



Guida per l'utente

AWSConfigurazione



AWSConfigurazione: Guida per l'utente

Copyright © 2023 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e il trade dress di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, secondo qualsiasi modalità che possa causare confusione tra i clienti o secondo qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

| | |
|---|----|
| Panoramica | 1 |
| | 1 |
| | 1 |
| Terminologia | 2 |
| | 2 |
| Amministratore | 2 |
| Account | 2 |
| Credenziali | 2 |
| Credenziali aziendali | 3 |
| Profilo | 3 |
| Utente | 3 |
| Credenziali utente root | 3 |
| Codice di verifica | 3 |
| AWSutenti e credenziali | 4 |
| Utente root | 4 |
| Utente IAM Identity Center | 5 |
| Identità federata | 5 |
| Utente IAM | 5 |
| AWSUtente Builder ID | 6 |
| Prerequisiti e considerazioni | 7 |
| Requisiti Account AWS | 7 |
| Considerazioni su IAM Identity Center | 8 |
| Active Directory o IdP esterno | 8 |
| AWS Organizations | 10 |
| Ruoli IAM | 10 |
| Firewall e gateway Web sicuri di nuova generazione | 10 |
| Utilizzo di più Account AWS | 11 |
| Parte 1: Configurare una nuovaAccount AWS | 13 |
| Fase 1: effettuare la registrazione per ottenere un account AWS | 13 |
| Passaggio 2: accedi come utente root | 14 |
| Per accedere come utente root | 15 |
| Passaggio 3: attiva l'autenticazione a più fattori per i tuoiAccount AWSutente root | 16 |
| Parte 2: creare un utente amministrativo in IAM Identity Center | 17 |
| Passaggio 1: abilitare IAM Identity Center | 17 |

| | |
|--|-----|
| Passaggio 2: scegli la fonte della tua identità | 18 |
| Connetti Active Directory o un altro IdP e specifica un utente | 19 |
| Usa la directory predefinita e crea un utente in IAM Identity Center | 21 |
| Fase 3: Creare un set di autorizzazioni amministrative | 22 |
| Fase 4: ConfigurazioneAccount AWSaccesso per un utente amministrativo | 23 |
| Passaggio 5: accedi alAWSaccedi al portale con le tue credenziali amministrative | 25 |
| Risoluzione problemiAccount AWSproblemi di creazione | 27 |
| Non ho ricevuto la chiamata daAWSper verificare il mio nuovo account | 27 |
| Ricevo un messaggio di errore relativo al «numero massimo di tentativi falliti» quando provo a verificare il mioAccount AWSper telefono | 28 |
| Sono passate più di 24 ore e il mio account non è stato attivato | 28 |
| | xxx |

Panoramica

Questa guida fornisce le istruzioni per creare una nuova Account AWS e configurare il tuo primo utente amministrativo in AWS IAM Identity Center seguendo le più recenti best practice di sicurezza.

Un Account AWS è necessario per accedere ai Servizi AWS e funge da due funzioni di base:

- **Contenitore**— Un Account AWS è un contenitore per tutti i AWS risorse che puoi creare come AWS cliente. Quando crei un bucket Amazon Simple Storage Service (Amazon S3) o un database Amazon Relational Database Service (Amazon RDS) per archiviare i tuoi dati o un'istanza Amazon Elastic Compute Cloud (Amazon EC2) per elaborare i tuoi dati, stai creando una risorsa nel tuo account. Ogni risorsa è identificata in modo univoco da un Amazon Resource Name (ARN) che include l'ID account dell'account che contiene o possiede la risorsa.
- **Limite di sicurezza**— Un Account AWS è il limite di sicurezza di base per il tuo AWS risorse. Le risorse che crei nel tuo account sono disponibili solo per gli utenti che dispongono delle credenziali per lo stesso account.

Tra le risorse chiave che puoi creare nel tuo account ci sono identità, ad esempio utenti e ruoli IAM e identità federate, ad esempio utenti della directory utente aziendale, un provider di identità Web, la directory IAM Identity Center o qualsiasi altro utente che accede ai Servizi AWS utilizzando le credenziali fornite tramite una fonte di identità. Queste identità dispongono di credenziali che qualcuno può utilizzare per accedere, oppure autenticano a AWS. Le identità dispongono anche di criteri di autorizzazione che specificano ciò che la persona che ha effettuato l'accesso è autorizzata a fare con le risorse dell'account.

Terminologia

Amazon Web Services (AWS) utilizza una [terminologia comune](#) per descrivere la procedura di accesso. Ti consigliamo di leggere e comprendere questi termini.

Amministratore

Chiamato anche Account AWS amministratore o amministratore IAM. L'amministratore, in genere personale IT (Information Technology), è un individuo che supervisiona un Account AWS. Gli amministratori dispongono di un livello di autorizzazioni più elevato Account AWS rispetto agli altri membri dell'organizzazione. Gli amministratori stabiliscono e implementano le impostazioni per Account AWS. Creano inoltre utenti IAM o IAM Identity Center. L'amministratore fornisce a questi utenti le credenziali di accesso e un URL di accesso a cui accedere. AWS

Account

Uno standard Account AWS contiene sia le AWS risorse che le identità che possono accedere a tali risorse. Gli account sono associati all'indirizzo e-mail e alla password del proprietario dell'account.

Credenziali

Chiamate anche credenziali di accesso o credenziali di sicurezza. Le credenziali sono le informazioni fornite dagli utenti per AWS effettuare l'accesso e accedere alle risorse. AWS Le credenziali possono includere un indirizzo e-mail, un nome utente, una password definita dall'utente, un ID account o un alias, un codice di verifica e un codice di autenticazione a più fattori (MFA) monouso. Nelle procedure di autenticazione e identificazione un sistema utilizza le credenziali per identificare chi effettuare una chiamata e stabilire se consentire l'accesso richiesto. [InAWS, queste credenziali sono in genere l'ID della chiave di accesso e la chiave di accesso segreta.](#)

Per ulteriori informazioni sulle credenziali, consulta [Comprendere e ottenere le AWS credenziali](#).

Note

Il tipo di credenziali che un utente deve inviare dipende dal tipo di utente.

Credenziali aziendali

Le credenziali fornite dagli utenti quando accedono alla rete e alle risorse aziendali. L'amministratore aziendale può configurare l'utente in Account AWS modo che sia accessibile con le stesse credenziali utilizzate per accedere alla rete e alle risorse aziendali. Queste credenziali vengono fornite dall'amministratore o dal dipendente dell'help desk.

Profilo

Quando ti registri per un AWS Builder ID, crei un profilo. Il tuo profilo include le informazioni di contatto che hai fornito e la possibilità di gestire i dispositivi di autenticazione a più fattori (MFA) e le sessioni attive. Puoi anche saperne di più sulla privacy e su come gestiamo i tuoi dati nel tuo profilo. Per ulteriori informazioni sul tuo profilo e su come si relaziona a unAccount AWS, consulta [AWSBuilder ID e altre AWS](#) credenziali.

