Microsoft CSP - GDAP

In This Article

Overview

Granular Delegated Admin Permissions (GDAP) is Microsoft's new security and compliance capabilities for Microsoft CSP partners like Evolve IP. GDAP allows you to define the level of access a CSP partner has to your 365 tenant. Microsoft's introduction of GDAP means you no longer need to give a CSP partner global admin permissions in your 365 tenant. Instead, you work with your CSP partner to configure time-limited access rights (using Azure AD roles) in your 365 tenant.

> **NOTE**
>
> **Establishing a GDAP relationship with Evolve IP is optional**. If you do not require any level of support and only want us to provision Microsoft subscription products in your 365 tenant, you can opt out of the GDAP relationship process. However, we will not be able to open any Microsoft Premier support tickets on your behalf. You will be responsible for opening support tickets with Microsoft.

GDAP Relationship Details

A GDAP relationship has 2 configuration items:

- The level of access to your 365 tenant, which is configured by selecting one or more **Azure AD Roles**
- A time limitation (in days) for the access to your 365 tenant

Additional GDAP Relationship Details

- You can have multiple GDAP relationship configurations with Evolve IP, and any other Microsoft CSP partners.
- Each GDAP relationship is time limited. The max is **2 years (730 days)**.
- A GDAP relationship will **automatically expire** when the duration (max 2 years) has completed.
- Before expiration, email notifications will be sent **30** days, **7** days, and **1** day before the GDAP expiration date. Emails are sent to your global administrators. Evolve IP is also notified.
- For GDAP relationships that **do not include** the Global Administrator role, Microsoft supports a 6-month auto-renewal process, which Evolve IP will enable by default.
- For GDAP relationships that **include** the Global Administrator role, a **new GDAP relationship** must be created to replace the old one.
- You can **terminate** a GDAP relationship in your Microsoft 365 Admin Center at any time.
- Evolve IP can also **terminate** a GDAP relationship at any time.

> **NOTE**
>
> In the GDAP model, some permissions within an Azure AD role may be limited by Microsoft. In other words, not all tasks within an Azure AD role can be performed with a GDAP relationship. Details on those limitations can be found in Microsoft's **Workloads Supported by GDAP** article.
>
> Additionally, GDAP is not a replacement for having a dedicated user account for Evolve IP to use in your 365 tenant. There may be situations where a dedicated user account in your 365 tenant is required. However, a GDAP relationship should be the preferred method of access, and **should always be configured** regardless of whether a user account is created for Evolve IP to use in your 365 tenant.

GDAP Relationship Setup Overview

Here's an overview of the GDAP relationship setup process:

- You work with the Evolve IP **Service Delivery** or **Support** teams to determine:
    - The level of access to your 365 tenant by choosing one or more Azure AD Roles.
    - The time limitation (in days) for the access. There's a minimum of 1 day and a maximum of 730 days (2 years).
- We give you a link to your Microsoft 365 Admin Center that specifies the level of access and the time limitation for the GDAP relationship.

- You click the link, and sign into your Microsoft 365 Admin Center with a user account that's a Global Administrator.
- After signing in, you review and approve the level of access and duration of the GDAP relationship request.

> **NOTE**
>
> You can request more than one GDAP relationship, each with their own level of access and time limitation. Also, by default, Evolve IP will enable Microsoft's 6-month auto-renewal feature for all GDAP relationships that do not include the Global Administrator role.

Minimum Level of Access

To give the Evolve IP **Service Delivery** & **Support** teams the ability to open Microsoft Premier support tickets on your behalf **Microsoft requires** you to approve the below Azure AD Roles, which provides us with the access we need to open the tickets. The GDAP relationship duration should be the maximum 2 years, but if you prefer to make it shorter, that's okay with us.

- **Global Reader** - Can read all configuration items that a Global administrator can, but can't update anything. Cannot view private organizational data.
- **Directory Readers** - Can read basic directory information. Commonly used to grant directory read access to applications and guests.
- **Service Support Administrator** - Can read service health information and manage support tickets.

Microsoft's Default Level of Access for New 365 Tenants

When you are **provisioned a new 365 tenant** by a Microsoft CSP partner like Evolve IP, that process adds the new 365 tenant to our Microsoft CSP partner portal and establishes Microsoft's default level of access using the below Azure AD roles. If the Azure AD roles do not meet your requirements, we can work with you to create a new GDAP relationship and remove the one created by Microsoft.

