Important Security Information: DAP changing to GDAP from MAY 22.

Beginning May 22, 2023, Microsoft will begin transitioning all DAP relationships to GDAP roles. This is an important step from Microsoft to secure the partner ecosystem and protect your customers tenants.
Partners should continue securing their access with the following steps:

- **Requesting granular delegated admin privileges (GDAP)**: If admin access is required for a customer tenant, then the partner (with the admin agent role within the partner organization) should request, and customer should approve a GDAP relationship with the appropriate Azure Active Directory (AD) roles.
- **Disabling delegated admin privileges (DAP)**: If admin access isn't required, then the partner (with the admin agent role within the partner organization) should review the DAP monitoring report and disable DAP relationships immediately. If admin access is needed, then the partner should complete the GDAP setup and then disable DAP.

What is happening May 22?

As Microsoft will begin transitioning DAP relationships to GDAP roles starting May 22, 2023, default roles will be automatically assigned to corresponding predefined CSP security groups, which could fall under either admin agents or help desk agents.

Admin agents security group

- **Directory readers:** Can read basic directory information; commonly used to grant directory read access to applications and guests
- **Directory writers:** Can read and write basic directory information; for granting access to applications, not intended for users
- **License administrator:** Can manage product licenses on users and groups
- User administrator: Can manage all aspects of users and groups, including resetting passwords for limited admins
- **Privileged role administrator:** Can manage role assignments in Azure AD and all aspects of Privileged Identity Management (PIM)
- **Privileged authentication administrator:** Can access view, set, and reset authentication method information for any user (admin or nonadmin)
- **Service support administrator:** Can read service health information and manage support tickets
- **Help desk administrator:** Can reset passwords for nonadministrators and help desk administrators

Help desk agents security group

- **Service support administrator:** Can read service health information and manage support tickets
- **Help desk administrator:** Can reset passwords for nonadministrators and help desk administrators

Next steps for partners:

- Review this information and share as appropriate within your organization.

- Ensure you have processes and policies in place to securely manage your customers.
- To help partners address questions around DAP and GDAP with customers, Microsoft has created a set of FAQs
- Visit the Microsoft Partner Security Site for more information on DAP and GDAP changes.
- Sign Up for dedicated CSP Security Q&A sessions.
- Engage with your TD SYNNEX team for any question related to these changes.