Panduan Pengguna

AWS Sign-In

AWS Sign-In: Panduan Pengguna

Table of Contents

Apa itu AWS Sign-In?

Panduan ini membantu Anda memahami berbagai cara masuk ke Amazon Web Services (AWS), tergantung pada jenis pengguna Anda. Untuk informasi selengkapnya tentang cara masuk berdasarkan jenis pengguna dan AWS sumber daya yang ingin Anda akses, lihat salah satu tutorial berikut.

- Masuk ke Konsol Manajemen AWS
- Masuk ke AWS portal akses
- Masuk sebagai identitas federasi
- Masuk melalui AWS Command Line Interface
- Masuk dengan ID AWS Builder

Jika Anda mengalami masalah saat masuk Akun AWS, lihatPemecahan Masalah Akun AWS masalah masuk. Untuk bantuan dengan kunjungan ID AWS Builder AndaMemecahkan masalah AWS Builder ID. Ingin membuat Akun AWS? Mendaftar untuk AWS. Untuk informasi selengkapnya tentang cara mendaftar AWS dapat membantu Anda atau organisasi Anda, lihat Hubungi Kami.

Topik

- Terminologi
- Ketersediaan wilayah untuk AWS Sign-In
- Sign-in pencatatan peristiwa
- Tentukan jenis pengguna Anda
- Tentukan URL masuk Anda
- Domain untuk ditambahkan ke daftar izin Anda
- Praktik terbaik keamanan untuk Akun AWS administrator

Terminologi

Amazon Web Services (AWS) menggunakan terminologi umum untuk menggambarkan proses masuk. Kami menyarankan Anda membaca dan memahami istilah-istilah ini.

Administrator

Juga disebut sebagai administrator atau Akun AWS administrator IAM. Administrator, biasanya personel Teknologi Informasi (TI), adalah individu yang mengawasi Akun AWS. Administrator memiliki tingkat izin yang lebih tinggi Akun AWS daripada anggota lain dari organisasi mereka. Administrator menetapkan dan mengimplementasikan pengaturan untuk. Akun AWS Mereka juga membuat pengguna IAM atau IAM Identity Center. Administrator memberi pengguna ini kredensyal akses mereka dan URL masuk untuk masuk. AWS

Akun

Standar Akun AWS berisi AWS sumber daya Anda dan identitas yang dapat mengakses sumber daya tersebut. Akun dikaitkan dengan alamat email dan kata sandi pemilik akun.

Kredensial

Juga disebut sebagai kredensial akses atau kredensial keamanan. Dalam autentikasi dan otorisasi, sistem menggunakan kredensial untuk mengidentifikasi siapa yang membuat panggilan dan apakah akan mengizinkan akses yang diminta. Kredensyal adalah informasi yang diberikan pengguna AWS untuk masuk dan mendapatkan akses ke AWS sumber daya. Kredensyal untuk pengguna manusia dapat mencakup alamat email, nama pengguna, kata sandi yang ditentukan pengguna, ID akun atau alias, kode verifikasi, dan kode otentikasi multi-faktor penggunaan tunggal (MFA). Untuk akses terprogram, Anda juga dapat menggunakan tombol akses. Sebaiknya gunakan kunci akses jangka pendek jika memungkinkan.

Untuk informasi selengkapnya tentang kredensyal, lihat kredensyal AWS keamanan.

> **Note**
>
> Jenis kredensyal yang harus dikirimkan pengguna tergantung pada jenis penggunanya.

Kredensi perusahaan

Kredensyal yang diberikan pengguna saat mengakses jaringan dan sumber daya perusahaan mereka. Administrator perusahaan Anda dapat mengatur Akun AWS agar Anda menggunakan kredensyal yang sama dengan yang Anda gunakan untuk mengakses jaringan dan sumber daya perusahaan Anda. Kredensyal ini diberikan kepada Anda oleh administrator atau karyawan help desk Anda.

Profil

Ketika Anda mendaftar untuk AWS Builder ID, Anda membuat profil. Profil Anda mencakup informasi kontak yang Anda berikan dan kemampuan untuk mengelola perangkat otentikasi multi-faktor (MFA) dan sesi aktif. Anda juga dapat mempelajari lebih lanjut tentang privasi dan cara kami menangani data Anda di profil Anda. Untuk informasi selengkapnya tentang profil Anda dan bagaimana kaitannya dengan profil Akun AWS, lihatID AWS Builder dan AWS kredensi lainnya.

Kredensial pengguna root

Kredensyal pengguna root adalah alamat email dan kata sandi yang digunakan untuk membuat file. Akun AWS Kami sangat menyarankan agar MFA ditambahkan ke kredensyal pengguna root untuk keamanan tambahan. Kredensyal pengguna root menyediakan akses lengkap ke semua AWS layanan dan sumber daya di akun. Untuk informasi selengkapnya tentang pengguna root, lihatPengguna root.

Pengguna

Pengguna adalah orang atau aplikasi yang memiliki izin untuk melakukan panggilan API ke AWS produk atau mengakses AWS sumber daya. Setiap pengguna memiliki seperangkat kredensyal keamanan unik yang tidak dibagikan dengan pengguna lain. Kredensial ini terpisah dari kredensial keamanan untuk Akun AWS. Untuk informasi selengkapnya, lihat Tentukan jenis pengguna Anda.

Kode verifikasi

Kode verifikasi memverifikasi identitas Anda selama proses masuk menggunakan otentikasi multi-faktor (MFA). Metode pengiriman untuk kode verifikasi bervariasi. Mereka dapat dikirim melalui pesan teks atau email. Periksa dengan administrator Anda untuk informasi lebih lanjut.

Ketersediaan wilayah untuk AWS Sign-In

AWS Sign-in tersedia dalam beberapa yang umum digunakan Wilayah AWS. Ketersediaan ini memudahkan Anda untuk mengakses AWS layanan dan aplikasi bisnis. Untuk daftar lengkap Wilayah yang Sign-in mendukung, lihat AWS Sign-In titik akhir dan kuota.

Sign-in pencatatan peristiwa

CloudTrail diaktifkan secara otomatis pada Anda Akun AWS dan merekam peristiwa saat aktivitas terjadi. Sumber daya berikut dapat membantu Anda mempelajari lebih lanjut tentang pencatatan dan pemantauan peristiwa masuk.

- CloudTrail log mencoba untuk masuk ke Konsol Manajemen AWS. Semua pengguna IAM, pengguna root, dan peristiwa login pengguna federasi menghasilkan catatan dalam CloudTrail file log. Untuk informasi selengkapnya, lihat peristiwa Konsol Manajemen AWS login di Panduan AWS CloudTrail Pengguna.
- Jika Anda menggunakan titik akhir Regional untuk masuk ke Konsol Manajemen AWS, CloudTrail mencatat `ConsoleLogin` peristiwa di Wilayah yang sesuai untuk titik akhir. Untuk informasi selengkapnya tentang AWS Sign-In titik akhir, lihat AWS Sign-In titik akhir dan kuota di Panduan Referensi AWS Umum.
- Untuk mempelajari selengkapnya tentang cara CloudTrail log masuk peristiwa login untuk Pusat Identitas IAM, lihat Memahami peristiwa masuk Pusat Identitas IAM di Panduan Pengguna Pusat Identitas IAM.
- Untuk mempelajari selengkapnya tentang cara CloudTrail mencatat informasi identitas pengguna yang berbeda di IAM, lihat Mencatat panggilan IAM dan AWS STS API AWS CloudTrail di AWS Identity and Access Management Panduan Pengguna.

AWS Sign-In mendukung kebijakan berbasis sumber daya dan kebijakan kontrol sumber daya yang memungkinkan Anda membatasi akses konsol berdasarkan lokasi jaringan dan identitas utama. Untuk pengguna root, lokasi jaringan divalidasi sebelum prompt kata sandi muncul. Untuk semua tipe utama, kebijakan dievaluasi pada pra-otentikasi dan pasca-otentikasi. Untuk informasi selengkapnya, lihat Mengontrol akses konsol dengan kebijakan berbasis sumber daya dan kebijakan kontrol sumber daya.

Tentukan jenis pengguna Anda

Cara Anda masuk tergantung pada jenis AWS pengguna Anda. Anda dapat mengelola Akun AWS sebagai pengguna root, pengguna IAM, pengguna di IAM Identity Center, atau identitas federasi. Anda dapat menggunakan profil AWS Builder ID untuk mengakses AWS layanan dan alat tertentu. Jenis pengguna yang berbeda tercantum di bawah ini.

Topik

- Pengguna root
- Pengguna IAM
- Pengguna Pusat Identitas IAM
- Identitas terfederasi
- AWS Pengguna ID Builder

Pengguna root

Juga disebut sebagai pemilik akun atau pengguna root akun. Sebagai pengguna root, Anda memiliki akses lengkap ke semua AWS layanan dan sumber daya di Anda Akun AWS. Saat pertama kali membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua AWS layanan dan sumber daya di akun. Identitas ini adalah pengguna root AWS akun. Anda dapat masuk sebagai pengguna root menggunakan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Pengguna root masuk dengan file Konsol Manajemen AWS. Untuk petunjuk langkah demi langkah tentang cara masuk, lihatMasuk ke Konsol Manajemen AWS sebagai pengguna root.

> **Important**
>
> Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang identitas IAM termasuk pengguna root, lihat Identitas IAM (pengguna, grup pengguna, dan peran).

Pengguna IAM

Pengguna IAM adalah entitas yang Anda buat. AWS Pengguna ini adalah identitas di dalam Anda Akun AWS yang diberikan izin khusus khusus. Kredensi pengguna IAM Anda terdiri dari nama dan kata sandi yang digunakan untuk masuk ke. Konsol Manajemen AWS Untuk petunjuk langkah demi langkah tentang cara masuk, lihatMasuk ke Konsol Manajemen AWS sebagai pengguna IAM.

Untuk informasi selengkapnya tentang identitas IAM termasuk pengguna IAM, lihat Identitas IAM (pengguna, grup pengguna, dan peran).

Pengguna Pusat Identitas IAM

Pengguna IAM Identity Center adalah anggota AWS Organizations dan dapat diberikan akses ke beberapa aplikasi Akun AWS dan melalui portal AWS akses Anda. Jika perusahaan mereka telah mengintegrasikan Active Directory atau penyedia identitas lain dengan IAM Identity Center, pengguna di IAM Identity Center dapat menggunakan kredensyal perusahaan mereka untuk masuk. IAM Identity Center juga dapat menjadi penyedia identitas tempat administrator dapat membuat pengguna. Terlepas dari penyedia identitas, pengguna di Pusat Identitas IAM masuk menggunakan portal AWS akses Anda, yang merupakan URL masuk khusus untuk organisasi mereka. Pengguna IAM Identity Center tidak dapat masuk melalui Konsol Manajemen AWS URL.

Pengguna manusia di IAM Identity Center bisa mendapatkan URL portal AWS akses Anda dari:

- Pesan dari administrator atau karyawan help desk
- Email dari AWS dengan undangan untuk bergabung dengan IAM Identity Center

> **Tip**
>
> Semua email yang dikirim oleh layanan IAM Identity Center berasal dari alamat no-reply@signin.aws atau no-reply@login.awsapps.com. Kami menyarankan Anda mengonfigurasi sistem email Anda sehingga menerima email dari alamat email pengirim ini dan tidak menanganinya sebagai sampah atau spam.

Untuk petunjuk langkah demi langkah tentang cara masuk, lihatMasuk ke AWS portal akses.

> **Note**
>
> Kami menyarankan Anda menandai URL login khusus organisasi Anda untuk portal AWS akses Anda sehingga Anda dapat mengaksesnya nanti.

Untuk informasi selengkapnya tentang Pusat Identitas IAM, lihat Apa itu Pusat Identitas IAM?

Identitas terfederasi

Identitas federasi adalah pengguna yang dapat masuk menggunakan penyedia identitas eksternal (IDP) yang terkenal, seperti Login with Amazon, Facebook, Google, atau iDP lain yang kompatibel dengan OpenID Connect (OIDC). Dengan federasi identitas web, Anda dapat menerima token otentikasi, dan kemudian menukar token itu dengan kredensyal keamanan sementara di peta AWS itu ke peran IAM dengan izin untuk menggunakan sumber daya di Anda. Akun AWS Anda tidak masuk dengan Konsol Manajemen AWS atau AWS mengakses portal. Sebagai gantinya, identitas eksternal yang digunakan menentukan cara Anda masuk.

Untuk informasi selengkapnya, lihat Masuk sebagai identitas federasi.

AWS Pengguna ID Builder

Sebagai pengguna AWS Builder ID, Anda secara khusus masuk ke AWS layanan atau alat yang ingin Anda akses. Pengguna AWS Builder ID melengkapi semua yang sudah Akun AWS Anda miliki atau ingin buat. AWS Builder ID mewakili Anda sebagai pribadi, dan Anda dapat menggunakannya untuk mengakses AWS layanan dan alat tanpa Akun AWS. Anda juga memiliki profil tempat Anda dapat melihat dan memperbarui informasi Anda. Untuk informasi selengkapnya, lihat Masuk dengan ID AWS Builder.

AWS Builder ID terpisah dari langganan AWS Skill Builder Anda, pusat pembelajaran online tempat Anda dapat belajar dari AWS para ahli dan membangun keterampilan cloud secara online. Untuk informasi selengkapnya tentang AWS Skill Builder, lihat AWS Skill Builder.

Tentukan URL masuk Anda

Gunakan salah satu URL berikut untuk mengakses AWS tergantung pada jenis AWS pengguna Anda. Untuk informasi selengkapnya, lihat Tentukan jenis pengguna Anda.

Topik

- Akun AWS URL masuk pengguna root
- AWS portal akses
- URL masuk pengguna IAM
- URL identitas federasi
- AWS URL ID Pembuat

Akun AWS URL masuk pengguna root

Pengguna root mengakses Konsol Manajemen AWS dari halaman AWS masuk:. https://console.aws.amazon.com/

Halaman login ini juga memiliki opsi untuk masuk sebagai pengguna IAM.

AWS portal akses

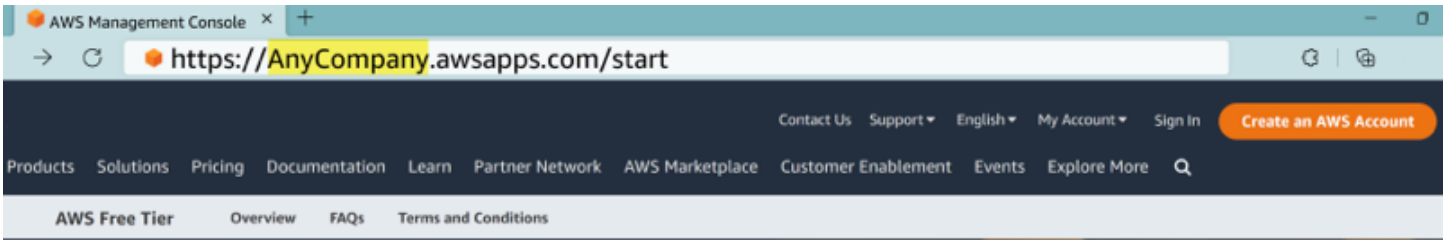
Portal AWS akses adalah URL masuk khusus bagi pengguna di Pusat Identitas IAM untuk masuk dan mengakses akun Anda. Saat administrator membuat pengguna di Pusat Identitas IAM, administrator memilih apakah pengguna menerima undangan email untuk bergabung dengan Pusat Identitas IAM atau pesan dari administrator atau karyawan help desk yang berisi kata sandi satu kali dan AWS URL portal akses. Format URL login tertentu seperti contoh berikut:

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

atau

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

URL login tertentu bervariasi karena administrator Anda dapat menyesuaikannya. URL login spesifik mungkin dimulai dengan huruf D diikuti oleh 10 angka dan huruf acak. Subdomain Anda juga dapat digunakan di URL masuk dan mungkin menyertakan nama perusahaan Anda seperti contoh berikut:



> **Note**
>
> Kami menyarankan Anda menandai URL masuk khusus untuk portal AWS akses Anda sehingga Anda dapat mengaksesnya nanti.

Untuk informasi selengkapnya tentang portal AWS akses Anda, lihat Menggunakan portal AWS akses.

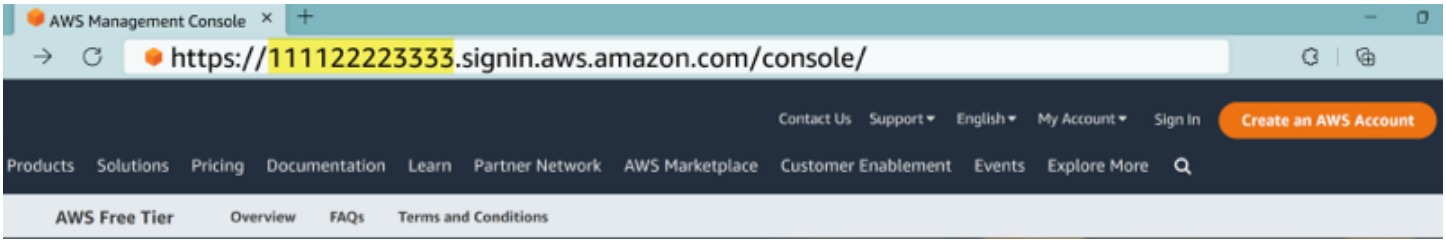
URL masuk pengguna IAM

Pengguna IAM dapat mengakses Konsol Manajemen AWS dengan URL masuk pengguna IAM tertentu. URL login pengguna IAM menggabungkan Akun AWS ID atau alias Anda dan `signin.aws.amazon.com/console`

Contoh tampilan URL masuk pengguna IAM:

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

Jika ID akun Anda adalah 111122223333, URL masuk Anda adalah:



Jika Anda mengalami masalah saat mengakses URL masuk pengguna IAM Anda, lihat Ketahanan untuk informasi selengkapnya. Akun AWS AWS Identity and Access Management

URL identitas federasi

URL masuk untuk identitas federasi bervariasi. Identitas eksternal atau Penyedia Identitas eksternal (iDP) menentukan URL masuk untuk identitas gabungan. Identitas eksternal dapat berupa Windows Active Directory, Login with Amazon, Facebook, atau Google. Hubungi administrator Anda untuk detail selengkapnya tentang cara masuk sebagai identitas federasi.

Untuk informasi selengkapnya tentang identitas federasi, lihat Tentang federasi identitas web.

AWS URL ID Pembuat

URL untuk profil AWS Builder ID Anda adalahhttps://profile.aws.amazon.com/. Saat menggunakan AWS Builder ID Anda, URL login bergantung pada layanan apa yang ingin Anda akses. Misalnya, untuk masuk ke Amazon CodeCatalyst, bukahttps://codecatalyst.aws/login.

Domain untuk ditambahkan ke daftar izin Anda

Jika Anda memfilter akses ke AWS domain atau titik akhir URL tertentu dengan menggunakan solusi pemfilteran konten web seperti firewall generasi berikutnya (NGFW) atau Secure Web

Gateways (SWG), Anda harus menambahkan domain atau titik akhir URL berikut ke daftar izin solusi pemfilteran konten web Anda.

AWS Sign-In domain untuk daftar yang diizinkan

Jika Anda atau organisasi Anda menerapkan pemfilteran IP atau domain, Anda mungkin perlu mengizinkan daftar domain untuk menggunakan. Konsol Manajemen AWS Domain berikut harus dapat diakses di jaringan tempat Anda mencoba mengakses. Konsol Manajemen AWS

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

AWS Sign-In domain administrasi untuk daftar yang diizinkan

Jika Anda mengonfigurasi kontrol akses konsol dengan menggunakan AWS CLI, Anda harus mengizinkan daftar titik akhir bidang AWS Sign-In kontrol. Titik akhir ini menangani administrasi kebijakan dan berbeda dari domain login konsol di bagian sebelumnya.

- `signin.[Region].api.aws`

  Ganti *[Region]* dengan AWS Wilayah yang Anda panggil. Tersedia di semua Wilayah komersial. Contoh:`signin.us-east-1.api.aws`.

Portal akses AWS domain untuk daftar yang diizinkan

Jika Anda memfilter akses ke AWS domain atau titik akhir URL tertentu dengan menggunakan solusi pemfilteran konten web seperti firewall generasi berikutnya (NGFW) atau Secure Web Gateways (SWG), Anda harus menambahkan domain atau titik akhir URL berikut ke daftar izin solusi pemfilteran konten web Anda. Melakukan hal itu memungkinkan Anda untuk mengakses Anda Portal akses AWS.

Daftar berikut menyediakan domain IPv4 dan dual-stack serta endpoint URL untuk ditambahkan ke daftar izin solusi penyaringan konten web Anda. Untuk informasi selengkapnya tentang titik akhir

dual-stack, lihat Memperbarui firewall dan gateway untuk mengizinkan akses ke Panduan Pengguna Pusat Identitas Portal akses AWS IAM.

IPv4 memungkinkan daftar

- *[Directory ID or alias]*.awsapps.com
- *[IAM Identity Center instance ID]*.*[Region]*.portal.amazonaws.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

Dual-stack izinkan daftar

- *[IAM Identity Center instance ID]*.portal.*[Region]*.app.aws
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.api.aws
- sso.*[Region]*.api.aws
- portal.sso.*[Region]*.api.aws
- *[Region]*.sso.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- cdn.us-east-1.threat-mitigation.aws.amazon.com
- us-east-1.threat-mitigation.aws.amazon.com
- amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com

ID AWS Builder domain untuk daftar yang diizinkan

Jika Anda atau organisasi Anda menerapkan pemfilteran IP atau domain, Anda mungkin perlu mengizinkan daftar domain untuk membuat dan menggunakan file. ID AWS Builder Domain berikut harus dapat diakses di jaringan tempat Anda mencoba mengakses ID AWS Builder.

- `view.awsapps.com/start`
- `*.portal.*.app.aws`
- `*.aws.dev`
- `*.api.aws`
- `*.uis.awsstatic.com`
- `*.console.aws.a2z.com`
- `oidc.*.amazonaws.com`
- `oidc.*.api.aws`
- `*.sso.amazonaws.com`
- `*.sso.*.amazonaws.com`
- `*.sso-portal.*.amazonaws.com`
- `sso.*.api.aws`
- `*.signin.aws`
- `*.cloudfront.net`
- `opfcaptcha-prod.s3.amazonaws.com`
- `profile.aws.amazon.com`

Praktik terbaik keamanan untuk Akun AWS administrator

Jika Anda adalah administrator akun yang telah membuat akun baru Akun AWS, kami menyarankan langkah-langkah berikut untuk membantu pengguna Anda mengikuti praktik terbaik AWS keamanan saat mereka masuk.

1. Masuk sebagai pengguna root untuk Aktifkan otentikasi multi-faktor (MFA) dan buat pengguna AWS administratif di IAM Identity Center jika Anda belum melakukannya. Kemudian, lindungi kredensyal root Anda dan jangan gunakan untuk tugas sehari-hari.
2. Masuk sebagai Akun AWS administrator dan atur identitas berikut:

- Buat pengguna dengan hak istimewa paling sedikit untuk manusia lain.
- Siapkan kredensial sementara untuk beban kerja.
- Buat kunci akses hanya untuk kasus penggunaan yang memerlukan kredensyal jangka panjang.

3. Tambahkan izin untuk memberikan akses ke identitas tersebut. Anda dapat memulai dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit.

   - Tambahkan set izin ke pengguna AWS IAM Identity Center (penerus AWS Single Sign-On).
   - Tambahkan kebijakan berbasis identitas ke peran IAM yang digunakan untuk beban kerja.
   - Tambahkan kebijakan berbasis identitas untuk pengguna IAM untuk kasus penggunaan yang memerlukan kredensyal jangka panjang.
   - Untuk informasi selengkapnya tentang pengguna IAM, lihat Praktik terbaik keamanan di IAM.

4. Simpan dan bagikan informasi tentangMasuk ke Konsol Manajemen AWS. Informasi ini bervariasi, tergantung pada jenis identitas yang Anda buat.
5. Perbarui alamat email pengguna root dan nomor telepon kontak akun utama Anda untuk memastikan bahwa Anda dapat menerima akun penting dan pemberitahuan terkait keamanan.

   - Ubah alamat email nama akun, atau kata sandi untuk Pengguna root akun AWS.
   - Akses atau perbarui kontak akun utama.

6. Tinjau praktik terbaik Keamanan di IAM untuk mempelajari tentang identitas tambahan dan praktik terbaik manajemen akses.
7. Menerapkan kontrol akses berbasis jaringan: Gunakan kebijakan Sign-in berbasis sumber daya atau kebijakan kontrol sumber daya (RCP) untuk membatasi login konsol ke permintaan dari rentang alamat IP atau VPC yang disetujui. Untuk lingkungan yang menggunakan Akses Pribadi Konsol, konfigurasikan kebijakan titik akhir VPC untuk mengontrol akun mana yang dapat diakses melalui titik akhir Anda (lihat Akses Pribadi Konsol). Bersama-sama, kebijakan Sign-in berbasis sumber daya, RCP, dan kebijakan titik akhir VPC menyediakan kontrol jaringan berlapis pada titik penegakan yang berbeda. Untuk pengguna root, Sign-in kebijakan memblokir halaman kredensyal sepenuhnya pada upaya akses dari jaringan yang tidak sah. AWS merekomendasikan mengonfigurasi prinsip yang dikecualikan untuk akses pemulihan guna mencegah penguncian akun, meskipun ini opsional. Lihat informasi yang lebih lengkap di Mengontrol akses konsol dengan kebijakan berbasis sumber daya dan kebijakan kontrol sumber daya.

Masuk ke Konsol Manajemen AWS

Ketika Anda masuk ke Konsol Manajemen AWS dari URL AWS masuk utama (https://console.aws.amazon.com/) Anda harus memilih jenis pengguna Anda, baik pengguna Root atau pengguna IAM. Jika Anda tidak yakin pengguna seperti apa Anda, lihatTentukan jenis pengguna Anda.