Here are the default Azure AD roles associated with Microsoft's default GDAP relationship:

- **Global Reader** - Can read all configuration items that a Global administrator can, but can't update anything. Cannot view private organizational data.
- **Directory Readers** - Can read basic directory information. Commonly used to grant directory read access to applications and guests.
- **Service Support Administrator** - Can read service health information and manage support tickets.
- **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.
- **Helpdesk Administrator** - Can reset passwords for non-administrators and Help Desk administrators.
- **Privileged Authentication Administrator** - Can access to view, set and reset authentication method information for any user (admin or non-admin).
- **Cloud Application Administrator** - Administrator Can create and manage all aspects of app registrations and enterprise apps except App Proxy.
- **Application Administrator** - Can create and manage all aspects of app registrations and enterprise apps.

> **IMPORTANT**
>
> The above default roles do not get applied when establishing a Reseller Relationship with a Microsoft CSP partner like Evolve IP. The above only applies to newly created 365 tenants.

Global Administrator Access

To provide support and troubleshooting for all of your 365 services the path of least resistance is to provide Evolve IP the **Global Administrator** role. Here are some things to consider:

- Evolve IP will have the ability to access, view and configure your 365 services including your Azure AD.
- If Microsoft restricts our access to certain 365 services in your tenant, we may request a dedicated user account in your 365 tenant for us to use.
- Even though the Global Administrator role is granted to Evolve IP, Microsoft does restrict access to view and export certain datasets in your 365 tenant.

> **NOTE**
>
> In the GDAP model, some permissions within an Azure AD role may be limited by Microsoft. In other words, not all tasks within an Azure AD role can be performed with a GDAP relationship. Details on those limitations can be found in Microsoft's **Workloads Supported by GDAP** article.

Supporting Teams Voice & Direct Routing

The below Azure AD Roles can be selected for a GDAP relationship when supporting an existing Teams Direct Routing configuration. During a direct routing implementation additional roles may be required.

- **Teams Communications Administrator** - **Required** role for creating, managing, and viewing a Teams direct routing configuration, and for provisioning, or deprovisioning, direct routing users. This role is also used to manage Teams voice policies, call queues, and auto attendants.
- **User Administrator** - **Required** role for creating and managing Azure AD users including Teams Resource Accounts used for call queues and auto attendants. This role does not have the permissions to manage MFA, or to create, modify, or disable user accounts in a local Active Directory that is synced to Azure AD.
- **Teams Devices Administrator** - **Optional** role to configure and manage Teams enabled devices (desk phones, conference room devices, etc.).
- **Teams Administrator** - **Optional** role used to manage all aspects of a Teams environment including the management of a Teams direct routing configuration. This role is required to manage Teams IP Phone policies

> **NOTE**
>
> In the GDAP model, some permissions within an Azure AD role may be limited by Microsoft. In other words, not all tasks within an Azure AD role can be performed with a GDAP relationship. Details on those limitations can be found in Microsoft's **Workloads Supported by GDAP** article.

Supporting Other 365 Services

Here's a table defining some additional Azure AD Roles that can be configured in a GDAP relationship.

> **NOTE**
>
> Each role listed in the below table is linked directly the role's description in Microsoft's **Azure AD Built-In Roles** article.

Azure AD Role	Description
Exchange Administrator	Provides global admin permissions within Microsoft Exchange Online, and has the ability to create and manage all Microsoft 365 groups, manage support tickets, and monitor service health.

