Granular Delegated Admin Privileges

RESELLERS 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 end customers behalf through our Reseller Administration Portal (RAP), 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.

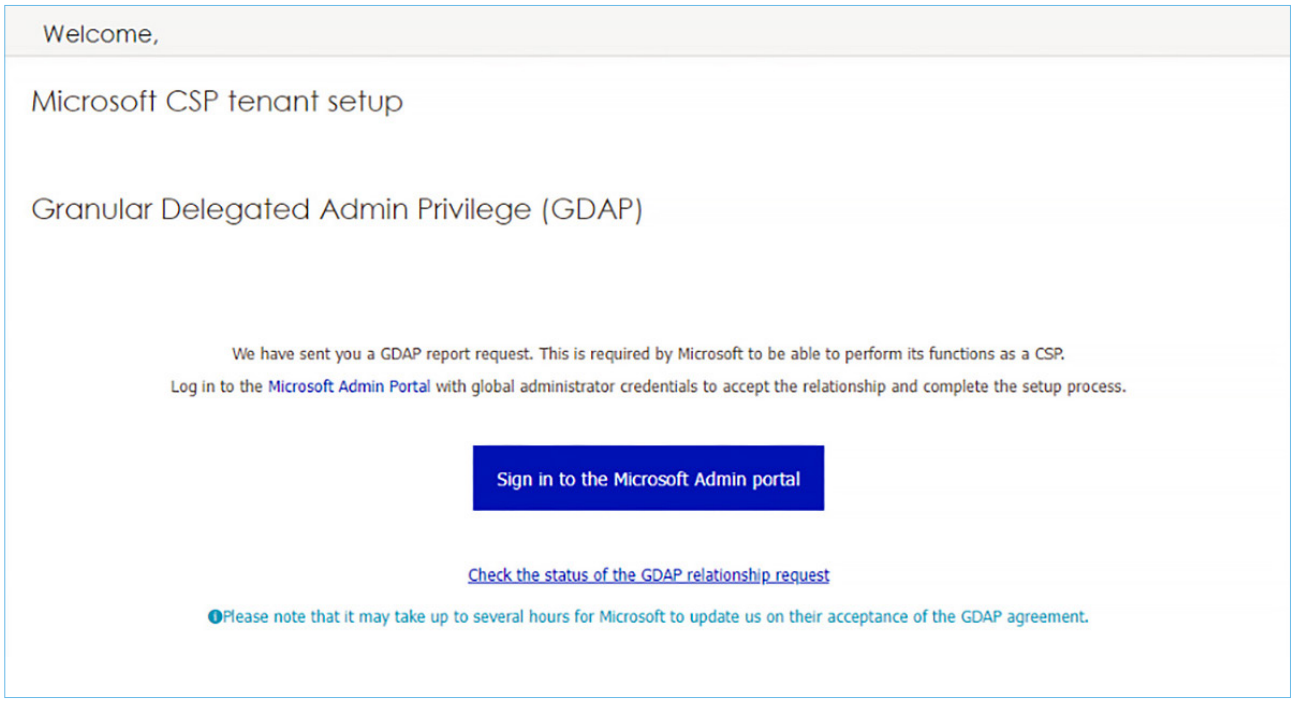
In order to onboard your end customers into our Reseller Administration portal you will be required to take the following actions:

1. Send the **Reseller Relationship link** (available in your Partner Center account) to your end customer to accept you as their local reseller of record. This will also enable Insight to have visibility of your end customers Microsoft tenant.
2. Send the **GDAP relationship link** (prompted as you first log into your end customer's storefront) to your end customer. This enables you to use all the functionalities of the portal including managing your end customers' subscriptions.

Note: User with Global Admin permission is required to accept both relationships.

How to approve the GDAP relationship link

1. Log into the Reseller Administration Portal,
2. Select the account of your end customer and log in using the log in as button,
3. You will then be prompted with the below pop-up window asking you to accept the GDAP relationship. You can click on the link "Microsoft Admin Portal", this will redirect you to the M365 Admin Center. However, please note that this link can only be approved by the Global Admin of your end customer's tenant. As a Reseller, you will need to take your own steps to ensure you have GDAP set between yourself and your end customers.



