

How to Set Up GDAP for Resellers

A Practical Guide for Resellers to Connect to Customer Microsoft Tenancies Using Granular Delegated Admin Privileges (GDAP)

Introduction

Granular Delegated Admin Privileges (GDAP) is a Microsoft security feature that enables resellers (MSPs/IT Providers) to obtain controlled, secure, and specific access to their customers' Microsoft Tenancies. Setting up GDAP allows you to assist customers with support, troubleshooting, and administrative tasks while maintaining a high level of security.

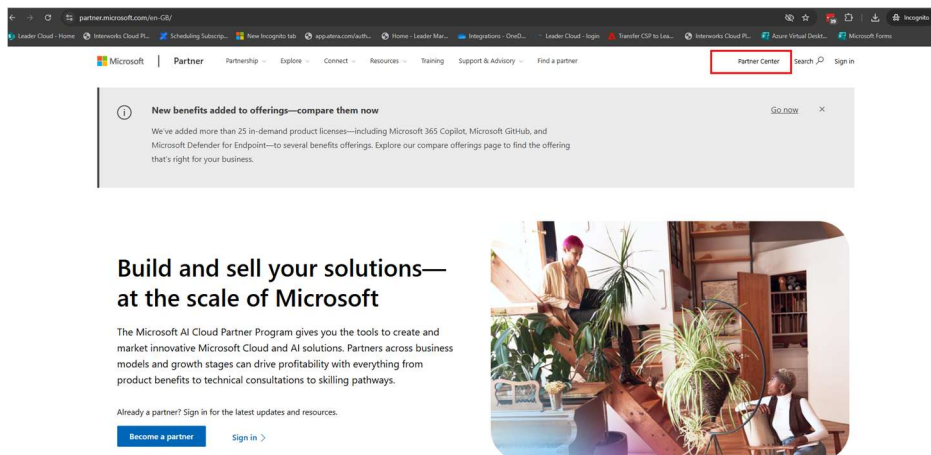
What is GDAP?

GDAP stands for Granular Delegated Admin Privileges. It provides more precise admin access to Microsoft Tenancies, differentiating between various roles and permission levels. GDAP does not impact licensing or procurement and does not cause downtime if inactive or expired.

How to Set Up GDAP as a Reseller

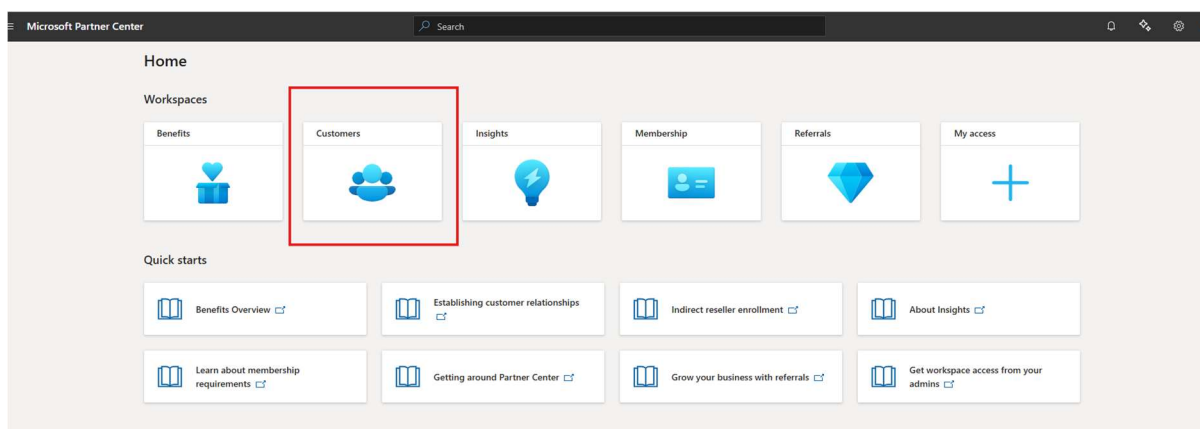
Step 1: Log in to Your Microsoft Partner Centre.

Ensure you have the necessary administrative credentials to manage customer relationships.

