Granular Delegated Admin Privileges (GDAP) in Cloud Solution Provider (CSP)

Value and vision

Vision

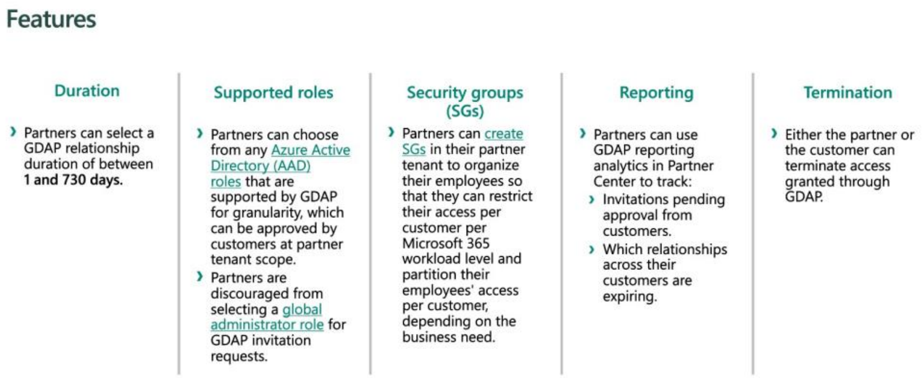
Cybersecurity continues to be one of the top challenges of our digital age. Creating a secure ecosystem requires the adoption of a holistic security approach that includes a **zero trust** mindset, cloud-first posture, and the investment in people and skills. Zero trust follows the principles of verify explicitly, use least privileged access, and assume breach. Organizations who operate under these principles are more resilient, consistent, and responsive to new attacks. With our partners, we're taking steps aligned to these principles to secure the channel.

Protecting access to customer data is a critical part of securing the ecosystem and partners should take action to employ tools for the principle of least privileged access.

Granular Delegated Admin Privileges (GDAP)

With the new GDAP capability, partners can control more granular and time-bound access to their customers' workloads. This means that partners can better address security concerns from their customers. Partners can also provide more services to customers who are uncomfortable with the current levels of partner access and who have regulatory requirements to **provide only least privileged access to partners.**

Features



Features

Duration

- Partners can select a GDAP relationship duration of between **1 and 730 days.**

Supported roles

- Partners can choose from any Azure Active Directory (AAD) roles that are supported by GDAP for granularity, which can be approved by customers at partner tenant scope.
- Partners are discouraged from selecting a global administrator role for GDAP invitation requests.

Security groups (SGs)

- Partners can create SGs in their partner tenant to organize their employees so that they can restrict their access per customer per Microsoft 365 workload level and partition their employees' access per customer, depending on the business need.

Reporting

- Partners can use GDAP reporting analytics in Partner Center to track:
  - Invitations pending approval from customers.
  - Which relationships across their customers are expiring.

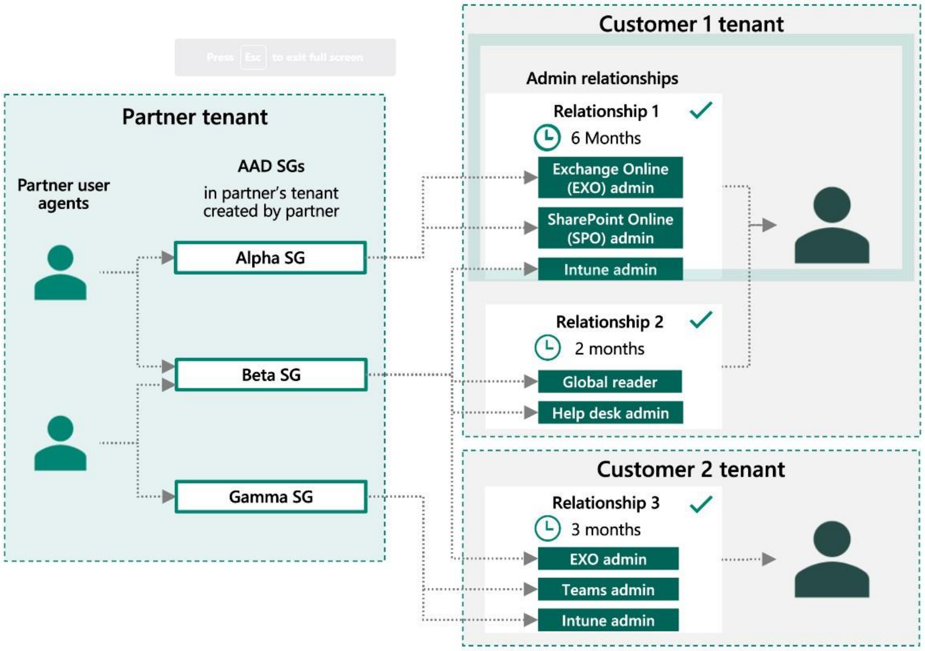
Termination

- Either the partner or the customer can terminate access granted through GDAP.

How GDAP works

GDAP provides restriction of access at the customer, partner tenant, partner user, and workload levels.

Partner user agents are assigned to SGs. Each SG is given access to customer workloads for a fixed duration of time. The access expires automatically at the end of the duration.

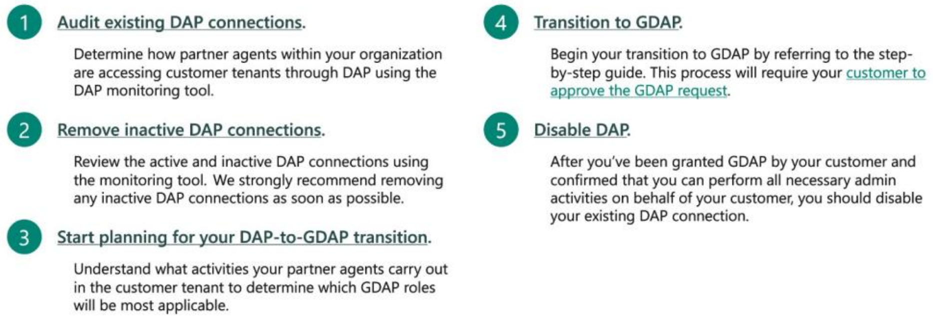


Considerations for transitioning from DAP to GDAP

- While DAP and GDAP will coexist during the transition period, GDAP will eventually replace DAP. This is to ensure that we provide a more secure solution for our partners and customers. We advise transitioning your customers to GDAP as soon as possible to ensure continuity.
- There are no changes to the existing DAP relationship flow while DAP and GDAP coexist.
- Partner earned credit (PEC) earnings won't be affected when you transition to GDAP. There will be no changes to the partner admin link (PAL) with the transition, ensuring that you continue to earn PEC. Disabling DAP will not remove PAL.
- GDAP permissions will take precedence over DAP permissions:
- The precedence for GDAP permissions over DAP permissions works at the partner tenant, customer tenant, and workload levels. For example, if a partner user signs in for a given workload and there's DAP for the global admin role and GDAP for the global reader role, the partner user will get the global reader permissions only.
- Transitioning a large customer base from DAP to GDAP:
- This can be carried out by APIs starting in late February. This will require customer consent.
- Microsoft have build a bulk transition tool for partners that will help them transition all their customers from DAP to GDAP without requiring customers' consent.
- GDAP will be required to turn on Microsoft 365 Lighthouse in the future.
- The partner user will need to have the right GDAP permissions on the customer's tenant if they want to view that customer in Microsoft 365 Lighthouse.
- If the GDAP relationship expires, that customer will no longer be visible in Microsoft 365 Lighthouse.

For information on how GDAP works for Azure, refer to the **[Granular delegated admin privileges (GDAP) introduction]** in Microsoft Docs.

Transitioning from DAP to GDAP



1 Audit existing DAP connections.

Determine how partner agents within your organization are accessing customer tenants through DAP using the DAP monitoring tool.

2 Remove inactive DAP connections.

Review the active and inactive DAP connections using the monitoring tool. We strongly recommend removing any inactive DAP connections as soon as possible.

3 Start planning for your DAP-to-GDAP transition.

Understand what activities your partner agents carry out in the customer tenant to determine which GDAP roles will be most applicable.

4 Transition to GDAP.

Begin your transition to GDAP by referring to the step-by-step guide. This process will require your customer to approve the GDAP request.

