Guida per l'utente

AWS Accedi

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Accedi: Guida per l'utente

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una 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

Che cos'è AWS l'accesso? 1
Terminologia 1
Amministratore 2
Account 2
Credenziali 2
Credenziali aziendali 2
Profilo 3
Credenziali utente root 3
Utente 3
Codice di verifica 3
Disponibilità nelle regioni 3
Eventi di accesso 4
Determina il tipo di utente 4
Utente root 5
Utente IAM 5
Utente IAM Identity Center 5
Identità federata 6
AWS Builder ID (utente) 7
Determina l'URL di accesso 7
Account AWS URL di accesso utente root 7
AWS portale di accesso 8
URL di accesso degli utenti IAM 8
URL di identità federata 9
AWS URL del Builder ID 9
Domini da aggiungere all'elenco dei domini consentiti 9
AWS Accedi ai domini nella lista consentita 10
Portale di accesso AWS domini da inserire nella lista consentita 10
ID Builder AWS domini da inserire nella lista consentita 10
Best practice di sicurezza 11
Accedi al AWS Management Console 13
Accesso come utente root 13
Per accedere come utente root 14
Informazioni aggiuntive 17
Accesso come utente IAM 17

Accesso come utente IAM 18
Accedi al portale di AWS accesso 19
Per accedere al portale di AWS accesso 19
Informazioni aggiuntive 20
Accedi tramite AWS Command Line Interface 22
Informazioni aggiuntive 22
Accedi come identità federata 23
Accedi con ID Builder AWS 24
Disponibilità nelle regioni 25
Crea il tuo ID Builder AWS 26
Dispositivi attendibili 27
AWS strumenti e servizi 27
Modifica il tuo profilo 28
Modifica la password 30
Elimina tutte le sessioni attive 31
Elimina il tuo ID Builder AWS 31
Gestione dell'autenticazione a più fattori (MFA) 32
Tipi di MFA disponibili 33
Registra il tuo ID Builder AWS dispositivo MFA 35
Registra una chiave di sicurezza come dispositivo ID Builder AWS MFA 37
Rinomina il tuo dispositivo ID Builder AWS MFA 37
Eliminare il dispositivo MFA 37
Privacy e dati 38
Richiedi i tuoi ID Builder AWS dati 38
ID Builder AWS e altre credenziali AWS 39
In che modo ID Builder AWS si collega alla tua identità IAM Identity Center esistente 39
Profili multipli ID Builder AWS 40
Esci da AWS 41
Esci dal AWS Management Console 41
Esci dal portale di AWS accesso 42
Esci da AWS Builder ID 43
Risoluzione dei problemi di Account AWS accesso 45
Le mie AWS Management Console credenziali non funzionano 46
La reimpostazione della password è richiesta per il mio utente root 47
Non ho accesso all'e-mail per il mio Account AWS 47
Il mio dispositivo MFA si è perso o ha smesso di funzionare 48

Non riesco ad accedere alla pagina di AWS Management Console accesso 49
Come posso trovare il mio ID o alias Account AWS 49
Ho bisogno del codice di verifica dell'account 52
Ho dimenticato la password dell'utente root per il mio Account AWS 52
Ho dimenticato la mia password utente IAM per il mio Account AWS 55
Ho dimenticato la mia password di identità federata per il mio Account AWS 57
Non riesco ad accedere al mio account esistente Account AWS e non riesco a crearne uno nuovo Account AWS con lo stesso indirizzo email 57
Devo riattivare il mio account sospeso Account AWS 57
Devo contattarci per problemi di accesso Supporto 58
Devo contattarci AWS Billing per problemi di fatturazione 58
Ho una domanda su un ordine al dettaglio 58
Ho bisogno di aiuto per gestire il mio Account AWS 58
Le mie credenziali del portale di AWS accesso non funzionano 58
Ho dimenticato la password del mio IAM Identity Center Account AWS 59
Ricevo un messaggio di errore che dice «Non sei tu, siamo noi» quando provo ad accedere 62
Risoluzione dei problemi relativi al AWS Builder ID 63
La mia e-mail è già in uso 63
Non è possibile completare la verifica dell'e-mail 64
Ricevo un messaggio di errore che dice «Non sei tu, siamo noi» quando provo ad accedere 64
Ho dimenticato la mia password 65
Non riesco a impostare una nuova password 65
La mia password non funziona 65
La mia password non funziona e non riesco più ad accedere alle e-mail inviate al mio indirizzo e-mail AWS Builder ID 66
Non riesco ad abilitare l'MFA 66
Non riesco ad aggiungere un'app di autenticazione come dispositivo MFA 66
Non riesco a rimuovere un dispositivo MFA 66
Ricevo il messaggio "An unexpected error has occurred" (Si è verificato un errore imprevisto) quando provo a registrarmi o accedere con un'app di autenticazione 67
Ricevo il messaggio «Non sei tu, siamo noi» quando provo ad accedere a Builder ID AWS 67
La disconnessione non mi disconnette completamente 67
Sto ancora cercando di risolvere il mio problema 67
Cronologia dei documenti 68
..... lxx

Che cos'è AWS l'accesso?

Questa guida ti aiuta a comprendere i diversi modi in cui puoi accedere ad Amazon Web Services (AWS), a seconda del tipo di utente. Per ulteriori informazioni su come accedere in base al tipo di utente e alle AWS risorse a cui desideri accedere, consulta uno dei seguenti tutorial.

- Accedi al AWS Management Console
- Accedi al portale di AWS accesso
- Accedi come identità federata
- Accedi tramite AWS Command Line Interface
- Accedi con ID Builder AWS

Se riscontri problemi di accesso al tuo Account AWS, consulta. Risoluzione dei problemi di Account AWS accesso Per assistenza con la tua ID Builder AWS vistaRisoluzione dei problemi relativi al AWS Builder ID. Stai cercando di creare un Account AWS? Iscriviti per AWS. Per ulteriori informazioni su come l'iscrizione AWS può aiutare te o la tua organizzazione, consulta Contattaci.

Argomenti

- Terminologia
- Disponibilità regionale per l' AWS accesso
- Registrazione degli eventi di accesso
- Determina il tipo di utente
- Determina l'URL di accesso
- Domini da aggiungere all'elenco dei domini consentiti
- Le migliori pratiche di sicurezza per Account AWS gli amministratori

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. Nelle procedure di autenticazione e identificazione un sistema utilizza le credenziali per identificare chi effettuare una chiamata e stabilire se consentire l'accesso richiesto. Le credenziali sono le informazioni fornite dagli utenti per AWS effettuare l'accesso e accedere alle risorse. AWS Le credenziali per gli utenti umani 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. Per l'accesso programmatico, puoi anche utilizzare le chiavi di accesso. Consigliamo di utilizzare chiavi di accesso a breve termine quando possibile.

Per ulteriori informazioni sulle credenziali, consulta Credenziali AWS di sicurezza.

> **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 utilizzi 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 è correlato a un Account AWS, vediID Builder AWS e altre credenziali AWS.

Credenziali utente root

Le credenziali dell'utente root sono l'indirizzo e-mail e la password utilizzati per creare il. Account AWS Si consiglia vivamente di aggiungere l'MFA alle credenziali dell'utente root per una maggiore sicurezza. Le credenziali dell'utente root forniscono l'accesso completo a tutti i AWS servizi e le risorse dell'account. Per ulteriori informazioni sull'utente root, vedereUtente root.

Utente

Un utente è una persona o un'applicazione che dispone delle autorizzazioni per effettuare chiamate API ai AWS prodotti o per accedere alle AWS risorse. Ogni utente dispone di un set unico di credenziali di sicurezza che non vengono condivise con altri utenti. Queste credenziali sono distinte dalle credenziali di sicurezza dell' Account AWS. Per ulteriori informazioni, consulta Determina il tipo di utente.

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.

Disponibilità regionale per l' AWS accesso

AWS L'accesso è disponibile in diverse versioni di uso comune. Regioni AWS Questa disponibilità semplifica l'accesso ai AWS servizi e alle applicazioni aziendali. Per un elenco completo delle regioni supportate da Sign-In, consulta Endpoint e quote di AWS accesso.

Registrazione degli eventi di accesso

CloudTrail è abilitato automaticamente sul tuo computer Account AWS e registra gli eventi quando si verifica un'attività. Le seguenti risorse possono aiutarti a saperne di più sulla registrazione e il monitoraggio degli eventi di accesso.

- CloudTrail registra i tentativi di accesso a. AWS Management Console Tutti gli eventi di accesso di utenti IAM, utenti root e utenti federati generano record nei CloudTrail file di registro. Per ulteriori informazioni, consulta Eventi di accesso alla AWS Management Console nella Guida per l'utente di AWS CloudTrail .
- Se si utilizza un endpoint regionale per accedere a AWS Management Console, CloudTrail registra l'`ConsoleLogin`evento nella regione appropriata per l'endpoint. Per ulteriori informazioni sugli endpoint di AWS accesso, consulta Endpoint e quote di AWS accesso nella Guida di riferimento generale.AWS
- Per ulteriori informazioni su come CloudTrail registra gli eventi di accesso per IAM Identity Center, consulta Comprendere gli eventi di accesso a IAM Identity Center nella Guida per l'utente di IAM Identity Center.
- Per ulteriori informazioni su come CloudTrail registrare le diverse informazioni sull'identità degli utenti in IAM, consulta la sezione Registrazione delle chiamate IAM e AWS STS API nella Guida per l'utente. AWS CloudTrailAWS Identity and Access Management

Determina il tipo di utente

Il modo in cui accedi dipende dal tipo di AWS utente che sei. Puoi gestirlo Account AWS come utente root, un utente IAM, un utente in IAM Identity Center o un'identità federata. Puoi utilizzare un profilo AWS Builder ID per accedere a determinati AWS servizi e strumenti. I diversi tipi di utente sono elencati di seguito.

Argomenti

- Utente root
- Utente IAM
- Utente IAM Identity Center
- Identità federata
- AWS Builder ID (utente)

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. La prima volta che ne crei un Account AWS, inizi con un'identità di accesso singolo che ha accesso completo a tutti i AWS servizi e le risorse dell'account. Questa identità è l'utente root dell' AWS account. Puoi accedere come utente root utilizzando l'indirizzo e-mail e la password usati per creare l'account. Gli utenti root accedono con AWS Management Console. Per istruzioni dettagliate su come accedere, vedereAccedi AWS Management Console come utente root.

> **Important**
>
> Quando ne crei uno Account AWS, inizi con un'unica identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso 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 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

Un utente IAM è un'entità in cui crei. AWS 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, vediAccedi 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).

Utente IAM Identity Center

Un utente IAM Identity Center è membro di AWS Organizations e può avere accesso a più Account AWS applicazioni tramite il portale di AWS accesso. Se la loro azienda ha integrato Active Directory o

un altro provider di identità con IAM Identity Center, gli utenti di IAM Identity Center possono utilizzare le proprie credenziali aziendali per accedere. IAM Identity Center può anche essere un provider di identità in cui un amministratore può creare utenti. Indipendentemente dal provider di identità, gli utenti di IAM Identity Center accedono utilizzando il portale di AWS accesso, che è un URL di accesso specifico per la loro organizzazione. Gli utenti di IAM Identity Center non possono accedere tramite l' AWS Management Console URL.

Gli utenti umani in IAM Identity Center possono ottenere l'URL del portale di AWS accesso da:

- Un messaggio dell'amministratore o del dipendente dell'help desk
- Un'e-mail AWS con un invito a iscriversi a IAM Identity Center

> **Tip**
>
> Tutte le e-mail inviate dal servizio IAM Identity Center provengono dall'indirizzo no-reply@signin.aws o no-reply@login.awsapps.com. Ti consigliamo di configurare il tuo sistema di posta elettronica in modo che accetti le e-mail da questi indirizzi e-mail dei mittenti e non le gestisca come posta indesiderata o spam.

Per istruzioni dettagliate su come accedere, consulta. Accedi al portale di AWS accesso

> **Note**
>
> Ti consigliamo di aggiungere ai preferiti l'URL di accesso specifico della tua organizzazione per il portale di AWS accesso in modo da potervi accedere 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 accedi né accedi al AWS

Management Console portale AWS . Al contrario, l'identità esterna in uso determina la modalità di accesso.

Per ulteriori informazioni, consulta Accedi come identità federata.

AWS Builder ID (utente)

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 Accedi con ID Builder AWS.

AWS Builder ID è separato dall'abbonamento a AWS Skill Builder, un centro di apprendimento online in cui puoi imparare dagli AWS esperti e sviluppare competenze online sul cloud. Per ulteriori informazioni su AWS Skill Builder, consulta AWS Skill Builder.

Determina l'URL di accesso

Usa uno dei seguenti metodi URLs per accedere AWS a seconda del tipo di AWS utente che sei. Per ulteriori informazioni, consulta Determina il tipo di utente.

Argomenti

- Account AWS URL di accesso utente root
- AWS portale di accesso
- URL di accesso degli utenti IAM
- URL di identità federata
- AWS URL del Builder ID

Account AWS URL di accesso utente root

L'utente root accede a AWS Management Console dalla pagina di AWS accesso:. `https://console.aws.amazon.com/`

Questa pagina di accesso ha anche la possibilità di accedere come utente IAM.

AWS portale di accesso

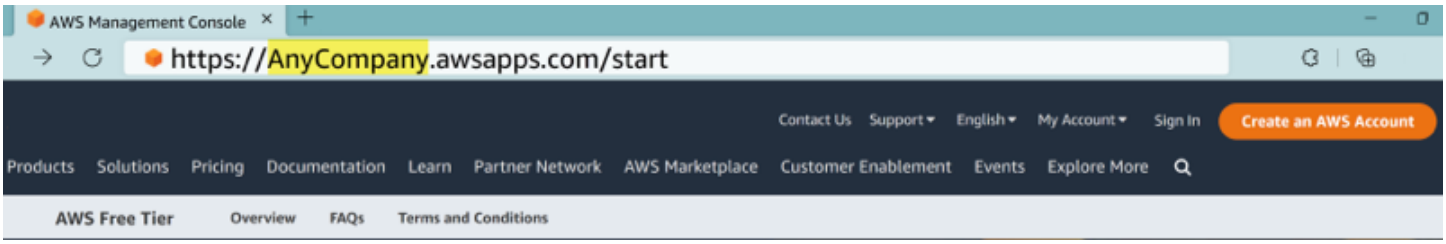
Il portale di AWS accesso è un URL di accesso specifico che consente agli utenti di IAM Identity Center di accedere al tuo account. Quando un amministratore crea l'utente in IAM Identity Center, l'amministratore sceglie se l'utente riceve un invito via e-mail a iscriversi a IAM Identity Center o un messaggio dall'amministratore o dal dipendente dell'help desk contenente una password monouso e AWS l'URL del portale di accesso. Il formato dell'URL di accesso specifico è simile ai seguenti esempi:

```
https://d-xxxxxxxxxx.awsapps.com/start
```

oppure

```
https://your_subdomain.awsapps.com/start
```

L'URL di accesso specifico varia perché l'amministratore può personalizzarlo. L'URL di accesso specifico potrebbe iniziare con la lettera D seguita da 10 numeri e lettere randomizzati. Il tuo sottodominio potrebbe essere utilizzato anche nell'URL di accesso e includere il nome della tua azienda, come nell'esempio seguente:



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

Per ulteriori informazioni sul portale di AWS accesso, vedere Utilizzo del portale di AWS accesso.

