Granular Delegated Admin Privileges

DIRECT CUSTOMERS USER GUIDE

Microsoft's GDAP is the next evolution towards zero trust, providing Cloud Solution Providers with the tools to only need the specific roles necessary to assist clients, rather than having full Global Admin privileges.

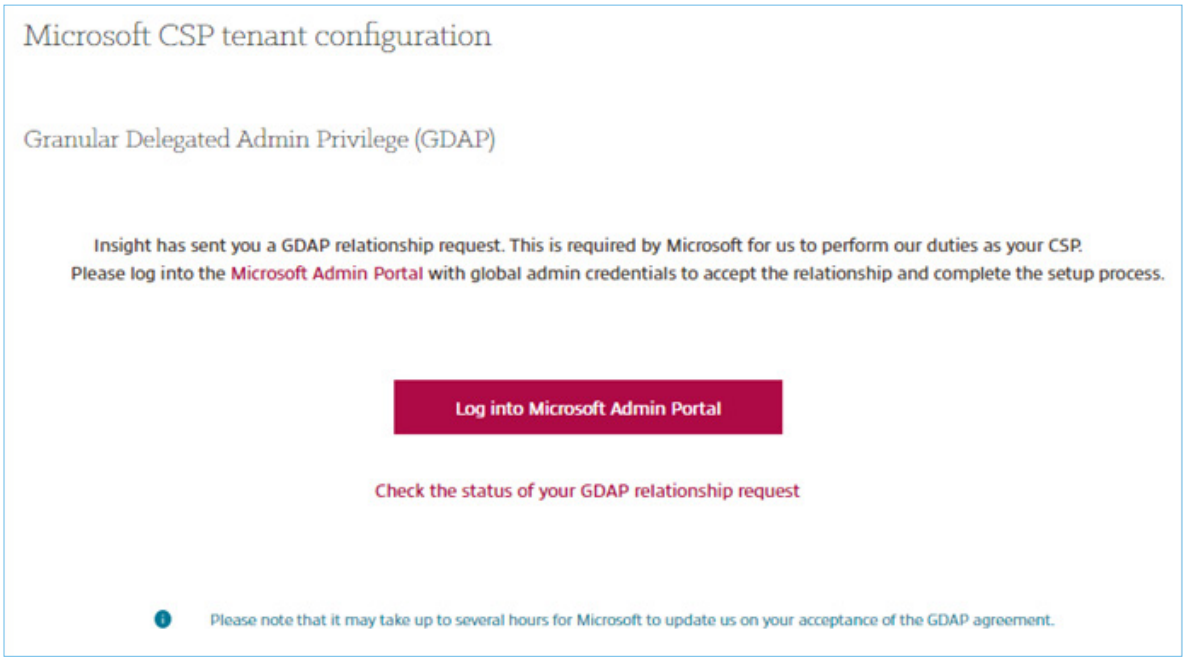
Aligning with Microsoft's GDAP recommendations, Insight has adopted Microsoft's recommended 17 roles as our standard GDAP relationship. This allows us the ability to purchase on your behalf through our Cloud Commerce Experience portal (CCx), have Global Reader to assist through our Cloud Care program, as well as the additional necessary roles to provide technical support per our agreement with Microsoft.

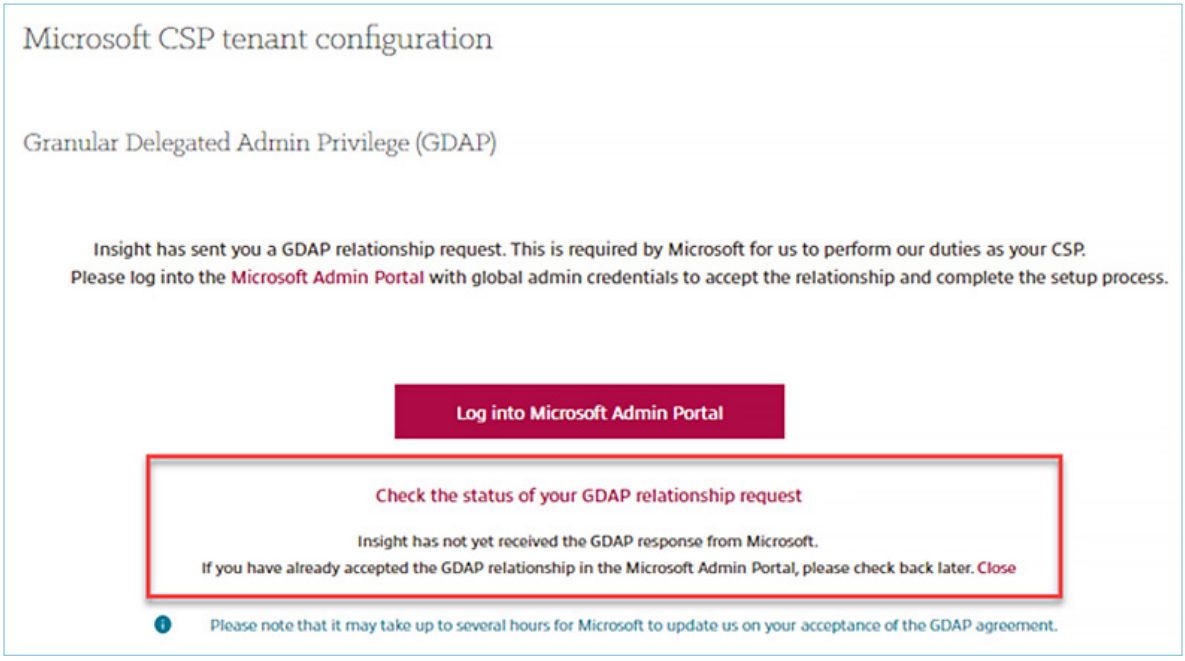
For you to be completely onboarded in our Cloud Commerce Experience portal you are currently required to approve 2 Microsoft links:

- **Reseller Relationship** link sent to you by your account manager - this enables Insight to have visibility of your Microsoft tenant;
- **GDAP relationship link** – which is generated as you first log into your new Cloud Commerce Experience portal – this enables you to use all the functionalities of the portal including managing your subscriptions.