Utente

Un utente è una persona o un'applicazione con un account che effettua chiamate API ai prodotti. AWS Ogni utente ha un nome univoco all'interno di Account AWS e un set di credenziali di sicurezza che non sono condivise con altri. Queste credenziali sono distinte dalle credenziali di sicurezza dell'Account AWS. Ogni utente è associato a un solo Account AWS.

Credenziali utente root

Le credenziali dell'utente root sono le stesse credenziali utilizzate per accedere AWS Management Console come utente root. Per ulteriori informazioni sull'utente root, vedere [Utente root](#).

Codice di verifica

Un codice di verifica verifica la tua identità durante il processo di accesso [utilizzando l'autenticazione a più fattori \(MFA\)](#). I metodi di consegna dei codici di verifica variano. Possono essere inviati tramite SMS o e-mail. Rivolgiti al tuo amministratore per ulteriori informazioni.

AWS utenti e credenziali

Quando interagisci con AWS, specifichi le tue credenziali di AWS sicurezza per verificare chi sei e se disponi dell'autorizzazione per accedere alle risorse che stai richiedendo. AWS utilizza credenziali di sicurezza per autenticare e autorizzare le richieste.

Ad esempio, se si desidera scaricare un file protetto da un bucket Amazon Simple Storage Service (Amazon S3), è necessario che le credenziali consentano tale accesso. Se le tue credenziali mostrano che non sei autorizzato a scaricare il file, AWS respinge la tua richiesta. Tuttavia, non sono necessarie credenziali di sicurezza per scaricare file in bucket Amazon S3 condivisi pubblicamente.

Utente root

Chiamato anche proprietario dell'account o utente root dell'account. In qualità di utente root, hai accesso completo a tutti i AWS servizi e le risorse del tuo Account AWS. Quando crei un Account AWS per la prima volta, inizi con una singola identità di accesso che ha accesso completo a tutti i servizi e le risorse AWS nell'account. Questa identità è l'utente root dell'AWS account. È possibile accedere [AWS Management Console](#) come utente root utilizzando l'indirizzo e-mail e la password utilizzati per creare l'account. Per istruzioni dettagliate su come accedere, vedi [Accedere AWS Management Console come utente root](#).

Important

Quando crei un Account AWS, inizi con una singola identità di accesso che ha accesso completo a tutti i Servizi AWS e le risorse nell'account. Tale identità è detta utente root Account AWS ed è possibile accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione [Tasks that require root user credentials](#) (Attività che richiedono le credenziali dell'utente root) nella Guida per l'utente IAM.

Per ulteriori informazioni sulle identità IAM, incluso l'utente root, consulta [Identità IAM \(utenti, gruppi di utenti e ruoli\)](#).

Utente IAM Identity Center

Un utente di IAM Identity Center accede tramite il portale di AWS accesso. Il portale di AWS accesso o l'URL di accesso specifico viene fornito dall'amministratore o dal dipendente dell'help desk. Se hai creato un utente IAM Identity Center per il tuo Account AWS, un invito a iscriversi a un utente IAM Identity Center è stato inviato all'indirizzo e-mail di. Account AWS L'URL di accesso specifico è incluso nell'e-mail di invito. Gli utenti di IAM Identity Center non possono accedere tramite AWS Management Console Per istruzioni dettagliate su come accedere, consulta [Accedere al portale di AWS accesso](#).

Note

Ti consigliamo di aggiungere ai preferiti l'URL di accesso specifico per il portale di AWS accesso in modo da potervi accedere rapidamente in un secondo momento.

Per ulteriori informazioni su IAM Identity Center, consulta [Cos'è IAM Identity Center?](#)

Identità federata

Un'identità federata è un utente che può accedere utilizzando un provider di identità esterno (IdP) noto, come Login with Amazon, Facebook, Google o qualsiasi altro IdP compatibile con [OpenID Connect \(OIDC\)](#). Con la federazione delle identità web, puoi ricevere un token di autenticazione e quindi scambiarlo con credenziali di sicurezza temporanee in AWS quella mappa con un ruolo IAM con le autorizzazioni per utilizzare le risorse del tuo Account AWS Non si accede né si AWS accede al AWS Management Console portale. Al contrario, l'identità esterna in uso determina la modalità di accesso.

Per ulteriori informazioni, vedi [Accedere come identità federata](#).

Utente IAM

Un utente IAM è un'entità in AWS cui crei. Questo utente è un'identità interna a Account AWS cui sono concesse autorizzazioni personalizzate specifiche. Le tue credenziali utente IAM sono costituite da un nome e una password utilizzati per accedere a [AWS Management Console](#) Per istruzioni dettagliate su come accedere, consulta [Accedere AWS Management Console come utente IAM](#).

Per ulteriori informazioni sulle identità IAM, incluso l'utente IAM, consulta [Identità IAM \(utenti, gruppi di utenti e ruoli\)](#).

AWSUtente Builder ID

Come utente AWS Builder ID, accedi specificamente al AWS servizio o allo strumento a cui desideri accedere. Un utente AWS Builder ID completa Account AWS quello che già possiedi o che desideri creare. Un AWS Builder ID ti rappresenta come persona e puoi utilizzarlo per accedere a AWS servizi e strumenti senza un Account AWS. Hai anche un profilo in cui puoi vedere e aggiornare le tue informazioni. Per ulteriori informazioni, consulta [Accedere con AWS Builder ID](#).

Prerequisiti e considerazioni

Prima di iniziare il processo di configurazione, verifica i requisiti dell'account e valuta se ne avrai bisogno più di uno. Account AWS e comprendi i requisiti per configurare il tuo account per l'accesso amministrativo in IAM Identity Center.

Requisiti Account AWS

Per iscriversi a un Account AWS, è necessario fornire le seguenti informazioni:

- Un nome di account— Il nome dell'account viene visualizzato in diverse posizioni, ad esempio sulla fattura, e in console come la dashboard di fatturazione e gestione dei costi e il AWS Organizations console.

Ti consigliamo di utilizzare uno standard di denominazione degli account in modo che il nome dell'account possa essere facilmente riconosciuto e distinto dagli altri account che potresti possedere. Se si tratta di un account aziendale, prendi in considerazione l'utilizzo di uno standard di denominazione come organizzazione-scopo-ambiente (ad esempio, AnyCompany-audit-pungolare). Se si tratta di un account personale, considera l'utilizzo di uno standard di denominazione come nome-cognome-scopo (ad esempio, paulo-santos-testaccount).