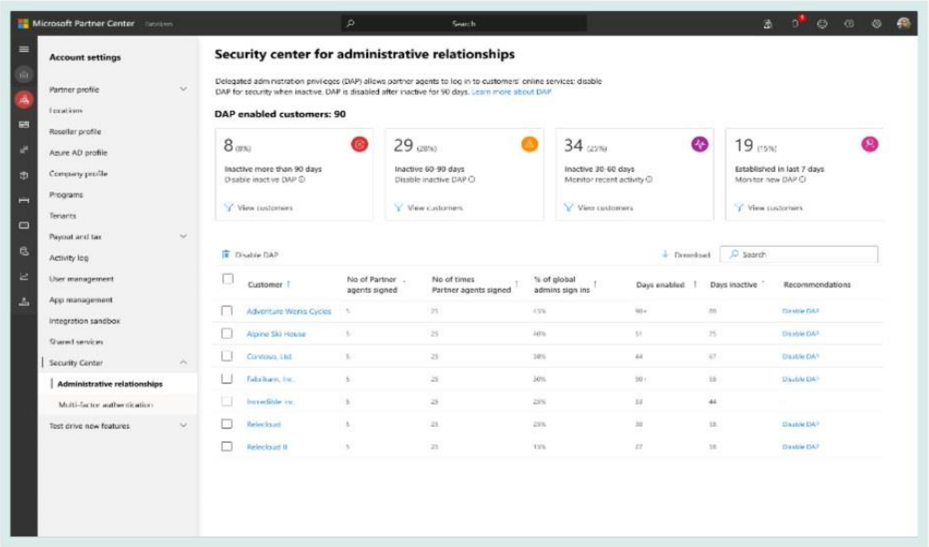
5 Disable DAP.

After you've been granted GDAP by your customer and confirmed that you can perform all necessary admin activities on behalf of your customer, you should disable your existing DAP connection.

- customer to approve the GDAP request.

1. Audit existing DAP connections

DAP monitoring report



Security center for administrative relationships

Delegated administration privileges (DAP) allows partner agents to log in to customers' online services; disable DAP for security when inactive. DAP is disabled after inactive for 90 days. Learn more about DAP

DAP enabled customers: 90

8 (8%)
Inactive more than 90 days
Disable inactive DAP

29 (28%)
Inactive 60-90 days
Disable inactive DAP

34 (25%)
Inactive 30-60 days
Monitor recent activity

19 (15%)
Established in last 7 days
Monitor new DAP

Customer	No of Partner agents signed	No of times Partner agents signed	% of global admins sign ins	Days enabled	Days inactive	Recommendations
Adventure Works Cycles	5	25	15%	90+	80	Disable DAP
Alpine Ski House	5	25	40%	51	75	Disable DAP
Contoso, Ltd.	5	25	38%	44	67	Disable DAP
Fabrikam, Inc.	5	25	30%	90+	55	Disable DAP
Incredible Inc.	5	25	25%	33	44	
Relecloud	5	25	25%	38	55	Disable DAP
Relecloud II	5	25	15%	27	58	Disable DAP

DAP monitoring report

- This report displays all the DAP-enabled customers for the partner.
- This report can be used by direct bill partners, indirect providers, and indirect resellers transacting through the CSP program.
- Partners with the admin agent role can access this reporting.
- Partners can access DAP reporting by going to:

Partner Center > Account settings > Security Center > Administrative relationships

Please note: APIs aren't currently supported for this reporting feature.

We're also offering service providers AAD Premium Plan 2, which provides extended access to sign-in logs and premium features such as AAD Privileged Identity Management (PIM) and risk-based conditional access capabilities for strengthening security controls.

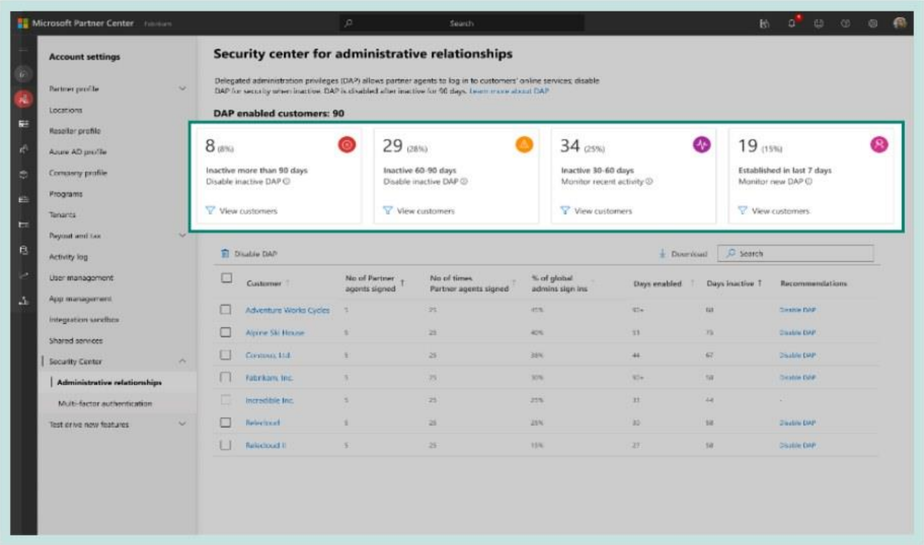
Filter options for managing DAP

- Inactive for more than 90 days: Displays the number of customers whose DAP relationship has been inactive for more than 90 days. Partners will be recommended to remove DAP if inactive for more than 90 days.

- Inactive for 60 to 90 days: Displays the number of customers whose DAP relationship has been inactive between 60 and 90 days. Partners will be recommended to remove DAP if inactive for more than 60 days.

- Inactive for 30 to 60 days: Displays the number of customers whose DAP relationship has been inactive between 30 and 60 days.

- Established in the last seven days: Displays the number of customers whose DAP relationship was established in the last seven days.



Security center for administrative relationships

Delegated administration privileges (DAP) allows partner agents to log in to customers' online services; disable DAP for security when inactive. DAP is disabled after inactive for 90 days. Learn more about DAP

DAP enabled customers: 90

8 (8%)	29 (28%)	34 (25%)	19 (15%)
Inactive more than 90 days Disable inactive DAP	Inactive 60-90 days Disable inactive DAP	Inactive 30-60 days Monitor recent activity	Established in last 7 days Monitor new DAP
View customers	View customers	View customers	View customers

□	Customer	No of Partner agents signed	No of times Partner agents signed	% of global admins sign ins	Days enabled	Days inactive	Recommendations
□	Adventure Works Cycles	5	25	45%	90+	68	Disable DAP
□	Alpine Ski House	5	23	40%	53	75	Disable DAP
□	Contoso Ltd.	5	25	38%	44	67	Disable DAP
□	Fabrikam Inc.	5	25	30%	90+	58	Disable DAP
□	Incredible Inc.	5	25	25%	33	44	-
□	Relecloud	5	28	25%	32	58	Disable DAP
□	Relecloud II	5	25	15%	27	58	Disable DAP

Note: Active DAP connection is defined as connections where partners are accessing the customer's tenant through the Partner Center portal and administer on behalf of (AOBO) or when partners use APIs to connect to the customer's tenant by exchange of tokens.

Field details

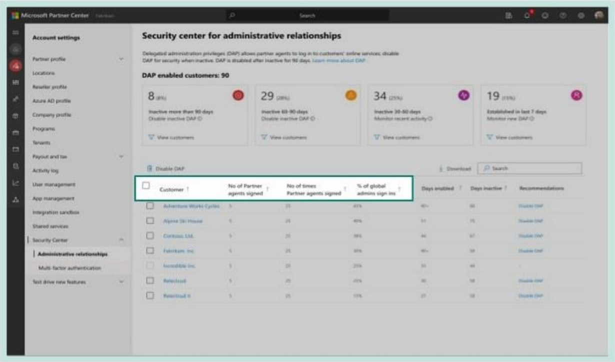
This report provides details about each customer's DAP connection and the activity associated with it. It includes:

- Customer name

- Number of partner agents signed in: The number of unique partner agents who have signed in to the customer tenant in the last 30 days.

- Number of times partner agents signed in: The number of times the partner agents signed in to the customer tenant in the last 30 days.

- Percentage of global admin sign ins: The percentage of times the partner agent signed in to the customer tenant as a global admin.



Security center for administrative relationships

Delegated administration privileges (DAP) allows partner agents to log in to customers' online services; disable DAP for security when inactive. DAP is disabled after inactive for 90 days. Learn more about DAP

DAP enabled customers: 90

8 (8%) Inactive more than 90 days · Disable inactive DAP · View customers

29 (28%) Inactive 60-90 days · Disable inactive DAP · View customers

34 (25%) Inactive 30-60 days · Monitor recent activity · View customers

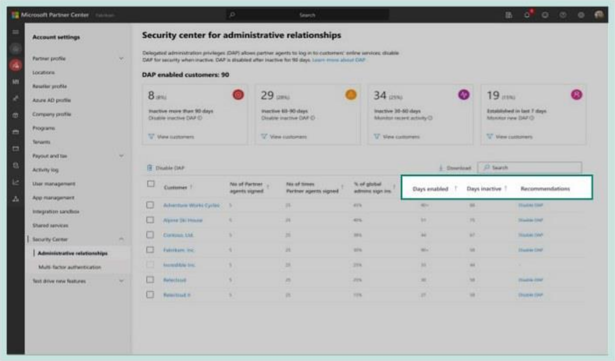
19 (15%) Established in last 7 days · Monitor new DAP · View customers

Disable DAP · Download · Search

□	Customer	No of Partner agents signed	No of times Partner agents signed	% of global admins sign ins	Days enabled	Days inactive	Recommendations
□	Adventure Works Cycles	5	25	45%	90+	88	Disable DAP
□	Alpine Ski House	5	25	40%	51	75	Disable DAP
□	Contoso, Ltd.	5	25	38%	44	67	Disable DAP
□	Fabrikam, Inc	5	25	30%	90+	58	Disable DAP
	Incredible Inc.	5	25	25%	33	44	-
□	Relecloud	5	25	23%	30	58	Disable DAP
□	Relecloud II	5	25	15%	27	58	Disable DAP

Note that this report took effect from December 7, 2021. However, some partners can see metrics that include data prior to this date.

