



Microsoft Granular Delegated Admin Privileges (GDAP) StreamOne Cloud Marketplace (SCM)

TD SYNEX introducing GDAP

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 protected 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.

What is GDAP?

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 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.

At TD SYNEX, we will be moving away from the current DAP model (which gives admin agents standing or perpetual global admin access) to a fine-grained delegated access model with a time limit.

What is TD SYNEX doing to address?

We have redesigned our current platform functionality with role-based permissions on the End Customers tenant as a part of this granular approach. Currently, Resellers have the option to check the GDAP Report to easily view status requests and manually shift customers from DAP to GDAP. Microsoft is planning to provide the necessary tools and enable TD SYNEX to automatically shift customers to GDAP.

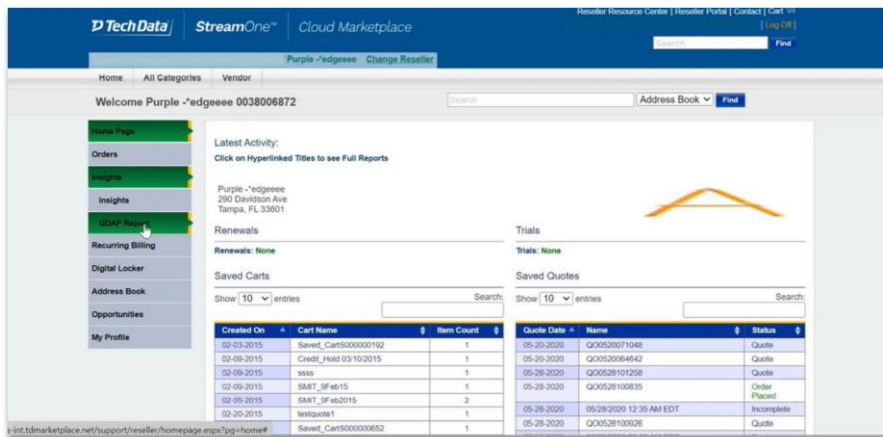
[Check out GDAP on StreamOne Cloud Marketplace video!](#)

GDAP Report and LCM on StreamOne Cloud Marketplace (SCM)

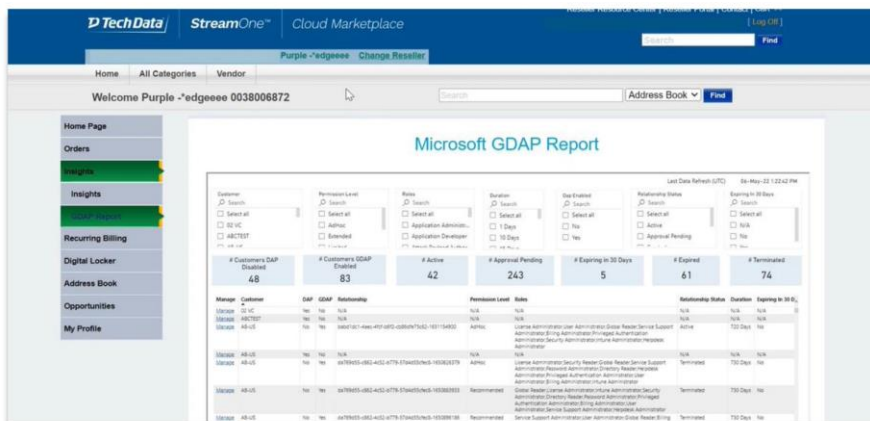
Reseller User Journey(s)

Viewing Settings on Dashboard

1. To check the settings for this actionable dashboard, the Resellers will log into SCM and from the Reseller portal click on Insights, and then the GDAP Report. The report is loaded based on the tenant's MPN ID, including tenants not currently transacting in SCM.



2. The GDAP report is designed to give the Reseller an overview, a one stop shop look, of all access TD SYNnex has on their End Customers. It only shows the access TD SYNnex has, not what the Reseller has. The permissions TD SYNnex has and the permissions the Reseller may have, from a GDAP perspective, are two separate items.