- Un indirizzo email— Questo indirizzo e-mail viene utilizzato come nome di accesso per l'utente root dell'account ed è necessario per il ripristino dell'account, ad esempio per dimenticare la password. Devi essere in grado di ricevere messaggi inviati a questo indirizzo email. Prima di poter eseguire determinate attività, è necessario verificare di avere accesso all'account di posta elettronica.

Important

Se questo account è per un'azienda, ti consigliamo di utilizzare una lista di distribuzione aziendale (ad esempio, `it.admins@example.com`). Evita di utilizzare l'indirizzo email aziendale di una persona (ad esempio, `paulo.santos@example.com`). Questo aiuta a garantire che la tua azienda possa accedere a Account AWS se un dipendente cambia posizione o lascia l'azienda. L'indirizzo e-mail può essere utilizzato per reimpostare le credenziali dell'utente root dell'account. Assicurati di proteggere l'accesso a questa lista di distribuzione o indirizzo.

- Un numero di telefono— Questo numero può essere utilizzato quando è richiesta la conferma della proprietà dell'account. Devi essere in grado di ricevere chiamate a questo numero di telefono.

Important

Se questo account è per un'azienda, ti consigliamo di utilizzare un numero di telefono aziendale anziché un numero di telefono personale. Questo aiuta a garantire che la tua azienda possa accedere aAccount AWSse un dipendente cambia posizione o lascia l'azienda.

- Un dispositivo di autenticazione a più fattori— Per proteggere il tuoAWSrisorse, abilita l'autenticazione a più fattori (MFA) sull'account utente root. Oltre alle normali credenziali di accesso, è richiesta un'autenticazione secondaria quando viene attivata l'autenticazione a più fattori, che fornisce un ulteriore livello di sicurezza. Per ulteriori informazioni sull'autenticazione a più fattori, vedere[Che cos'è l'MFA?](#)nelGuida per l'utente IAM.
- AWS Supportpiano— Ti verrà chiesto di scegliere uno dei piani disponibili durante il processo di creazione dell'account. Per una descrizione dei piani disponibili, consulta[ConfrontaAWS Supportpiani](#).

Considerazioni su IAM Identity Center

I seguenti argomenti forniscono indicazioni per la configurazione di IAM Identity Center per ambienti specifici. Comprendi le linee guida applicabili al tuo ambiente prima di procedere[Parte 2: creare un utente amministrativo in IAM Identity Center](#).

Argomenti

- [Active Directory o IdP esterno](#)
- [AWS Organizations](#)
- [Ruoli IAM](#)
- [Firewall e gateway Web sicuri di nuova generazione](#)

Active Directory o IdP esterno

Se gestisci già utenti e gruppi in Active Directory o in un IdP esterno, ti consigliamo di connettere questa fonte di identità quando abiliti IAM Identity Center e scegli la tua fonte di identità. Questa

operazione prima di creare utenti e gruppi nella directory predefinita di Identity Center consente di evitare la configurazione aggiuntiva richiesta se si modifica l'origine dell'identità in un secondo momento.

Se si desidera utilizzare Active Directory come fonte di identità, la configurazione deve soddisfare i seguenti prerequisiti:

- Se stai usando AWS Managed Microsoft AD, devi abilitare IAM Identity Center nello stesso Regione AWS dove il tuo AWS Managed Microsoft AD la cartella è impostata. IAM Identity Center archivia i dati di assegnazione nella stessa regione della directory. Per amministrare IAM Identity Center, potrebbe essere necessario passare alla regione in cui è configurato IAM Identity Center. Inoltre, si noti che AWS il portale di accesso utilizza lo stesso URL di accesso della rubrica.
- Usa un Active Directory che risiede nel tuo account di gestione:

È necessario disporre di un connettore AD esistente o AWS Managed Microsoft AD cartella impostata in AWS Directory Service e deve risiedere all'interno del tuo AWS Organizations account di gestione. È possibile connettere solo un connettore AD o uno AWS Managed Microsoft AD alla volta. Se devi supportare più domini o foreste, usa AWS Managed Microsoft AD. Per ulteriori informazioni, consultare:

- [Collega una cartella in AWS Managed Microsoft AD a IAM Identity Center](#) nel AWS IAM Identity Center Guida per l'utente.
- [Connetti una directory autogestita in Active Directory a IAM Identity Center](#) nel AWS IAM Identity Center Guida per l'utente.
- Usa un Active Directory che risiede nell'account amministratore delegato:

Se prevedi di abilitare l'amministratore delegato di IAM Identity Center e utilizzare Active Directory come fonte di identità IAM, puoi utilizzare un connettore AD esistente o AWS Managed Microsoft AD cartella impostata in AWS directory che risiede nell'account amministratore delegato.

Se decidi di cambiare l'origine di IAM Identity Center da qualsiasi altra fonte ad Active Directory o da Active Directory a qualsiasi altra fonte, la directory deve risiedere (essere di proprietà) nell'account membro amministratore delegato di IAM Identity Center, se esistente; in caso contrario, deve trovarsi nell'account di gestione.

AWS Organizations

Il tuo Account AWS deve essere gestito da AWS Organizations. Se non hai creato un'organizzazione, non devi farlo. Quando abiliti IAM Identity Center, sceglierai se avere AWS crea un'organizzazione per te.

Se hai già configurato AWS Organizations, assicurati che tutte le funzionalità siano abilitate. Per ulteriori informazioni, consulta la sezione [Abilitazione di tutte le caratteristiche nell'organizzazione](#) nella Guida per l'utente di AWS Organizations.

Per abilitare IAM Identity Center, devi accedere al AWS Management Console utilizzando le tue credenziali AWS Organizations account di gestione. Non puoi abilitare IAM Identity Center se hai effettuato l'accesso con le credenziali di un AWS Organizations account membro. Per ulteriori informazioni, vedere [Creare e gestire un'AWS Organizzazione](#) nel AWS Organizations Guida per l'utente.

Ruoli IAM

Se hai già configurato i ruoli IAM nel tuo Account AWS, ti consigliamo di verificare se il tuo account si avvicina alla quota per i ruoli IAM. Per ulteriori informazioni, vedere [Quote degli oggetti IAM](#).

Se ti stai avvicinando alla quota, valuta la possibilità di richiedere un aumento della quota. Altrimenti, potresti riscontrare problemi con IAM Identity Center quando fornisci set di autorizzazioni agli account che hanno superato la quota di ruoli IAM. Per informazioni su come richiedere un aumento della quota, consulta [Richiesta di aumento della quota](#) nel Guida per l'utente di Service Quotas.

Firewall e gateway Web sicuri di nuova generazione

Se si filtra l'accesso a determinati AWS domini o endpoint URL utilizzando una soluzione di filtraggio dei contenuti Web come NGFW o SWG, è necessario aggiungere i seguenti domini o endpoint URL agli elenchi consentiti della soluzione di filtraggio dei contenuti Web.

