Questions	Réponses
Quelles modifications sont décrites dans cette FAQ?	Cette FAQ décrit les modifications apportées aux droits dont dispose Swisscom sur les Microsoft Cloud Tenants des clients au sein du programme Cloud Solution Provider (CSP) de Microsoft. Microsoft rendra les modifications obligatoires pour tous les partenaires CSP dans le monde entier à compter de janvier 2023. L'objectif de la modification est de renforcer la sécurité en réduisant à un modèle Least-Privilege les droits dont dispose Swisscom en tant que partenaire CSP sur les Microsoft Cloud Tenants des clients. Les modifications sont donc pertinentes pour tous les clients CSP de Swisscom.
Que signifient les abréviations DAP et GDAP?	DAP signifie *Delegated Administrator Privileges* (droits d'administration délégués). À l'aide des DAP, votre partenaire CSP Microsoft peut accéder dans le rôle d'administrateur global à votre environnement Microsoft. Swisscom a ainsi, en tant que partenaire CSP, la possibilité d'identifier rapidement les problèmes, de trouver des solutions et d'apporter rapidement son aide. GDAP signifie *Granular Delegated Administrator Privileges* (droits d'administration délégués différenciés). Grâce aux GDAP, l'accès à un environnement Microsoft peut être limité sur le plan fonctionnel et temporel. Le service à la clientèle de Swisscom n'a ainsi accès qu'aux secteurs requis pour le dépannage.
Comment se déroule actuellement la gestion de mon environnement Microsoft via Swisscom (*avant* la migration de DAP vers GDAP)?	Le service à la clientèle de Swisscom dispose d'un accès aléatoire à votre environnement Microsoft Cloud grâce aux DAP. Avec cette autorisation, il est possible d'apporter une assistance rapide et efficace. Cet accès est cependant - tel que décrit ci-dessus - très puissant, ce qui fait que la migration vers GDAP entraîne une amélioration de la sécurité.
Comment se déroule la gestion de mon environnement Microsoft via Swisscom (*après* la migration de DAP vers GDAP)?	Le service à la clientèle de Swisscom ne dispose plus que de droits d'accès limités à votre environnement Microsoft Cloud et peut vous aider à la suppression des perturbations en fonction des droits limités. La sécurité de l'environnement

	client est ainsi renforcée. Si ces droits ne suffisent pas pour la suppression des perturbations, le service à la clientèle de Swisscom peut demander (temporairement) des droits supérieurs. Ces droits supérieurs ne deviendront actifs que si, en tant qu'administrateur global, vous les avez autorisés sur votre Microsoft Cloud Tenant.
Quels rôles GDAP existe-t-il et quels sont ceux dont le service à la clientèle de Swisscom a besoin pour être efficace?	Pour les différentes activités pouvant être exécutées au sein d'un environnement Microsoft, divers rôles AAD (Azure Active Directory) sont disponibles. Pour que le service à la clientèle de Swisscom puisse apporter une aide efficace, les rôles GDAP suivants sont nécessaires. Ils remplacent les rôles DAP pour tous les clients et sont appliqués par défaut pour les nouveaux clients: • *Administrateur du support technique (Service support administrator)*: ce rôle dispose des droits pour ouvrir/gérer des tickets d'assistance auprès de Microsoft et pour lire les informations sur l'intégrité du service. Seul votre partenaire CSP dispose actuellement des droits techniques pour ouvrir des tickets d'assistance auprès de Microsoft via votre environnement client. Pour cela, le service à la clientèle de Swisscom doit avoir le rôle d'*administrateur du support technique*. Sans ce rôle, le service à la clientèle ne peut pas traiter les incidents qui proviennent de l'environnement Microsoft. En cas d'erreurs critiques en particulier, il est nécessaire d'adresser rapidement les problèmes existants à Microsoft afin de ne pas retarder inutilement le processus de dépannage. • *Administrateur des utilisateurs (User administrator):* ce rôle peut gérer tous les aspects des utilisateurs et groupes, y compris la réinitialisation des mots de passe pour les administrateurs limités.