3. The report fields can be further filtered and include the following sections:

a. Customer

Manage	Customer	DAP	GDAP	Relationship	Permission Level	Roles	Relationship Status	Duration	Expiring in 30 Days
Microsoft	US-IT	Yes	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Microsoft	ARCTEST	Yes	No	N/A	N/A	N/A	N/A	N/A	N/A
Microsoft	AS-US	No	Yes	666f1c1-44e1-47d1-8d52-d98d975d32-181194900	Admin	License Administrator, User Administrator, Global Reader, Service Support Administrator, Billing Administrator, Privileged Administrator, Administrator, Security Administrator, Intune Administrator, Helpdesk Administrator	Active	730 Days	No
Microsoft	AS-US	Yes	No	N/A	N/A	N/A	N/A	N/A	N/A
Microsoft	AS-US	No	Yes	6a789d55-d8d2-4c52-d779-37d4d55fcd6c-160926379	Admin	License Administrator, Security Reader, Global Reader, Service Support Administrator, Password Administrator, Directory Reader, Helpdesk Administrator, Privileged Administrator, Authentication Administrator, Billing Administrator, User Administrator	Terminated	730 Days	No
Microsoft	AS-US	No	Yes	6a789d55-d8d2-4c52-d779-37d4d55fcd6c-160883393	Recommended	Global Reader, License Administrator, Billing Administrator, Security Administrator, Directory Reader, Password Administrator, Privileged Administrator, Authentication Administrator, Billing Administrator, User Administrator	Terminated	730 Days	No
Microsoft	AS-US	No	Yes	6a789d55-d8d2-4c52-d779-37d4d55fcd6c-160881366	Recommended	Service Support Administrator, User Administrator, Global Reader, Billing Administrator, License Administrator, Directory Reader, Privileged Administrator, Authentication Administrator, Security Administrator, Intune Administrator, Password Administrator, Helpdesk Administrator, Administrator	Terminated	730 Days	No
Microsoft	AS-US	No	Yes	6a789d55-d8d2-4c52-d779-37d4d55fcd6c-160883361	Recommended	Directory Reader, Intune Administrator, Security Administrator, User Administrator, Billing Administrator, Service Support Administrator, Password Administrator, Global Reader, Helpdesk Administrator, Privileged Administrator, Authentication Administrator, License Administrator	Active	730 Days	No
Microsoft	AS-US	No	Yes	6a789d55-d8d2-4c52-d779-37d4d55fcd6c-160883941	Recommended	Security Administrator, Password Administrator, Directory Reader, License Administrator, User Administrator, Helpdesk Administrator, Intune Administrator, Global Administrator, Service Support Administrator, Billing Administrator, Global	Terminated	730 Days	No
Total									

b. Permission Levels:

GDAP Limited access: Basic help desk resolution and service desk delivery

- Enable TD SYNEX to open support cases on End Customer behalf
- Platform functionalities will be limited for Resellers to use on those End Customers tenants
- GDAP Link duration 2 years
- Roles given to TD SYNEX on End Customer tenants: Directory Reader, Service Support Administrator

GDAP Recommended access: In-depth technical support (recommended – default)

- Enable TD SYNEX to provide high level of Technical break/fix support, Managed Services, deploy Click to Run Solutions, & Consulting Services
- Resellers will be able to assign licenses through our platforms among other platforms functionalities.
- End Customer tenant Active Directory will have "TD SYNEX StreamOne Integration" within Enterprise Applications
- GDAP Link duration 2 years
- Roles given to TD SYNEX on End Customer tenants: License Administrator, Billing Administrator, Password Administrator, Global Reader, Intune Administrator, Global Administrator, Service Support Administrator, Helpdesk Administrator, Privileged Authentication Administrator, Directory Reader, Security Reader

GDAP Ad hoc

NB: Will be available at a later stage.