Domini DNS specifici

- *.awsapps.com (http://awsapps.com/)
- *.accedi.aws

Endpoint URL specifici

- https://[la tua rubrica].awsapps.com/start
- https://[la tua rubrica].awsapps.com/login

- [https://\[la tua regione\].signin.aws/platform/login](https://[la tua regione].signin.aws/platform/login)

Utilizzo di più Account AWS

Account AWS fungono da limite di sicurezza fondamentale in AWS. Fungono da contenitore di risorse che fornisce un utile livello di isolamento. La capacità di isolare risorse e utenti è un requisito fondamentale per creare un ambiente sicuro e ben governato.

Separazione delle risorse in risorse separate Account AWS ti aiuta a supportare i seguenti principi nel tuo ambiente cloud:

- **Controllo della sicurezza**— Applicazioni diverse possono avere profili di sicurezza diversi che richiedono politiche e meccanismi di controllo diversi. Ad esempio, è più facile parlare con un revisore ed essere in grado di indicarne uno solo Account AWS che ospita tutti gli elementi del carico di lavoro soggetti a [Standard di sicurezza del settore delle carte di pagamento \(PCI\)](#).
- **Isolamento**— Un Account AWS è un'unità di protezione della sicurezza. I potenziali rischi e le minacce alla sicurezza devono essere contenuti in un Account AWS senza influire sugli altri. Potrebbero esserci esigenze di sicurezza diverse a causa dei diversi team o dei diversi profili di sicurezza.
- **Molte squadre**— Team diversi hanno responsabilità ed esigenze di risorse diverse. Puoi evitare che i team interferiscano tra loro spostandoli in modo che si separino Account AWS.
- **Isolamento dei dati**— Oltre a isolare i team, è importante isolare gli archivi dati in un account. Questo può aiutare a limitare il numero di persone che possono accedere e gestire quell'archivio dati. Ciò aiuta a contenere l'esposizione a dati altamente privati e quindi può contribuire alla conformità con [Regolamento generale sulla protezione dei dati \(GDPR\) dell'Unione europea](#).
- **Processo aziendale**— Unità aziendali o prodotti diversi possono avere scopi e processi completamente diversi. Con multiplo Account AWS, puoi supportare le esigenze specifiche di un'unità aziendale.
- **Fatturazione**— Un account è l'unico vero modo per separare gli articoli a livello di fatturazione. Gli account multipli consentono di separare gli articoli a livello di fatturazione tra unità aziendali, team funzionali o singoli utenti. Puoi comunque far consolidare tutte le tue fatture a un unico pagatore (utilizzando AWS Organization e fatturazione consolidata) con le voci separate da Account AWS.
- **Assegnazione delle quote**— AWS le quote di servizio vengono applicate separatamente per ciascuna Account AWS. Separazione dei carichi di lavoro in diversi Account AWS impedisce loro di consumare quote l'uno per l'altro.

Tutte le raccomandazioni e le procedure descritte in questa guida sono conformi al [AWS Framework ben architettato](#). Questo framework ha lo scopo di aiutarti a progettare un'infrastruttura cloud flessibile, resiliente e scalabile. Anche quando si inizia in piccolo, si consiglia di procedere in conformità con le linee guida contenute nel framework. Ciò può aiutarti a scalare il tuo ambiente in modo sicuro e senza influire sulle operazioni in corso man mano che cresci.

Prima di iniziare ad aggiungere più account, ti consigliamo di sviluppare un piano per gestirli. Per questo, ti consigliamo di utilizzare [AWS Organizations](#), che è gratuito AWS servizio, per gestire tutti i Account AWS nella tua organizzazione.

AWS offre anche AWS Control Tower, che aggiunge strati di AWS automazione gestita per le organizzazioni e la integra automaticamente con altri AWS servizi come AWS CloudTrail, AWS Config, Amazon CloudWatch, AWS Service Catalog e altri ancora. Questi servizi possono comportare costi aggiuntivi. Per ulteriori informazioni, consulta [Prezzi di AWS Control Tower](#).

Parte 1: Configurare una nuova Account AWS

Queste istruzioni ti aiuteranno a creare un Account AWS e proteggi le credenziali dell'utente root.

Completa tutti i passaggi prima di procedere [Parte 2: creare un utente amministrativo in IAM Identity Center](#).

Argomenti

- [Fase 1: effettuare la registrazione per ottenere un account AWS](#)
- [Passaggio 2: accedi come utente root](#)
- [Passaggio 3: attiva l'autenticazione a più fattori per i tuoi Account AWS utente root](#)

Fase 1: effettuare la registrazione per ottenere un account AWS

1. Aprire la pagina all'indirizzo <https://portal.aws.amazon.com/billing/signup>.
2. Scegli **Crea un Account AWS**.

Note

Se hai effettuato l'accesso a AWS recentemente, scegli **Accedi alla console**. Se l'opzione **Crea un nuovo Account AWS** non è visibile, scegli prima **Accedi a un altro account**, quindi scegli **Crea un nuovo Account AWS**.

3. Inserisci le informazioni del tuo account, quindi scegli **Continua**.

Assicurati di inserire correttamente le informazioni del tuo account, in particolare il tuo indirizzo email. Se inserisci il tuo indirizzo email in modo errato, non puoi accedere al tuo account.

4. Scegli **Personale** o **Professionista**.

La differenza tra queste opzioni è solo nelle informazioni che ti chiediamo. Entrambi i tipi di account hanno le stesse caratteristiche e funzioni.

5. Inserisci i tuoi dati aziendali o personali in base alle indicazioni fornite in [Requisiti Account AWS](#).
6. Leggi e accetta il [AWS Contratto con il cliente](#).
7. Scegli **Crea un account** e continua.

A questo punto, riceverai un messaggio e-mail per confermare che il tuo Account AWS è pronto all'uso. Puoi accedere al tuo nuovo account utilizzando l'indirizzo e-mail e la password

che hai fornito durante la registrazione. Tuttavia, non puoi usarne AWS servizi fino al termine dell'attivazione del tuo account.

8. Sull'Informazioni sul pagamento pagina, inserisci le informazioni sul tuo metodo di pagamento. Se desideri utilizzare un indirizzo diverso da quello che hai usato per creare l'account, scegli Usa un nuovo indirizzo e inserisci l'indirizzo che desideri utilizzare per la fatturazione.
9. Scegli Verifica e aggiungi.

Note

Se il tuo indirizzo di contatto è in India, il tuo contratto di utilizzo per il tuo account è con AISPL, un ente locale AWS venditore in India. È necessario fornire il CVV come parte del processo di verifica. Potrebbe anche essere necessario inserire una password monouso, a seconda della banca. AISPL addebita 2 INR sul tuo metodo di pagamento come parte del processo di verifica. AISPL rimborsa i 2 INR dopo aver completato la verifica.