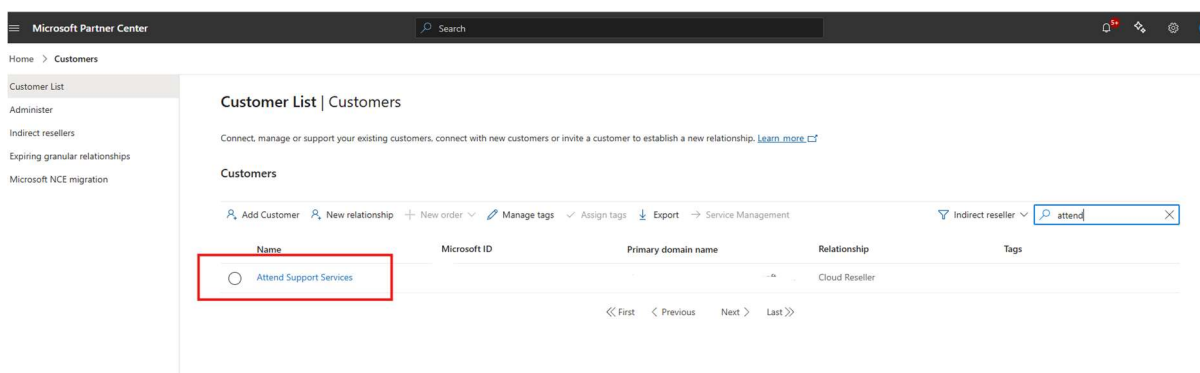


Step 2: Select the Customer

- In your Microsoft Reseller Tenancy portal, navigate to the Customers section.

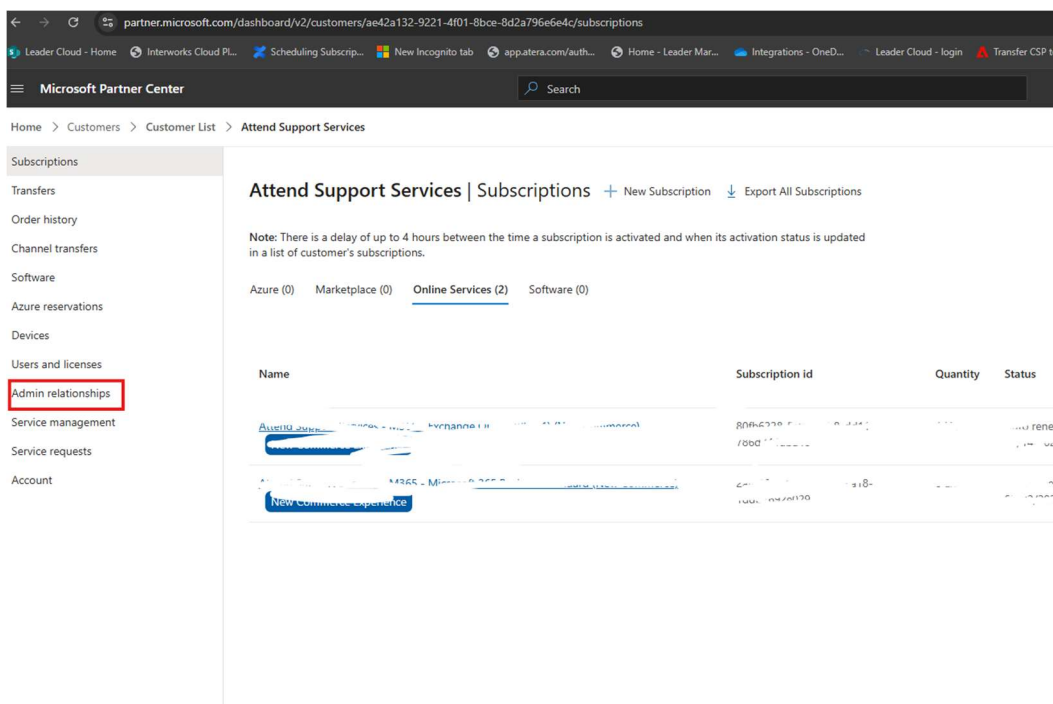


- Choose the customer tenancy you wish to connect to using GDAP.




Step 3: Request a New Admin Relationship

- On the left-hand menu, select Admin Relationship.





- Click Request for new relationship.

 Please enable Auto Extend using [Partner Center UI](#) or [API](#) for needed MLT GDAPs nearing their ex

Attend Support Services | Admin Relationships

Below is a list of admin relationships with the customer that are currently active, pending,

 [Request for new relationship](#)

 Terminate relationship

Admin relationship name	Status
-------------------------	--------

Step 4: Enter Required Information

- Admin Relationship Name: Use the format Reseller Name (replace with the customer's company name).
- Duration: Enter 730 days (or less, if preferred).

