



Panduan Pengguna

# Amazon Satu



# Amazon Satu: Panduan Pengguna

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

---

# Table of Contents

Apa itu Amazon One Enterprise? .....	1
Perangkat Amazon One .....	1
Konsol Amazon One Enterprise .....	2
Membeli perangkat Amazon One .....	3
Harga Amazon One Enterprise .....	3
Bagaimana Amazon One bekerja .....	4
Alur kerja Amazon One .....	4
Amazon Salah satu istilah kunci .....	5
Menyiapkan konsol Amazon One .....	6
Mendaftar untuk akun AWS .....	6
Buat pengguna dengan akses administratif .....	7
Mengamankan akun AWS Anda .....	7
Membuat pengguna dengan akses administratif .....	7
Masuk sebagai administrator .....	8
Menetapkan akses ke pengguna tambahan .....	8
Tambahkan pengguna Amazon One .....	9
Buat situs .....	11
Buat instance perangkat .....	12
Buat templat konfigurasi .....	12
Konfigurasi instance perangkat untuk aktivasi .....	14
Menginstal dan mengaktifkan Amazon One .....	16
Memahami persyaratan .....	16
Standar yang didukung .....	16
Persyaratan jaringan .....	17
Kebutuhan daya .....	17
Memahami konsep instalasi .....	17
Memasang Amazon One Pedestal .....	18
Memasang perangkat Amazon One yang dapat dipasang di dinding .....	20
Menginstal Amazon One Device I/O Hub untuk akses aman .....	29
Mengaktifkan perangkat Amazon One .....	33
Mendaftar dan memasukkan pengguna .....	35
Membuat kebijakan endpoint .....	35
Otentikasi untuk entri .....	35
Mengelola pengguna .....	36

Melihat pengguna terdaftar .....	36
Menghapus pengguna terdaftar dan biometrik mereka .....	36
Mengelola perangkat Amazon One .....	38
Memelihara dan membersihkan perangkat Amazon One .....	38
Untuk membersihkan perangkat Amazon One .....	39
Pengelolaan Situs .....	39
Mengubah nama situs .....	40
Memperbarui alamat situs .....	40
Manajemen Instans Perangkat .....	40
Melihat status instans perangkat .....	41
Mem-boot ulang perangkat Amazon One .....	41
Memperbarui konfigurasi perangkat Amazon One .....	41
Memperbarui kredensi Wi-fi .....	42
Menonaktifkan instance perangkat .....	42
Keamanan .....	44
Perlindungan data .....	44
Untuk menggunakan enkripsi default data saat istirahat .....	46
Mengkripsi data saat transit .....	46
Manajemen identitas dan akses .....	46
Audiens .....	46
Mengautentikasi dengan identitas .....	47
Mengelola akses menggunakan kebijakan .....	48
Bagaimana Amazon One Enterprise bekerja dengan IAM .....	50
Contoh kebijakan berbasis identitas .....	56
AWS kebijakan terkelola .....	64
Tindakan, sumber daya, dan kunci kondisi .....	67
Tindakan .....	67
Jenis sumber daya .....	72
Kunci syarat .....	73
Validasi kepatuhan .....	74
Memantau .....	75
Pemantauan peristiwa .....	75
Berlangganan acara Amazon One Enterprise .....	75
Jenis peristiwa perubahan status perangkat .....	77
Jenis acara profil pengguna .....	78
Contoh acara .....	79

Status kesehatan perangkat berubah menjadi sehat .....	79
Status kesehatan perangkat berubah menjadi kritis .....	80
Konektivitas perangkat diubah menjadi online .....	81
Konektivitas perangkat diubah menjadi offline .....	82
CloudTrail log .....	83
Informasi Amazon One Enterprise di CloudTrail .....	84
Memahami entri file log Amazon One Enterprise .....	85
Pemecahan masalah .....	87
Pemecahan masalah identitas dan akses .....	87
Saya tidak berwenang untuk melakukan tindakan di Amazon One .....	87
Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Amazon One saya .....	88
Memecahkan Masalah Konsol Amazon One .....	88
Saya tidak dapat membuat situs .....	89
Saya tidak dapat membuat instance perangkat .....	89
Saya tidak dapat membuat templat konfigurasi .....	89
Saya tidak dapat membuat kode QR aktivasi .....	89
Memecahkan masalah perangkat Amazon One .....	89
Layar kosong .....	90
Saya tidak dapat terhubung ke Wi-Fi atau jaringan .....	91
Mem-boot ulang perangkat dengan peringatan aktif .....	91
Kesalahan sistem .....	91
Kode QR tidak dikenali .....	92
Tidak dapat membaca kode QR .....	92
Beberapa kode QR terdeteksi .....	92
Instans perangkat tidak ada .....	92
Situs tidak ditemukan .....	93
Kode Pos tidak cocok .....	93
Gateway habis waktu .....	93
Saya tidak dapat mengonfigurasi perangkat .....	93
Perangkat dimulai ulang dengan pesan kesalahan dan kode kesalahan .....	94
Logo Amazon di layar perangkat tanpa aktivitas lebih lanjut .....	94
Tidak tersedia untuk sementara .....	94
Ada yang tidak beres di pihak kami .....	94
Sementara keluar dari layanan .....	95
Perangkat Amazon One mengalami kerusakan fisik .....	95

---

Tidak dapat membaca telapak tangan .....	95
Telapak tangan tidak dikenali .....	95
Perangkat terkunci karena ketidakaktifan yang diperpanjang .....	96
Perangkat terkunci karena peristiwa tamper .....	96
Riwayat dokumen .....	97
.....	xcix

# Apa itu Amazon One Enterprise?

Amazon One Enterprise adalah layanan otentikasi berbasis sawit baru yang memberi karyawan akses aman ke gedung dan aset perusahaan, tanpa menggunakan lencana,, atau kode sandi. PINs

## Topik

- [Perangkat Amazon One](#)
- [Konsol Amazon One Enterprise](#)
- [Membeli perangkat Amazon One](#)
- [Harga Amazon One Enterprise](#)

## Perangkat Amazon One

Perangkat Amazon One dirancang untuk Amazon One Enterprise, layanan identitas berbasis telapak tangan yang aman untuk kontrol akses perusahaan. Perhatikan spesifikasi perangkat berikut:

- Masukan pengguna — Biometrik Palm, pencocokan Kode QR
- Antarmuka host - Wi-Fi (2.4 GHz dan 5 GHz), Ethernet, 2x USB Tipe-A, 1 USB Tipe-B
- Umpan balik pengguna - Layar Sentuh 5,5 “, Lightring, speaker, headphone
- Protokol Kontrol Akses Fisik - OSDP dan Wiegand
- Catu daya - POE, 110/220 VAC input AC ke adaptor DC disediakan, 30W @ 15V
- Keamanan - Sakelar tamper
- Dimensi (HxWxD mm) — 86 x 85 x 256



## Konsol Amazon One Enterprise

Amazon One Enterprise menyertakan konsol, yang dapat digunakan dengan cara-cara berikut:

- Manajer TI atau fasilitas menggunakan Amazon One Enterprise untuk membuat dan mengelola situs. Situs ini menyerupai lokasi fisik untuk tugas-tugas yang dilakukan tim saat memantau dan mengelola perangkat Amazon One Enterprise dan profil pengguna. Tugas manajer TI atau fasilitas meliputi:
  - Membuat situs yang berisi semua instance perangkat Amazon One di lokasi fisik
  - Menambahkan pengguna admin untuk mengelola situs, dan pengguna installer untuk mengakses kode QR aktivasi
- Admin menggunakan Amazon One Enterprise untuk membuat instance perangkat dan mengelola perangkat Amazon One. Tugas admin meliputi:
  - Membuat instance perangkat di bawah situs
  - Membuat template konfigurasi untuk diterapkan ke instance perangkat
  - Memantau kesehatan perangkat dan memperbarui konfigurasi perangkat
  - Membatalkan pendaftaran pengguna

- Penginstal menggunakan Amazon One Enterprise untuk mengakses kode QR aktivasi untuk mengaktifkan perangkat. Tugas penginstal meliputi:
  - Mengakses kode QR aktivasi di konsol
  - Memilih kode QR yang sesuai dengan instance perangkat yang akan diaktifkan
  - Memindai kode QR yang dipilih dengan perangkat Amazon One diinstal

## Membeli perangkat Amazon One

[Hubungi kami](#) untuk mempelajari lebih lanjut tentang Amazon One Enterprise, dan anggota tim Pengembangan Bisnis akan menghubungi kami untuk membagikan detail lebih lanjut tentang penawaran kami, termasuk harga, dan menjawab pertanyaan apa pun yang mungkin Anda miliki.

## Harga Amazon One Enterprise

[Hubungi kami](#) untuk mempelajari lebih lanjut tentang harga Amazon One Enterprise.

# Bagaimana Amazon One bekerja

Amazon One adalah layanan biometrik berbasis cloud yang menggunakan perangkat Amazon One untuk mengautentikasi pengguna dengan biometrik telapak tangan mereka. Anda dapat memesan perangkat Amazon One dengan [menghubungi kami](#).

Setelah menginstal perangkat Amazon One, Anda dapat mengaktifkan dan mendaftarkan perangkat Anda dengan akun AWS Anda di Amazon One Console dan aplikasi otentikasi. Anda dapat melihat profil biometrik pengguna terdaftar. Jika diperlukan, Anda dapat membatalkan pendaftaran mereka dan menghapus data biometrik mereka.

Amazon One Console berfungsi sebagai hub terpusat untuk mengelola aktivitas operasional, seperti perangkat pelacak dan melihat tagihan bulanan. Pengguna dapat mendaftar dengan memindai telapak tangan mereka di stasiun pendaftaran yang diawasi di tempat. Setelah terdaftar, pengguna dapat masuk atau keluar dari lokasi aman dengan mengarahkan telapak tangan mereka ke perangkat yang diaktifkan Amazon One.

## Topik

- [Alur kerja Amazon One](#)
- [Amazon Salah satu istilah kunci](#)

## Alur kerja Amazon One

Berikut ini merinci alur kerja dasar Amazon One:

1. Beli dan instal perangkat Amazon One dengan [menghubungi kami](#).
2. Setelah menginstal perangkat, aktifkan Amazon One.
3. Masuk ke akun Amazon One Anda.
4. Konfigurasi perangkat pendaftaran dan entri pengguna.
5. Daftarkan telapak tangan karyawan.
6. Gunakan fitur manajemen dan pemantauan untuk memastikan kesehatan perangkat, memperbarui konfigurasi, dan melacak pendaftaran pengguna untuk pengawasan menyeluruh.

# Amazon Salah satu istilah kunci

Ini adalah istilah kunci untuk Amazon One:

- **Situs** — Pelanggan mengelola bangunan fisik tempat pelanggan memasang perangkat Amazon One. Situs harus memenuhi persyaratan fasilitas, jaringan, dan daya untuk perangkat Amazon One Anda.
- **Perangkat** — Perangkat biometrik pemindaian telapak tangan Amazon One untuk otentikasi.
- **Device Instance** — Representasi logis dari perangkat dengan konfigurasi. Penggunaan instance perangkat memungkinkan untuk menukar perangkat Amazon One sambil secara otomatis mewarisi konfigurasi dan nama yang telah ditetapkan sebelumnya. Instans perangkat memiliki nama yang ditentukan pengguna (konvensi penamaan bersama dengan perangkat lunak kontrol akses Anda) dan serangkaian konfigurasi komunikasi. Instans perangkat memiliki tiga status utama:
  - Membutuhkan konfigurasi
  - Siap untuk aktivasi
  - Aktif
- **Template Konfigurasi** — Satu set konfigurasi all-inclusive yang diterapkan pada instance perangkat.

# Menyiapkan konsol Amazon One

Bab ini menjelaskan langkah-langkah dasar untuk memulai dengan konsol Amazon One.

Menyiapkan situs, instance perangkat, dan templat konfigurasi —Ikuti langkah-langkah berikut untuk membuat kerangka kerja untuk menambahkan lokasi fisik untuk menampung perangkat Amazon One Anda, lalu mengonfigurasi dan mengelolanya menggunakan konsol Amazon One Enterprise. Anda akan menggunakan proses ini hanya sesekali, atau bahkan hanya sekali, tergantung pada jumlah situs, instance perangkat, dan templat konfigurasi Anda.