Pengguna root memiliki akses akun yang tidak terbatas dan dikaitkan dengan orang yang membuat akun. Akun AWS Pengguna root kemudian membuat jenis pengguna lain, seperti pengguna IAM dan pengguna di Pusat Identitas AWS IAM, dan memberi mereka kredensi akses.

Pengguna IAM adalah identitas di dalam Anda Akun AWS yang memiliki izin khusus khusus. Saat pengguna IAM masuk, mereka dapat menggunakan URL masuk yang menyertakan Akun AWS atau alias mereka, seperti `https://account_alias_or_id.signin.aws.amazon.com/console/` alih-alih URL AWS masuk utama. `https://console.aws.amazon.com/`

Anda dapat masuk hingga 5 identitas berbeda secara bersamaan dalam satu browser di file. Konsol Manajemen AWS Ini bisa berupa kombinasi pengguna root, pengguna IAM, atau peran federasi di akun yang berbeda atau di akun yang sama. Untuk detailnya, lihat Masuk ke beberapa akun di Panduan Konsol Manajemen AWS Memulai.

Tutorial

- Masuk ke Konsol Manajemen AWS sebagai pengguna root
- Masuk ke Konsol Manajemen AWS sebagai pengguna IAM

Jika Anda tidak yakin pengguna seperti apa Anda, lihatTentukan jenis pengguna Anda.

Tutorial

- Masuk ke Konsol Manajemen AWS sebagai pengguna root
- Masuk ke Konsol Manajemen AWS sebagai pengguna IAM

Masuk ke Konsol Manajemen AWS sebagai pengguna root

Saat pertama kali membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna

Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun.

> **Important**
>
> Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Untuk masuk sebagai pengguna root

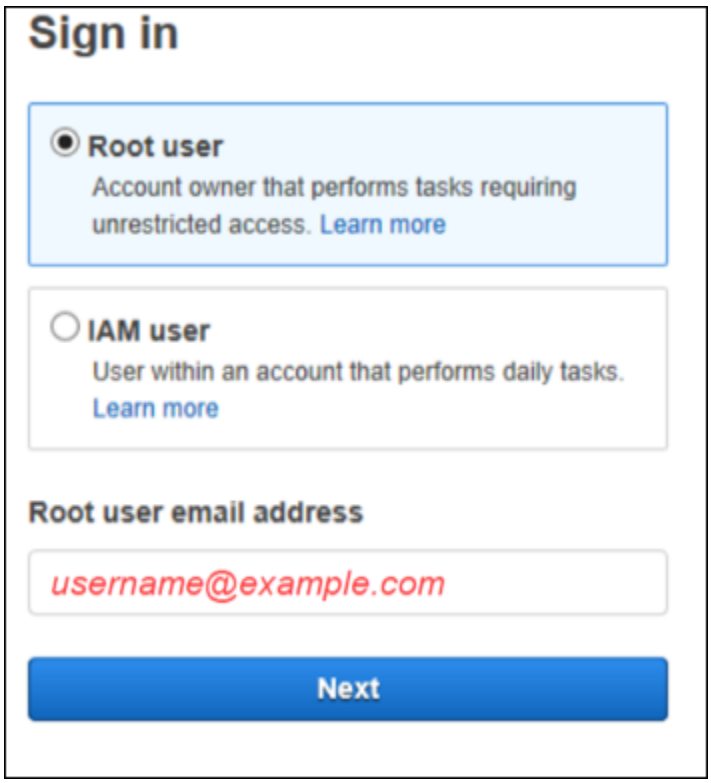
Anda dapat masuk sebagai pengguna root saat Anda sudah masuk ke identitas lain di file Konsol Manajemen AWS. Untuk detailnya, lihat Masuk ke beberapa akun di Panduan Konsol Manajemen AWS Memulai.

Akun AWS dikelola menggunakan AWS Organizations mungkin tidak memiliki kredensi pengguna root, dan Anda harus menghubungi administrator untuk melakukan tindakan pengguna root di akun anggota Anda. Jika Anda tidak dapat masuk sebagai pengguna root, lihatPemecahan Masalah Akun AWS masalah masuk.

1. Buka Konsol Manajemen AWS dihttps://console.aws.amazon.com/.

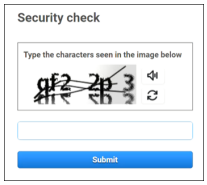
   > **Note**
   >
   > Jika Anda login sebelumnya sebagai pengguna IAM menggunakan browser ini, browser Anda mungkin menampilkan halaman login pengguna IAM sebagai gantinya. Pilih Masuk menggunakan email pengguna root.

2. Pilih pengguna Root.



3. Di bawah alamat email pengguna Root, masukkan alamat email yang terkait dengan pengguna root Anda. Kemudian, pilih Berikutnya.
4. Jika Anda diminta untuk menyelesaikan pemeriksaan keamanan, masukkan karakter yang disajikan kepada Anda untuk melanjutkan. Jika Anda tidak dapat menyelesaikan pemeriksaan keamanan, coba dengarkan audio atau segarkan pemeriksaan keamanan untuk set karakter baru.

> **Tip**
>
> Ketik karakter alfanumerik yang Anda lihat (atau dengar) secara berurutan tanpa spasi.



5. Masukkan kata sandi Anda.

6. Otentikasi dengan MFA. MFA diberlakukan secara default pada pengguna root. Untuk pengguna root akun mandiri dan anggota, Anda harus mengaktifkan MFA secara manual, yang sangat disarankan. Untuk informasi selengkapnya, lihat Autentikasi multi-faktor untuk pengguna Akun AWS root di Panduan AWS Identity and Access Management Pengguna.

> **Tip**
>
> Sebagai praktik keamanan terbaik, sebaiknya hapus semua kredensi pengguna root dari akun anggota di AWS organisasi Anda untuk membantu mencegah penggunaan yang tidak sah. Jika Anda memilih opsi ini, akun anggota tidak dapat masuk sebagai pengguna root, melakukan pemulihan kata sandi, atau mengatur MFA. Dalam hal ini, hanya administrator akun manajemen yang dapat melakukan tugas yang memerlukan kredensi pengguna root di akun anggota. Untuk detailnya, lihat Mengelola akses root untuk akun anggota secara terpusat di Panduan AWS Identity and Access Management Pengguna.

7. Pilih Masuk. Konsol Manajemen AWS Muncul.

Setelah otentikasi Konsol Manajemen AWS terbuka ke halaman Beranda Konsol.

Informasi tambahan

Jika Anda ingin informasi lebih lanjut tentang pengguna Akun AWS root, lihat sumber daya berikut.

- Untuk ikhtisar pengguna root, lihat pengguna Akun AWS root.
- Untuk detail tentang menggunakan pengguna root, lihat Menggunakan pengguna Akun AWS root.
- Untuk step-by-step petunjuk tentang cara mengatur ulang kata sandi pengguna root Anda, lihatSaya lupa kata sandi pengguna root saya untuk saya Akun AWS.

Masuk ke Konsol Manajemen AWS sebagai pengguna IAM

Pengguna IAM adalah identitas yang dibuat dalam sebuah Akun AWS yang memiliki izin untuk berinteraksi dengan AWS sumber daya. Pengguna IAM masuk menggunakan ID akun atau alias mereka, nama pengguna mereka, dan kata sandi. Nama pengguna IAM dikonfigurasi oleh administrator Anda. Nama pengguna IAM dapat berupa nama ramah, seperti*Zhang*, atau alamat email seperti*zhang@example.com*. Nama pengguna IAM tidak dapat menyertakan spasi, tetapi dapat menyertakan huruf besar dan kecil, angka, dan simbol`+ = , . @ _ -`.

> **Tip**
>
> Jika pengguna IAM Anda mengaktifkan otentikasi multi-faktor (MFA), Anda harus memiliki akses ke perangkat otentikasi. Untuk detailnya, lihat Menggunakan perangkat MFA dengan halaman masuk IAM Anda.

Untuk masuk sebagai pengguna IAM

Anda dapat masuk sebagai pengguna IAM saat Anda sudah masuk ke identitas lain di Konsol Manajemen AWS. Untuk detailnya, lihat Masuk ke beberapa akun di Panduan Konsol Manajemen AWS Memulai.

1. Buka Konsol Manajemen AWS dihttps://console.aws.amazon.com/.
2. Halaman masuk utama muncul. Masukkan ID akun (12 digit) atau alias, nama pengguna IAM Anda, dan kata sandi.

   > **Note**
   >
   > Anda mungkin tidak perlu memasukkan ID akun atau alias jika sebelumnya Anda telah masuk sebagai pengguna IAM dengan browser Anda saat ini atau jika Anda menggunakan URL masuk akun Anda.

3. Pilih Masuk.
4. Jika MFA diaktifkan untuk pengguna IAM Anda, AWS mengharuskan Anda untuk mengonfirmasi identitas Anda dengan autentikator. Untuk informasi selengkapnya, lihat Menggunakan otentikasi multi-faktor (MFA) di. AWS

Setelah otentikasi Konsol Manajemen AWS terbuka ke halaman Beranda Konsol.

Informasi tambahan

Jika Anda ingin informasi lebih lanjut tentang pengguna IAM, lihat sumber daya berikut.

- Untuk ikhtisar IAM, lihat Apa itu Identity and Access Management?
- Untuk detail tentang AWS akun IDs, lihat ID AWS akun Anda dan aliasnya.
- Untuk step-by-step petunjuk tentang cara mengatur ulang kata sandi pengguna IAM Anda, lihatSaya lupa kata sandi pengguna IAM saya untuk saya Akun AWS.

Mengontrol akses konsol dengan kebijakan berbasis sumber daya dan kebijakan kontrol sumber daya

> **Important**
>
> Akses masuk konsol diaktifkan secara default. AWS Sign-In memungkinkan akses konsol tidak terbatas pada awalnya. Untuk menambahkan batasan, aktifkan konfigurasi otorisasi konsol untuk akun atau organisasi Anda. Pernyataan izin sumber daya yang Anda buat tidak berpengaruh hingga Anda mengaktifkan otorisasi konsol. Lihat Memulai kontrol akses konsol menggunakan kebijakan sumber daya.

AWS Sign-In mendukung kebijakan berbasis sumber daya dan kebijakan kontrol sumber daya (RCP) untuk mengontrol akses ke. AWS Sign-In Gunakan kebijakan ini untuk memverifikasi identitas pengguna dan lokasi jaringan di seluruh Konsol Manajemen AWS akses — sebelum, selama, dan setelah otentikasi. Untuk pengguna root, kebijakan ini memvalidasi lokasi jaringan dan identitas pengguna sebelum pengumpulan kredensi dimulai. Kredensil hanya dapat dimasukkan ketika akses berasal dari jaringan yang diharapkan.

AWS Sign-In kebijakan berbasis sumber daya:

- Terapkan ke AWS akun individu.
- Biarkan administrator akun membatasi akses konsol berdasarkan parameter jaringan dan identitas utama.

Kebijakan kontrol sumber daya (RCP):

- Terapkan di seluruh organisasi melalui AWS Organizations.
- Menyediakan tata kelola terpusat di semua akun anggota.

Kedua jenis kebijakan memverifikasi akses sebelum autentikasi. Ini memblokir prinsipal untuk mengakses halaman masuk dari jaringan yang tidak terduga.

Kebijakan ini tidak menggantikan kebijakan berbasis identitas IAM, yang terus berlaku.

> **Note**
>
> Untuk dokumentasi lengkap tentang kebijakan kontrol sumber daya, termasuk konfigurasi dan manajemen tingkat organisasi, lihat Kebijakan kontrol sumber daya di Panduan Pengguna AWS Organizations. Bagian ini berfokus terutama pada kebijakan AWS Sign-In berbasis sumber daya.

AWS Sign-In Kebijakan dan RCP berbasis sumber daya berlaku untuk metode otentikasi berikut:

- Konsol Manajemen AWS— Masuk langsung menggunakan halaman login konsol.
- AWS IAM Identity Center — Masuk konsol menggunakan Pusat Identitas IAM.
- Penyedia identitas federasi — Sign-in melalui federasi SAMP atau OIDC.
- Aplikasi terintegrasi dengan AWS Sign-In — Amazon Connect, Amazon, Dasbor AWS Kesehatan QuickSight, Amazon AppStream, Amazon Lightsail, AWS IQ.

Kontrol ini tidak berlaku untuk akses terprogram menggunakan kunci akses (AWS SDK atau panggilan API yang ditandatangani dengan SigV4).

Bagaimana AWS Sign-In mengevaluasi kebijakan berbasis sumber daya

AWS Sign-In mengevaluasi kebijakan berbasis sumber daya atau kebijakan kontrol sumber daya (RCP) yang berlaku pada dua titik selama akses konsol: sebelum otentikasi (fase pra-otentikasi) dan setelah otentikasi berhasil (fase pasca-otentikasi). Setiap evaluasi memeriksa kunci kondisi yang ditentukan dalam kebijakan Anda. Kunci yang tersedia tergantung pada fase dan tindakan. Lihat perinciannya di Kunci kondisi yang didukung.

> **Note**
>
> Untuk login pengguna root, upaya akses dari jaringan tak terduga diblokir sebelum prompt kata sandi muncul. Ini mencegah pengiriman kredensil dari jaringan yang tidak terduga.

Setelah otentikasi, evaluasi juga mempertimbangkan kebijakan berbasis identitas kepala sekolah. Kebijakan IAM yang menolak tindakan masuk yang relevan dapat mencegah sesi konsol diberikan, bahkan ketika kondisi jaringan terpenuhi.

Tindakan yang didukung

AWS Sign-In kebijakan sumber daya (kebijakan berbasis sumber daya dan RCP) mendukung tindakan berikut:

`signin:Authenticate`

Ini adalah tindakan evaluasi saja (tidak dapat dipanggil) yang dinilai saat permintaan masuk diterima. Ini adalah pemeriksaan pra-otentikasi dan terjadi ketika prinsipal memasukkan kredensil pada halaman login (pengguna root, pengguna IAM) atau memulai login konsol menggunakan kredensil dari penyedia identitas atau AWS STS (pengguna federasi, peran).

Kunci kondisi yang didukung:`aws:SourceIp`,`aws:SourceVpc`,`aws:SourceVpce`,`aws:VpcSourceIp`,`aws:RequestedRe`

Principal-based kunci kondisi global (`aws:PrincipalArn`,`aws:PrincipalAccount`) tidak tersedia untuk tindakan ini karena identitas pengguna belum dikonfirmasi.

`signin:AuthorizeOAuth2Access`

Digunakan untuk pembuatan kode otorisasi OAuth. Setelah otentikasi berhasil, tindakan ini dipicu ketika sistem menghasilkan kode otorisasi OAuth. Pada titik ini, pengguna diautentikasi dan kunci kondisi berbasis prinsip tersedia.

Kunci kondisi yang didukung:`aws:SourceIp`,`aws:SourceVpc`,`aws:SourceVpce`,`aws:VpcSourceIp`,`aws:RequestedRe`

`signin:CreateOAuth2Token`

Tindakan pasca-otentikasi ini digunakan untuk pembuatan dan pertukaran token OAuth. Tindakan ini dipicu saat menukarkan kode otorisasi untuk token akses, menyegarkan token, atau melakukan operasi pertukaran token. Principal-based kunci kondisi tersedia selama fase ini.

Kunci kondisi yang didukung:`aws:SourceIp`,`aws:SourceVpc`,`aws:SourceVpce`,`aws:VpcSourceIp`,`aws:RequestedRe`

> **Important**
>
> Saat membuat AWS Sign-In kebijakan (kebijakan berbasis sumber daya atau RCP), tutupi ketiga tindakan di seluruh kebijakan Anda — `signin:Authenticate` dalam pernyataan pra-otentikasi, dan dalam pernyataan pasca-autentikasi. `signin:AuthorizeOAuth2Access` `signin:CreateOAuth2Token` Masuk konsol menggunakan OAuth 2.0, yang mengalir melalui ketiga tindakan secara berurutan. Jika kebijakan Anda menghilangkan tindakan, fase terkait tidak dilindungi. Untuk tindakan kebijakan titik akhir VPC termasuk, `signin:CreateAccount` lihat AWS Management Console Private Access.

Kunci kondisi yang didukung

AWS Sign-In mendukung kunci kondisi berikut dalam kebijakan berbasis sumber daya dan kebijakan kontrol sumber daya (RCP). Gunakan tombol ini untuk mengontrol akses konsol berdasarkan lokasi jaringan dan identitas utama:

- Network-based (semua tindakan):`aws:SourceIp`,`aws:SourceVpc`,`aws:SourceVpce`,`aws:VpcSourceIp`,`aws:RequestedRe`
- Identity-based (tindakan pasca-otentikasi):`aws:PrincipalArn`,. `aws:PrincipalAccount`
- Service-specific (hanya pra-otentikasi):. `signin:PrincipalArn`

Untuk aturan penggunaan terperinci, kompatibilitas operator, batasan kombinasi, dan matriks ketersediaan berdasarkan tindakan, lihatAWS Sign-In referensi kunci kondisi.

Memulai kontrol akses konsol menggunakan kebijakan sumber daya

Prasyarat

- AWS CLI diinstal dan dikonfigurasi.
- Izin IAM yang sesuai (lihatAWS kebijakan terkelola: AWSSignInResourcePolicyManagement).
- Perimeter jaringan yang teridentifikasi (rentang IP, VPC, atau titik akhir VPC).
- Prinsipal yang dikecualikan yang ditunjuk untuk mempertahankan akses (disarankan tetapi opsional).

- Jika jaringan Anda menggunakan pemfilteran jalan keluar, izinkan daftar titik akhir bidang AWS Sign-In kontrol (lihat). AWS Sign-In domain administrasi untuk daftar yang diizinkan

> **Important**
>
> Sebelum mengaktifkan otorisasi konsol dalam produksi, AWS rekomendasikan untuk mengonfigurasi setidaknya satu prinsipal yang dikecualikan untuk mempertahankan akses pemulihan darurat. Semua prinsipal, termasuk pengguna root, tunduk pada kebijakan kecuali secara eksplisit dikecualikan. Prinsipal yang dikecualikan bersifat opsional, tetapi menghilangkannya meningkatkan risiko penguncian akun jika kondisi jaringan berubah secara tak terduga.

Tentukan `--region us-east-1` untuk semua operasi penulisan pada AWS Sign-In kebijakan. AWS mereplikasi kebijakan secara global dari Wilayah ini. Operasi baca dapat menargetkan Wilayah mana pun.

Langkah 1: Buat pernyataan izin sumber daya

Buat pernyataan izin yang menentukan kontrol akses Anda. Semua operasi tulis memerlukan `--region us-east-1` (AWS Sign-In layanan hanya menerima perubahan kebijakan di Wilayah ini). Parameter yang tersisa (`--source-vpc--source-ip`,`--requested-region`,,`--excluded-principal`) menentukan kondisi dalam kebijakan Anda. Misalnya, `--requested-region us-west-2` menambahkan kondisi yang membatasi proses masuk ke titik akhir masuk regional us-west-2.

Contoh - Batasi akses ke VPC perusahaan:

```
aws signin put-resource-permission-statement \
  --source-vpc vpc-0abc123def456789 \
  --requested-region us-west-2 \
  --excluded-principal "arn:aws:iam::123456789012:user/EmergencyAdmin" \
  --client-token unique-request-id-12345 \
  --region us-east-1
```

Contoh - Batasi akses ke rentang IP tertentu:

```
aws signin put-resource-permission-statement \
```

```
  --source-ip "IP_ADDRESS" \
  --excluded-principal "arn:aws:iam::123456789012:role/BreakGlassRole" \
  --region us-east-1
```

> **Note**
>
> `--excluded-principal`Parameter menunjuk prinsipal yang dikecualikan yang melewati batasan jaringan, menjaga akses darurat jika kondisi jaringan berubah.

Langkah 2: Aktifkan konfigurasi otorisasi konsol

Langkah berikut mengaktifkan penegakan kebijakan untuk proses login konsol di akun atau organisasi Anda. Pernyataan izin sumber daya dapat dibuat kapan saja, tetapi tidak dievaluasi sampai otorisasi konsol diaktifkan.

> **Warning**
>
> Mengaktifkan otorisasi konsol dapat mengunci prinsipal jika kondisi jaringan Anda salah dikonfigurasi, atau jika kebijakan kontrol layanan (SCP) atau kebijakan kontrol sumber daya (RCP) yang ada menolak tindakan tersebut. AWS Sign-In Sebelum Anda mengaktifkan otorisasi konsol, konfirmasikan pernyataan izin Anda sudah benar, dan hapus atau sesuaikan SCP atau RCP yang menolak`signin:Authenticate`,, atau. `signin:AuthorizeOAuth2Access` `signin:CreateOAuth2Token`

Untuk akun mandiri:

```
aws signin put-console-authorization-configuration \
  --target-id <your-aws-account-id> \
  --region us-east-1
```

Untuk AWS Organizations:

```
aws signin put-console-authorization-configuration \
  --target-id <your-aws-organization-id> \
  --region us-east-1
```

Verifikasi konfigurasi:

```
aws signin get-console-authorization-configuration \
  --target-id <your-target-id> \
  --region <your-region>
```

Hapus konfigurasi otorisasi konsol:

```
aws signin delete-console-authorization-configuration \
  --target-id <your-target-id> \
  --region us-east-1
```

Langkah 3: Verifikasi kebijakan Anda

Daftar semua pernyataan izin:

```
aws signin list-resource-permission-statements \
  --max-results 50 \
  --region <your-region>
```

Ambil kebijakan konsolidasi lengkap:

```
aws signin get-resource-policy \
  --region <your-region>
```

`get-resource-policy`Perintah mengembalikan kebijakan berbasis sumber daya lengkap yang terdiri dari semua pernyataan izin Anda. Tinjau kebijakan ini untuk mengonfirmasi bahwa kebijakan tersebut mencerminkan kontrol akses yang Anda inginkan sebelum menguji akses konsol.

Ketersediaan wilayah

API otorisasi konsol tersedia di semua Wilayah AWS komersial. Anda dapat memanggil API ini dari Wilayah mana pun tempat Anda beroperasi.

> **Important**
>
> Operasi tulis (`put-console-authorization-configurationput-resource-permission-statement`,`delete-console-authorization-configuration`,,`delete-resource-permission-statement`) harus dilakukan di `us-east-1` Wilayah. Kebijakan yang dibuat secara `us-east-1` otomatis mereplikasi secara global. Operasi baca (`get-console-authorization-configuration`,`list-`

`resource-permission-statements`,`get-resource-policy`) dapat dilakukan dari Wilayah mana pun.

Memahami struktur kebijakan

AWS Sign-In kebijakan berisi dua pernyataan yang melindungi fase alur masuk konsol yang berbeda:

- Pre-authentication pernyataan (Tindakan:**`signin:Authenticate`**): Dievaluasi saat permintaan masuk diterima, sebelum otentikasi selesai. Kunci global tidak `aws:PrincipalArn` tersedia pada fase ini karena identitas kepala sekolah belum dikonfirmasi. Dalam fase ini `signin:PrincipalArn` tersedia untuk membebaskan prinsip-prinsip tertentu dari pembatasan jaringan. Network-based kunci kondisi tersedia untuk evaluasi dalam fase ini.
- Post-authentication pernyataan (Tindakan:**`signin:AuthorizeOAuth2Access`**,**`signin:CreateOAuth2Token`**): Dievaluasi setelah otentikasi, selama pertukaran token OAuth. Digunakan `aws:PrincipalArn` untuk membebaskan prinsipal tertentu. Semua kunci kondisi berbasis jaringan dan berbasis identitas tersedia untuk evaluasi dalam fase ini.

Kedua pernyataan diperlukan karena login konsol menggunakan OAuth 2.0, yang mengalir melalui ketiga tindakan secara berurutan. Kebijakan dengan hanya satu pernyataan membuat fase lainnya tidak terlindungi. `signin:PrincipalArn`mendukung pengguna root, pengguna IAM, dan tipe utama peran. `aws:PrincipalArn`mendukung semua tipe utama (pengguna root, pengguna IAM, pengguna federasi, peran).

Contoh kebijakan

Contoh 1: RCP dengan perimeter jaringan dan prinsipal yang dikecualikan

Kebijakan kontrol sumber daya (RCP) berikut menolak Konsol Manajemen AWS login dari luar jaringan perusahaan Anda di semua akun di organisasi Anda. Prinsipal yang dikecualikan yang ditunjuk dibebaskan untuk akses darurat. Karena ID VPC hanya unik di dalam Wilayah, kebijakan tersebut mencakup pernyataan ketiga yang menyematkan VPC-based akses ke Wilayah yang diharapkan.