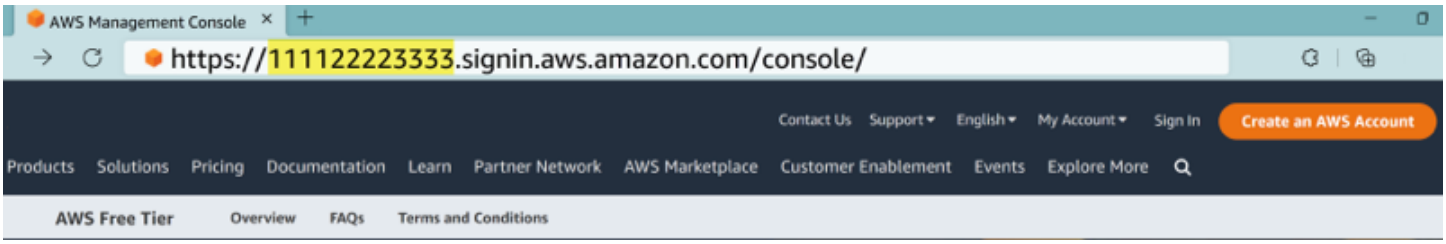
URL di accesso degli utenti IAM

Gli utenti IAM possono accedere a AWS Management Console con un URL di accesso utente IAM specifico. L'URL di accesso utente IAM combina il tuo Account AWS ID o alias e `signin.aws.amazon.com/console`

Un esempio di come appare l'URL di accesso di un utente IAM:

```
https://account_alias_or_id.signin.aws.amazon.com/console/
```

Se l'ID del tuo account è 111122223333, l'URL di accesso sarebbe:



Se riscontri problemi di accesso Account AWS con l'URL di accesso utente IAM, consulta Resilience in AWS Identity and Access Management per ulteriori informazioni.

URL di identità federata

L'URL di accesso per un'identità federata varia. L'identità esterna o l'Identity Provider (IdP) esterno determina l'URL di accesso per le identità federate. L'identità esterna potrebbe essere Windows Active Directory, Login with Amazon, Facebook o Google. Contatta il tuo amministratore per maggiori dettagli su come accedere come identità federata.

Per ulteriori informazioni sulle identità federate, consulta Informazioni sulla federazione delle identità web.

AWS URL del Builder ID

L'URL del tuo profilo AWS Builder ID è. https://profile.aws.amazon.com/ Quando usi il tuo AWS Builder ID, l'URL di accesso dipende dal servizio a cui desideri accedere. Ad esempio, per accedere ad Amazon CodeCatalyst, vai ahttps://codecatalyst.aws/login.

Domini da aggiungere all'elenco dei domini consentiti

Se si filtra l'accesso a AWS domini o endpoint URL specifici utilizzando una soluzione di filtraggio dei contenuti Web come firewall di nuova generazione (NGFW) o Secure Web Gateways (SWG), è necessario aggiungere i seguenti domini o endpoint URL agli elenchi consentiti della soluzione di filtraggio dei contenuti Web.

AWS Accedi ai domini nella lista consentita

Se tu o la tua organizzazione implementate il filtraggio degli IP o dei domini, potrebbe essere necessario consentire l'utilizzo di. AWS Management Console I seguenti domini devono essere accessibili sulla rete da cui si sta tentando di accedere a. AWS Management Console

- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

Portale di accesso AWS domini da inserire nella lista consentita

Se si filtra l'accesso a AWS domini o endpoint URL specifici utilizzando una soluzione di filtraggio dei contenuti Web come firewall di nuova generazione (NGFW) o Secure Web Gateways (SWG), è necessario aggiungere i seguenti domini o endpoint URL agli elenchi consentiti della soluzione di filtraggio dei contenuti Web. In questo modo è possibile accedere a. Portale di accesso AWS

- *[Directory ID or alias]*.awsapps.com
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- *.sso-portal.*[Region]*.amazonaws.com

ID Builder AWS domini da inserire nella lista consentita

Se tu o la tua organizzazione implementate il filtraggio degli IP o dei domini, potrebbe essere necessario consentire i domini in elenco per creare e utilizzare un. ID Builder AWS I seguenti domini devono essere accessibili sulla rete da cui si sta tentando di accedere. ID Builder AWS

- view.awsapps.com/start

- `*.aws.dev`
- `*.uis.awsstatic.com`
- `*.console.aws.a2z.com`
- `oidc.*.amazonaws.com`
- `*.sso.amazonaws.com`
- `*.sso.*.amazonaws.com`
- `*.sso-portal.*.amazonaws.com`
- `*.signin.aws`
- `*.cloudfront.net`
- `opfcaptcha-prod.s3.amazonaws.com`
- `profile.aws.amazon.com`

Le migliori pratiche di sicurezza per Account AWS gli amministratori

Se sei un amministratore di account che ne ha creato uno nuovo Account AWS, ti consigliamo di seguire i seguenti passaggi per aiutare i tuoi utenti a seguire le migliori pratiche di AWS sicurezza al momento dell'accesso.

1. Accedi come utente root per abilitare l'autenticazione a più fattori (MFA) e crea AWS un utente amministrativo in IAM Identity Center se non l'hai già fatto. Quindi, proteggi le tue credenziali root e non usarle per le attività quotidiane.
2. Accedi come Account AWS amministratore e configura le seguenti identità:
   - Crea utenti con privilegi minimi per altri umani.
   - Imposta credenziali temporanee per i carichi di lavoro.
   - Crea chiavi di accesso solo per casi d'uso che richiedono credenziali a lungo termine.
3. Aggiungi le autorizzazioni per concedere l'accesso a tali identità. Puoi iniziare con le policy AWS gestite e passare alle autorizzazioni con privilegi minimi.
   - Aggiungi set di autorizzazioni agli utenti di AWS IAM Identity Center (successore di Single Sign-On). AWS
   - Aggiungi policy basate sull'identità ai ruoli IAM utilizzati per i carichi di lavoro.
   - Aggiungi policy basate sull'identità per gli utenti IAM per i casi d'uso che richiedono credenziali a lungo termine.

- Per ulteriori informazioni sugli utenti IAM, consulta Best practice di sicurezza in IAM.

4. Salva e condividi informazioni suAccedi al AWS Management Console. Queste informazioni variano a seconda del tipo di identità che hai creato.
5. Mantieni aggiornati l'indirizzo e-mail dell'utente root e il numero di telefono di contatto dell'account principale per assicurarti di poter ricevere notifiche importanti relative all'account e alla sicurezza.

   - Modifica il nome dell'account, l'indirizzo email o la password per. Utente root dell'account AWS
   - Accedere o aggiornare il contatto principale dell'account.
6. Consulta le best practice di sicurezza in IAM per scoprire altre best practice di gestione delle identità e degli accessi.

Accedi al AWS Management Console

Quando accedi AWS Management Console dall'URL di AWS accesso principale (https://console.aws.amazon.com/), devi scegliere il tipo di utente, utente root o utente IAM. Se non sei sicuro del tipo di utente che sei, vediDetermina il tipo di utente.

L'utente root ha accesso illimitato all'account ed è associato alla persona che ha creato il Account AWS. L'utente root crea quindi altri tipi di utenti, come gli utenti IAM e utenti in Centro identità AWS IAM, e assegna loro le credenziali di accesso.

Un utente IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni personalizzate specifiche. Quando un utente IAM accede, può utilizzare un URL di accesso che include il proprio alias Account AWS or, ad esempio `https://account_alias_or_id.signin.aws.amazon.com/console/` anziché l'URL di AWS accesso principale. `https://console.aws.amazon.com/`

Puoi accedere a un massimo di 5 identità diverse contemporaneamente in un unico browser in. AWS Management Console Questi possono essere una combinazione di utenti root, utenti IAM o ruoli federati in account diversi o nello stesso account. Per i dettagli, consulta Accedere a più account nella Guida AWS Management Console introduttiva.

Tutorial

- Accedi AWS Management Console come utente root
- Accedi AWS Management Console come utente IAM

Se non sei sicuro del tipo di utente che sei, consultaDetermina il tipo di utente.

Tutorial

- Accedi AWS Management Console come utente root
- Accedi AWS Management Console come utente IAM

Accedi AWS Management Console come utente root

La prima volta che crei un account Account AWS, inizi con un'unica identità di accesso con accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità si chiama utente Account AWS

root ed è accessibile effettuando l'accesso 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 Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Per accedere come utente root

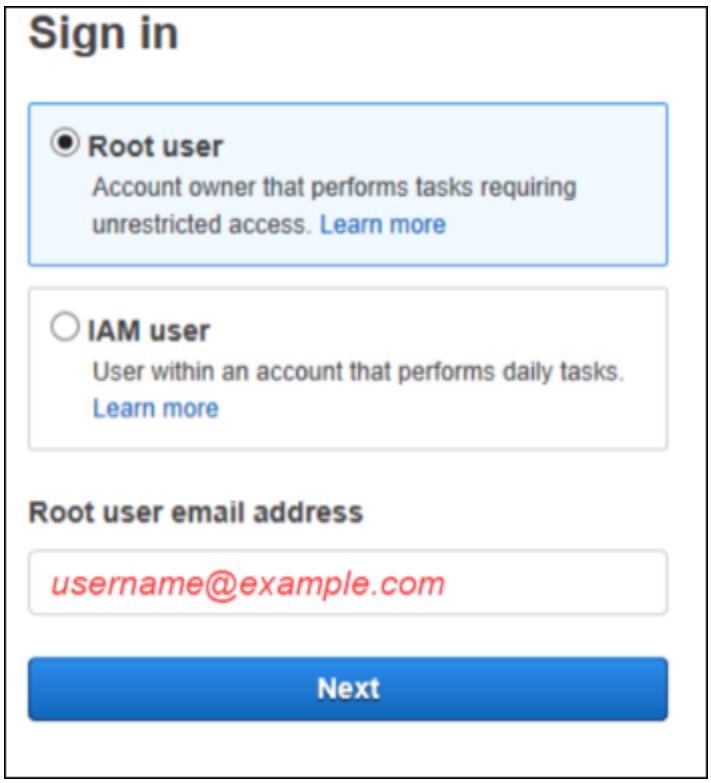
Puoi accedere come utente root mentre hai già effettuato l'accesso a un'altra identità in AWS Management Console. Per i dettagli, consulta Accesso a più account nella Guida AWS Management Console introduttiva.

Account AWS managed using AWS Organizations potrebbe non avere credenziali utente root ed è necessario contattare un amministratore per eseguire azioni come utente root nel proprio account membro. Se non riesci ad accedere come utente root, consultaRisoluzione dei problemi di Account AWS accesso.

1. Apri il AWS Management Console filehttps://console.aws.amazon.com/.

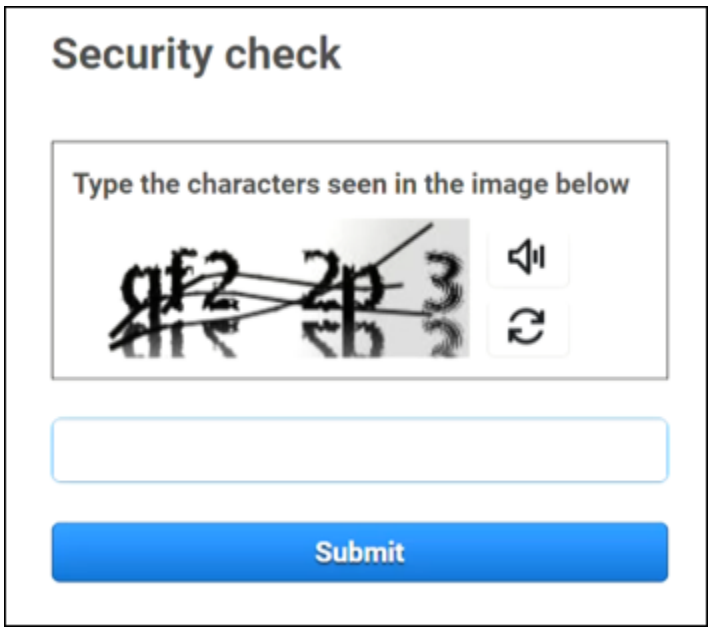
   > **Note**
   >
   > Se hai effettuato l'accesso in precedenza come utente IAM utilizzando questo browser, il tuo browser potrebbe invece visualizzare la pagina di accesso degli utenti IAM. Scegli Accedi utilizzando l'e-mail dell'utente root.

2. Scegli Utente root.



3. In Indirizzo e-mail dell'utente root, inserisci l'indirizzo e-mail associato all'utente root. Quindi, seleziona Avanti.
4. Se ti viene richiesto di completare un controllo di sicurezza, inserisci i caratteri visualizzati per continuare. 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.

> **Tip**
>
> Digita i caratteri alfanumerici che vedi (o ascolti) in ordine senza spazi.



5. Inserisci la password.

6. Autenticazione con MFA. L'MFA viene applicata per impostazione predefinita all'utente root. Per gli utenti root di account indipendenti e membri, è necessario abilitare manualmente l'MFA, operazione fortemente consigliata. Per ulteriori informazioni, consulta Autenticazione a più fattori per utenti Account AWS root nella Guida per l'utente.AWS Identity and Access Management

> **Tip**
>
> Come best practice in materia di sicurezza, consigliamo di rimuovere tutte le credenziali dell'utente root dagli account dei membri AWS dell'organizzazione per prevenire l'uso non autorizzato. Se scegli questa opzione, gli account membro non possono accedere come utente root, eseguire il ripristino della password o configurare l'MFA. In questo caso, solo l'amministratore dell'account di gestione può eseguire un'operazione che richiede le credenziali dell'utente root in un account membro. Per i dettagli, consulta Gestire centralmente l'accesso root per gli account dei membri nella Guida per l'AWS Identity and Access Management utente.

7. Selezionare Sign in (Accedi). AWS Management Console Appare.

Dopo l'autenticazione, AWS Management Console si apre la home page della console.

Informazioni aggiuntive

Se desideri maggiori informazioni sull'utente Account AWS root, consulta le seguenti risorse.

- Per una panoramica dell'utente root, vedi utente Account AWS root.
- Per i dettagli sull'utilizzo dell'utente root, vedere Uso dell'utente Account AWS root.
- Per step-by-step istruzioni su come reimpostare la password dell'utente root, vedereHo dimenticato la password dell'utente root per il mio Account AWS.

Accedi AWS Management Console come utente IAM

Un utente IAM è un'identità creata all'interno di un utente Account AWS che dispone del permesso di interagire con AWS le risorse. Gli utenti IAM accedono utilizzando l'ID o l'alias dell'account, il nome utente e una password. I nomi utente IAM sono configurati dall'amministratore. I nomi utente IAM possono essere nomi descrittivi*Zhang*, ad esempio, o indirizzi e-mail come*zhang@example.com*. I nomi utente IAM non possono includere spazi, ma possono includere lettere maiuscole e minuscole, numeri e simboli`+ = , . @ _ -`.

> **Tip**
>
> Se il tuo utente IAM ha abilitato l'autenticazione a più fattori (MFA), devi avere accesso al dispositivo di autenticazione. Per i dettagli, consulta Utilizzo dei dispositivi MFA con la pagina di accesso IAM.

Accesso come utente IAM

Puoi accedere come utente IAM mentre hai già effettuato l'accesso a un'altra identità in AWS Management Console. Per i dettagli, consulta Accesso a più account nella Guida AWS Management Console introduttiva.

1. Apri il AWS Management Console filehttps://console.aws.amazon.com/.
2. Viene visualizzata la pagina di accesso principale. Inserisci l'ID dell'account (12 cifre) o l'alias, il nome utente IAM e la password.

   > **Note**
   >
   > Potresti non dover inserire l'ID o l'alias del tuo account se hai già effettuato l'accesso come utente IAM con il tuo browser attuale o se stai utilizzando l'URL di accesso del tuo account.

3. Selezionare Sign in (Accedi).
4. Se l'MFA è abilitata per il tuo utente IAM, AWS richiede di confermare la tua identità con un autenticatore. Per ulteriori informazioni, vedere Utilizzo dell'autenticazione a più fattori (MFA) in. AWS

Dopo l'autenticazione, AWS Management Console si apre la home page della console.

Informazioni aggiuntive

Se desideri maggiori informazioni sugli utenti IAM, consulta le seguenti risorse.

- Per una panoramica di IAM, consulta What is Identity and Access Management?
- Per informazioni dettagliate sull' AWS account IDs, consulta L'ID AWS dell'account e il suo alias.
- Per step-by-step istruzioni su come reimpostare la password utente IAM, consultaHo dimenticato la mia password utente IAM per il mio Account AWS.

Accedi al portale di AWS accesso

Un utente di IAM Identity Center è membro di AWS Organizations. Un utente di IAM Identity Center può accedere a più Account AWS applicazioni aziendali accedendo al portale di AWS accesso con un URL di accesso specifico. Per ulteriori informazioni sull'URL di accesso specifico, consulta. AWS portale di accesso

Prima di accedere Account AWS come utente a IAM Identity Center, raccogli le seguenti informazioni obbligatorie.