## Topik

- [Mendaftar untuk akun AWS](#)
- [Buat pengguna dengan akses administratif](#)
- [Tambahkan pengguna Amazon One](#)
- [Buat situs](#)
- [Buat instance perangkat](#)
- [Buat templat konfigurasi](#)
- [Konfigurasi instance perangkat untuk aktivasi](#)

## Mendaftar untuk akun AWS

Jika Anda tidak memiliki akun AWS, selesaikan langkah berikut untuk membuatnya.

Untuk mendaftar akun AWS

1. Buka <https://portal.aws.amazon.com/billing/signup>
2. Ikuti petunjuk online.

Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

Saat Anda mendaftar untuk akun AWS, pengguna root akun AWS akan dibuat. Pengguna root memiliki akses ke semua layanan dan sumber daya AWS di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan [tugas yang memerlukan akses pengguna root](#)

AWS mengirimkan email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan membuka <https://aws.amazon.com/> dan memilih Akun Saya

## Buat pengguna dengan akses administratif

Setelah Anda mendaftar untuk akun AWS, amankan pengguna root akun AWS Anda, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Topik

- [Mengamankan akun AWS Anda](#)
- [Membuat pengguna dengan akses administratif](#)
- [Masuk sebagai administrator](#)
- [Menetapkan akses ke pengguna tambahan](#)

## Mengamankan akun AWS Anda

Sekarang setelah Anda masuk ke akun Amazon One, amankan akun Anda.

Untuk mengamankan pengguna root akun AWS Anda

1. Masuk ke AWS Management Console sebagai pemilik akun dengan memilih Pengguna akar dan memasukkan alamat email akun AWS Anda.
2. Di laman berikutnya, masukkan kata sandi.

Untuk bantuan masuk menggunakan pengguna root, lihat [Masuk sebagai pengguna root](#) di Panduan Pengguna Masuk AWS.

3. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

Untuk petunjuknya, lihat [Mengaktifkan perangkat MFA virtual untuk pengguna root akun AWS \(konsol\)](#) Anda di Panduan Pengguna IAM.

## Membuat pengguna dengan akses administratif

Sekarang setelah Anda mengamankan akun Amazon One Anda, buat pengguna dengan akses administratif.

Untuk membuat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

Untuk petunjuk, lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center.

2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

Untuk tutorial tentang menggunakan direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengonfigurasi akses pengguna dengan direktori Pusat Identitas IAM default di Panduan Pengguna AWS IAM Identity Center.

## Masuk sebagai administrator

Sekarang setelah Anda membuat pengguna dengan akses administratif, masuk sebagai administrator.

Untuk masuk sebagai pengguna dengan akses administratif

- Masuk dengan pengguna Pusat Identitas IAM Anda, menggunakan URL masuk yang dikirim ke alamat email Anda saat Anda membuat pengguna Pusat Identitas IAM.

Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal akses AWS di Panduan Pengguna Masuk AWS.

## Menetapkan akses ke pengguna tambahan

Setelah masuk sebagai administrator, Anda dapat menetapkan akses ke pengguna tambahan.

Untuk menetapkan akses ke pengguna tambahan

- Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

Untuk petunjuknya, lihat Menambahkan grup di Panduan Pengguna AWS IAM Identity Center.

# Tambahkan pengguna Amazon One

Selain pengguna admin, Anda juga dapat menambahkan pengguna yang tidak memiliki izin admin. Misalnya, pengguna ini mungkin penginstal yang mengakses konsol Amazon One hanya untuk mengambil kode QR aktivasi perangkat untuk mengaktifkan perangkat Amazon One.

Untuk menambahkan pengguna Amazon One


1. Ikuti prosedur masuk yang sesuai dengan jenis pengguna Anda seperti yang dijelaskan [dalam Cara masuk](#) AWS di Panduan AWS Sign-In Pengguna.
2. Di panel navigasi, pilih Pengguna, lalu pilih Tambah pengguna.
3. Pada halaman Tentukan detail pengguna, di bawah Rincian pengguna, di Nama pengguna, masukkan nama untuk pengguna baru. Ini adalah nama masuk mereka untuk AWS.

## Note

Jumlah dan ukuran sumber daya IAM di sebuah Akun AWS terbatas. Untuk informasi selengkapnya, lihat [kuota IAM dan AWS STS](#). Nama pengguna dapat berupa kombinasi hingga 64 huruf, digit, dan karakter berikut: plus (+), sama (=), koma (,), titik (.), pada tanda (@), garis bawah (\_), dan tanda hubung (-). Nama harus unik dalam akun. Grup tidak dibedakan berdasarkan huruf besar-kecil. Misalnya, Anda tidak dapat membuat dua pengguna yang diberi nama TESTUSER dan testuser. Ketika nama pengguna digunakan dalam kebijakan atau sebagai bagian dari ARN, nama tersebut peka huruf besar/kecil. Ketika nama pengguna muncul ke pelanggan di konsol, seperti selama proses login, nama pengguna tidak peka huruf besar/kecil.


4. Anda ditanya apakah Anda menyediakan akses konsol ke seseorang. Pilih Berikan akses pengguna ke — Konsol Manajemen AWS opsional.
5. Pilih Saya ingin membuat pengguna IAM.
6. Untuk kata sandi Konsol, pilih salah satu dari berikut ini:
  - Kata sandi yang dibuat secara otomatis — Pengguna diberikan kata sandi yang dibuat secara acak yang memenuhi kebijakan [kata sandi akun](#). Anda dapat melihat atau mengunduh kata sandi saat Anda masuk ke halaman Ambil kata sandi.
  - Kata sandi khusus - Pengguna diberi kata sandi yang Anda masukkan di bidang.

7. (Opsional) Secara default, Pengguna harus membuat kata sandi baru saat login berikutnya (disarankan) dipilih untuk memastikan bahwa pengguna diharuskan mengubah kata sandi mereka saat pertama kali masuk.

 Note

Jika administrator telah mengaktifkan [pengaturan Izinkan pengguna mengubah kebijakan kata sandi akun kata sandi mereka sendiri](#), maka kotak centang ini tidak melakukan apa-apa. Jika tidak, akan otomatis melampirkan kebijakan terkelola AWS yang bernama [IAMUserChangePassword](#) ke pengguna baru. Kebijakan tersebut memberi mereka izin untuk mengubah kata sandi mereka sendiri.

8. Pilih Selanjutnya.
9. Pada halaman Setel izin, pilih Lampirkan kebijakan secara langsung.
10. Pilih kebijakan yang ingin Anda lampirkan ke pengguna.
  - [AmazonOneEnterpriseReadOnlyAccess](#)
  - [AmazonOneEnterpriseInstallerAccess](#)

 Note

[AmazonOneEnterpriseInstallerAccess](#) kebijakan terkelola akan memberikan akses pengguna ke kode QR aktivasi hanya di konsol Amazon One Enterprise. Kebijakan ini sangat ideal untuk perusahaan yang mempekerjakan pihak ketiga untuk menginstal perangkat Amazon One.

11. Pilih Selanjutnya.
12. (Opsional) Pada halaman Tinjau dan buat, di bawah Tag, pilih Tambahkan tag baru untuk menambahkan metadata ke pengguna dengan melampirkan tag sebagai pasangan nilai kunci. Untuk informasi lebih lanjut tentang penggunaan tanda dan IAM, lihat [Penandaan sumber daya IAM](#).
13. Tinjau semua pilihan yang Anda buat sampai saat ini. Ketika Anda siap untuk melanjutkan, pilih Buat pengguna.
14. Pada halaman Ambil kata sandi, dapatkan kata sandi yang ditetapkan untuk pengguna:

- Pilih Tampilkan di sebelah kata sandi untuk melihat kata sandi pengguna sehingga Anda dapat merekamnya secara manual.
  - Pilih Unduh.csv untuk mengunduh kredensi masuk pengguna sebagai file.csv yang dapat Anda simpan ke lokasi yang aman.
15. Pilih Petunjuk masuk Email. Klien email lokal Anda terbuka dengan draf yang dapat Anda sesuaikan dan kirim ke pengguna. Templat email mencakup perincian berikut untuk setiap pengguna:
- Nama pengguna
  - URL ke halaman masuk akun. Gunakan contoh berikut, yang mengganti nomor ID akun atau alias akun yang benar:

```
https://AWS-account-ID or alias.signin.aws.amazon.com/console
```

#### Important

Kata sandi pengguna tidak disertakan dalam email yang dibuat. Anda harus memberikan kata sandi kepada pengguna dengan cara yang sesuai dengan pedoman keamanan organisasi Anda.

## Buat situs

Sekarang setelah Anda masuk Konsol Manajemen AWS, Anda dapat menggunakan konsol Amazon One untuk membuat situs Anda.

#### Important

Amazon One hanya tersedia di Wilayah AS Timur (Virginia N.).

Untuk membuat situs

1. Buka konsol Amazon One <https://console.aws.amazon.com/one-enterprise>.
2. Pilih Pergi ke Ikhtisar.

3. Di panel navigasi, pilih Situs.
4. Pilih Buat situs.
5. Di bawah informasi Situs, untuk nama Situs, masukkan nama untuk situs.
6. Di bawah Alamat fisik, masukkan alamat untuk situs tempat perangkat Amazon One Anda akan diinstal.
7. (Opsional) Untuk menambahkan tag ke situs, masukkan pasangan kunci-nilai di bawah Tag, lalu pilih Tambahkan tag baru. Untuk menghapus tag ini sebelum membuat situs, pilih Hapus.
8. Pilih Buat situs untuk membuat situs.

## Buat instance perangkat

Setelah membuat situs di AWS Management Console, Anda dapat menggunakan konsol Amazon One untuk membuat instance perangkat.

Untuk membuat instance perangkat

1. Buka konsol Amazon One <https://console.aws.amazon.com/di/one-enterprise>.
2. Di panel navigasi, pilih instance perangkat. Pastikan Anda berada di tab Instance Tidak Aktif.
3. Di bawah Detail instans, pilih situs dari drop-down Situs, atau buat situs baru dengan memilih tombol Buat situs.
4. Masukkan setiap nama instance Perangkat secara manual.
5. (Opsional) Untuk menambahkan tag ke instance perangkat, masukkan pasangan nilai kunci di bawah Tag, lalu pilih Tambahkan tag baru. Untuk menghapus tag ini sebelum membuat instance perangkat, pilih Hapus.
6. Pilih Buat instance untuk membuat instance perangkat.

### Note

Catatan: instance perangkat perlu dikonfigurasi sebelum penginstalan dapat terjadi.

## Buat templat konfigurasi

Sekarang setelah Anda membuat instance perangkat, Anda dapat menggunakan konsol Amazon One untuk membuat templat konfigurasi.

## Untuk membuat template konfigurasi

1. Buka konsol Amazon One <https://console.aws.amazon.com/di/one-enterprise>.
2. Di panel navigasi, pilih Templat konfigurasi.
3. Pilih Buat templat.
4. Di bawah informasi Template, untuk nama Template, masukkan nama untuk template konfigurasi.
5. Di bawah Konfigurasi perangkat, pilih mode Operasi.

### To configure Enrollment operating mode

1. (Opsional) Di bawah konfigurasi Wifi, berikan kredensi Wifi Anda.
2. (Opsional) Untuk menambahkan tag ke situs, masukkan pasangan kunci-nilai di bawah Tag, lalu pilih Tambahkan tag baru. Untuk menghapus tag ini sebelum membuat situs, pilih Hapus.
3. Pilih Konfigurasikan

### To configure Entry operating mode

1. Di bawah Pengaturan panel kontrol, berikan pengaturan komunikasi untuk perangkat Amazon One untuk berkomunikasi dengan panel kontrol Anda.
2. Di bawah Pengaturan format rencana, berikan pengaturan konfigurasi yang menentukan tata letak format rencana perusahaan Anda.
3. (Opsional) Di bawah konfigurasi Wifi, berikan kredensi Wifi Anda.
4. (Opsional) Untuk menambahkan tag ke situs, masukkan pasangan kunci-nilai di bawah Tag, lalu pilih Tambahkan tag baru. Untuk menghapus tag ini sebelum membuat situs, pilih Hapus.
5. Pilih Konfigurasikan

#### Important

Anda harus mengonfigurasi setidaknya satu perangkat Pendaftaran dan satu perangkat Entri untuk mengaktifkan kemampuan penuh Amazon One untuk akses yang aman.

## Konfigurasi instance perangkat untuk aktivasi

Setelah instance perangkat dibuat, Anda mengonfigurasi instance perangkat dengan templat konfigurasi yang dibuat sebelumnya (lihat [Buat templat konfigurasi](#)), atau Anda dapat menambahkan konfigurasi secara manual.