How to approve the GDAP relationship link

1. Log into the Cloud Commerce Experience portal,
2. You will be prompted with the below pop-up window asking you to accept the GDAP relationship.
3. You can click on the link "Microsoft Admin Portal", this will redirect you to the M365 Admin Center.
   Please note that this link can only be approved by the Global Admin of the tenant.





4. After the Global Admin has approved the GDAP request in M365 Admin Center, the notification box in CCx will disappear shortly after.
   Please keep in mind that the sync may last up to 4 Hours.

Other considerations

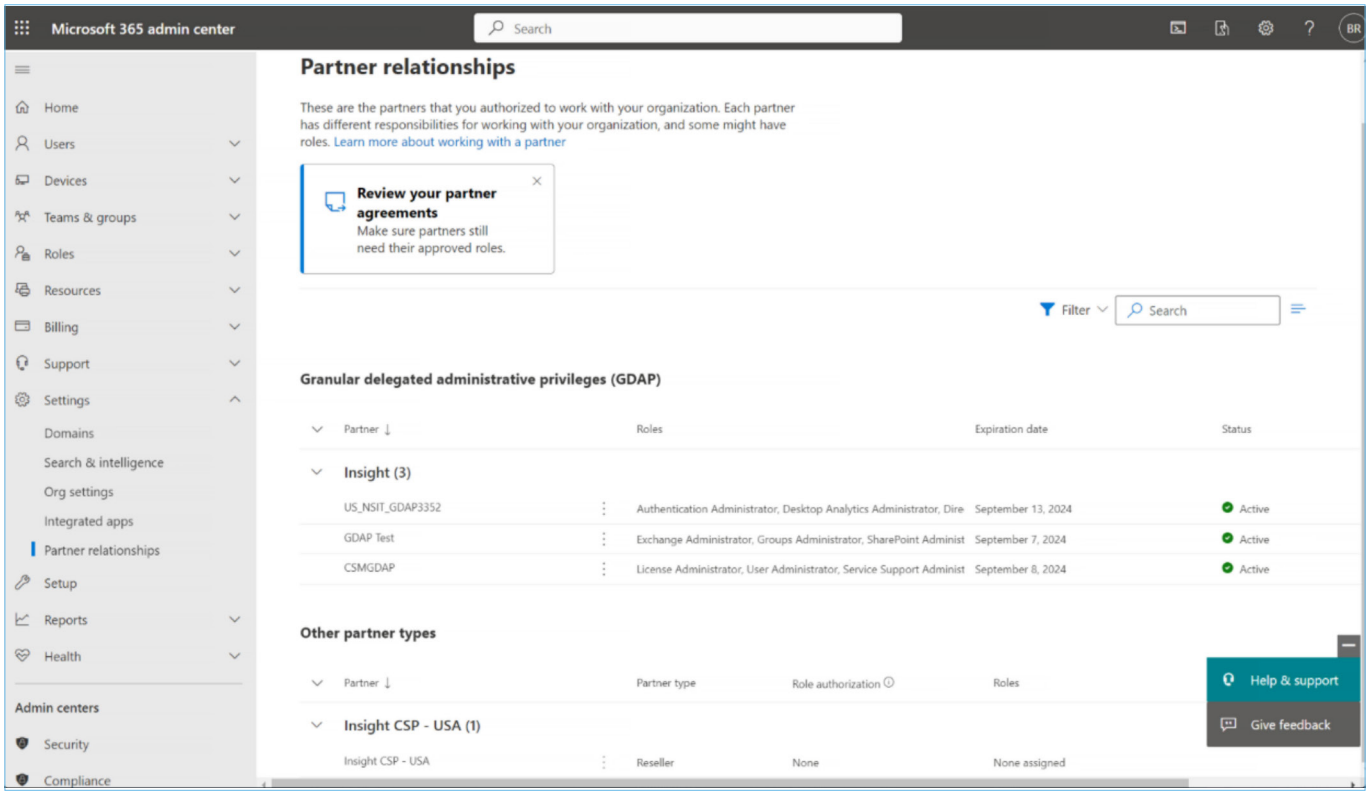
We realize that some of our clients have stricter policy controls or regulatory requirements in place. For those clients, we have the below recommendation:

Conditional Access: A client can create a conditional access policy to block Insight from accessing their Microsoft Admin Center or Azure Portal by default. This is our preferred methodology as it is less impactful to our client and Insight.

You can review your GDAP and DAP relationships in your Microsoft Admin Center under Partner Relationships. Please see the screenshot below.

If you have any questions or concerns, please reach out to your Insight representative.

Microsoft Admin Center: Partner Relationships View



Conditional Access

We recommend that our clients with security and access concerns limit Insight's access by using Conditional Access policies. This is a recommended security best practice regardless of the purchasing method. One method is for you to implement a block on all Guest User Access for Cloud Apps. You can then create exclusions to that policy for either the tenant or the specific directory roles. You can also create exclusions for specific Cloud Apps as to not impact their other Guest Users.

Conditional Access: Block access

Create or update a dynamic group in Azure Active Directory

Creating a group of guests only

If you have any questions or concerns, please raise a support request in Service Now or reach out to your Insight representative.