Microsoft GDAP Report

Customer: ID Search, Permission Level: Select all, Role: Select all, Duration: Select all, Day Enabled: Select all, Relationship Status: Select all, Expiring in 30 Days: Select all

Customers DAP Disabled: 48, # Customers GDAP Enabled: 83, # Active: 42, # Approval Pending: 243, # Expiring in 30 Days: 5, # Expired: 61, # Terminated: 74

Manage	Customer	DAP	GDAP	Relationship	Permission Level	Roles	Relationship Status	Duration	Expiring in 30 D.
Manage	48-US	Yes	No	N/A	N/A	N/A	N/A	N/A	N/A
Manage	48-US	Yes	No	N/A	N/A	N/A	N/A	N/A	N/A
Manage	48-US	Yes	No	aa78683-d82-452-6779-5764055c4d-16119490	Admin	License Administrator, Administrator Global Reader, Service Support, Administrator Billing, Administrator Privileged, Administrator Security, Administrator In-House Administrator Helpdesk Administrator	Active	732 Days	No
Manage	48-US	Yes	No	N/A	N/A	N/A	N/A	N/A	N/A
Manage	48-US	Yes	No	aa78683-d82-452-6779-5764055c4d-163000379	Admin	License Administrator, Security Reader, Global Reader, Service Support, Administrator Billing, Administrator Privileged, Administrator Security, Administrator In-House Administrator Helpdesk Administrator	Terminated	730 Days	No
Manage	48-US	Yes	No	aa78683-d82-452-6779-5764055c4d-163000383	Recommended	Global Reader, License Administrator, In-House Administrator Security, Administrator Billing, Administrator Privileged, Administrator Security, Administrator In-House Administrator Helpdesk Administrator	Terminated	730 Days	No
Manage	48-US	Yes	No	aa78683-d82-452-6779-5764055c4d-163000186	Recommended	Service Support, Administrator User, Administrator Global Reader, Billing, Administrator License Administrator, Directory Reader, Privileged, Administrator Security, Administrator In-House Administrator Helpdesk Administrator	Terminated	730 Days	No
Manage	48-US	Yes	No	aa78683-d82-452-6779-5764055c4d-163000381	Recommended	Directory Reader, In-House Administrator Security, Administrator User, Administrator Billing, Administrator Service Support, Administrator License Administrator, Administrator Security, Administrator Global Reader, Password Administrator, Privileged, Authentication Administrator, License Administrator	Active	730 Days	No
Manage	48-US	Yes	No	aa78683-d82-452-6779-5764055c4d-163000841	Recommended	Security Administrator, Password Administrator, Directory Reader, License Administrator, Administrator User, Administrator Helpdesk Administrator, In-House Administrator, Service Support, Administrator Billing, Administrator Global Reader, Administrator Directory Reader, Service Support, Administrator Security	Terminated	730 Days	No
Total									

f. Relationship Status: (view of all activity), Expiring in 30 Days (view accounts expiring in 30 days), and Last Data Refresh date/time.

Microsoft GDAP Report

Customer: ID Search, Permission Level: Select all, Role: Select all, Duration: Select all, Day Enabled: Select all, Relationship Status: Select all, Expiring in 30 Days: Select all

Customers DAP Disabled: 48, # Customers GDAP Enabled: 83, # Active: 42, # Approval Pending: 243, # Expiring in 30 Days: 5, # Expired: 61, # Terminated: 74