`EnforceNetworkPerimeterPreAuth`Pernyataan tersebut digunakan `signin:PrincipalArn` untuk membebaskan prinsipal yang dikecualikan selama fase

pra-otentikasi. `EnforceNetworkPerimeterPostAuth`Pernyataan tersebut digunakan `aws:PrincipalArn` untuk membebaskan prinsipal yang dikecualikan setelah otentikasi. `EnforceSourceVPCRegion`Pernyataan tersebut memastikan Wilayah permintaan cocok dengan Wilayah VPC, membatasi akses ke Wilayah yang diharapkan untuk VPC yang ditentukan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceNetworkPerimeterPreAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["signin:Authenticate"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "signin:PrincipalArn": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::444455556666:root",
            "arn:aws:iam::777788889999:user/EmergencyUser",
            "arn:aws:iam::777788889999:role/OrgBreakGlassRole"
          ]
        },
        "NotIpAddressIfExists": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringNotEquals": {
          "aws:SourceVpc": "<my-vpc>"
        }
      }
    },
    {
      "Sid": "EnforceNetworkPerimeterPostAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["signin:CreateOAuth2Token", "signin:AuthorizeOAuth2Access"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "aws:PrincipalArn": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::444455556666:root",
            "arn:aws:iam::777788889999:user/EmergencyUser",
```

```
            "arn:aws:iam::777788889999:role/OrgBreakGlassRole"
          ]
        },
        "NotIpAddressIfExists": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringNotEquals": {
          "aws:SourceVpc": "<my-vpc>"
        }
      }
    },
    {
      "Sid": "EnforceSourceVPCRegion",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "signin:Authenticate",
        "signin:CreateOAuth2Token",
        "signin:AuthorizeOAuth2Access"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceVpc": "<my-vpc>"
        },
        "StringNotEqualsIfExists": {
          "aws:RequestedRegion": "<my-vpc-region>"
        }
      }
    }
  ]
}
```

Kebijakan ini:

- Menolak akses ke halaman masuk kecuali permintaan tersebut berasal dari rentang IP perusahaan atau VPC perusahaan. Akun root yang dikecualikan dan pengguna IAM dikecualikan melalui `signin:PrincipalArn` (pra-otentikasi).
- Menolak pertukaran token OAuth kecuali dari rentang IP perusahaan atau VPC. Akun root yang dikecualikan, pengguna IAM, dan peran dikecualikan melalui `aws:PrincipalArn` (kunci global pasca-otentikasi).

- Jika permintaan berasal dari VPC yang ditentukan tetapi Wilayah tidak cocok, akses ditolak. AWS ID VPC unik dalam suatu Wilayah, dan ID VPC yang sama dapat ada di Wilayah yang berbeda.
- Berlaku secara global di seluruh AWS Organization Anda saat dikonfigurasi sebagai RCP.

Contoh 2: Resource-based kebijakan untuk IP-based akses dengan prinsipal yang dikecualikan

Kebijakan berbasis sumber daya berikut menolak akses konsol ke semua prinsipal yang membuat permintaan dari luar rentang IP yang ditentukan, dengan prinsipal yang dikecualikan dikecualikan. Kebijakan ini berisi dua pernyataan: pernyataan pra-otentikasi yang menggunakan `signin:PrincipalArn` kunci khusus layanan, dan pernyataan pasca-otentikasi yang menggunakan kunci global. `aws:PrincipalArn`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:Authenticate"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "signin:PrincipalArn": "<excluded-principal-arn>"
        },
        "NotIpAddress": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringEquals": {
          "aws:ResourceAccount": "<my-aws-account-id>"
        }
      }
    },
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:CreateOAuth2Token", "signin:AuthorizeOAuth2Access"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
```

```
          "aws:PrincipalArn": "<excluded-principal-arn>"
        },
        "NotIpAddress": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringEquals": {
          "aws:ResourceAccount": "<my-aws-account-id>"
        }
      }
    }
  ]
}
```

Kebijakan ini:

- Menolak akses ke semua prinsipal kecuali mereka terhubung dari rentang IP. `<my-corporate-cidr>`
- Mengecualikan prinsipal yang dikecualikan dari pembatasan jaringan menggunakan `signin:PrincipalArn` (pra-otentikasi) dan `aws:PrincipalArn` (pasca-otentikasi).
- Hanya berlaku untuk akun tertentu di mana kebijakan berbasis sumber daya dikonfigurasi (diidentifikasi oleh). `<my-aws-account-id>`

Praktik terbaik

Konfigurasikan prinsip yang dikecualikan untuk akses pemulihan darurat

AWS merekomendasikan untuk mengonfigurasi setidaknya satu pengguna yang dikecualikan sebelum menerapkan kebijakan otorisasi konsol dalam produksi. Pada tahap pra-otentikasi, kunci `signin:PrincipalArn` kondisi mengecualikan pengguna root, pengguna IAM, dan prinsip peran. Pada tahap pasca-otentikasi, kunci `aws:PrincipalArn` kondisi mengecualikan semua jenis utama (pengguna root, pengguna IAM, pengguna federasi, peran).

Prinsipal yang dikecualikan bersifat opsional, tetapi menghilangkannya meningkatkan risiko penguncian akun jika kondisi jaringan berubah secara tidak terduga atau jika kebijakan salah dikonfigurasi.

Direkomendasikan langkah-langkah konfigurasi utama yang dikecualikan:

1. Buat peran IAM yang dikecualikan (misalnya,`BreakGlassRole`).

2. Untuk peran yang dikecualikan, mewajibkan MFA dalam kebijakan kepercayaan peran.
3. Berikan identitas yang dikecualikan hanya izin minimum yang diperlukan untuk pemulihan darurat.
4. Sertakan ARN utama yang dikecualikan dalam pernyataan kebijakan pra-otentikasi (`signin:PrincipalArn`) dan pasca-otentikasi (). `aws:PrincipalArn`
5. Dokumentasikan prosedur pemulihan dan simpan dengan aman di luar AWS.
6. Uji akses utama yang dikecualikan secara berkala untuk mengonfirmasi bahwa itu berfungsi bila diperlukan.

Pertahankan jalur akses pemulihan

Selain prinsip yang dikecualikan yang dijelaskan di atas, pastikan metode akses alternatif tersedia jika kebijakan otorisasi konsol memblokir proses masuk secara tidak terduga:

- Role-based akses terprogram: Kebijakan otorisasi konsol hanya berlaku untuk login konsol interaktif. Mereka tidak berlaku untuk permintaan API yang ditandatangani dengan SiGv4. Jika Anda memiliki akses terprogram (misalnya, kunci akses yang ada, peran lintas akun), gunakan untuk memanggil `signin:DeleteConsoleAuthorizationConfiguration` dan menghapus kebijakan pembatasan. Kredensi harus menyertakan `signin:DeleteConsoleAuthorizationConfiguration` izin (termasuk dalam kebijakan `AWSSignInResourcePolicyManagement` terkelola). AWS merekomendasikan kredensi sementara atas kunci akses pengguna IAM jangka panjang. Untuk akun anggota, administrator akun manajemen dapat berasumsi `OrganizationAccountAccessRole` di akun anggota (`aws sts assume-role`) untuk mendapatkan kredensi sementara ini.
- AWS pemulihan dukungan: Jaga agar email akun pengguna root dan nomor telepon Anda tetap terkini. Jika akses prinsipal dan program yang dikecualikan tidak tersedia, AWS Support dapat menyediakan tautan portal pemulihan setelah verifikasi identitas. Lihat Saya terkunci dari akun saya setelah mengaktifkan otorisasi konsol untuk proses pemulihan penuh.

Uji sebelum penyebaran produksi

AWS merekomendasikan agar Anda tidak melampirkan RCP yang membatasi ke akar organisasi Anda tanpa menguji secara menyeluruh dampak kebijakan terhadap akun. Sebagai gantinya, buat OU yang dapat Anda pindahkan akun Anda menjadi satu per satu, atau setidaknya dalam jumlah

kecil, untuk memastikan bahwa Anda tidak secara tidak sengaja mengunci pengguna dari akun utama.

Menguji alur kerja:

1. Buat pernyataan izin tunggal dengan batasan jaringan utama Anda.
2. Aktifkan otorisasi konsol di akun non-produksi.
3. Uji akses konsol dari jaringan yang diizinkan dan ditolak.
4. Tinjau CloudTrail log Amazon untuk mengonfirmasi perilaku evaluasi kebijakan.
5. Uji akses menggunakan prinsipal Anda yang dikecualikan.
6. Secara bertahap memperluas ke jaringan dan akun tambahan.
7. Pantau sebelum ditegakkan di akun produksi.

Desain dengan defense-in-depth

Gunakan kebijakan AWS Sign-In berbasis sumber daya dan kebijakan kontrol sumber daya sebagai satu lapisan dalam strategi keamanan yang lebih luas. AWS Sign-In kebijakan membatasi akses konsol berdasarkan lokasi jaringan dan identitas utama. Gabungkan mereka dengan jenis kebijakan lain untuk membuat kontrol akses yang komprehensif:

- AWS Sign-In kebijakan (kebijakan berbasis sumber daya dan RCP): Membatasi akses konsol berdasarkan lokasi jaringan dan identitas utama sebelum, selama, dan setelah otentikasi.
- Kebijakan IAM: Kontrol tindakan apa yang dapat dilakukan pengguna setelah masuk.
- Kebijakan kontrol layanan (SCP): Menerapkan pagar pembatas izin di seluruh organisasi di semua kepala sekolah.
- Kebijakan titik akhir VPC: Kontrol layanan dan akun mana yang dapat diakses melalui titik akhir VPC.

Memantau dan mengaudit secara terus menerus

AWS CloudTrail secara otomatis mencatat semua evaluasi AWS Sign-In kebijakan dan perubahan konfigurasi. Lihat peristiwa ini di Riwayat CloudTrail acara hingga 90 hari. Untuk retensi yang lebih lama, kirimkan peristiwa ke Amazon S3 dengan membuat jejak (lihat Membuat jejak). Untuk peringatan waktu nyata, buat EventBridge aturan Amazon yang cocok dengan AWS Sign-In

peristiwa, konfigurasikan jejak Anda untuk dikirimkan ke grup CloudWatch log Log untuk alarm berbasis filter metrik, atau teruskan peristiwa ke solusi SIEM yang ada.

Kasus penggunaan

Penegakan perimeter jaringan

Batasi akses konsol ke VPC perusahaan atau rentang IP yang disetujui. Gunakan kebijakan berbasis sumber daya untuk akun individu atau kebijakan kontrol sumber daya (RCP) untuk penegakan hukum di seluruh organisasi guna memastikan bahwa pengguna hanya dapat masuk dari lokasi jaringan tepercaya, mencegah akses tidak sah dari jaringan publik atau tidak tepercaya.

Contoh skenario: Sebuah perusahaan membutuhkan semua akses konsol untuk berasal dari jaringan perusahaan mereka atau AWS VPC yang disetujui. Mereka mengonfigurasi kebijakan berbasis sumber daya untuk satu akun, atau RCP di seluruh organisasi mereka, yang menolak akses dari semua jaringan lain sambil mempertahankan akses pemulihan darurat untuk administrator darurat.

Persyaratan kepatuhan

Memenuhi persyaratan peraturan untuk kontrol akses berbasis jaringan. Banyak kerangka kerja kepatuhan mengharuskan organisasi untuk membatasi akses ke sistem sensitif berdasarkan lokasi jaringan. AWS Sign-In kebijakan menyediakan kontrol yang dapat diaudit dan dapat ditegakkan yang menunjukkan kepatuhan terhadap persyaratan ini.

Contoh skenario: Perusahaan jasa keuangan harus mematuhi peraturan yang mewajibkan akses konsol hanya dari jaringan yang disetujui. Mereka menggunakan RCP untuk menegakkan pembatasan jaringan di seluruh organisasi dan memelihara AWS CloudTrail log sebagai bukti kepatuhan.

Multi-account tata kelola

Menerapkan kebijakan akses konsol yang konsisten di seluruh AWS Organizations. Gunakan RCP untuk memberlakukan pembatasan jaringan standar di semua akun anggota, memastikan postur keamanan yang konsisten tanpa memerlukan konfigurasi tingkat akun individual.

Contoh skenario: Perusahaan dengan 100+ AWS akun menggunakan RCP untuk menerapkan kebijakan yang mengharuskan semua akses konsol berasal dari titik akhir VPC dalam organisasinya, mengonfirmasi kontrol jaringan yang konsisten di semua akun.

Third-party kontrol akses

Berikan akses konsol sementara ke mitra atau kontraktor dari jaringan tertentu. Organizations dapat membuat akses konsol terbatas waktu dan dibatasi jaringan untuk pihak eksternal tanpa mengorbankan postur keamanan secara keseluruhan.

Contoh skenario: Perusahaan perlu memberikan akses konsol sementara perusahaan konsultan. Mereka membuat kebijakan berbasis sumber daya yang memungkinkan akses hanya dari rentang IP perusahaan konsultan yang diketahui dan hanya untuk peran IAM yang ditugaskan ke konsultan.

Batasi akses konsol ke prinsipal tertentu

Izinkan hanya satu set prinsip yang ditentukan untuk masuk ke Konsol Manajemen AWS, dan tolak semua yang lain, terlepas dari lokasi jaringan. Ini berguna bagi pelanggan yang tidak menggunakan titik akhir VPC dan menginginkan pembatasan konsol berbasis identitas. Prinsipal yang ditolak masuk konsol mempertahankan akses programatiknya; AWS Sign-In kebijakan hanya masuk ke konsol, dan hanya prinsipal yang Anda kecualikan yang dapat masuk.

Contoh skenario: Perusahaan hanya ingin administratornya menggunakan konsol. Mereka mengonfigurasi RCP yang menolak masuk konsol untuk semua prinsipal kecuali ARN utama administrator. Peran instans Amazon EC2 dengan kredensi yang valid tidak dapat masuk ke konsol, karena ini bukan prinsipal yang dikecualikan, meskipun tetap mempertahankan izin terprogramnya. Ini membahas kasus umum kredensil peran instance yang digunakan untuk login konsol.

Memecahkan masalah kontrol akses konsol

Saya tidak dapat masuk karena kondisi jaringan dalam kebijakan berbasis Sign-in sumber daya

Anda mungkin melihat salah satu pesan galat berikut ketika akses ditolak oleh AWS Sign-In kebijakan:

- “Informasi otentikasi Anda salah. Silakan coba lagi.” (penolakan pra-otentikasi berdasarkan kebijakan berbasis sumber daya)
- “Otentikasi gagal Permintaan tidak valid” (penolakan pra-otentikasi oleh RCP)
- “Otentikasi gagal: Untuk mengakses akun ini, masuk dari jaringan lain, atau hubungi administrator Anda untuk informasi lebih lanjut” (penolakan pasca-autentikasi)

Jika Anda melihat salah satu kesalahan ini dan yakin akses Anda harus diizinkan, hubungi AWS administrator Anda. Mereka dapat meninjau CloudTrail log untuk `ConsoleLogin` peristiwa dengan `errorMessage` “Otorisasi ditolak karena kebijakan berbasis sumber daya” atau “Otorisasi ditolak karena kebijakan kontrol sumber daya” untuk mengidentifikasi pernyataan kebijakan mana yang ditolak aksesnya.

Kemungkinan penyebabnya:

- Alamat IP sumber Anda tidak dalam kisaran CIDR yang diizinkan.
- Anda tidak terhubung ke titik akhir VPC atau VPC yang diperlukan.
- Anda mengakses titik akhir masuk regional yang tidak sesuai dengan Wilayah yang diharapkan dalam kebijakan.
- ARN utama Anda tidak tercantum dengan benar dalam prinsipal yang dikecualikan kebijakan.
- Kebijakan ini baru-baru ini diperbarui, dan perubahan tersebut belum direplikasi secara global.

Resolusi:

- Pastikan Anda terhubung ke jaringan perusahaan atau VPN Anda.
- Konfirmasikan bahwa Anda mengakses melalui titik akhir VPC yang benar jika pembatasan berbasis titik akhir VPC dikonfigurasi.
- Hubungi AWS administrator Anda untuk memverifikasi konfigurasi kebijakan dan mengonfirmasi jaringan mana yang diotorisasi.
- Jika Anda dikonfigurasi sebagai prinsipal yang dikecualikan, verifikasi bahwa ARN utama Anda dikonfigurasi dengan benar dalam daftar prinsipal yang dikecualikan.
- Jika perubahan kebijakan baru-baru ini dibuat, tunggu beberapa menit hingga replikasi global selesai.

Untuk administrator yang mendiagnosis masalah ini:

- Tinjau AWS CloudTrail log untuk peristiwa evaluasi kebijakan guna mengidentifikasi pernyataan kebijakan mana yang ditolak aksesnya.
- Gunakan `aws signin get-resource-policy` untuk meninjau konfigurasi kebijakan saat ini.
- Pastikan lokasi jaringan pengguna cocok dengan kondisi dalam kebijakan.
- Konfirmasikan bahwa prinsipal yang dikecualikan dikonfigurasi dengan benar jika pengguna harus dibebaskan dari pembatasan jaringan.

Saya terkunci dari akun saya setelah mengaktifkan otorisasi konsol

Jika Anda mengonfigurasi otorisasi konsol dan tidak dapat lagi mengakses akun Anda, Anda mungkin belum mengonfigurasi prinsip yang dikecualikan sebelum menerapkan kebijakan.

Ada beberapa jalur untuk mendapatkan kembali akses, tergantung pada jenis akun Anda dan kredensi yang tersedia.

Opsi 1: Gunakan akses terprogram (AWS CLI atau SDK)

Kebijakan otorisasi konsol hanya berlaku untuk login konsol interaktif. Mereka tidak berlaku untuk permintaan API yang ditandatangani dengan SiGv4. Jika Anda memiliki akses terprogram (misalnya, kunci akses yang ada, peran lintas akun), gunakan untuk memanggil `signin:DeleteConsoleAuthorizationConfiguration` dan menghapus kebijakan pembatasan. Kredensi yang Anda gunakan harus memiliki izin untuk menelepon. `signin:DeleteConsoleAuthorizationConfiguration` Kebijakan `AWSSignInResourcePolicyManagement` terkelola mencakup izin ini. AWS merekomendasikan kredensi sementara atas kunci akses pengguna IAM jangka panjang. Untuk akun anggota, administrator akun manajemen dapat berasumsi `OrganizationAccountAccessRole` di akun anggota untuk mendapatkan kredensi sementara. Peran ini tidak secara otomatis dibuat di akun yang diundang untuk bergabung dengan organisasi.

```
aws signin delete-console-authorization-configuration \
  --target-id <your-aws-account-id> \
  --region us-east-1
```

Atau hapus pernyataan izin tertentu:

```
# First, list statements to get the statement ID
aws signin list-resource-permission-statements \
  --region us-east-1

# Then delete the problematic statement
aws signin delete-resource-permission-statement \
  --statement-id <statement-id> \
  --region us-east-1
```

Opsi 2: Hubungi AWS Support

Jika Anda tidak memiliki akses terprogram dan tidak dapat menggunakan akses akun `OrganizationAccountAccessRole` for, hubungi AWS Support untuk memulai proses pemulihan lockout.

Proses pemulihan bekerja sebagai berikut:

1. Jika Anda tidak dapat menyelesaikan masalah menggunakan opsi di atas, buka kasus dukungan di Pusat AWS Dukungan. AWS Support akan memverifikasi identitas Anda sebelum memeriksa akun Anda. Metode verifikasi mungkin termasuk mengonfirmasi alamat email akun pengguna root, menanggapi panggilan verifikasi telepon, atau menjawab pertanyaan keamanan akun.
2. AWS Support mengonfirmasi bahwa masalah akses konsol disebabkan oleh penguncian kebijakan berbasis sumber daya.
3. AWS Support membagikan tautan portal pemulihan. Gunakan tautan ini untuk masuk dengan prinsipal IAM di akun yang memiliki `signin:DeleteConsoleAuthorizationConfiguration` izin. Izin ini memungkinkan kepala sekolah untuk menghapus konfigurasi otorisasi konsol yang menyebabkan penguncian.

> **Important**
>
> Portal pemulihan menghapus seluruh konfigurasi otorisasi konsol untuk akun, termasuk semua pernyataan izin sumber daya. Portal pemulihan tidak mengizinkan konfigurasi ulang kebijakan berbasis AWS Sign-In sumber daya.

Tautan portal pemulihan kedaluwarsa 72 jam setelah AWS Support membagikannya. Jika Anda tidak menyelesaikan pemulihan dalam jendela itu, hubungi AWS Support untuk memulai kembali proses.

Setelah mendapatkan kembali akses:

- Tinjau dan perbarui pernyataan izin sumber daya Anda untuk menyertakan prinsipal yang dikecualikan yang dikonfigurasi dengan benar.
- Uji akses konsol dari jaringan yang diharapkan sebelum mengaktifkan kembali otorisasi konsol.
- Dokumentasikan prosedur pemulihan Anda untuk referensi future.

Perubahan yang saya buat tidak selalu langsung terlihat

Perubahan kebijakan mereplikasi secara global, tetapi replikasi mungkin memakan waktu beberapa menit.

Resolusi:

- Tunggu beberapa menit setelah membuat perubahan kebijakan agar replikasi global selesai.
- Verifikasi perubahan Anda menggunakan `get-resource-policy` perintah:

```
aws signin get-resource-policy --region <your-region>
```

- Periksa AWS CloudTrail log untuk peristiwa evaluasi kebijakan untuk mengonfirmasi kebijakan baru sedang dievaluasi.
- Konfirmasikan bahwa Anda menggunakan Wilayah yang benar untuk operasi Anda (operasi tulis harus digunakan`us-east-1`).
- Jika menggunakan kondisi berbasis titik akhir VPC, verifikasi bahwa kebijakan titik akhir VPC juga dikonfigurasi dengan benar.

Masalah replikasi kebijakan umum:

- Halaman masuk yang di-cache: Browser dapat menyimpan halaman masuk ke cache. Kosongkan cache browser Anda atau gunakan jendela penyamaran untuk menguji perubahan kebijakan.
- Pernyataan yang bertentangan: Jika Anda memiliki beberapa pernyataan izin, konfirmasikan bahwa pernyataan tersebut tidak bertentangan satu sama lain. Gunakan `get-resource-policy` untuk meninjau kebijakan konsolidasi.
- Kebijakan titik akhir VPC: kebijakan bekerja bersama dengan AWS Sign-In kebijakan titik akhir VPC. Keduanya harus memungkinkan akses yang diinginkan.

AWS Sign-In referensi kunci kondisi

Halaman ini mencantumkan kunci kondisi yang dapat Anda gunakan dalam kebijakan AWS Sign-In berbasis sumber daya dan kebijakan kontrol sumber daya (RCP), dan menunjukkan fase evaluasi dan tindakan yang diterapkan setiap kunci. Hanya `signin:PrincipalArn` khusus untuk AWS Sign-In; yang lain adalah kunci kondisi AWS global. Untuk definisi kunci global, lihat kunci konteks kondisi AWS global.

Untuk daftar lengkap tindakan dan kunci kondisi dalam Referensi Otorisasi Layanan, lihat Tindakan, sumber daya, dan kunci kondisi untuk AWS Sign-In.

Network-based kunci kondisi

Kunci kondisi ini memeriksa dari mana permintaan berasal. AWS Sign-In mengevaluasi mereka untuk semua AWS Sign-In tindakan (`signin:Authenticate`,`signin:Authorize0Auth2Access`, dan`signin:Create0Auth2Token`) dalam kebijakan berbasis sumber daya dan RCP.

Network-based kunci kondisi

Kunci syarat	Operator	Deskripsi	Aturan penggunaan
`aws:SourceIp`	`IpAddress` , `NotIpAddress`	Alamat IP publik atau rentang CIDR	Tidak ada saat permintaan menggunakan titik akhir VPC. Gunakan `IfExists` operator saat menggabungkan dengan VPC-based kondisi dalam pernyataan yang sama.
`aws:SourceVpc`	`StringEquals` , `StringNotEquals`	ID VPC () `vpc-xxxxxxxx`	Hanya hadir saat permintaan menggunakan titik akhir VPC. Gunakan dengan `aws:RequestedRegion` untuk mencegah tabrakan ID VPC lintas wilayah.

Kunci syarat	Operator	Deskripsi	Aturan penggunaan
`aws:SourceVpce`	`StringEquals`, `StringNotEquals`	ID titik akhir VPC () `vpce-xxxxxxxx`	Hanya hadir saat permintaan menggunakan titik akhir VPC.
`aws:VpcSourceIp`	`IpAddress`, `NotIpAddress`	IP pribadi dalam VPC	Selalu gunakan tombol `aws:VpcSourceIp` kondisi dengan tombol `aws:SourceVpc` atau `aws:SourceVpce` kondisi.
`aws:RequestedRegion`	`StringEquals`, `StringNotEquals`	Kode AWS Wilayah Target	Direkomendasikan saat menggunakan `aws:SourceVpc` untuk mencegah tabrakan ID VPC lintas wilayah. Beberapa Wilayah dapat ditentukan.

> **Important**
>
> Satu permintaan berisi `aws:SourceIp` (jaringan publik) atau `aws:SourceVpc` (titik akhir VPC), bukan keduanya. Saat menulis penolakan kecuali kebijakan yang mencakup kedua jalur, gunakan `IfExists` operator (misalnya,`NotIpAddressIfExists`) atau buat pernyataan terpisah.

Identity-based kunci kondisi

Kunci kondisi ini memeriksa siapa yang membuat permintaan. Mereka hanya tersedia untuk tindakan pasca-otentikasi (`signin:AuthorizeOAuth2Accessdansignin:CreateOAuth2Token`), di mana identitas utama telah ditetapkan.

Identity-based kunci kondisi

Kunci syarat	Operator	Deskripsi	Contoh
`aws:PrincipalArn`	`ArnEquals` , `ArnLike`, `ArnNotEquals` , `StringEquals` , `StringLike`	ARN dari prinsipal IAM yang diautentikasi	`arn:aws:iam::123456789012:user/alice` , `arn:aws:iam::123456789012:role/Admin`
`aws:PrincipalAccount`	`StringEquals` , `StringNotEquals`	AWS ID akun kepala sekolah	`123456789012`

Service-specific kunci kondisi: masuk: PrincipalArn

Kunci kondisi berikut khusus untuk AWS Sign-In dan bukan AWS kunci global. Ini hanya tersedia selama evaluasi pra-otentikasi. Gunakan `signin:PrincipalArn` untuk mengidentifikasi prinsipal yang memulai proses masuk sebelum otentikasi selesai. Ini adalah pra-otentikasi yang setara dengan`aws:PrincipalArn`, yang tidak tersedia sampai setelah otentikasi.

Operator

Operator ARN (`ArnEquals`,, `ArnLikeArnNotEquals`,`ArnNotLike`) dan operator string (`StringEquals`,`StringLike`).

Ketersediaan

AWS Sign-In menyertakan kunci ini dalam konteks permintaan selama fase pra-otentikasi (`signin:Authenticate`tindakan). Ini tidak tersedia untuk tindakan pasca-otentikasi (`signin:AuthorizeOAuth2Access`dan`signin:CreateOAuth2Token`).

Jenis data

ARN. Gunakan operator ARN daripada operator string.

Tipe nilai

Single-valued.

Didukung di

Resource-based kebijakan dan RCP.