10. Per verificare il tuo numero di telefono, scegli il prefisso del tuo Paese o della tua area geografica dall'elenco e inserisci un numero di telefono a cui puoi essere chiamato nei prossimi minuti. Inserisci il codice CAPTCHA e invia.
11. La AWS il sistema di verifica automatico ti chiama e fornisce un PIN. Inserisci il PIN utilizzando il telefono e quindi scegli Continua.
12. Seleziona un AWS Support piano.

Per una descrizione dei piani disponibili, consulta [Confronta AWS Support piani](#).

Viene visualizzata una pagina di conferma che indica che il tuo account è in fase di attivazione. Questa operazione richiede in genere solo pochi minuti, ma a volte può richiedere fino a 24 ore. Durante l'attivazione, puoi accedere al tuo nuovo Account AWS. Fino al completamento dell'attivazione, potresti visualizzare un [Registrazione completa](#) pulsante. Puoi ignorarla.

AWS invia un messaggio e-mail di conferma quando l'attivazione dell'account è completa. Controlla la tua e-mail e la cartella spam per il messaggio e-mail di conferma. Dopo aver ricevuto questo messaggio, avrai pieno accesso a tutti AWS servizi.

Passaggio 2: accedi come utente root

Quando si crea un Account AWS per la prima volta, si inizia con una singola identità di accesso che ha accesso completo a tutti i Servizi AWS e le risorse nell'account. Tale identità è detta utente

root Account AWS ed è possibile accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account.

Important

Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione [Tasks that require root user credentials](#) (Attività che richiedono le credenziali dell'utente root) nella Guida per l'utente IAM.

Per accedere come utente root

1. Apri l'AWS Management Console all'indirizzo <https://console.aws.amazon.com/>.

Note

Se in precedenza hai effettuato l'accesso come utente root in questo browser, il tuo browser potrebbe ricordare l'indirizzo email perAccount AWS.

Se hai effettuato l'accesso in precedenza come utente IAM utilizzando questo browser, il browser potrebbe invece visualizzare la pagina di accesso degli utenti IAM. Per tornare alla pagina di accesso principale, seleziona Accedi tramite e-mail utente root.

2. Se non è stato effettuato l'accesso in precedenza utilizzando questo browser, la pagina di accesso principale viene visualizzata. Se sei il proprietario dell'account, scegli Utente root. Inserisci il tuo indirizzo Account AWS email associato al tuo account e scegli Avanti.
3. È possibile che ti venga richiesto di completare un controllo di sicurezza. Completa questa operazione per passare alla fase successiva. Se non riesci a completare il controllo di sicurezza, prova ad ascoltare l'audio o ad aggiornare il controllo di sicurezza per un nuovo set di caratteri.
4. Inserire la password e selezionare Sign in (Accedi).

Passaggio 3: attiva l'autenticazione a più fattori per i tuoi Account AWS utente root

Per migliorare la sicurezza delle credenziali dell'utente root, ti consigliamo di seguire le best practice di sicurezza per attivare l'autenticazione a più fattori (MFA) per il tuo Account AWS. Poiché l'utente root può eseguire operazioni riservate nel tuo account, l'aggiunta di questo livello di autenticazione aggiuntivo ti aiuta a proteggere meglio il tuo account. Disponibilità di diversi tipi di MFA.

Per istruzioni sull'attivazione dell'autenticazione a più fattori per l'utente root, vedi [Attivazione dei dispositivi MFA per gli utenti in AWS](#) nella Guida per l'utente IAM.

Parte 2: creare un utente amministrativo in IAM Identity Center

Dopo aver completato [Parte 1: Configurare una nuova Account AWS](#), i seguenti passaggi ti aiuteranno a configurare Account AWS accesso per un utente amministrativo, che verrà utilizzato per eseguire attività quotidiane.

Note

Questo argomento fornisce i passaggi minimi richiesti per configurare correttamente l'accesso da amministratore per un Account AWS. Se crea un utente amministrativo in IAM Identity Center. Per ulteriori informazioni, vedere [Guida introduttiva](#) nel AWS IAM Identity Center Guida per l'utente.

Argomenti

- [Passaggio 1: abilitare IAM Identity Center](#)
- [Passaggio 2: scegli la fonte della tua identità](#)
- [Fase 3: Creare un set di autorizzazioni amministrative](#)
- [Fase 4: Configurazione Account AWS accesso per un utente amministrativo](#)
- [Passaggio 5: accedi al AWS accedi al portale con le tue credenziali amministrative](#)

Passaggio 1: abilitare IAM Identity Center

Note

Se non hai attivato l'autenticazione a più fattori (MFA) per l'utente root, completa [Passaggio 3: attiva l'autenticazione a più fattori per i tuoi Account AWS utente root](#) prima di procedere.

Per abilitare IAM Identity Center

1. Accedi alla [AWS Management Console](#) come proprietario dell'account scegliendo Utente root e immettendo l'indirizzo email dell'Account AWS. Nella pagina successiva, inserisci la password.
2. Apri il [Console IAM Identity Center](#).

3. SottoAbilita IAM Identity Center, scegliAbilita.
4. IAM Identity Center richiedeAWS Organizations. Se non hai creato un'organizzazione, devi scegliere se avereAWScreane uno per te. ScegliCreaAWSorganizzazioneper completare questo processo.

AWS Organizationsinvia automaticamente un'e-mail di verifica all'indirizzo associato al tuo account di gestione. Potrebbe verificarsi un ritardo prima di ricevere l'e-mail di verifica. Verificare l'indirizzo e-mail entro 24 ore.

Note

Se utilizzi un ambiente con più account, ti consigliamo di configurare l'amministrazione delegata. Con l'amministrazione delegata, puoi limitare il numero di persone che richiedono l'accesso all'account di gestione inAWS Organizations. Per ulteriori informazioni, vedere[Amministrare delegata](#)nelAWS IAM Identity CenterGuida per l'utente.

Passaggio 2: scegli la fonte della tua identità

La tua fonte di identità in IAM Identity Center definisce dove vengono gestiti gli utenti e i gruppi. Puoi scegliere una delle seguenti opzioni come fonte di identità:

- Elenco IAM Identity Center— Quando abiliti IAM Identity Center per la prima volta, viene automaticamente configurato con una directory IAM Identity Center come fonte di identità predefinita. Qui puoi creare utenti e gruppi e assegnare il loro livello di accesso agli account e alle applicazioni AWS.
- Active Directory— Scegli questa opzione se desideri continuare a gestire gli utenti nella tua directory Microsoft AD gestita da AWS utilizzando AWS Directory Service o nella tua directory autogestita in Active Directory (AD).
- Provider di identità esterno— Scegli questa opzione se desideri gestire gli utenti in un provider di identità esterno (IdP) come Okta o Azure Active Directory.

