



Domande	Risposte
Quali modifiche vengono descritte in queste FAQ?	Queste FAQ descrivono le modifiche dei diritti che Swisscom detiene sui Microsoft Cloud Tenant dei clienti nel programma Microsoft Cloud Solution Provider (CSP). Microsoft rende le modifiche obbligatorie in tutto il mondo per tutti i partner CSP da gennaio 2023. L'obiettivo della modifica è l'aumento della sicurezza attraverso la riduzione a un modello Least Privilege dei diritti che Swisscom ha in quanto partner CSP sui Microsoft Cloud Tenant dei clienti. Le modifiche sono rilevanti per tutti i clienti Swisscom CSP.
Cosa significa DAP e GDAP?	<p>DAP significa <i>Delegated Administrator Privileges</i> (diritti di amministrazione delegati). Mediante i DAP il vostro partner Microsoft CSP può accedere con il ruolo di amministratore globale al vostro ambiente Microsoft. Swisscom in quanto partner CSP ha pertanto la possibilità di identificare rapidamente i problemi, di qualificare le risposte e di venire subito in aiuto.</p> <p>GDAP significa <i>Granular Delegated Administrator Privileges</i> (diritti di amministrazione delegati differenziati). Mediante i GDAP l'accesso a un ambiente Microsoft può essere limitato dal punto di vista funzionale e temporale. Il servizio alla clientela di Swisscom ha quindi solo accesso ai settori necessari per la risoluzione dei problemi.</p>
Come funziona al momento la gestione del mio ambiente Microsoft mediante Swisscom (<i>prima</i> del passaggio da DAP a GDAP)?	<p>Il servizio alla clientela di Swisscom ha in generale accesso mediante DAP al vostro ambiente Microsoft Cloud. Tramite questa autorizzazione è possibile prestare supporto in modo rapido ed efficiente.</p> <p>Tuttavia, questo accesso, come descritto, è molto incisivo, ragion per cui il passaggio a GDAP costituisce un miglioramento per la Security.</p>
Come funziona al momento la gestione del mio ambiente Microsoft mediante Swisscom (<i>dopo</i> il passaggio da DAP a GDAP)?	Il servizio alla clientela di Swisscom detiene diritti di accesso al vostro ambiente Microsoft Cloud solo in misura limitata e può supportarvi nell'eliminazione dei guasti in funzione dei diritti ridotti. In questo modo la sicurezza dell'ambiente clienti viene aumentata. Se questi diritti non sono sufficienti per l'eliminazione del guasto, il servizio



	alla clientela di Swisscom può richiedere (temporaneamente) diritti maggiori. Questi maggior diritti diventano attivi se li avete autorizzati come amministratore globale nel vostro Microsoft Cloud Tenant.
Quali ruoli GDAP esistono e quali sono necessari per un servizio alla clientela efficiente da parte di Swisscom?	<p>Per le diverse attività che possono essere svolte nell'ambito di un ambiente Microsoft sono disponibili i ruoli Azure Active Directory (AAD) più disparati. Affinché il servizio alla clientela Swisscom possa supportarvi in modo efficiente, sono necessari i seguenti ruoli GDAP, che sostituiranno i ruoli DAP in tutti i clienti e saranno utilizzati di default con i nuovi clienti:</p> <ul style="list-style-type: none">• <i>Amministratore Service Support (Service support administrator)</i>: questo ruolo detiene i diritti di aprire/gestire Support Ticket in Microsoft e di leggere informazioni Service Health. <p>Solo il vostro partner CSP al momento è autorizzato tecnicamente ad aprire in Microsoft dei Support Ticket dal vostro ambiente clienti. Per farlo, il servizio alla clientela Swisscom ha bisogno del ruolo di <i>amministratore del Service Support</i>. Senza questo ruolo il servizio alla clientela non può provvedere a eliminare i guasti derivanti dall'ambiente Microsoft. Soprattutto in caso di errori urgenti è necessario affrontare rapidamente i problemi esistenti con l'ausilio di Microsoft, al fine di non ritardare inutilmente il processo di eliminazione degli errori.</p> <ul style="list-style-type: none">• <i>Amministratore utente (User administrator)</i>: questo ruolo può gestire tutti gli aspetti degli utenti e dei gruppi, compreso il ripristino della password per le amministratrici e gli amministratori limitati.• <i>Amministratore di gruppo (Group administrator)</i>: questo ruolo può sia gestire le impostazioni di gruppo sia