Manage	Customer	DAP	GDAP	Relationship	Permission Level	Roles	Relationship Status	Duration	Expiring in 30 D.
Manage	48-US	Yes	No	N/A	N/A	N/A	N/A	N/A	N/A
Manage	48-US	Yes	No	N/A	N/A	N/A	N/A	N/A	N/A
Manage	48-US	Yes	No	aa78683-d82-452-6779-5764055c4d-16119490	Admin	License Administrator, Administrator Global Reader, Service Support, Administrator Billing, Administrator Privileged, Administrator Security, Administrator In-House Administrator Helpdesk Administrator	Active	732 Days	No
Manage	48-US	Yes	No	N/A	N/A	N/A	N/A	N/A	N/A
Manage	48-US	Yes	No	aa78683-d82-452-6779-5764055c4d-163000379	Admin	License Administrator, Security Reader, Global Reader, Service Support, Administrator Billing, Administrator Privileged, Administrator Security, Administrator In-House Administrator Helpdesk Administrator	Terminated	730 Days	No
Manage	48-US	Yes	No	aa78683-d82-452-6779-5764055c4d-163000383	Recommended	Global Reader, License Administrator, In-House Administrator Security, Administrator Billing, Administrator Privileged, Administrator Security, Administrator In-House Administrator Helpdesk Administrator	Terminated	730 Days	No
Manage	48-US	Yes	No	aa78683-d82-452-6779-5764055c4d-163000186	Recommended	Service Support, Administrator User, Administrator Global Reader, Billing, Administrator License Administrator, Directory Reader, Privileged, Administrator Security, Administrator In-House Administrator Helpdesk Administrator	Terminated	730 Days	No
Manage	48-US	Yes	No	aa78683-d82-452-6779-5764055c4d-163000381	Recommended	Directory Reader, In-House Administrator Security, Administrator User, Administrator Billing, Administrator Service Support, Administrator License Administrator, Administrator Security, Administrator Global Reader, Password Administrator, Privileged, Authentication Administrator, License Administrator	Active	730 Days	No
Manage	48-US	Yes	No	aa78683-d82-452-6779-5764055c4d-163000841	Recommended	Security Administrator, Password Administrator, Directory Reader, License Administrator, Administrator User, Administrator Helpdesk Administrator, In-House Administrator, Service Support, Administrator Billing, Administrator Global Reader, Administrator Directory Reader, Service Support, Administrator Security	Terminated	730 Days	No
Total									

g. Dashboard Details include: Manage Customer Link (takes you directly to customer Digital Locker), Customer Name, do they have DAP or GDAP, is the Relationship established with the ID, Permission Level, Roles (from a GDAP perspective), Relationship status, Duration, Does it Expire soon, Created Date, Activated Date, End Date, and Last Modified Date.

Customer: ID Search, Permission Level: Select all, Role: Select all, Duration: Select all, Day Enabled: Select all, Relationship Status: Select all, Expiring in 30 Days: Select all

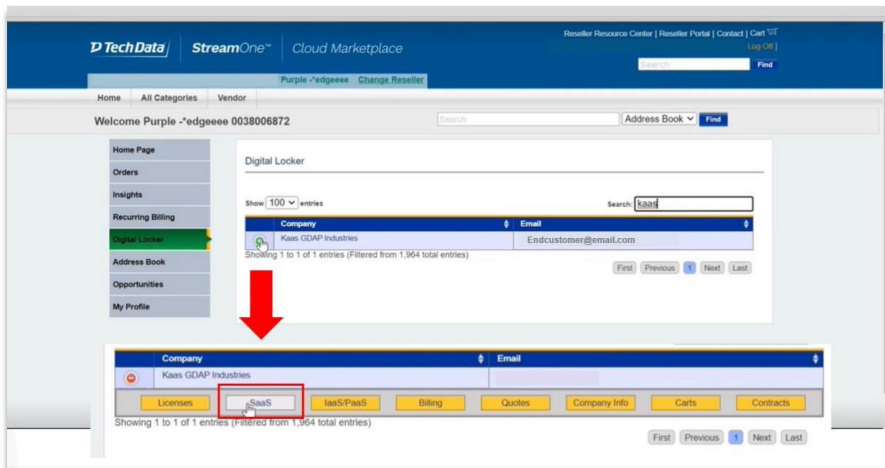
Customers DAP Disabled: 48, # Customers GDAP Enabled: 83, # Active: 42, # Approval Pending: 243, # Expiring in 30 Days: 5, # Expired: 61, # Terminated: 74

