Fragen	Antworten
Welche Änderungen werden in diesem FAQ beschrieben?	Dieses FAQ beschreibt Änderungen der Rechte, welche Swisscom auf die Microsoft Cloud Tenants der Kunden im Microsoft Cloud Solution Provider (CSP) Programm hat. Microsoft macht die Änderungen per Januar 2023 obligatorisch für alle CSP Partner weltweit. Ziel der Änderung ist die Erhöhung der Sicherheit mittels Reduktion auf ein Least-Privilege Modell der Rechte, welche Swisscom als CSP Partner auf die Microsoft Cloud Tenants der Kunden hat. Die Änderungen sind entsprechend relevant für alle Swisscom CSP Kunden.
Wofür stehen DAP und GDAP?	DAP steht für *Delegated Administrator Privileges* (delegierte Administrationsrechte). Mithilfe von DAP kann Ihr Microsoft CSP Partner über die Rolle eines globalen Administrators auf Ihre Microsoft-Umgebung zugreifen. Damit erhält Swisscom als CSP-Partner die Möglichkeit, schnell Probleme zu identifizieren, Lösungen zu qualifizieren und schnell Hilfe zu leisten. GDAP steht für *Granular Delegated Administrator Privileges* (differenzierte delegierte Administrationsrechte). Über GDAP kann der Zugang auf eine Microsoft-Umgebung funktional und zeitlich eingeschränkt werden. Damit hat der Kundenservice von Swisscom nur Zugriff auf die Bereiche, welche für die Problembehebung benötigt werden.
Wie verläuft die Verwaltung meiner Microsoft-Umgebung über Swisscom aktuell (*vor* der Umstellung von DAP auf GDAP)?	Der Swisscom Kundenservice hat pauschal via DAP-Zugriff auf Ihre Microsoft Cloud Umgebung. Durch diese Berechtigung ist es möglich, schnell und effizient Support zu leisten. Dieser Zugriff ist allerdings - wie vorab beschrieben - sehr mächtig, womit die Umstellung auf GDAP eine Verbesserung für die Security bedeutet.
Wie verläuft die Verwaltung meiner Microsoft-Umgebung über Swisscom *nach* der Umstellung von DAP auf GDAP?	Der Swisscom Kundenservice hat nur noch reduzierte Zugriffsrechte auf Ihre Microsoft Cloud Umgebung und kann Sie gemäss den reduzierten Rechten bei der Störungsbehebung unterstützen. Damit wird die Sicherheit der Kundenumgebung

	erhöht. Wenn diese Rechte für die Störungsbehebung nicht ausreichen, so kann der Swisscom Kundenservice höhere Rechte (temporär) anfordern. Diese höheren Rechte werden aktiv, wenn Sie diese als Globaler Administrator auf Ihrem Microsoft Cloud Tenant bewilligt haben.
Welche GDAP Rollen gibt es und welche werden für einen effizienten Swisscom Kundenservice benötigt?	Für die verschiedenen Tätigkeiten, die innerhalb einer Microsoft-Umgebung ausgeführt werden können, stehen unterschiedlichste Azure Active Directory (AAD) Rollen zur Verfügung. Damit der Swisscom Kundenservice Sie effizient unterstützen kann, werden folgende GDAP-Rollen benötigt, ersetzen bei allen Kunden die DAP-Rollen und werden bei Neukunden per Default angewandt: • *Dienstsupportadministrator (Service support administrator)*: Diese Rolle hat die Rechte, Support Tickets bei Microsoft zu eröffnen/verwalten und Service Health-Informationen zu lesen. Nur Ihr CSP-Partner ist aktuell technisch berechtigt, über Ihre Kundenumgebung Support-Tickets bei Microsoft zu eröffnen. Dafür benötigt der Swisscom Kundenservice die Rolle des *Service-Support-Administrators*. Ohne diese Rolle kann der Kundenservice keine Entstörungen angehen, die innerhalb der Microsoft-Umgebung ihren Ursprung haben. Gerade bei zeitkritischen Fehlern ist es erforderlich, bestehende Probleme schnell in Richtung Microsoft zu adressieren, um den Prozess der Fehlerbehebung nicht unnötig zu verzögern. • *Benutzeradministrator (User administrator):* Diese Rolle kann alle Aspekte von Benutzenden und Gruppen verwalten, einschliesslich der Kennwortzurücksetzung für eingeschränkte Administrator*innen.