- Days enabled: The number of days since the DAP or GDAP relationship has been established between the partner and the customer. If it's more than 90 days, it will be displayed as 90+, otherwise you'll see an absolute number.
- Days inactive: The number of days since the DAP or GDAP relationship has been inactive between the partner and the customer. If it's more than 90 days, it will be displayed as 90+, otherwise you'll see an absolute number.
- Recommendation: Recommendation to turn off DAP will be provided if the partner agent has not signed in to any of the customer's workload in the last 60 days.


Security center for administrative relationships

Delegated administration privileges (DAP) allows partner agents to log in to customers' online services; disable DAP for security when inactive. DAP is disabled after inactive for 90 days. Learn more about DAP

DAP enabled customers: 90

8 (8%) Inactive more than 90 days · Disable inactive DAP · View customers

29 (28%) Inactive 60-90 days · Disable inactive DAP · View customers

34 (25%) Inactive 30-60 days · Monitor recent activity · View customers

19 (15%) Established in last 7 days · Monitor new DAP · View customers

Disable DAP · Download · Search

□	Customer	No of Partner agents signed	No of times Partner agents signed	% of global admins sign ins	Days enabled	Days inactive	Recommendations
□	Adventure Works Cycles	5	25	45%	90+	88	Disable DAP
□	Alpine Ski House	5	25	40%	51	75	Disable DAP
□	Contoso, Ltd.	5	25	38%	44	67	Disable DAP
□	Fabrikam, Inc	5	25	30%	90+	58	Disable DAP
	Incredible Inc.	5	25	25%	33	44	-
□	Relecloud	5	25	23%	30	58	Disable DAP
□	Relecloud II	5	25	15%	27	58	Disable DAP

2. Remove inactive DAP connections

Considerations for turning off DAP access

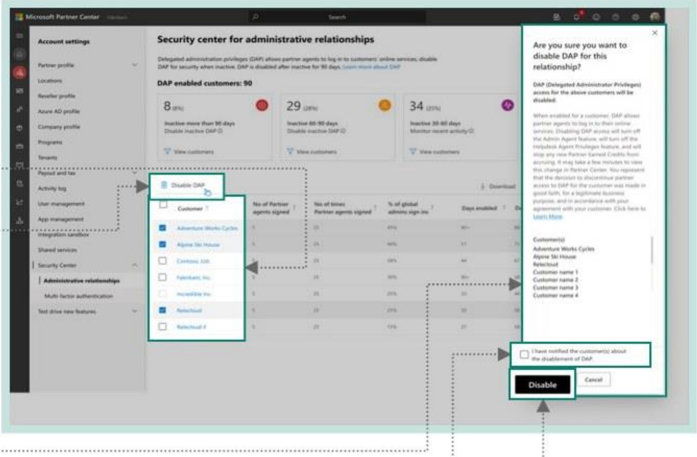
- Ensure that you notify your customer about turning off DAP.
- Partner agents won't have access to the customer's online services.
- Turning off DAP access for a customer will turn off the partner's administrator privilege to manage capabilities on the customer tenant.
- Transacting partners can continue to place orders on behalf of their customers.

- Partner agents can no longer raise a support ticket on behalf of their customers to Microsoft.
- It can take a few minutes for the changes to reflect in Partner Center.
- Turning off DAP won’t affect current role-based access control roles on a subscription, so it won’t affect PECs.

DAP removal

Partners have the option to remove DAP access if admin privileges are no longer required for a customer. Follow these steps to remove DAP access:

1. Select the customer for whom you would like to turn off the DAP relationship.
2. Select Disable DAP on the upper-right corner of the report.
3. A prompt will appear, asking you to confirm if you’d like to turn off DAP.
4. Check the box confirming that you’ve notified the customer(s) about turning off DAP.
5. Select the Disable button.



Microsoft Partner Center

Security center for administrative relationships

Delegated administration privileges (DAP) allows partner agents to log in to customers' online services; disable DAP for security when inactive. DAP is disabled after inactive for 90 days. Learn more about DAP

DAP enabled customers: 90

Are you sure you want to disable DAP for this relationship?

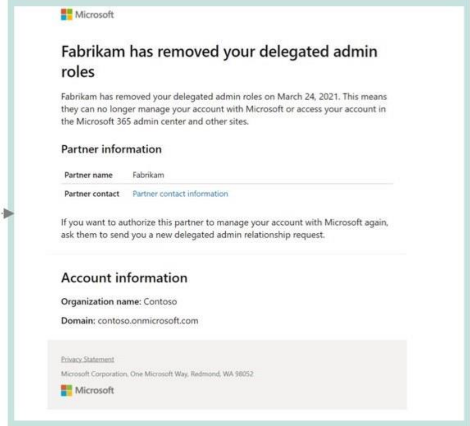
DAP (Delegated Administrator Privileges) access for the above customers will be disabled.

When enabled for a customer, DAP allows partner agents to log in to their online services. Disabling DAP access will turn off the Admin Agent feature, will turn off the Helpdesk Agent Privileges feature, and will stop any new Partner Earned Credits from accruing. It may take a few minutes to view this change in Partner Center. You represent that the decision to discontinue partner access to DAP for the customer was made in good faith, for a legitimate business purpose, and in accordance with your agreement with your customer. Click here to Learn More

Customer(s)
Adventure Works Cycles
Alpine Ski House
Relecloud
Customer name 1
Customer name 2
Customer name 3
Customer name 4

□ I have notified the customer(s) about the disablement of DAP

6. The customer will receive an email notification informing them that the partner has removed the delegated admin role on their account.



Microsoft

Fabrikam has removed your delegated admin roles

Fabrikam has removed your delegated admin roles on March 24, 2021. This means they can no longer manage your account with Microsoft or access your account in the Microsoft 365 admin center and other sites.

Partner information

Partner name	Fabrikam
Partner contact	Partner contact information

If you want to authorize this partner to manage your account with Microsoft again, ask them to send you a new delegated admin relationship request.

Account information

Organization name: Contoso

Domain: contoso.onmicrosoft.com

Privacy Statement

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

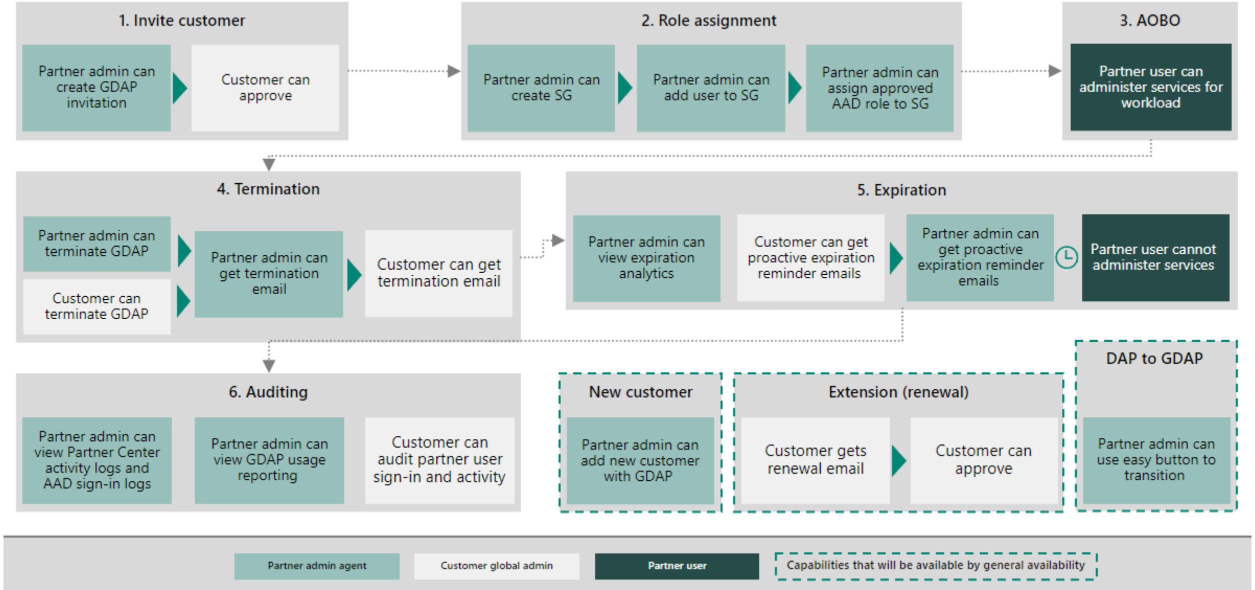
Microsoft

3. Start planning for your DAP-to-GDAP transition

Prepare for your transition

- Understand what activities your partner agents carry out in the customer tenant.
- We recommend granting your partner agents the least privileged roles based on the tasks that they carry out.
- Refer to the guidance to help you determine which GDAP roles will be the most applicable.