SharePoint Administrator	Provides global admin permissions within Microsoft SharePoint Online, as well as the ability to create and manage all Microsoft 365 groups, manage support tickets, and monitor service health.
Intune Administrator	Provides global admin permissions within Microsoft Intune Online. Additionally, this role contains the ability to manage users and devices in order to associate policy, as well as create and manage groups.
Application Administrator	Can create and manage all aspects of enterprise applications, application registrations, and application proxy settings.
Billing Administrator	Manages subscriptions, manages support tickets, and monitors service health.
Security Administrator	Provides permissions to manage security-related features in the Microsoft 365 Defender portal, Azure AD Identity Protection, Azure AD Authentication, Azure Information Protection, and Office 365 Security & Compliance Center.
Conditional Access Administrator	Manage Azure Active Directory Conditional Access settings.
Security Reader	Global read-only access on security-related features, including all information in Microsoft 365 security center, Azure Active Directory, Identity Protection, Privileged Identity Management, as well as the ability to read Azure Active Directory sign-in reports and audit logs, and in Office 365 Security & Compliance Center.
Compliance Administrator	Manage compliance-related features in the Microsoft Purview compliance portal, Microsoft 365 admin center, Azure, and Office 365 Security & Compliance Center. Can also manage all features within the Exchange admin center and create support tickets for Azure and Microsoft 365.
Domain Name Administrator	Manage (read, add, verify, update, and delete) domain names.
User Administrator	Provides permissions for creating and managing Azure AD users including user account license assignments & blocking user account sign ins. Cannot manage MFA.
Authentication Administrator	Provides permissions to reset authentication methods (including passwords) for non-administrators and some roles.
Privileged Authentication Administrator	Set or reset any authentication method (including passwords) for any user, including Global Administrators. Delete or restore any users, including Global Administrators.
Privileged Role Administrator	Manage role assignments in Microsoft Entra ID, as well as within Microsoft Entra Privileged Identity Management. Manage all aspects of Privileged Identity Management (PIM) and Administrative Units (AUs).
Helpdesk Administrator	Change passwords, invalidate refresh tokens, create and manage support requests with Microsoft for Azure and Microsoft 365 services, and monitor service health.
Licensing Administrator	Can add, remove, and update license assignments on users, groups (using group-based licensing), and manage the usage location on users.
Groups Administrator	Manage all groups in the organization across various workloads like Teams, SharePoint, Yammer in addition to Outlook.

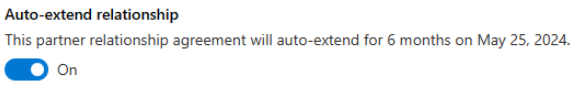
Windows Update Administrator	Provides permissions to create and manage all aspects of Windows Update deployments through the Windows Update for Business deployment service.
Reports Reader	Can view usage reporting data and the reports dashboard in Microsoft 365 admin center.

> **NOTE**
>
> In the GDAP model, some permissions within an Azure AD role may be limited by Microsoft. In other words, not all tasks within an Azure AD role can be performed with a GDAP relationship. Details on those limitations can be found in Microsoft's **Workloads Supported by GDAP** article.

GDAP Relationship Auto-Renewal

Microsoft's GDAP relationship model includes a 6-month (180 day) auto-renewal feature, which will automatically extend a GDAP relationship for 6 months upon its expiration date.

- When enabled, the GDAP relationship will auto-renew every 6 months (180 days).
- When disabled, the GDAP relationship will terminate on its expiration date.
- If a GDAP relationship has auto renewed, and then auto-renewal is disabled afterwards, the GDAP relationship will terminate on its new expiration date.
- GDAP relationships that include the Global Administrator role cannot be auto-renewed. A new GDAP relationship must be created.
- Evolve IP will enable the auto-renewal feature for all GDAP relationships that do not include the Global Administrator role.
- If you don't want the GDAP relationship to auto-renew, please let our Service Delivery or Support teams know.
- Alternatively, you can disable auto-renew for the GDAP relationship in your M365 Admin Center: Settings > Partner Relationships



Accepting a GDAP Relationship

The following section covers the requirements and the process for accepting a GDAP relationship.

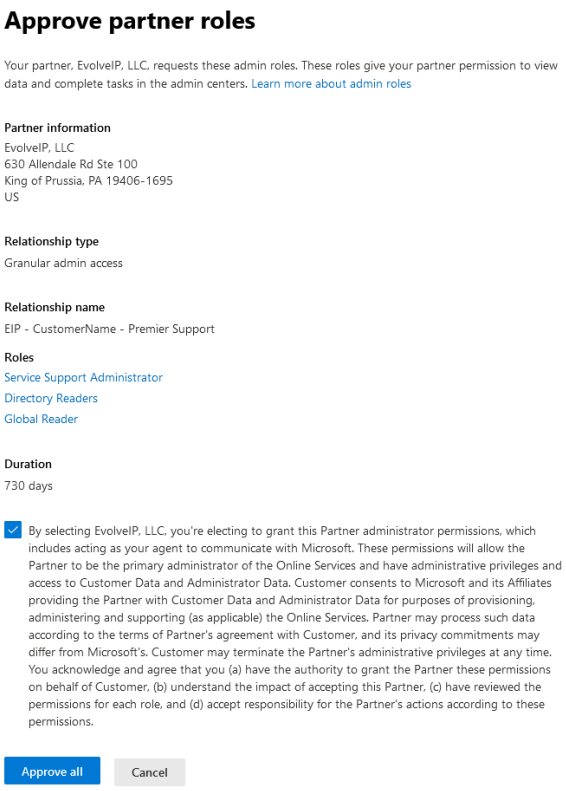
> **NOTE**
>
> Upon the GDAP relationship being established, all user accounts assigned the Global Administrator role in your 365 tenant will be notified by email of the new GDAP relationship.