	• *Administrateur des groupes (Group administrator):* ce rôle peut gérer aussi bien les paramètres de groupes que les rapports d'activité et de surveillance des groupes. • *Administrateur de licences (Licence administrator):* ce rôle a la possibilité d'attribuer, de supprimer et de mettre à jour les attributions de licences. Pour les réservations et attributions de licences par le service à la clientèle de Swisscom au nom du client, il est important de disposer de ces autorisations. En outre, les activités ne peuvent pas toutes être réalisées sans problème sur la Swisscom Marketplace sans ces autorisations. • *Lecteur global (Global reader):* ce rôle dispose des mêmes autorisations en lecture qu'un administrateur global, mais ne peut pas réaliser de mise à jour. Le lecteur global permet un accès en lecture à votre environnement Microsoft 365 ou Office 365 afin de pouvoir identifier rapidement les causes possibles de dérangements. Comme son nom l'indique, ce rôle ne dispose aucunement de droits d'écriture et ne peut donc procéder à aucune modification dans l'environnement. Les droits sont également limités en matière de consultation. Les contenus d'e-mails ou OneDrive ne peuvent notamment pas être consultés avec ces droits. • *Lecteurs de répertoires (Directory readers):* ce rôle peut lire des informations fondamentales sur les répertoires et est fréquemment utilisé pour accorder l'accès en lecture aux répertoires pour les applications et les hôtes. Le rôle de lecteur de répertoires est indispensable pour pouvoir consulter un

	abonnement à Microsoft Azure, afin de garantir une aide rapide en cas de problèmes avec Microsoft Azure. De plus, ce rôle est nécessaire pour une intégration fluide dans la Swisscom Marketplace. • *Administrateur d'authentification privilégiée (Privileged authentication administrator)*: ce rôle peut réinitialiser le mot de passe de l'administrateur de l'environnement client. Pour les petits clients notamment, il arrive souvent que ce mot de passe soit oublié. Ce rôle est indispensable pour que le service à la clientèle de Swisscom soit en mesure de réinitialiser le mot de passe. En l'absence de ce rôle, il faut malheureusement passer par un processus d'assistance chronophage auprès de Microsoft pour pouvoir rénitialiser le mot de passe de l'administrateur. Sans l'accès à votre compte d'administrateur, les tâches administratives comme la création de nouveaux utilisateurs, l'attributation de licences ou la suppression d'utilisateurs seront impossibles. Parce que ce rôle a beaucoup d'influence, il est attribué au sein de Swisscom à moins de cinq collaborateurs. Les abus sont ainsi réduits au minimum. • *Administrateur d'application cloud (Cloud application administrator)*: ce rôle peut gérer tous les aspects de l'enregistrement des applications et les applications d'entreprise. Ce rôle est nécessaire pour une intégration fluide dans la Swisscom Marketplace. Autres rôles: • Pour les clients des Swisscom Managed Services, l'équipe d'exploitation de Swisscom a besoin selon la version des

	Managed Services de différents rôles supérieurs permanents. • Pour la configuration de votre environnement client ou le dépannage, le service à la clientèle de Swisscom a temporairement besoin de droits supérieurs sur votre environnement. Le service à la clientèle vous envoie alors une demande individuelle avec les rôles nécessaires et la durée requise. Ce n'est qu'après avoir obtenu votre accord que l'équipe de Swisscom peut accéder aux secteurs demandés et fournir le service. • Vous trouverez un aperçu de tous les rôles Azure AD existants sur la page mise en lien. En outre, Microsoft offre une autre vue d'ensemble dans laquelle les tâches sont illustrées en fonction des rôles AAD correspondants.
Pendant combien de temps les droits sont-ils accordés?	Actuellement, les droits GDAP peuvent être accordés pendant une durée de un à 730 jours. Un renouvellement actif s'impose ensuite.
Quand aura lieu la migration vers GDAP?	Si vous disposez actuellement d'une relation DAP avec Swisscom, celle-ci sera migrée d'ici la fin de l'année 2022 vers le jeu de rôles GDAP décrit. Cela garantira que votre accès fonctionne selon le meilleur concept de sécurité et que le service à la clientèle soit à votre disposition dans la qualité habituelle. Ensuite, les rôles GDAP seront appliqués directement pour les nouveaux clients CSP de Swisscom.
Que se passera-t-il si je ne souhaite pas migrer vers GDAP?	Microsoft a annoncé que les relations DAP inactives (inutilisées depuis plus de 90 jours) seront supprimées d'ici fin janvier 2023. Le service à la clientèle de Swisscom n'aurait alors plus d'autorisations. Il serait alors par exemple impossible d'ouvrir des tickets d'assistance via Swisscom auprès de Microsoft. Sur le portail de commande des licences, la Swisscom Marketplace, il ne serait plus non plus possible de réaliser toutes les activités. Pour cette raison, Swisscom migrera toutes les relations DAP existantes automatiquement vers le jeu de rôles décrit. La