	<p>visualizzare rapporti di attività e monitoraggio dei gruppi.</p> <ul style="list-style-type: none">• <i>Amministratore licenze (Licence administrator)</i>: questo ruolo ha la possibilità di assegnare, rimuovere e aggiornare le assegnazioni delle licenze. <p>Perché il servizio alla clientela Swisscom possa prenotare e assegnare le licenze per conto del cliente, è importante avere queste autorizzazioni. Inoltre, senza queste autorizzazioni non è possibile svolgere correttamente tutte le attività dallo Swisscom Marketplace.</p> <ul style="list-style-type: none">• <i>Lettore globale (Global reader)</i>: questo ruolo ha gli stessi diritti di lettura di un amministratore globale, ma non è in grado di fare gli aggiornamenti. <p>Il lettore globale consente un accesso con diritto di lettura nel vostro ambiente Microsoft 365 o Office 365, per poter identificare rapidamente possibili cause di guasto. Questo ruolo di lettura, come già dice il nome, non contempla alcun diritto di scrittura e non può pertanto effettuare alcuna modifica nell'ambiente. Hanno inoltre delle limitazioni a livello di visualizzazione. Per esempio con questi diritti non possono visualizzare i contenuti di e-mail e OneDrive.</p> <ul style="list-style-type: none">• <i>Lettore directory (Directory readers)</i>: questo ruolo può leggere informazioni di base relativi alle directory e viene utilizzato spesso per dare l'accesso alle directory per applicazioni e ospiti. <p>Il lettore directory viene utilizzato per poter vedere una sottoscrizione Microsoft Azure, affinché sia possibile prestare un rapido aiuto in caso di problemi con Microsoft Azure. Inoltre, questo ruolo è necessario per assicurare un'integrazione corretta con Swisscom Marketplace.</p>
--	--



	<ul style="list-style-type: none">• <i>Amministratore per autenticazione privilegiata (Privileged authentication administrator):</i> Questo ruolo può svolgere un reset della password dell'amministratore dell'ambiente clienti. Soprattutto con i clienti più piccoli succede spesso che non si conosca più la password dell'amministratore. Affinché il servizio alla clientela Swisscom sia in grado di ripristinarla per voi, questo ruolo è necessario. In assenza di questo ruolo, il ripristino della password dell'amministratore è possibile solo attraverso una complessa procedura di supporto in Microsoft. Senza l'accesso al vostro account Admin i compiti amministrativi, tra cui l'impostazione di nuovi utenti, l'assegnazione di licenze o la rimozione degli utenti, non può più essere eseguita. Essendo molto influente, questo ruolo viene assegnato in Swisscom a meno di cinque collaboratrici o collaboratori. In questo modo è possibile ridurre al minimo gli eventuali abusi.• <i>Amministratore applicazione cloud (Cloud application administrator):</i> questo ruolo può creare e gestire tutti gli aspetti delle registrazioni delle app e delle app Enterprise. Questo ruolo è necessario per assicurare un'integrazione corretta con Swisscom Marketplace. <p>Altri ruoli:</p> <ul style="list-style-type: none">• con Swisscom managed Service Clienti, il team di gestione Swisscom ha bisogno, a seconda della configurazione del managed service, di diversi diritti permanenti di maggiore entità.• Per l'allestimento del vostro ambiente clienti o per la risoluzione di problemi, il servizio alla clientela Swisscom ha bisogno solitamente di diritti
--	---