Transition to GDAP



1. Invite customer

Partner admin can create GDAP invitation

Customer can approve

2. Role assignment

Partner admin can create SG

Partner admin can add user to SG

Partner admin can assign approved AAD role to SG

3. AOBO

Partner user can administer services for workload

4. Termination

Partner admin can terminate GDAP

Customer can terminate GDAP

Partner admin can get termination email

Customer can get termination email

5. Expiration

Partner admin can view expiration analytics

Customer can get proactive expiration reminder emails

Partner admin can get proactive expiration reminder emails

Partner user cannot administer services

6. Auditing

Partner admin can view Partner Center activity logs and AAD sign-in logs

Partner admin can view GDAP usage reporting

Customer can audit partner user sign-in and activity

New customer

Partner admin can add new customer with GDAP

Extension (renewal)

Customer gets renewal email

Customer can approve

DAP to GDAP

Partner admin can use easy button to transition

Partner admin agent

Customer global admin

Partner user

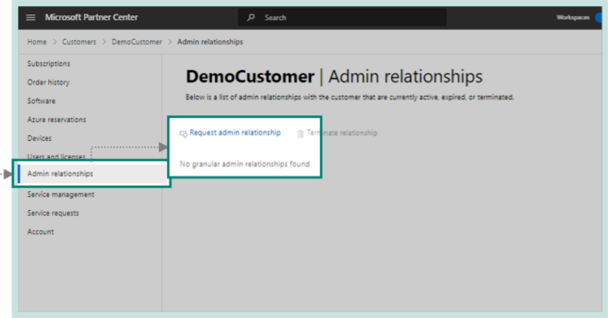
Capabilities that will be available by general availability

Inviting the customer

Create admin relationship invitation request

1 Only the partner admin agent within the partner organization can raise a GDAP invitation request.
From the Partner Center menu, select Customers, and on the Customers page, select a customer.

2 For that customer, select Admin relationships, and then select Request admin relationship.



DemoCustomer | Admin relationships

Below is a list of admin relationships with the customer that are currently active, expired, or terminated.

No granular admin relationships found

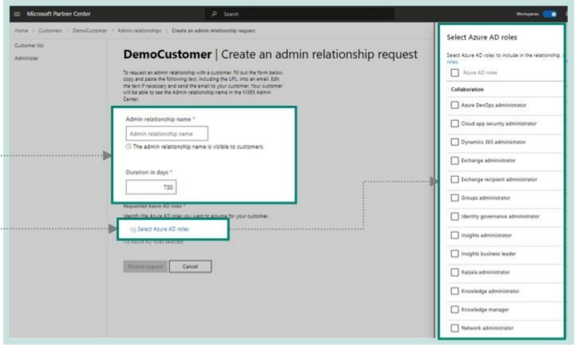
Create admin relationship invitation request

3 On the next page, enter the appropriate details in the Admin relationship name and Duration in days fields.

4 Select Azure AD roles, which opens a side panel with a list of granular AAD roles.
Review which least privileged AAD built-in role can be selected here.

The **admin relationship name** must be unique and visible to the customers in the Microsoft 365 Admin Center.

Duration in days is the time after which the granular admin relationship will automatically expire. After expiration, you will no longer have admin access to manage customer services. The maximum duration is 730 days.



DemoCustomer | 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.

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

Duration in days *
730

Requested Azure AD roles *
Identify the Azure AD roles you want to assume for your customer.
No Azure AD roles selected

Select Azure AD roles

Select Azure AD roles to include in the relationship.

□ Azure AD roles

Collaboration

□ Azure DevOps administrator
□ Cloud app security administrator
□ Dynamics 365 administrator
□ Exchange administrator
□ Exchange recipient administrator
□ Groups administrator
□ Identity governance administrator
□ Insights administrator
□ Insights business leader
□ Kaizala administrator
□ Knowledge administrator
□ Knowledge manager
□ Network administrator

Review which least privileged AAD built-in role can be selected here.

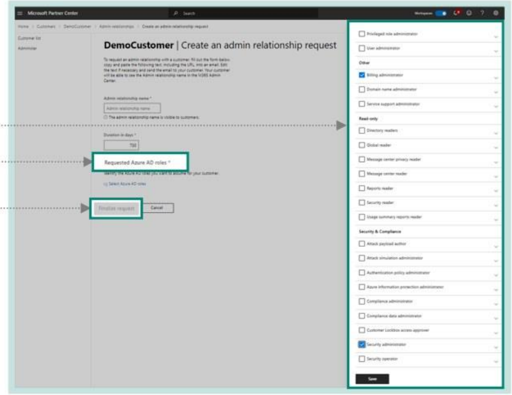
Create admin relationship invitation request

5 Select the roles that you want to request access to, and select Save.

6 All selected AAD roles will appear under the Requested Azure AD roles section.

You can repeat these steps multiple times for addition or deletion of selected roles.

7 To confirm, select Finalize request, which will initiate an email that will go to your customer, requesting the admin access.



Microsoft Partner Center
Search
Workspaces
Home > Customers > DemoCustomer > Admin relationships > Create an admin relationship request
Customer list
Administer

DemoCustomer | 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.

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

Duration in days *
730

Requested Azure AD roles *
Identify the Azure AD roles you want to assume for your customer.
Select Azure AD roles

- □ Privileged role administrator
- □ User administrator

Other
- ☑ Billing administrator
- □ Domain name administrator
- □ Service support administrator

Read-only
- □ Directory readers
- □ Global reader
- □ Message center privacy reader
- □ Message center reader
- □ Reports reader
- □ Security reader
- □ Usage summary reports reader

Security & Compliance
- □ Attack payload author
- □ Attack simulation administrator
- □ Authentication policy administrator
- □ Azure information protection administrator
- □ Compliance administrator
- □ Compliance data administrator
- □ Customer Lockbox access approver
- ☑ Security administrator
- □ Security operator

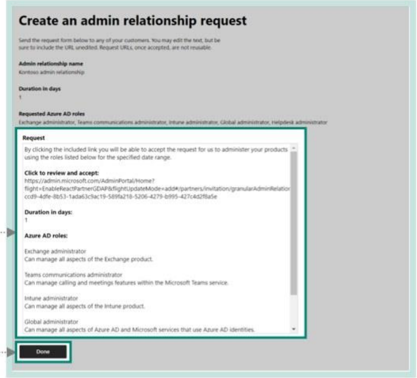
Create admin relationship invitation request

8 Review the draft email message. You can open the draft message in your default email application, or you can copy the message that has the GDAP invitation link to your clipboard and paste it into an email for your customer.

9 Send the email to your customer.

10 Select Done when you've reviewed the email and sent it to your customer.

You can edit the text in the email, but be sure **not to edit the GDAP invitation link** because it's personalized to link the customer directly to your account.



Create an admin relationship request

Send the request form below to any of your customers. You may edit the text, but be sure to include the URL unedited. Request URLs, once accepted, are not reusable.

Admin relationship name
Kontoso admin relationship

Duration in days
1

Requested Azure AD roles
Exchange administrator, Teams communications administrator, Intune administrator, Global administrator, Helpdesk administrator

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.

Click to review and accept:
https://admin.microsoft.com/AdminPortal/Home?flight=EnableReactPartnerGDAP&flightUpdateMode=add#/partners/invitation/granularAdminRelation
ccd9-4dfe-8b53-1ada63c9ac19-589fa218-5206-4279-b995-427c4d2f8a5e

Duration in days:
1

Azure AD roles:

Exchange administrator
Can manage all aspects of the Exchange product.

Teams communications administrator
Can manage calling and meetings features within the Microsoft Teams service.

Intune administrator
Can manage all aspects of the Intune product.

Global administrator
Can manage all aspects of Azure AD and Microsoft services that use Azure AD identities.

Approve admin relationship invitation request

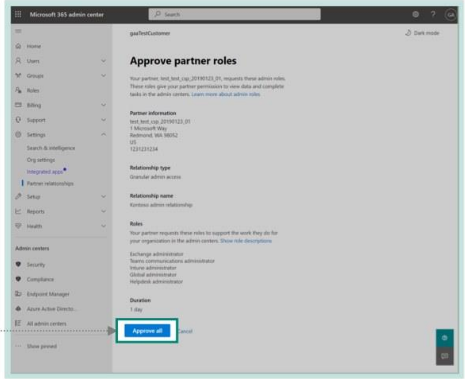
Your customer can approve your GDAP request.