Manage	Customer	DAP	GDAP	Relationship	Permission Level	Roles	Relationship Status	Duration	Expiring in 30 D.
Manage	48-US	Yes	No	N/A	N/A	N/A	N/A	N/A	N/A
Manage	48-US	Yes	No	aa78683-d82-452-6779-5764055c4d-163000379	Admin	License Administrator, Security Reader, Global Reader, Service Support, Administrator Billing, Administrator Privileged, Administrator Security, Administrator In-House Administrator Helpdesk Administrator	Active	732 Days	No
Manage	48-US	Yes	No	aa78683-d82-452-6779-5764055c4d-163000383	Recommended	Global Reader, License Administrator, In-House Administrator Security, Administrator Billing, Administrator Privileged, Administrator Security, Administrator In-House Administrator Helpdesk Administrator	Terminated	730 Days	No
Manage	48-US	Yes	No	aa78683-d82-452-6779-5764055c4d-163000186	Recommended	Service Support, Administrator User, Administrator Global Reader, Billing, Administrator License Administrator, Directory Reader, Privileged, Administrator Security, Administrator In-House Administrator Helpdesk Administrator	Terminated	730 Days	No
Manage	48-US	Yes	No	aa78683-d82-452-6779-5764055c4d-163000381	Recommended	Directory Reader, In-House Administrator Security, Administrator User, Administrator Billing, Administrator Service Support, Administrator License Administrator, Administrator Security, Administrator Global Reader, Password Administrator, Privileged, Authentication Administrator, License Administrator	Active	730 Days	No
Manage	48-US	Yes	No	aa78683-d82-452-6779-5764055c4d-163000841	Recommended	Security Administrator, Password Administrator, Directory Reader, License Administrator, Administrator User, Administrator Helpdesk Administrator, In-House Administrator, Service Support, Administrator Billing, Administrator Global Reader, Administrator Directory Reader, Service Support, Administrator Security	Terminated	730 Days	No
Total									

Relationship Status	Duration	Expiring in 30 Days	Domains	Created Date	Activated Date	End Date	Last Modified Date
Administrator (Intune Administrator Helpdesk)	N/A	Not	Not	11-Jan-22 02:46:00 AM	11-Jan-22 02:46:00 AM	11-Jan-22 02:46:00 AM	25-Apr-22 6:41:01 AM
Security Reader (Global Reader Service Support)	730 Days	No	Yes	11-Jan-22 02:46:00 AM	22-Apr-22 11:19:41 AM	22-Apr-22 11:29:50 AM	25-Apr-22 6:41:01 AM
Authentication Administrator (Intune Administrator)	730 Days	No	Yes	11-Jan-22 02:46:00 AM	25-Apr-22 10:52:14 AM	25-Apr-22 2:04:07 PM	25-Apr-22 2:09:01 PM
Authentication Administrator (Intune Administrator Security)	730 Days	No	Yes	11-Jan-22 02:46:00 AM	25-Apr-22 2:16:28 PM	25-Apr-22 2:17:44 PM	25-Apr-22 3:45:01 AM
Global Administrator (Billing Administrator Global Reader Billing)	730 Days	No	Yes	11-Jan-22 02:46:00 AM	25-Apr-22 2:16:28 PM	25-Apr-22 2:17:44 PM	25-Apr-22 3:45:01 AM
Global Administrator (Billing Administrator Intune)	730 Days	No	Yes	11-Jan-22 02:46:00 AM	25-Apr-22 2:16:28 PM	25-Apr-22 2:17:44 PM	25-Apr-22 3:45:01 AM
Global Administrator (Billing Administrator Security)	730 Days	No	Yes	11-Jan-22 02:46:00 AM	25-Apr-22 2:16:28 PM	25-Apr-22 2:17:44 PM	25-Apr-22 3:45:01 AM
Global Administrator (Billing Administrator Security Support)	730 Days	No	Yes	11-Jan-22 02:46:00 AM	25-Apr-22 2:16:28 PM	25-Apr-22 2:17:44 PM	25-Apr-22 3:45:01 AM
Global Administrator (Billing Administrator Security Support)	730 Days	No	Yes	11-Jan-22 02:46:00 AM	25-Apr-22 2:16:28 PM	25-Apr-22 2:17:44 PM	25-Apr-22 3:45:01 AM
Global Administrator (Billing Administrator Security Support)	730 Days	No	Yes	11-Jan-22 02:46:00 AM	25-Apr-22 2:16:28 PM	25-Apr-22 2:17:44 PM	25-Apr-22 3:45:01 AM
Global Administrator (Billing Administrator Security Support)	730 Days	No	Yes	11-Jan-22 02:46:00 AM	25-Apr-22 2:16:28 PM	25-Apr-22 2:17:44 PM	25-Apr-22 3:45:01 AM
Global Administrator (Billing Administrator Security Support)	730 Days	No	Yes	11-Jan-22 02:46:00 AM	25-Apr-22 2:16:28 PM	25-Apr-22 2:17:44 PM	25-Apr-22 3:45:01 AM
Global Administrator (Billing Administrator Security Support)	730 Days	No	Yes	11-Jan-22 02:46:00 AM	25-Apr-22 2:16:28 PM	25-Apr-22 2:17:44 PM	25-Apr-22 3:45:01 AM
Global Administrator (Billing Administrator Security Support)	730 Days	No	Yes	11-Jan-22 02:46:00 AM	25-Apr-22 2:16:28 PM	25-Apr-22 2:17:44 PM	25-Apr-22 3:45:01 AM