Untuk mengonfigurasi instance perangkat untuk aktivasi

1. Buka konsol Amazon One <https://console.aws.amazon.com/di/one-enterprise>.
2. Di panel navigasi, pilih Instans perangkat. Pastikan Anda berada di tab Instance Tidak Aktif.
3. Pilih satu atau beberapa contoh untuk dikonfigurasi.
4. Pilih Konfigurasi
5. Di bawah Konfigurasi Perangkat, pilih salah satu dari dua metode input:
  - a. Untuk opsi Use template, pilih template dari drop-down. Tinjau atau buat perubahan pada informasi konfigurasi yang diimpor ini.

Untuk opsi Buat template, lihat [Buat templat konfigurasi](#).

- b. Untuk opsi Input secara manual, pilih mode Operasi.

To configure Enrollment operating mode

- a. (Opsional) Di bawah konfigurasi Wifi, berikan kredensi Wifi.
  - b. (Opsional) Untuk menambahkan tag ke situs, masukkan pasangan kunci-nilai di bawah Tag, lalu pilih Tambahkan tag baru. Untuk menghapus tag ini sebelum membuat situs, pilih Hapus.
  - c. Pilih Konfigurasi


To configure Entry operating mode

- a. Di bawah Pengaturan panel kontrol, berikan pengaturan komunikasi untuk perangkat Amazon One untuk berkomunikasi dengan panel kontrol Anda.
  - b. Di bawah Pengaturan format rencana, berikan pengaturan konfigurasi yang menentukan tata letak format rencana perusahaan Anda.
  - c. (Opsional) Di bawah konfigurasi Wifi, berikan kredensi Wifi.

- d. (Opsional) Untuk menambahkan tag ke situs, masukkan pasangan kunci-nilai di bawah Tag, lalu pilih Tambahkan tag baru. Untuk menghapus tag ini sebelum membuat situs, pilih Hapus.
  - e. Pilih Konfigurasi
6. Di bawah tabel Instance Tidak Aktif, status Instance akan ditampilkan.

 **Ready for activation**

7. Validasi bahwa kode QR aktivasi tersedia untuk aktivasi. Di panel navigasi, pilih Kode QR Aktivasi.
8. Dari daftar drop-down Pilih situs, pilih Situs.
9. Di bawah informasi Situs, validasi alamat Situs.
10. Di bawah kode QR Aktivasi, setiap instance perangkat memiliki kode QR yang sesuai. Pilih Dapatkan kode QR untuk menampilkan kode QR aktivasi.

 **Important**

Anda harus mengonfigurasi setidaknya satu perangkat Pendaftaran dan satu perangkat Entri untuk mengaktifkan kemampuan penuh Amazon One untuk akses yang aman.

# Menginstal dan mengaktifkan Amazon One

Setelah berhasil menyiapkan konsol Amazon One Anda, langkah selanjutnya melibatkan menginstal perangkat Amazon One di situs Anda dan memastikannya diaktifkan dengan benar. Proses ini termasuk menempatkan perangkat secara fisik di area yang ditentukan, menghubungkannya ke jaringan Anda, dan menyelesaikan proses aktivasi untuk memungkinkan identifikasi pengguna dan kemampuan transaksi yang mulus. Setelah diaktifkan, perangkat Amazon One Anda akan siap memberikan pengalaman yang aman dan tanpa sentuhan bagi pelanggan atau karyawan Anda.

## Note

Bagian ini berfokus pada instalasi, dan menggunakan browser seluler untuk mengakses Konsol Manajemen AWS untuk mendapatkan kode QR aktivasi perangkat.

## Topik

- [Memahami persyaratan](#)
- [Memahami konsep instalasi](#)
- [Memasang Amazon One Pedestal](#)
- [Memasang perangkat Amazon One yang dapat dipasang di dinding](#)
- [Menginstal Amazon One Device I/O Hub untuk akses aman](#)
- [Mengaktifkan perangkat Amazon One](#)

## Memahami persyaratan

Perangkat Amazon One dapat dipasang di lokasi perusahaan atau bisnis mana pun yang memiliki pintu yang dapat dikontrol secara elektrik.

## Persyaratan panel kontrol

Perangkat Amazon One dapat terhubung ke sebagian besar panel kontrol akses standar sebagai pembaca. Perangkat Amazon One mendukung protokol berikut:

- OSDP (v1 dan v2)
- Wiegand

## Persyaratan jaringan

Perangkat Amazon One harus selalu terhubung ke internet untuk operasi normal. Konektivitas internet dapat disediakan oleh Ethernet kabel atau Wi-Fi. Bandwidth minimum yang dibutuhkan adalah 10 Mbps.

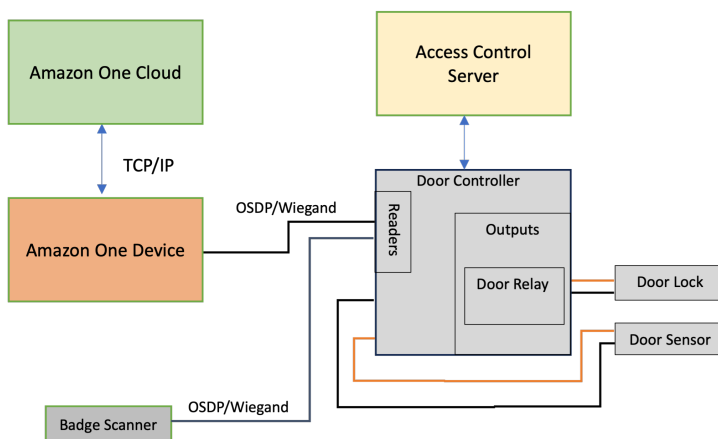
## Kebutuhan daya

Perangkat Amazon One dapat diberdayakan dengan salah satu dari dua cara:

- Dengan menggunakan adaptor daya 120V yang disediakan di dalam kotak.
- Dengan menggunakan perangkat berkemampuan PoE+.

## Memahami konsep instalasi

Untuk mengamankan akses bangunan dengan benar, Amazon One menyarankan Anda menginstal perangkat sebagai bagian dari lingkungan kontrol akses biasa, seperti yang dijelaskan dalam diagram blok berikut.



Lingkungan kontrol akses biasanya terdiri dari komponen-komponen ini:

- **Perangkat Amazon One:** Ini adalah perangkat pengenalan telapak tangan yang akan melakukan otentikasi biometrik untuk mengidentifikasi individu yang mencoba mendapatkan akses ke area aman bangunan.
- **Server kontrol akses:** Komponen ini biasanya mengontrol hak akses pengguna ke area aman. Lencana individu IDs yang memiliki akses ke area tersebut disimpan di server ini. Server ini menyimpan cache yang relevan dengan IDs pengontrol pintu yang sesuai.

- Pengontrol pintu:
  - Perangkat Amazon One terhubung ke server pengontrol pintu melalui antarmuka OSDP.
  - Jika antarmuka Wiegand diperlukan, OSDP-to-Wiegand konverter COTS dapat digunakan.
  - Setelah otentikasi berhasil, perangkat Amazon One mengirimkan ID lencana pengguna ke pengontrol pintu.
  - Pengontrol pintu merespons dengan keputusan, yang kemudian memungkinkan perangkat Amazon One menampilkan pesan Akses yang Diberikan atau Akses Ditolak.
- Pemindai lencana: Pemindai lencana biasanya digunakan untuk memindai lencana RFID dan mengirim nomor lencana ke server kontrol akses. Dengan Amazon One, pemindai lencana terhubung ke perangkat Amazon One, memungkinkan pengguna untuk memindai lencana mereka, yang mengaitkannya dengan profil telapak tangan mereka.

## Memasang Amazon One Pedestal

Amazon One Pedestal adalah komponen kunci dari sistem identifikasi dan transaksi Amazon One, yang dirancang untuk memberikan pengalaman tanpa sentuhan yang mulus bagi pengguna. Perangkat ini memiliki otentikasi biometrik yang aman. Anda dapat mengintegrasikannya ke berbagai lokasi untuk memberikan akses tanpa gesekan atau solusi pembayaran.

Bagian ini memberikan persyaratan lokasi dan step-by-step instruksi untuk menginstal Amazon One Pedestal. Persiapan dan pemasangan yang tepat adalah kunci untuk memastikan sistem beroperasi dengan aman dan efisien, memberikan pengalaman yang lancar dan andal kepada pengguna.



### Prasyarat dan persiapan untuk memasang Amazon One Pedestal

Sebelum memulai instalasi, pastikan kondisi berikut terpenuhi untuk pengaturan yang aman, aman, dan efektif:

- Persyaratan daya: Jika Anda menggunakan POE+ (Power over Ethernet) untuk memberi daya pada perangkat, verifikasi bahwa kabel Cat6 sudah terpasang, dan injektor atau sakelar POE+ tersedia untuk digunakan. Atau, jika daya AC (120V) digunakan, pastikan stopkontak AC yang dapat diakses terletak dalam jarak 20 kaki dari alas.
- Pengaturan fisik: Lantai harus rata, bersih, dan bebas dari puing-puing untuk memastikan pemasangan alas yang stabil dan aman.
- Lokasi alas: Pasang alas di lokasi yang tidak akan menghalangi pintu, jalur, atau titik akses, memungkinkan pergerakan mudah di sekitar area tersebut.
- Manajemen kabel: Rutekan dan amankan semua kabel berlebih di dalam alas untuk menghindari kekacauan dan mencegah potensi kerusakan selama penggunaan normal.

Setelah prasyarat ini dikonfirmasi, Anda dapat melanjutkan proses instalasi.

Untuk menginstal Amazon One Pedestal

1. Lepaskan Amazon One Pedestal dari kemasannya.
2. Lepaskan pintu dengan membuka kedua sekrup tahan tamper M4.
3. Colokkan kabel daya.
4. Rutekan kabel melalui lubang di pelat dasar alas.
5. Gulung kabel daya berlebih di dalam alas.
6. Rutekan kabel Ethernet (Cat5E atau lebih baik) melalui pelat bawah alas dan colokkan ke port Ethernet.
7. Pasang loop ferit pada kabel Ethernet 2 inci di atas dasar alas.
8. Umpan kabel RS485 serial dari panel kontrol akses (atau pembaca lencana) ke alas, dengan panjang kelebihan 1 kaki.
9. Pasang loop ferit pada RS485 kabel 2 inci di atas dasar alas.
10. Colokkan daya ke stopkontak dan konfirmasikan bahwa perangkat Amazon One menyala.
11. Pasang kembali pintu ke alas dan pasang kembali kedua sekrup resistansi tamper M4 untuk mengamankan.

Setelah menginstal perangkat Amazon One Anda, Anda siap untuk mengaktifkan perangkat.

# Memasang perangkat Amazon One yang dapat dipasang di dinding

Perangkat Amazon One yang dapat dipasang di dinding adalah sistem identifikasi biometrik ringkas dan serbaguna yang dirancang untuk memberikan pengalaman tanpa sentuhan yang mulus bagi pengguna di berbagai lingkungan. Ini menggunakan teknologi pengenalan telapak tangan canggih untuk akses atau pembayaran yang aman, menjadikannya ideal untuk lokasi dengan lalu lintas tinggi seperti ruang ritel, pintu masuk kantor, dan banyak lagi.

Bagian ini menguraikan persyaratan lokasi yang diperlukan dan langkah-langkah terperinci untuk memasang perangkat Amazon One yang dapat dipasang di dinding untuk memastikan kinerja dan keamanan yang optimal.

Prasyarat dan persiapan untuk memasang perangkat Amazon One yang dapat dipasang di dinding

Sebelum Anda memulai instalasi, pastikan bahwa kondisi berikut terpenuhi untuk menjamin perangkat beroperasi secara efektif dan diatur dengan benar di dalam ruang Anda:

- Hanya penggunaan di dalam ruangan: Perangkat Amazon One yang dapat dipasang di dinding hanya ditujukan untuk penggunaan di dalam ruangan, jadi pastikan itu dipasang di lingkungan yang sesuai.
- Persyaratan dinding: Dinding harus rata untuk memastikan keselarasan dan fungsionalitas perangkat yang tepat.
- Tinggi pemasangan: Bagian atas dudukan dinding harus diposisikan tidak lebih tinggi dari 44-46 inci dari tanah setelah pemasangan, memastikan kemudahan akses bagi pengguna.
- Manajemen kabel: Pastikan semua kabel berlebih diarahkan ke belakang dudukan dinding dan diikat dengan aman untuk mencegah kerusakan atau kekacauan.
- Power Over Ethernet (PoE++): Jika menggunakan Power Over Ethernet (PoE++), verifikasi bahwa sakelar IEEE 802.3bt (Tipe 3) Kelas 6 PoE++ (rentang akhir) atau injektor (midspan) tersedia. Sumber PoE ++ harus terdaftar atau disertifikasi dan mematuhi standar IEC 62368-1. Yang penting, sumber PoE++ harus berada di dalam gedung yang sama dengan perangkat. Hanya gunakan sumber PoE++ yang disetujui dengan perangkat AOE.
- Input Daya DC 15V: Jika menggunakan input daya DC 15V, pastikan hanya NEC Kelas 2 atau catu daya yang disetujui terbatas daya yang digunakan. Catu daya harus terdaftar atau disertifikasi untuk keamanan dan kompatibilitas.