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

Other considerations

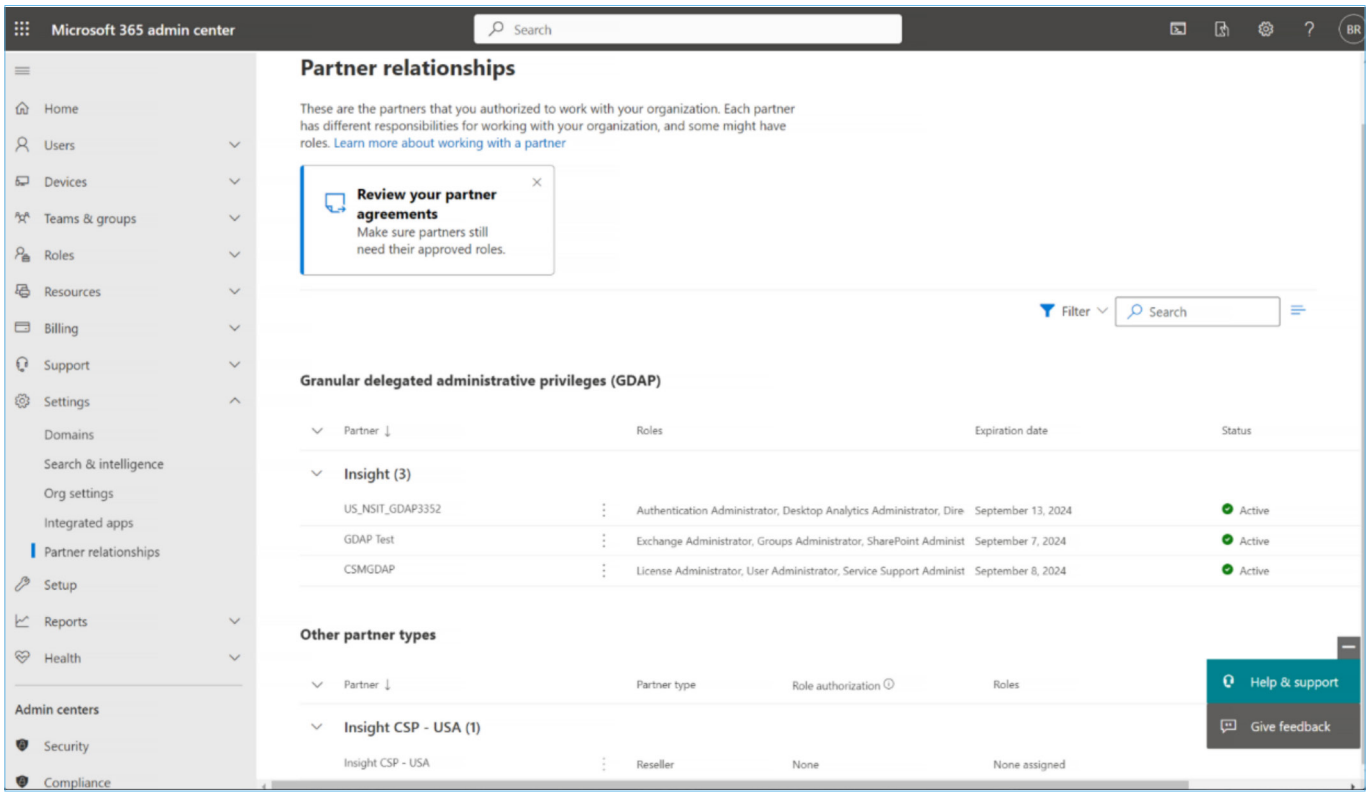
We realize that some of our clients have stricter policy controls or regulatory requirements in place. For those clients, we have the below recommendation:

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.