Gunakan operator ARN untuk membandingkan nilai. Anda dapat menentukan jenis utama berikut:

- Akun AWS pengguna root (`arn:aws:iam::123456789012:root`)
- Pengguna IAM () `arn:aws:iam::123456789012:user/user-name`
- Peran IAM () `arn:aws:iam::123456789012:role/role-name`

Kasus penggunaan: Mengecualikan identitas utama yang dikecualikan dari pembatasan jaringan, mencegah penguncian sambil tetap menerapkan kontrol jaringan untuk semua upaya akses lainnya.

Contoh — Tolak akses pra-otentikasi dari jaringan yang tidak sah, kecuali untuk pengguna root:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:Authenticate"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "signin:PrincipalArn": "arn:aws:iam::123456789012:root"
        },
        "NotIpAddress": {
          "aws:SourceIp": "203.0.113.0/24"
        },
        "StringEquals": {
          "aws:ResourceAccount": "123456789012"
        }
      }
    },
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:CreateOAuth2Token", "signin:AuthorizeOAuth2Access"],
      "Resource": "*",
      "Condition": {
```

```
        "ArnNotEquals": {
          "aws:PrincipalArn": "arn:aws:iam::123456789012:root"
        },
        "NotIpAddress": {
          "aws:SourceIp": "203.0.113.0/24"
        },
        "StringEquals": {
          "aws:ResourceAccount": "123456789012"
        }
      }
    }
  ]
}
```

Kebijakan ini menolak akses konsol dari luar rentang `203.0.113.0/24` IP, kecuali untuk pengguna root akun. Pernyataan pra-otentikasi digunakan `signin:PrincipalArn` untuk membebaskan pengguna root sebelum otentikasi selesai. Pernyataan pasca-otentikasi digunakan `aws:PrincipalArn` untuk mengecualikan prinsip yang sama setelah otentikasi, selama pertukaran token OAuth. Lihat Contoh kebijakan.

Kondisi ketersediaan kunci berdasarkan tindakan

Kondisi ketersediaan kunci berdasarkan tindakan

Kunci syarat	Signin:Otentikasi	masuk: Authorize OAuth2Access	masuk: CreateOAuth2Token
`aws:SourceIp`	Ya	Ya	Ya
`aws:SourceVpc`	Ya	Ya	Ya
`aws:SourceVpce`	Ya	Ya	Ya
`aws:VpcSourceIp`	Ya	Ya	Ya
`aws:RequestedRegion`	Ya	Ya	Ya
`aws:PrincipalArn`	–	Ya	Ya

Kunci syarat	Signin:Otentikasi	masuk: Authorize OAuth2Access	masuk: CreateOAuth2Token
`aws:PrincipalAccount`	–	Ya	Ya
`signin:PrincipalArn`	Ya	–	–

> **Note**
>
> `signin:CreateAccount`Tindakan ini digunakan secara eksklusif dalam kebijakan titik akhir VPC untuk Akses Pribadi Konsol dan tidak tersedia untuk kebijakan atau RCP berbasis sumber daya. Tidak ada kunci kondisi khusus layanan yang terkait dengannya. Lihat Akses Pribadi Konsol.

Informasi Terkait

- Mengontrol akses konsol dengan kebijakan berbasis sumber daya dan kebijakan kontrol sumber daya
- Konsol Manajemen AWS Akses Pribadi
- AWS kunci konteks kondisi global
- Tindakan, sumber daya, dan kunci kondisi untuk AWS Sign-In

Masuk ke AWS portal akses

Seorang pengguna di IAM Identity Center adalah anggota dari. AWS Organizations Pengguna di Pusat Identitas IAM dapat mengakses beberapa Akun AWS aplikasi bisnis dengan masuk ke portal AWS akses Anda dengan URL masuk tertentu. Untuk informasi selengkapnya tentang URL login tertentu, lihatAWS portal akses.

Sebelum Anda masuk Akun AWS sebagai pengguna di Pusat Identitas IAM, kumpulkan informasi yang diperlukan berikut ini.

- Nama pengguna perusahaan
- Kata sandi perusahaan
- URL masuk khusus

> **Note**
>
> Setelah Anda masuk, sesi portal AWS akses Anda berlaku selama 8 jam. Anda diminta untuk masuk lagi setelah 8 jam.

Untuk masuk ke AWS portal akses

1. Di jendela browser Anda, tempelkan URL login yang diberikan melalui email, seperti `https://your_subdomain.awsapps.com/start` atau format URL dual-stack. `https://[IAM Identity Center instance ID].portal.[Region].app.aws` Kemudian, tekan Enter.
2. Masuk menggunakan kredensi perusahaan Anda (seperti nama pengguna dan kata sandi).

   > **Note**
   >
   > Jika administrator Anda mengirimi Anda email kata sandi satu kali (OTP) dan ini adalah pertama kalinya Anda masuk, masukkan kata sandi itu. Setelah masuk, Anda harus membuat kata sandi baru untuk login di masa mendatang.

3. Jika Anda diminta untuk kode verifikasi, periksa email Anda untuk itu. Kemudian salin dan tempel kode ke halaman masuk.

> **Note**
>
> Kode verifikasi biasanya dikirim melalui email, tetapi metode pengirimannya mungkin berbeda. Jika belum menerimanya di email Anda, tanyakan kepada administrator Anda untuk detail tentang kode verifikasi Anda.

4. Jika MFA diaktifkan untuk pengguna Anda di Pusat Identitas IAM, Anda kemudian mengautentikasi menggunakannya.
5. Setelah otentikasi, Anda dapat mengakses aplikasi apa pun Akun AWS dan yang muncul di portal.

   a. Untuk masuk ke Konsol Manajemen AWS pilih tab Akun dan pilih akun individual yang akan dikelola.

      Peran untuk pengguna Anda ditampilkan. Pilih nama peran untuk akun untuk membuka Konsol Manajemen AWS. Pilih tombol Access untuk mendapatkan kredensi untuk baris perintah atau akses terprogram.

   b. Pilih tab Aplikasi untuk menampilkan aplikasi yang tersedia dan pilih ikon aplikasi yang ingin Anda akses.

Masuk sebagai pengguna di Pusat Identitas IAM memberi Anda kredensi untuk mengakses sumber daya selama durasi waktu tertentu, yang disebut sesi. Secara default, pengguna dapat masuk ke dalam Akun AWS selama 8 jam. Administrator Pusat Identitas IAM dapat menentukan durasi yang berbeda, dari minimal 15 menit hingga maksimum 90 hari. Setelah sesi Anda berakhir, Anda dapat masuk lagi.

Informasi tambahan

Jika Anda ingin informasi lebih lanjut tentang pengguna di Pusat Identitas IAM, lihat sumber daya berikut.

- Untuk gambaran umum tentang Pusat Identitas IAM, lihat Apa itu Pusat Identitas IAM?
- Untuk detail tentang portal AWS akses Anda, lihat Menggunakan portal AWS akses.
- Untuk detail tentang sesi Pusat Identitas IAM, lihat Autentikasi pengguna.

- Untuk petunjuk langkah demi langkah tentang cara mengatur ulang kata sandi pengguna Pusat Identitas IAM Anda, lihatSaya lupa kata sandi Pusat Identitas IAM saya untuk saya Akun AWS.
- Jika Anda atau organisasi Anda menerapkan pemfilteran IP atau domain, Anda mungkin perlu mengizinkan daftar domain untuk membuat dan menggunakan portal akses Anda AWS . IAM Identity Center mendukung titik akhir IPv4 dan dual-stack. Jika jaringan Anda menggunakan IPv6, gunakan domain endpoint dual-stack. Untuk detail tentang domain daftar yang diizinkan, lihat. Domain untuk ditambahkan ke daftar izin Anda

Masuk melalui AWS Command Line Interface

Anda harus menetapkan bagaimana AWS CLI otentikasi dengan AWS. Pilih metode yang paling sesuai dengan alur kerja dan persyaratan keamanan Anda.

- Login dengan kredenal konsol (Disarankan)jika Anda menggunakan root, pengguna IAM atau federasi dengan IAM untuk akses AWS akun.
- Login dengan kredensi IAM Identity Centerjika Anda menggunakan Pusat Identitas untuk akses AWS akun.

Login dengan kredenal konsol (Disarankan)

Metode otentikasi ini memungkinkan Anda menggunakan kredenal konsol Anda dengan AWS CLI, sehingga mudah untuk memulai AWS pemrograman dalam beberapa menit setelah pengaturan akun. Anda bisa mendapatkan kredensi sementara yang bekerja dengan mulus di seluruh alat pengembangan lokal seperti, dan AWS CLI. AWS SDKs Alat AWS untuk PowerShell

Prasyarat

- Instal AWS CLI. Untuk informasi selengkapnya, lihat Menginstal atau memperbarui ke versi terbaru AWS CLI. Versi minimum 2.32.0 diperlukan untuk menggunakan perintah. `aws login`
- Akses untuk masuk ke Konsol Manajemen AWS sebagai pengguna root, pengguna IAM, atau melalui federasi dengan IAM. Jika Anda menggunakan IAM Identity Center, pergi ke Login dengan kredensi IAM Identity Center sebagai gantinya.
- Pastikan identitas IAM memiliki izin yang sesuai. Lampirkan kebijakan SignInLocalDevelopmentAccessterkelola ke pengguna, peran, atau grup IAM Anda. Jika Anda masuk sebagai pengguna root, tidak diperlukan izin tambahan.

Untuk login dengan kredenal konsol

1. Jalankan perintah berikut untuk memulai proses otentikasi berbasis browser:

   ```
   $ aws login
   ```

   `aws login`Perintah ini mendukung beberapa parameter opsional:

- `aws login --remote`- Untuk otentikasi lintas-perangkat saat perangkat Anda tidak mendukung browser

> **Note**
>
> Anda dapat mengontrol akses ke otentikasi same-device (`aws login`) dan cross-device (`aws login --remote`). Gunakan sumber daya berikut ARNs dalam kebijakan IAM yang relevan.
>
> - `arn:aws:signin:region:account-id:oauth2/public-client/localhost`— Gunakan ARN ini untuk otentikasi perangkat yang sama dengan. `aws login`
> - `arn:aws:signin:region:account-id:oauth2/public-client/remote`— Gunakan ARN ini untuk otentikasi lintas-perangkat dengan. `aws login --remote`

- `aws login --profile profile-name`- Untuk mengautentikasi dengan profil tertentu
- `aws login --region region`- Untuk mengautentikasi di wilayah tertentu

2. Ikuti petunjuk di terminal Anda. Perintah akan secara otomatis membuka browser default Anda dan memandu Anda melalui proses otentikasi. Setelah otentikasi berhasil, AWS CLI sesi Anda akan berlaku hingga 12 jam.
3. Untuk mengakhiri sesi Anda, gunakan:

```
$ aws logout
```

Jika Anda mengakses AWS layanan secara terprogram dengan menggunakan Alat AWS untuk PowerShell, silakan lihat Mengautentikasi Alat AWS dengan AWS. PowerShell Jika Anda menggunakan AWS SDKs, silakan lihat Otentikasi dan akses menggunakan AWS SDKs dan alat.

Login dengan kredensi IAM Identity Center

Portal AWS akses memudahkan pengguna IAM Identity Center untuk memilih Akun AWS dan mendapatkan kredensi keamanan sementara untuk. AWS CLI Untuk informasi selengkapnya tentang cara mendapatkan kredensi ini, lihat. Ketersediaan wilayah untuk ID AWS Builder Anda juga dapat mengonfigurasi AWS CLI langsung untuk mengautentikasi pengguna dengan IAM Identity Center.

Untuk login dengan kredensi IAM Identity Center

1. Periksa apakah Anda telah menyelesaikan Prasyarat.
2. Jika Anda masuk untuk pertama kalinya, konfigurasikan profil Anda dengan `aws configure sso` wizard.
3. Setelah Anda mengonfigurasi profil Anda, jalankan perintah berikut, lalu ikuti petunjuk di terminal Anda:

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

Informasi tambahan

Jika Anda ingin informasi lebih lanjut tentang masuk menggunakan baris perintah, lihat sumber daya berikut.

- Untuk informasi selengkapnya tentang penggunaan kredenal konsol Anda untuk masuk ke pengembangan AWS lokal, lihat Autentikasi dan akses kredenal untuk AWS CLI.
- Untuk informasi selengkapnya tentang proses AWS CLI masuk, lihat Mengautentikasi dengan kredensi jangka pendek untuk proses login. AWS CLI
- Untuk detail tentang konfigurasi Pusat Identitas IAM, lihat Mengkonfigurasi AWS CLI untuk menggunakan Pusat Identitas IAM.

Masuk sebagai identitas federasi

Identitas federasi adalah pengguna yang dapat mengakses Akun AWS sumber daya aman dengan identitas eksternal. Identitas eksternal dapat berasal dari toko identitas perusahaan (seperti LDAP atau Windows Active Directory) atau dari pihak ketiga (seperti Login dengan Amazon, Facebook, atau Google). Identitas federasi tidak masuk dengan portal Konsol Manajemen AWS atau AWS akses. Jenis identitas eksternal yang digunakan menentukan bagaimana identitas federasi masuk.

Administrator harus membuat URL khusus yang menyertakan`https://signin.aws.amazon.com/federation`. Untuk informasi selengkapnya, lihat Mengaktifkan akses broker identitas kustom ke. Konsol Manajemen AWS

> **Note**
>
> Administrator Anda membuat identitas federasi. Hubungi administrator Anda untuk detail selengkapnya tentang cara masuk sebagai identitas federasi.

Untuk informasi selengkapnya tentang identitas federasi, lihat Tentang federasi identitas web.

Masuk dengan ID AWS Builder

ID AWS Builder adalah profil pribadi yang menyediakan akses ke alat dan layanan tertentu termasuk Amazon CodeCatalyst, Pengembang Amazon Q, AWS Training dan Sertifikasi. ID AWS Builder mewakili Anda sebagai individu dan independen dari kredensi dan data apa pun yang mungkin Anda miliki di akun yang ada AWS . Seperti profil pribadi lainnya, ID AWS Builder tetap bersama Anda saat Anda maju melalui tujuan pribadi, pendidikan, dan karir Anda.

Anda ID AWS Builder melengkapi apa pun yang mungkin sudah Akun AWS Anda miliki atau ingin buat. Sementara Akun AWS bertindak sebagai wadah untuk AWS sumber daya yang Anda buat dan menyediakan batas keamanan untuk sumber daya tersebut, Anda ID AWS Builder mewakili Anda sebagai individu. Untuk informasi selengkapnya, lihat ID AWS Builder dan AWS kredensi lainnya.

ID AWS Builder gratis. Anda hanya membayar untuk AWS sumber daya yang Anda konsumsi di Anda Akun AWS. Untuk informasi selengkapnya tentang harga, lihat AWS Harga.

Jika Anda atau organisasi Anda menerapkan pemfilteran IP atau domain, Anda mungkin perlu mengizinkan daftar domain untuk membuat dan menggunakan file. ID AWS Builder Untuk detail tentang domain daftar yang diizinkan, lihat. Domain untuk ditambahkan ke daftar izin Anda

> **Note**
>
> AWS Builder ID terpisah dari langganan AWS Skill Builder Anda, pusat pembelajaran online tempat Anda dapat belajar dari AWS para ahli dan membangun keterampilan cloud secara online. Untuk informasi selengkapnya tentang AWS Skill Builder, lihat AWS Skill Builder.

Topik

- Hapus ID AWS Builder
- Kelola otentikasi ID AWS Builder multi-faktor (MFA)
- Privasi dan data di ID AWS Builder
- ID AWS Builder dan AWS kredensi lainnya

Untuk masuk dengan ID AWS Builder

1. Arahkan ke ID AWS Builder profil atau halaman masuk AWS alat atau layanan yang ingin Anda akses. Misalnya, untuk mengakses Amazon CodeCatalyst, bukahttps://codecatalyst.aws.
2. Pilih cara masuk ke ID AWS Builder
   - Saya memiliki akun yang sudah ada
   - Saya memiliki Akun Google
   - Saya memiliki Akun Apple
   - Saya memiliki GitHub Akun
   - Saya memiliki Akun Amazon

Saya memiliki akun yang sudah ada

1. Untuk akun yang ada, masukkan email yang Anda gunakan untuk membuat ID AWS Builder dan pilih Masuk.
2. Masukkan email yang Anda gunakan untuk membuat ID AWS Builder dan pilih Masuk.
3. Pada Masuk dengan ID AWS Builder halaman Anda, masukkan Kata Sandi Anda.
4. (Opsional) Jika Anda ingin login di masa mendatang dari perangkat ini tidak meminta verifikasi tambahan, centang kotak di sebelah Ini adalah perangkat tepercaya.
5. Pilih Lanjutkan.
6. Jika diminta dengan halaman verifikasi tambahan yang diperlukan, ikuti petunjuk dari browser Anda untuk memberikan kode atau kunci keamanan yang diperlukan.

> **Note**
>
> Demi keamanan Anda, kami menganalisis browser, lokasi, dan perangkat masuk Anda. Jika Anda memberi tahu kami untuk mempercayai perangkat ini, Anda tidak perlu memberikan

kode otentikasi multi-faktor (MFA) setiap kali Anda masuk. Untuk informasi selengkapnya, lihat Perangkat tepercaya.

Saya memiliki Akun Google

Jika Akun Google Anda sudah dikaitkan dengan ID AWS Builder, Anda harus menggunakan alamat email lain untuk masuk ke aplikasi. Untuk informasi selengkapnya, lihat Saya tidak bisa masuk dengan Google.

1. Untuk menggunakan Akun Google Anda untuk masuk ID AWS Builder, pilih Lanjutkan dengan Google.
2. Pada halaman Masuk dengan Google, masukkan informasi untuk Akun Google Anda untuk masuk.
3. Pilih Lanjutkan untuk memuat beranda AWS aplikasi.

Saya memiliki Akun Apple

Jika Akun Apple Anda sudah dikaitkan dengan ID AWS Builder, Anda harus menggunakan alamat email lain untuk masuk ke aplikasi. Untuk informasi selengkapnya, lihat Saya tidak bisa masuk dengan Apple.

1. Untuk menggunakan Akun Apple Anda untuk masuk ID AWS Builder, pilih Lanjutkan dengan Apple.
2. Pada halaman Masuk dengan Apple, masukkan informasi untuk akun Apple Anda untuk masuk.
3. Pilih Lanjutkan untuk memuat beranda AWS aplikasi.

Saya memiliki GitHub Akun

Jika GitHub Akun Anda sudah dikaitkan dengan ID AWS Builder, Anda harus menggunakan alamat email yang berbeda untuk masuk ke aplikasi. Untuk informasi selengkapnya, lihat Saya tidak bisa masuk dengan GitHub.

1. Untuk menggunakan GitHub Akun Anda untuk masuk ID AWS Builder, pilih Lanjutkan dengan GitHub.

2. Pada GitHub halaman Masuk dengan, masukkan informasi untuk GitHub Akun Anda untuk masuk.
3. Pilih Lanjutkan untuk memuat beranda AWS aplikasi.

Saya memiliki Akun Amazon

Jika Akun Amazon Anda sudah dikaitkan dengan ID AWS Builder, Anda harus menggunakan alamat email lain untuk masuk ke aplikasi. Untuk informasi selengkapnya, lihat Saya tidak bisa masuk dengan Amazon.

1. Untuk menggunakan Akun Amazon Anda untuk masuk ID AWS Builder, pilih Lanjutkan dengan Amazon.
2. Pada halaman Masuk dengan Amazon, masukkan informasi untuk Akun Amazon Anda untuk masuk.
3. Pilih Lanjutkan untuk memuat beranda AWS aplikasi.

Ketersediaan wilayah untuk ID AWS Builder

ID AWS Builder tersedia di berikut ini Wilayah AWS. Aplikasi yang menggunakan ID AWS Builder dapat beroperasi di Wilayah lain.

Nama	Kode
US East (Northern Virginia)	us-east-1

Buat Anda ID AWS Builder

Anda membuat ID AWS Builder ketika Anda mendaftar untuk salah satu AWS alat dan layanan yang menggunakannya. Daftar dengan alamat email, nama, dan kata sandi Anda sebagai bagian dari proses pendaftaran untuk AWS alat atau layanan.

Kata sandi Anda harus mematuhi persyaratan berikut:

- Password bersifat case-sensitive.
- Kata sandi harus memiliki panjang antara 8 dan 64 karakter.

- Kata sandi harus mengandung setidaknya satu karakter dari masing-masing dari empat kategori berikut:
  - Huruf kecil (a-z)
  - Huruf besar (A-Z)
  - Angka (0-9)
  - Karakter non-alfanumerik (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- Tiga kata sandi terakhir tidak dapat digunakan kembali.
- Kata sandi yang diketahui publik melalui kumpulan data yang bocor dari pihak ketiga tidak dapat digunakan.

> **Note**
>
> Alat dan layanan yang digunakan ID AWS Builder mengarahkan Anda untuk membuat dan menggunakan ID AWS Builder saat dibutuhkan.

Untuk membuat Anda ID AWS Builder

1. Arahkan ke ID AWS Builder profil atau halaman pendaftaran AWS alat atau layanan yang ingin Anda akses. Misalnya, untuk mengakses Amazon CodeCatalyst, bukahttps://codecatalyst.aws.
2. Pilih cara membuat ID AWS Builder
   - Untuk menggunakan Akun Google Anda, pilih Lanjutkan dengan Google dan ikuti petunjuk untuk menyelesaikan proses pendaftaran. Ini melewati langkah 3-8 di bawah ini. Pergi ke langkah 9.
   - Untuk menggunakan Akun Apple Anda, pilih Lanjutkan dengan Apple dan ikuti petunjuk untuk menyelesaikan proses pendaftaran. Ini melewati langkah 3-8 di bawah ini. Pergi ke langkah 9.

     > **Note**
     >
     > Jika Anda memilih untuk mengaktifkan fitur “Sembunyikan Email Saya” iCloud+ untuk Masuk dengan Apple, Anda ID AWS Builder akan dibuat dengan alamat Sembunyikan Email Saya yang ditunjuk di Akun Apple Anda, bukan alamat email asli Anda. Anda tidak akan dapat mengubah alamat email ini, tetapi nama depan dan belakang Anda masih dapat diedit. Jika Anda perlu masuk ID AWS Builder,

Anda harus menggunakan alamat Sembunyikan Email Saya. ID AWS Builder akan menggunakan alamat Sembunyikan Email Saya untuk mengirim komunikasi email kepada Anda. Untuk detail selengkapnya, lihat Cara menggunakan Sembunyikan Email Saya dengan Masuk dengan Apple.

- Untuk menggunakan GitHub Akun Anda, pilih Lanjutkan dengan GitHub dan ikuti petunjuk untuk menyelesaikan proses pendaftaran. Ini melewati langkah 3-8 di bawah ini. Pergi ke langkah 9.
- Untuk menggunakan Akun Amazon Anda, pilih Lanjutkan dengan Amazon dan ikuti petunjuk untuk menyelesaikan proses pendaftaran. Ini melewati langkah 3-8 di bawah ini. Pergi ke langkah 9.
- Untuk membuat akun dengan email dan kata sandi, lanjutkan dengan langkah-langkah berikut.

3. Pada ID AWS Builder halaman Buat, masukkan alamat email Anda. Kami menyarankan Anda menggunakan email pribadi.
4. Pilih Berikutnya.
5. Masukkan nama Anda, lalu pilih Berikutnya.
6. Pada halaman verifikasi Email, masukkan kode verifikasi yang kami kirimkan ke alamat email Anda. Pilih Verifikasi. Tergantung pada penyedia email Anda, mungkin perlu beberapa menit bagi Anda untuk menerima email. Periksa folder spam dan sampah Anda untuk kode. Jika Anda tidak melihat email AWS setelah lima menit, pilih Kirim ulang kode.
7. Setelah kami memverifikasi email Anda, pada halaman Pilih kata sandi, masukkan Kata Sandi dan Konfirmasi kata sandi.
8. Jika Captcha muncul sebagai keamanan tambahan, masukkan karakter yang Anda lihat.
9. Pilih Buat ID AWS Builder.

Perangkat tepercaya

Setelah Anda memilih opsi Ini adalah perangkat tepercaya dari halaman masuk, kami menganggap semua login di masa mendatang dari browser web tersebut di perangkat tersebut diotorisasi. Ini berarti Anda tidak perlu memberikan kode MFA pada perangkat tepercaya itu. Namun, jika browser, cookie, atau alamat IP Anda berubah, Anda mungkin harus menggunakan kode MFA Anda untuk verifikasi tambahan.

AWS alat dan layanan yang menggunakan ID AWS Builder

Anda dapat masuk dengan Anda ID AWS Builder untuk mengakses AWS alat dan layanan berikut. Akses ke kemampuan atau manfaat yang ditawarkan dengan biaya memerlukan Akun AWS.

Secara default, saat Anda masuk ke AWS alat atau layanan menggunakan alat ID AWS Builder, durasi sesi berlangsung selama 30 hari kecuali Amazon Q Developer, yang memiliki durasi sesi 90 hari. Setelah sesi Anda berakhir, Anda harus masuk lagi.

AWS Komunitas Cloud

Community.aws adalah platform oleh dan untuk komunitas AWS pembangun yang dapat Anda akses dengan Anda. ID AWS Builder Ini adalah tempat untuk menemukan konten pendidikan, berbagi pemikiran dan proyek pribadi Anda, mengomentari posting orang lain, dan mengikuti pembangun favorit Anda.

Amazon CodeCatalyst

Anda akan membuat ID AWS Builder ketika Anda mulai menggunakan Amazon CodeCatalyst dan memilih alias yang akan dikaitkan dengan aktivitas seperti masalah, komit kode, dan permintaan tarik. Undang orang lain ke CodeCatalyst ruang Amazon Anda, yang lengkap dengan alat, infrastruktur, dan lingkungan yang dibutuhkan tim Anda untuk membangun proyek sukses Anda berikutnya. Anda akan memerlukan sebuah Akun AWS untuk menyebarkan proyek baru ke cloud.

AWS Migration Hub

Akses AWS Migration Hub(Migration Hub) dengan ID AWS Builder. Migration Hub menyediakan satu tempat untuk menemukan server yang ada, merencanakan migrasi, dan melacak status setiap migrasi aplikasi.

Amazon Q Developer

Amazon Q Developer adalah asisten percakapan bertenaga AI generatif yang dapat membantu Anda memahami, membangun, memperluas, dan mengoperasikan aplikasi. AWS Untuk informasi selengkapnya, lihat Apa itu Pengembang Amazon Q? di Panduan Pengguna Pengembang Amazon Q.

AWS re:Post

AWS re:Postmemberi Anda bimbingan teknis ahli sehingga Anda dapat berinovasi lebih cepat dan meningkatkan efisiensi operasional menggunakan AWS layanan. Anda dapat masuk dengan

Anda ID AWS Builder dan bergabung dengan komunitas di re:Post tanpa kartu kredit Akun AWS atau.

AWS Startup

Gunakan Anda ID AWS Builder untuk bergabung dengan AWS Startup di mana Anda dapat menggunakan konten pembelajaran, alat, sumber daya, dan dukungan untuk mengembangkan startup Anda. AWS

AWS Training dan Sertifikasi

Anda dapat menggunakan ID AWS Builder untuk mengakses AWS Training dan Sertifikasi di mana Anda dapat membangun AWS Cloud keterampilan Anda dengan AWS Skill Builder, belajar dari AWS para ahli, dan memvalidasi keahlian cloud Anda dengan kredensi yang diakui industri.

Kiro

Kiro adalah IDE agen yang membantu Anda beralih dari prototipe ke produksi dengan pengembangan berbasis spesifikasi. Dari tugas sederhana hingga yang rumit, Kiro bekerja bersama Anda untuk mengubah petunjuk menjadi spesifikasi terperinci, kemudian menjadi kode kerja, dokumen, dan pengujian. Dengan Kiro, apa yang Anda bangun persis seperti yang Anda inginkan dan siap untuk dibagikan dengan tim Anda. Agen Kiro membantu Anda memecahkan masalah yang menantang dan mengotomatiskan tugas seperti membuat dokumentasi dan pengujian unit. Dengan Kiro, Anda dapat membangun di luar prototipe saat berada di kursi pengemudi di setiap langkah.

Portal Pendaftaran Situs Web (WRP)

Anda dapat menggunakan identitas pelanggan Anda ID AWS Builder sebagai profil pendaftaran dan identitas pelanggan yang gigih untuk Situs Web AWS Pemasaran. Untuk mendaftar webinar baru dan melihat semua webinar yang telah Anda daftarkan atau hadiri, lihat Webinar Saya.

Edit ID AWS Builder profil Anda

Anda dapat mengubah informasi profil Anda kapan saja. Anda dapat mengedit alamat Email dan Nama yang Anda gunakan untuk membuat ID AWS Builder, serta Nama Panggilan Anda. Saat menggunakan login sosial seperti Google atau Apple, hanya Nama dan Nama Panggilan yang dapat diedit.

Nama Anda adalah cara Anda dirujuk dalam alat dan layanan saat berinteraksi dengan orang lain. Nama Panggilan Anda menunjukkan bagaimana Anda ingin dikenal oleh AWS, teman, dan orang lain yang berkolaborasi dengan Anda.

> **Note**
>
> Alat dan layanan yang digunakan ID AWS Builder mengarahkan Anda untuk membuat dan menggunakan ID AWS Builder saat dibutuhkan.

Untuk mengedit informasi profil Anda

1. Masuk ke ID AWS Builder profil Anda dihttps://profile.aws.amazon.com.
2. Pilih Detail Saya.
3. Pada halaman Detail saya, pilih tombol Edit di sebelah Profil.
4. Pada halaman Edit profil, buat perubahan yang diinginkan pada Nama dan Nama Panggilan Anda.
5. Pilih Simpan perubahan. Pesan konfirmasi hijau muncul di bagian atas halaman untuk memberi tahu Anda bahwa Anda memperbarui profil Anda.

> **Note**
>
> Mengubah nama dan nama panggilan Anda dengan salah satu mitra masuk kami yang lain tidak memperbarui pengaturan yang sama untuk Anda ID AWS Builder.

Untuk mengedit informasi kontak Anda

1. Masuk ke ID AWS Builder profil Anda dihttps://profile.aws.amazon.com.
2. Pilih Detail Saya.
3. Pada halaman Detail saya, pilih tombol Edit di samping Informasi kontak.
4. Pada halaman Edit informasi kontak, ubah alamat Email Anda.
5. Pilih Verifikasi email. Sebuah kotak dialog muncul.
6. Dalam kotak dialog Verifikasi email, setelah Anda menerima kode di email Anda, masukkan kode di Kode verifikasi. Pilih Verifikasi.

Ubah ID AWS Builder kata sandi Anda

Kata sandi Anda harus mematuhi persyaratan berikut:

- Password bersifat case-sensitive.
- Kata sandi harus memiliki panjang antara 8 dan 64 karakter.
- Kata sandi harus mengandung setidaknya satu karakter dari masing-masing dari empat kategori berikut:
  - Huruf kecil (a-z)
  - Huruf besar (A-Z)
  - Angka (0-9)
  - Karakter non-alfanumerik (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- Tiga kata sandi terakhir tidak dapat digunakan kembali.

> **Note**
>
> Perubahan kata sandi tidak tersedia untuk ID AWS Builder akun yang menggunakan login sosial seperti Google atau Apple. Jika Anda masuk menggunakan login sosial, Anda mengelola kata sandi Anda melalui akun login sosial Anda. Untuk mengubah kata sandi Anda untuk login sosial:
>
> - Untuk Akun Google, lihat Mengubah atau mengatur ulang kata sandi (Google) Anda.
> - Untuk Akun Apple, lihat Mengubah kata sandi Akun Apple Anda.
> - Untuk GitHub Akun, lihat Memperbarui kredenal GitHub akses Anda.
> - Untuk Akun Amazon, lihat Cara mengubah kata sandi Amazon.

Untuk mengubah ID AWS Builder kata sandi Anda

1. Masuk ke ID AWS Builder profil Anda dihttps://profile.aws.amazon.com.
2. Pilih Keamanan.
3. Pada halaman Keamanan, pilih Ubah kata sandi. Ini membawa Anda ke halaman baru.
4. Pada halaman Masukkan kembali kata sandi Anda, di bawah Kata Sandi, masukkan kata sandi Anda saat ini. Kemudian pilih Masuk.
5. Pada halaman Ubah kata sandi Anda, di bawah Kata sandi baru, masukkan kata sandi baru yang ingin Anda gunakan. Kemudian di bawah Konfirmasi kata sandi, masukkan kembali kata sandi baru yang ingin Anda gunakan.
6. Pilih Ubah kata sandi. Anda diarahkan ke ID AWS Builder profil Anda.

Hapus semua sesi aktif untuk ID AWS Builder

Di bawah Perangkat yang masuk, Anda dapat melihat semua perangkat yang saat ini Anda masuki. Jika Anda tidak mengenali perangkat, sebagai praktik terbaik keamanan, pertama-tama ubah kata sandi Anda dan kemudian keluar di mana-mana. Anda dapat keluar dari semua perangkat dengan menghapus semua sesi aktif Anda di halaman Keamanan untuk Anda ID AWS Builder.

> **Note**
>
> ID AWS Builder mendukung sesi diperpanjang 90 hari untuk Pengembang Amazon Q dalam IDE. Untuk setiap login IDE baru, Anda dapat melihat dua entri sesi. Saat keluar dari IDE, Anda dapat terus melihat sesi IDE yang tercantum di bawah Perangkat yang masuk meskipun tidak valid lagi. Sesi ini menghilang setelah 90 hari kedaluwarsa.

Untuk menghapus semua sesi aktif

1. Masuk ke ID AWS Builder profil Anda dihttps://profile.aws.amazon.com.
2. Pilih Keamanan.
3. Pada halaman Keamanan, pilih Hapus semua sesi aktif.
4. Dalam Hapus semua sesi kotak dialog, masukkan hapus semua. Dengan menghapus semua sesi, Anda keluar dari semua perangkat yang mungkin telah Anda masuki menggunakan ID AWS Builder, termasuk browser yang berbeda. Kemudian pilih Hapus semua sesi.

> **Note**
>
> Saat menggunakan akun login sosial seperti Google atau Apple, menghapus ID AWS Builder sesi aktif tidak akan membuat Anda keluar dari akun login sosial Anda.

Hapus ID AWS Builder

Prosedur berikut menjelaskan cara menghapus ID AWS Builder akun Anda.

> **Warning**
>
> Menghapus Anda ID AWS Builder akan menghasilkan hal berikut:

- Kehilangan akses — Anda tidak dapat lagi mengakses AWS alat dan layanan apa pun yang sebelumnya Anda akses ID AWS Builder. Akun Anda ID AWS Builder terpisah dari AWS akun apa pun yang mungkin Anda miliki, dan penghapusan akun Anda tidak ID AWS Builder akan menutup akun Anda AWS .
- Penghapusan konten — Setiap konten yang tersisa yang terkait hanya dengan Anda ID AWS Builder akan dihapus dan Anda tidak akan lagi dapat mengakses atau memulihkan konten Anda dari aplikasi yang menggunakan Anda. ID AWS Builder
- Penghapusan informasi pribadi — Setiap informasi pribadi yang Anda berikan sehubungan dengan pembuatan dan administrasi Anda ID AWS Builder akan dihapus, kecuali yang AWS dapat menyimpan informasi pribadi sebagaimana diwajibkan atau diizinkan oleh hukum, seperti catatan permintaan penghapusan Anda atau data dalam bentuk yang tidak mengidentifikasi Anda.

  Anda dapat mengetahui lebih lanjut tentang cara kami menangani informasi Anda di Pemberitahuan Privasi AWS. Anda dapat memperbarui preferensi AWS komunikasi atau berhenti berlangganan dengan mengunjungi Pusat Preferensi Komunikasi AWS.