	sécurité de votre environnement sera ainsi renforcé et Swisscom pourra continuer à garantir le service.
J'ai déjà supprimé la relation DAP. Vais-je maintenant être migré vers GDAP?	Non. La migration vers GDAP requiert une relation DAP existante. Vous pouvez aussi bénéficier de GDAP sans relation DAP. Si nécessaire, Swisscom émet une demande GDAP que vous devez valider dans le Microsoft 365 Admin Center. Il est recommandé d'approuver un jeu de rôles minimal pour un fonctionnement optimal du service à la clientèle et des réservations fluides via la Swisscom Marketplace (voir les rôles décrits ci-dessus). Cependant, libre à vous de décider à qui vous accordez quel accès à votre environnement.
Avec GDAP, puis-je supprimer le rôle Foreign Principal de Swisscom de mon abonnement Microsoft Azure?	Non. Ce rôle est la condition préalable pour acheter Microsoft Azure via Swisscom. Il est géré séparément sur Azure et n'a rien à voir avec les rôles basés sur Azure Active Directory (GDAP). Le fait que ce rôle Azure est toujours nécessaire a quelque chose à voir avec le modèle de produit actuel de Microsoft. La suppression de ce rôle entraîne la résiliation de votre/vos abonnement(s) Azure via Swisscom. Cette règle est inscrite telle quelle dans nos conditions contractuelles.
Comment puis-je consulter et gérer les droits d'accès par l'intermédiaire du service à la clientèle de Swisscom ou d'autres partenaires CSP?	Pour consulter l'état actuel des droits d'accès à votre environnement Microsoft, connectez-vous avec vos identifiants d'administrateur au Microsoft 365-Admincenter. Là vous pouvez consulter et gérer les accès qui vous sont accordés sur la page gauche sous l'onglet «Paramètres» > «Relations avec les partenaires». Remarque: avant de supprimer des autorisations à ce stade, veuillez réfléchir aux conséquences que cela peut avoir sur les options de réservation et la fourniture du service à la clientèle de Swisscom. Toute demande de droit d'accès est créée par votre partenaire CSP. Vous ne pouvez pas l'initier vous-même. Via le lien que votre partenaire vous a envoyé, vous pouvez approuver une nouvelle relation GDAP dans votre Microsoft 365-Admincenter.

Quelles autres mesures de sécurité sont judicieuses pour protéger mon environnement Microsoft?	Via Azure Active Directory et les fonctions de sécurité de Microsoft 365, vous pouvez activer les mesures de sécurité de base, comme par exemple l'authentification à plusieurs facteurs (MFA, nous recommandons de l'appliquer pour tous les collaborateurs) ou Conditional Access Policies (directives d'accès sous condition) afin de mieux garantir les accès de vos collaborateurs. Par ailleurs, il est possible d'acquérir des solutions supplémentaires de Microsoft, par exemple la gamme Defender. Celle-ci offre des fonctions avancées pour garantir une meilleure sécurité. Vous trouverez des recommandations pour les configurations de la sécurité du Département américain de la sécurité intérieure ici: https://www.us-cert.gov/ncas/analysis-reports/AR19-133A En outre, les experts de Swisscom (et nos partenaires) vous conseillent sur la sécurité de votre environnement TIC, notamment pour la mise en œuvre de paramètres de sécurité des fonctions Microsoft.