	• *Gruppenadministrator (Group administrator):* Diese Rolle kann sowohl Gruppeneinstellungen verwalten als auch Aktivitäts- und Überwachungsberichte von Gruppen anzeigen. • *Lizenzadministrator (Licence administrator):* Diese Rolle hat die Möglichkeit zum Zuweisen, Entfernen und Aktualisieren von Lizenzzuweisungen. Für Lizenzbuchungen und -zuweisungen durch den Swisscom Kundenservice im Auftrag des Kunden ist es wichtig, diese Berechtigungen zu haben. Ausserdem können ohne diese Berechtigungen nicht alle Aktivitäten über den Swisscom Marketplace reibungslos durchgeführt werden. • *Globaler Leser (Global reader):* Diese Rolle hat die gleichen Leseberechtigungen wie ein globaler Administrator, kann jedoch keine Aktualisierungen durchführen. Der globale Leser erlaubt einen lesenden Zugriff auf Ihre Microsoft 365- bzw. Office 365-Umgebung, um mögliche Störungsursachen schnell identifizieren zu können. Diese lesende Rolle hat, wie der Name schon vermittelt, keinerlei Schreibrechte und kann somit keine Änderungen in der Umgebung vornehmen. Sie sind ausserdem in der Einsicht eingeschränkt. E-Mail- oder OneDrive-Inhalte können beispielsweise mit diesen Rechten nicht eingesehen werden. • *Verzeichnisleseberechtigte (Directory readers):* Diese Rolle kann grundlegende Verzeichnisinformationen lesen und wird häufig zum Gewähren von Verzeichnislesezugriff für Anwendungen und Gäste verwendet. Der Verzeichnisleser wird benötigt, um eine Microsoft Azure Subscription

	einsehen zu können, damitschnelle Hilfe bei Problemen mit Microsoft Azure geleistet werden kann. Zusätzlich wird diese Rolle für eine reibungslose Integration mit dem Swisscom Marketplace benötigt. • *Administrator für privilegierte Authentifizierung (Privileged authentication administrator)*: Diese Rolle kann ein Passwort-Reset des Administrierenden der Kundenumgebung durchführen. Gerade bei kleineren Kunden kommt es häufig vor, dass das Administrator-Passwort nicht mehr bekannt ist. Damit der Swisscom Kundenservice in der Lage ist, dieses für Sie zurückzusetzen, wird diese Rolle benötigt. Ist diese Rolle nicht vorhanden, ist es leider nur über einen sehr langwierigen Support-Prozess bei Microsoft möglich, das Administratorpasswort wiederherzustellen. Ohne den Zugang zu Ihrem Admin-Account können administrative Aufgaben, wie das Anlegen neuer Benutzer, die Zuweisung von Lizenzen oder das Entfernen von Benutzern nicht mehr ausgeführt werden. Weil diese Rolle sehr einflussreich ist, wird sie innerhalb Swisscom weniger als fünf Mitarbeiter*innen zugeordnet. Damit soll der Missbrauch auf ein absolutes Minimum reduziert werden. • *Cloudanwendungsadministrator (Cloud application administrator)*: Diese Rolle kann sämtliche Aspekte von App-Registrierungen und Enterprise-Apps erstellen und verwalten. Diese Rolle wird für eine reibungslose Integration mit dem Swisscom Marketplace benötigt. Weitere Rollen:

	• Bei Swisscom managed Service Kunden benötigt das Swisscom Betriebsteam je nach Ausprägung des managed Services unterschiedliche permanente, höhere Rechte. • Für die Einrichtung Ihrer Kundenumgebung oder die Problembehebung benötigt der Swisscom Kundenservice in der Regel temporär höhere Rechte auf Ihrer Umgebung. Dabei wird Ihnen durch den Kundenservice eine individuelle Anfrage mit den benötigten Rollen und der benötigten Dauer gestellt. Erst nachdem Sie dieser zugestimmt haben, kann das Swisscom Team auf die angeforderten Bereiche zugreifen und den Service erbringen. • Auf der verlinkten Seite finden Sie eine Übersicht aller vorhandenen Azure AD-Rollen. Ausserdem bietet Microsoft eine weitere Übersicht, in der die Aufgaben nach den entsprechenden AAD-Rollen dargestellt werden.
Wie lange werden die Rechte vergeben?	Zum aktuellen Zeitpunkt können GDAP-Rechte für die Dauer von einem bis zu 730 Tagen vergeben werden. Anschliessend ist eine aktive Erneuerung notwendig.
Wann erfolgt die Umstellung auf GDAP?	Wenn Sie aktuell eine bestehende DAP-Beziehung mit Swisscom haben, wird diese bis voraussichtlich Ende des Jahres 2022 auf das beschriebene GDAP Rollen-Set umgestellt. Damit ist gewährleistet, dass auch Ihr Zugriff unter dem aktuell besten Sicherheitskonzept läuft, und dass der Kundenservice in gewohnter Qualität für Sie da sein kann. Danach werden für neue Swisscom CSP Kunden direkt die GDAP Rollen angewandt.
Was passiert, wenn ich nicht auf GDAP umstellen will?	Microsoft hat angekündigt, bis Ende Januar 2023 inaktive DAP-Beziehungen (länger als 90 Tage nicht in Gebrauch) zu entfernen. Damit hätte der Kundenservice von Swisscom keine Berechtigungen mehr. Es könnten dann zum Beispiel über Swisscom keine Supporttickets bei Microsoft mehr eröffnet werden. Auch im