1 The customer will need to select the GDAP invitation link.

2 On the Approve partner roles page, the customer will select Approve all.

3 Both you and the customer will get a confirmation email notification after approval.

Only the global admin on the customer's tenant can approve the GDAP request.



gaaTestCustomer

Approve partner roles

Your partner, test_test_csp_20190123_01, requests these admin roles. These roles give your partner permission to view data and complete tasks in the admin centers. Learn more about admin roles

Partner information
test_test_csp_20190123_01
1 Microsoft Way
Redmond, WA 98052
US
1231231234

Relationship type
Granular admin access

Relationship name
Kontoso admin relationship

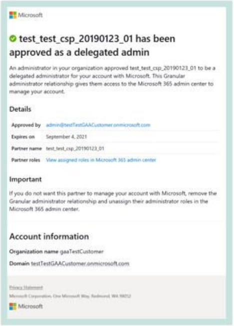
Roles
Your partner requests these roles to support the work they do for your organization in the admin centers. Show role descriptions

Exchange administrator
Teams communications administrator
Intune administrator
Global administrator
Helpdesk administrator

Duration
1 day

Email confirmation sent to customer

Subject: You have a granular administrator relationship with *name of customer's organization*



Microsoft

test_test_csp_20190123_01 has been approved as a delegated admin

An administrator in your organization approved test_test_csp_20190123_01 to be a delegated administrator for your account with Microsoft. This Granular administrator relationship gives them access to the Microsoft 365 admin center to manage your account.

Details

Approved by	admin@testTestGAACustomer.onmicrosoft.com
Expires on	September 4, 2021
Partner name	test_test_csp_20190123_01
Partner roles	View assigned roles in Microsoft 365 admin center

Important

If you do not want this partner to manage your account with Microsoft, remove the Granular administrator relationship and unassign their administrator roles in the Microsoft 365 admin center.

Account information

Organization name gaaTestCustomer

Domain testTestGAACustomer.onmicrosoft.com

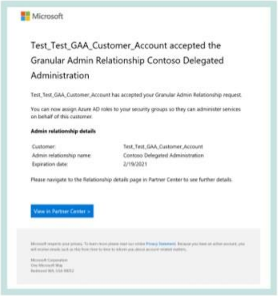
Privacy Statement

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Microsoft

Email notification confirming approval sent to partner

Subject: Your customer has accepted the granular administrator request



Microsoft

Test_Test_GAA_Customer_Account accepted the Granular Admin Relationship Contoso Delegated Administration

Test_Test_GAA_Customer_Account has accepted your Granular Admin Relationship request.

You can now assign Azure AD roles to your security groups so they can administer services on behalf of this customer.

Admin relationship details

Customer:	Test_Test_GAA_Customer_Account
Admin relationship name:	Contoso Delegated Administration
Expiration date:	2/19/2021

Please navigate to the Relationship details page in Partner Center to see further details.

View in Partner Center >

Microsoft respects your privacy. To learn more please read our online Privacy Statement. Because you have an active account, you will receive emails such as this from time to time to inform you about account related matters.

Microsoft Corporation
One Microsoft Way
Redmond WA, USA 98052

The admin agent role within the partner organization will receive this email notification.

Role Assignment

1. The partner can create a security group in the AAD portal.

2. The partner can add a user to an SG in the AAD portal.

3. Assign AAD roles to SG:
   - Select SG.
   - Assign SGs to roles in approved admin relationships.

The partner can create a security group in the AAD portal.

The partner can add a user to an SG in the AAD portal.

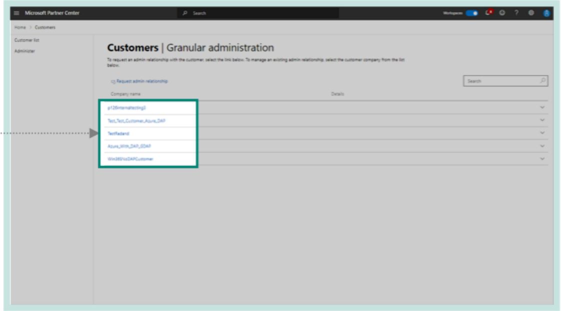
If you prefer to have different partner users managing different customers, then you should assign those partner users to separate security groups for per-customer isolation.

Role assignment works at the customer-to-GDAP relationship level through the Partner Center interface. If you want multicustomer role assignment, you can automate using an API.

View admin relationships

To grant permission to the SGs, complete the following steps:

1 From the Partner Center menu, select Customer, and then select Administer. Select the customer that you want to manage.



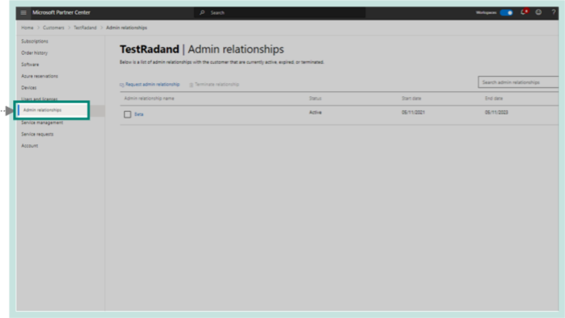
Customers | Granular administration

To request an admin relationship with the customer, select the link below. To manage an existing admin relationship, select the customer company from the list below.

Company name	Details
p126internaltesting3	
Test_Test_Customer_Azure_DAP	
TestRadiend	
Azure_With_DAP_GDAP	
Win365NoDAPCustomer	

Select SG

2 Select Admin relationships, and then select the specific admin relationship that you want to change.



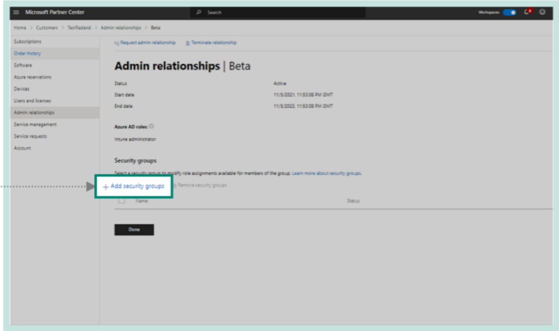
TestRadand | Admin relationships

Below is a list of admin relationships with the customer that are currently active, expired, or terminated.

Admin relationship name	Status	Start date	End date
□ Beta	Active	05/11/2021	05/11/2023

Select SG

3 Under Security groups, select Add security groups.



Admin relationships | Beta

Status Active

Start date 11/5/2021, 11:53:08 PM GMT

End date 11/5/2023, 11:53:08 PM GMT

Azure AD roles:

Intune administrator

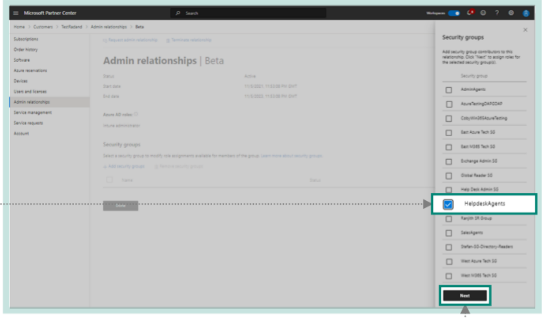
Security groups

Select a security group to modify role assignments available for members of the group. Learn more about security groups.

Select SG

4 On the Security groups panel, select the SG that you want to grant permissions to.

5 Select Next. The SG now appears in the Security groups section.



Security groups

Add security group contributors to this relationship. Click "Next" to assign roles for the selected security group(s).

Security group
- □ AdminAgents
- □ AzureTestingDAPGDAP
- □ CobyWin365AzureTesting
- □ East Azure Tech SG
- □ East M365 Tech SG
- □ Exchange Admin SG
- □ Global Reader SG
- □ Help Desk Admin SG
- ☑ HelpdeskAgents
- □ Ranjith SR Group
- □ SalesAgents
- □ Stefan-SG-Directory-Readers
- □ West Azure Tech SG
- □ West M365 Tech SG

Partners can implement PIM on a GDAP SG on the partner's tenant to elevate the access of a few high-privilege users, just in time (JIT) to grant them high-privilege roles like password admins with automatic removal of access. Microsoft is offering a free AAD premium plan 2 license for this.

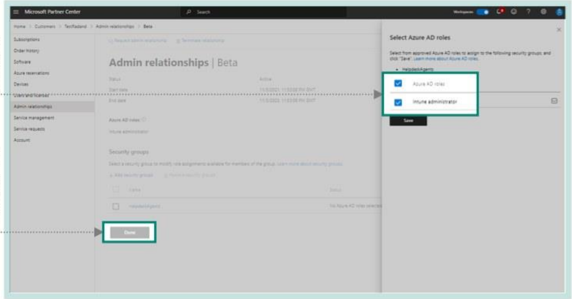
Assign SGs to roles in approved admin relationships

6 On the Select Azure AD roles panel, select the AAD roles that you want to assign to the SG within that admin relationship. With the AAD roles assigned, users in the SG can administer services.

