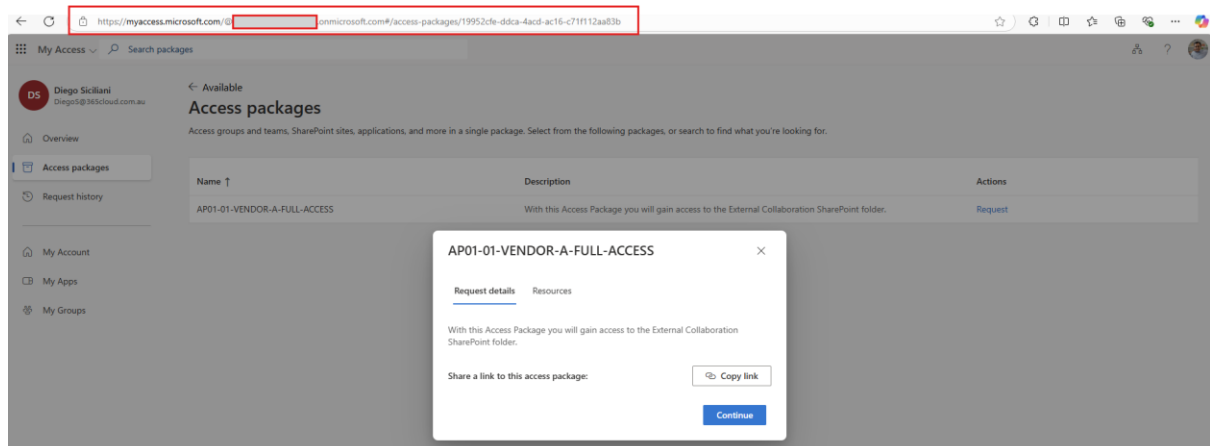
## Accessing the My Access Portal

External users must receive a link to the Access Package they need. This link is typically provided via email or a direct message from the project or business manager they are collaborating with.

The link format includes a directory hint and access package ID (e.g., [https://myaccess.microsoft.com/@<directory\\_hint>#/access-packages/<access\\_package\\_id>](https://myaccess.microsoft.com/@<directory_hint>#/access-packages/<access_package_id>)).


When users open the link, they will be redirected to the My Access portal of the hosting organization.

By using the directory hint link, organizations ensure that external users are securely directed to the relevant Access Packages while maintaining governance and oversight.



## Signing In

Users sign in with their organizational account (e.g., work or school email) and may need to reauthenticate to ensure secure access.



← diegos@365cloud.com.au

## Enter password

.....

[Forgot my password](#)

[Sign in](#)

365Cloud

### Requesting Access

Once signed in, users can view the linked Access Package and follow guided steps to submit their request.

← Additional questions

Business justification \*

Add your business justification here!

[Continue](#)

← Consent form

☐ By requesting access, you are sharing your name, email address, and organization name with [redacted]. If your request is approved, you'll be invited to participate in [redacted] and your information will be managed in accordance with [redacted] privacy policies.

[Submit request](#)

## Approval and Access

After approval, access is granted automatically. External users are:

- Automatically created in the target tenant.
- Added to the appropriate Entra-ID security group (e.g., SG-EXT-Vendor-A).
- Able to access the requested resources directly using their existing organizational account.

The screenshot shows the 'Approvals' page in the Microsoft Entra ID portal. The user is Alex Wilber. The page shows 1 pending approval. A table lists the request: Diego Siciliani requested 'AP01-01-VENDOR-A-FULL-ACCESS' on Dec 11, 2024, due by Dec 16, 2024. A red box highlights the 'Pending' tab, and another red box highlights the 'Review' button. A red arrow points from the 'Review' button to a side panel titled 'Access request'. The side panel shows details: Access to AP01-01-VENDOR-A-FULL-ACCESS, Requested by Diego Siciliani, Requested for Diego Siciliani, and a due date of Dec 16, 2024, 11:02 AM AEDT. It also has links for 'Request details', 'Package details', and 'Approval history'. At the bottom, there are radio buttons for 'Approve' and 'Deny', a 'Provide reason' field, and 'Submit' and 'Cancel' buttons.

The screenshot shows the 'AP01-01-VENDOR-A-FULL-ACCESS | Requests' page. The page has a left sidebar with navigation options: Overview, Manage, Resource roles, Policies, Separation of Duties, Assignments, Requests, and Access reviews. The main area shows a table of requests. A red box highlights the 'First stage approved' sub-status in the table. The table has columns: Name, Policy, Status, Sub-status, and Request time. The row for Diego Siciliani shows a status of 'Pending approval' and a sub-status of 'First stage approved'.