Dopo aver abilitato IAM Identity Center, devi scegliere la tua fonte di identità. L'origine di identità scelta determina dove IAM Identity Center cerca utenti e gruppi che necessitano dell'accesso Single Sign-On. Dopo aver scelto la fonte della tua identità, dovrai creare o specificare un utente e assegnargli le autorizzazioni amministrative al tuoAccount AWS.

Important

Se gestisci già utenti e gruppi in Active Directory o in un provider di identità esterno (IdP), ti consigliamo di connettere questa fonte di identità quando abiliti IAM Identity Center e scegli la tua fonte di identità. Questa operazione deve essere eseguita prima di creare utenti e gruppi nella directory predefinita di Identity Center ed effettuare qualsiasi assegnazione. Se stai già gestendo utenti e gruppi in un'unica origine di identità, il passaggio a un'altra origine di identità potrebbe rimuovere tutte le assegnazioni di utenti e gruppi configurate in IAM Identity Center. In tal caso, tutti gli utenti, incluso l'utente amministrativo di IAM Identity Center, perderanno l'accesso Single Sign-On al proprio Account AWS e applicazioni.

Argomenti

- [Connetti Active Directory o un altro IdP e specifica un utente](#)
- [Usa la directory predefinita e crea un utente in IAM Identity Center](#)

Connetti Active Directory o un altro IdP e specifica un utente

Se stai già utilizzando Active Directory o un provider di identità esterno (IdP), i seguenti argomenti ti aiuteranno a connettere la tua directory a IAM Identity Center.

Puoi connettere unAWS Managed Microsoft ADdirectory, una directory autogestita in Active Directory o un IdP esterno con IAM Identity Center. Se prevedi di connettere unAWS Managed Microsoft ADdirectory o directory autogestita in Active Directory, assicurati che la configurazione di Active Directory soddisfi i prerequisiti in[Active Directory o IdP esterno](#).

Note

Come best practice di sicurezza, ti consigliamo vivamente di abilitare l'autenticazione a più fattori. Se prevedi di connettere unAWS Managed Microsoft ADdirectory o directory autogestita in Active Directory e non si utilizza RADIUS MFA conAWS Directory Service, abilita l'autenticazione a più fattori in IAM Identity Center. Se prevedi di utilizzare un provider di identità esterno, tieni presente che l'IdP esterno, non IAM Identity Center, gestisce le impostazioni MFA. L'autenticazione a più fattori in IAM Identity Center non è supportata per l'uso da parte di utenti esterni IdPs. Per ulteriori informazioni, vedere[Abilita l'autenticazione a più fattori](#)inl'AWS IAM Identity CenterGuida per l'utente.

AWS Managed Microsoft AD

1. Consulta le linee guida in [Connettersi a Microsoft Active Directory](#).
2. Segui i passaggi in [Collega una cartella in AWS Managed Microsoft AD a IAM Identity Center](#).
3. Configura Active Directory per sincronizzare l'utente a cui desideri concedere le autorizzazioni amministrative in IAM Identity Center. Per ulteriori informazioni, vedere [Sincronizzazione di un utente amministrativo in IAM Identity Center](#).

Directory autogestita in Active Directory

1. Consulta le linee guida in [Connettersi a Microsoft Active Directory](#).
2. Segui i passaggi in [Connetti una directory autogestita in Active Directory a IAM Identity Center](#).
3. Configura Active Directory per sincronizzare l'utente a cui desideri concedere le autorizzazioni amministrative in IAM Identity Center. Per ulteriori informazioni, vedere [Sincronizza un utente amministrativo in IAM Identity Center](#).

IdP esterno

1. Consulta le linee guida in [Connettiti a un provider di identità esterno](#).
2. Segui i passaggi in [Come connettersi a un provider di identità esterno](#).
3. Configura il tuo IdP per fornire agli utenti l'accesso a IAM Identity Center.

Note

Prima di configurare il provisioning automatico e basato su gruppi di tutte le identità della forza lavoro dal tuo IdP a IAM Identity Center, ti consigliamo di sincronizzare l'unico utente a cui desideri concedere le autorizzazioni amministrative in IAM Identity Center.

Sincronizzazione di un utente amministrativo in IAM Identity Center

Dopo aver collegato la tua directory a IAM Identity Center, puoi specificare un utente a cui concedere le autorizzazioni amministrative e quindi sincronizzare quell'utente dalla tua directory in IAM Identity Center.

1. Apri il [Console IAM Identity Center](#).

2. Selezionare Settings (Impostazioni).
3. Sull'Impostazioni pagina, scegli Fonte di identità scheda, scegli Azioni, quindi scegli Gestisci sincronizzazione.
4. Sul Gestisci sincronizzazione pagina, scegli Utenti scheda, quindi scegli Aggiungere utenti e gruppi.
5. Sul Utenti scheda, sotto Utente, inserisci il nome utente esatto e scegli Inserisci.
6. Sotto Utenti e gruppi aggiunti, effettuate le seguenti operazioni:
 - a. Conferma che l'utente a cui desideri concedere le autorizzazioni amministrative sia specificato.
 - b. Seleziona la casella di controllo a sinistra del nome utente.
 - c. Scegli Submit (Invia).
7. Nel Gestisci la sincronizzazione pagina, l'utente che hai specificato appare nella Utenti nell'ambito della sincronizzazione elenco.
8. Nel riquadro di navigazione, seleziona Users (Utenti).
9. Sul Utenti pagina, potrebbe essere necessario del tempo prima che l'utente specificato compaia nell'elenco. Scegli l'icona di aggiornamento per aggiornare l'elenco degli utenti.

A questo punto, l'utente non ha accesso all'account di gestione. Configurerai l'accesso amministrativo a questo account creando un set di autorizzazioni amministrative e assegnando l'utente a quel set di autorizzazioni.

Fase successiva: [Fase 3: Creare un set di autorizzazioni amministrative](#)


Usa la directory predefinita e crea un utente in IAM Identity Center

Quando abiliti IAM Identity Center per la prima volta, viene automaticamente configurato con una directory IAM Identity Center come fonte di identità predefinita. Completa i seguenti passaggi per creare un utente in IAM Identity Center.

1. Accedi alla [AWS Management Console](#) come proprietario dell'account scegliendo Utente root e immettendo l'indirizzo email dell'Account AWS. Nella pagina successiva, inserisci la password.
2. Apri il [Console IAM Identity Center](#).
3. Segui i passaggi in [Aggiungi utenti](#) per creare un utente.

Quando specifichi i dettagli utente, puoi inviare un'e-mail con le istruzioni per la configurazione della password (questa è l'opzione predefinita) o generare una password monouso. Se invii un'e-mail, assicurati di specificare un indirizzo e-mail a cui puoi accedere.