Alat yang dibutuhkan

- 1/4" dinding kering atau mata bor batu jika jangkar dinding diperlukan
- Penari telanjang kawat
- Mata bor 7/64" untuk mengebor lubang pilot
- #2 Obeng Phillips
- Obeng flathead 0.5mm x 2mm
- Driver Torx Aman T12
- Pensil
- Tingkat

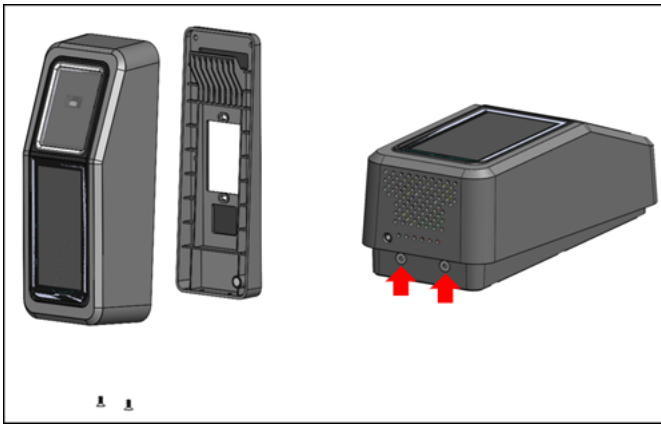
Termasuk dengan perangkat Amazon One yang dapat dipasang di dinding

- 6x #8 Jangkar drywall
- 6x #8 -32 sekrup panjang 1in
- 2x #6 -32 Sekrup Mesin 1in
- 2x 6 Posisi konektor blok terminal
- 2 sekrup flathead Torx Security M4x10

Setelah prasyarat ini dikonfirmasi, Anda dapat melanjutkan dengan langkah-langkah instalasi untuk memasang dan mengonfigurasi perangkat Amazon One yang dapat dipasang di dinding dengan aman.

Untuk memasang pelat pemasangan di dinding untuk perangkat Amazon One Anda

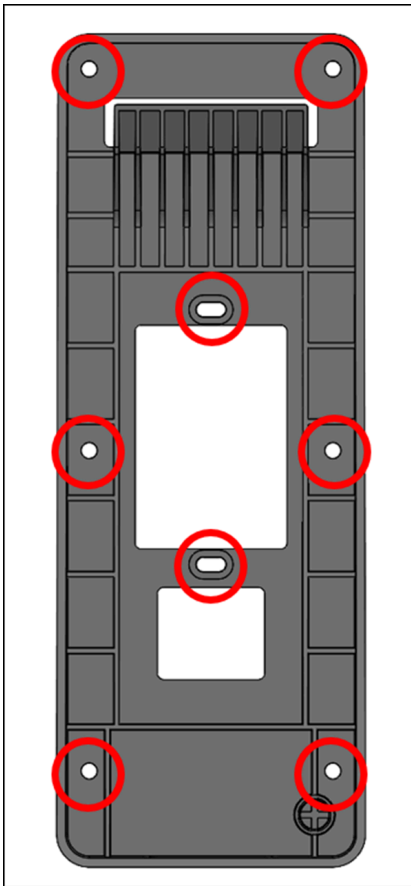
1. Hapus perangkat Amazon One Anda dari kemasan.
2. Pisahkan pelat pemasangan dari perangkat Amazon One Anda dengan melepas dua sekrup keamanan Torx bawah.



3. Posisikan pelat pemasangan di dinding di lokasi yang diinginkan. Gunakan braket sebagai templat untuk menandai enam lubang sekrup luar seperti yang ditunjukkan pada gambar berikut.

(Opsional) Jika satu kotak geng tersedia di posisi instalasi, lakukan hal berikut:

- Pasang pelat secara longgar ke kotak geng dengan memasukkan sekrup mesin #6 -32 yang disertakan melalui lubang lonjong.
- Pastikan pelat pemasangan rata.
- Gunakan pelat pemasangan sebagai templat untuk menandai enam posisi sekrup dengan pensil. Anda dapat menggunakan lubang lonjong dan sekrup #6 -32 sebagai dukungan tambahan untuk pelat pemasangan. Jangan gunakan posisi sekrup #6 -32 sebagai sarana utama pemasangan pelat dinding.



4. Jika dipasang ke permukaan plesteran, drywall, bata, atau beton, bor lubang 1/4" di setiap lokasi yang ditandai, dan kemudian pasang jangkar dinding dengan menekannya ke dalam lubang sampai jangkar rata dengan dinding.

Jika dipasang ke permukaan kayu, jangkar tidak diperlukan dan hanya lubang pilot 7/64" yang diperlukan di lokasi yang ditandai.

5. Kencangkan pelat dinding secara longgar ke dinding menggunakan sekrup kayu #8 di posisi jangkar.
6. Setelah semua pengencang terpasang, pastikan pelat pemasangan rata.
7. Kencangkan sekrup untuk mengamankan pelat pemasangan ke dinding.

Untuk menghubungkan perangkat Amazon One yang dapat dipasang di dinding

Anda dapat mengonfigurasi perangkat Amazon One dengan protokol kontrol akses OSDP dan Weigand. Untuk menyederhanakan instalasi, perangkat Amazon One menggunakan konektor blok terminal (Mfg P/N: Phoenix Contact 1767694). Anda juga memiliki opsi untuk mengonfigurasi

perangkat Amazon One untuk mengontrol perangkat eksternal secara langsung dengan menggunakan relai internal atau koneksi Input dan Output Tujuan Umum.

1. Untuk menentukan konfigurasi kabel yang sesuai untuk aplikasi Anda, lihat diagram dan Tabel Koneksi berikut.

Untuk karakteristik kelistrikan sinyal yang terperinci, lihat instruksi Pengkabelan.

### Koneksi



Pin	Koneksi	Deskripsi	Gunakan
1	GPO	Output tujuan umum	Sinyal output digital - Opsional
2	GPI	Masukan tujuan umum	Sinyal input digital - Opsional
3	DIPIMPIN	LED Wiegand	Wiegand LED - Opsional
4	D1	Wiegand D1	Data Wiegand 1 - Kabel putih
5	D0	Wiegand D0	Data Wiegand 0 — Kabel hijau
6	RTN	Sinyal kembali	Wiegand Ground - Kawat hitam
7	Com	Relay umum	Relai kontak umum - Kabel putih

Pin	Koneksi	Deskripsi	Gunakan
8	NC	Relay biasanya ditutup	Relai kontak biasanya tertutup - Kawat oranye
9	TIDAK	Relay biasanya terbuka	Relai kontak biasanya terbuka - Kabel kuning
10	RTN	Sinyal kembali	Pengembalian OSDP - Kabel hitam
11	A	RS485_A/D1/ Clock	OSDP D1 - kawat putih
12	B	RS485_B/D0/ Data	OSDP D0 - Kawat hijau

2. Saat memasang kawat, lepaskan 3mm-5mm dari ujung kawat.
3. Masukkan ujung kabel yang dilucuti ke posisi terminal yang diinginkan.
4. Dengan menggunakan obeng pipih, putar sekrup retensi terminal searah jarum jam untuk menjepit kabel sampai pas. Jangan terlalu kencang.
5. Setelah diikat, tarik kabel dengan lembut untuk memastikannya terpasang.
6. Setelah Anda membuat koneksi yang diperlukan, masukkan steker ke stopkontak yang sesuai dari blok terminal perangkat Amazon One Anda.
7. Masukkan kabel Cat6 Ethernet ke RJ45 jack.
8. Posisikan perangkat Amazon One sehingga kait pada pelat dinding meluncur ke bukaan di bagian belakang perangkat.
9. Pastikan kabel tidak tersangkut di antara perangkat dan pelat pemasangan, dan biarkan perangkat berputar dan duduk pada posisinya.
10. Amankan perangkat Amazon One Anda ke pelat pemasangan dengan dua sekrup flathead Torx Security M4x10.

11. Kencangkan sekrup dengan tangan. Jangan terlalu kencang.

Untuk memasang kabel perangkat Amazon One yang dapat dipasang di dinding

Instal hanya kabel yang diperlukan untuk aplikasi Anda.

#### Koneksi Wiegand

- Masukkan kabel biru di Pin 3 (LED).
- Masukkan kabel putih di Pin 4 (D1).
- Masukkan kabel hijau di Pin 5 (D0).
- Masukkan kabel hitam di Pin 6 (RTN).



#### Kabel keluaran Wiegand

Pin	Koneksi	Deskripsi	Gunakan
3	DIPIMPIN	LED Wiegand	Masukan LED Wiegand - Opsional (5V TTL)
4	D1	Wiegand D1	Keluaran Wiegand D1 (5V TTL)
5	D0	Wiegand D0	Keluaran Wiegand D0 (5V TTL)
6	RTN	Sinyal kembali	Referensi Wiegand GND

Hidupkan sakelar RS485 terminasi “ON” jika perangkat adalah unit terakhir di telepon. Sakelar ini mengaktifkan terminasi resistor 120 Ohm pada saluran.

## RS485 koneksi

- Masukkan kabel hitam di Pin 10 (RTN).
- Masukkan kabel putih di Pin 11 (A).
- Masukkan kabel hijau di Pin 12 (B).



## RS485 kabel

Pin	Koneksi	Deskripsi	Gunakan
10	RTN	Sinyal kembali	Tanah
11	A	RS485_A/D1/ Clock	RS485 sinyal non-pembalik
12	B	RS485_B/D0/ Data	RS485 sinyal pembalik

## Koneksi relai

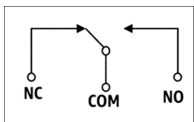
- Masukkan kabel putih di Pin 7 (COM).
- Masukkan kawat oranye di Pin 8 (NC).
- Masukkan kabel kuning di Pin 9 (NO).



## Kabel relai

Pin	Koneksi	Deskripsi	Gunakan
7	COM	Relay umum	Relai kontak Umum - Kabel putih

Pin	Koneksi	Deskripsi	Gunakan
8	NC	Relay biasanya ditutup	Relai kontak biasanya tertutup - Kawat oranye
9	TIDAK	Relay biasanya terbuka	Relai kontak biasanya terbuka - Kabel kuning



Relai harus dioperasikan sesuai dengan peringkat keselamatan yang ditentukan 30VAC/60VDC, 60W Max.

input/output Koneksi digital

- Masukkan kabel biru di Pin 1 (GPO).
- Masukkan kabel biru di Pin 2 (GPI).



input/output Kabel digital

Pin	Koneksi	Deskripsi	Gunakan
1	GPO	Output tujuan umum	Sinyal keluaran digital (5V)
2	GPI	Masukan tujuan umum	Sinyal input digital (3.6V - 5V)

- input/output Koneksi digital harus dioperasikan seperti yang tercantum.

Setelah menginstal perangkat Amazon One Anda, Anda siap untuk mengaktifkan perangkat.

## Menginstal Amazon One Device I/O Hub untuk akses aman

Perangkat Amazon One dengan I/O Hub merupakan bagian integral dari sistem Amazon One Enterprise, yang dirancang untuk meningkatkan keamanan dan merampingkan kontrol akses untuk berbagai lingkungan. Perangkat ini memanfaatkan pengenalan telapak tangan biometrik untuk memberikan otentikasi tanpa sentuhan yang aman bagi pengguna, sehingga ideal untuk digunakan di area dengan keamanan tinggi seperti gedung perkantoran, titik masuk terbatas, atau fasilitas yang membutuhkan manajemen akses tanpa batas. I/O Hub bertindak sebagai jembatan antara perangkat dan infrastruktur keamanan yang ada, memungkinkan komunikasi dengan kunci pintu, alarm, dan sistem kontrol akses lainnya.