- Akun login sosial tetap tidak berubah — Jika Anda menggunakan login sosial seperti Google atau Apple, menghapus akun Anda ID AWS Builder tidak akan menghapus apa pun yang terkait dengan akun login sosial Anda. Lihat dokumentasi dari penyedia login sosial Anda untuk mempelajari cara menghapus akun tersebut. Menghapus ID AWS Builder koneksi dari akun login sosial Anda tidak menghapus ID AWS Builder akun Anda, tetapi Anda tidak lagi dapat mengakses ID AWS Builder profil Anda.

Untuk menghapus ID AWS Builder

1. Masuk ke ID AWS Builder profil Anda dihttps://profile.aws.amazon.com.
2. Pilih Privasi & data.
3. Pada halaman Privasi & data, di bawah Menghapus ID AWS Builder, pilih Hapus ID AWS Builder.
4. Pilih kotak centang di samping setiap penafian untuk mengonfirmasi bahwa Anda siap untuk melanjutkan.
5. Pilih Hapus ID AWS Builder.

Kelola otentikasi ID AWS Builder multi-faktor (MFA)

Otentikasi multi-faktor (MFA) adalah mekanisme sederhana dan efektif untuk meningkatkan keamanan Anda. Faktor pertama — kata sandi Anda — adalah rahasia yang Anda hafal, juga dikenal sebagai faktor pengetahuan. Faktor lain dapat berupa faktor kepemilikan (sesuatu yang Anda miliki, seperti kunci keamanan) atau faktor warisan (sesuatu yang Anda miliki, seperti pemindaian biometrik). Kami sangat menyarankan Anda mengkonfigurasi MFA untuk menambahkan lapisan tambahan untuk Anda. ID AWS Builder

Anda dapat mendaftarkan autentikator bawaan dan juga mendaftarkan kunci keamanan yang Anda simpan di lokasi yang aman secara fisik. Jika Anda tidak dapat menggunakan autentikator bawaan Anda, maka Anda dapat menggunakan kunci keamanan terdaftar Anda. Untuk aplikasi autentikator, Anda juga dapat mengaktifkan fitur pencadangan atau sinkronisasi cloud di aplikasi tersebut. Ini membantu Anda menghindari kehilangan akses ke profil Anda jika Anda kehilangan atau merusak perangkat MFA Anda.

Poin kunci

- Kami menyarankan Anda mendaftarkan beberapa perangkat MFA. Jika Anda kehilangan akses ke semua perangkat MFA terdaftar, Anda tidak akan dapat memulihkan perangkat MFA Anda. ID AWS Builder
- Kami menyarankan Anda meninjau perangkat MFA terdaftar secara berkala untuk memastikan perangkat tersebut mutakhir dan fungsional. Selain itu, Anda harus menyimpan perangkat tersebut di tempat yang aman secara fisik saat tidak digunakan.
- Jika Anda membuat akun menggunakan Lanjutkan dengan Google, Anda dapat mengaktifkan otentikasi multi-faktor melalui akun Google Anda. Untuk detailnya, lihat Mengaktifkan Verifikasi 2 Langkah.
- Jika Anda membuat akun menggunakan Lanjutkan dengan Apple, autentikasi multi-faktor kemungkinan sudah diaktifkan di Akun Apple Anda. Jika tidak, untuk detail tentang cara mengaktifkannya, lihat Autentikasi dua faktor untuk Akun Apple.
- Jika Anda membuat akun menggunakan Lanjutkan dengan GitHub, Anda dapat mengaktifkan otentikasi multi-faktor melalui Akun Anda GitHub. Untuk detailnya, lihat Mengonfigurasi (GitHub) otentikasi dua faktor.
- Jika Anda membuat akun menggunakan Lanjutkan dengan Amazon, Anda dapat mengaktifkan otentikasi multi-faktor melalui Akun Amazon Anda. Untuk detailnya, lihat Apa itu Verifikasi Dua Langkah? .

Tersedia tipe MFA untuk ID AWS Builder

ID AWS Builder mendukung jenis perangkat otentikasi multi-faktor (MFA) berikut.

FIDO2 autentikator

FIDO2adalah standar yang mencakup CTAP2 dan WebAuthndan didasarkan pada kriptografi kunci publik. Kredensi FIDO tahan terhadap phishing karena unik untuk situs web tempat kredensialnya dibuat. AWS

AWS mendukung dua faktor bentuk yang paling umum untuk otentikator FIDO: autentikator bawaan dan kunci keamanan. Lihat di bawah untuk informasi selengkapnya tentang jenis autentikator FIDO yang paling umum.

Topik

- Autentikator bawaan
- Kunci keamanan
- Pengelola kata sandi, penyedia kunci sandi, dan otentikator FIDO lainnya

Autentikator bawaan

Beberapa perangkat memiliki autentikator bawaan, seperti TouchID aktif MacBook atau kamera yang kompatibel dengan Windows Hello. Jika perangkat Anda kompatibel dengan protokol FIDO, termasuk WebAuthn, Anda dapat menggunakan sidik jari atau wajah Anda sebagai faktor kedua. Untuk informasi selengkapnya, lihat Otentikasi FIDO.

Kunci keamanan

Anda dapat membeli kunci keamanan FIDO2 yang terhubung dengan USB, BLE, atau NFC eksternal yang kompatibel. Saat Anda diminta untuk perangkat MFA, ketuk sensor tombol. YubiKey atau Feitian membuat perangkat yang kompatibel. Untuk daftar semua kunci keamanan yang kompatibel, lihat Produk Bersertifikat FIDO.

Pengelola kata sandi, penyedia kunci sandi, dan otentikator FIDO lainnya

Beberapa penyedia pihak ketiga mendukung otentikasi FIDO dalam aplikasi seluler, sebagai fitur dalam pengelola kata sandi, kartu pintar dengan mode FIDO, dan faktor bentuk lainnya. Perangkat yang kompatibel dengan FIDO ini dapat bekerja dengan IAM Identity Center, tetapi kami menyarankan Anda menguji autentikator FIDO sendiri sebelum mengaktifkan opsi ini untuk MFA.

> **Note**
>
> Beberapa autentikator FIDO dapat membuat kredensil FIDO yang dapat ditemukan yang dikenal sebagai kunci sandi. Passkey mungkin terikat ke perangkat yang membuatnya, atau mereka dapat disinkronkan dan dicadangkan ke cloud. Misalnya, Anda dapat mendaftarkan kunci sandi menggunakan Apple Touch ID di Macbook yang didukung, lalu masuk ke situs dari laptop Windows menggunakan Google Chrome dengan kunci sandi Anda di iCloud dengan mengikuti petunjuk di layar saat masuk. Untuk informasi selengkapnya tentang perangkat mana yang mendukung kunci sandi yang dapat disinkronkan dan interoperabilitas kunci sandi saat ini antara sistem operasi dan browser, lihat Dukungan Perangkat di passkeys.dev, sumber daya yang dikelola oleh FIDO Alliance And World Wide Web Consortium (W3C).

Aplikasi Authenticator

Aplikasi Authenticator adalah one-time password (OTP) berbasis third party authenticator. Anda dapat menggunakan aplikasi autentikator yang diinstal pada perangkat seluler atau tablet Anda sebagai perangkat MFA resmi. Aplikasi autentikator pihak ketiga harus sesuai dengan RFC 6238, yang merupakan algoritma kata sandi satu kali berbasis waktu (TOTP) berbasis waktu berbasis standar yang mampu menghasilkan kode otentikasi enam digit.

Saat diminta untuk MFA, Anda harus memasukkan kode yang valid dari aplikasi autentikator Anda di dalam kotak input yang disajikan. Setiap perangkat MFA yang ditetapkan ke pengguna harus unik. Dua aplikasi autentikator dapat didaftarkan untuk setiap pengguna tertentu.

Anda dapat memilih dari aplikasi otentikator pihak ketiga terkenal berikut. Namun, aplikasi apa pun yang sesuai dengan TOTP berfungsi dengan MFA. ID AWS Builder

Sistem operasi	Aplikasi autentikator yang diuji
Android	1 Kata Sandi, Authy, Duo Mobile, Microsoft Authenticator,Google Authenticator
iOS	1 Kata Sandi, Authy, Duo Mobile, Microsoft Authenticator,Google Authenticator

Daftarkan perangkat ID AWS Builder MFA Anda

> **Note**
>
> Setelah mendaftar ke MFA, keluar, lalu masuk di perangkat yang sama, Anda mungkin tidak akan diminta untuk MFA di perangkat tepercaya.

Untuk mendaftarkan perangkat MFA Anda menggunakan aplikasi autentikator

1. Masuk ke ID AWS Builder profil Anda dihttps://profile.aws.amazon.com.
2. Pilih Keamanan.
3. Pada halaman Keamanan, pilih Daftarkan perangkat.
4. Pada halaman Daftarkan perangkat MFA, pilih aplikasi Authenticator.
5. ID AWS Builder mengoperasikan dan menampilkan informasi konfigurasi, termasuk grafik kode QR. Grafik adalah representasi dari “kunci konfigurasi rahasia” yang tersedia untuk entri manual di aplikasi otentikator yang tidak mendukung kode QR.
6. Buka aplikasi autentikator Anda. Untuk daftar aplikasi, lihatAplikasi Authenticator.

   Jika aplikasi autentikator mendukung beberapa perangkat atau akun MFA, pilih opsi untuk membuat perangkat atau akun MFA baru.
7. Tentukan apakah aplikasi MFA mendukung kode QR, lalu lakukan salah satu hal berikut di halaman Siapkan aplikasi autentikator Anda:

   1. Pilih Tampilkan kode QR, lalu gunakan aplikasi untuk memindai kode QR. Misalnya, Anda dapat memilih ikon kamera atau memilih opsi yang mirip dengan kode Pindai. Kemudian gunakan kamera perangkat untuk memindai kode.
   2. Pilih Tampilkan kunci rahasia, lalu masukkan kunci rahasia itu ke aplikasi MFA Anda.

   Setelah selesai, aplikasi autentikator Anda akan menghasilkan dan menampilkan kata sandi satu kali.
8. Di kotak kode Authenticator, masukkan kata sandi satu kali yang saat ini muncul di aplikasi autentikator Anda. Pilih Tugaskan MFA.

> **Important**
>
> Kirim permintaan Anda segera setelah membuat kode. Jika Anda membuat kode dan kemudian menunggu terlalu lama untuk mengirimkan permintaan, perangkat MFA berhasil dikaitkan dengan Anda ID AWS Builder, tetapi perangkat MFA tidak sinkron. Hal ini terjadi karena kata sandi sekali pakai berbasis waktu (TOTP) kedaluwarsa setelah periode waktu yang singkat. Jika ini terjadi, Anda dapat menyinkronisasi ulang perangkat. Untuk informasi selengkapnya, lihat Saya mendapatkan pesan 'Kesalahan tak terduga telah terjadi' ketika saya mencoba mendaftar atau masuk dengan aplikasi autentikator.

9. Untuk memberikan nama yang ramah pada perangkat Anda ID AWS Builder, pilih Ganti nama. Nama ini membantu Anda membedakan perangkat ini dari perangkat lain yang Anda daftarkan.

Perangkat MFA sekarang siap digunakan. ID AWS Builder

Daftarkan kunci keamanan sebagai perangkat ID AWS Builder MFA Anda

Untuk mendaftarkan perangkat MFA Anda menggunakan kunci keamanan

1. Masuk ke ID AWS Builder profil Anda dihttps://profile.aws.amazon.com.
2. Pilih Keamanan.
3. Pada halaman Keamanan, pilih Daftarkan perangkat.
4. Pada halaman Daftarkan perangkat MFA, pilih Kunci keamanan.
5. Pastikan kunci keamanan Anda diaktifkan. Jika Anda menggunakan kunci keamanan fisik terpisah, sambungkan ke komputer Anda.
6. Ikuti instruksi di layar Anda. Pengalaman Anda bervariasi berdasarkan sistem operasi dan browser Anda.
7. Untuk memberikan nama yang ramah pada perangkat Anda ID AWS Builder, pilih Ganti nama. Nama ini membantu Anda membedakan perangkat ini dari perangkat lain yang Anda daftarkan.

Perangkat MFA sekarang siap digunakan. ID AWS Builder

Ganti nama perangkat ID AWS Builder MFA Anda

Untuk mengganti nama perangkat MFA Anda

1. Masuk ke ID AWS Builder profil Anda dihttps://profile.aws.amazon.com.
2. Pilih Keamanan. Ketika Anda tiba di halaman, Anda melihat bahwa Ganti nama berwarna abu-abu.
3. Pilih perangkat MFA yang ingin Anda ubah. Ini memungkinkan Anda untuk memilih Ganti nama. Kemudian kotak dialog muncul.
4. Pada prompt yang terbuka, masukkan nama baru di nama perangkat MFA, dan pilih Ganti nama. Perangkat yang diganti namanya muncul di bawah perangkat otentikasi multi-faktor (MFA).

Hapus perangkat MFA Anda

Kami menyarankan Anda menyimpan dua atau lebih perangkat MFA aktif. Sebelum Anda menghapus perangkat, lihat Daftarkan perangkat ID AWS Builder MFA Anda untuk mendaftarkan perangkat MFA pengganti. Untuk menonaktifkan otentikasi multi-faktor untuk Anda ID AWS Builder, hapus semua perangkat MFA terdaftar dari profil Anda.

Untuk menghapus perangkat MFA

1. Masuk ke ID AWS Builder profil Anda dihttps://profile.aws.amazon.com.
2. Pilih Keamanan.
3. Pilih perangkat MFA yang ingin Anda ubah dan pilih Hapus.
4. Di perangkat Hapus MFA? modal, ikuti petunjuk untuk menghapus perangkat Anda.
5. Pilih Hapus.

Perangkat yang dihapus tidak lagi muncul di bawah perangkat otentikasi multi-faktor (MFA).

Privasi dan data di ID AWS Builder

Pemberitahuan AWS Privasi menguraikan cara kami menangani data pribadi Anda. Untuk informasi tentang cara menghapus ID AWS Builder profil Anda, lihatHapus ID AWS Builder.

Minta ID AWS Builder data Anda

Anda dapat meminta dan melihat informasi pribadi yang terkait dengan Anda ID AWS Builder dan AWS aplikasi dan layanan yang Anda akses dengan Anda ID AWS Builder. Untuk informasi lebih lanjut tentang penggunaan hak subjek data Anda, termasuk untuk informasi pribadi yang diberikan sehubungan dengan AWS situs web, aplikasi, produk, layanan, acara, dan pengalaman lain, lihat. https://aws.amazon.com/privacy

Untuk meminta data Anda

1. Masuk ke ID AWS Builder profil Anda dihttps://profile.aws.amazon.com.
2. Pilih ID AWS Builder Data saya.
3. Pada halaman ID AWS Builder Data saya, di bawah Menghapus ID AWS Builder, pilih Minta data Anda.
4. Pesan konfirmasi hijau muncul di bagian atas halaman yang kami terima permintaan Anda dan akan menyelesaikannya dalam waktu 30 hari.
5. Ketika Anda menerima email dari kami bahwa permintaan telah diproses, navigasikan kembali ke halaman Privasi & data ID AWS Builder profil Anda. Pilih tombol yang baru tersedia Unduh arsip ZIP dengan data Anda.

   Saat permintaan data Anda tertunda, Anda tidak akan dapat menghapus permintaan data Anda ID AWS Builder.

ID AWS Builder dan AWS kredensi lainnya

Anda ID AWS Builder terpisah dari kredensi apa pun Akun AWS atau masuk. Anda dapat menggunakan email yang sama untuk Anda ID AWS Builder dan untuk email pengguna root dari file Akun AWS.

Sebuah ID AWS Builder:

- Memungkinkan Anda mengakses alat dan layanan yang digunakan ID AWS Builder.
- Tidak memengaruhi kontrol keamanan yang ada, seperti kebijakan dan konfigurasi yang telah Anda tentukan pada aplikasi Akun AWS atau aplikasi Anda.
- Tidak menggantikan root yang ada, Pusat Identitas IAM, atau pengguna IAM, kredensi, atau akun.
- Tidak dapat memperoleh kredensi AWS IAM untuk mengakses Konsol Manajemen AWS,, AWS CLI AWS SDKs, atau Toolkit. AWS

An Akun AWS adalah wadah sumber daya dengan informasi kontak dan pembayaran. Ini menetapkan batas keamanan untuk mengoperasikan AWS layanan yang ditagih dan diukur, seperti S3, EC2, atau Lambda. Pemilik akun dapat masuk ke Akun AWS dalam Konsol Manajemen AWS. Untuk informasi lebih lanjut, lihat Masuk ke Konsol Manajemen AWS.

Bagaimana ID AWS Builder kaitannya dengan identitas Pusat Identitas IAM Anda yang ada

Sebagai individu yang memiliki identitas yang Anda kelola. ID AWS Builder Ini tidak terhubung dengan identitas lain yang mungkin Anda miliki untuk organisasi lain, seperti sekolah atau tempat kerja. Anda dapat menggunakan identitas tenaga kerja di IAM Identity Center untuk mewakili diri kerja Anda dan ID AWS Builder untuk mewakili diri pribadi Anda. Identitas ini beroperasi secara independen.

Pengguna di AWS IAM Identity Center (penerus AWS Single Sign-On) dikelola oleh administrator TI atau cloud perusahaan, atau oleh administrator penyedia identitas organisasi, seperti Okta, Ping, atau Azure. Pengguna di Pusat Identitas IAM dapat mengakses sumber daya di beberapa akun di AWS Organizations.

Beberapa ID AWS Builder profil

Anda dapat membuat lebih dari satu ID AWS Builder selama setiap ID menggunakan alamat email yang unik. Namun, menggunakan lebih dari satu ID AWS Builder dapat membuat sulit untuk mengingat yang ID AWS Builder Anda gunakan untuk tujuan apa. Jika memungkinkan, kami sarankan menggunakan single ID AWS Builder untuk semua aktivitas Anda dalam AWS alat dan layanan.

Keluar dari AWS

Bagaimana Anda keluar dari Anda Akun AWS tergantung pada jenis AWS pengguna Anda. Anda dapat menjadi pengguna root akun, pengguna IAM, pengguna di IAM Identity Center, identitas federasi, atau pengguna AWS Builder ID. Jika Anda tidak yakin pengguna seperti apa Anda, lihatTentukan jenis pengguna Anda.

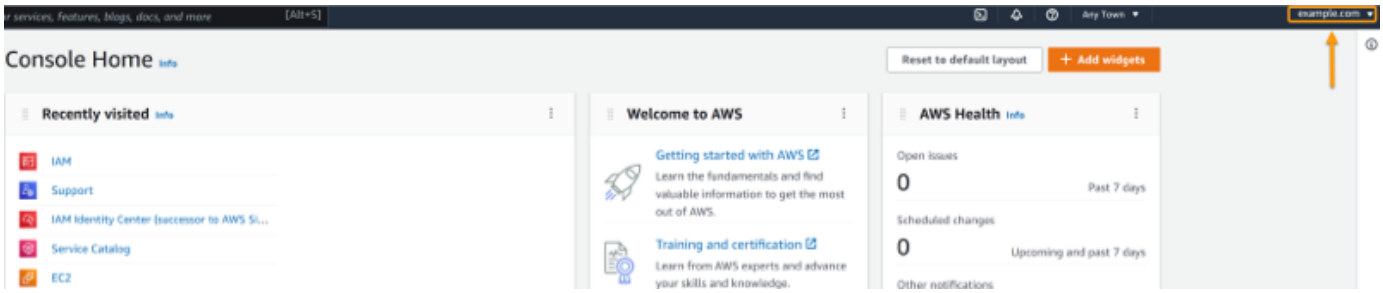
Topik

- Keluar dari Konsol Manajemen AWS
- Keluar dari portal AWS akses Anda
- Keluar dari AWS Builder ID

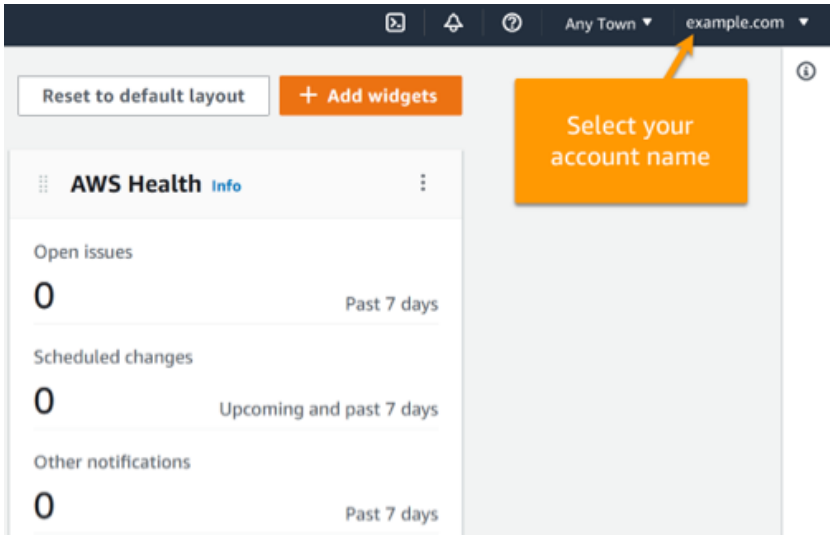
Keluar dari Konsol Manajemen AWS

Untuk keluar dari Konsol Manajemen AWS

1. Setelah Anda masuk ke halaman Konsol Manajemen AWS, Anda tiba di halaman yang mirip dengan yang ditunjukkan pada gambar berikut. Nama akun Anda atau nama pengguna IAM ditampilkan di sudut kanan atas.



2. Di bilah navigasi di kanan atas, pilih nama pengguna Anda.



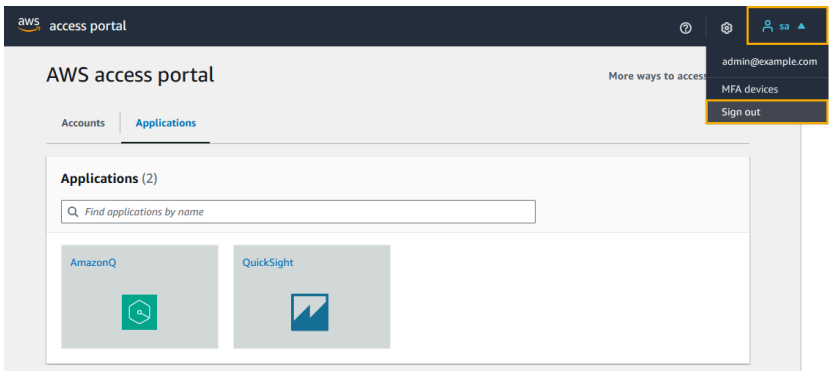
3. Pilih opsi Keluar. Opsi tombol berbeda berdasarkan berapa banyak akun yang Anda masuki.
   - Pilih Keluar jika Anda hanya masuk ke satu akun.
   - Pilih Keluar dari semua sesi untuk keluar dari semua identitas Anda secara bersamaan.
   - Pilih Keluar dari sesi saat ini untuk keluar dari identitas yang telah Anda pilih.
4. Anda dikembalikan ke Konsol Manajemen AWS halaman web.

Untuk informasi selengkapnya tentang masuk ke beberapa akun, lihat Masuk ke beberapa akun di Panduan Konsol Manajemen AWS Memulai.

Keluar dari portal AWS akses Anda

Untuk keluar dari portal AWS akses Anda

1. Di bilah navigasi di kanan atas, pilih nama pengguna Anda.
2. Pilih Keluar seperti yang ditunjukkan pada gambar berikut.



3. Jika Anda berhasil keluar, Anda sekarang melihat halaman masuk portal AWS akses Anda.

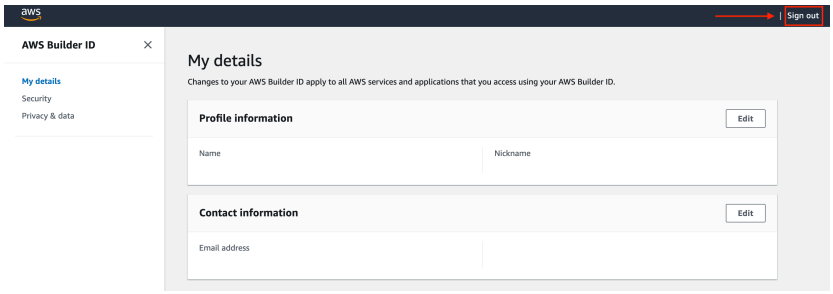
Jika Anda menggunakan penyedia identitas eksternal (iDP) sebagai sumber identitas Anda, sesi aktif untuk kredensi Anda tidak akan dihentikan saat Anda keluar. Jika Anda menavigasi kembali ke portal AWS akses, Anda mungkin masuk secara otomatis tanpa harus memberikan kredensialnya.

Keluar dari AWS Builder ID

Untuk keluar dari AWS layanan yang telah diakses menggunakan AWS Builder ID, Anda harus keluar dari layanan. Jika Anda ingin keluar dari profil AWS Builder ID Anda, lihat prosedur berikut.

Untuk keluar dari profil AWS Builder ID

1. Setelah Anda masuk ke profil AWS Builder ID Anda dihttps://profile.aws.amazon.com/, Anda tiba di Detail Saya.
2. Di kanan atas halaman profil AWS Builder ID Anda, pilih Keluar.



3. Anda keluar ketika Anda tidak lagi melihat profil AWS Builder ID Anda.

Pemecahan Masalah Akun AWS masalah masuk

Gunakan informasi di sini untuk membantu Anda memecahkan masalah masuk dan masalah lainnya. Akun AWS Untuk petunjuk langkah demi langkah saat masuk ke sebuah Akun AWS, lihatMasuk ke Konsol Manajemen AWS.

Jika tidak ada topik pemecahan masalah yang membantu Anda mengatasi masalah masuk, Anda dapat membuat kasus Dukungan dengan mengisi formulir ini: Saya AWS pelanggan dan saya sedang mencari penagihan atau dukungan akun. Sebagai praktik keamanan terbaik, tidak Dukungan dapat mendiskusikan detail apa pun Akun AWS selain akun yang Anda masuki. AWS Support juga tidak dapat mengubah kredensional yang terkait dengan akun karena alasan apa pun.

> **Note**
>
> Dukungan tidak mempublikasikan nomor telepon langsung untuk mencapai perwakilan dukungan.

Untuk bantuan selengkapnya tentang pemecahan masalah login Anda, lihat Apa yang harus saya lakukan jika saya mengalami masalah saat masuk atau mengakses? Akun AWS Jika Anda mengalami masalah saat masuk Amazon.com, lihat Layanan Pelanggan Amazon, bukan halaman ini.

Topik

- Saya lupa kata sandi identitas federasi saya untuk Akun AWS
- Saya tidak bisa masuk ke tempat saya yang ada Akun AWS dan saya tidak bisa membuat yang baru Akun AWS dengan alamat email yang sama
- Saya harus mengaktifkan kembali suspensi saya Akun AWS
- Saya perlu menghubungi Dukungan untuk masalah masuk
- Saya perlu menghubungi AWS Billing untuk masalah penagihan
- Saya punya pertanyaan tentang pesanan eceran
- Saya butuh bantuan untuk mengelola Akun AWS
- Saya AWS kredensyal portal akses tidak berfungsi
- Saya lupa kata sandi Pusat Identitas IAM saya untuk saya Akun AWS
- Saya menerima kesalahan yang menyatakan 'Bukan Anda, ini kami' ketika saya mencoba masuk ke konsol Pusat Identitas IAM

Saya Konsol Manajemen AWS kredensyal tidak berfungsi

Jika Anda ingat nama pengguna dan kata sandi Anda, tetapi kredensialnya tidak berfungsi, Anda mungkin berada di halaman yang salah. Coba masuk di halaman yang berbeda:

Halaman masuk pengguna akar

- Jika Anda membuat atau memiliki Akun AWS dan sedang melakukan tugas yang memerlukan kredensi pengguna root, masukkan alamat email akun Anda di file. Konsol Manajemen AWS Untuk mempelajari cara mengakses pengguna root, lihatUntuk masuk sebagai pengguna root. Jika Anda lupa kata sandi pengguna root Anda, Anda dapat mengatur ulang. Untuk informasi selengkapnya, lihat Saya lupa kata sandi pengguna root saya untuk saya Akun AWS. Jika Anda lupa alamat email pengguna root Anda, periksa kotak masuk email Anda untuk email dari. AWS
- Jika Anda mencoba masuk ke akun pengguna root Anda dan menerima kesalahan: Pemulihan kata sandi dinonaktifkan untuk akun pengguna root saya, Anda tidak memiliki kredenal pengguna root. Anda tidak dapat masuk sebagai pengguna root atau melakukan pemulihan kata sandi untuk pengguna root akun Anda. AWS Akun anggota yang dikelola menggunakan AWS Organizations mungkin tidak memiliki kata sandi pengguna root, kunci akses, sertifikat penandatanganan, atau otentikasi multi-faktor aktif (MFA).

  Hanya akun manajemen atau administrator yang didelegasikan untuk IAM yang dapat melakukan tindakan pengguna root di akun anggota Anda. Hubungi administrator Anda jika Anda perlu

melakukan tugas yang memerlukan kredensi pengguna root. Untuk informasi selengkapnya, lihat Mengelola akses root untuk akun anggota secara terpusat di Panduan AWS Identity and Access Management Pengguna.

Halaman masuk pengguna IAM