Lifecycle Management

1. Log into the Digital Locker and choose a customer. The idea behind GDAP is to ensure the right level of access is granted from an End Customer perspective, so the platform can operate its various lifecycle management features. This is currently a manual process but will be automated once Microsoft releases tools to enable the automatic shift.



2. Access can be checked and granted through the Digital Locker:

- If you do not have access, the below GDAP message will appear requiring the Reseller to request access and submit for approval to the End Customer Admin.

Manage User

You do not currently have the necessary permissions to perform this action on behalf of your Customer. Microsoft has introduced Granular Delegated Administrative Privileges (GDAP) which your Customer must approve for transactions on their Tenant.

To request GDAP roles from your Customer proceed below. Once your Customer has approved the roles you will be able to return to this page and complete your transaction.

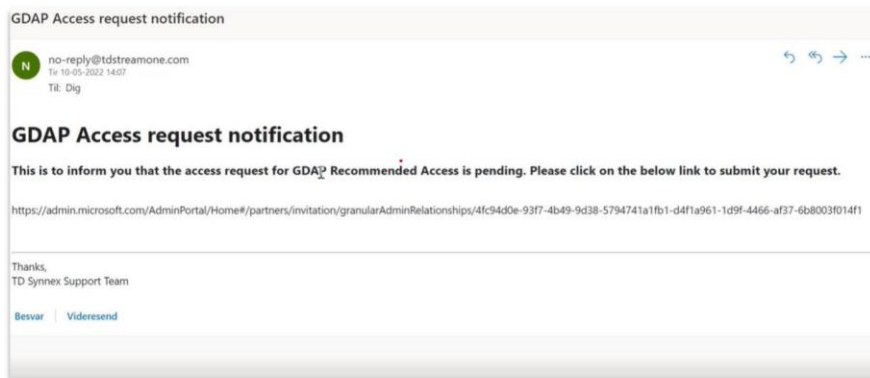
GDAP Recommended Access
 Provides access to the following roles:
 License Administrator, Billing Administrator, Password Administrator, Global Reader, Intune Administrator, Service Support Administrator, Helpdesk Administrator, Privileged Authentication Administrator, Directory Reader, Security Reader.

Reseller Email address *
 Email address where notification will be sent when approval is complete.

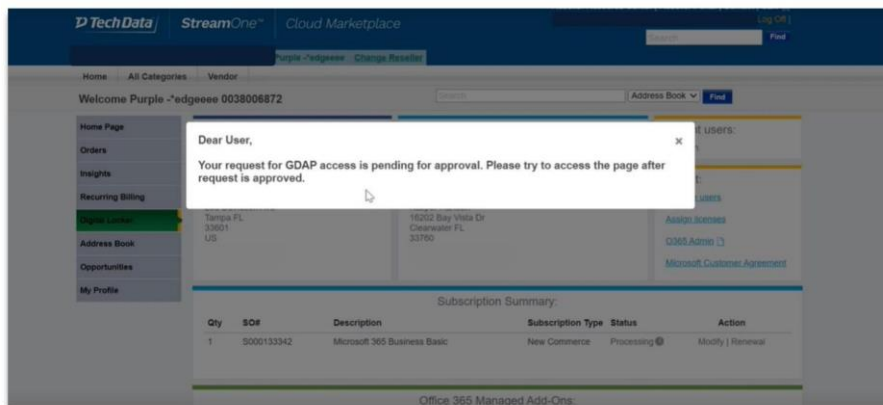
End Customer Email address *
 Email address where Customer will be notified of GDAP role approval.

