

Granular Delegated Admin Privileges (GDAP) einrichten

Was ist GDAP?

GDAP ist eine Sicherheitsfunktion, die Partnern gemäß dem Zero-Trust-Cybersicherheitsprotokoll Zugriff mit den *geringsten Rechten* bietet. Es ermöglicht Partnern, einen *granularen und zeitgebundenen Zugriff auf die Workloads ihrer Kunden* in Produktions- und Sandbox-Umgebungen zu konfigurieren. Dieser Zugang mit den geringsten Rechten *muss den Partnern von ihren Kunden explizit gewährt* werden.

Der Zugriff der Partner kann pro Kunde partitioniert werden. *Mit GDAP haben Partner standardmäßig nicht mehr über Admin-Agents Zugriff auf alle Kundenmandanten* in Azure-Abonnements. Stattdessen sind Partner, die Azure verwalten, Teil einer *separaten Sicherheitsgruppe*, die Mitglied der Admin-Agentgruppe ist.

Für die Einrichtung von GDAP ist eine Aufklärung und enge Zusammenarbeit mit Ihrem Endkunden nötig.

Wie richte ich GDAP ein?

Loggen Sie sich zunächst im [Microsoft Partner Center](#) ein, wo Sie als CSP indirekt Reseller Ihre Kunden verwalten. Wählen Sie einen Kunden aus und gehen Sie zum Punkt „Administratorbeziehungen“.



Dort könnten Sie beim Endkunden eine neue Admin Beziehung anfordern.



Request admin relationship

Es empfiehlt sich an dieser Stelle einen Namen anzugeben, mit dem der Endkunde auch was anfangen kann (da er diesem in seinem Admin-Center angezeigt wird) und z. B. Rückschluss auf den Partner und dessen Zugriffs-Recht gibt.

Z. B. könnte dieser Name bei Ihnen lauten „GlobalAdmin_NameIhrerGesellschaft_NameKunde“ oder da es ja um *granulare* Admin Rechte geht „TeamsAdmin_NameIhrerGesellschaft_NameKunde“, wenn Sie konkret nur Rechte für die Administration von Microsoft Teams anfragen möchten.

Name der Administratorbeziehung *

ⓘ Der Name der Administratorbeziehung ist für Kunden sichtbar.

Dauer in Tagen *

Angeforderte Azure AD-Rollen *

Geben Sie die Azure AD-Rollen an, die Sie für Ihren Kunden annehmen möchten.

[Azure AD-Rollen auswählen](#)

Keine Azure AD-Rollen ausgewählt.

Der Zeitraum ist auf max. 2 Jahre begrenzt und muss dann neu bestätigt werden.

Unter „Azure AD-Rollen“ können Sie dann konkret die Rechte anhaken, die Sie beim Endkunden explizit anfragen wollen.

Wählen Sie in der Liste die gewünschten Zugriffsrechte je nach der oberen Bezeichnung aus und gehen Sie auf „speichern“.

Global

Globaler Administrator ▼

Identität

Schicken Sie anschließend die Anforderung an den Endkunden. Es wird Ihnen hierzu ein Link angezeigt, den der globale Admin des Endkunden öffnen und bestätigen muss.

Administratorbeziehungen | Administratorbeziehungen

Senden Sie das Anforderungsformular an einen Ihrer Kunden. Sie können den Text bearbeiten, aber die URL muss unverändert beibehalten werden. Anforderungs-URLs sind nach dem Akzeptieren nicht wiederverwendbar.

Name der Administratorbeziehung
GlobalAdmin_bluechip_ABC

Dauer in Tagen
730

Angeforderte Azure AD-Rollen
Globaler Administrator

Anforderung [In E-Mail öffnen](#) [In die Zwischenablage kopieren](#)

Durch Klicken auf den angezeigten Link können Sie unsere Anforderung akzeptieren, Ihre Produkte unter Verwendung der unten aufgeführten Rollen für den angegebenen Datumsbereich zu verwalten.