- Jika Anda atau orang lain membuat pengguna IAM dalam sebuah Akun AWS, Anda harus mengetahui Akun AWS ID atau alias tersebut untuk masuk. Masukkan ID akun atau alias, nama pengguna, dan kata sandi Anda ke dalam. Konsol Manajemen AWS Untuk mempelajari cara mengakses halaman login pengguna IAM, lihat. Untuk masuk sebagai pengguna IAM Jika Anda lupa kata sandi pengguna IAM Anda, Anda dapat melihat Saya lupa kata sandi pengguna IAM saya untuk saya Akun AWS informasi tentang mengatur ulang kata sandi pengguna IAM Anda. Jika Anda lupa nomor akun Anda, cari email, favorit browser, atau riwayat browser Anda untuk URL yang disertakan`signin.aws.amazon.com/`. ID akun atau alias Anda akan mengikuti `"account="` teks di URL. Jika Anda tidak dapat menemukan ID akun atau alias Anda, hubungi administrator Anda. Dukungan tidak dapat membantu Anda memulihkan informasi ini. Anda tidak dapat melihat ID akun atau alias Anda sampai setelah Anda masuk.

Reset kata sandi diperlukan untuk pengguna root saya

Untuk perlindungan akun Anda, Anda mungkin menerima pesan berikut ketika Anda mencoba masuk ke Konsol Manajemen AWS:

Reset kata sandi diperlukan. Untuk masalah keamanan, Anda perlu mengatur ulang kata sandi Anda. Untuk menjaga keamanan akun Anda, Anda harus memilih Lupa kata sandi di bawah ini dan mengatur ulang kata sandi Anda.

Selain pesan ini, AWS juga memberi tahu Anda ketika kami mengidentifikasi potensi masalah melalui email yang terkait dengan akun Anda. Email ini mencakup alasan pengaturan ulang kata sandi diperlukan. Misalnya, ketika kami mengidentifikasi aktivitas login yang tidak biasa ke Anda Akun AWS atau kredensi yang terkait dengan Anda Akun AWS tersedia untuk umum secara online.

Perbarui kata sandi Anda untuk memastikan kredensi pengguna root Anda tetap aman. Untuk mempelajari cara mengatur ulang kata sandi pengguna root Anda, lihat Saya lupa kata sandi pengguna root saya untuk kata sandi saya Akun AWS.

Saya tidak memiliki akses ke email untuk saya Akun AWS

Saat Anda membuat Akun AWS, Anda memberikan alamat email dan kata sandi. Ini adalah kredensial untuk Pengguna root akun AWS. Jika Anda tidak yakin dengan alamat email yang terkait dengan alamat email Anda Akun AWS, cari korespondensi tersimpan yang diakhiri dengan @signin .aws atau @verify .signin.aws ke alamat email apa pun untuk organisasi Anda yang mungkin telah digunakan untuk membuka. Akun AWS Tanyakan kepada anggota lain dari tim, organisasi, atau keluarga Anda. Jika seseorang yang Anda kenal membuat akun, mereka dapat membantu Anda mendapatkan akses.

Jika Anda mengetahui alamat email tetapi tidak lagi memiliki akses ke email, coba pulihkan akses ke email terlebih dahulu menggunakan salah satu opsi berikut:

- Jika Anda memiliki domain untuk alamat email, Anda dapat mengembalikan alamat email yang dihapus. Atau, Anda dapat menyiapkan catch-all untuk akun email Anda, yang mengirimkan pesan “menangkap semua” ke alamat email yang tidak lagi ada di server email dan mengarahkannya ke alamat email lain.
- Jika alamat email pada akun adalah bagian dari sistem email perusahaan Anda, kami sarankan untuk menghubungi administrator sistem IT Anda. Mereka mungkin dapat membantu Anda mendapatkan akses ke email tersebut.

Jika Anda masih tidak dapat masuk Akun AWS, Anda dapat menemukan opsi dukungan alternatif dengan menghubungi Dukungan.

Perangkat MFA saya hilang atau berhenti bekerja

Jika perangkat MFA Anda hilang, rusak, atau tidak berfungsi, Anda tidak menerima kode sandi satu kali (OTP) saat mengirim permintaan verifikasi MFA.

Pengguna IAM:

Anda dapat masuk menggunakan perangkat MFA lain yang terdaftar ke pengguna IAM yang sama.

Pengguna IAM harus menghubungi administrator untuk menonaktifkan perangkat MFA yang tidak berfungsi. Pengguna ini tidak dapat memulihkan perangkat MFA mereka tanpa bantuan administrator. Administrator Anda biasanya adalah personel Teknologi Informasi (TI) yang

memiliki tingkat izin yang lebih tinggi Akun AWS daripada anggota organisasi Anda yang lain. Individu ini membuat akun Anda dan memberi pengguna kredensi akses mereka untuk masuk.

Pengguna root

Untuk memulihkan akses ke pengguna root, Anda harus masuk menggunakan perangkat MFA lain yang terdaftar ke pengguna root yang sama. Kemudian, tinjau opsi berikut untuk memulihkan atau memperbarui perangkat MFA Anda:

- Untuk petunjuk langkah demi langkah untuk memulihkan perangkat MFA, lihat Bagaimana jika perangkat MFA hilang atau berhenti bekerja?
- Untuk petunjuk langkah demi langkah tentang cara memperbarui nomor telepon untuk perangkat MFA, lihat Bagaimana cara memperbarui nomor telepon saya untuk mengatur ulang perangkat MFA saya yang hilang?
- Untuk petunjuk langkah demi langkah untuk mengaktifkan perangkat MFA, lihat Mengaktifkan perangkat MFA untuk pengguna di. AWS
- Jika Anda tidak dapat memulihkan perangkat MFA Anda, hubungi. Dukungan

> **Note**
>
> Pengguna IAM harus menghubungi administrator mereka untuk mendapatkan bantuan dengan perangkat MFA. Dukungan tidak dapat membantu pengguna IAM dengan masalah perangkat MFA.

Saya tidak bisa mengakses Konsol Manajemen AWS halaman masuk

Jika Anda tidak dapat melihat halaman login, domain mungkin diblokir oleh firewall. Hubungi administrator jaringan Anda untuk menambahkan domain atau titik akhir URL berikut ke daftar izin solusi pemfilteran konten web Anda tergantung pada jenis pengguna Anda dan cara Anda masuk.

Pengguna root dan pengguna IAM	*.signin.aws.amazon.com
Amazon.com masuk akun	www.amazon.com
Pengguna IAM Identity Center dan masuk aplikasi pihak pertama	• *.awsapps.com () http://awsapps.com/ • *.signin.aws

Saya tidak dapat masuk karena kondisi jaringan dalam kebijakan berbasis Sign-in sumber daya

Jika Anda melihat salah satu pesan galat berikut, kebijakan Sign-in berbasis sumber daya atau kebijakan kontrol sumber daya (RCP) mungkin membatasi akses berdasarkan lokasi jaringan Anda:

- “Informasi otentikasi Anda salah. Silakan coba lagi.”
- “Otentikasi gagal Permintaan tidak valid”
- “Otentikasi gagal: Untuk mengakses akun ini, masuk dari jaringan lain, atau hubungi administrator Anda untuk informasi lebih lanjut”

Hubungi administrator Anda atau lihat langkah-langkah Saya tidak dapat masuk karena kondisi jaringan dalam kebijakan berbasis Sign-in sumber daya pemecahan masalah terperinci.

Saya terkunci dari akun saya setelah mengaktifkan otorisasi konsol

Jika Anda mengonfigurasi otorisasi konsol dan tidak dapat lagi mengakses akun, Anda mungkin belum mengonfigurasi prinsipal yang dikecualikan atau akses pemulihan darurat sebelum menerapkan kebijakan. Untuk langkah-langkah resolusi termasuk layanan mandiri AWS CLI, opsi, `OrganizationAccountAccessRole` dan AWS Dukungan, lihat. Saya terkunci dari akun saya setelah mengaktifkan otorisasi konsol

Perubahan kebijakan saya tidak berlaku

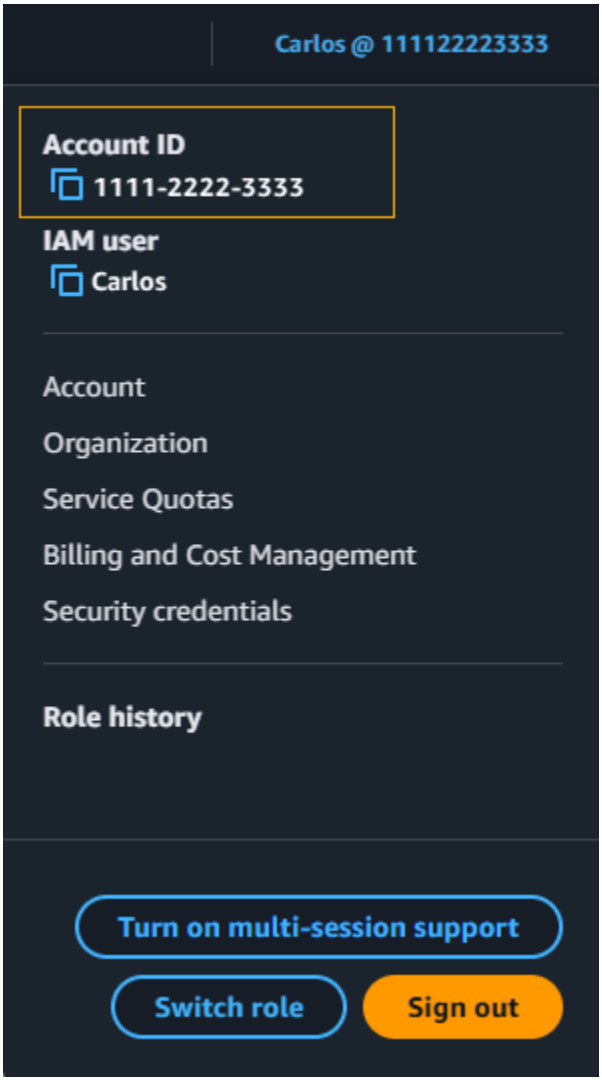
Perubahan pada konfigurasi otorisasi konsol dan pernyataan izin sumber daya mereplikasi secara global dan mungkin memerlukan beberapa menit untuk diterapkan. Jika perubahan Anda tidak terlihat setelah menunggu, lihat langkah Perubahan yang saya buat tidak selalu langsung terlihat pemecahan masalah.

Bagaimana saya bisa menemukan Akun AWS ID atau alias

Jika Anda adalah pengguna IAM dan Anda tidak masuk, tanyakan administrator Anda untuk Akun AWS ID atau alias. Administrator Anda biasanya adalah personel Teknologi Informasi (TI) yang memiliki tingkat izin yang lebih tinggi Akun AWS daripada anggota organisasi Anda yang lain. Individu ini membuat akun Anda dan memberi pengguna kredensi akses mereka untuk masuk.

Jika Anda adalah pengguna IAM dengan akses ke Konsol Manajemen AWS, ID akun Anda dapat ditemukan di URL login Anda. Periksa email Anda dari administrator untuk URL masuk. ID akun adalah dua belas digit pertama di URL masuk. Misalnya, di URL berikut, `https://111122223333.signin.aws.amazon.com/console` Akun AWS ID Anda adalah 111122223333.

Setelah Anda masuk ke Konsol Manajemen AWS, Anda dapat menemukan informasi akun Anda yang terletak di bilah navigasi di sebelah Wilayah Anda. Misalnya pada tangkapan layar berikut, pengguna IAM Carlos memiliki 1111-2222-3333 Akun AWS .



Untuk informasi selengkapnya tentang Akun AWS ID dan alias Anda serta cara menemukannya, lihat Akun AWS ID Anda dan aliasnya.

Saya perlu kode verifikasi akun saya

Jika Anda memberikan alamat email dan kata sandi akun Anda, AWS terkadang mengharuskan Anda untuk memberikan kode verifikasi satu kali. Untuk mengambil kode verifikasi, periksa email yang terkait dengan Anda Akun AWS untuk pesan dari Amazon Web Services. Alamat email diakhiri dengan @signin .aws atau @verify .signin.aws. Ikuti petunjuk pada pesan. Jika Anda tidak melihat pesan di akun Anda, periksa folder spam dan sampah Anda. Jika Anda tidak lagi memiliki akses ke email tersebut, lihat Saya tidak memiliki akses ke email untuk saya Akun AWS.

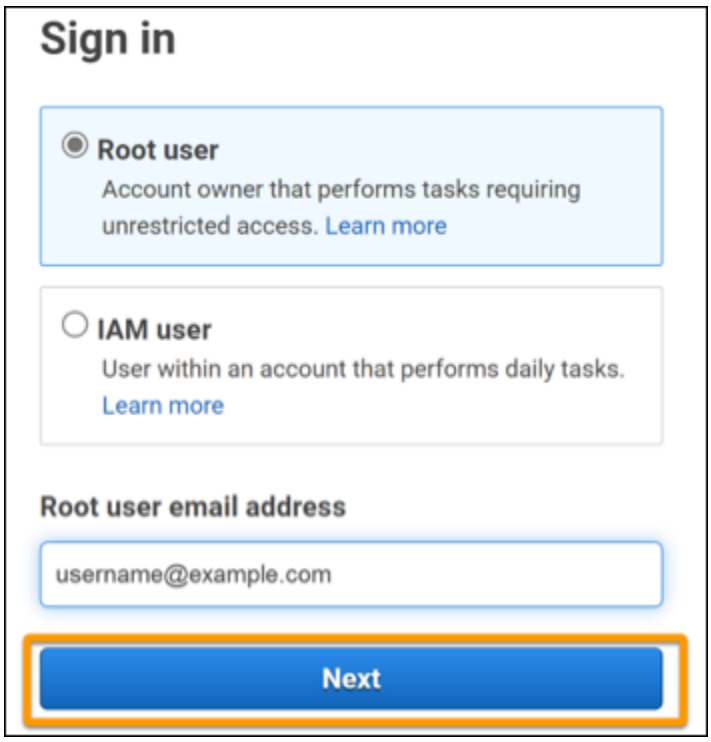
Saya lupa kata sandi pengguna root saya untuk saya Akun AWS

Jika Anda adalah pengguna root dan Anda telah kehilangan atau lupa kata sandi untuk Anda Akun AWS, Anda dapat mengatur ulang kata sandi Anda dengan memilih tautan “Lupa Kata Sandi” di Konsol Manajemen AWS. Anda harus mengetahui alamat email AWS akun Anda dan harus memiliki akses ke akun email. Anda akan dikirimi email tautan selama proses pemulihan kata sandi untuk mengatur ulang kata sandi Anda. Tautan akan dikirim ke alamat email yang Anda gunakan untuk membuat Akun AWS.

Untuk mengatur ulang kata sandi akun yang Anda buat menggunakan AWS Organizations, lihat Mengakses akun anggota sebagai pengguna root.

Untuk mengatur ulang kata sandi pengguna root Anda

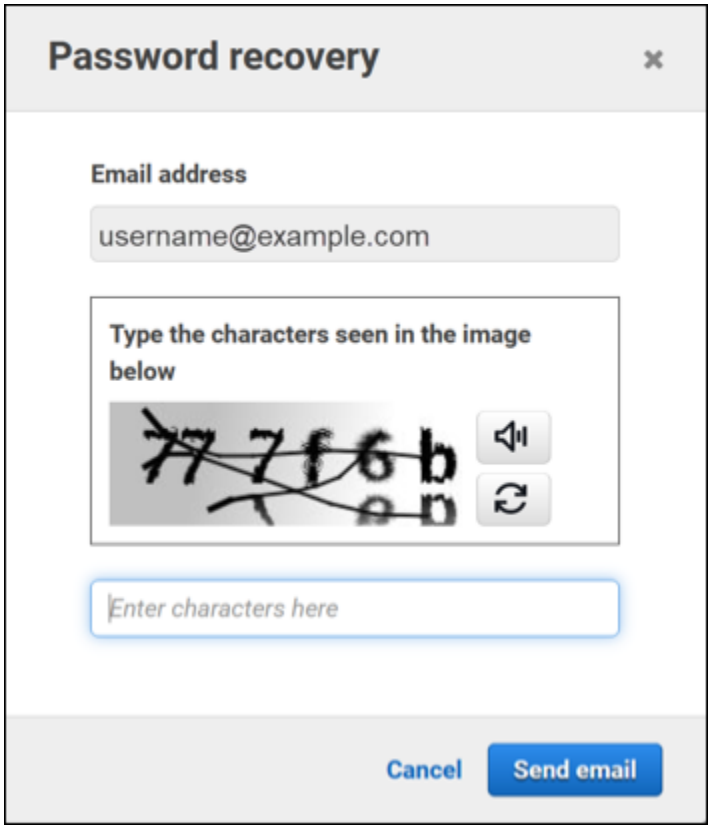
1. Gunakan alamat AWS email Anda untuk mulai masuk ke AWS Management Console sebagai pengguna root. Lalu, pilih Selanjutnya.



> **Note**
>
> Jika Anda masuk ke kredensi pengguna Konsol Manajemen AWSdengan IAM, maka Anda harus keluar sebelum Anda dapat mengatur ulang kata sandi pengguna root. Jika Anda melihat halaman login pengguna IAM khusus akun, pilih Sign-in menggunakan kredensi akun root di dekat bagian bawah halaman. Jika perlu, berikan alamat email akun Anda dan pilih Selanjutnya untuk mengakses halaman Masuk ke pengguna akar.

2. Pilih Lupa kata sandi?

3. Selesaikan langkah-langkah pemulihan kata sandi. Jika Anda tidak dapat menyelesaikan pemeriksaan keamanan, coba dengarkan audio atau segarkan pemeriksaan keamanan untuk set karakter baru. Contoh halaman pemulihan kata sandi ditunjukkan pada gambar berikut.

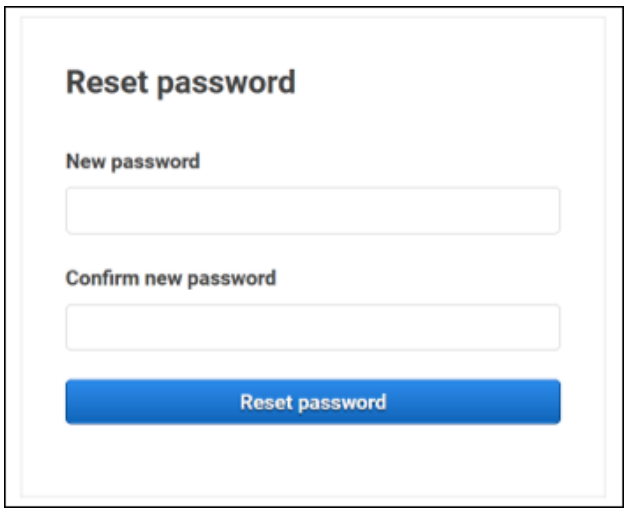


4. Setelah Anda menyelesaikan langkah-langkah pemulihan kata sandi, Anda menerima pesan bahwa instruksi lebih lanjut telah dikirim ke alamat email yang terkait dengan Anda Akun AWS.

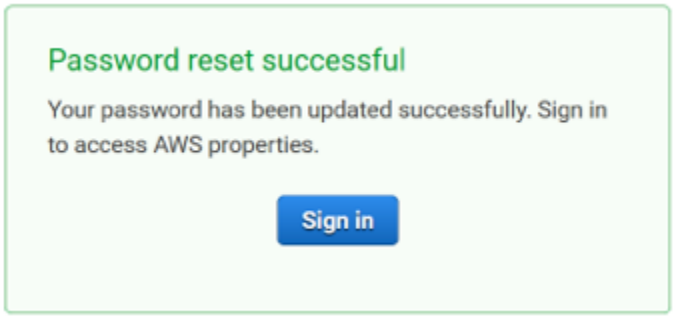
   Email dengan tautan untuk mengatur ulang kata sandi Anda dikirim ke email yang digunakan untuk membuat Akun AWS.

   > **Note**
   >
   > Email akan berasal dari alamat yang diakhiri dengan @signin .aws atau @verify .signin.aws.

5. Pilih tautan yang disediakan di AWS email untuk mengatur ulang kata sandi pengguna AWS root Anda.
6. Tautan mengarahkan Anda ke halaman web baru untuk membuat kata sandi pengguna root baru.



Anda menerima konfirmasi bahwa pengaturan ulang kata sandi Anda berhasil. Reset kata sandi yang berhasil ditunjukkan pada gambar berikut.

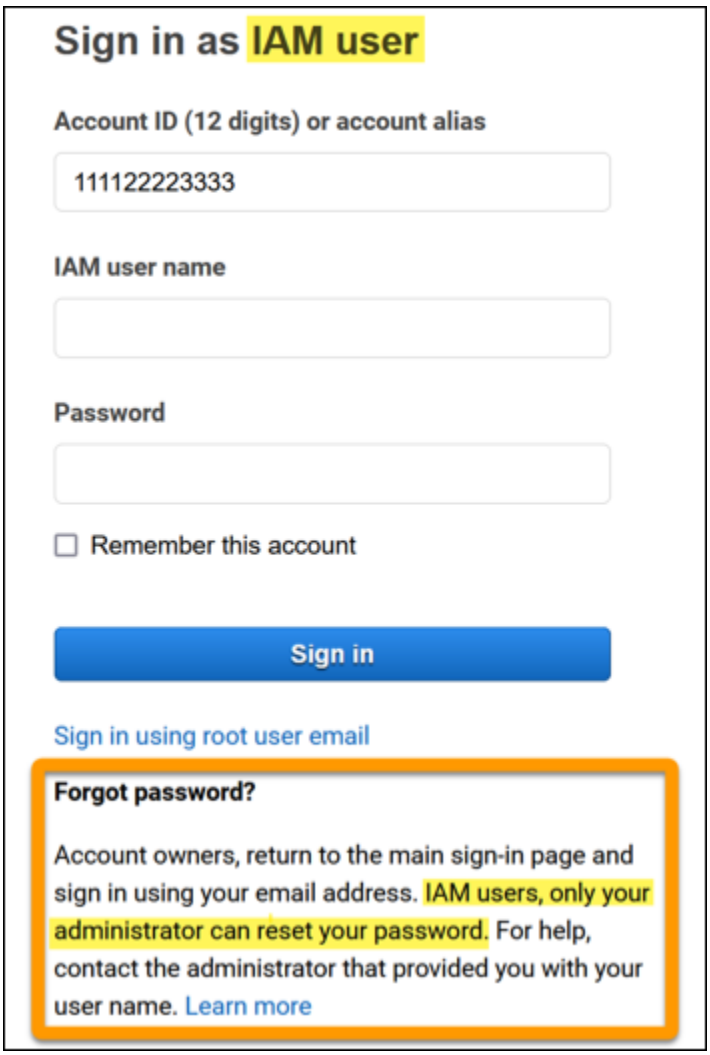


Untuk informasi selengkapnya tentang mengatur ulang kata sandi pengguna root Anda, lihat Bagaimana cara memulihkan kata AWS sandi yang hilang atau terlupakan?

Saya lupa kata sandi pengguna IAM saya untuk saya Akun AWS

Untuk mengubah kata sandi pengguna IAM Anda, Anda harus memiliki izin yang tepat. Untuk informasi selengkapnya tentang mengatur ulang kata sandi pengguna IAM Anda, lihat Cara pengguna IAM mengubah kata sandi mereka sendiri.

Jika Anda tidak memiliki izin untuk mengatur ulang kata sandi Anda, maka hanya administrator IAM Anda yang dapat mengatur ulang kata sandi pengguna IAM. Pengguna IAM harus menghubungi administrator IAM mereka untuk mengatur ulang kata sandi mereka. Administrator Anda biasanya adalah personel Teknologi Informasi (TI) yang memiliki tingkat izin yang lebih tinggi Akun AWS daripada anggota organisasi Anda yang lain. Individu ini membuat akun Anda dan memberi pengguna kredensi akses mereka untuk masuk.



Untuk tujuan keamanan, Dukungan tidak memiliki akses untuk melihat, menyediakan, atau mengubah kredensi Anda.

Untuk informasi selengkapnya tentang mengatur ulang kata sandi pengguna IAM Anda, lihat Bagaimana cara memulihkan kata sandi yang hilang atau terlupakan? AWS

Untuk mempelajari cara administrator mengelola kata sandi Anda, lihat Mengelola kata sandi untuk pengguna IAM.

Saya lupa kata sandi identitas federasi saya untuk Akun AWS

Identitas federasi masuk untuk mengakses Akun AWS dengan identitas eksternal. Jenis identitas eksternal yang digunakan menentukan bagaimana identitas federasi masuk. Administrator Anda membuat identitas federasi. Hubungi administrator Anda untuk detail selengkapnya tentang cara mengatur ulang kata sandi Anda. Administrator Anda biasanya adalah personel Teknologi Informasi

(TI) yang memiliki tingkat izin yang lebih tinggi Akun AWS daripada anggota organisasi Anda yang lain. Individu ini membuat akun Anda dan memberi pengguna kredensi akses mereka untuk masuk.

Saya tidak bisa masuk ke tempat saya yang ada Akun AWS dan saya tidak bisa membuat yang baru Akun AWS dengan alamat email yang sama

Anda dapat mengaitkan alamat email hanya dengan satu Pengguna root akun AWS. Jika Anda menutup akun pengguna root Anda dan tetap ditutup selama lebih dari 90 hari, maka Anda tidak dapat membuka kembali akun Anda atau membuat yang baru Akun AWS menggunakan alamat email yang terkait dengan akun ini.

Untuk memperbaiki masalah ini, Anda dapat menggunakan subaddressing di mana Anda menambahkan tanda plus (+) setelah alamat email Anda yang biasa ketika Anda mendaftar untuk akun baru. Tanda plus (+) dapat diikuti dengan huruf besar atau kecil, angka, atau karakter lain yang didukung Simple Mail Transfer Protocol (SMTP). Misalnya, Anda dapat menggunakan `email+1@yourcompany.com` atau `email+tag@yourcompany.com` di mana email biasa Anda beradaemail@yourcompany.com. Ini dianggap sebagai alamat baru meskipun terhubung ke kotak masuk yang sama dengan alamat email Anda yang biasa. Sebelum Anda mendaftar untuk akun baru, kami sarankan Anda mengirim email pengujian ke alamat email Anda yang ditambahkan untuk mengonfirmasi bahwa penyedia email Anda mendukung subaddressing.

Saya harus mengaktifkan kembali suspensi saya Akun AWS

Jika Anda Akun AWS ditangguhkan dan Anda ingin mengembalikannya, lihat Bagaimana saya bisa mengaktifkan kembali suspensi saya? Akun AWS

Saya perlu menghubungi Dukungan untuk masalah masuk

Jika Anda mencoba semuanya, Anda bisa mendapatkan bantuan Dukungan dengan menyelesaikan permintaan Billing and Account Support.

Saya perlu menghubungi AWS Billing untuk masalah penagihan

Jika Anda tidak dapat masuk Akun AWS dan ingin menghubungi AWS Billing untuk masalah penagihan, Anda dapat melakukannya melalui permintaan Penagihan dan Dukungan Akun. Untuk

informasi selengkapnya AWS Manajemen Penagihan dan Biaya, termasuk biaya dan metode pembayaran Anda, lihat Mendapatkan bantuan AWS Billing.

Saya punya pertanyaan tentang pesanan eceran

Jika Anda memiliki masalah dengan akun www.amazon.com Anda atau pertanyaan tentang pesanan ritel, lihat Opsi Dukungan & Hubungi Kami.

Saya butuh bantuan untuk mengelola Akun AWS

Jika Anda memerlukan bantuan untuk mengubah kartu kredit untuk Anda Akun AWS, melaporkan aktivitas penipuan, atau menutup Akun AWS, lihat Memecahkan masalah lainnya. Akun AWS

Saya AWS kredensyal portal akses tidak berfungsi

Jika Anda tidak dapat masuk ke portal AWS akses, coba ingat bagaimana Anda mengakses sebelumnya AWS.

Jika Anda tidak ingat menggunakan kata sandi sama sekali

Anda mungkin telah mengakses sebelumnya AWS tanpa menggunakan AWS kredensil. Ini umum untuk sistem masuk tunggal perusahaan melalui IAM Identity Center. Mengakses dengan cara AWS ini berarti Anda menggunakan kredensi perusahaan Anda untuk mengakses AWS akun atau aplikasi tanpa memasukkan kredensil Anda.

- AWS portal akses - Jika administrator mengizinkan Anda menggunakan kredensil dari luar AWS untuk mengakses AWS, Anda memerlukan URL untuk portal Anda. Periksa email, favorit browser, atau riwayat browser Anda untuk URL yang menyertakan `awsapps.com/start` atau`signin.aws/platform/login`.

  Misalnya, URL kustom Anda mungkin menyertakan ID atau domain seperti`https://d-1234567890.awsapps.com/start`. Jika Anda tidak dapat menemukan tautan portal Anda, hubungi administrator Anda. Dukungan tidak dapat membantu Anda memulihkan informasi ini.

Jika Anda ingat nama pengguna dan kata sandi Anda, tetapi kredensialnya tidak berfungsi, Anda mungkin berada di halaman yang salah. Lihat URL di browser web Anda, jika https://

signin.aws.amazon.com/ itu pengguna federasi atau pengguna Pusat Identitas IAM tidak dapat masuk menggunakan kredensialnya.

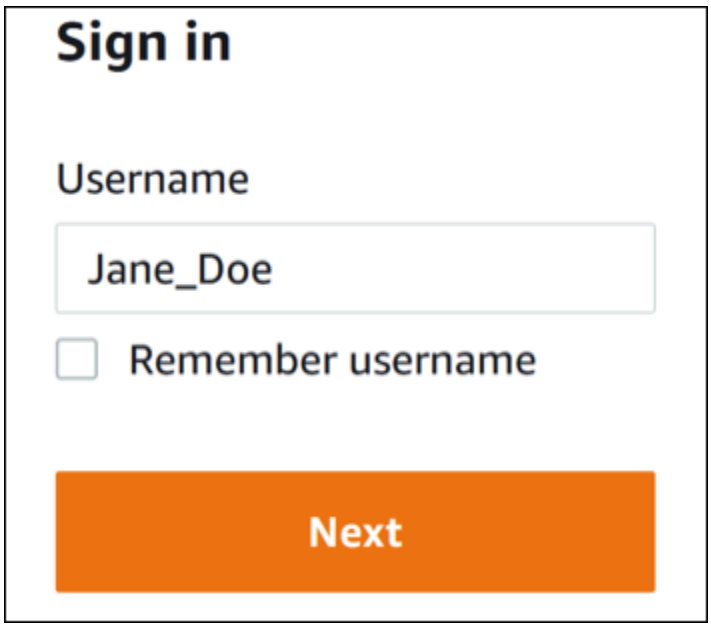
- AWS portal akses - Jika administrator menyiapkan sumber identitas Pusat AWS Identitas IAM (penerus AWS Tunggal Sign-On) AWS, Anda harus masuk menggunakan nama pengguna dan kata sandi di portal AWS akses untuk organisasi Anda. Untuk menemukan URL portal Anda, periksa email Anda, penyimpanan kata sandi aman, favorit browser, atau riwayat browser untuk URL yang menyertakan `awsapps.com/start` atau`signin.aws/platform/login`. Misalnya, URL kustom Anda mungkin menyertakan ID atau domain seperti `https://d-1234567890.awsapps.com/start`. Jika Anda tidak dapat menemukan tautan portal, hubungi administrator Anda. Dukungan tidak dapat membantu Anda memulihkan informasi ini.

Saya lupa kata sandi Pusat Identitas IAM saya untuk saya Akun AWS

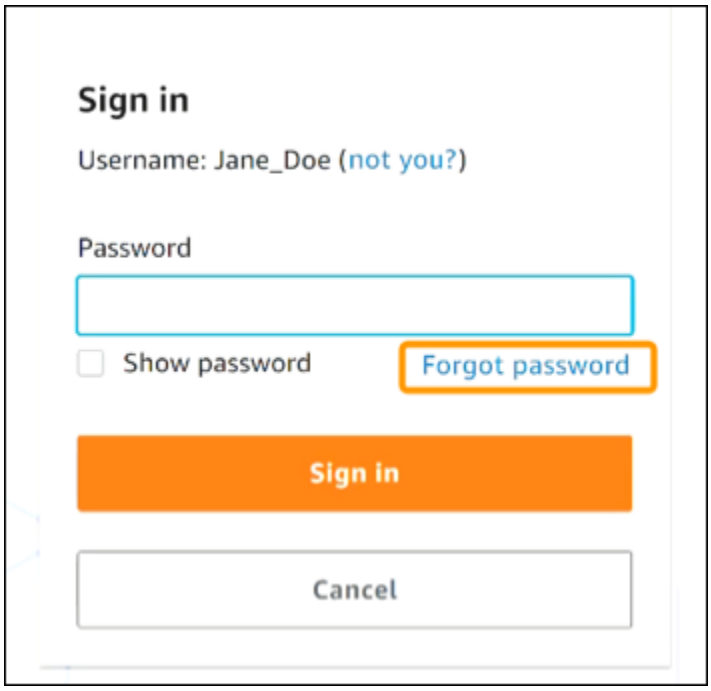
Jika Anda adalah pengguna di IAM Identity Center dan Anda telah kehilangan atau lupa kata sandi untuk Anda Akun AWS, Anda dapat mengatur ulang kata sandi Anda. Anda harus mengetahui alamat email yang digunakan untuk akun Pusat Identitas IAM dan memiliki akses ke sana. Tautan untuk mengatur ulang kata sandi Anda dikirim ke Akun AWS email Anda.

Untuk mengatur ulang pengguna Anda dengan kata sandi Pusat Identitas IAM

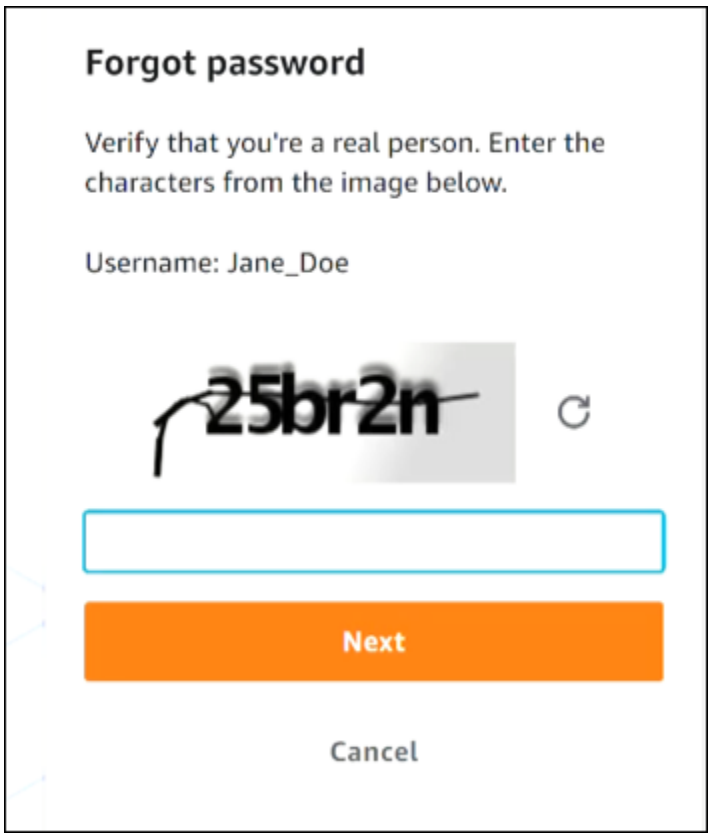
1. Gunakan tautan URL portal AWS akses Anda dan masukkan nama pengguna Anda. Lalu, pilih Selanjutnya.



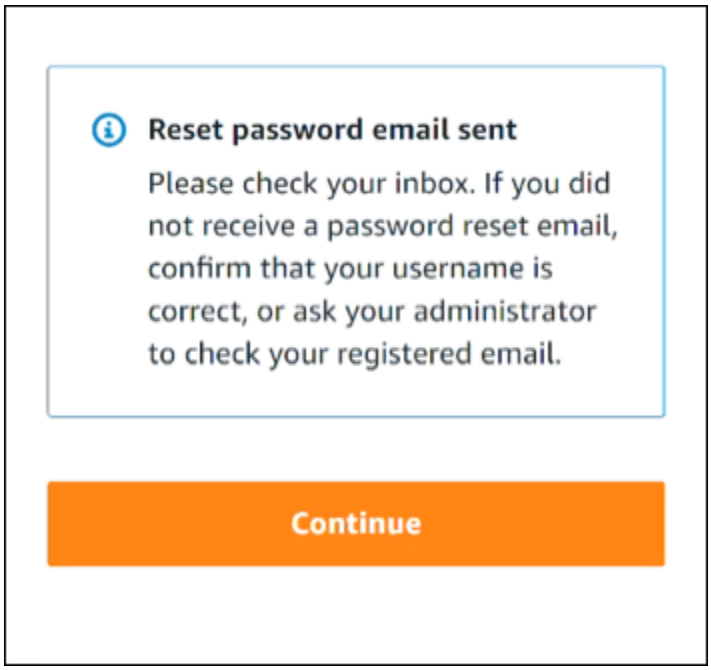
2. Pilih Lupa kata sandi seperti yang ditunjukkan pada gambar berikut.



3. Selesaikan langkah-langkah pemulihan kata sandi.



4. Setelah menyelesaikan langkah-langkah pemulihan kata sandi, Anda menerima pesan berikut yang mengonfirmasi bahwa Anda telah dikirimi pesan email yang dapat Anda gunakan untuk mengatur ulang kata sandi Anda.



Email dengan tautan untuk mengatur ulang kata sandi Anda dikirim ke email yang terkait dengan akun pengguna Pusat Identitas IAM. Pilih tautan yang disediakan di AWS email untuk mengatur ulang kata sandi Anda. Tautan mengarahkan Anda ke halaman web baru untuk membuat kata sandi baru. Setelah membuat kata sandi baru, Anda menerima konfirmasi bahwa pengaturan ulang kata sandi berhasil.

Jika Anda tidak menerima email untuk mengatur ulang kata sandi, mintalah administrator Anda untuk mengonfirmasi email mana yang terdaftar dengan pengguna Anda di Pusat Identitas IAM.

Saya menerima kesalahan yang menyatakan 'Bukan Anda, ini kami' ketika saya mencoba masuk ke konsol Pusat Identitas IAM

Kesalahan ini menunjukkan ada masalah penyiapan dengan instance Pusat Identitas IAM Anda atau penyedia identitas eksternal (iDP) yang digunakannya sebagai sumber identitasnya. Kami menyarankan Anda memverifikasi hal-hal berikut:

- Verifikasi pengaturan tanggal dan waktu pada perangkat yang Anda gunakan untuk masuk. Kami menyarankan agar Anda mengizinkan tanggal dan waktu diatur secara otomatis. Jika itu tidak tersedia, kami sarankan untuk menyinkronkan tanggal dan waktu Anda ke server Network Time Protocol (NTP) yang dikenal.
- Verifikasi bahwa sertifikat IDP yang diunggah ke IAM Identity Center sama dengan yang diberikan oleh penyedia identitas Anda. Anda dapat memeriksa sertifikat dari konsol Pusat Identitas IAM dengan menavigasi ke Pengaturan. Di tab Sumber Identitas, di bawah Tindakan, pilih Kelola Otentikasi. Anda mungkin perlu mengimpor sertifikat baru.
- Dalam file metadata SAMP IDP Anda, pastikan bahwa Format NameID adalah. `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
- Jika Anda menggunakan AD Connector, verifikasi bahwa kredensi untuk akun layanan sudah benar dan belum kedaluwarsa. Untuk informasi selengkapnya, lihat Memperbarui kredenal akun layanan AD Connector Anda di. Directory Service

Memecahkan masalah AWS Builder ID

Gunakan informasi di sini untuk membantu Anda memecahkan masalah yang mungkin Anda miliki dengan Anda. ID AWS Builder

Topik

- Saya mendapatkan pesan 'Bukan kamu, ini kami' ketika mencoba masuk ke Builder ID AWS
- Keluar tidak membuat saya keluar sepenuhnya
- Saya masih mencari untuk menyelesaikan masalah saya

Email saya sudah digunakan

Jika email yang Anda masukkan sudah digunakan dan Anda mengenalinya sebagai milik Anda, maka Anda mungkin sudah mendaftar untuk AWS Builder ID. Coba masuk menggunakan alamat email tersebut. Jika Anda tidak ingat kata sandi Anda, lihatSaya lupa kata sandi saya.

Saya tidak dapat menyelesaikan verifikasi email

Jika Anda mendaftar untuk AWS Builder ID tetapi belum menerima email verifikasi, selesaikan tugas pemecahan masalah berikut.