7 Select Save from the panel, and then select Done.

i You can remove or add more SGs and AAD roles.

All the users assigned to the SG can now administer services from the Service management page.



Select Azure AD roles

Select from approved Azure AD roles to assign to the following security groups and click "Save". Learn more about Azure AD roles.

- HelpdeskAgents

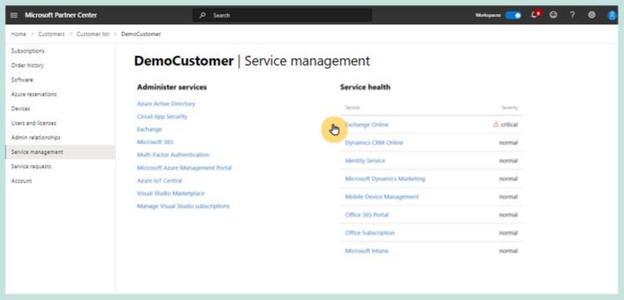
☑ Azure AD roles

☑ Intune administrator

Refer to this article for information needed to restrict a user's administrator permissions by assigning least privileged roles in AAD. We recommend assigning the service support administrator for partner users looking to create support tickets for customers.

AOBO Services

The partner user can administer services for the customer's workload by going to the customer's Service management page.



DemoCustomer | Service management

Administer services

Azure Active Directory
Cloud App Security
Exchange
Microsoft 365
Multi-Factor Authentication
Microsoft Azure Management Portal
Azure IoT Central
Visual Studio Marketplace
Manage Visual Studio subscriptions

Service health

Service	Severity
Exchange Online	⚠ critical
Dynamics CRM Online	normal
Identity Service	normal
Microsoft Dynamics Marketing	normal
Mobile Device Management	normal
Office 365 Portal	normal
Office Subscription	normal
Microsoft Intune	normal

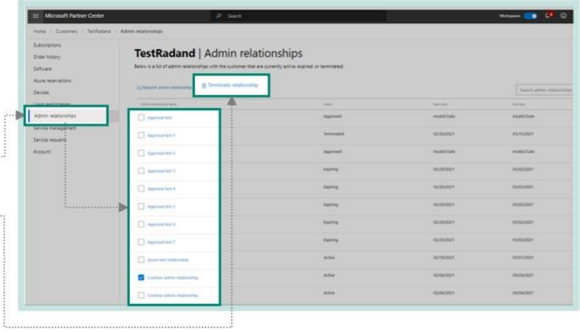
You don't need GDAP to fulfill orders for new and existing customers. You can continue to use the same process to fulfill customer orders in Partner Center.

Termination of GDAP

Terminate an admin relationship (initiated by partner)

To terminate the granular admin relationship with a customer, complete the following steps:

1. From the Partner Center menu, select Administer, and then select the customer whose admin relationship you want to terminate.
2. Select Admin relationships, and then select the admin relationship that you want to terminate.
3. Select Terminate relationship.

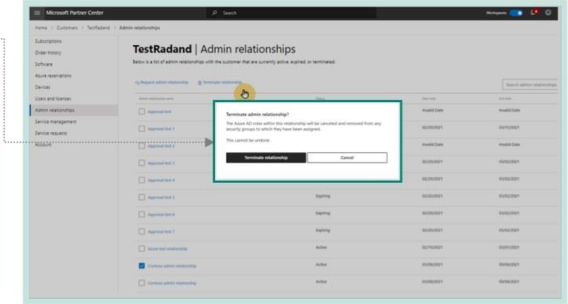


TestRadand | Admin relationships

Below is a list of admin relationships with the customer that are currently active, expired, or terminated.

Terminate an admin relationship (initiated by partner)

4. In the dialog box, confirm that you'd like to terminate the relationship.



TestRadand | Admin relationships

Below is a list of admin relationships with the customer that are currently active, expired, or terminated.

Terminate admin relationship?

The Azure AD roles within this relationship will be canceled and removed from any security groups to which they have been assigned.

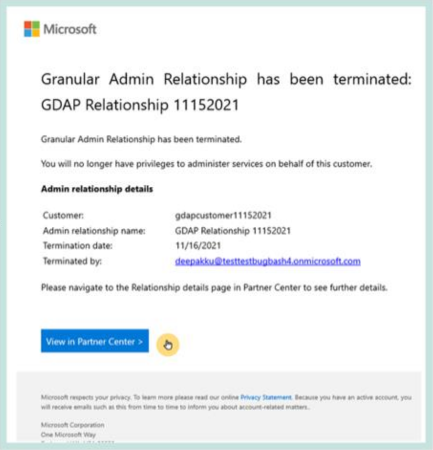
This cannot be undone.

Terminate relationship | Cancel

Users who are members of the SG that was mapped to this relationship will no longer have access to administer services. Both the partner and customer will get termination confirmation email notifications.

Terminate an admin relationship (initiated by partner)

5 The admin agent role within the partner organization will receive a confirmation email stating that the relationship has been terminated.



Microsoft

Granular Admin Relationship has been terminated: GDAP Relationship 11152021

Granular Admin Relationship has been terminated.

You will no longer have privileges to administer services on behalf of this customer.

Admin relationship details

Customer:	gdapcustomer11152021
Admin relationship name:	GDAP Relationship 11152021
Termination date:	11/16/2021
Terminated by:	deepakku@testtestbugbash4.onmicrosoft.com

Please navigate to the Relationship details page in Partner Center to see further details.

Microsoft respects your privacy. To learn more please read our online Privacy Statement. Because you have an active account, you will receive emails such as this from time to time to inform you about account-related matters.

Microsoft Corporation
One Microsoft Way

Terminate an admin relationship (initiated by customer)

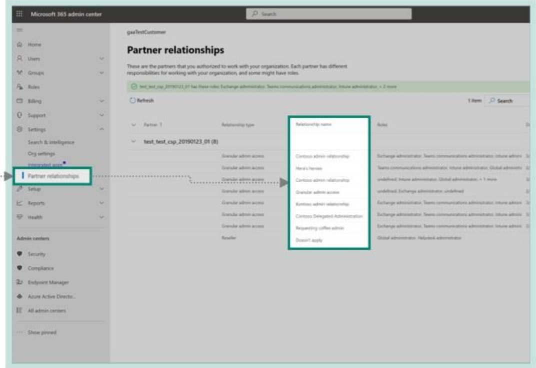
Your customer can decide to remove your GDAP from their tenant. Customers manage rights and permissions to their Microsoft 365 accounts on the Partner relationships page in the Microsoft 365 Admin Center.

On this page, customers can:

- See which partners they have a relationship with and which partners have GDAP.
- Remove a partner's GDAP from the tenant.

To remove DAP from a partner:

1 On the Partner relationships page, select the partner of interest.



gaaTestCustomer

Partner relationships

These are the partners that you authorized to work with your organization. Each partner has different responsibilities for working with your organization, and some might have roles.

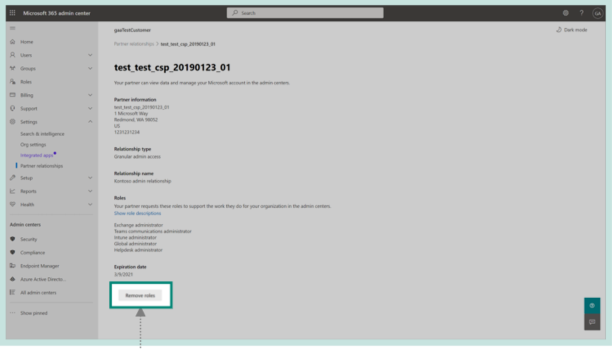
test_test_csp_20190123_01 has these roles: Exchange administrator, Teams communications administrator, Intune administrator, + 2 more

Partner ↑	Relationship type	Relationship name	Roles
test_test_csp_20190123_01 (8)			
	Granular admin access	Contoso admin relationship	Exchange administrator, Teams communications administrator, Intune admini
	Granular admin access	Hera's heroes	Teams communications administrator, Intune administrator, Global administr
	Granular admin access	Contoso admin relationship	undefined, Intune administrator, Global administrator, + 1 more
	Granular admin access	Granular admin access	undefined, Exchange administrator, undefined
	Granular admin access	Kontoso admin relationship	Exchange administrator, Teams communications administrator, Intune admini
	Granular admin access	Contoso Delegated Administration	Exchange administrator, Teams communications administrator, Intune admini
	Granular admin access	Requesting coffee admin	Exchange administrator, Teams communications administrator, Intune admini
	Reseller	Doesn't apply	Global administrator, Helpdesk administrator

Terminate an admin relationship (initiated by customer)

2 On the details pane, select Remove roles.

3 On the confirmation pane, select Yes.



gaaTestCustomer

Partner relationships > test_test_csp_20190123_01

test_test_csp_20190123_01

Your partner can view data and manage your Microsoft account in the admin centers.