4. Dopo aver aggiunto l'utente, torna a questa procedura. Se hai mantenuto l'opzione predefinita per inviare un'e-mail con le istruzioni per la configurazione della password, procedi come segue:
 - a. Riceverai un'email con l'oggetto `Invito a partecipare AWS Accesso singolo`. Apri l'email e scegli `Accetta l'invito`.
 - b. Sul `Registrazione di un nuovo utente` pagina, inserisci e conferma una password, quindi scegli `Imposta una nuova password`.

 Note

Assicurati di salvare la password. Ne avrai bisogno più tardi per [Passaggio 5: accedi a AWS](#) [Accedi al portale con le tue credenziali amministrative](#).

A questo punto, l'utente non ha accesso all'account di gestione. Configurerai l'accesso amministrativo a questo account creando un set di autorizzazioni amministrative e assegnando l'utente a quel set di autorizzazioni.

Fase successiva: [Fase 3: Creare un set di autorizzazioni amministrative](#)

Fase 3: Creare un set di autorizzazioni amministrative

I set di autorizzazioni sono archiviati in IAM Identity Center e definiscono il livello di accesso di utenti e gruppi a un Account AWS. Esegui i seguenti passaggi per creare un set di autorizzazioni che conceda autorizzazioni amministrative.

1. Accedi alla [AWS Management Console](#) come proprietario dell'account scegliendo Utente root e immettendo l'indirizzo email dell'Account AWS. Nella pagina successiva, inserisci la password.
2. Apri il [Console IAM Identity Center](#).
3. Nel riquadro di navigazione di IAM Identity Center, sotto `Autorizzazioni per più account`, scegli `Set di autorizzazioni`.
4. Scegli `Create permission set (Crea set di autorizzazioni)`.

5. PerPassaggio 1: selezionare il tipo di set di autorizzazioni, sulSeleziona il tipo di set di autorizzazionipagina, mantieni le impostazioni predefinite e scegliProssimo. Le impostazioni predefinite garantiscono l'accesso completo aAWSservizi e risorse che utilizzanoAdministratorAccessset di autorizzazioni predefinito.

Note

Il predefinitoAdministratorAccessil set di autorizzazioni utilizza ilAdministratorAccessAWSpolitica gestita.

6. PerPassaggio 2: specificare i dettagli del set di autorizzazioni, sulSpecificare i dettagli del set di autorizzazionipagina, mantieni le impostazioni predefinite e scegliProssimo. L'impostazione predefinita limita la sessione a un'ora.
7. PerFase 3: Rivedi e crea, sulRivedi e creapagina, effettuate le seguenti operazioni:
 1. Controlla il tipo di set di autorizzazioni e conferma che lo siaAdministratorAccess.
 2. Rivedi ilAWSpolitica gestita e conferma che lo siaAdministratorAccess.
 3. Scegli Create (Crea).


Fase 4: ConfigurazioneAccount AWSaccesso per un utente amministrativo

Da configurareAccount AWSaccesso per un utente amministrativo in IAM Identity Center, è necessario assegnare l'utente alAdministratorAccessset di autorizzazioni.

1. Accedi alla [AWS Management Console](#) come proprietario dell'account scegliendo Utente root e immettendo l'indirizzo email dell'Account AWS. Nella pagina successiva, inserisci la password.
2. Apri il [Console IAM Identity Center](#).
3. Nel riquadro di navigazione, sottoAutorizzazioni per più account, scegliAccount AWS.
4. SulAccount AWSpagina, viene visualizzato un elenco ad albero della tua organizzazione. Seleziona la casella di controllo accanto aAccount AWSa cui si desidera assegnare l'accesso amministrativo. Se hai più account nell'organizzazione, seleziona la casella di controllo accanto all'account di gestione.
5. ScegliAssegna utenti o gruppi.


6. Per Fase 1: Seleziona utenti e gruppi, sulAssegna utenti e gruppi a»**AWS-nome-account**«pagina, effettuate le seguenti operazioni:
 1. SulUtentischeda, seleziona l'utente a cui desideri concedere le autorizzazioni amministrative.

Per filtrare i risultati, inizia a digitare il nome dell'utente desiderato nella casella di ricerca.
 2. Dopo aver confermato che è stato selezionato l'utente corretto, scegliProssimo.
7. PerPassaggio 2: selezionare i set di autorizzazioni, sulAssegna set di autorizzazioni a»**AWS-nome-account**«pagina, sottoSet di autorizzazioni, selezionaAdministratorAccessset di autorizzazioni.
8. Seleziona Successivo.
9. Per Fase 3: Rivedi e invia, sulRivedi e invia incarichi a»**AWS-nome-account**«pagina, effettuate le seguenti operazioni:
 1. Controlla l'utente e il set di autorizzazioni selezionati.
 2. Dopo aver confermato che l'utente corretto è stato assegnato aAdministratorAccessset di autorizzazioni, scegliInvia.

 Important

Il completamento del processo di assegnazione degli utenti potrebbe richiedere alcuni minuti. Lascia aperta questa pagina fino al completamento del processo.

10. Se si verifica una delle seguenti condizioni, segui i passaggi in [Abilita l'autenticazione a più fattori](#) per abilitare l'autenticazione a più fattori per IAM Identity Center:
 - Stai utilizzando la directory predefinita di Identity Center come fonte di identità.
 - Stai usando unAWS Managed Microsoft ADdirectory o directory autogestita in Active Directory come fonte di identità e non si utilizza RADIUS MFA conAWS Directory Service.

 Note

Se utilizzi un provider di identità esterno, tieni presente che l'IdP esterno, non IAM Identity Center, gestisce le impostazioni MFA. L'autenticazione a più fattori in IAM Identity Center non è supportata per l'uso da parte di utenti esternildPs.

Quando si configura l'accesso all'account per l'utente amministrativo, il Centro identità IAM crea un ruolo IAM corrispondente. Questo ruolo, controllato da IAM Identity Center, viene creato nell'area pertinenteAccount AWS e le politiche specificate nel set di autorizzazioni sono associate al ruolo.

Passaggio 5: accedi alAWSaccedi al portale con le tue credenziali amministrative

Completa i seguenti passaggi per confermare che puoi accedere alAWSaccedere al portale utilizzando le credenziali dell'utente amministrativo e al quale è possibile accedereAccount AWS.