- Nome utente aziendale
- Password aziendale
- URL di accesso specifico

> **Note**
>
> Dopo l'accesso, la sessione del portale di AWS accesso è valida per 8 ore. È necessario effettuare nuovamente l'accesso dopo 8 ore.

Per accedere al portale di AWS accesso

1. Nella finestra del browser, incolla l'URL di accesso che ti è stato fornito tramite e-mail, ad esempio`https://your_subdomain.awsapps.com/start`. Quindi, premere Invio.
2. Accedi utilizzando le tue credenziali aziendali (come nome utente e password).

   > **Note**
   >
   > Se l'amministratore ti ha inviato un'e-mail con una password monouso (OTP) e questa è la prima volta che accedi, inserisci quella password. Dopo aver effettuato l'accesso, devi creare una nuova password per gli accessi futuri.

3. Se ti viene chiesto un codice di verifica, controlla la tua email. Quindi copia e incolla il codice nella pagina di accesso.

> **Note**
>
> I codici di verifica vengono generalmente inviati tramite e-mail, ma il metodo di consegna potrebbe variare. Se non ne hai ricevuto uno nella tua email, contatta l'amministratore per i dettagli sul codice di verifica.

4. Se l'MFA è abilitata per il tuo utente in IAM Identity Center, esegui l'autenticazione utilizzandola.
5. Dopo l'autenticazione, puoi accedere a qualsiasi Account AWS applicazione visualizzata nel portale.

   a. Per accedere, AWS Management Console scegli la scheda Account e seleziona il singolo account da gestire.

      Viene visualizzato il ruolo dell'utente. Scegli il nome del ruolo per l'account da aprire AWS Management Console. Scegli le chiavi di accesso per ottenere le credenziali per l'accesso da riga di comando o programmatico.

   b. Scegli la scheda Applicazioni per visualizzare le applicazioni disponibili e scegli l'icona dell'applicazione a cui desideri accedere.

L'accesso come utente in IAM Identity Center fornisce le credenziali per accedere alle risorse per un determinato periodo di tempo, chiamato sessione. Per impostazione predefinita, un utente può accedere a un account Account AWS per 8 ore. L'amministratore di IAM Identity Center può specificare una durata diversa, da un minimo di 15 minuti a un massimo di 90 giorni. Al termine della sessione, puoi accedere nuovamente.

Informazioni aggiuntive

Se desideri maggiori informazioni sugli utenti in IAM Identity Center, consulta le seguenti risorse.

- Per una panoramica di IAM Identity Center, consulta Cos'è IAM Identity Center?
- Per i dettagli sul portale di AWS accesso, consulta Utilizzo del portale di AWS accesso.
- Per i dettagli sulle sessioni di IAM Identity Center, consulta Autenticazioni degli utenti.
- Per step-by-step istruzioni su come reimpostare la password utente di IAM Identity Center, consulta. Ho dimenticato la password del mio IAM Identity Center Account AWS
- Se tu o la tua organizzazione implementate il filtraggio degli IP o dei domini, potresti dover consentire ai domini di creare e utilizzare il tuo AWS portale di accesso. Per informazioni

dettagliate sulla creazione di domini consentiti, consulta. Domini da aggiungere all'elenco dei domini consentiti

Accedi tramite AWS Command Line Interface

Ti consigliamo di configurare un utente in IAM Identity Center se prevedi di utilizzare il AWS Command Line Interface. L'interfaccia utente del portale di AWS accesso consente agli utenti di IAM Identity Center di selezionare facilmente Account AWS e AWS CLI utilizzare le credenziali di sicurezza temporanee. Per ulteriori informazioni su come ottenere queste credenziali, consulta. Disponibilità regionale per ID Builder AWS Puoi anche configurarlo AWS CLI direttamente per autenticare gli utenti con IAM Identity Center.

Per accedere tramite le credenziali AWS CLI con IAM Identity Center

- Verifica di aver completato i prerequisiti.
- Se accedi per la prima volta, configura il tuo profilo con la `aws configure sso` procedura guidata.
- Dopo aver configurato il profilo, esegui il comando seguente, quindi segui le istruzioni nel tuo terminale.

```
$ aws sso login --profile my-profile
```

Informazioni aggiuntive

Se desideri maggiori informazioni sull'accesso tramite la riga di comando, consulta le seguenti risorse.

- Per i dettagli sull'utilizzo delle credenziali di IAM Identity Center, consulta Ottenere le credenziali utente di IAM Identity Center for the or. AWS CLI AWS SDKs
- Per i dettagli sulla configurazione, consulta Configurazione per l' AWS CLI utilizzo di IAM Identity Center.
- Per maggiori dettagli sulla procedura di AWS CLI accesso, consulta Accesso e ottenimento delle credenziali.

Accedi come identità federata

Un'identità federata è un utente che può accedere a Account AWS risorse sicure con identità esterne. Le identità esterne possono provenire da un archivio di identità aziendali (ad esempio LDAP o Windows Active Directory) o da terze parti (ad esempio Login with Amazon, Facebook e Google). Le identità federate non accedono né accedono al AWS Management Console portale. AWS Il tipo di identità esterna in uso determina il modo in cui le identità federate accedono.

Gli amministratori devono creare un URL personalizzato che includa `https://signin.aws.amazon.com/federation`. Per ulteriori informazioni, consulta Abilitazione dell'accesso del gestore di identità personalizzato alla AWS Management Console.

> **Note**
>
> L'amministratore crea le identità federate. Contatta il tuo amministratore per maggiori dettagli su come accedere come identità federata.

Per ulteriori informazioni sulle identità federate, consulta About web identity federation.

Accedi con ID Builder AWS

ID Builder AWS è un profilo personale che fornisce l'accesso a strumenti e servizi selezionati, tra cui Amazon CodeCatalyst, Amazon Q Developer AWS Training e Certification. ID Builder AWS ti rappresenta come individuo ed è indipendente dalle credenziali e dai dati che potresti avere negli AWS account esistenti. Come gli altri profili personali, ID Builder AWS rimane con te mentre progredisci verso i tuoi obiettivi personali, educativi e di carriera.

I ID Builder AWS complementi Account AWS che possiedi già o che desideri creare. Sebbene un Account AWS funga da contenitore per AWS le risorse che crei e fornisca un limite di sicurezza per tali risorse, il tuo ti ID Builder AWS rappresenta come individuo. Per ulteriori informazioni, consulta ID Builder AWS e altre credenziali AWS.

ID Builder AWS è gratuito. Paghi solo per le AWS risorse che consumi nel tuo Account AWS. Per ulteriori informazioni sui prezzi, consulta Prezzi di AWS.

Se tu o la tua organizzazione implementate il filtraggio degli IP o dei domini, potrebbe essere necessario consentire ai domini di creare e utilizzare un. ID Builder AWS Per informazioni dettagliate sulla creazione di domini consentiti, consulta. Domini da aggiungere all'elenco dei domini consentiti

> **Note**
>
> AWS Builder ID è separato dall'abbonamento a AWS Skill Builder, un centro di apprendimento online in cui puoi imparare dagli AWS esperti e sviluppare competenze online sul cloud. Per ulteriori informazioni su AWS Skill Builder, consulta AWS Skill Builder.

Per accedere con ID Builder AWS

1. Vai al ID Builder AWS profilo o alla pagina di accesso dello AWS strumento o del servizio a cui desideri accedere. Ad esempio, per accedere ad Amazon CodeCatalyst, vai su https://codecatalyst.aws e scegli Accedi.
2. In Il tuo indirizzo e-mail, inserisci l'indirizzo e-mail che hai usato per creare il tuo ID Builder AWS e scegli Avanti.
3. (Facoltativo) Se desideri che i futuri accessi da questo dispositivo non richiedano ulteriori verifiche, seleziona la casella accanto a Questo è un dispositivo affidabile.

> **Note**
>
> Per la tua sicurezza, analizziamo il browser di accesso, la posizione e il dispositivo. Se indichi questo dispositivo come attendibile, non dovrai fornire un codice di autenticazione a più fattori (MFA) ogni volta che accedi. Per ulteriori informazioni, consulta Dispositivi attendibili.

4. Nella pagina Inserisci la password, inserisci la password, quindi scegli Accedi.
5. Se viene richiesta una pagina di verifica aggiuntiva, segui le istruzioni del browser per fornire il codice o la chiave di sicurezza richiesti.

Argomenti

- Disponibilità regionale per ID Builder AWS
- Crea il tuo ID Builder AWS
- AWS strumenti e servizi che utilizzano ID Builder AWS
- Modifica il tuo profilo ID Builder AWS
- Cambia la tua ID Builder AWS password
- Elimina tutte le sessioni attive per il tuo ID Builder AWS
- Elimina il tuo ID Builder AWS
- Gestione dell' ID Builder AWS autenticazione a più fattori (MFA)
- Privacy e accesso ai dati ID Builder AWS
- ID Builder AWS e altre credenziali AWS

Disponibilità regionale per ID Builder AWS

ID Builder AWS è disponibile di seguito Regioni AWS. Le applicazioni che utilizzano ID Builder AWS possono funzionare in altre regioni.

Nome	Codice
US East (N. Virginia)	us-east-1

Crea il tuo ID Builder AWS

Il tuo lo crei ID Builder AWS quando ti iscrivi a uno degli AWS strumenti e servizi che lo utilizzano. Registrati con il tuo indirizzo e-mail, nome e password nell'ambito della procedura di registrazione a uno strumento o servizio AWS .

La tua password deve soddisfare i seguenti requisiti:

- Le password distinguono tra maiuscole e minuscole.
- La lunghezza delle password deve essere compresa tra 8 e 64 caratteri.
- Le password devono contenere almeno un carattere per ognuna delle quattro categorie seguenti:
  - Lettere minuscole (a-z)
  - Lettere maiuscole (A-Z)
  - Numeri (0-9)
  - Caratteri non alfanumerici (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- Le ultime tre password non possono essere riutilizzate.
- Le password che sono note pubblicamente attraverso un set di dati divulgato da terzi non possono essere utilizzate.

> **Note**
>
> Gli strumenti e i servizi che utilizzi ID Builder AWS ti consentono di crearli e utilizzarli ID Builder AWS quando necessario.

Per creare il tuo ID Builder AWS

1. Vai al ID Builder AWS profilo o alla pagina di registrazione dello AWS strumento o del servizio a cui desideri accedere. Ad esempio, per accedere ad Amazon CodeCatalyst, vai ahttps://codecatalyst.aws.
2. Nella ID Builder AWS pagina Crea, inserisci il tuo indirizzo email. Consigliamo di utilizzare un indirizzo e-mail personale.
3. Scegli Next (Successivo).
4. Inserisci il tuo nome, quindi scegli Avanti.

5. Nella pagina Email verification (Verifica e-mail), inserisci il codice di verifica inviato al tuo indirizzo e-mail. Selezionare Verify (Verifica). A seconda del tuo provider di posta elettronica, per ricevere l'e-mail potrebbero essere necessari alcuni minuti. Controlla le cartelle dello spam e della posta indesiderata. Se non vedi l'email inviata AWS dopo cinque minuti, scegli Reinvia codice.
6. Dopo aver verificato la tua e-mail, nella pagina Choose a password (Scegli una password), inserisci una password e poi scegli Confirm password (Conferma password).
7. Se viene visualizzato un Captcha come protezione aggiuntiva, inserisci i caratteri che vedi.
8. Scegli Create ID Builder AWS (Crea).

Dispositivi attendibili

Dopo aver selezionato l'opzione This is a trusted device (Questo è un dispositivo attendibile) dalla pagina di accesso, considereremo autorizzati tutti gli accessi futuri da quel browser Web su quel dispositivo. Ciò significa che non sarà più necessario fornire un codice MFA per quel dispositivo attendibile. Tuttavia, se il browser, i cookie o l'indirizzo IP cambiano, potrebbe essere necessario utilizzare il codice MFA per una verifica aggiuntiva.

AWS strumenti e servizi che utilizzano ID Builder AWS

Puoi accedere con il tuo ID Builder AWS per accedere ai seguenti AWS strumenti e servizi. L'accesso alle funzionalità o ai vantaggi offerti a pagamento richiede un Account AWS.

Per impostazione predefinita, quando accedi a AWS uno strumento o servizio utilizzando il tuo ID Builder AWS, la durata della sessione dura 30 giorni ad eccezione di Amazon Q Developer, che ha una durata della sessione di 90 giorni. Al termine della sessione, dovrai effettuare nuovamente l'accesso.

AWS Comunità cloud

> Community.aws è una piattaforma di e per la community di AWS costruttori a cui puoi accedere con il tuo. ID Builder AWSÈ un posto dove scoprire contenuti didattici, condividere pensieri e progetti personali, commentare i post degli altri e seguire i tuoi costruttori preferiti.

Amazon CodeCatalyst

> Creerai un alias ID Builder AWS quando inizierai a usare Amazon CodeCatalyst e sceglierai un alias da associare ad attività come issue, code commit e pull request. Invita altre persone nel tuo

CodeCatalyst spazio Amazon, che è completo degli strumenti, dell'infrastruttura e degli ambienti di cui il tuo team ha bisogno per realizzare il tuo prossimo progetto di successo. Ti servirà un Account AWS account per implementare un nuovo progetto nel cloud.

AWS Migration Hub

Accedi a AWS Migration Hub(Migration Hub) con il tuo ID Builder AWS. Migration Hub offre un unico posto per scoprire i server esistenti, pianificare le migrazioni e monitorare lo stato di ogni migrazione di applicazioni.

Amazon Q Developer

Amazon Q Developer è un assistente conversazionale generativo basato sull'intelligenza artificiale che può aiutarti a comprendere, creare, estendere e utilizzare le applicazioni. AWS Per ulteriori informazioni, consulta Cos'è Amazon Q Developer? nella Guida per l'utente di Amazon Q Developer.

AWS re:Post

AWS re:Postti fornisce una guida tecnica esperta in modo da poter innovare più velocemente e migliorare l'efficienza operativa utilizzando i servizi. AWS Puoi accedere con la tua ID Builder AWS ed entrare a far parte della community su re:post senza carta di credito Account AWS .

AWS Startup

Usa il tuo ID Builder AWS per iscriverti a AWS Startup dove puoi utilizzare contenuti didattici, strumenti, risorse e supporto per far crescere la tua startup. AWS

AWS Training e certificazione

Puoi utilizzare la tua certificazione ID Builder AWS per accedere AWS Training e sviluppare Cloud AWS le tue competenze con AWS Skill Builder, imparare dagli AWS esperti e convalidare la tua esperienza nel cloud con una credenziale riconosciuta nel settore.

Portale di registrazione del sito Web (WRP)

È possibile utilizzare l'identità ID Builder AWS del cliente e il profilo di registrazione permanenti per il sito Web AWS di marketing. Per registrarti a nuovi webinar e per visualizzare tutti i webinar a cui ti sei registrato o a cui hai partecipato, consulta La sezione I miei webinar.

Modifica il tuo profilo ID Builder AWS

Puoi modificare le informazioni del tuo profilo in qualsiasi momento. Puoi modificare l'indirizzo e-mail e il nome che hai usato per creare un account ID Builder AWS, oltre al tuo soprannome.

Il nome è il modo in cui vieni chiamato negli strumenti e nei servizi mentre interagisci con gli altri. Il nickname indica come vuoi essere riconosciuto da AWS, amici e altre persone con cui collabori a stretto contatto.

> **Note**
>
> Gli strumenti e i servizi che ID Builder AWS utilizzi ti consentono di creare e utilizzare il tuo ID Builder AWS quando necessario.

Modifica delle informazioni del profilo

1. Accedi al tuo ID Builder AWS profilo suhttps://profile.aws.amazon.com.
2. Scegli My details (I miei dettagli).
3. Nella pagina My details (I miei dettagli), scegli il pulsante Edit (Modifica) accanto a Profile (Profilo).
4. Nella pagina Edit profile (Modifica profilo), apporta le modifiche desiderate al nome e al soprannome.
5. Scegli Save changes (Salva modifiche). Nella parte superiore della pagina viene visualizzato un messaggio di conferma che il profilo è stato aggiornato.