Partner information
test_test_csp_20190123_01
1 Microsoft Way
Redmond, WA 98052
US
1231231234

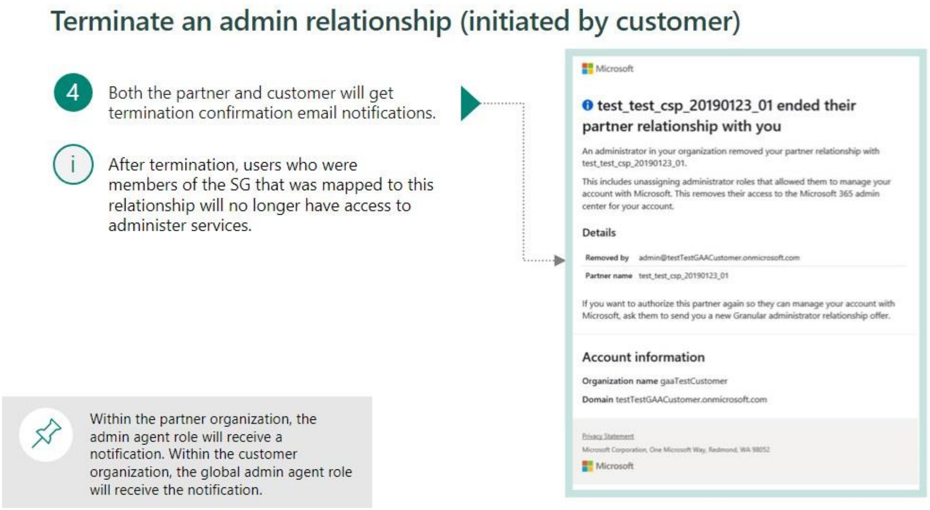
Relationship type
Granular admin access

Relationship name
Kontoso admin relationship

Roles
Your partner requests these roles to support the work they do for your organization in the admin centers.
Show role descriptions

Exchange administrator
Teams communications administrator
Intune administrator
Global administrator
Helpdesk administrator

Expiration date
3/9/2021



Terminate an admin relationship (initiated by customer)

4 Both the partner and customer will get termination confirmation email notifications.

After termination, users who were members of the SG that was mapped to this relationship will no longer have access to administer services.

Within the partner organization, the admin agent role will receive a notification. Within the customer organization, the global admin agent role will receive the notification.

Microsoft

test_test_csp_20190123_01 ended their partner relationship with you

An administrator in your organization removed your partner relationship with test_test_csp_20190123_01.

This includes unassigning administrator roles that allowed them to manage your account with Microsoft. This removes their access to the Microsoft 365 admin center for your account.

Details

Removed by	admin@testTestGAACustomer.onmicrosoft.com
Partner name	test_test_csp_20190123_01

If you want to authorize this partner again so they can manage your account with Microsoft, ask them to send you a new Granular administrator relationship offer.

Account information

Organization name gaaTestCustomer

Domain testTestGAACustomer.onmicrosoft.com

Privacy Statement

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Microsoft

Expiration of GDAP

- The GDAP relationship automatically expires on the set expiration date based on the duration that was requested in the GDAP invitation. The default expiration is set to two years (maximum). Permanent GDAP relationships with customers aren’t possible for security purposes.

- Before expiration, both you and your customer will receive proactive email notifications 30 days, 7 days, and 1 day before the expiration date.

- On the expiration date, an email notification will be sent to both you and your customer, confirming the expiration of your granular admin relationship.

- After expiration, users who were members of the SG assigned to this relationship will no longer have access to administer services. To extend or renew the GDAP relationship, partners will need to resend the GDAP relationship request to the customer.

- There will be no change to the customer’s existing subscriptions if the GDAP relationship expires.

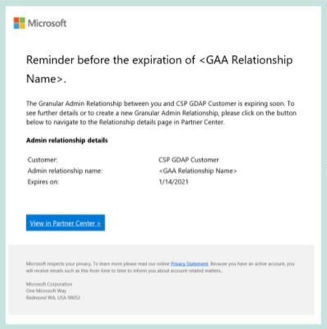
- Autorenewal of GDAP relationships with customers isn’t permitted for security purposes.

- To view expired relationships, select Admin relationships.

- The status column will indicate that the relationship has expired.

Email notification for upcoming expiring relationships

A reminder email notification is sent to the **partner** for upcoming expiring relationships.



Microsoft

Reminder before the expiration of <GAA Relationship Name>.

The Granular Admin Relationship between you and CSP GDAP Customer is expiring soon. To see further details or to create a new Granular Admin Relationship, please click on the button below to navigate to the Relationship details page in Partner Center.

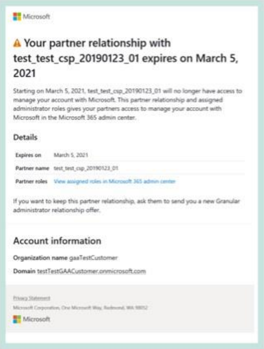
Admin relationship details

Customer:	CSP GDAP Customer
Admin relationship name:	<GAA Relationship Name>
Expires on:	1/14/2021

Microsoft respects your privacy. To learn more please read our online Privacy Statement. Because you have an active account, you will receive emails such as this from time to time to inform you about account related matters.

Microsoft Corporation
One Microsoft Way
Redmond WA, USA 98052

A reminder email notification is also sent to the **customer** for upcoming expiring relationships.



Microsoft

⚠ Your partner relationship with test_test_csp_20190123_01 expires on March 5, 2021

Starting on March 5, 2021, test_test_csp_20190123_01 will no longer have access to manage your account with Microsoft. This partner relationship and assigned administrator roles gives your partners access to manage your account with Microsoft in the Microsoft 365 admin center.

Details

Expires on	March 5, 2021
Partner name	test_test_csp_20190123_01
Partner roles	View assigned roles in Microsoft 365 admin center

If you want to keep this partner relationship, ask them to send you a new Granular administrator relationship offer.

Account information

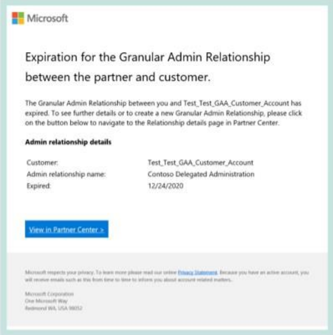
Organization name gaaTestCustomer

Domain testTestGAACustomer.onmicrosoft.com

Privacy Statement
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052
Microsoft

Expired relationship email notification

An expired relationship email notification is sent to the **partner**.



Microsoft

Expiration for the Granular Admin Relationship between the partner and customer.

The Granular Admin Relationship between you and Test_Test_GAA_Customer_Account has expired. To see further details or to create a new Granular Admin Relationship, please click on the button below to navigate to the Relationship details page in Partner Center.

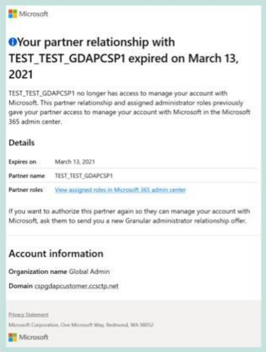
Admin relationship details

Customer:	Test_Test_GAA_Customer_Account
Admin relationship name:	Contoso Delegated Administration
Expired:	12/24/2020

Microsoft respects your privacy. To learn more please read our online Privacy Statement. Because you have an active account, you will receive emails such as this from time to time to inform you about account related matters.

Microsoft Corporation
One Microsoft Way
Redmond WA, USA 98052

An expired relationship email notification is sent to the **customer**.



Microsoft

ℹYour partner relationship with TEST_TEST_GDAPCSP1 expired on March 13, 2021

TEST_TEST_GDAPCSP1 no longer has access to manage your account with Microsoft. This partner relationship and assigned administrator roles previously gave your partner access to manage your account with Microsoft in the Microsoft 365 admin center.

Details

Expires on	March 13, 2021
Partner name	TEST_TEST_GDAPCSP1
Partner roles	View assigned roles in Microsoft 365 admin center

If you want to authorize this partner again so they can manage your account with Microsoft, ask them to send you a new Granular administrator relationship offer.