- The End Customer will receive the GDAP Access Request Notification email, similar to the below message, for approval.

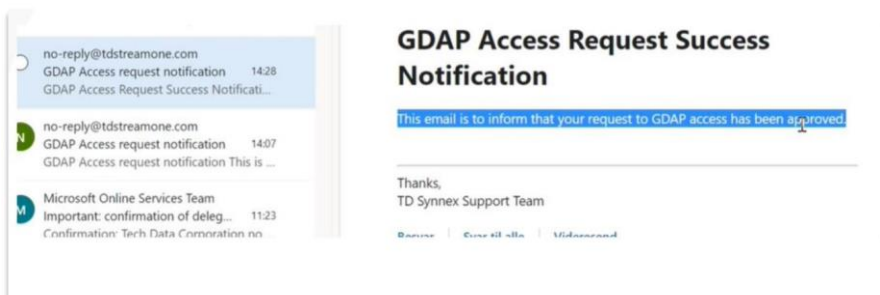
Important: The email address of the End Customer needs to be the Administrator user of the tenant.



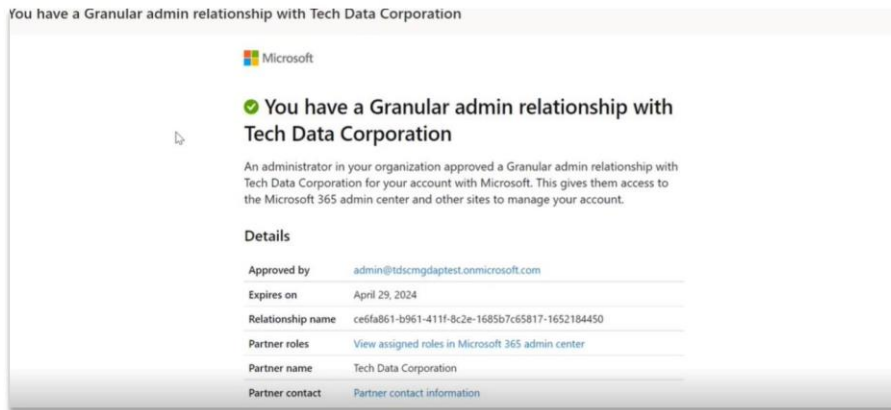
- In case the Reseller is unsure if the request was submitted, they can check by clicking on the manage users link which will display the pending approval message.



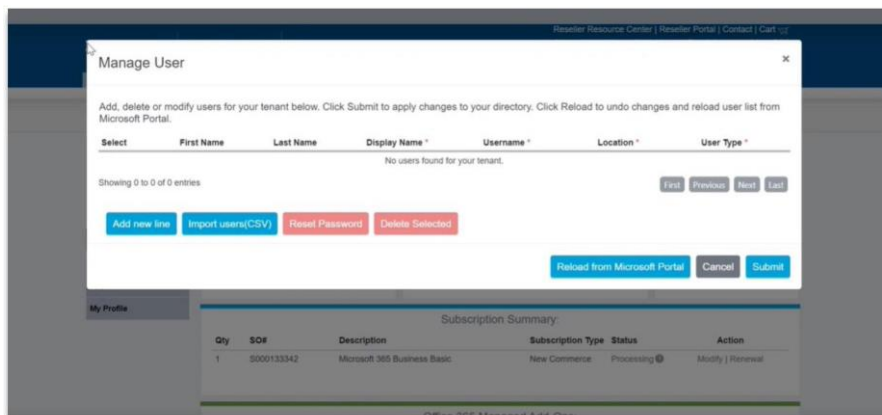
- Once approved, an email notification, similar to the below message, will be sent to the Reseller of the GDAP Access approval.



- Additionally, Microsoft will send an email to the End Customer with the new approved role information.



- To confirm the permission process was successful, the Reseller would go back to the Manage Users section and see access to the tenant on a GDAP level. You would only see this view of the manage user section, if you had access to the tenant on a GDAP level.



GDAP Frequently Asked Questions

Who can create a GDAP invitation request?