GDAP Relationship Requirements

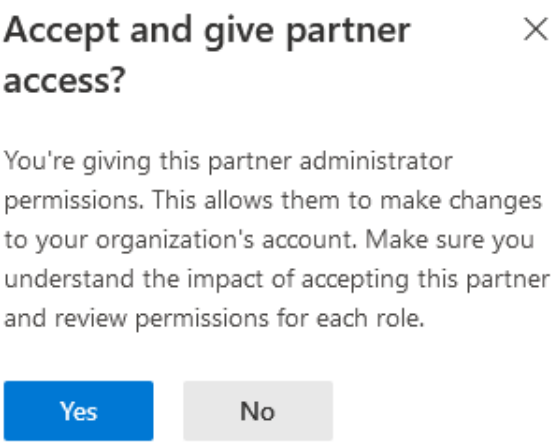
- A user account in your 365 tenant assigned the Global Administrator role.
- A unique configuration URL provided by Evolve IP to start the GDAP relationship process

GDAP Relationship Process

- Open a private/incognito browser window (Microsoft Edge is recommended)
- Paste in the configuration URL provided by the Evolve IP Service Delivery or Support teams
- Sign into your 365 tenant with a user account assigned the Global Administrator role
- Review and approve the GDAP relationship (see example screenshot below)



- Confirm the GDAP relationship (see example screenshot below)



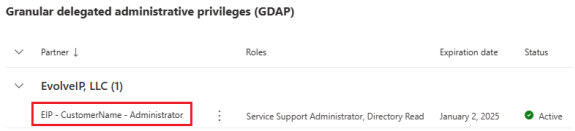
> **NOTE**
>
> Upon the GDAP relationship being established, all user accounts assigned the Global Administrator role will be notified by email of the new GDAP relationship.

Managing an Existing GDAP Relationship

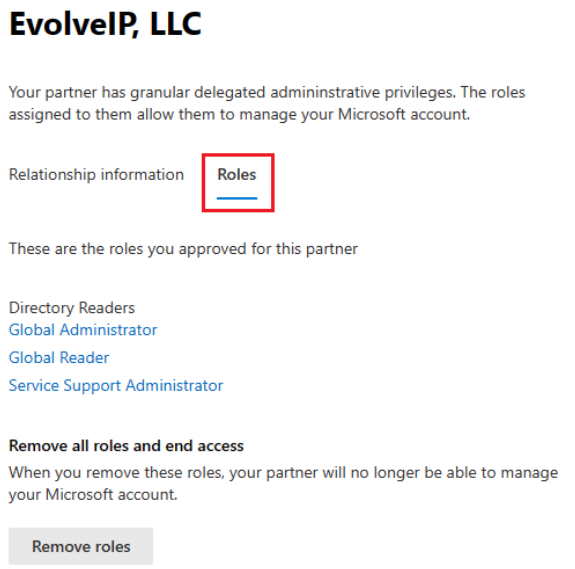
To view and manage a GDAP relationship you must sign into your 365 tenant with a user account assigned the Global Administrator role.

- Sign into your **Microsoft 365 Admin Center**: https://admin.microsoft.com
- Browse to: **Settings** > **Partner Relationships**

- All of your GDAP relationships are listed by partner in the **Granular Delegated Administrative Privileges (GDAP)** section
- To view the details of a GDAP relationship, click on the relationship's name (see example screenshot below)



- To remove a GDAP relationship, select the **Roles** (tab), and click the **Remove Roles** button
- An email notification will be sent to Evolve IP and all of the global admin user accounts in your 365 tenant