Bagian ini memberikan persyaratan lokasi dan step-by-step instruksi untuk menginstal perangkat Amazon One dengan I/O Hub. Persiapan dan pemasangan yang tepat adalah kunci untuk memastikan sistem beroperasi dengan aman dan efisien, memberikan pengalaman yang lancar dan andal kepada pengguna.

### Prasyarat dan persiapan untuk menginstal Perangkat Amazon One dengan Hub I/O

Sebelum memulai instalasi, pastikan kondisi berikut terpenuhi untuk memastikan pengaturan yang aman, aman, dan efektif:

- Hanya penggunaan di dalam ruangan: Perangkat Amazon One dengan I/O Hub dirancang hanya untuk penggunaan di dalam ruangan. Pastikan dipasang di lingkungan yang sesuai.
- Power Over Ethernet (PoE++): Jika menggunakan Power Over Ethernet (PoE++), verifikasi bahwa sakelar IEEE 802.3bt (Tipe 3) Kelas 6 PoE++ (rentang akhir) atau injektor (midspan) tersedia. Sumber PoE ++ harus terdaftar atau disertifikasi dan mematuhi standar IEC 62368-1. Yang penting, sumber PoE++ harus berada di dalam gedung yang sama dengan perangkat. Hanya gunakan sumber PoE++ yang disetujui dengan perangkat AOE.
- Input daya DC 15V: Jika Anda menggunakan input daya DC 15V, pastikan hanya NEC Kelas 2 atau catu daya terbatas yang disetujui yang digunakan. Catu daya harus terdaftar atau disertifikasi untuk keselamatan. Untuk detail lebih lanjut, lihat bagian DC Opsional di bawah ini.

### Alat yang dibutuhkan

- Penari telanjang kawat

- #2 Obeng Phillips
- Obeng flathead 0.5mm x 2mm

Termasuk dengan perangkat Amazon One dengan I/O Hub

- Konektor blok terminal 2x 6 posisi
- Konektor steker DC
- 72" kabel power/data

Setelah prasyarat ini dikonfirmasi, Anda dapat melanjutkan proses instalasi, memastikan pengaturan perangkat Amazon One Anda yang aman dan efisien dengan Hub. I/O Persiapan yang tepat akan membantu menjamin fungsi perangkat sebagaimana dimaksud dan terintegrasi dengan lancar ke dalam sistem akses aman Anda.

Untuk menginstal I/O hub untuk perangkat Amazon One Anda

1. Hapus perangkat Amazon One Anda dengan I/O Hub dari kemasannya.
2. Amankan I/O hub di lokasi yang diinginkan.
3. Colokkan kabel USB Amazon One ke port I/O hub.
  -
4. Untuk daya POE ++, colokkan kabel Ethernet dari sumber POE ++ ke port hub. I/O

Opsional: Untuk daya DC, lihat bagian pemasangan kabel DC di bawah ini.

■

Untuk menghubungkan I/O hub untuk perangkat Amazon One Anda

- Pasang loop tetes untuk menghindari cairan yang tidak sengaja mengalir ke kabel dan masuk ke hub. I/O
- Pasang penjepit pelepas regangan untuk melindungi kabel dari kerusakan atau stres, seperti yang ditunjukkan pada gambar berikut.

1. Masukkan colokan blok terminal ke I/O hub.

2. Masukkan hanya kabel yang diperlukan untuk aplikasi Anda melalui colokan blok terminal. Lihat tabel dan diagram pengkabelan berikut.

### Koneksi

=

Pin	Koneksi	Deskripsi	Gunakan
1	RTN	Sinyal kembali	Tanah Wiegand - Kawat hitam
2	D1	Wiegand D1	Wiegand Data 1 - Kabel putih
3	D0	Wiegand D0	Data Wiegand 0 — Kabel hijau
4	DIPIMPIN	LED Wiegand	Wiegand LED - Opsional
5	GPI	Masukan tujuan umum	Sinyal input digital - Opsional
6	GPO	Output tujuan umum	Sinyal output digital - Opsional
7	B	RS485_B/D0/ Data	OSDP D0 - Kawat hijau
8	A	RS485_A/D1/ Clock	OSDP D1 - kawat putih
9	RTN	Sinyal kembali	Pengembalian OSDP - Kabel hitam
10	COM	Relay Umum	Relai kontak umum - Kabel putih

Pin	Koneksi	Deskripsi	Gunakan
11	NC	Relay biasanya ditutup	Relai kontak biasanya tertutup - Kawat oranye
12	TIDAK	Relay Biasanya Terbuka	Relai kontak biasanya terbuka - Kabel kuning

### Koneksi Wiegand

- Masukkan kabel hitam di Pin 1 (RTN).
- Masukkan kabel putih di Pin 2 (D1).
- Masukkan kabel hijau di Pin 3 (D0).
- Opsional: Masukkan kabel hijau di Pin 4 (LED).

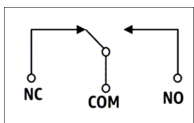


### Koneksi relai

- Masukkan kabel putih di Pin 10 (COM).
- Masukkan kawat oranye di Pin 11 (NC).
- Masukkan kabel kuning di Pin 12 (NO).



### Diagram relai



Relai harus dioperasikan sesuai dengan peringkat keselamatan yang ditentukan 30VAC/60VDC, 60W Max.

### RS485 koneksi

- Masukkan kabel hijau di Pin 7 (B).
- Masukkan kabel putih di Pin 8 (A).
- Masukkan kabel hitam di Pin 9 (RTN).



Hidupkan sakelar RS485 terminasi “ON” jika perangkat adalah unit terakhir di telepon. Sakelar ini mengaktifkan terminasi resistor 120 Ohm pada saluran.

input/output Koneksi digital

- Masukkan kabel hitam di Pin 5 (GPI).
- Masukkan kabel putih di Pin 6 (GPO).



- input/output Koneksi digital harus dioperasikan seperti yang tercantum.

Opsional: Untuk memasang kabel DC

1. Lepaskan 3mm-5mm dari ujung kabel merah untuk positif (+) dan kabel hitam untuk negatif (-).
2. Masukkan ujung kabel DC yang dilucuti ke dalam steker DC.



3. Sekrup kawat ke posisinya.
4. Masukkan steker DC kabel ke port Input DC.

Setelah menginstal perangkat Amazon One Anda, Anda siap untuk mengaktifkan perangkat.

## Mengaktifkan perangkat Amazon One

Ketika perangkat Amazon One Anda diinstal dan dinyalakan, Anda siap untuk mengaktifkannya.

Untuk mengaktifkan perangkat Amazon One Anda

1. Di perangkat Amazon One, ketuk layar untuk memulai.


2. Pilih Ethernet atau Wifi untuk terhubung ke internet.

Segera setelah perangkat terhubung ke internet, ia akan mulai mengunduh paket perangkat lunak terbaru.

3. Saat layar menunjukkan Unduhan perangkat lunak selesai! , pilih OK.
4. Pilih kode QR.

Layar perangkat Amazon One akan menampilkan Pindai kode QR.

5. [Untuk mengambil kode QR aktivasi, buka konsol Amazon One Enterprise di https://console.aws.amazon.com/one-enterprise.](https://console.aws.amazon.com/one-enterprise)

 Note

Kami sangat menyarankan Anda memberikan izin terbatas kepada penginstal Anda sehingga mereka hanya memiliki akses ke kode QR aktivasi di konsol Amazon One Enterprise Anda. Lihat [Tambahkan pengguna Amazon One](#).

6. Di panel navigasi, pilih Kode QR Aktivasi.
7. Dari daftar drop-down Pilih situs, pilih Situs tempat perangkat Amazon One diinstal.
8. Di bawah informasi Situs, konfirmasi alamat Situs.
9. Di bawah kode QR Aktivasi, cari nama instance perangkat yang Anda aktifkan, dan pilih kode Dapatkan QR yang sesuai untuk mengambil kode QR.
10. Pindai kode QR dengan perangkat Amazon One. Perhatikan bahwa kode QR disegarkan secara berkala untuk keamanan, Anda hanya dapat menggunakan kode QR sekali.
11. Masukkan kode pos situs, dan pilih Konfirmasi Pengaturan setelah memverifikasi situs yang benar ditampilkan.
12. Saat layar perangkat Amazon One menunjukkan Aktivasi selesai! , perangkat siap digunakan.

# Mendaftar dan memasukkan pengguna

Sekarang setelah perangkat Amazon One Anda diaktifkan, karyawan Anda dapat mulai mendaftarkan telapak tangan mereka dan mengautentikasi telapak tangan mereka untuk mendapatkan akses.

Topik

- [Membuat kebijakan endpoint](#)
- [Otentikasi untuk entri](#)

## Membuat kebijakan endpoint

Sebelum pengguna dapat mengotentikasi telapak tangan mereka untuk masuk, mereka harus melalui proses pendaftaran. Petugas keamanan harus selalu memeriksa identitas pengguna sebelum mengizinkan pengguna untuk mendaftar.

Untuk mendaftarkan telapak tangan Anda di perangkat Amazon One

1. Di perangkat pendaftaran Amazon One Enterprise, tekan Memulai.
2. Pindai lencana karyawan dengan pemindai lencana yang terhubung ke perangkat pendaftaran Amazon One Enterprise Anda.

Ketika lencana berhasil dipindai, layar perangkat Amazon One menunjukkan Lencana dipindai.

3. Baca Ketentuan Penggunaan, lalu tekan OK.
4. Baca Persetujuan - Informasi Biometrik Telapak Tangan Anda, dan tekan Saya setuju jika Anda menyetujui.
5. Ikuti petunjuk di layar untuk menyelesaikan proses pendaftaran.

## Otentikasi untuk entri

Setelah Anda berhasil mendaftarkan telapak tangan Anda, Anda siap untuk mengautentikasi dengan telapak tangan Anda di perangkat entri Amazon One Enterprise Anda.

Untuk mengautentikasi telapak tangan Anda untuk masuk di perangkat Amazon One

- Arahkan telapak tangan Anda di atas perangkat dan ikuti petunjuk di layar untuk memindai telapak tangan Anda.

# Mengelola pengguna

Anda dapat menggunakan halaman manajemen pengguna terdaftar untuk melacak pengguna terdaftar dan menghapus biometrik pengguna. Pengguna yang biometrik terkaitnya dihapus tidak akan lagi memiliki akses ke perangkat Amazon One untuk otentikasi.

Topik

- [Melihat pengguna terdaftar](#)
- [Menghapus pengguna terdaftar dan biometrik mereka](#)

## Melihat pengguna terdaftar

Prosedur berikut merinci cara mendaftarkan pengguna.

Untuk melihat pengguna terdaftar

1. Buka konsol Amazon One Enterprise di <https://console.aws.amazon.com/one-enterprise>.
2. Di panel navigasi, pilih Manajemen pengguna terdaftar.
3. Di bawah Pengguna terdaftar, Anda akan menemukan semua pengguna terdaftar dan detail berikut:
  - ID Lencana — Informasi pengenalan lencana yang ditangkap oleh pembaca lencana RFID pada saat pendaftaran.
  - Sumber pendaftaran - Detail perangkat Amazon One yang digunakan untuk pendaftaran.
  - Tanggal pendaftaran - Tanggal dan waktu pendaftaran.

## Menghapus pengguna terdaftar dan biometrik mereka

Prosedur berikut merinci cara menghapus pengguna terdaftar dan biometrik mereka.

Untuk menghapus pengguna terdaftar dan biometrik mereka

1. Buka konsol Amazon One Enterprise di <https://console.aws.amazon.com/one-enterprise>.
2. Di panel navigasi, pilih Manajemen pengguna terdaftar.

3. Di bawah Pengguna terdaftar, pilih ID lencana pengguna yang data biometrik telapak tangannya ingin Anda hapus.
4. Pilih Hapus Biometrik.
5. Pilih Hapus untuk mengonfirmasi penghapusan data biometrik pengguna.

 **Important**

Tindakan ini menghasilkan penghapusan permanen biometrik telapak tangan pengguna dari Amazon One Enterprise. Pengguna harus mendaftar lagi dengan perangkat pendaftaran Amazon One Enterprise untuk dapat menggunakan Amazon One Enterprise untuk otentikasi. Menghapus biometrik pengguna juga akan menghapus atribut profil lainnya secara permanen seperti ID lencana dari Amazon One Enterprise.