1. Periksa folder spam, sampah, dan item yang dihapus.

   > **Note**
   >
   > Email verifikasi ini berasal dari alamat no-reply@signin.aws atau no-reply@login.awsapps.com. Kami menyarankan Anda mengonfigurasi sistem surat Anda sehingga menerima email dari alamat email pengirim ini dan tidak menanganinya sebagai sampah atau spam.

2. Pilih Kirim ulang kode, segarkan kotak masuk Anda, dan periksa kembali folder spam, sampah, dan item yang dihapus.
3. Jika Anda masih tidak melihat email verifikasi, periksa kembali alamat email AWS Builder ID Anda untuk kesalahan ketik. Jika Anda memasukkan alamat email yang salah, daftar lagi dengan alamat email yang Anda miliki.

Saya tidak bisa masuk dengan Google

Jika Anda memiliki ID AWS Builder profil yang sudah ada dengan alamat email yang sama dengan akun Google Anda, gunakan ID AWS Builder kata sandi Anda untuk masuk ke akun Anda. Jika Anda tidak ingat kata sandi Anda, lihatSaya lupa kata sandi saya.

Untuk bantuan saat masuk dengan kata sandi Google, lihat Tidak dapat masuk ke Akun Google Anda.

Saya tidak bisa masuk dengan Apple

Jika Anda memiliki ID AWS Builder profil yang sudah ada dengan alamat email yang sama dengan Akun Apple Anda, gunakan ID AWS Builder kata sandi Anda untuk masuk ke akun Anda. Jika Anda tidak ingat kata sandi Anda, lihatSaya lupa kata sandi saya.

Untuk bantuan masuk dengan kata sandi Apple, lihat Jika Anda tidak dapat masuk ke Akun Apple.

Saya tidak bisa masuk dengan GitHub

Jika Anda memiliki ID AWS Builder profil yang sudah ada dengan alamat email yang sama dengan GitHub akun Anda, gunakan ID AWS Builder kata sandi Anda untuk masuk ke akun Anda. Jika Anda tidak ingat kata sandi Anda, lihatSaya lupa kata sandi saya.

Untuk bantuan masuk dengan GitHub kata sandi Anda, lihat Tidak dapat masuk - GitHub Support.

Saya tidak bisa masuk dengan Amazon

Jika Anda memiliki ID AWS Builder profil yang sudah ada dengan alamat email yang sama dengan akun Amazon Anda, gunakan ID AWS Builder kata sandi Anda untuk masuk ke akun Anda. Jika Anda tidak ingat kata sandi Anda, lihatSaya lupa kata sandi saya.

Untuk bantuan masuk dengan kata sandi Amazon Anda, lihat Bantuan untuk masuk.

Saya menerima kesalahan masuk ketika saya mencoba mendaftar untuk ID AWS Builder menggunakan lanjutkan dengan Google

Ini berarti bahwa Anda memiliki alamat email ID AWS Builder yang sama dengan Akun Google Anda, atau bahwa alamat email yang terkait dengan Akun Google Anda tidak diverifikasi. Dalam kedua kasus tersebut, silakan coba mendaftar lagi dengan memasukkan alamat email Anda dan memberikan kata sandi.

Saya menerima kesalahan masuk ketika saya mencoba mendaftar untuk ID AWS Builder menggunakan lanjutkan dengan Apple

Ini berarti bahwa Anda memiliki alamat email yang sama dengan Akun Apple Anda, atau bahwa alamat email yang terkait dengan Akun Apple Anda tidak diverifikasi atau dikelola oleh perusahaan Anda dengan Apple Business Manager atau oleh sekolah Anda dengan Apple School Manager. ID AWS Builder Dalam kedua kasus tersebut, silakan coba mendaftar lagi dengan memasukkan alamat email Anda dan memberikan kata sandi.

Saya menerima kesalahan masuk ketika saya mencoba mendaftar untuk ID AWS Builder menggunakan lanjutkan dengan GitHub

Ini berarti bahwa Anda memiliki alamat email ID AWS Builder yang sama dengan GitHub Akun Anda, atau bahwa alamat email yang terkait dengan GitHub Akun Anda tidak diverifikasi. Dalam kedua kasus tersebut, silakan coba mendaftar lagi dengan memasukkan alamat email Anda dan memberikan kata sandi.

Saya menerima kesalahan masuk ketika saya mencoba mendaftar untuk ID AWS Builder menggunakan lanjutkan dengan Amazon

Ini berarti bahwa Anda memiliki alamat email ID AWS Builder yang sama dengan Akun Amazon Anda, atau bahwa alamat email yang terkait dengan Akun Amazon Anda tidak diverifikasi. Dalam kedua kasus tersebut, silakan coba mendaftar lagi dengan memasukkan alamat email Anda dan memberikan kata sandi.

Saya menerima kesalahan yang menyatakan 'Bukan Anda, ini kami' ketika saya mencoba masuk dengan saya ID AWS Builder

Jika Anda menerima pesan galat ini saat mencoba masuk, mungkin ada masalah dengan pengaturan lokal atau alamat email Anda.

- Verifikasi pengaturan tanggal dan waktu pada perangkat yang Anda gunakan untuk masuk. Kami menyarankan agar Anda mengizinkan tanggal dan waktu diatur secara otomatis. Jika itu tidak tersedia, kami sarankan untuk menyinkronkan tanggal dan waktu Anda ke server Network Time Protocol (NTP) yang dikenal.

- Tinjau alamat email Anda untuk kesalahan pemformatan. Masalah berikut akan mengembalikan kesalahan saat mencoba masuk dengan Anda ID AWS Builder.
  - Spasi di alamat email
  - Teruskan garis miring (/) di alamat email
  - Dua periode (.) dalam alamat email
  - Dua ampersand (@) di alamat email
  - Koma (,) di akhir alamat email
  - Bracket (]) di akhir alamat email

Saya lupa kata sandi saya

Untuk mengatur ulang kata sandi Anda yang terlupakan

1. Pada halaman Masuk dengan AWS Builder ID, masukkan email yang Anda gunakan untuk membuat AWS Builder ID di alamat Email. Pilih Berikutnya.
2. Pilih Lupa kata sandi? . Kami mengirimkan tautan ke alamat email yang terkait dengan AWS Builder ID Anda di mana Anda dapat mengatur ulang kata sandi Anda.
3. Ikuti instruksi di email.

Saya tidak dapat mengatur kata sandi baru

Untuk keamanan Anda, Anda harus mengikuti persyaratan ini setiap kali Anda menetapkan atau mengubah kata sandi Anda:

- Kata sandi peka huruf besar/kecil.
- Kata sandi harus memiliki panjang antara 8 dan 64 karakter.
- Kata sandi harus mengandung setidaknya satu karakter dari masing-masing dari empat kategori berikut:
  - Huruf kecil (a-z)
  - Huruf besar (A-Z)
  - Angka (0-9)
  - Karakter non-alfanumerik (~! @#$%^portal manajemen*_-+=`|\ () {} []:; "'<>,.? /)
- Tiga kata sandi terakhir tidak dapat digunakan kembali.

- Kata sandi yang diketahui publik melalui kumpulan data yang bocor dari pihak ketiga tidak dapat digunakan.

Kata sandi saya tidak berfungsi

Jika Anda mengingat kata sandi, tetapi tidak berfungsi saat Anda masuk dengan AWS Builder ID, pastikan:

- Caps lock dimatikan.
- Anda tidak menggunakan kata sandi yang lebih lama.
- Anda menggunakan kata sandi AWS Builder ID Anda dan bukan kata sandi untuk Akun AWS.

Jika Anda memverifikasi bahwa kata sandi Anda up-to-date dan dimasukkan dengan benar, tetapi masih tidak berfungsi, ikuti instruksi Saya lupa kata sandi saya untuk mengatur ulang kata sandi Anda.

Kata sandi saya tidak berfungsi dan saya tidak dapat lagi mengakses email yang dikirim ke alamat email AWS Builder ID saya

Jika Anda masih dapat masuk ke AWS Builder ID Anda, gunakan halaman Profil untuk memperbarui email AWS Builder ID Anda ke alamat email baru Anda. Setelah Anda menyelesaikan verifikasi email, Anda dapat masuk AWS dan menerima komunikasi di alamat email baru Anda.

Jika Anda menggunakan alamat email kantor atau perguruan tinggi, dan telah meninggalkan perusahaan atau sekolah dan tidak dapat menerima email yang dikirim ke alamat itu, hubungi administrator sistem email tersebut. Mereka mungkin dapat meneruskan email Anda ke alamat baru, memberi Anda akses sementara, atau membagikan konten dari kotak pesan Anda.

Saya tidak bisa mengaktifkan MFA

Untuk mengaktifkan MFA, tambahkan satu atau beberapa perangkat MFA ke profil Anda dengan mengikuti langkah-langkah di. Kelola otentikasi ID AWS Builder multi-faktor (MFA)

Saya tidak dapat menambahkan aplikasi autentikator sebagai perangkat MFA

Jika Anda menemukan bahwa Anda tidak dapat menambahkan perangkat MFA lain, Anda mungkin telah mencapai batas perangkat MFA yang dapat Anda daftarkan di aplikasi itu. Coba hapus perangkat MFA yang tidak digunakan atau gunakan aplikasi autentikator yang berbeda.

Saya tidak dapat menghapus perangkat MFA

Jika Anda bermaksud menonaktifkan MFA, lanjutkan dengan menghapus perangkat MFA Anda dengan mengikuti langkah-langkah di. Hapus perangkat MFA Anda Namun, jika Anda ingin tetap mengaktifkan MFA, Anda harus menambahkan perangkat MFA lain sebelum mencoba menghapus perangkat MFA yang ada. Untuk informasi selengkapnya tentang menambahkan perangkat MFA lain, lihat. Kelola otentikasi ID AWS Builder multi-faktor (MFA)

Saya mendapatkan pesan 'Kesalahan tak terduga telah terjadi' ketika saya mencoba mendaftar atau masuk dengan aplikasi autentikator

Sistem kata sandi satu kali berbasis waktu (TOTP), seperti yang digunakan oleh AWS Builder ID dalam kombinasi dengan aplikasi autentikator berbasis kode, bergantung pada sinkronisasi waktu antara klien dan server. Pastikan perangkat tempat aplikasi autentikator diinstal disinkronkan dengan benar ke sumber waktu yang andal, atau atur waktu di perangkat secara manual agar sesuai dengan sumber terpercaya, seperti NIST atau setara lainnya. local/regional

Saya mendapatkan pesan 'Bukan kamu, ini kami' ketika mencoba masuk ke Builder ID AWS

Verifikasi pengaturan tanggal dan waktu pada perangkat yang Anda gunakan untuk masuk. Kami menyarankan Anda mengatur tanggal dan waktu yang akan diatur secara otomatis. Jika itu tidak tersedia, kami sarankan untuk menyinkronkan tanggal dan waktu Anda ke server Network Time Protocol (NTP) yang dikenal.

Keluar tidak membuat saya keluar sepenuhnya

Sistem ini dirancang untuk segera keluar, tetapi keluar penuh mungkin memakan waktu hingga satu jam.

> **Note**
>
> Saat menggunakan akun login sosial seperti Google atau Apple, menghapus ID AWS Builder sesi aktif tidak akan membuat Anda keluar dari akun login sosial Anda.

Saya masih mencari untuk menyelesaikan masalah saya

Anda dapat mengisi formulir Support Feedback. Di bagian Minta informasi, di bawah Bagaimana kami dapat membantu Anda, sertakan bahwa Anda menggunakan AWS Builder ID. Berikan detail sebanyak mungkin sehingga kami dapat mengatasi masalah Anda dengan paling efisien.

AWS kebijakan terkelola untuk AWS Sign-In

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pemutakhiran akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat Kebijakan terkelola AWS dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: AmazonManagedSignUpServicePolicy

`AmazonManagedSignUpServicePolicy`Kebijakan ini memberikan izin yang diperlukan untuk menyelesaikan proses pendaftaran AWS akun.

Anda dapat melampirkan `AmazonManagedSignUpServicePolicy` ke pengguna, grup, dan peran Anda.

Detail izin

Kebijakan ini mencakup izin berikut:

- Verifikasi pelanggan - Memungkinkan membuat, mengambil, dan memperbarui detail verifikasi pelanggan dan status kelayakan, termasuk membuat URL unggahan untuk dokumen verifikasi.

Untuk melihat detail selengkapnya tentang kebijakan, termasuk versi terbaru dari dokumen kebijakan JSON, lihat AmazonManagedSignUpServicePolicydi Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: ApplicationProvisioningPolicy

ApplicationProvisioningPolicy Kebijakan ini memberikan izin komprehensif untuk penyediaan aplikasi dan operasi manajemen identitas, termasuk peran IAM dan manajemen kebijakan, konfigurasi SSO, dan operasi penyimpanan identitas.

Anda dapat melampirkan `ApplicationProvisioningPolicy` ke pengguna, grup, dan peran Anda.

Detail izin

Kebijakan ini mencakup izin berikut:

- Manajemen IAM - Memungkinkan operasi IAM yang komprehensif termasuk membuat, memperbarui, dan menghapus peran dan kebijakan, mengelola lampiran peran, dan membuat peran terkait layanan.
- Studio Penelitian dan Rekayasa di AWS- Memungkinkan semua operasi pada Studio Penelitian dan Rekayasa di AWS sumber daya.
- Role passing - Memungkinkan meneruskan peran IAM ke layanan lain.
- IAM Identity Center - Memungkinkan mengelola instans IAM Identity Center, aplikasi, tugas, hibah, dan metode otentikasi.
- Identity Store - Memungkinkan membaca informasi pengguna dan grup dari Identity Store.
- IAM Identity Center OAuth - Memungkinkan otentikasi sesi IAM melalui IAM Identity Center OAuth.
- Profil Pengguna dan Direktori - Memungkinkan mengelola konektor Pusat Identitas IAM, profil pengguna, dan konfigurasi direktori termasuk pengaturan penyedia identitas eksternal.
- Langganan Pengguna - Memungkinkan daftar langganan pengguna.

Untuk melihat detail selengkapnya tentang kebijakan, termasuk versi terbaru dari dokumen kebijakan JSON, lihat ApplicationProvisioningPolicydi Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: SignInLocalDevelopmentAccess

`SignInLocalDevelopmentAccess`Kebijakan ini memberikan izin untuk akses terprogram untuk AWS menggunakan kredenal konsol Anda.

Anda dapat melampirkan `SignInLocalDevelopmentAccess` ke pengguna, grup, dan peran Anda.

Detail izin

Kebijakan ini mencakup izin berikut:

- Mengotorisasi akses OAuth2 - Memberikan izin untuk mengautentikasi melalui browser dan mendapatkan kode otorisasi OAuth 2.0 untuk pertukaran kredensi
- Pembuatan token OAuth2 - Memberikan izin untuk menukar kode otorisasi untuk token akses OAuth 2.0 dan token penyegaran yang dapat digunakan untuk mengakses AWS layanan dari alat dan aplikasi pengembang

> **Note**
>
> Menambahkan kebijakan AWS terkelola ini memberi Anda izin untuk autentikasi perangkat dan lintas perangkat yang sama. Kebijakan ini mengotorisasi tindakan pada sumber daya berikut:
>
> - `arn:aws:signin:region:account-id:oauth2/public-client/localhost`— Digunakan untuk otentikasi perangkat yang sama dengan. `aws login`
> - `arn:aws:signin:region:account-id:oauth2/public-client/remote`— Digunakan untuk otentikasi lintas-perangkat dengan. `aws login --remote`
>
> Untuk mengontrol akses ke salah satu metode otentikasi, Anda dapat membuat kebijakan terkelola atau kebijakan kontrol layanan (SCP) Anda sendiri. Gunakan ARN sumber daya ini untuk mengizinkan atau menolak akses terprogram ke AWS menggunakan kredenal konsol Anda.

Untuk informasi selengkapnya, lihat Login dengan kredenal konsol (Disarankan). Untuk melihat detail selengkapnya tentang kebijakan, termasuk versi terbaru dari dokumen kebijakan JSON, lihat SignInLocalDevelopmentAccessdi Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: AWSSignInResourcePolicyManagement

`AWSSignInResourcePolicyManagement`Kebijakan ini memberikan izin untuk mengelola konfigurasi otorisasi konsol dan pernyataan izin sumber daya untuk. AWS Sign-In

Anda dapat melampirkan `AWSSignInResourcePolicyManagement` ke pengguna, grup, dan peran Anda.

Detail izin

Kebijakan ini mencakup izin berikut:

- `signin:PutConsoleAuthorizationConfiguration`— Buat atau perbarui pengaturan otorisasi konsol.
- `signin:GetConsoleAuthorizationConfiguration`— Ambil konfigurasi otorisasi konsol saat ini.
- `signin:DeleteConsoleAuthorizationConfiguration`— Hapus konfigurasi otorisasi konsol.
- `signin:PutResourcePermissionStatement`— Buat atau perbarui pernyataan izin sumber daya.
- `signin:DeleteResourcePermissionStatement`— Hapus pernyataan izin sumber daya.
- `signin:ListResourcePermissionStatements`— Daftar pernyataan izin sumber daya untuk akun.
- `signin:GetResourcePolicy`— Mengambil kebijakan berbasis sumber daya terkonsolidasi.

Berikut ini adalah kebijakan JSON:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "signin:PutConsoleAuthorizationConfiguration",
                "signin:GetConsoleAuthorizationConfiguration",
                "signin:DeleteConsoleAuthorizationConfiguration",
                "signin:PutResourcePermissionStatement",
                "signin:DeleteResourcePermissionStatement",
                "signin:ListResourcePermissionStatements",
                "signin:GetResourcePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Lampirkan kebijakan ini ke kepala sekolah IAM (pengguna atau peran) yang mengelola kebijakan berbasis sumber daya untuk. AWS Sign-In Ini termasuk administrator keamanan yang bertanggung jawab untuk mengonfigurasi kontrol akses berbasis jaringan, petugas kepatuhan yang perlu mengaudit kebijakan akses konsol, dan tim operasi yang mengelola konfigurasi akses pemulihan darurat.

> **Important**
>
> Kebijakan ini memberikan akses administratif ke kontrol otorisasi konsol. Terapkan prinsip hak istimewa paling sedikit saat menetapkan kebijakan ini. Pertimbangkan untuk menggunakan kondisi IAM untuk lebih membatasi kapan dan bagaimana izin ini dapat digunakan.

Untuk melihat detail selengkapnya tentang kebijakan, termasuk versi terbaru dari dokumen kebijakan JSON, lihat AWSSignInResourcePolicyManagementdi Panduan Referensi Kebijakan AWS Terkelola.

AWS Sign-In update ke AWS kebijakan terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola AWS Sign-In sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman Riwayat AWS Sign-In dokumen.

Ubah	Deskripsi	Date
AWSSignInResourcePolicyManagement – Kebijakan baru	Menambahkan kebijakan AWS terkelola baru yang memberikan izin untuk mengelola konfigurasi otorisasi konsol dan pernyataan izin sumber daya untuk. AWS Sign-In	Juni 10, 2026
SignInLocalDevelopmentAccess – Kebijakan baru	Menambahkan kebijakan AWS terkelola baru yang memberikan izin untuk akses terprogram untuk AWS	November 19, 2025

Ubah	Deskripsi	Date
	menggunakan kredenal konsol yang ada.	
ApplicationProvisioningPolicy – Kebijakan baru	Menambahkan kebijakan AWS terkelola baru yang memberikan izin komprehen sif untuk penyediaan aplikasi dan operasi manajemen identitas, termasuk peran IAM dan manajemen kebijakan , konfigurasi Pusat Identitas IAM, dan operasi Toko Identitas.	September 30, 2025
AmazonManagedSignU pServicePolicy – Kebijakan baru	Menambahkan kebijakan AWS terkelola baru yang memberikan izin yang diperlukan untuk proses pendaftaran AWS akun, termasuk verifikasi pelanggan dan operasi penyiapan pembayaran.	September 30, 2025
AWS Sign-In mulai melacak perubahan	AWS Sign-In mulai melacak perubahan untuk kebijakan AWS terkelolanya.	September 30, 2025

Riwayat dokumen

Tabel berikut menjelaskan penambahan penting pada AWS Sign-In dokumentasi. Kami juga rutin memperbarui dokumentasi untuk menjawab umpan balik yang Anda kirimkan kepada kami.

- Pembaruan dokumentasi utama terbaru: 10 Juni 2026

Perubahan	Deskripsi	Tanggal
Support untuk kebijakan Sign-in berbasis sumber daya dan kebijakan pengendalian sumber daya	Menambahkan dokumentasi untuk mengontrol Konsol Manajemen AWS akses dengan menggunakan kebijakan Sign-in berbasis sumber daya dan kebijakan kontrol sumber daya (RCP), referensi kunci kondisi baru, kebijakan `AWSSignInResourcePolicyManagement` terkelola, dan pemecahan masalah terkait.	Juni 10, 2026
Support untuk Masuk dengan GitHub dan Amazon	AWS Sign-In sekarang mendukung Masuk dengan GitHub dan Masuk dengan Amazon sehingga Anda dapat membuat ID AWS Builder menggunakan Akun Amazon GitHub atau Anda.	10 Maret 2026
Support untuk Masuk dengan Apple	AWS Sign-In sekarang mendukung Masuk dengan Apple sehingga Anda dapat membuat ID AWS Builder menggunakan Akun Apple Anda. ID AWS Builder	Februari 5, 2026

	topik diperbarui dan topik pemecahan masalah baru ditambahkan ke masalah Pemecahan masalah ID AWS Builder.	
Kebijakan Terkelola Baru	AWS Sign-In telah merilis kebijakan terkelola baru. `SignInLocalDevelopmentAccess` memberikan izin untuk akses terprogram untuk akses terprogram untuk AWS menggunakan kredenal konsol yang ada. Untuk selengkapnya, lihat AWS Sign-In pembaruan kebijakan AWS terkelola.	November 19, 2025
Support untuk Masuk dengan Google	AWS Sign-In sekarang mendukung Masuk dengan Google sehingga Anda dapat membuat ID AWS Builder menggunakan Akun Google Anda. ID AWS Builder topik diperbarui dan topik pemecahan masalah baru ditambahkan ke masalah Pemecahan masalah ID AWS Builder.	September 30, 2025

Kebijakan terkelola baru	AWS Sign-In telah merilis dua kebijakan terkelola baru. `AmazonManagedSignUpServicePolicy` memberikan izin yang diperlukan untuk menyelesaikan proses pendaftaran AWS akun. `ApplicationProvisioningPolicy` memberikan izin komprehensif untuk penyediaan aplikasi dan operasi manajemen identitas. Untuk selengkapnya, lihat AWS Sign-In pembaruan kebijakan AWS terkelola.	September 30, 2025
Topik pemecahan masalah yang diperbarui	Menambahkan topik pemecahan masalah baru untuk masuk ID AWS Builder dan. Konsol Manajemen AWS	Februari 27, 2024
Memperbarui beberapa topik untuk organisasi	Jenis Pengguna yang Diperbarui, Dihapus Tentukan jenis pengguna dan masukkan kontennya ke dalam tipe Pengguna, Cara masuk ke AWS	15 Mei 2023
Diperbarui beberapa topik dan spanduk teratas	Jenis Pengguna yang Diperbarui, Tentukan jenis pengguna AWS, Cara masuk, Apa itu AWS Sign-in? . Juga memperbarui prosedur pengguna root dan pengguna IAM.	3 Maret 2023

Paragraf intro yang diperbarui untuk Konsol Manajemen AWS masuk	Dipindahkan Tentukan jenis pengguna ke bagian atas halaman dan hapus catatan yang ada di pengguna root Akun.	27 Februari 2023
Ditambahkan ID AWS Builder	Menambahkan ID AWS Builder topik ke Panduan AWS Sign-In Pengguna dan konten terintegrasi ke dalam topik yang ada.	31 Januari 2023
Pembaruan organisasi	Berdasarkan umpan balik pelanggan, memperbarui TOC agar lebih jelas tentang metode masuk. Memperbarui tutorial masuk. Terminologi yang Diperbarui dan Tentukan tipe pengguna. Peningkatan cross-linking untuk mendefinisikan istilah seperti pengguna IAM dan pengguna root.	22 Desember 2022
Panduan baru	Ini adalah rilis pertama dari Panduan AWS Sign-In Pengguna.	31 Agustus 2022

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.