Per modificare le informazioni di contatto,

1. Accedi al tuo ID Builder AWS profilo all'indirizzohttps://profile.aws.amazon.com.
2. Scegli My details (I miei dettagli).
3. Nella pagina My details (I miei dettagli), scegli il pulsante Edit (Modifica) accanto a Contact information (Informazioni di contatto).
4. Nella pagina Edit contact information (Modifica le informazioni di contatto), modifica il tuo indirizzo e-mail.
5. Scegli Verifica email. Viene visualizzata una finestra di dialogo.
6. Nella finestra di dialogo Verifica e-mail, dopo aver ricevuto il codice nell'e-mail, inserisci il codice in Codice di verifica. Selezionare Verify (Verifica).

Cambia la tua ID Builder AWS password

La tua password deve soddisfare i seguenti requisiti:

- Le password distinguono tra maiuscole e minuscole.
- La lunghezza delle password deve essere compresa tra 8 e 64 caratteri.
- Le password devono contenere almeno un carattere per ognuna delle quattro categorie seguenti:
  - Lettere minuscole (a-z)
  - Lettere maiuscole (A-Z)
  - Numeri (0-9)
  - Caratteri non alfanumerici (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- Le ultime tre password non possono essere riutilizzate.

> **Note**
>
> Gli strumenti e i servizi che ID Builder AWS utilizzi ti consentono di crearli e utilizzarli ID Builder AWS quando necessario.

Per modificare la ID Builder AWS password

1. Accedi al tuo ID Builder AWS profilo all'indirizzohttps://profile.aws.amazon.com.
2. Scegliere Sicurezza.
3. Nella pagina Security (Sicurezza), scegli Change password (Modifica password). Verrai reindirizzato a una nuova pagina.
4. Nella pagina Reinserisci la password, in Password, inserisci la password attuale. Quindi scegli Accedi.
5. Nella pagina Modifica la password, in Nuova password, inserisci la nuova password che desideri utilizzare. Quindi, in Conferma password, inserisci nuovamente la nuova password che desideri utilizzare.
6. Scegli Cambia password. Verrai reindirizzato al tuo ID Builder AWS profilo.

Elimina tutte le sessioni attive per il tuo ID Builder AWS

In Dispositivi connessi, puoi visualizzare tutti i dispositivi a cui hai attualmente effettuato l'accesso. Se non riconosci un dispositivo, come procedura consigliata in materia di sicurezza, devi prima modificare la password e poi disconnetterti ovunque. Puoi disconnetterti da tutti i dispositivi eliminando tutte le sessioni attive nella pagina Sicurezza relativa a ID Builder AWS.

> **Note**
>
> ID Builder AWS supporta sessioni estese di 90 giorni per Amazon Q Developer in un IDE. Per ogni nuovo accesso IDE, puoi visualizzare due voci di sessione. Quando esci dal tuo IDE, puoi continuare a vedere le sessioni IDE elencate in Dispositivi connessi anche se non sono più valide. Queste sessioni scompaiono una volta scaduti i 90 giorni.

Per eliminare tutte le sessioni attive

1. Accedi al tuo ID Builder AWS profilo all'indirizzohttps://profile.aws.amazon.com.
2. Scegliere Sicurezza.
3. Nella pagina Security (Sicurezza), scegli Delete all active sessions (Elimina tutte le sessioni attive).
4. Nella finestra di dialogo Elimina tutte le sessioni, inserisci elimina tutto. Eliminando tutte le sessioni, ti disconnetti da tutti i dispositivi a cui potresti aver effettuato l'accesso utilizzando il tuo ID Builder AWS, compresi i diversi browser. Quindi scegli Elimina tutte le sessioni.

Elimina il tuo ID Builder AWS

> **Warning**
>
> Dopo aver eliminato il tuo ID Builder AWS, non potrai più accedere agli AWS strumenti e ai servizi a cui accedevi in precedenza. ID Builder AWS Il tuo ID Builder AWS è separato da tutti quelli Account AWS che potresti avere, e la cancellazione del tuo non ID Builder AWS comporterà la chiusura del tuo Account AWS.

Per eliminare il tuo ID Builder AWS

1. Accedi al tuo ID Builder AWS profilo all'indirizzohttps://profile.aws.amazon.com.
2. Scegli I miei ID Builder AWS dati.
3. Nella pagina I miei ID Builder AWS dati, in Eliminazione ID Builder AWS, scegli Elimina ID Builder AWS.
4. Seleziona la casella di controllo accanto a ogni dichiarazione di non responsabilità per confermare che sei pronto per procedere.

> **Important**
>
> Dopo aver eliminato il tuo ID Builder AWS, tutti i contenuti rimanenti associati esclusivamente a te ID Builder AWS verranno eliminati e non potrai più accedere o recuperare i contenuti dalle applicazioni che utilizzano il tuo. ID Builder AWS ID Builder AWS Verranno inoltre eliminate tutte le informazioni personali fornite dall'utente in relazione alla creazione e all'amministrazione delle informazioni, ad eccezione di quelle che AWS potrebbero conservare le informazioni personali come richiesto o consentito dalla legge, come le registrazioni della richiesta di cancellazione o i dati in un formato che non consente l'identificazione dell'utente.
>
> Puoi scoprire di più su come gestiamo le tue informazioni nell'AWS Informativa sulla privacy.
>
> Ricorda che puoi aggiornare le tue preferenze di AWS comunicazione o annullare l'iscrizione visitando il Centro preferenze di AWS comunicazione.

5. Scegli Delete ID Builder AWS (Elimina).

Gestione dell' ID Builder AWS autenticazione a più fattori (MFA)

L'autenticazione a più fattori (MFA) è un meccanismo semplice ed efficace per migliorare la sicurezza. Il primo fattore, la password, è un segreto che viene memorizzato, noto anche come fattore di conoscenza. Altri fattori possono essere fattori di possesso (qualcosa che possiedi, come una chiave di sicurezza) o fattori intrinseci (qualcosa che sei, come una scansione biometrica). Ti consigliamo vivamente di configurare l'MFA per aggiungere un livello aggiuntivo per il tuo. ID Builder AWS

> **Important**
>
> Consigliamo di registrare più dispositivi MFA. Se perdi l'accesso a tutti i dispositivi MFA registrati, non potrai ripristinare i tuoi. ID Builder AWS

Puoi registrare un autenticatore integrato e anche registrare una chiave di sicurezza da conservare in un luogo fisicamente sicuro. Se non riesci a utilizzare l'autenticatore integrato, puoi utilizzare la chiave di sicurezza registrata. Per le applicazioni di autenticazione, puoi anche abilitare la funzionalità di backup o sincronizzazione su cloud in tali app. Questo ti aiuta a evitare di perdere l'accesso al tuo profilo in caso di smarrimento o danneggiamento del dispositivo MFA.

> **Note**
>
> Ti consigliamo di controllare periodicamente i dispositivi MFA registrati per assicurarti che siano aggiornati e funzionanti. Inoltre, è necessario conservare tali dispositivi in un luogo fisicamente sicuro quando non vengono utilizzati.

Tipi di MFA disponibili per ID Builder AWS

ID Builder AWS supporta i seguenti tipi di dispositivi di autenticazione a più fattori (MFA).

FIDO2 autenticatori

FIDO2è uno standard che include CTAP2 WebAuthne si basa sulla crittografia a chiave pubblica. Le credenziali FIDO sono resistenti al phishing perché sono uniche per il sito Web in cui sono state create, ad esempio. AWS

AWS supporta i due fattori di forma più comuni per gli autenticatori FIDO: autenticatori integrati e chiavi di sicurezza. Di seguito sono riportate ulteriori informazioni sui tipi più comuni di autenticatori FIDO.

Argomenti

- Autenticatori integrati
- Chiavi di sicurezza
- Gestori di password, fornitori di chiavi di accesso e altri autenticatori FIDO

Autenticatori integrati

Alcuni dispositivi dispongono di autenticatori integrati, come TouchID on o una fotocamera compatibile con Windows Hello. MacBook Se il dispositivo è compatibile con i protocolli FIDO, tra cui WebAuthn, è possibile utilizzare l'impronta digitale o il viso come secondo fattore. Per ulteriori informazioni, consulta Autenticazione FIDO.

Chiavi di sicurezza

È possibile acquistare una chiave di FIDO2 sicurezza esterna compatibile con USB, BLE o NFC. Quando ti viene richiesto un dispositivo MFA, tocca il sensore della chiave. YubiKey o Feitian crea dispositivi compatibili. Per un elenco di tutte le chiavi di sicurezza compatibili, consulta Prodotti certificati FIDO.

Gestori di password, fornitori di chiavi di accesso e altri autenticatori FIDO

Diversi provider terzi supportano l'autenticazione FIDO nelle applicazioni mobili, come funzionalità nei gestori di password, nelle smart card con modalità FIDO e in altri fattori di forma. Questi dispositivi compatibili con FIDO possono funzionare con IAM Identity Center, ma ti consigliamo di testare personalmente un autenticatore FIDO prima di abilitare questa opzione per l'MFA.

> **Note**
>
> Alcuni autenticatori FIDO possono creare credenziali FIDO individuabili note come passkey. Le passkey possono essere associate al dispositivo che le crea oppure possono essere sincronizzate e salvate su un cloud. Ad esempio, puoi registrare una passkey utilizzando Apple Touch ID su un Macbook supportato, quindi accedere a un sito da un laptop Windows utilizzando Google Chrome con la tua passkey in iCloud seguendo le istruzioni sullo schermo al momento dell'accesso. Per ulteriori informazioni sui dispositivi che supportano le passkey sincronizzabili e l'attuale interoperabilità delle passkey tra sistemi operativi e browser, vedere Device Support su passkeys.dev, una risorsa gestita da FIDO Alliance And World Wide Web Consortium (W3C).

Applicazioni di autenticazione

Le applicazioni di autenticazione sono autenticatori di terze parti basati su codice OTP (One-Time Password). È possibile utilizzare un'applicazione di autenticazione installata sul dispositivo mobile o sul tablet come dispositivo MFA autorizzato. L'applicazione di autenticazione di terze parti deve

essere conforme a RFC 6238, un algoritmo TOTP (password monouso) basato su standard in grado di generare codici di autenticazione a sei cifre.

Quando viene richiesta l'autenticazione MFA, è necessario inserire un codice valido dall'app di autenticazione nella casella di input visualizzata. Ogni dispositivo MFA assegnato a un utente deve essere univoco. È possibile registrare due app di autenticazione per ogni utente.

Puoi scegliere tra le seguenti famose app di autenticazione di terze parti. Tuttavia, qualsiasi applicazione conforme a TOTP funziona con l'MFA. ID Builder AWS

Sistema operativo	Applicazione di autenticazione testata
Android	1Password, Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator
iOS	1Password, Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator

Registra il tuo ID Builder AWS dispositivo MFA

> **Note**
>
> Dopo aver effettuato la registrazione all'MFA, esserti disconnesso e aver effettuato l'accesso sullo stesso dispositivo, potresti non ricevere alcuna richiesta di autenticazione a MFA sui dispositivi considerati attendibili.

Registrazione del dispositivo MFA tramite un'app di autenticazione

1. Accedi al tuo ID Builder AWS profilo all'indirizzohttps://profile.aws.amazon.com.
2. Scegliere Sicurezza.
3. Nella pagina Security (Sicurezza), scegli Register device (Registra dispositivo).
4. Nella pagina Register MFA device (Registra dispositivo MFA), scegli l'app di autenticazione.
5. ID Builder AWS gestisce e visualizza le informazioni di configurazione, inclusa una grafica con codice QR. Il grafico è una rappresentazione della "chiave di configurazione segreta" disponibile per l'inserimento manuale nelle applicazioni di autenticazione che non supportano i codici QR.

6. Apri l'app di autenticazione. Per un elenco di applicazioni, consulta Applicazioni di autenticazione.

   Se l'applicazione di autenticazione supporta più account o dispositivi MFA, seleziona l'opzione che consente di creare un nuovo account o dispositivo MFA.

7. Determina se l'app MFA supporta i codici QR e completa una delle seguenti operazioni sulla pagina Set up your authenticator app (Configurazione dell'applicazione di autenticazione):

   1. Scegli Show QR code (Mostra codice QR) e utilizza l'app per eseguire la scansione del codice QR. Ad esempio, è possibile selezionare l'icona della fotocamera o un'opzione simile a Scan code (Scannerizza codice). Quindi usa la fotocamera del dispositivo per la scansione del codice.
   2. Scegli Show secret key (Mostra chiave segreta), quindi inserisci la chiave segreta nell'app MFA.

   Al termine, l'app di autenticazione genererà e visualizzerà una password monouso.

8. Nella casella Authenticator (Autenticatore), digitar la password monouso visualizzata nell'app di autenticazione. Scegliere Assign MFA (Assegna MFA).

   > **Important**
   >
   > Invia la richiesta immediatamente dopo la generazione del codice. Se generi il codice e poi attendi troppo a lungo per inviare la richiesta, il dispositivo MFA viene associato correttamente al tuo ID Builder AWS, ma il dispositivo MFA non è sincronizzato. Ciò accade perché le password monouso temporanee (TOTP) scadono dopo un breve periodo di tempo. Se ciò accade, è possibile sincronizzare nuovamente il dispositivo. Per ulteriori informazioni, consulta Ricevo il messaggio "An unexpected error has occurred" (Si è verificato un errore imprevisto) quando provo a registrarmi o accedere con un'app di autenticazione.

9. Per assegnare al dispositivo un nome descrittivo ID Builder AWS, scegli Rinomina. Questo nome ti aiuta a distinguere il dispositivo dagli altri registrati.

Il dispositivo MFA è ora pronto per l'uso con. ID Builder AWS

Registra una chiave di sicurezza come dispositivo ID Builder AWS MFA

Registrazione del dispositivo MFA tramite una chiave di sicurezza

1. Accedi al tuo ID Builder AWS profilo all'indirizzohttps://profile.aws.amazon.com.
2. Scegliere Sicurezza.
3. Nella pagina Security (Sicurezza), scegli Register device (Registra dispositivo).
4. Nella pagina Register MFA device (Registra dispositivo MFA), scegli Security key (Chiave di sicurezza).
5. Assicurati che la chiave di sicurezza sia abilitata. Se utilizzi una chiave di sicurezza fisica separata, collegala al computer.
6. Segui le istruzioni riportate sullo schermo. La tua esperienza varierà in base al sistema operativo e al browser.
7. Per assegnare al dispositivo un nome descrittivo ID Builder AWS, scegli Rinomina. Questo nome ti aiuta a distinguere il dispositivo dagli altri registrati.

Il dispositivo MFA è ora pronto per l'uso con. ID Builder AWS

Rinomina il tuo dispositivo ID Builder AWS MFA

Ridenominazione del dispositivo MFA

1. Accedi al tuo ID Builder AWS profilo all'indirizzo. https://profile.aws.amazon.com
2. Scegliere Sicurezza. Quando arrivi alla pagina, il campo Rename (RinominaI è disattivato.
3. Seleziona il dispositivo MFA che desideri modificare. Questo ti permette di scegliere Rename (Rinomina). Quindi, si apre una finestra di dialogo.
4. Nel prompt visualizzato, inserisci il nuovo nome in MFA device name (Nome del dispositivo MFA) e scegli Rename (Rinomina). Il dispositivo rinominato viene visualizzato in Multi-factor authentication (MFA) devices (Dispositivi di autenticazione a più fattori (MFA).

Eliminare il dispositivo MFA

Consigliamo di mantenere attivi due o più dispositivi MFA. Prima di rimuovere un dispositivo, consulta Registra il tuo ID Builder AWS dispositivo MFA per registrare un dispositivo MFA sostitutivo. Per

disabilitare l'autenticazione a più fattori per il tuo ID Builder AWS, rimuovi tutti i dispositivi MFA registrati dal tuo profilo.

Eliminazione di un dispositivo MFA

1. Accedi al tuo ID Builder AWS profilo all'indirizzo. https://profile.aws.amazon.com
2. Scegliere Sicurezza.
3. Seleziona il dispositivo MFA che desideri eliminare e scegli Delete (Elimina).
4. Nella finestra Delete MFA device? (Eliminare il dispositivo MFA?), segui le istruzioni per eliminare il dispositivo.
5. Scegliere Delete (Elimina).

Il dispositivo non sarà più visualizzato in Multi-factor authentication (MFA) devices (Dispositivi di autenticazione a più fattori (MFA).

Privacy e accesso ai dati ID Builder AWS

Nella sezione Informativa sulla privacy di AWS è riportato come gestiamo i tuoi dati personali. Per informazioni su come eliminare il tuo ID Builder AWS profilo, consultaElimina il tuo ID Builder AWS.