Email us today at help@leadercloud.com.au

- Entra ID Roles: Select the following roles (adapt as necessary for your needs):
 - **Header: Identity**
 - Helpdesk Administrator
 - License Administrator
 - Privileged Authentication Administrator
 - Privileged Role Administrator
 - User Administrator
 - Application Administrator
 - Cloud Application Administrator
 - External Identity Provider Administrator
 - **Header: Other**
 - Service Support Administrator
 - Directory Writers
 - Domain Name Administrator
 - **Header: Read Only**
 - Directory Readers
 - Global Reader

Customers > Granular Administration > Create an admin relationship request

ns

ry

nsfers

ations

censes

ionships

agement

ests

Attend Support Services | Create an admin relationship request

To request an admin relationship with a customer, fill out the form below, copy and paste the following text, including the URL, into an email. Edit the text if necessary and send the email to your customer. Your customer will be able to see the Admin relationship name in the M365 Admin Center. Please note this will not establish a Reseller relationship. Go to the [Customer List](#) page to request a [Reseller relationship](#).

Admin relationship name *
The admin relationship name is visible to customers.

Duration in days *

Requested Microsoft Entra roles *
Identify the Microsoft Entra roles you want to assume for your customer.

[Select Microsoft Entra roles](#)

No Microsoft Entra roles selected

Auto Extend

☐ Yes

☒ No

Step 5: Finalize the Request

- Once all required fields are filled in and roles selected, click Finalize Request.

Admin relationship name *

The admin relationship name is visible to customers.

✓ Reseller Name_Attend Sup

Duration in days *

Requested Microsoft Entra roles *

Identify the Microsoft Entra roles you want to assume for your customer.

[Select Microsoft Entra roles](#)

Cloud application administrator
Directory readers
Directory writers
Domain name administrator
External identity provider administrator
Global reader
Helpdesk administrator
License administrator
Privileged authentication administrator
Privileged role administrator
[Show more \(2\)](#)

Auto Extend

☒ Yes
☐ No

Auto Extend by 6 Months

- A connection URL will be generated for the GDAP relationship.

Request

By clicking the included link you will be able to accept the request for us to administer your products using the roles listed below for the specified date range.
This admin relationship would be auto extended by 6 months. You could modify in Microsoft admin center.

Click to review and accept:
<https://admin.microsoft.com/AdminPortal/Home#/partners/invitation/granularAdminRelationships/ca65d65c-5ecb-458f-a052-634a860cfa7e-efdefed5-708b-45fa-9f9a-fb3dd540bff3>

Duration in days:
730


Requested Microsoft Entra roles:

Helpdesk administrator
Can reset passwords for non-administrators and Helpdesk administrators.




License administrator
Ability to assign, remove and update license assignments.

Privileged authentication administrator
Allowed to view, set and reset authentication method information for any user (admin or non-admin).

[Open in email](#)
[Copy to clipboard](#)



Select Microsoft Entra roles

Select from approved Microsoft Entra roles to assign to the following security groups, and click "Save". [Learn more about Microsoft Entra roles.](#)

- HelpdeskAgents

<input checked="" type="checkbox"/>	Microsoft Entra roles	Description
<input checked="" type="checkbox"/>	Application administrator	Can create and manage all aspects of app registrations and enterprise apps.
<input checked="" type="checkbox"/>	Cloud application administrator	Can create and manage all aspects of app registrations and enterprise apps except App Proxy.
<input checked="" type="checkbox"/>	Directory readers	Can read basic directory information. Commonly used to grant directory read access to applications and guests.
<input checked="" type="checkbox"/>	Directory writers	Can read and write basic directory information. For granting access to applications, not intended for users.
<input checked="" type="checkbox"/>	Global reader	Can read everything that a global administrator can, but not update anything.
<input checked="" type="checkbox"/>	Helpdesk administrator	Can reset passwords for non-administrators and Helpdesk administrators.
<input checked="" type="checkbox"/>	License administrator	Ability to assign, remove and update license assignments.
<input checked="" type="checkbox"/>	Privileged authentication administrator	Allowed to view, set and reset authentication method information for any user (admin or non-admin).
<input checked="" type="checkbox"/>	Privileged role administrator	Can manage role assignments in Microsoft Entra ID, and all aspects of Privileged Identity Management.

Save

Cancel

Click Save and give it 5 minutes to sync. Then you are ready to go 😊