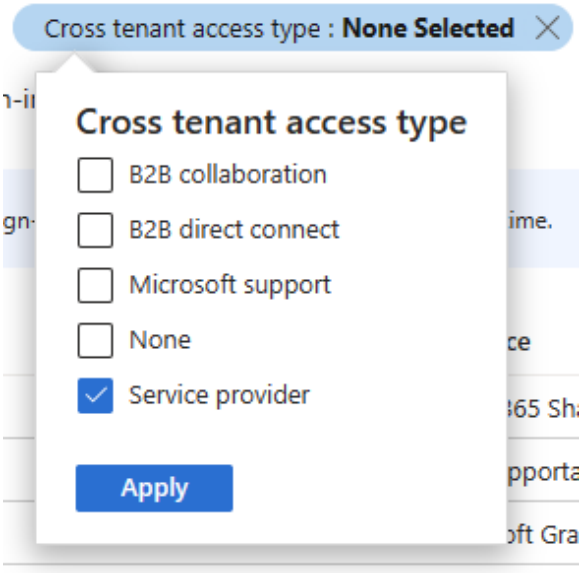
Sign In & Audit Logs

On the partner side, GDAP comes with visibility and activity logs that illustrate the lifecycle of the GDAP relationship. These logs are only generated on the partner side, and Microsoft is continuing to expand upon the GDAP activity items being logged. Refer to Microsoft's **GDAP Partner Activity Logs** article for the latest information.

On your side, you can view partner activity in the **Azure AD sign in logs** & **Azure AD audit logs**. Micros oft recently added the capability to view sign-ins by partners like Evolve IP who have delegated permissions.

You can view those sign-in logs by going to the **Azure AD admin portal**:

- Browse to: **Azure Active Directory** > **Sign-In Logs**
- Select: **User-sign ins (non-interactive)** tab
- Click on: **Add Filters**
- Select: **Cross-Tenant Access Type**
- Click: **Apply**
- Click on: **Cross-Tenant Access Type: None Selected**
- Select: **Service Provider**
- Click: **Apply**



GDAP Service Principal Identities in Azure AD

The first time a GDAP relationship is accepted, there are two Microsoft first-party service principals that get created in your Azure AD tenant.

In this context, "first-party" means that consent is implicitly provided by Microsoft at API call time and the "OAuth 2.0 Access Token" is validated on each API call to enforce role or permissions for the calling identity to managed GDAP relationships.

Name	Application ID
Partner customer delegated administration	2832473f-ec63-45fb-976f-5d45a7d4bb91
Partner customer delegated admin offline processor	a3475900-ccec-4a69-98f5-a65cd5dc5306

Partner customer delegated administration
This service principal is required at the time of the acceptance of a GDAP relationship. The Service Principal sets up the XTAP "service provider" policy and prepares permissions to allow expiration and role management. Only the GDAP SP may set or modify the XTAP policies for Service Providers.

Partner customer delegated admin offline processor
This identity is required for the entire lifecycle of the GDAP relationship, and will be automatically removed at the time the last GDAP relationship ends. The identity's primary permission and function is to manage XTAP policies and access assignments. A customer admin should not attempt to manually remove this identity. The identity implements functions for trusted expiration and role management. The recommended method for a customer to view or remove existing GDAP relationships is in the Microsoft 365 Admin Center as outlined in the previous section.

Frequently Asked Questions

Establishing a GDAP relationship with Evolve IP is optional. If you do not require any level of support and only want us to provide O365/M365 subscription products, you can opt out of the GDAP relationship process. However, we will not be able to open any Microsoft Premier support tickets on your behalf. You will be responsible for opening support tickets with Microsoft.

The duration of a GDAP relationship can be as little as 1 day, and up to a maximum of 2 years.

Yes. You can have multiple GDAP relationships with their own level of access and duration. You can also have GDAP relationships with multiple CSP partners.

No. Microsoft does not allow this. Your GDAP relationships must have a duration of 1-720 days (2 years).

Yes. Microsoft has a 6-month (180 day) auto-renewal process, and Evolve IP enables this by default. However, if a GDAP relationship includes the Global Administrator role, auto-renewal cannot be enabled. A new GDAP relationship must be configured and approved.

Yes. Microsoft sends email notifications to user accounts assigned the Global Administrator role. Notifications are sent out **30** days, **7** days, and **1** day before the GDAP expiration date.

No. There's no change to your existing subscriptions when a GDAP relationship expires.

Yes. You can configure a filter in your Azure AD sign-in and audit logs to view our activity in your 365 tenant.