Richiedi i tuoi ID Builder AWS dati

Puoi richiedere e visualizzare le informazioni personali associate a te e alle AWS applicazioni ID Builder AWS e ai servizi a cui hai avuto accesso tramite il tuo ID Builder AWS. Per ulteriori informazioni sull'esercizio dei diritti dell'interessato, incluse le informazioni personali fornite in relazione ad altri AWS siti Web, applicazioni, prodotti, servizi, eventi ed esperienze, consultahttps://aws.amazon.com/privacy.

Richiesta dei dati

1. Accedi al tuo ID Builder AWS profilo all'indirizzohttps://profile.aws.amazon.com.
2. Scegli I miei ID Builder AWS dati.
3. Nella pagina I miei ID Builder AWS dati, in Eliminazione ID Builder AWS, scegli Richiedi i tuoi dati.
4. Nella parte superiore della pagina viene visualizzato un messaggio verde di conferma, in cui è indicato che abbiamo ricevuto la tua richiesta e che verrà completata entro 30 giorni.

5. Quando ricevi un'email da noi indicante che la richiesta è stata elaborata, torna alla pagina Privacy e dati del tuo ID Builder AWS profilo. Scegli il nuovo pulsante disponibile Download ZIP archive with your data (Scarica il file ZIP con i tuoi dati).

   Mentre la tua richiesta di dati è in sospeso, non potrai eliminare i tuoi ID Builder AWS.

ID Builder AWS e altre credenziali AWS

ID Builder AWS La tua è separata da Account AWS qualsiasi credenziale di accesso. Puoi utilizzare la stessa e-mail per la tua e-mail ID Builder AWS e per quella dell'utente root di un Account AWS.

Un ID Builder AWS:

- Consente di accedere agli strumenti e ai servizi che utilizza ID Builder AWS.
- Non influisce sui controlli di sicurezza esistenti, come le politiche e le configurazioni che hai specificato sulle tue Account AWS applicazioni.
- Non sostituisce utenti, credenziali o account root, IAM Identity Center o IAM esistenti.
- Impossibile ottenere le credenziali AWS IAM per accedere a AWS Management Console, AWS CLI AWS SDKs, o AWS Toolkit.

An Account AWS è un contenitore di risorse con informazioni di contatto e pagamento. Stabilisce un limite di sicurezza entro il quale gestire AWS servizi fatturati e misurati, come S3 o Lambda. EC2 I proprietari di account possono accedere a un account. Account AWS AWS Management Console Per ulteriori informazioni, consulta Firma nella AWS Management Console.

In che modo ID Builder AWS si collega alla tua identità IAM Identity Center esistente

In qualità di individuo proprietario dell'identità, gestisci il ID Builder AWS. Non è collegato ad alcun'altra identità che potresti avere per un'altra organizzazione, come scuola o lavoro. Potresti utilizzare un'identità della forza lavoro in IAM Identity Center per rappresentare la tua identità lavorativa e una ID Builder AWS per rappresentare la tua personalità privata. Queste identità operano in modo indipendente.

Gli utenti in AWS IAM Identity Center (successore di AWS Single Sign-On) sono gestiti da un amministratore IT o cloud aziendale o dall'amministratore del provider di identità dell'organizzazione,

come Okta, Ping o Azure. Gli utenti nel Centro identità IAM possono accedere alle risorse su più account in AWS Organizations.

Profili multipli ID Builder AWS

Puoi crearne più di uno ID Builder AWS purché ogni ID utilizzi un indirizzo email univoco. Tuttavia, utilizzarne più di uno ID Builder AWS può rendere difficile ricordare quale ID Builder AWS hai usato per quale scopo. Quando possibile, ti consigliamo di utilizzarne uno ID Builder AWS per tutte le tue attività relative a AWS strumenti e servizi.

Esci da AWS

Il modo in cui ti Account AWS disconnetti dipende dal tipo di AWS utente che sei. Puoi essere un utente root dell'account, un utente IAM, un utente in IAM Identity Center, un'identità federata o un utente AWS Builder ID. Se non sei sicuro del tipo di utente che sei, consulta. Determina il tipo di utente

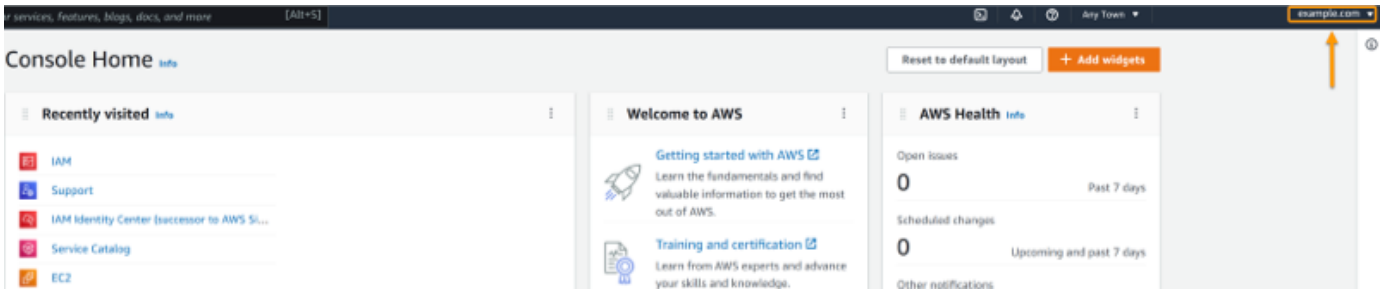
Argomenti

- Esci dal AWS Management Console
- Esci dal portale di AWS accesso
- Esci da AWS Builder ID

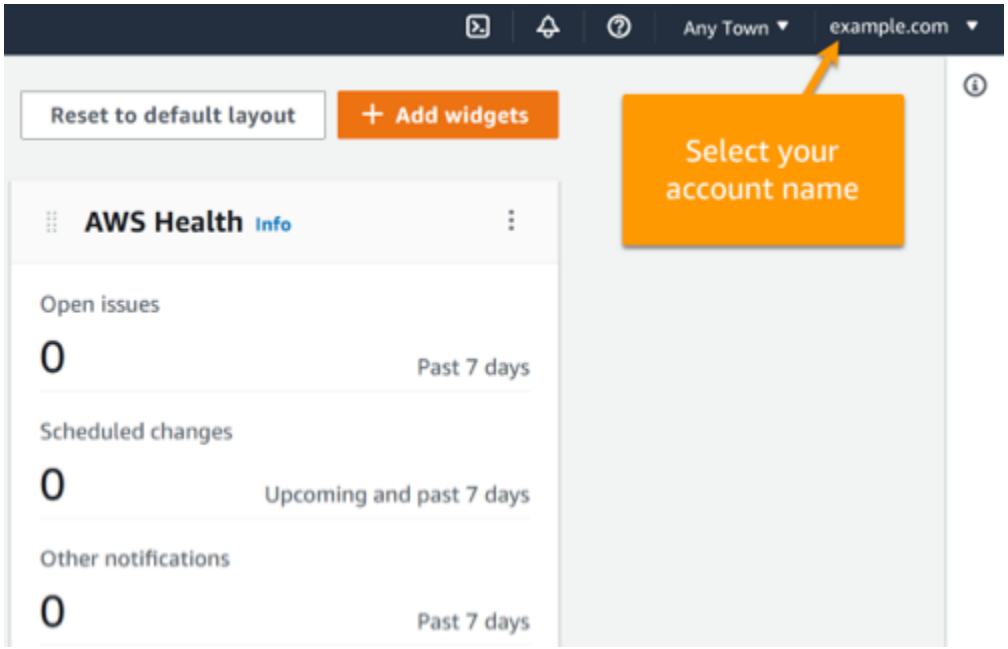
Esci dal AWS Management Console

Per disconnettersi da AWS Management Console

1. Dopo aver effettuato l'accesso a AWS Management Console, arriverai a una pagina simile a quella mostrata nell'immagine seguente. Il nome del tuo account o il nome utente IAM è mostrato nell'angolo in alto a destra.



2. Nella barra di navigazione in alto a destra, scegli il tuo nome utente.



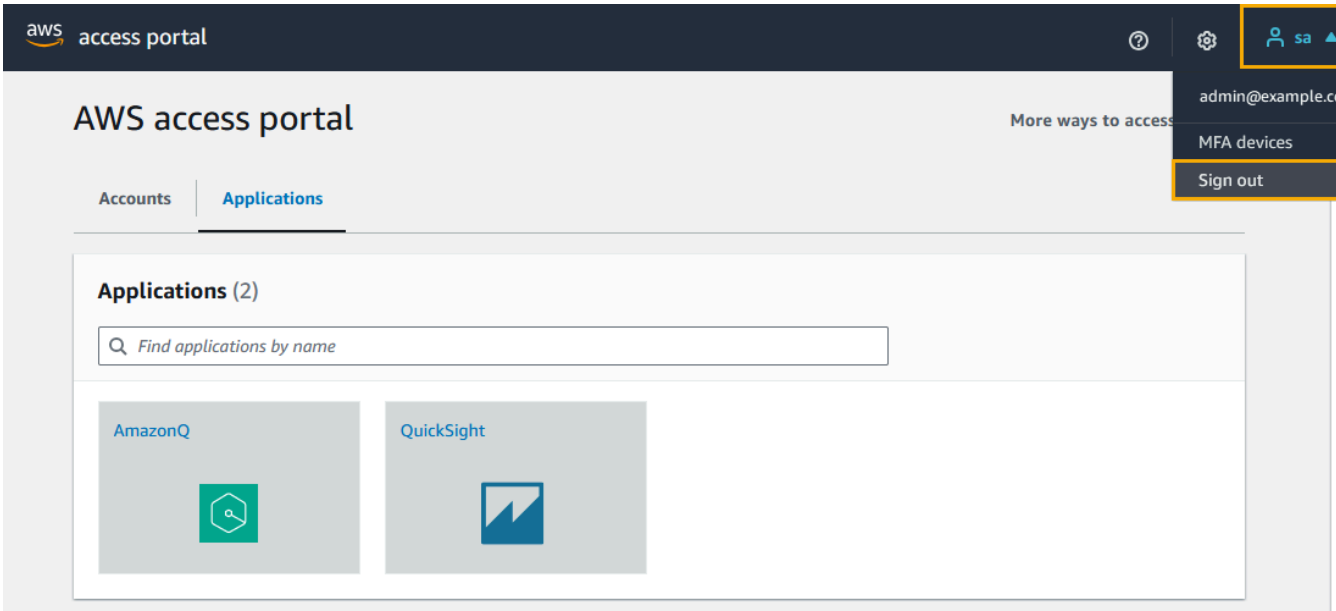
3. Scegli un'opzione di disconnessione. Le opzioni dei pulsanti variano in base al numero di account a cui hai effettuato l'accesso.
   - Seleziona Esci se hai effettuato l'accesso a un solo account.
   - Seleziona Esci da tutte le sessioni per disconnetterti da tutte le tue identità contemporaneamente.
   - Seleziona Esci dalla sessione corrente per disconnetterti dall'identità che hai selezionato.
4. Verrai reindirizzato alla AWS Management Console pagina web.

Per ulteriori informazioni sull'accesso a più account, consulta Accesso a più account nella Guida AWS Management Console introduttiva.

Esci dal portale di AWS accesso

Per uscire dal portale di AWS accesso

1. Nella barra di navigazione in alto a destra, scegli il tuo nome utente.
2. Seleziona Esci come mostrato nell'immagine seguente.



3. Se ti disconnetti con successo, ora viene visualizzata la pagina di AWS accesso al portale di accesso.

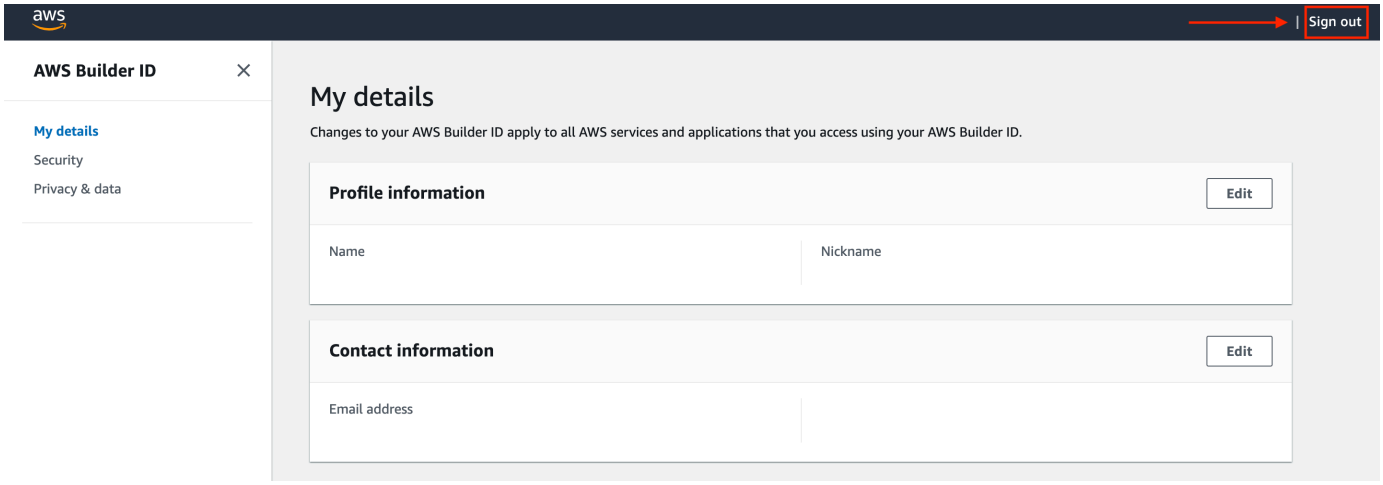
Se utilizzi un provider di identità esterno (IdP) come fonte di identità, la sessione attiva per le tue credenziali non viene interrotta quando ti disconnetti. Se si torna al portale di AWS accesso, è possibile che venga effettuato automaticamente l'accesso senza dover fornire le proprie credenziali.

Esci da AWS Builder ID

Per uscire da un AWS servizio a cui hai effettuato l'accesso utilizzando il tuo AWS Builder ID, devi disconnetterti dal servizio. Se vuoi uscire dal tuo profilo AWS Builder ID, consulta la procedura seguente.

Per uscire dal tuo profilo AWS Builder ID

1. Dopo aver effettuato l'accesso al tuo profilo AWS Builder ID all'indirizzohttps://profile.aws.amazon.com/, accedi alla pagina I miei dati.
2. In alto a destra della pagina del tuo profilo AWS Builder ID, scegli Esci.



3. Ti disconnetti quando non vedi più il tuo profilo AWS Builder ID.

Risoluzione dei problemi di Account AWS accesso

Utilizza le informazioni qui per aiutarti a risolvere i problemi di accesso e altri problemi. Account AWS Per step-by-step istruzioni su come accedere a un Account AWS, vedi. Accedi al AWS Management Console

Se nessuno degli argomenti di risoluzione dei problemi ti aiuta a risolvere il problema di accesso, puoi creare un caso Supporto compilando questo modulo: Sono un AWS cliente e cerco assistenza per la fatturazione o l'account. Come procedura consigliata in materia di sicurezza, non Supporto puoi parlare dei dettagli di Account AWS persone diverse dall'account a cui hai effettuato l'accesso. Inoltre, AWS Support non può modificare le credenziali associate a un account per nessun motivo.

> **Note**
>
> Supporto non pubblica un numero di telefono diretto per contattare un rappresentante dell'assistenza.

Per ulteriore assistenza sulla risoluzione dei problemi di accesso, vedi Cosa devo fare se ho problemi ad accedere o accedere al mio? Account AWS Se riscontri problemi di accesso ad Amazon.com, consulta il Servizio clienti Amazon anziché questa pagina.