	<p>temporaneamente maggiori nel vostro ambiente. Attraverso il servizio alla clientela vi viene inviata una richiesta individuale con i ruoli e la durata necessari. Solo dopo il vostro consenso il team Swisscom può accedere ai settori necessari ed erogare il servizio.</p> <ul style="list-style-type: none">• Nella pagina collegata con il link trovate una panoramica di tutti i ruoli AD Azure disponibili. Inoltre, Microsoft offre un'altra panoramica in cui vengono rappresentati i compiti secondo i relativi ruoli AAD.
Per quanto tempo vengono assegnati i diritti?	Al momento i diritti GDAP possono essere assegnati per la durata che va da uno a 730 giorni. Successivamente è necessario un ruolo attivo.
Quando avviene il passaggio a GDAP?	Se al momento avete una relazione DAP in essere con Swisscom, questa passerà ai ruoli GDAP descritti presumibilmente entro la fine del 2022. In questo modo potete essere certi che anche il vostro accesso avviene nel rispetto degli standard di sicurezza al momento più rigorosi, e che il vostro servizio alla clientela può essere al vostro fianco nella consueta qualità. Successivamente per i nuovi clienti Swisscom CSP saranno utilizzati direttamente i ruoli GDAP.
Cosa succede se non voglio passare a GDAP?	Microsoft ha annunciato di rimuovere le relazioni DAP inattive (inutilizzate da più di 90 giorni) entro la fine di gennaio 2023. In questo modo il servizio alla clientela Swisscom non ha più autorizzazioni. Per esempio, Swisscom non potrebbe più aprire dei Support Ticket in Microsoft. Anche nel portale di ordinazione delle licenze, Swisscom Marketplace, non potrebbero essere più svolte tutte le attività. Per questa ragione Swisscom trasformerà le relazioni DAP presenti automaticamente nel set di ruoli descritto. In questo modo viene aumentata la sicurezza del vostro ambiente e Swisscom potrà continuare a offrire il servizio.
Ho già rimosso la relazione DAP. Passerò ora a GDAP?	No, non succederà. Il passaggio a GDAP richiede una relazione DAP in essere. Ma anche senza relazione DAP potete beneficiare di GDAP.



	<p>Swisscom redige all'occorrenza una richiesta GDAP, che voi dovete confermare nel Microsoft 365 Admin Center. Si consiglia di autorizzare un set di ruoli minimo per il corretto svolgimento del servizio alla clientela e delle prenotazioni mediante Swisscom Marketplace (vedi i ruoli sopraccitati). Ma sta unicamente a voi decidere a chi concedere quale accesso al vostro ambiente.</p>
<p>Con GDAP posso rimuovere il ruolo Foreign Principal di Swisscom dal mio abbonamento Microsoft Azure?</p>	<p>No. Questo ruolo continua a essere un presupposto di base per l'acquisizione di Microsoft Azure mediante Swisscom ed è un ruolo su Azure che viene gestito separatamente e non ha nulla a che vedere con i ruoli basati sulla Azure Active Directory (GDAP). Il fatto che questo modello di Azure continui a essere utilizzato ha a che vedere con l'attuale modello di prodotto di Microsoft. Una rimozione di questo ruolo comporta la disdetta della vostra sottoscrizione di Azure da parte di Swisscom. Questa regola è stabilita anche nelle nostre condizioni contrattuali.</p>
<p>Come posso visualizzare e gestire le autorizzazioni d'accesso da parte del servizio alla clientela Swisscom o di altri partner CSP?</p>	<p>Per avere una panoramica delle autorizzazioni d'accesso nel vostro ambiente Microsoft, effettuate il login con il vostro amministratore nel Microsoft 365 Admin Center.</p> <p>Cliccando a sinistra in basso su «Impostazioni» > «Relazioni con i partner» potete visualizzare e gestire gli accessi che avete concesso.</p> <p>Avviso: prima di rimuovere le autorizzazioni in questa sede, riflettete sulle conseguenze che ciò potrebbe avere sulle possibilità di prenotazione e sull'erogazione delle prestazioni del servizio alla clientela Swisscom.</p> <p>Ogni richiesta di autorizzazione d'accesso viene generata dal vostro partner CSP, voi non potete avviarla autonomamente. Attraverso il link inviato dal vostro partner potete autorizzare una nuova relazione GDAP nel vostro Microsoft 365 Admin Center.</p>
<p>Quali altre misure di sicurezza sono auspicabili per proteggere il mio ambiente Microsoft?</p>	<p>Mediante Azure Active Directory e le funzioni Security di Microsoft 365 potete attivare le misure di sicurezza di base, per esempio l'autenticazione multifattore (MFA, che consigliamo di utilizzare</p>



	<p>per tutti i collaboratori e le collaboratrici) o le Conditional Access Policy (direttive di accesso condizionato), per proteggere meglio gli accessi delle vostre collaboratrici e dei vostri collaboratori. Sussiste altresì la possibilità di acquisire ulteriori soluzioni di Microsoft, per esempio la famiglia Defender. Queste offrono funzioni ampliate per una migliore sicurezza. Qui trovate consigli per le configurazioni della Security a cura dello US Department of Homeland Security: https://www.us-cert.gov/ncas/analysis-reports/AR19-133A</p> <p>Le esperte e gli esperti di Swisscom (e dei nostri partner) vi supportano in relazione alla sicurezza del vostro ambiente ICT, per esempio nell'implementazione dei parametri di sicurezza delle funzioni di sicurezza di Microsoft.</p>
--	--