The screenshot shows the 'Approvals' page with the 'Approval history' side panel open. The side panel shows a list of approvals. A red box highlights the 'Not reviewed' status in the history. The history shows that Alex Wilber approved the request as the first of two approvers on Dec 11, 2024, 11:12 AM AEDT. The second approver is 'Not reviewed' as of Dec 16, 2024, 11:12 AM AEDT.

## AP01-01-VENDOR-A-FULL-ACCESS | Requests

Overview

Manage

Search by user name

Status: 9 selected

Policy: Vendor A Policy 1

Request type: 6 selected

Name	Policy	Status	Sub-status	Request time
Diego Siciliani	Vendor A Policy 1	Delivering	Delivering	12/11/2024, 11:02:32 AM

## AP01-01-VENDOR-A-FULL-ACCESS | Requests

Overview

Manage

Search by user name

Status: 9 selected

Policy: Vendor A Policy 1

Request type: 6 selected

Name	Policy	Status	Sub-status	Request time
Diego Siciliani	Vendor A Policy 1	Delivered	Delivered	12/11/2024, 11:02:32 AM

External Guest user was automatically created in target tenant.

Search

+ New user Delete Download users Bulk operations Refresh Manage view

All users

Azure Active Directory is now Microsoft Entra ID.

Search: diego

1 user found

Display name	User principal name	User type	On-premises sy...
Diego Siciliani	DiegoS_365cloud.com.au...	Guest	No

External Guest user was automatically added to the Security Group "SG-EXT-Vendor-A". This has happened without administrative intervention.

## Diego Siciliani | Groups

Search

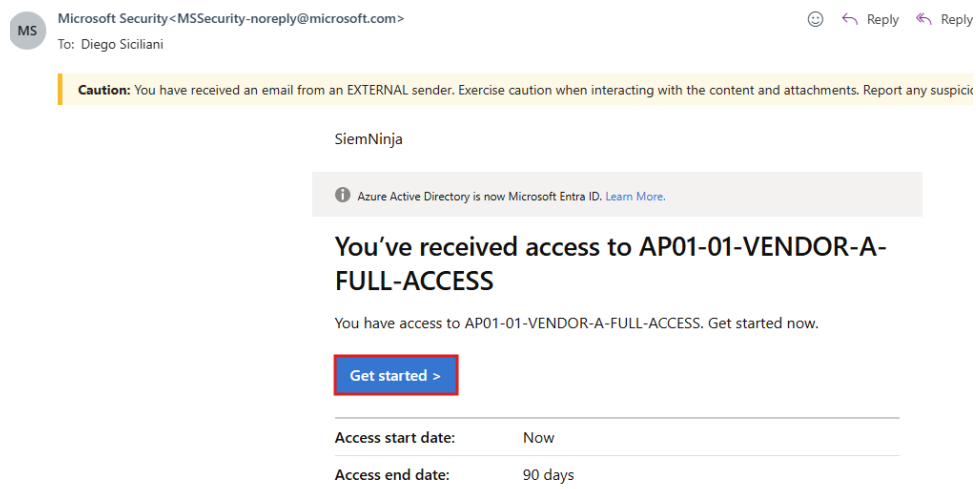
+ Add memberships Remove memberships Refresh Columns Got feedback?