Argomenti

- Le mie AWS Management Console credenziali non funzionano
- La reimpostazione della password è richiesta per il mio utente root
- Non ho accesso all'e-mail per il mio Account AWS
- Il mio dispositivo MFA si è perso o ha smesso di funzionare
- Non riesco ad accedere alla pagina di AWS Management Console accesso
- Come posso trovare il mio ID o alias Account AWS
- Ho bisogno del codice di verifica dell'account
- Ho dimenticato la password dell'utente root per il mio Account AWS
- Ho dimenticato la mia password utente IAM per il mio Account AWS
- Ho dimenticato la mia password di identità federata per il mio Account AWS
- Non riesco ad accedere al mio account esistente Account AWS e non riesco a crearne uno nuovo Account AWS con lo stesso indirizzo email

- Devo riattivare il mio account sospeso Account AWS
- Devo contattarci per problemi di accesso Supporto
- Devo contattarci AWS Billing per problemi di fatturazione
- Ho una domanda su un ordine al dettaglio
- Ho bisogno di aiuto per gestire il mio Account AWS
- Le mie credenziali del portale di AWS accesso non funzionano
- Ho dimenticato la password del mio IAM Identity Center Account AWS
- Ricevo un messaggio di errore che dice «Non sei tu, siamo noi» quando provo ad accedere alla console IAM Identity Center

Le mie AWS Management Console credenziali non funzionano

Se ricordi nome utente e password, ma le credenziali non funzionano, è possibile che ti trovi nella pagina sbagliata. Prova ad accedere da un'altra pagina:

Pagina di accesso utente root

- Se hai creato o possiedi un account Account AWS e stai eseguendo un'operazione che richiede le credenziali dell'utente root, inserisci l'indirizzo e-mail del tuo account nel campo. AWS Management Console Per informazioni su come accedere all'utente root, consultaPer accedere come utente root. Se hai dimenticato la password dell'utente root, puoi reimpostarla. Per ulteriori informazioni, consulta Ho dimenticato la password dell'utente root per il mio Account AWS. Se hai dimenticato l'indirizzo e-mail dell'utente root, controlla se nella tua casella di posta elettronica è presente un'e-mail inviata da. AWS
- Se hai provato ad accedere al tuo account utente root e hai ricevuto l'errore: Il recupero della password è disabilitato per il mio account utente root, non hai le credenziali dell'utente root. Non puoi accedere come utente root o eseguire il recupero della password per l'utente root del tuo account. AWS gli account membro gestiti utilizzando AWS Organizations potrebbero non avere una password utente root, chiavi di accesso, certificati di firma o autenticazione a più fattori (MFA) attiva.

  Solo l'account di gestione o l'amministratore delegato di IAM può eseguire azioni utente root nell'account membro. Contatta l'amministratore se devi eseguire un'operazione che richiede le credenziali dell'utente root. Per ulteriori informazioni, consulta Gestire centralmente l'accesso root per gli account dei membri nella Guida per l'AWS Identity and Access Management utente.

Pagina di accesso utente IAM

- Se tu o qualcun altro avete creato un utente IAM all'interno di un Account AWS, devi conoscere quell' Account AWS ID o alias per accedere. Inserisci l'ID o l'alias del tuo account, il nome utente e la password in. AWS Management Console Per sapere come accedere alla pagina di accesso degli utenti IAM, consulta. Accesso come utente IAM Se hai dimenticato la password utente IAM, puoi consultare la pagina Ho dimenticato la mia password utente IAM per il mio Account AWS per informazioni sulla reimpostazione della password utente IAM. Controlla la tua e-mail, i preferiti del browser o la cronologia del browser per trovare un URL che includa `signin.aws.amazon.com/`. L'ID o l'alias del tuo account seguiranno il testo `"account="` nell'URL. Se non riesci a trovare l'ID o l'alias del tuo account, contatta l'amministratore. Supporto non posso aiutarti a recuperare queste informazioni. Non puoi vedere l'ID o l'alias del tuo account se non dopo aver effettuato l'accesso.

La reimpostazione della password è richiesta per il mio utente root

Per proteggere il tuo account, potresti ricevere il seguente messaggio quando tenti di accedere a AWS Management Console:

È richiesta la reimpostazione della password. Per motivi di sicurezza, è necessario reimpostare la password. Per proteggere il tuo account, devi scegliere Password dimenticata qui sotto e reimpostare la password.

Oltre a questo messaggio, ti avvisa AWS anche quando identifichiamo un potenziale problema tramite l'e-mail associata al tuo account. Questa e-mail include il motivo per cui è richiesta la reimpostazione della password. Ad esempio, quando identifichiamo attività di accesso insolite Account AWS o le credenziali associate all'utente Account AWS sono disponibili pubblicamente online.

Aggiorna la password per assicurarti che le credenziali dell'utente root rimangano sicure. Per informazioni su come reimpostare la password dell'utente root, consulta Ho dimenticato la password dell'utente root per il mio. Account AWS

Non ho accesso all'e-mail per il mio Account AWS

Quando ne crei un Account AWS, fornisci un indirizzo e-mail e una password. Queste sono le credenziali per Utente root dell'account AWS. Se non sei sicuro dell'indirizzo e-mail associato al tuo Account AWS, cerca la corrispondenza salvata che termina con @signin .aws o @verify .signin.aws

a qualsiasi indirizzo e-mail della tua organizzazione che potrebbe essere stato utilizzato per aprire il. Account AWS Chiedi agli altri membri del tuo team, della tua organizzazione o della tua famiglia. Se qualcuno che conosci ha creato l'account, può aiutarti ad accedervi.

Se conosci l'indirizzo e-mail ma non hai più accesso all'e-mail, prova innanzitutto a recuperare l'accesso all'e-mail utilizzando una delle seguenti opzioni:

- Se sei il proprietario del dominio dell'indirizzo e-mail, puoi ripristinare un indirizzo e-mail eliminato. In alternativa, puoi impostare un catch-all per il tuo account e-mail che "acquisisce tutti" i messaggi inviati a indirizzi e-mail che non esistono più nel server di posta e li reindirizza a un altro indirizzo e-mail.
- Se l'indirizzo e-mail dell'account è parte del sistema di posta elettronica aziendale, si consiglia di contattare gli amministratori del sistema IT. Potrebbero essere in grado di aiutare a ottenere nuovamente l'accesso all'e-mail.

Se ancora non riesci ad accedere al tuo Account AWS, puoi trovare opzioni di supporto alternative Supportocontattando.

Il mio dispositivo MFA si è perso o ha smesso di funzionare

Se il tuo dispositivo MFA viene smarrito, danneggiato o non funziona, non ricevi un codice di accesso monouso (OTP) quando invii una richiesta di verifica MFA.

Utenti IAM

Puoi accedere utilizzando un altro dispositivo MFA registrato allo stesso utente IAM.

Gli utenti IAM devono contattare un amministratore per disattivare un dispositivo MFA che non funziona. Questi utenti non possono ripristinare il proprio dispositivo MFA senza l'assistenza dell'amministratore. L'amministratore è in genere un personale IT (Information Technology) che dispone di un livello di autorizzazioni più elevato Account AWS rispetto agli altri membri dell'organizzazione. Questa persona ha creato l'account e fornisce agli utenti le credenziali di accesso per l'accesso.

Utenti root

Per ripristinare l'accesso all'utente root, è necessario accedere utilizzando un altro dispositivo MFA registrato per lo stesso utente root. Quindi, esamina le seguenti opzioni per ripristinare o aggiornare il tuo dispositivo MFA:

- Per step-by-step istruzioni su come ripristinare un dispositivo MFA, vedi Cosa succede se un dispositivo MFA viene perso o smette di funzionare?
- Per step-by-step istruzioni su come aggiornare un numero di telefono per un dispositivo MFA, vedi Come posso aggiornare il mio numero di telefono per reimpostare il mio dispositivo MFA smarrito?
- Per step-by-step istruzioni su come attivare i dispositivi MFA, consulta Abilitazione dei dispositivi MFA per gli utenti in. AWS
- Se non riesci a ripristinare il tuo dispositivo MFA, contatta. Supporto

> **Note**
>
> Gli utenti IAM devono contattare il proprio amministratore per ricevere assistenza con i dispositivi MFA. Supporto non può assistere gli utenti IAM con problemi relativi ai dispositivi MFA.

Non riesco ad accedere alla pagina di AWS Management Console accesso

Se non riesci a visualizzare la tua pagina di accesso, il dominio potrebbe essere bloccato da un firewall. Contatta l'amministratore di rete per aggiungere i seguenti domini o endpoint URL agli elenchi di consentiti della tua soluzione di filtraggio dei contenuti web, a seconda del tipo di utente e della modalità di accesso.

Utente root e utenti IAM	*.signin.aws.amazon.com
Accesso all'account Amazon.com	www.amazon.com
Accesso agli utenti di IAM Identity Center e alle applicazioni proprietarie	• *.awsapps.com (http://awsapps.com/) • *.signin.aws

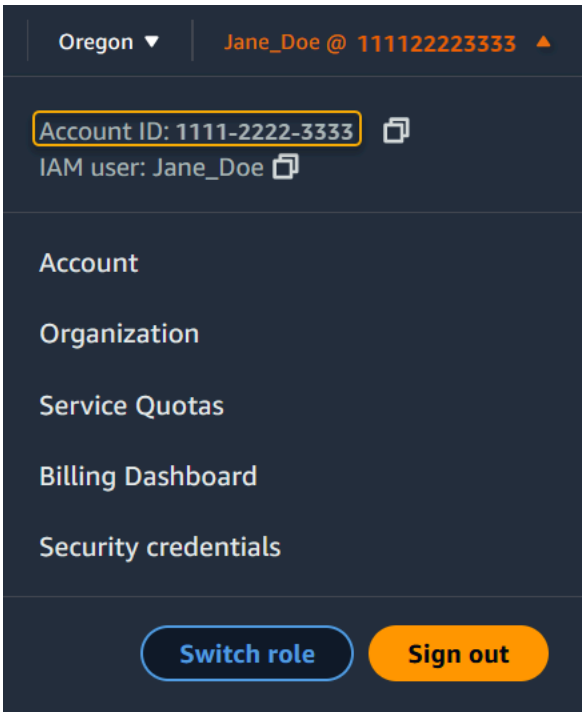
Come posso trovare il mio ID o alias Account AWS

Se sei un utente IAM e non hai effettuato l'accesso, chiedi all'amministratore l' Account AWS ID o l'alias. L'amministratore è in genere un personale IT (Information Technology) che dispone di un

livello di autorizzazioni più elevato Account AWS rispetto agli altri membri dell'organizzazione. Questa persona ha creato l'account e fornisce agli utenti le credenziali di accesso per l'accesso.

Se sei un utente IAM con accesso a AWS Management Console, l'ID del tuo account si trova nell'URL di accesso. Controlla le e-mail del tuo amministratore per l'URL di accesso. L'ID dell'account è costituito dalle prime dodici cifre dell'URL di accesso. Ad esempio, nel seguente URL`https://111122223333.signin.aws.amazon.com/console`, il tuo Account AWS ID è 111122223333.

Dopo aver effettuato l'accesso AWS Management Console, puoi trovare le informazioni sul tuo account nella barra di navigazione accanto alla tua regione. Ad esempio, nella schermata seguente, l'utente IAM Jane Doe ha un valore Account AWS di 1111-2222-3333.



Consulta la tabella seguente per ulteriori informazioni su come trovare il tuo in Account AWS base al tipo di utente.

Tipi di utenti e Account AWS IDs

Tipo di utente	Procedura		
Utente root	Seleziona il nome utente in alto a destra nella barra di		

Tipo di utente	Procedura		
	navigazione e quindi Le mie credenziali di sicurezza. Il numero dell'account viene visualizzato sotto Identificatori dell'account.		
Utente IAM	Seleziona il nome utente in alto a destra nella barra di navigazione e quindi Le mie credenziali di sicurezza. Il numero dell'account viene visualizzato sotto Dettagli dell'account.		
Ruolo presunto	Nella barra di spostamento in alto a destra scegliere Supporto, quindi Centro supporto. Il numero di account (ID) a 12 cifre al momento dell'accesso viene visualizzato nel riquadro di navigazione del Support Center.		

Per ulteriori informazioni sul tuo Account AWS ID e alias e su come trovarli, vedi Il tuo Account AWS ID e il suo alias.

Ho bisogno del codice di verifica dell'account

Se hai fornito l'indirizzo e-mail e la password del tuo account, AWS a volte è necessario fornire un codice di verifica valido una tantum. Per recuperare il codice di verifica, controlla l'indirizzo e-mail associato al tuo indirizzo Account AWS per cercare un messaggio da Amazon Web Services. L'indirizzo e-mail termina con @signin .aws o @verify .signin.aws. Seguire le istruzioni nel messaggio. Se non vedi il messaggio nel tuo account, controlla le cartelle dello spam e della posta indesiderata. Se non si dispone più dell'accesso all'e-mail, consultare Non ho accesso all'e-mail per il mio Account AWS.

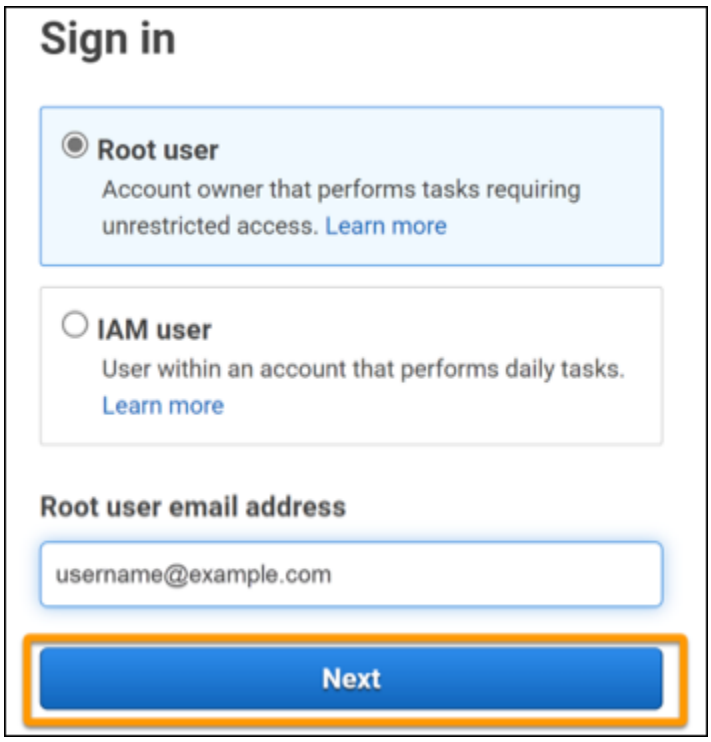
Ho dimenticato la password dell'utente root per il mio Account AWS

Se sei un utente root e hai perso o dimenticato la password del tuo account Account AWS, puoi reimpostarla selezionando il link «Password dimenticata» nel AWS Management Console. Devi conoscere l'indirizzo e-mail del tuo AWS account e devi avere accesso all'account e-mail. Durante il processo di recupero della password, ti verrà inviato via email un link per reimpostare la password. Il link verrà inviato all'indirizzo e-mail che hai utilizzato per creare il tuo Account AWS.

Per reimpostare la password per un account creato utilizzando AWS Organizations, vedi Accesso a un account membro come utente root.

Per reimpostare la password dell'utente root

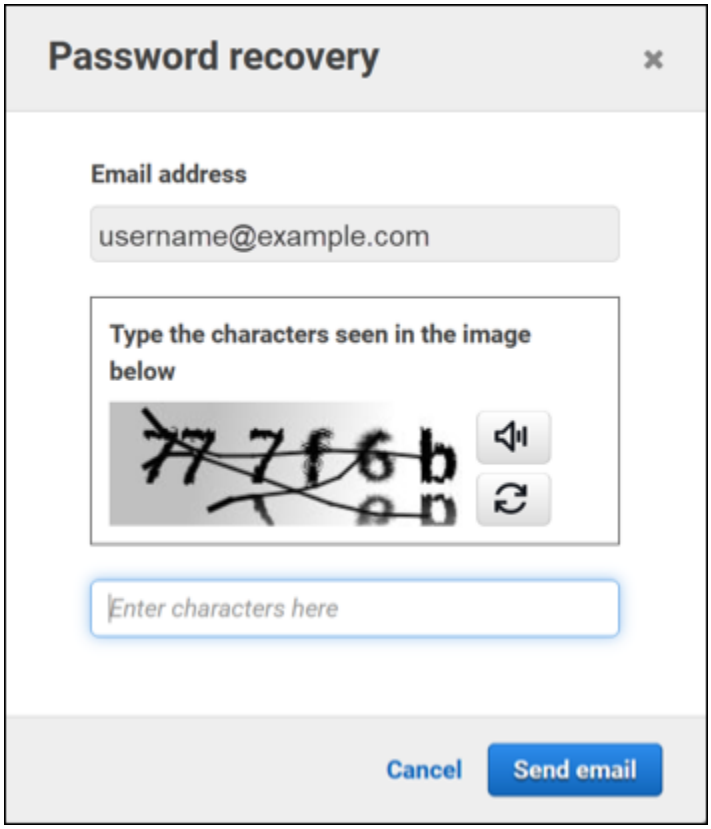
1. Usa il tuo indirizzo AWS e-mail per iniziare ad accedere alla Console di AWS gestione come utente root. Quindi, seleziona Next (Successivo).