Account information

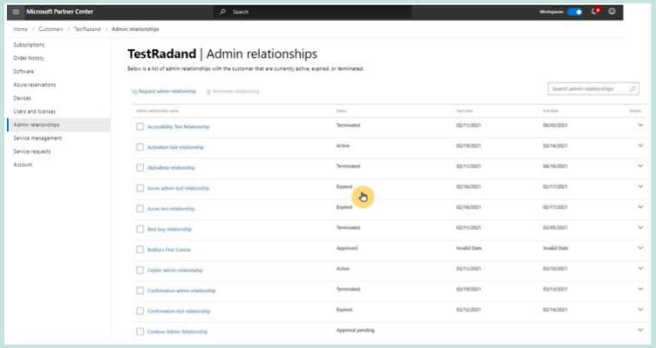
Organization name Global Admin

Domain cspgdapcustomer.ccsctp.net

Privacy Statement
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052
Microsoft

Partner can view expired relationships

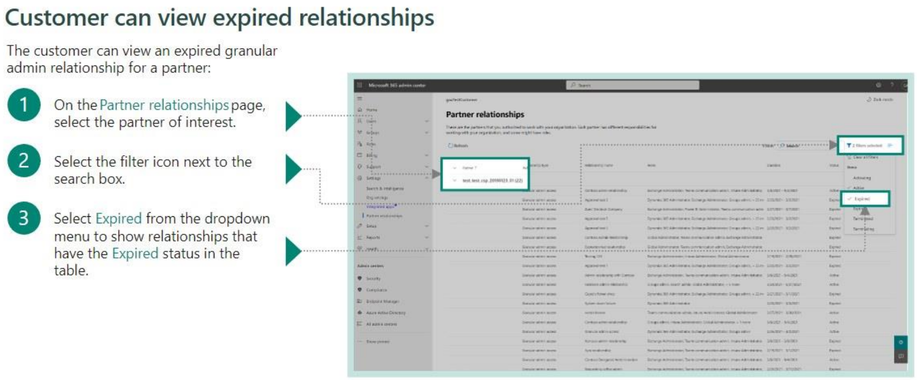
The partner can go to the Admin relationships page to view expired relationships. You can see details of the expired relationship on the Relationship details page.



TestRadand | Admin relationships

Below is a list of admin relationships with the customer that are currently active, expired, or terminated.

Admin relationship name	Status	Start date	End date	Details
□ Accessibility Test Relationship	Terminated	02/11/2021	06/02/2021	⌄
□ Activation test relationship	Active	02/19/2021	03/14/2021	⌄
□ AlphaBeta relationship	Terminated	02/11/2021	04/16/2021	⌄
□ Azure admin test relationship	Expired	02/16/2021	02/17/2021	⌄
□ Azure test relationship	Expired	02/16/2021	02/17/2021	⌄
□ Best buy relationship	Terminated	02/11/2021	03/05/2021	⌄
□ Bubba's Fine Cuisine	Approved	Invalid Date	Invalid Date	⌄
□ Ceylon admin relationship	Active	02/11/2021	03/10/2021	⌄
□ Confirmation admin relationship	Terminated	02/19/2021	03/13/2021	⌄
□ Confirmation test relationship	Expired	02/12/2021	02/14/2021	⌄
□ Contoso Admin Relationship	Approval pending			⌄

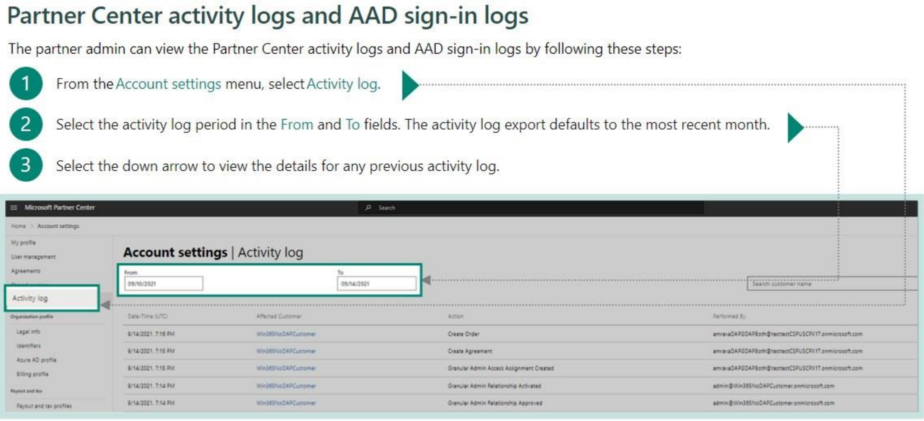


Customer can view expired relationships

The customer can view an expired granular admin relationship for a partner:

1. On the Partner relationships page, select the partner of interest.
2. Select the filter icon next to the search box.
3. Select Expired from the dropdown menu to show relationships that have the Expired status in the table.

Auditing



Partner Center activity logs and AAD sign-in logs

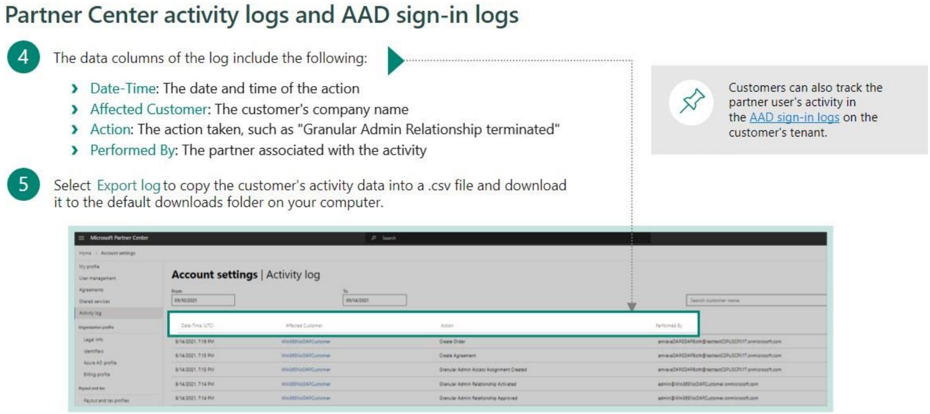
The partner admin can view the Partner Center activity logs and AAD sign-in logs by following these steps:

1. From the Account settings menu, select Activity log.
2. Select the activity log period in the From and To fields. The activity log export defaults to the most recent month.
3. Select the down arrow to view the details for any previous activity log.

Account settings | Activity log

From 09/10/2021 To 09/14/2021

Date-Time (UTC)	Affected Customer	Action	Performed By
9/14/2021, 7:16 PM	Win365NoDAPCustomer	Create Order	amravaDAPGDAPBoth@testtestCSPUSCPX1T.onmicrosoft.com
9/14/2021, 7:15 PM	Win365NoDAPCustomer	Create Agreement	amravaDAPGDAPBoth@testtestCSPUSCPX1T.onmicrosoft.com
9/14/2021, 7:15 PM	Win365NoDAPCustomer	Granular Admin Access Assignment Created	amravaDAPGDAPBoth@testtestCSPUSCPX1T.onmicrosoft.com
9/14/2021, 7:14 PM	Win365NoDAPCustomer	Granular Admin Relationship Activated	admin@Win365NoDAPCustomer.onmicrosoft.com
9/14/2021, 7:14 PM	Win365NoDAPCustomer	Granular Admin Relationship Approved	admin@Win365NoDAPCustomer.onmicrosoft.com



Partner Center activity logs and AAD sign-in logs

4. The data columns of the log include the following:
   - Date-Time: The date and time of the action
   - Affected Customer: The customer's company name
   - Action: The action taken, such as "Granular Admin Relationship terminated"
   - Performed By: The partner associated with the activity
5. Select Export log to copy the customer's activity data into a .csv file and download it to the default downloads folder on your computer.

Customers can also track the partner user's activity in the AAD sign-in logs on the customer's tenant.

Customers can also track the partner user's activity in the AAD sign-in logs on the customer's tenant.

Disable DAP

- After you've been granted GDAP by your customer and have confirmed that you can perform all necessary admin activities on behalf of your customer, you should disable your existing DAP connection.
- To disable DAP, follow the same steps in the Remove inactive DAP connections section.

Customer Email Template

What is this?

To help our partners accurately communicate the changes from DAP to GDAP to their customers we have created an email template you can choose utilise in your customer communications so they understand what's changing and how GDAP will be improve security to their Microsoft services.

Email Template: Significant Security Updates in Microsoft CSP

Dear Customer,

As part of their **zero trust policies** Microsoft are introducing "Granular Delegated Admin Privileges" (GDAP) to replace the more basic "Delegated Admin Privileges" (DAP) previously used for Microsoft CSP administration.

GDAP is a security feature that provides partners with least-privileged access following the Zero Trust cybersecurity protocol. It lets Microsoft partners configure granular and time-bound access to their customers' workloads in production and sandbox environments. This least-privileged access needs to be explicitly granted to partners by their customers. For more information please click here.

As part of Microsoft's Cloud Solution Provider Program we are partnered with TD SYNNEX (UK) Ltd. We invite you to accept the relationship invitation that will receive shortly from TD SYNNEX (UK) Ltd in order for us to establish the new GDAP relationship with TD SYNNEX (UK) Ltd in the Microsoft CSP-model.

TD SYNNEX (UK) Ltd is one of the world’s largest technology distributors and Microsoft Gold Partner working exclusively with the IT channel to provide range wide range of products and solutions including Microsoft CSP.

If you have any questions don’t hesitate to contact us.

Kind regards

{Reseller name and contact details}