Zum Überprüfen und Akzeptieren hier klicken:
<https://admin.microsoft.com/AdminPortal/Home#/partners/invitation/granularAdminRelationships/12c28092-26ac-4234-991a-4b24a37fd0d0-f04ec3e4-0415-44cd-8836-59e730659aae>

Dauer (in Tagen)
730

Azure AD-Rollen:

Globaler Administrator
Kann alle Aspekte von Azure AD und Microsoft-Dienste verwalten, die Azure AD Identitäten verwenden. Wählen Sie diese Rolle nur aus, wenn dies unbedingt erforderlich ist.

Solange dies noch nicht bestätigt wurde, steht der Status auf ausstehend/Pending

| | |
|---|------------------|
| <input type="checkbox"/> GlobalAdmin_bluechip_ABC | Approval pending |
|---|------------------|

So sieht es nun der globale Admin des Endkunden, wenn er den Link aufruft und sich angemeldet hat:

Partnerrollen genehmigen

Ihr Partner, bluechip Computer, fordert diese Administratorrollen an. Diese Rollen erteilen Ihrem Partner die Berechtigung zum Anzeigen von Daten und Abschließen von Aufgaben in den Admin Centern. [Weitere Informationen zu Administratorrollen](#)

Partnerinformationen
bluechip Computer
Geschwister-Scholl-Str. 11a
Meuselwitz, Thüringen 04610
DE

Beziehungstyp
Differenzierter Administratorzugriff

Beziehungsname:
GlobalAdmin_bluechip_ABC


Rollen
[Globaler Administrator](#)

Dauer
730 Tage

Wenn Sie bluechip Computer auswählen, können Sie diesem Partneradministrator Berechtigungen erteilen. Dazu gehört auch, als Ihr Agent für die Kommunikation mit Microsoft zu fungieren. Diese Berechtigungen ermöglichen es dem Partner, der primäre Administrator der Onlinedienste zu sein und über Administratorrechte und Zugriff auf Kundendaten und Administratordaten zu verfügen. Der Kunde stimmt Microsoft und seinen verbundenen Unternehmen zu, die dem Partner Kundendaten und Administratordaten zum Zweck der Bereitstellung, Verwaltung und Unterstützung (sofern zutreffend) der Onlinedienste zur Verfügung stellen. Der Partner kann solche Daten gemäß den Bedingungen der Vereinbarung des Partners mit dem Kunden verarbeiten, und seine Datenschutzverpflichtungen können von denjenigen von Microsoft abweichen. Der Kunde kann die Administratorrechte des Partners jederzeit kündigen. Sie bestätigen und stimmen zu, dass Sie (a) berechtigt sind, dem Partner diese Berechtigungen im Namen des Kunden zu erteilen, (b) die Auswirkungen der Annahme dieses Partners verstehen, (c) die Berechtigungen für jede Rolle überprüft haben und (d) die Verantwortung für die Aktionen des Partners gemäß diesen Berechtigungen übernehmen.

[Alle genehmigen](#) [Abbrechen](#)

Sie erhalten eine Mail, wenn der Endkunde die Anforderung bestätigt hat:



[Redacted] hat die granulare Administratorbeziehung GlobalAdmin_bluechip_ABC akzeptiert

[Redacted] hat die Anfrage für die granulare Administratorbeziehung akzeptiert.

Sie können Ihren Sicherheitsgruppen jetzt Azure AD-Rollen zuweisen, damit diese Gruppen Dienste im Auftrag dieses Kunden verwalten können.

Details zur Administratorbeziehung

| | |
|----------------------------------|--------------------------|
| Kunde: | [Redacted] |
| Name der Administratorbeziehung: | GlobalAdmin_bluechip_ABC |
| Ablaufdatum: | 9/22/2024 |

Auf der Detailseite für Beziehungen in Partner Center finden Sie weitere Informationen.