# Mengelola perangkat Amazon One

Setelah perangkat Amazon One Anda diinstal dan diaktifkan, perangkat mulai melaporkan kesehatan perangkat di konsol Amazon One Enterprise. Anda dapat menggunakan konsol Amazon One Enterprise untuk melakukan tugas manajemen perangkat seperti me-reboot perangkat atau memperbarui konfigurasi.

Topik

- [Memelihara dan membersihkan perangkat Amazon One](#)
- [Pengelolaan Situs](#)
- [Manajemen Instans Perangkat](#)

## Memelihara dan membersihkan perangkat Amazon One

Mempertahankan perangkat Amazon One Anda memberikan lingkungan pengoperasian perangkat dan pengalaman perangkat yang optimal.

Sebelum membersihkan perangkat Amazon One, pastikan hal berikut:

- Meskipun Anda tidak perlu mengaktifkan atau menonaktifkan Amazon One, pastikan perangkat terhubung ke daya, memiliki konektivitas jaringan, dan perangkat perifer dan pendamping apa pun (jika ada) terhubung.
- Tingkatkan masalah ke administrator Anda jika konektivitas jaringan tidak tersedia (layar kesalahan akan terlihat di perangkat Amazon One jika ini terjadi), layar kesalahan akan terlihat di perangkat Amazon One atau masalah koneksi perangkat akan terlihat di konsol.
- Perangkat yang aman secara fisik sehingga individu yang tidak berwenang tidak dapat mengutak-atik mereka.
- Periksa secara visual perangkat Amazon One setiap hari, periksa koneksi yang tidak sah ke perangkat Amazon One.
- Periksa semua sisi perangkat untuk mencari tanda-tanda gangguan, termasuk sekrup perangkat yang terlihat dan casing untuk memastikan tidak ada komponen gaps/openings internal/sirkuit internal perangkat Amazon One.
- Jika terjadi kesalahan atau kegagalan, ikuti petunjuk di layar perangkat Amazon One atau lihat panduan pemecahan masalah untuk memperbaiki masalah.

## Untuk membersihkan perangkat Amazon One

Membersihkan perangkat Amazon One Anda secara teratur menghilangkan noda atau bekas seperti sidik jari dan sidik jari.

### Note

Jangan gunakan produk pembersih lain di luar yang tercantum dalam panduan ini. Jadwal pembersihan yang disarankan adalah sekali atau dua kali seminggu, atau setiap kali kotoran, debu, atau noda terlihat pada perangkat, tetapi tidak pernah lebih dari sekali per hari.

1. Bersihkan perangkat Amazon One dengan Tisu Isopropyl Alcohol (IPA). Hanya bersihkan permukaan sentuh perangkat. Jangan menyentuh jendela optik, atau gunakan produk pembersih lainnya kecuali diperintahkan untuk melakukannya oleh Amazon One.
2. Bersihkan goresan dengan kain microfiber kering.
3. Debu Ringan (jangan bersihkan) kotoran atau kotoran yang terlihat dari jendela optik. Batasi pembersihan jendela optik tidak lebih dari sekali per hari and/or ketika jendela kotor secara visual (misalnya, finger/hand cetakan/noda). Bagian perangkat ini tidak dimaksudkan untuk disentuh, tetapi mungkin ada sentuhan yang tidak disengaja dari pelanggan baru.
4. Gunakan pembersih kartu KIC Smart untuk membersihkan bagian dalam pembaca kartu, jika ada.
5. Bersihkan perangkat sekali atau dua kali seminggu, atau kapan pun kotoran, debu, atau noda terlihat di perangkat.

## Pengelolaan Situs

Sebuah situs mewakili lokasi fisik di mana kumpulan instance perangkat diinstal dan beroperasi di. Anda dapat menggunakan situs untuk mengatur perangkat Amazon One yang berbagi alamat fisik yang sama.

Topik

- [Mengubah nama situs](#)
- [Memperbarui alamat situs](#)

## Mengubah nama situs

Prosedur berikut merinci cara mengubah nama situs untuk perangkat Anda.

Untuk mengubah nama situs

1. Buka konsol Amazon One Enterprise di <https://console.aws.amazon.com/one-enterprise>.
2. Di panel navigasi, pilih Situs.
3. Di bawah Situs, pilih situs yang ingin Anda edit namanya.
4. Pilih Edit.
5. Di bawah informasi Situs masukkan nama situs dan deskripsi situs yang diinginkan (opsional).
6. Pilih Simpan perubahan untuk diperbarui.

## Memperbarui alamat situs

Prosedur berikut merinci cara memperbarui alamat situs untuk perangkat Anda.

Untuk memperbarui alamat situs

1. Buka konsol Amazon One Enterprise di <https://console.aws.amazon.com/one-enterprise>.
2. Di panel navigasi, pilih Situs.
3. Di bawah Situs, pilih situs yang ingin Anda perbarui alamatnya.
4. Di bawah Instans Perangkat, pastikan jumlah instans yang diaktifkan adalah 0.
5. (Opsional) Jika jumlah instance yang diaktifkan bukan 0, lihat
6. Pilih Edit.
7. Di bawah Alamat fisik masukkan alamat fisik yang benar.
8. Pilih Simpan perubahan untuk diperbarui.

## Manajemen Instans Perangkat

Sebuah instance perangkat adalah representasi logis dari perangkat dengan konfigurasi.

Penggunaan instance perangkat memungkinkan untuk menukar perangkat Amazon One sambil secara otomatis mewarisi konfigurasi dan nama yang telah ditetapkan sebelumnya. Instans perangkat memiliki nama yang ditentukan pengguna (konvensi penamaan bersama dengan perangkat lunak kontrol akses Anda) dan serangkaian konfigurasi komunikasi.

## Topik

- [Melihat status instans perangkat](#)
- [Mem-boot ulang perangkat Amazon One](#)
- [Memperbarui konfigurasi perangkat Amazon One](#)
- [Memperbarui kredensi Wi-fi](#)
- [Menonaktifkan instance perangkat](#)

## Melihat status instans perangkat

Prosedur berikut merinci cara melihat status instans perangkat Anda.

Untuk melihat status instans perangkat

1. Buka konsol Amazon One Enterprise di <https://console.aws.amazon.com/one-enterprise>.
2. Di panel navigasi, pilih Instans perangkat.
3. Di bawah Instans yang diaktifkan, Anda akan melihat daftar perangkat Amazon One yang diaktifkan.
4. Pilih nama instance perangkat untuk melihat detail instance perangkat.

## Mem-boot ulang perangkat Amazon One

Prosedur berikut merinci cara me-reboot perangkat Amazon One Anda.

Untuk me-reboot perangkat Amazon One

1. Buka konsol Amazon One Enterprise di <https://console.aws.amazon.com/one-enterprise>.
2. Di panel navigasi, pilih Instans perangkat.
3. Di bawah Instance yang diaktifkan, pilih nama instans perangkat yang ingin Anda reboot.
4. Pilih Reboot untuk memulai ulang perangkat Amazon One.

## Memperbarui konfigurasi perangkat Amazon One

Prosedur berikut merinci cara memperbarui konfigurasi perangkat Amazon One.

## Untuk Memperbarui konfigurasi perangkat Amazon One

1. Buka konsol Amazon One Enterprise di <https://console.aws.amazon.com/one-enterprise>.
2. Di panel navigasi, pilih Instans perangkat.
3. Di bawah Instans yang diaktifkan, pilih nama instans perangkat yang ingin Anda perbarui.
4. Di bawah Konfigurasi perangkat, pilih Edit.

### Note

Untuk mengubah mode perangkat Amazon One, Anda harus terlebih dahulu menonaktifkan instance perangkat, dan kemudian mengkonfigurasinya dengan mode perangkat yang diinginkan (lihat [Konfigurasi instance perangkat untuk aktivasi](#)). Kemudian, Anda dapat melalui proses aktivasi perangkat (lihat [Mengaktifkan perangkat Amazon One](#)).

5. Setelah Anda membuat perubahan yang diinginkan, pilih Perbarui konfigurasi perangkat untuk mengonfirmasi pembaruan.

## Memperbarui kredensi Wi-fi

Prosedur berikut merinci cara memperbarui kredensial Wi-Fi.

Untuk memperbarui kredensi Wifi

1. Buka konsol Amazon One Enterprise di <https://console.aws.amazon.com/one-enterprise>.
2. Di panel navigasi, pilih Instans perangkat.
3. Di bawah Instans yang diaktifkan, pilih nama instans perangkat yang ingin Anda perbarui.
4. Di bawah Jaringan, pilih Edit.
5. Di bawah konfigurasi Wi-Fi, buat perubahan yang diinginkan.
6. Pilih Perbarui jaringan untuk mengonfirmasi pembaruan.

## Menonaktifkan instance perangkat

Prosedur berikut merinci cara menonaktifkan instance perangkat.

## Untuk menonaktifkan instance perangkat

1. Buka konsol Amazon One Enterprise di <https://console.aws.amazon.com/one-enterprise>.
2. Di panel navigasi, pilih Instans perangkat.
3. Di bawah Instans yang diaktifkan, pilih nama instance perangkat yang ingin Anda nonaktifkan.
4. Pilih Nonaktifkan perangkat.
5. Untuk mengonfirmasi penonaktifan, ketik 'nonaktifkan' di kotak pesan dan pilih Nonaktifkan perangkat.

# Keamanan

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. [Model tanggung jawab bersama](#) menjelaskan hal ini sebagai keamanan dari cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari [Program AWS Kepatuhan Program AWS Kepatuhan](#) . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon One Enterprise, lihat [AWS Layanan dalam Lingkup berdasarkan AWS Layanan Program Kepatuhan](#) .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Amazon One Enterprise. Topik berikut menunjukkan cara mengonfigurasi Amazon One Enterprise untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Amazon One Enterprise Anda.

## Topik

- [Perlindungan data di Amazon One Enterprise](#)
- [Manajemen identitas dan akses untuk Amazon One Enterprise](#)
- [Tindakan, sumber daya, dan kunci kondisi untuk Amazon One Enterprise](#)
- [Validasi kepatuhan untuk Amazon One Enterprise](#)

## Perlindungan data di Amazon One Enterprise

[Model tanggung jawab AWS bersama model](#) berlaku untuk perlindungan data di Amazon One Enterprise. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi

infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam [Pertanyaan Umum Privasi Data](#). Lihat informasi tentang perlindungan data di Eropa di pos blog [Model Tanggung Jawab Bersama dan GDPR AWS](#) di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensial dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat [Bekerja dengan CloudTrail jejak](#) di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di [Standar Pemrosesan Informasi Federal \(FIPS\) 140-3](#).

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Amazon One Enterprise atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDKs. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

## Untuk menggunakan enkripsi default data saat istirahat

Amazon One Enterprise menyediakan enkripsi secara default untuk melindungi data sensitif saat istirahat menggunakan kunci enkripsi AWS.

Kunci yang dimiliki AWS — Amazon One Enterprise menggunakan kunci ini secara default untuk mengenkripsi data pengguna akhir yang sensitif secara otomatis. Anda tidak dapat melihat, mengelola, atau menggunakan kunci yang dimiliki AWS, atau mengaudit penggunaannya. Namun, Anda tidak perlu mengambil tindakan apa pun atau mengubah program apa pun untuk melindungi kunci yang mengenkripsi data Anda. Untuk informasi selengkapnya, lihat kunci yang dimiliki AWS di Panduan Pengembang AWS Key Management Service.

## Mengenkripsi data saat transit

Amazon One Enterprise menggunakan Transport Layer Security (TLS) untuk mengamankan data dan Signature Versi 4 untuk mengautentikasi semua permintaan API masuk ke layanan AWS. Enkripsi ini diaktifkan secara default.

## Manajemen identitas dan akses untuk Amazon One Enterprise

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diotorisasi (memiliki izin) untuk menggunakan sumber daya Amazon One Enterprise. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- [Audiens](#)
- [Mengautentikasi dengan identitas](#)
- [Mengelola akses menggunakan kebijakan](#)
- [Bagaimana Amazon One Enterprise bekerja dengan IAM](#)
- [Contoh kebijakan berbasis identitas untuk Amazon One Enterprise](#)
- [AWS kebijakan terkelola untuk Amazon One Enterprise](#)

## Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda berdasarkan peran Anda:

- Pengguna layanan - minta izin dari administrator Anda jika Anda tidak dapat mengakses fitur (lihat [Memecahkan masalah identitas dan akses Amazon One](#))
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat [Bagaimana Amazon One Enterprise bekerja dengan IAM](#))
- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat [Contoh kebijakan berbasis identitas untuk Amazon One Enterprise](#))

## Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensial identitas Anda. Anda harus diautentikasi sebagai Pengguna root akun AWS, pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk sebagai identitas federasi menggunakan kredensial dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), autentikasi masuk tunggal, atau kredensial. Google/Facebook Untuk informasi selengkapnya tentang cara masuk, lihat [Cara masuk ke Akun AWS Anda](#) dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS sediakan SDK dan CLI untuk menandatangani permintaan secara kriptografis. Untuk informasi selengkapnya, lihat [AWS Signature Version 4 untuk permintaan API](#) dalam Panduan Pengguna IAM.