TD SYNnex Partners can raise a GDAP invitation request.

When a Partner sends a GDAP relationship request to a customer, and the customer does not take any action on it, does this request itself expire at any time?

Yes. Pending relationships expire after a number of days typically 90 days. This information will be available to Partners and on the email invitation sent.

When is the expiry of the GDAP relationship?

The expiry of the GDAP relationship is two years (maximum). However, End Customers and Reseller can review it at any time.

Is it possible to make the GDAP relationship with the customer permanent?

No. Permanent GDAP relationships with customers aren't possible for security purposes. The maximum duration for a GDAP relationship is two years.

How can I continue to administer services for my customers if DAP for inactive customers is removed?

While DAP and GDAP coexist, you can continue to administer services for your customers by establishing a GDAP relationship or recreating the DAP relationship with them through our platforms. We recommend establishing a GDAP relationship to ensure you have the most secure and least privileged access to your customer's tenant.

In the future, you will be required to have a GDAP relationship with any customers you wish to administer services to.

Is GDAP going to replace DAP?

Yes. During the transition period, both DAP and GDAP will coexist, with GDAP permissions taking precedence over DAP permissions for Microsoft 365 and Dynamics 365 workloads. Azure isn't in scope yet for GDAP. Eventually, GDAP will replace DAP.

Will there be any impact to my PEC earnings if I transition from DAP to GDAP? Any impact to PAL?

No, there will be no impact to your PEC earnings when you transition to GDAP. There will be no changes made to PAL with the transition, ensuring you continue to earn PEC.

Key Benefits

Partner

- Granular control and time limit to your customers workloads
- Better approach to security concerns
- Provide more services to End Users with restrictive security policies
- Utilize our Technical Support (break & fix) as it should be provided by TD SYNEX on your behalf
- Learn about new GDAP functionalities to manage license assignments and solution deployments
- Avoid creating Resellers Users on End Customers environments. In case Reseller needs to establish direct GDAP access [GUIDE to GDAP](#)

End User/ Customer

With the new GDAP capability, End Customers can work with Partners to accommodate control more granular and time-bound access to their customers' workloads, which will address better security customers concerns while receive more services from Partners.

Critical Dates

Critical dates:

- **June 1st, 2022:**

- Microsoft's GDAP General Availability. New functionalities will be available on TD SYNEX StreamOne platforms such as actionable reports and user GDAP permissions request management.
- **January / February 2023:**
- TD SYNEX-led transition active DAPs to GDAP starts for existing customers without end customer consent and remove all DAP relationships. End Customer tenant Active Directory will have "TD SYNEX StreamOne Integration" within Enterprise Applications
- **January 17th:**
- Microsoft will stop creating DAP relationships when a new customer or reseller relationship is created. New Tenant & Reseller Relationships invitation updated. Microsoft will start removing inactive DAP relationships that haven't been used in 90 days.
- **March 1st:**
- Microsoft will begin to transition remaining active DAP relationships to GDAP with limited Azure Active Directory (Azure AD) roles to perform least-privilege customer management activities. Partners will be required to perform more steps to continue to have access to Azure subscriptions after the limited roles are granted, as [documented](#). The limited GDAP roles (Directory reader, Global reader, User administrator, License administrator, Service support administrator, and Helpdesk administrator) granted by Microsoft during the transition will only allow you to perform least-privilege activities.

Protect your Business on Cyber-attacks on End Customers tenants

As a Partner in the Cloud Solution Provider program, you are responsible for your customer's Microsoft Cloud consumption, so it is important that you are aware of any potential fraud activity on your customers' Azure and per user subscriptions. This will allow you to take immediate action to determine if the behavior is legitimate or fraudulent and, if necessary, suspend the affected Azure resources or Azure subscription to mitigate the issue. [Learn more](#)

Best practice to protect your business

- Implement Mandatory security policies in Azure and M365: All end customer should enable MFA at the administrator level - Microsoft Guide [HERE](#)
- Continuous monitoring and evaluation (Cost Management Portal - security alerts)
- [Use the Microsoft 365 Lighthouse to secure and standardize Microsoft 365](#)