GDAP IN AUTOPILOT

Frequently Asked Questions

Microsoft Solutions Partner

What Is GDAP?

GDAP stands for Granular Delegated Admin Privileges and—in the case of Microsoft Cloud Service Providers (CSP)—refers to the capability to assign specific administrative permissions to users or groups within a Microsoft environment such as Entra ID or Microsoft 365. These privileges can be finely tuned to grant access only to the resources and functions necessary for users to perform their roles effectively without providing unnecessary or excessive permissions.

The Benefits of GDAP in CSP

- **Enhanced Security:** By assigning only the necessary permissions to each user or group, GDAP reduces the risk of unauthorized access and potential security breaches.
- **Improved Compliance:** CSPs can establish compliance with regulatory standards by meticulously regulating access to sensitive data and administrative capabilities within your Microsoft environment.
- **Efficient Resource Management:** Detailed authorization allows for more effective resource management by providing administrators the ability to focus on specific tasks and responsibilities, leading to enhanced productivity and streamlined operations.
- **Flexibility and Scalability:** Administrators can quickly and easily alter and finetune permissions as organizational needs change to accommodate growth, restructuring, or changes in roles and responsibilities.
- **Reduced Administrative Overhead:** By delegating administrative tasks to appropriate personnel at the correct level, organizations can diminish administrative overhead and ensure that tasks are handled by those with the necessary expertise and authority.
- **Enhanced User Experience:** Users benefit from a smoother and more intuitive experience as they only have access to the tools and resources they need to perform their specific tasks without unnecessary clutter or complication.

What Does This Mean and What Has Changed?

- A new GDAP relationship is needed for every new CSP relationship established with Connection. This requirement is more relaxed for standard CSP licensing and Azure customers. However, work cannot be performed without GDAP for Autopilot and MSP.
- The roles being requested for non-MSP customers are:
  - Service Support Administrator to read service health information and manage support tickets.
  - Directory Reader to read basic directory information and grant directory read access to applications and guests.
  - License Administrator to grant the ability to assign, remove, and update licensing assignments.
  - Global Reader Access to read everything that a global administrator can—without the ability to perform updates.

What Is the Process for Establishing GDAP?

Once received, you will need to accept the request for the Autopilot engagement to continue. You can assign Security Groups after accepting the request.

What Are Security Groups?

Security Groups are groups of individuals within Connection who can access their approved role. These roles are available only to those who need access.

Do I Need to Do This Every Time I Order Devices that Need to Be Imaged?

No. However, GDAP roles will need to be renewed every two years—not for each Autopilot engagement.

What Happens If I Don't Set Up Roles?

The Autopilot engagement cannot be completed if roles are not established.

Can I Remove This Once All the Devices Are Set Up?

Removing the roles will impact our ability to perform the Autopilot engagement and Connection will not be able to provide the support required.

For more information on GDAP, contact your Connection Account Team today.

Connection®
we solve IT®

Business Solutions
1.800.800.0014

Enterprise Solutions
1.800.369.1047

Public Sector Solutions
1.800.800.0019

www.connection.com/Microsoft