	Lizenzbestellportal, dem Swisscom Marketplace, könnten dann nicht mehr alle Aktivitäten durchgeführt werden. Aus diesem Grund wird Swisscom vorhandene DAP-Beziehungen automatisch auf das beschriebene Rollen-Set umstellen. Damit wird die Sicherheit für Ihre Umgebung erhöht und Swisscom kann den Service weiterhin gewährleisten.
Ich habe die DAP-Beziehung bereits entfernt. Werde ich nun auf GDAP umgestellt?	Nein, das passiert nicht. Die Umstellung auf GDAP erfordert eine bestehende DAP Beziehung. Sie können auch ohne DAP Beziehung von GDAP profitieren. Swisscom erstellt bei Bedarf eine GDAP Anfrage, welche Sie im Microsoft 365 Admin Center bestätigen müssen. Die Empfehlung ist die Genehmigung eines minimalen Rollen-Sets für einen reibungslosen Ablauf des Kundenservice und der Buchungen über den Swisscom Marketplace (siehe die oben genannten Rollen). Es ist aber Ihre alleinige Entscheidung, wem Sie welchen Zugriff auf Ihre Umgebung gewähren.
Kann ich mit GDAP die Foreign Principal Rolle von Swisscom aus meinem Microsoft Azure Abonnement entfernen?	Nein. Diese Rolle ist weiterhin Grundvoraussetzung für den Bezug von Microsoft Azure über Swisscom und ist eine Rolle auf Azure, welche separat gesteuert wird und nichts mit den Azure Active Directory basierten Rollen (GDAP) zu tun hat. Dass diese Azure Rolle weiterhin benötigt wird, hat mit dem aktuellen Produktmodell von Microsoft zu tun. Eine Entfernung dieser Rolle führt zu einer Kündigung Ihrer Azure-Subscription(s) durch Swisscom. Diese Regelung ist so auch in unseren Vertragsbedingungen festgehalten.
Wie kann ich die Zugriffsberechtigungen durch den Swisscom Kundenservice oder andere CSP Partner einsehen und verwalten?	Um einen aktuellen Stand über die Zugriffsberechtigungen auf Ihre Microsoft-Umgebung einzusehen, loggen Sie sich mit Ihrem Administrator im Microsoft 365-Admincenter ein. Dort können Sie auf der linken Seite unter dem Reiter „Einstellungen“ > „Partnerbeziehungen“ Ihre gewährten Zugriffe einsehen und verwalten. Hinweis: Bevor Sie an dieser Stelle Berechtigungen entziehen, bedenken Sie bitte, welche Konsequenzen dies möglicherweise für Buchungsmöglichkeiten sowie die Erbringung des

	Swisscom Kundenservices hat. Jede Anfrage für eine Zugriffsberechtigung wird durch Ihren CSP-Partner erstellt, Sie können diese nicht selbst initiieren. Über den Link, der durch Ihren Partner zugesandt wird, können Sie eine neue GDAP-Beziehung in Ihrem Microsoft 365-Admincenter genehmigen.
Welche weiteren Sicherheitsmassnahmen sind sinnvoll, um meine Microsoft-Umgebung zu schützen?	Über Azure Active Directory und die Security-Funktionen von Microsoft 365 können Sie grundlegende Sicherheitsmassnahmen aktivieren, wie zum Beispiel Multifaktor-Authentifizierung (MFA, wir empfehlen das für alle Mitarbeiter*innen anzuwenden) oder Conditional Access Policies (bedingter Zugriff Richtlinien), um die Zugänge Ihrer Mitarbeiter*innen besser abzusichern. Darüber hinaus besteht die Möglichkeit, zusätzliche Lösungen von Microsoft zu erwerben, zum Beispiel die Defender Familie. Diese bieten erweiterte Funktionen für eine bessere Sicherheit. Empfehlungen für Security Konfigurationen vom US Department of Homeland Security finden Sie hier: https://www.us-cert.gov/ncas/analysis-reports/AR19-133A Ausserdem unterstützen Sie die Expert*innen von Swisscom (und unseren Partnern) rund um die Sicherheit Ihrer ICT Umgebung, zum Beispiel bei der Umsetzung von Sicherheitseinstellungen der Microsoft Sicherheitsfunktionen.