1. Accedi alla [AWS Management Console](#) come proprietario dell'account scegliendo Utente root e immettendo l'indirizzo email dell'Account AWS. Nella pagina successiva, inserisci la password.
2. Apri ilAWS IAM Identity Centerconsole a <https://console.aws.amazon.com/singlesignon/>.
3. Nel pannello di navigazione seleziona Pannello di controllo.
4. SulPannello di controllopagina, sottoRiepilogo delle impostazioni, copia ilAWSaccedere all'URL del portale.
5. Apri un browser separato, incolla ilAWSaccedi all'URL del portale che hai copiato e premiEntra.
6. Accedi utilizzando uno dei seguenti metodi:
 - Se utilizzi Active Directory o un provider di identità esterno (IdP) come origine di identità, accedi utilizzando le credenziali dell'utente Active Directory o IdP che hai assegnato alAdministratorAccessset di autorizzazioni in IAM Identity Center.
 - Se utilizzi la directory predefinita di IAM Identity Center come fonte di identità, accedi utilizzando il nome utente che hai specificato quando hai creato l'utente e la nuova password che hai specificato per l'utente.
7. Dopo aver effettuato l'accesso, unAccount AWSl'icona appare nel portale.
8. Quando si selezionaAccount AWSvengono visualizzati l'icona, il nome dell'account, l'ID dell'account e l'indirizzo e-mail associati all'account.
9. Scegli il nome dell'account per visualizzareAdministratorAccessset di autorizzazioni e selezionareConsole di gestione link a destra diAdministratorAccess.

Quando si accede, il nome del set di autorizzazioni a cui è assegnato l'utente viene visualizzato come ruolo disponibile inAWSaccesso al portale. Perché hai assegnato questo utente alAdministratorAccessset di autorizzazioni, il ruolo verrà visualizzato nelAWSaccedi al portale come:AdministratorAccess/*nome utente*

10. Se vieni reindirizzato all'AWS Console di gestione, hai completato con successo la configurazione dell'accesso amministrativo all'Account AWS. Procedi al passaggio 10.
11. Passa al browser che hai utilizzato per accedere all'AWS Management Console e configura IAM Identity Center ed esci dal tuo Account AWS utente root.

 Important

Ti consigliamo vivamente di attenerci alla migliore pratica di utilizzo delle credenziali dell'utente amministrativo quando accedi all'AWS. Accedi al portale e che non utilizzi le credenziali dell'utente root per le tue attività quotidiane.

Per consentire ad altri utenti di accedere ai tuoi account e alle tue applicazioni e amministrare IAM Identity Center, crea e assegna set di autorizzazioni solo tramite IAM Identity Center.

Risoluzione problemi Account AWS problemi di creazione

Usa le informazioni qui per aiutarti a risolvere i problemi relativi alla creazione di un Account AWS.

Problemi

- [Non ho ricevuto la chiamata da AWS per verificare il mio nuovo account](#)
- [Ricevo un messaggio di errore relativo al «numero massimo di tentativi falliti» quando provo a verificare il mio Account AWS per telefono](#)
- [Sono passate più di 24 ore e il mio account non è stato attivato](#)

Non ho ricevuto la chiamata da AWS per verificare il mio nuovo account

Quando crei un Account AWS, è necessario fornire un numero di telefono sul quale è possibile ricevere un SMS o una chiamata vocale. Si specifica il metodo da utilizzare per verificare il numero.

Se non ricevi il messaggio o la chiamata, verifica quanto segue:

- Hai inserito il numero di telefono corretto e selezionato il prefisso internazionale corretto durante la procedura di registrazione.
- Se utilizzi un telefono cellulare, assicurati di disporre di un segnale cellulare per ricevere SMS o chiamate.
- Le informazioni che hai inserito per il tuo [metodo di pagamento](#) è corretto.

Se non hai ricevuto un SMS o una chiamata per completare il processo di verifica dell'identità, AWS Support può aiutarti ad attivare il tuo Account AWS manualmente. Utilizza le fasi seguenti:

1. Assicurati di essere raggiungibile al [numero di telefono](#) che hai fornito per il tuo Account AWS.
2. Apri il [AWS Support](#) [plancia](#), quindi scegli Crea caso.
 - a. Scegli Account and billing support (Supporto account e fatturazione).
 - b. Per Tipo, seleziona Account.
 - c. Per Categoria, seleziona Attivazione.
 - d. Nella Descrizione del caso sezione, fornisci una data e un'ora in cui puoi essere contattato.

- e. NelOpzioni di contattosezione, selezionaChatperMetodi di contatto.
- f. Scegli Submit (Invia).

Note

Puoi creare una custodia conAWS Supportanche se il tuoAccount AWSnon è attivato.

Ricevo un messaggio di errore relativo al «numero massimo di tentativi falliti» quando provo a verificare il mioAccount AWSper telefono

AWS Supportpuò aiutarti ad attivare manualmente il tuo account. Completare la procedura riportata di seguito.

1. [Accedi al tuoAccount AWS](#)utilizzando l'indirizzo e-mail e la password che hai specificato durante la creazione del tuo account.
2. Apri il[AWS Supportplancia](#), quindi scegliCrea caso.
3. ScegliSupporto per account e fatturazione.
4. PerTipo, selezionaAccount.
5. PerCategoria, selezionaAttivazione.
6. NelDescrizione del casosezione, fornisci una data e un'ora in cui puoi essere contattato.
7. NelOpzioni di contattosezione, selezionaChatperMetodi di contatto.
8. Scegli Submit (Invia).

AWS Supportti contatterà e tenterà di attivare manualmente il tuoAccount AWS.

Sono passate più di 24 ore e il mio account non è stato attivato

L'attivazione dell'account a volte può essere ritardata. Se il processo richiede più di 24 ore, controlla quanto segue:

- Completa il processo di attivazione dell'account.

Se hai chiuso la finestra per la procedura di registrazione prima di aggiungere tutte le informazioni necessarie, apri il [registrazione](#) pagina. Scegli [Accedi a un account esistente](#) Account AWS e accedi utilizzando l'indirizzo e-mail e la password che hai scelto per l'account.

- Controlla le informazioni associate al tuo metodo di pagamento.

Nel [AWS Billing and Cost Management](#) console, controlla [Metodi di pagamento](#) per errori.

- Contatta il tuo istituto finanziario.

A volte gli istituti finanziari rifiutano le richieste di autorizzazione di AWS. Contatta l'istituto associato al tuo metodo di pagamento e chiedi loro di approvare le richieste di autorizzazione di AWS. AWS annulla la richiesta di autorizzazione non appena viene approvata dal tuo istituto finanziario, quindi non ti viene addebitato alcun costo per la richiesta di autorizzazione. Le richieste di autorizzazione potrebbero comunque apparire come un piccolo addebito (di solito 1 USD) sugli estratti conto del tuo istituto finanziario.

- Controlla la tua e-mail e la cartella spam per le richieste di informazioni aggiuntive.
- Prova con un altro browser.
- Contatti [AWS Support](#).

Contatti [AWS Support](#) per chiedere aiuto. Indica eventuali passaggi per la risoluzione dei problemi che hai già provato.

Note

Non fornire informazioni sensibili, come i numeri delle carte di credito, in nessuna corrispondenza con AWS.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.