> **Note**
>
> Se hai effettuato l'accesso AWS Management Consolecon le credenziali utente IAM, devi disconnetterti prima di poter reimpostare la password dell'utente root. Se viene visualizzata la pagina di accesso dell'utente IAM specifica dell'account, seleziona Accedi con le credenziali dell'account root nella parte inferiore della pagina. Se necessario, fornisci l'indirizzo e-mail dell'account e scegli Next (Avanti) per accedere alla pagina Root user sign in (Accesso utente root).

2. Scegli Password dimenticata?

3. Completa i passaggi per il recupero della password. 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. Un esempio di pagina di recupero della password è mostrato nell'immagine seguente.

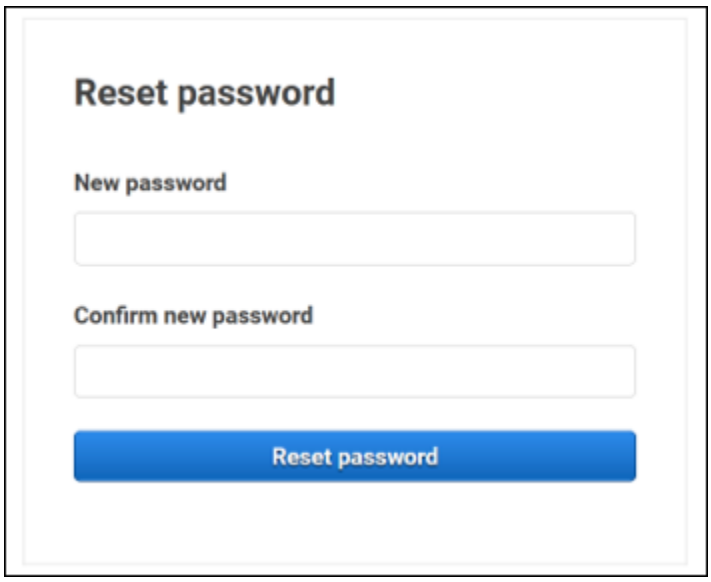


4. Dopo aver completato la procedura di recupero della password, riceverai un messaggio che ti comunica che sono state inviate ulteriori istruzioni all'indirizzo e-mail associato al tuo Account AWS.

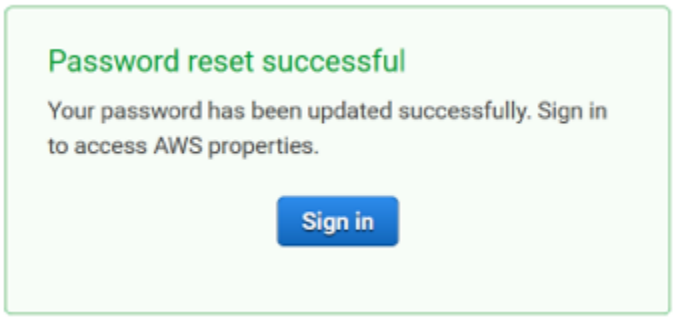
   Un'e-mail con un link per reimpostare la password viene inviata all'indirizzo e-mail utilizzato per creare il Account AWS.

   > **Note**
   >
   > L'e-mail verrà inviata da un indirizzo che termina con @signin .aws o @verify .signin.aws.

5. Seleziona il link fornito nell' AWS e-mail per reimpostare la password dell'utente root. AWS
6. Il link ti indirizza a una nuova pagina web per creare una nuova password per l'utente root.



Riceverai una conferma che la reimpostazione della password è avvenuta con successo. L'immagine seguente mostra una corretta reimpostazione della password.



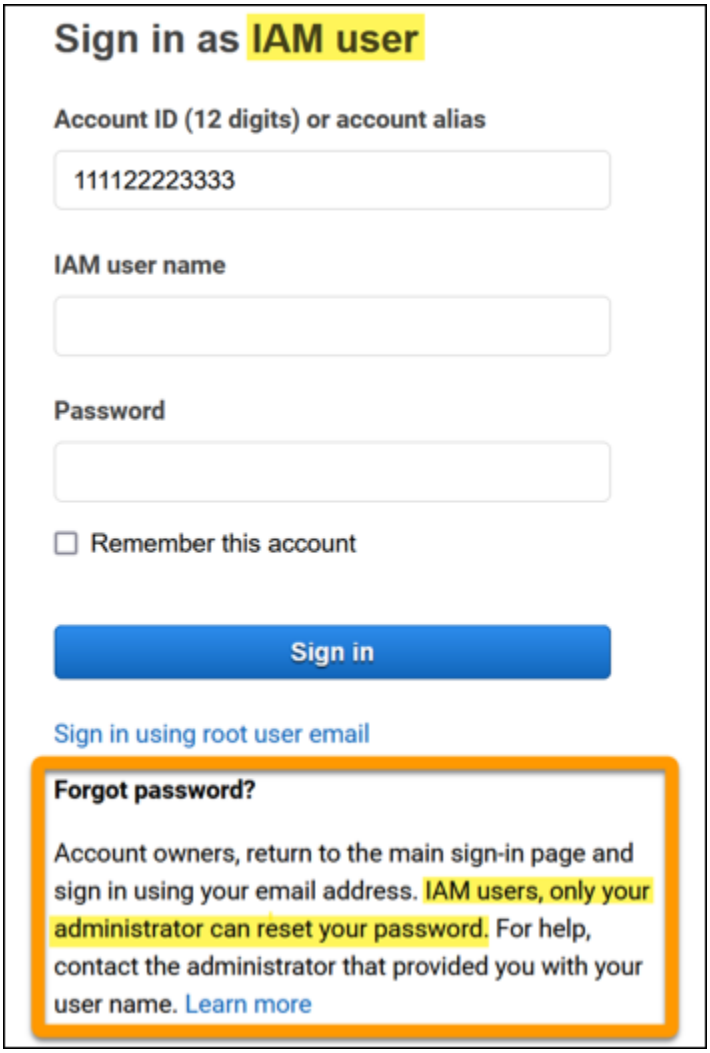
Per ulteriori informazioni sulla reimpostazione della password dell'utente root, vedi Come posso recuperare una password persa o dimenticata? AWS

Ho dimenticato la mia password utente IAM per il mio Account AWS

Per modificare la password utente IAM, devi disporre delle autorizzazioni appropriate. Per ulteriori informazioni sulla reimpostazione della password utente IAM, consulta Come un utente IAM cambia la propria password.

Se non disponi dell'autorizzazione per reimpostare la password, solo l'amministratore IAM può reimpostare la password utente IAM. Gli utenti IAM devono contattare il proprio amministratore IAM per reimpostare la password. L'amministratore è in genere un personale IT (Information

Technology) che dispone di un livello di autorizzazioni più elevato Account AWS rispetto agli altri membri dell'organizzazione. Questa persona ha creato l'account e fornisce agli utenti le credenziali di accesso per l'accesso.



Per motivi di sicurezza, Supporto non ha accesso per visualizzare, fornire o modificare le tue credenziali.

Per ulteriori informazioni sulla reimpostazione della password utente IAM, vedi Come posso recuperare una password persa o dimenticata? AWS

Per sapere come un amministratore può gestire la tua password, consulta Gestione delle password per gli utenti IAM.

Ho dimenticato la mia password di identità federata per il mio Account AWS

Le identità federate accedono per accedere Account AWS con identità esterne. Il tipo di identità esterna in uso determina il modo in cui le identità federate accedono. L'amministratore crea le identità federate. Rivolgiti all'amministratore per maggiori dettagli su come reimpostare la password. L'amministratore è in genere un personale IT (Information Technology) che dispone di un livello di autorizzazioni più elevato Account AWS rispetto agli altri membri dell'organizzazione. Questa persona ha creato l'account e fornisce agli utenti le credenziali di accesso per l'accesso.

Non riesco ad accedere al mio account esistente Account AWS e non riesco a crearne uno nuovo Account AWS con lo stesso indirizzo email

Puoi associare un indirizzo email a uno solo Utente root dell'account AWS. Se chiudi il tuo account utente root e questo rimane chiuso per più di 90 giorni, non potrai riaprire l'account o crearne uno nuovo Account AWS utilizzando l'indirizzo e-mail associato a questo account.

Per risolvere questo problema, puoi utilizzare il sottoindirizzamento in cui aggiungi un segno più (+) dopo il tuo indirizzo e-mail abituale quando registri un nuovo account. Il segno più (+) può essere seguito da lettere maiuscole o minuscole, numeri o altri caratteri supportati dal Simple Mail Transfer Protocol (SMTP). Ad esempio, puoi usare `email+1@yourcompany.com` o `email+tag@yourcompany.com` dove si trova la tua email abituale. `email@yourcompany.com` Questo è considerato un nuovo indirizzo anche se è collegato alla stessa casella di posta in arrivo del tuo indirizzo email abituale. Prima di registrare un nuovo account, ti consigliamo di inviare un'email di prova all'indirizzo e-mail aggiunto per confermare che il tuo provider di posta elettronica supporti il subindirizzamento.

Devo riattivare il mio account sospeso Account AWS

Se il tuo Account AWS è sospeso e desideri ripristinarlo, vedi Come posso riattivare il mio dispositivo sospeso? Account AWS

Devo contattarci per problemi di accesso Supporto

Se hai provato tutto, puoi ricevere assistenza Supporto completando la richiesta Billing and Account Support.

Devo contattarci AWS Billing per problemi di fatturazione

Se non riesci ad accedere al tuo account Account AWS e desideri contattarci AWS Billing per problemi di fatturazione, puoi farlo tramite una richiesta di Billing and Account Support. Per ulteriori informazioni AWS Billing and Cost Management, inclusi addebiti e metodi di pagamento, consulta Ottenere assistenza per. AWS Billing

Ho una domanda su un ordine al dettaglio

Se hai un problema con il tuo account www.amazon.com o una domanda su un ordine al dettaglio, consulta Opzioni di supporto e Contattaci.

Ho bisogno di aiuto per gestire il mio Account AWS

Se hai bisogno di aiuto per cambiare una carta di credito Account AWS, segnalare attività fraudolente o chiudere la tua Account AWS, consulta Risoluzione di altri problemi con. Account AWS

Le mie credenziali del portale di AWS accesso non funzionano

Quando non riesci ad AWS accedere al portale di accesso, prova a ricordare come hai effettuato l'accesso AWS in precedenza.

Se non ricordi di aver usato una password

Potresti aver effettuato l'accesso in precedenza AWS senza utilizzare AWS credenziali. Questo è comune per il single sign-on aziendale tramite IAM Identity Center. L'accesso in AWS questo modo significa che si utilizzano le credenziali aziendali per accedere agli AWS account o alle applicazioni senza inserire le proprie credenziali.

- AWS portale di accesso: se un amministratore consente di utilizzare credenziali esterne AWS per accedere AWS, è necessario l'URL del portale. Controlla la tua e-mail, i preferiti del browser o la

cronologia del browser per trovare un URL che includa `awsapps.com/start` o `signin.aws/platform/login`.

Ad esempio, il tuo URL personalizzato potrebbe includere un ID o un dominio come `https://d-1234567890.awsapps.com/start`. Se non riesci a trovare il link al portale, contatta l'amministratore. Supporto non posso aiutarti a recuperare queste informazioni.

Se ricordi nome utente e password, ma le credenziali non funzionano, è possibile che ti trovi nella pagina sbagliata. Controlla l'URL nel tuo browser web: se è https://signin.aws.amazon.com/allora un utente federato o un utente di IAM Identity Center non può accedere utilizzando le proprie credenziali.

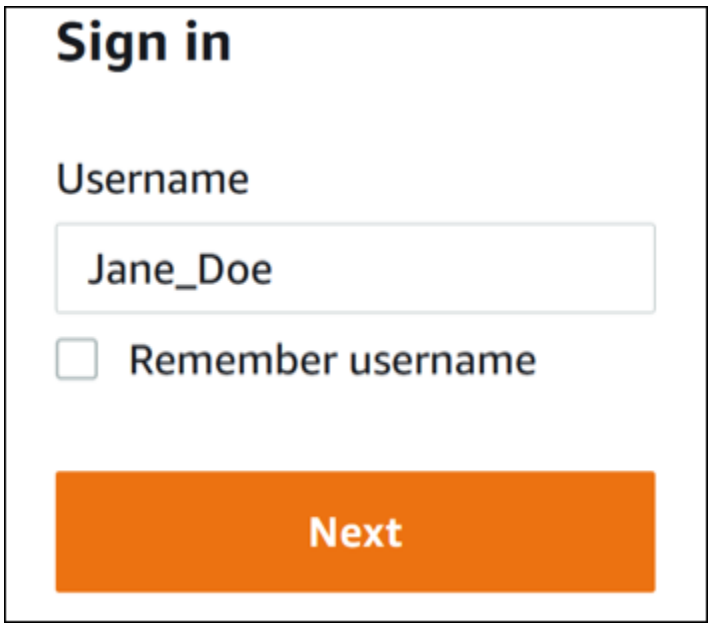
- AWS portale di accesso: se un amministratore configura una fonte di identità AWS IAM Identity Center (successore di AWS Single Sign-On) per AWS, devi accedere utilizzando il tuo nome utente e password al portale di accesso della AWS tua organizzazione. Per individuare l'URL del portale, controlla la posta elettronica, l'archiviazione sicura delle password, i preferiti del browser o la cronologia del browser per individuare un URL che includa o. `awsapps.com/start` `signin.aws/platform/login` Ad esempio, l'URL personalizzato potrebbe includere un ID o un dominio, ad esempio `https://d-1234567890.awsapps.com/start.` Se non riesci a trovare il link al portale, contatta l'amministratore. Supporto non posso aiutarti a recuperare queste informazioni.

Ho dimenticato la password del mio IAM Identity Center Account AWS

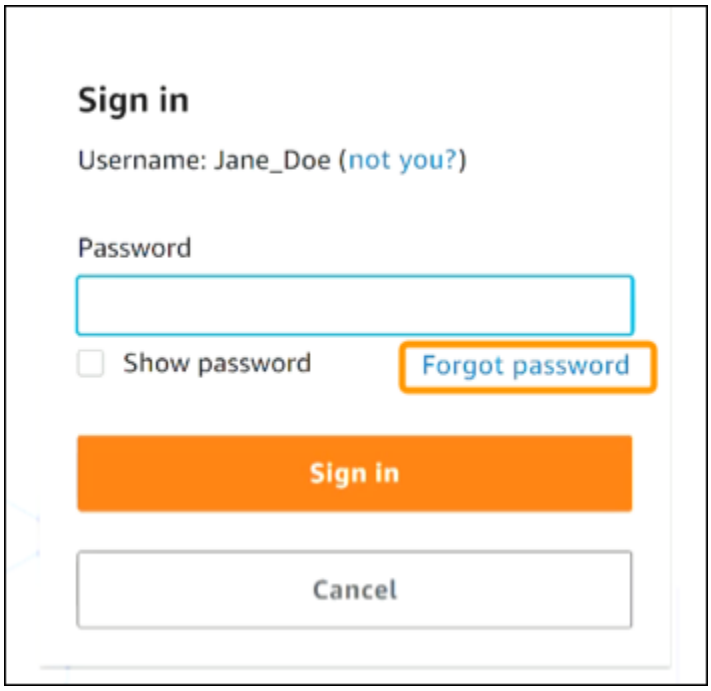
Se sei un utente di IAM Identity Center e hai perso o dimenticato la password del tuo account Account AWS, puoi reimpostarla. Devi conoscere l'indirizzo e-mail utilizzato per l'account IAM Identity Center e potervi accedere. Un link per reimpostare la password viene inviato alla tua Account AWS email.