Overview

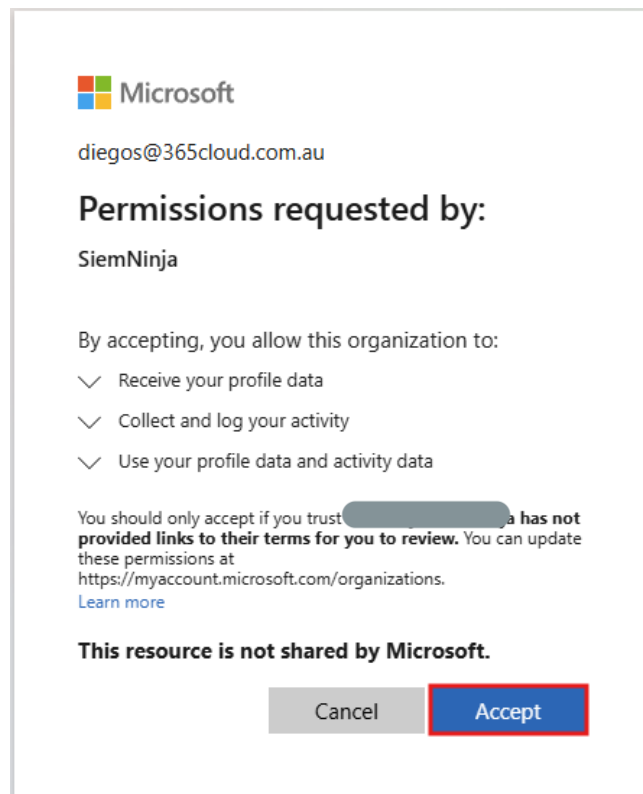
Search groups

Name	Object Id	Group Type	Membership Type	Email	Source
SG-EXT-Vendor-A	f3326405-7c7f-40c8-b6ec-ce178...	Security	Assigned		Cloud

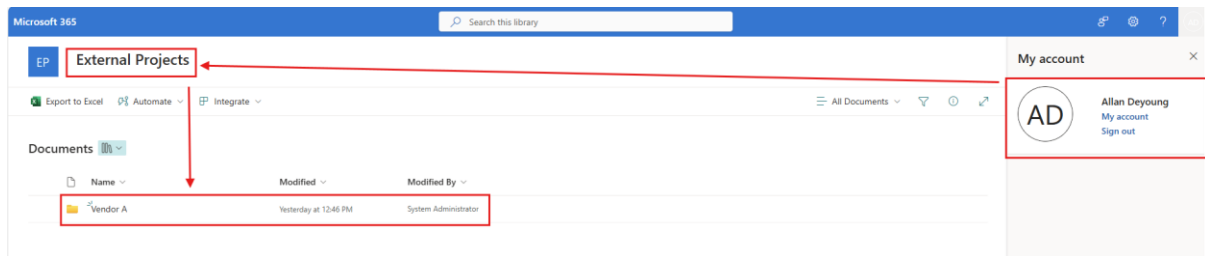
## External user receives email confirming Access Package delivery.



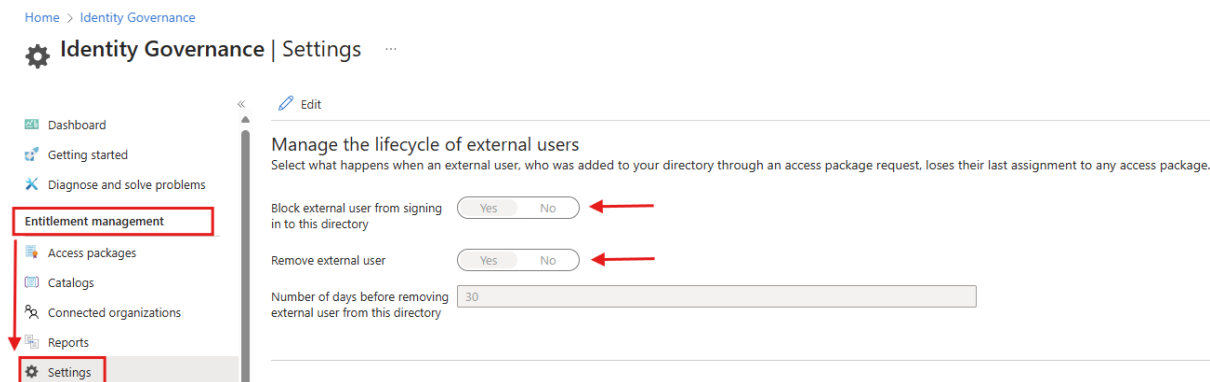
Once the external user accepts the permissions requested by the source tenant, access to resources will be permitted.



**Note:** Ensure that external users also receive direct links to the shared resources (e.g., SharePoint folders). This can be done e.g., through the Access Package via Description details, Teams or Email.



**Pro-tip:** Manage the lifecycle and automated offboarding of external users by defining what occurs when an external user added via an access package request no longer has any active assignments.



## Microsoft Documentation Links

For further details and step-by-step guidance, refer to the official Microsoft documentation:

### Entitlement Management Overview

<https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-overview>

### Set Up Connected Organizations:

<https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-organization>

### Create and Manage Access Packages

<https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-access-package-create>

### Configure Cross-Tenant Access Settings

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/cross-tenant-access-overview>

### Request Access Through Access Packages

<https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-request-access>

### External Sharing in SharePoint

<https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off>