[In Partner Center anzeigen >](#)

Der Status sollte sich nach der Genehmigung in Ihrer Ansicht auf „aktiv“ umgestellt haben:

| | |
|---|--------|
| <input type="checkbox"/> GlobalAdmin_bluechip_ABC | Active |
|---|--------|

Wenn der Status bestätigt wurde und als aktiv angezeigt wird, klicken Sie darauf. Jetzt müssen Sie den Admin noch einer Sicherheitsgruppe in Ihrer Umgebung hinzufügen (+Add security groups).

| | |
|------------|-----------------------------|
| Status | Active |
| Start date | 4/27/2022, 4:36:21 PM GMT+2 |
| End date | 4/26/2024, 4:36:21 PM GMT+2 |

Azure AD roles: ⓘ

Global administrator

Security groups

Select a security group to modify role assignments available for members of the group. Role assignments can be modified [more about security groups](#).

+ Add security groups - Remove security groups

Name

Done

Es öffnet sich ein Fenster, wo Ihnen Ihre bestehenden Sicherheitsgruppen angezeigt werden. Sofern Sie noch keine haben, legen Sie z. B. eine Gruppe „AdminAgents“ an (dies machen Sie in Ihrem Microsoft 365 Admin Center -> Gruppen -> Sicherheitsgruppen -> fügen Sie die Benutzer Ihrer Umgebung dieser Gruppe hinzu, die Administrative Aufgaben bei Kunden übernehmen sollen). Kehren Sie nach Erstellung der Gruppe ggf. an diese Stelle zurück und wählen Sie nun diese Gruppe aus. Schließen Sie den Vorgang ab.

Security groups

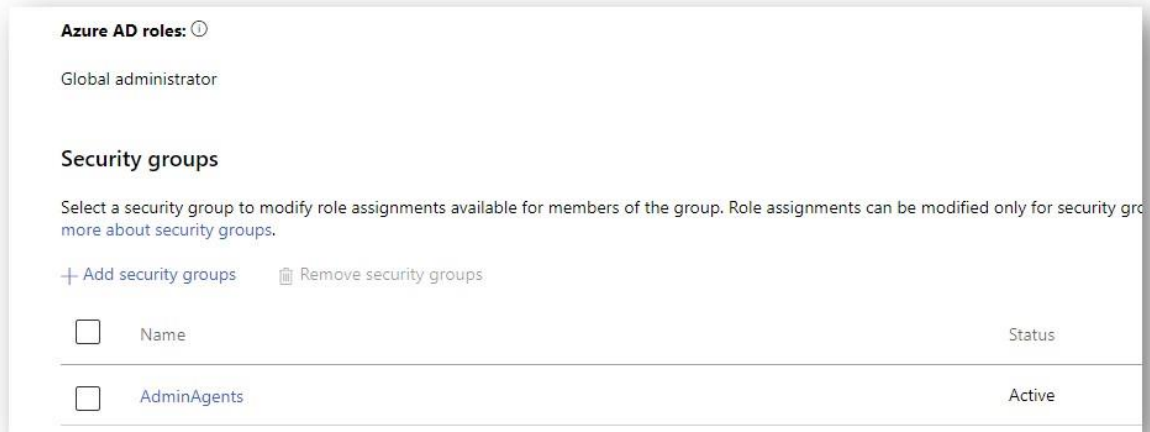
Add security group contributors to this relationship. Click "Next" to assign roles for the selected security group(s).

Search security groups

Security group

AdminAgents

Die ausgewählte Sicherheitsgruppe mit den damit verbundenen Admin-Rechten sollte nun zunächst als ausstehend, später als aktiv angezeigt werden.



Jetzt bestehen GDAP Admin Rechte für den Endkunden-Tenant.

Führen Sie dies bei allen Endkunden-Tenants durch.