Per reimpostare la password dell'utente in IAM Identity Center

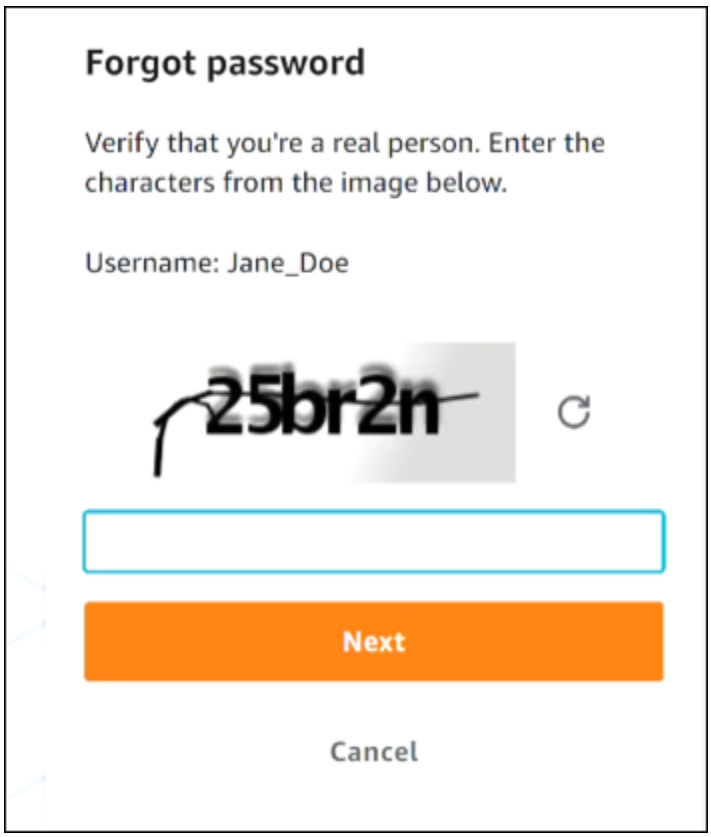
1. Usa il link URL del portale di AWS accesso e inserisci il tuo nome utente. Quindi, seleziona Next (Successivo).



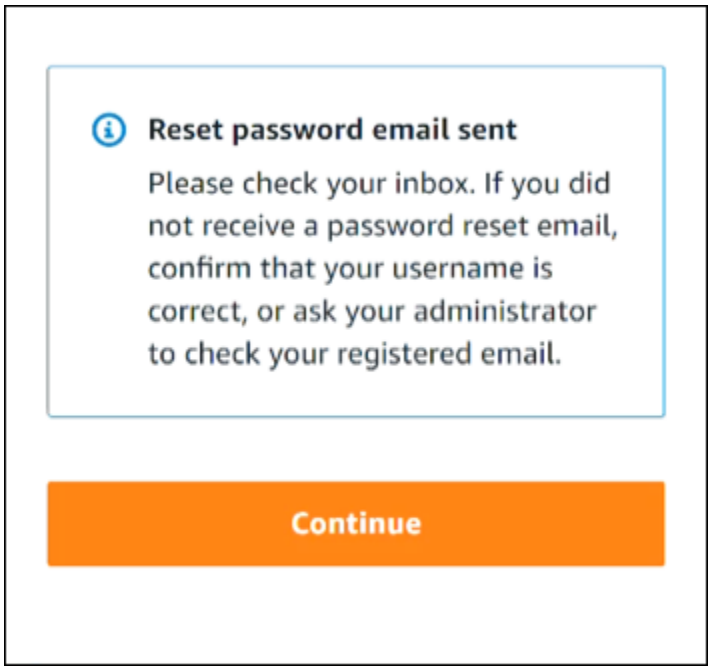
2. Seleziona Password dimenticata come mostrato nell'immagine seguente.



3. Completa i passaggi per il recupero della password.



4. Dopo aver completato la procedura di recupero della password, ricevi il seguente messaggio che conferma che ti è stato inviato un messaggio e-mail che puoi utilizzare per reimpostare la password.



Un'e-mail con un link per reimpostare la password viene inviata all'e-mail associata all'account utente IAM Identity Center. Seleziona il link fornito nell' AWS e-mail per reimpostare la password. Il link ti indirizza a una nuova pagina Web per creare una nuova password. Dopo aver creato una nuova password, riceverai la conferma che la reimpostazione della password è avvenuta con successo.

Se non hai ricevuto un'e-mail per reimpostare la password, chiedi all'amministratore di confermare quale e-mail è registrata con il tuo utente in IAM Identity Center.

Ricevo un messaggio di errore che dice «Non sei tu, siamo noi» quando provo ad accedere alla console IAM Identity Center

Questo errore indica che c'è un problema di configurazione con l'istanza di IAM Identity Center o con il provider di identità esterno (IdP) che utilizza come fonte di identità. Ti consigliamo di verificare quanto segue:

- Verifica le impostazioni di data e ora sul dispositivo che stai utilizzando per accedere. Ti consigliamo di consentire l'impostazione automatica di data e ora. Se non è disponibile, ti consigliamo di sincronizzare la data e l'ora con un server Network Time Protocol (NTP) noto.
- Verifica che il certificato IdP caricato su IAM Identity Center sia lo stesso fornito dal tuo provider di identità. Puoi controllare il certificato dalla console IAM Identity Center accedendo a Impostazioni. Nella scheda Identity Source, in Azione, scegli Gestisci autenticazione. Potrebbe essere necessario importare un nuovo certificato.
- Nel file di metadati SAML del tuo IdP, assicurati che il formato NameID sia. `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
- Se utilizzi AD Connector, verifica che le credenziali per l'account di servizio siano corrette e non siano scadute. Per ulteriori informazioni, consulta Aggiornare le credenziali dell'account del servizio AD Connector in AWS Directory Service.

Risoluzione dei problemi relativi al AWS Builder ID

Utilizza le informazioni qui per aiutarti a risolvere i problemi che potresti avere con il tuo. ID Builder AWS

Argomenti

- La mia e-mail è già in uso
- Non è possibile completare la verifica dell'e-mail
- Ricevo un errore che dice «Non sei tu, siamo noi» quando provo ad accedere con il mio ID Builder AWS
- Ho dimenticato la mia password
- Non riesco a impostare una nuova password
- La mia password non funziona
- La mia password non funziona e non riesco più ad accedere alle e-mail inviate al mio indirizzo e-mail AWS Builder ID
- Non riesco ad abilitare l'MFA
- Non riesco ad aggiungere un'app di autenticazione come dispositivo MFA
- Non riesco a rimuovere un dispositivo MFA
- Ricevo il messaggio "An unexpected error has occurred" (Si è verificato un errore imprevisto) quando provo a registrarmi o accedere con un'app di autenticazione
- Ricevo il messaggio «Non sei tu, siamo noi» quando provo ad accedere a Builder ID AWS
- La disconnessione non mi disconnette completamente
- Sto ancora cercando di risolvere il mio problema

La mia e-mail è già in uso

Se l'email che hai inserito è già in uso e la riconosci come tua, allora potresti aver già registrato un AWS Builder ID. Prova ad accedere utilizzando quell'indirizzo e-mail. Se non ricordi la password, consulta Ho dimenticato la mia password.

Non è possibile completare la verifica dell'e-mail

Se ti sei registrato a AWS Builder ID ma non hai ricevuto l'email di verifica, completa le seguenti attività di risoluzione dei problemi.

1. Controlla la cartella dello spam, della posta indesiderata e degli elementi eliminati.

   > **Note**
   >
   > Questa email di verifica proviene dall'indirizzo no-reply@signin.aws o no-reply@login.awsapps.com. Ti consigliamo di configurare il tuo sistema di posta in modo che accetti le e-mail da questi indirizzi del mittente e non le gestisca come posta indesiderata o spam.

2. Scegli Resend code (Reinvia codice), aggiorna la tua casella di posta e controlla nuovamente le cartelle dello spam, della posta indesiderata e degli elementi eliminati.
3. Se continui a non visualizzare l'email di verifica, ricontrolla l'indirizzo email del AWS Builder ID per eventuali errori di battitura. Se hai inserito l'indirizzo e-mail sbagliato, registrati nuovamente con un indirizzo e-mail di tua proprietà.

Ricevo un errore che dice «Non sei tu, siamo noi» quando provo ad accedere con il mio ID Builder AWS

Se ricevi questo messaggio di errore quando tenti di accedere, potrebbe esserci un problema con le impostazioni locali o l'indirizzo email.

- Verifica le impostazioni di data e ora sul dispositivo che stai utilizzando per accedere. Ti consigliamo di consentire l'impostazione automatica di data e ora. Se non è disponibile, ti consigliamo di sincronizzare la data e l'ora con un server Network Time Protocol (NTP) noto.
- Controlla il tuo indirizzo email per eventuali errori di formattazione. I seguenti problemi restituiranno un errore quando provi ad accedere con il tuo ID Builder AWS.
  - Spazio in un indirizzo email
  - Barra (/) in un indirizzo e-mail
  - Due punti (.) in un indirizzo e-mail
  - Due e commerciali (@) in un indirizzo e-mail

- Virgola (,) alla fine di un indirizzo e-mail
- Parentesi (]) alla fine di un indirizzo e-mail

Ho dimenticato la mia password

Reimpostazione della password dimenticata

1. Nella pagina Accedi con AWS Builder ID, inserisci l'email che hai usato per creare il tuo ID AWS Builder in Indirizzo e-mail. Scegli Next (Successivo).
2. Seleziona Forgot Password? (Password dimenticata?). Inviamo un link all'indirizzo email associato al tuo ID AWS Builder dove puoi reimpostare la password.
3. Segui le istruzioni nell'e-mail.

Non riesco a impostare una nuova password

Per motivi di sicurezza, devi seguire questi requisiti ogni volta che imposti o modifichi la password:

- Le password distinguono tra maiuscole e minuscole.
- La lunghezza delle password deve essere compresa tra 8 e 64 caratteri.
- Le password devono contenere almeno un carattere per ognuna delle quattro categorie seguenti:
  - Lettere minuscole (a-z)
  - Lettere maiuscole (A-Z)
  - Numeri (0-9)
  - Caratteri non alfanumerici (~!@#$%^portale di gestione*_-+=`|\(){}[]:;'"<>,.?/)
- Le ultime tre password non possono essere riutilizzate.
- Le password che sono note pubblicamente attraverso un set di dati divulgato da terze parti non possono essere utilizzate.

La mia password non funziona

Se ricordi la password, ma non funziona quando accedi con AWS Builder ID, assicurati che:

- Il blocco delle maiuscole sia disattivato.
- Non stai utilizzando una password più vecchia.

- Stai usando la tua password AWS Builder ID e non una password per un. Account AWS

Se verifichi che la password up-to-date sia stata inserita correttamente, ma continua a non funzionare, segui le istruzioni Ho dimenticato la mia password per reimpostare la password.

La mia password non funziona e non riesco più ad accedere alle e-mail inviate al mio indirizzo e-mail AWS Builder ID

Se riesci ancora ad accedere al tuo AWS Builder ID, usa la pagina Profilo per aggiornare l'email del AWS Builder ID con il tuo nuovo indirizzo email. Dopo aver completato la verifica dell'email, potrai accedere AWS e ricevere comunicazioni al tuo nuovo indirizzo email.

Se hai utilizzato un indirizzo e-mail aziendale o universitario e hai lasciato l'azienda o la scuola e non riesci a ricevere alcuna e-mail inviata a quell'indirizzo, contatta l'amministratore del sistema di posta elettronica. Potrebbero essere in grado di inoltrare la tua e-mail a un nuovo indirizzo, concederti un accesso temporaneo o condividere contenuti dalla tua casella di posta.

Non riesco ad abilitare l'MFA

Per abilitare l'autenticazione a più fattori, aggiungi uno o più dispositivi MFA al tuo profilo seguendo i passaggi riportati in Gestione dell' ID Builder AWS autenticazione a più fattori (MFA).

Non riesco ad aggiungere un'app di autenticazione come dispositivo MFA

Se non riesci ad aggiungere un altro dispositivo MFA, potresti aver raggiunto il limite di dispositivi MFA che puoi registrare in quell'applicazione. Prova a rimuovere un dispositivo MFA inutilizzato o a utilizzare un'altra app di autenticazione.

Non riesco a rimuovere un dispositivo MFA

Se desideri disabilitare l'autenticazione a più fattori, procedi con la rimozione del dispositivo MFA seguendo i passaggi riportati in Eliminare il dispositivo MFA. Tuttavia, se desideri lasciare l'MFA abilitata, prima di provare a eliminare un dispositivo MFA esistente dovrai aggiungere un altro dispositivo MFA. Per ulteriori informazioni sull'aggiunta di un altro dispositivo MFA, consulta Gestione dell' ID Builder AWS autenticazione a più fattori (MFA).

Ricevo il messaggio "An unexpected error has occurred" (Si è verificato un errore imprevisto) quando provo a registrarmi o accedere con un'app di autenticazione

Un sistema di password monouso (TOTP) basato sul tempo, come quello utilizzato da AWS Builder ID in combinazione con un'app di autenticazione basata su codice, si basa sulla sincronizzazione temporale tra il client e il server. Assicurati che il dispositivo su cui è installata l'app di autenticazione sia sincronizzato correttamente con una origine temporale affidabile o imposta manualmente l'ora sul dispositivo in modo che corrisponda a un'origine attendibile, come il NIST o altri equivalenti locali/regionali.

Ricevo il messaggio «Non sei tu, siamo noi» quando provo ad accedere a Builder ID AWS

Verifica le impostazioni di data e ora sul dispositivo che stai utilizzando per accedere. Ti consigliamo di impostare la data e l'ora in modo che vengano impostate automaticamente. Se non è disponibile, ti consigliamo di sincronizzare la data e l'ora con un server Network Time Protocol (NTP) noto.

La disconnessione non mi disconnette completamente

Il sistema è progettato per disconnettersi immediatamente, ma la disconnessione completa può richiedere fino a un'ora.

Sto ancora cercando di risolvere il mio problema

Puoi compilare il modulo di feedback per l'assistenza. Nella sezione Richiedi informazioni, sotto Come possiamo aiutarti, indica che stai utilizzando AWS Builder ID. Fornisci il maggior numero di dettagli possibile in modo che possiamo risolvere il problema nel modo più efficiente.

Cronologia dei documenti

La tabella seguente descrive importanti aggiunte alla documentazione di AWS accesso. Inoltre, aggiorniamo frequentemente la documentazione tenendo conto dei feedback ricevuti.

- Ultimo aggiornamento importante della documentazione: 27 febbraio 2024

Modifica	Descrizione	Data
Argomenti aggiornati per la risoluzione	Sono stati aggiunti nuovi argomenti di risoluzione dei problemi relativi all'accesso a ID Builder AWS e al AWS Management Console.	27 febbraio 2024
Sono stati aggiornati diversi argomenti per l'organizzazione	Tipi di utente aggiornati, rimossi Determina il tipo di utente e ne ha incorporato il contenuto nei tipi di utente, Come accedere a AWS	15 maggio 2023
Sono stati aggiornati diversi argomenti e il banner principal e	Tipi di utenti aggiornati, Determina il tipo di utente , come accedere AWS, Cos'è AWS l'accesso? . Sono state inoltre aggiornate le procedure di accesso per utenti root e utenti IAM.	3 marzo 2023
Paragrafo introduttivo aggiornato per l' AWS Management Console accesso	È stato spostato Determine del tipo di utente nella parte superiore della pagina e ha rimosso la nota esistente in Account root user.	27 febbraio 2023
Aggiunto ID Builder AWS	Sono stati aggiunti ID Builder AWS argomenti alla Guida	31 gennaio 2023

	per AWS l'utente di accesso e contenuto integrato negli argomenti esistenti.	
Aggiornamento organizzativo	In base al feedback dei clienti, il sommario è stato aggiornato per essere più chiaro sui metodi di accesso. Sono stati aggiornati i tutorial di accesso. Terminologia aggiornata e determinazione del tipo di utente. Collegamento incrociato migliorato per definire termini come utente IAM e utente root.	22 dicembre 2022
Nuova guida	Questa è la prima versione della guida per l'utente di AWS accesso.	31 agosto 2022

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.