### Akun AWS pengguna root

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.

### Identitas terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS menggunakan kredensial sementara.

Identitas federasi adalah pengguna dari direktori perusahaan Anda, penyedia identitas web, atau Directory Service yang mengakses Layanan AWS menggunakan kredensial dari sumber identitas. Identitas terfederasi mengambil peran yang memberikan kredensial sementara.

Untuk manajemen akses terpusat, kami menyarankan AWS IAM Identity Center. Untuk informasi selengkapnya, lihat [Apa itu Pusat Identitas IAM?](#) dalam Panduan Pengguna AWS IAM Identity Center

## Pengguna dan grup IAM

[Pengguna IAM](#) adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk informasi selengkapnya, lihat [Mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredensial sementara](#) di Panduan Pengguna IAM.

[Grup IAM](#) menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat [Kasus penggunaan untuk pengguna IAM](#) dalam Panduan Pengguna IAM.

## Peran IAM

[Peran IAM](#) adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan [beralih dari pengguna ke peran IAM \(konsol\)](#) atau dengan memanggil operasi AWS CLI atau AWS API. Untuk informasi selengkapnya, lihat [Metode untuk mengambil peran](#) dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna terfederasi, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon EC2. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.

## Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat [Gambaran umum kebijakan JSON](#) dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukannya.

## Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan](#) dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat berupa kebijakan inline (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan pada banyak identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat [Pilih antara kebijakan terkelola dan kebijakan inline](#) dalam Panduan Pengguna IAM.

## Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contohnya termasuk kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Anda harus [menentukan principal](#) dalam kebijakan berbasis sumber daya.

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

## Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang dapat menetapkan izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat [Batasan izin untuk entitas IAM](#) dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCPs) — Tentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat [Kebijakan kontrol layanan](#) dalam Panduan Pengguna AWS Organizations .

- Kebijakan kontrol sumber daya (RCPs) — Tetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat [Kebijakan kontrol sumber daya \(RCPs\)](#) di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. Untuk informasi selengkapnya, lihat [Kebijakan sesi](#) dalam Panduan Pengguna IAM.

## Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat [Logika evaluasi kebijakan](#) di Panduan Pengguna IAM.

## Bagaimana Amazon One Enterprise bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Amazon One Enterprise, pelajari fitur IAM apa yang tersedia untuk digunakan dengan Amazon One Enterprise.

### Fitur IAM yang dapat Anda gunakan dengan Amazon One Enterprise

Fitur IAM	Dukungan Amazon One Enterprise
<a href="#">Kebijakan berbasis identitas</a>	Ya
<a href="#">Kebijakan berbasis sumber daya</a>	Tidak
<a href="#">Tindakan kebijakan</a>	Ya
<a href="#">Sumber daya kebijakan</a>	Ya
<a href="#">Kunci kondisi kebijakan</a>	Ya
<a href="#">ACLs</a>	Tidak
<a href="#">ABAC (tanda dalam kebijakan)</a>	Ya
<a href="#">Kredensial sementara</a>	Ya
<a href="#">Izin principal</a>	Ya

Fitur IAM	Dukungan Amazon One Enterprise
<a href="#">Peran layanan</a>	Tidak
<a href="#">Peran terkait layanan</a>	Tidak

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Amazon One Enterprise dan AWS layanan lainnya dengan sebagian besar fitur IAM, lihat [AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM](#).

## Kebijakan berbasis identitas untuk Amazon One Enterprise

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan](#) dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat [Referensi elemen kebijakan JSON IAM](#) dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk Amazon One Enterprise

Untuk melihat contoh kebijakan berbasis identitas Amazon One Enterprise, lihat. [Contoh kebijakan berbasis identitas untuk Amazon One Enterprise](#)

## Kebijakan berbasis sumber daya dalam Amazon One Enterprise

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya,

administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan principal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai principal dalam kebijakan berbasis sumber daya. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.

## Tindakan kebijakan untuk Amazon One Enterprise

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar tindakan Amazon One Enterprise, lihat [Tindakan, sumber daya, dan kunci kondisi untuk Amazon One Enterprise](#).

Tindakan kebijakan di Amazon One Enterprise menggunakan awalan berikut sebelum tindakan:

```
one
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [  
  "one:action1",  
  "one:action2"  
]
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard (\*). Sebagai contoh, untuk menentukan semua tindakan yang dimulai dengan kata Describe, sertakan tindakan berikut:

```
"Action": "one:Describe*"
```

Untuk melihat contoh kebijakan berbasis identitas Amazon One Enterprise, lihat. [Contoh kebijakan berbasis identitas untuk Amazon One Enterprise](#)

## Sumber daya kebijakan untuk Amazon One Enterprise

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen kebijakan JSON Resource menentukan objek yang menjadi target penerapan tindakan. Praktik terbaiknya, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, gunakan wildcard (\*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*" "
```

Untuk melihat daftar jenis sumber daya Amazon One Enterprise beserta jenisnya ARNs, dan untuk mempelajari tindakan yang dapat Anda gunakan untuk menentukan ARN dari setiap sumber daya, lihat. [Tindakan, sumber daya, dan kunci kondisi untuk Amazon One Enterprise](#)

Untuk melihat contoh kebijakan berbasis identitas Amazon One Enterprise, lihat. [Contoh kebijakan berbasis identitas untuk Amazon One Enterprise](#)

## Kunci kondisi kebijakan untuk Amazon One Enterprise

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. Anda dapat membuat ekspresi bersyarat yang menggunakan [operator kondisi](#), misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta. Untuk melihat semua kunci kondisi AWS global, lihat [kunci konteks kondisi AWS global](#) di Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi Amazon One Enterprise dan untuk mempelajari tindakan dan sumber daya yang dapat digunakan untuk menggunakan kunci kondisi, lihat [Tindakan, sumber daya, dan kunci kondisi untuk Amazon One Enterprise](#).

Untuk melihat contoh kebijakan berbasis identitas Amazon One Enterprise, lihat [Contoh kebijakan berbasis identitas untuk Amazon One Enterprise](#)

## ACLs di Amazon One Enterprise

Mendukung ACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON.

## ABAC dengan Amazon One Enterprise

Mendukung ABAC (tanda dalam kebijakan): Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut tanda. Anda dapat melampirkan tag ke entitas dan AWS sumber daya IAM, lalu merancang kebijakan ABAC untuk mengizinkan operasi saat tag prinsipal cocok dengan tag pada sumber daya.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di [elemen kondisi](#) dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat [Tentukan izin dengan otorisasi ABAC](#) dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat [Menggunakan kontrol akses berbasis atribut \(ABAC\)](#) dalam Panduan Pengguna IAM.

## Menggunakan kredensial sementara dengan Amazon One Enterprise

Mendukung kredensial sementara: Ya

Kredensial sementara menyediakan akses jangka pendek ke AWS sumber daya dan secara otomatis dibuat saat Anda menggunakan federasi atau beralih peran. AWS merekomendasikan agar Anda menghasilkan kredensial sementara secara dinamis alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat [Kredensial keamanan sementara di IAM](#) dan [Layanan AWS yang berfungsi dengan IAM](#) dalam Panduan Pengguna IAM.

## Izin utama lintas layanan untuk Amazon One Enterprise

Mendukung sesi akses terusan (FAS): Ya

Sesi akses terusan (FAS) menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat [Sesi akses terusan](#).

## Peran layanan untuk Amazon One Enterprise

Mendukung peran layanan: Tidak

Peran layanan adalah [peran IAM](#) yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS](#) dalam Panduan pengguna IAM.

### Warning

Mengubah izin untuk peran layanan dapat merusak fungsionalitas Amazon One Enterprise. Edit peran layanan hanya jika Amazon One Enterprise memberikan panduan untuk melakukannya.

## Peran terkait layanan untuk Amazon One Enterprise

Mendukung peran terkait layanan: Tidak

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul

di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang pembuatan atau manajemen peran terkait layanan, lihat [Layanan AWS yang berfungsi dengan IAM](#). Cari layanan dalam tabel yang memiliki Yes di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

## Contoh kebijakan berbasis identitas untuk Amazon One Enterprise

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Amazon One Enterprise. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihat [Membuat kebijakan IAM \(konsol\) di Panduan Pengguna IAM](#).

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Amazon One Enterprise, termasuk format ARNs untuk setiap jenis sumber daya, lihat [Tindakan, sumber daya, dan kunci kondisi untuk Amazon One Enterprise](#) di Referensi Otorisasi Layanan.

### Topik

- [Praktik terbaik kebijakan](#)
- [Menggunakan konsol Amazon One Enterprise](#)
- [Mengizinkan pengguna melihat izin mereka sendiri](#)
- [Akses hanya-baca ke Amazon One Enterprise](#)
- [Akses penuh ke Amazon One Enterprise](#)
- [Izin Tingkat Sumber Daya yang Didukung untuk Tindakan API Aturan Amazon One Enterprise](#)
- [Informasi tambahan](#)

### Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Amazon One Enterprise di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola

yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat [Kebijakan yang dikelola AWS](#) atau [Kebijakan yang dikelola AWS untuk fungsi tugas](#) dalam Panduan Pengguna IAM.

- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat [Kebijakan dan izin dalam IAM](#) dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti CloudFormation. Untuk informasi selengkapnya, lihat [Elemen kebijakan JSON IAM: Kondisi](#) dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat [Validasi kebijakan dengan IAM Access Analyzer](#) dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat [Amankan akses API dengan MFA](#) dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat [Praktik terbaik keamanan di IAM](#) dalam Panduan Pengguna IAM.

## Menggunakan konsol Amazon One Enterprise

Untuk mengakses konsol Amazon One Enterprise, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Amazon One Enterprise di Akun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang coba mereka lakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan konsol Amazon One Enterprise, lampirkan juga Amazon One Enterprise *ConsoleAccess* atau kebijakan *ReadOnly* AWS terkelola ke entitas. Untuk informasi selengkapnya, lihat [Menambah izin untuk pengguna](#) dalam Panduan Pengguna IAM.

## Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
```

```

    "Effect": "Allow",
    "Action": [
      "iam:GetGroupPolicy",
      "iam:GetPolicyVersion",
      "iam:GetPolicy",
      "iam:ListAttachedGroupPolicies",
      "iam:ListGroupPolicies",
      "iam:ListPolicyVersions",
      "iam:ListPolicies",
      "iam:ListUsers"
    ],
    "Resource": "*"
  }
]
}

```

## Akses hanya-baca ke Amazon One Enterprise

Contoh berikut menunjukkan kebijakan AWS terkelola, `AmazonOneEnterpriseReadOnlyAccess` yang memberikan akses hanya-baca ke Amazon One Enterprise.

Dalam pernyataan kebijakan, `Effect` elemen menentukan apakah tindakan diizinkan atau ditolak. `Action` Elemen mencantumkan tindakan spesifik yang diizinkan dilakukan pengguna. `Resource` Elemen mencantumkan AWS sumber daya yang diizinkan pengguna untuk melakukan tindakan tersebut. Untuk kebijakan yang mengontrol akses ke tindakan Amazon One Enterprise, `Resource` elemen selalu disetel ke `*`, wildcard yang berarti "semua sumber daya."

Nilai-nilai dalam `Action` elemen sesuai dengan APIs yang didukung layanan. Tindakan didahului oleh `config:` untuk menunjukkan bahwa mereka mengacu pada tindakan Amazon One Enterprise. Anda dapat menggunakan karakter `*` wildcard dalam `Action` elemen, seperti dalam contoh berikut:

- `"Action": ["one:*DeviceInstanceConfiguration"]`

Ini memungkinkan semua tindakan Amazon One Enterprise yang diakhiri dengan `DeviceInstance` "" (`GetDeviceInstanceConfiguration`, `CreateDeviceInstanceConfiguration`).

- `"Action": ["one:*"]`

Ini memungkinkan semua tindakan Amazon One Enterprise, tetapi bukan tindakan untuk AWS layanan lain.

- `"Action": ["*"]`

Ini memungkinkan semua AWS tindakan. Izin ini cocok untuk pengguna yang bertindak sebagai AWS administrator untuk akun Anda.

Kebijakan hanya-baca tidak memberikan izin pengguna untuk tindakan seperti `CreateDeviceInstance`, `UpdateDeviceInstance`, dan `DeleteDeviceInstance`. Pengguna dengan kebijakan ini tidak diizinkan untuk membuat instance perangkat, memperbarui instance perangkat, atau menghapus instance perangkat. Untuk daftar tindakan Amazon One Enterprise, lihat [Tindakan, sumber daya, dan kunci kondisi untuk Amazon One Enterprise](#).

## Akses penuh ke Amazon One Enterprise

Contoh berikut menunjukkan kebijakan yang memberikan akses penuh ke Amazon One Enterprise. Ini memberi pengguna izin untuk melakukan semua tindakan Amazon One Enterprise.

### Important

Kebijakan ini memberikan izin yang luas. Sebelum memberikan akses penuh, pertimbangkan untuk memulai dengan seperangkat izin minimum dan memberikan izin tambahan seperlunya. Melakukannya adalah praktik yang lebih baik daripada memulai dengan izin yang terlalu lunak dan kemudian mencoba mengencangkannya nanti.

## Izin Tingkat Sumber Daya yang Didukung untuk Tindakan API Aturan Amazon One Enterprise

Izin tingkat sumber daya mengacu pada kemampuan untuk menentukan sumber daya mana yang boleh digunakan oleh para pengguna untuk melakukan tindakan. Amazon One Enterprise mendukung izin tingkat sumber daya untuk tindakan API aturan Amazon One Enterprise tertentu. Ini berarti bahwa untuk tindakan aturan Amazon One Enterprise tertentu, Anda dapat mengontrol kondisi di mana pengguna diizinkan untuk menggunakan tindakan tersebut. Kondisi ini dapat berupa tindakan yang harus dipenuhi, atau sumber daya tertentu yang diizinkan untuk digunakan pengguna.

Tabel berikut menjelaskan tindakan API aturan Amazon One Enterprise yang saat ini mendukung izin tingkat sumber daya. Ini juga menjelaskan sumber daya yang didukung dan mereka ARNs untuk setiap tindakan. Saat menentukan ARN, Anda dapat menggunakan wildcard \* di jalur Anda; misalnya, ketika Anda tidak dapat atau tidak ingin menentukan sumber daya yang tepat. IDs

**⚠ Important**

Jika tindakan API aturan Amazon One Enterprise tidak tercantum dalam tabel ini, maka tindakan tersebut tidak mendukung izin tingkat sumber daya. Jika tindakan aturan Amazon One Enterprise tidak mendukung izin tingkat sumber daya, Anda dapat memberikan izin kepada pengguna untuk menggunakan tindakan tersebut, tetapi Anda harus menentukan \* untuk elemen sumber daya pernyataan kebijakan Anda.

Tindakan API	Sumber daya
CreateDeviceInstance	Instans Perangkat <i>arn:aws:one::device-instance/ region:accountID deviceInstanceId</i>
GetDeviceInstance	Instans Perangkat <i>arn:aws:one::device-instance/ region:accountID deviceInstanceId</i>
UpdateDeviceInstance	Instans Perangkat <i>arn:aws:one::device-instance/ region:accountID deviceInstanceId</i>
DeleteDeviceInstance	Instans Perangkat <i>arn:aws:one::device-instance/ region:accountID deviceInstanceId</i>
CreateDeviceActivationQrCode	Instans Perangkat <i>arn:aws:one::device-instance/ region:accountID deviceInstanceId</i>
DeleteAssociatedDevice	Instans Perangkat

Tindakan API	Sumber daya
	arn:aws:one ::device-instance/ <i>region:accountID deviceInstanceId</i>
RebootDevice	Instans Perangkat
	arn:aws:one ::device-instance/ <i>region:accountID deviceInstanceId</i>
CreateDeviceInstanceConfiguration	Konfigurasi Instans Perangkat
	arn:aws:one ::device-instance/ /configuration/ <i>region:accountID deviceInstanceId version</i>
GetDeviceInstanceConfiguration	Konfigurasi Instans Perangkat
	arn:aws:one ::device-instance/ /configuration/ <i>region:accountID deviceInstanceId version</i>
CreateSite	Situs
	arn:aws:one ::site/ <i>region:accountID siteId</i>
DeleteSite	Situs
	arn:aws:one ::site/ <i>region:accountID siteId</i>
GetSiteAddress	Situs
	arn:aws:one ::site/ <i>region:accountID siteId</i>
UpdateSite	Situs
	arn:aws:one ::site/ <i>region:accountID siteId</i>
UpdateSiteAddress	Situs
	arn:aws:one ::site/ <i>region:accountID siteId</i>

Tindakan API	Sumber daya
CreateDeviceConfigurationTemplate	Template Konfigurasi Perangkat arn:aws:one:: <i>region:accountID</i> device-configuration-template <i>templateId</i>
DeleteDeviceConfigurationTemplate	Template Konfigurasi Perangkat arn:aws:one:: <i>region:accountID</i> device-configuration-template <i>templateId</i>
GetDeviceConfigurationTemplate	Template Konfigurasi Perangkat arn:aws:one:: <i>region:accountID</i> device-configuration-template <i>templateId</i>
UpdateDeviceConfigurationTemplate	Template Konfigurasi Perangkat arn:aws:one:: <i>region:accountID</i> device-configuration-template <i>templateId</i>

Misalnya, Anda ingin mengizinkan akses baca dan menolak akses tulis ke aturan tertentu untuk pengguna tertentu.

Dalam kebijakan pertama, Anda mengizinkan tindakan membaca AWS Config aturan seperti `GetSite` pada aturan yang ditentukan.

Dalam kebijakan kedua, Anda menolak tindakan penulisan aturan Amazon One Enterprise pada aturan tertentu.

Dengan izin tingkat sumber daya, Anda dapat mengizinkan akses baca dan menolak akses tulis untuk melakukan tindakan tertentu pada tindakan API aturan Amazon One Enterprise.

## Informasi tambahan

Untuk mempelajari selengkapnya tentang membuat pengguna, grup, kebijakan, dan izin IAM, lihat [Membuat Grup Pengguna dan Administrator IAM Pertama Anda dan Manajemen Akses](#) di Panduan Pengguna IAM.

## AWS kebijakan terkelola untuk Amazon One Enterprise

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, pembaruan 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.

### AmazonOneEnterpriseFullAccess

Kebijakan ini memberikan izin administratif yang memungkinkan akses ke semua sumber daya dan operasi Amazon One Enterprise.

one : \*Memungkinkan Anda melakukan semua tindakan Amazon One Enterprise.

#### JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "FullAccessStatementID",
```

```
"Effect": "Allow",
"Action": [
  "one:*"
],
"Resource": "*"
}
]
}
```

## AmazonOneEnterpriseReadOnlyAccess

Kebijakan ini memberikan izin baca saja ke semua sumber daya dan operasi Amazon One Enterprise.

one:Get\*Mendapatkan sumber daya Amazon One Enterprise.

one:List\*Daftar sumber daya Amazon One Enterprise.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ReadOnlyAccessStatementID",
      "Effect": "Allow",
      "Action": [
        "one:Get*",
        "one:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

## AmazonOneEnterpriseInstallerAccess

Kebijakan ini memberikan izin baca dan tulis terbatas yang memungkinkan Anda membuat kode QR aktivasi untuk instans perangkat yang dikonfigurasi untuk mengaktifkan perangkat di situs mana pun.

`one:CreateDeviceActivationQrCode` Memungkinkan Anda membuat kode QR untuk mengaktifkan perangkat.

`one:GetDeviceInstance` Memungkinkan Anda mengambil informasi tentang instans perangkat Amazon One.

`one:GetSite` Memungkinkan Anda mengambil informasi tentang situs Amazon One Enterprise.

`one:GetSiteAddress` Memungkinkan Anda mengambil alamat fisik situs Amazon One Enterprise.

`one:ListDeviceInstances` Memungkinkan Anda membuat daftar instans perangkat Amazon One.

`one:ListSites` Memungkinkan Anda membuat daftar situs Amazon One Enterprise.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "InstallerAccessStatementID",
      "Effect": "Allow",
      "Action": [
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceInstances",
        "one:ListSites"
      ],
      "Resource": "*"
    }
  ]
}
```

Amazon One Enterprise memperbarui kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Amazon One Enterprise yang telah dibuat sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman riwayat Amazon One Enterprise Document.

Ubah	Deskripsi	Date
Amazon One Enterprise ditambahkan AmazonOneMetricPublishAccess	Kebijakan izin peran bernama AmazonOneMetricPublishAccess memungkinkan Amazon One Enterprise untuk melakukan CloudWatch: PutMetricData di CloudWatch Namespace AWS/AmazonOne	Februari 6, 2025
Amazon One Enterprise mulai melacak perubahan	Amazon One Enterprise mulai melacak perubahan untuk kebijakan yang AWS dikelola.	1 Desember 2023

## Tindakan, sumber daya, dan kunci kondisi untuk Amazon One Enterprise

Amazon One Enterprise (awalan layanan:one) menyediakan kunci konteks sumber daya, tindakan, dan kondisi khusus layanan berikut untuk digunakan dalam kebijakan izin IAM.

### Topik

- [Tindakan yang ditentukan oleh Amazon One Enterprise](#)
- [Jenis sumber daya yang ditentukan oleh Amazon One Enterprise](#)
- [Kunci kondisi untuk Amazon One Enterprise](#)

## Tindakan yang ditentukan oleh Amazon One Enterprise

Anda dapat menyebutkan tindakan berikut dalam elemen `Action` pernyataan kebijakan IAM. Gunakan kebijakan untuk memberikan izin untuk melaksanakan operasi dalam AWS. Saat Anda

menggunakan sebuah tindakan dalam sebuah kebijakan, Anda biasanya mengizinkan atau menolak akses ke operasi API atau perintah CLI dengan nama yang sama. Namun, dalam beberapa kasus, satu tindakan tunggal mengontrol akses ke lebih dari satu operasi. Atau, beberapa operasi memerlukan beberapa tindakan yang berbeda.

Kolom tipe sumber daya pada tabel Tindakan menunjukkan apakah setiap tindakan mendukung izin tingkat sumber daya. Jika tidak ada nilai untuk kolom ini, Anda harus menentukan semua sumber daya (“\*”) yang berlaku kebijakan dalam Resource elemen pernyataan kebijakan Anda. Jika kolom mencantumkan jenis sumber daya, maka Anda dapat menyebutkan ARN dengan jenis tersebut dalam sebuah pernyataan dengan tindakan tersebut. Jika tindakan memiliki satu atau lebih sumber daya yang diperlukan, pemanggil harus memiliki izin untuk menggunakan tindakan dengan sumber daya tersebut. Sumber daya yang diperlukan ditunjukkan dalam tabel dengan tanda bintang (\*). Jika Anda membatasi akses sumber daya dengan Resource elemen dalam kebijakan IAM, Anda harus menyertakan ARN atau pola untuk setiap jenis sumber daya yang diperlukan. Beberapa tindakan mendukung berbagai jenis sumber daya. Jika jenis sumber daya opsional (tidak ditunjukkan sesuai kebutuhan), maka Anda dapat memilih untuk menggunakan salah satu jenis sumber daya opsional.

Kolom Condition keys pada tabel Actions menyertakan kunci yang dapat Anda tentukan dalam Condition elemen pernyataan kebijakan. Untuk informasi selengkapnya tentang kunci kondisi yang terkait dengan sumber daya untuk layanan, lihat kolom Kunci kondisi pada tabel Jenis sumber daya.

#### Note

Kunci kondisi sumber daya tercantum dalam tabel [Jenis sumber daya](#). Anda dapat menemukan tautan ke jenis sumber daya yang berlaku untuk tindakan di kolom Jenis sumber daya (\*wajib) pada tabel Tindakan. Jenis sumber daya dalam tabel Jenis sumber daya menyertakan kolom Kunci kondisi, yang merupakan kunci kondisi sumber daya yang berlaku untuk tindakan dalam tabel Tindakan.

Untuk detail tentang kolom dalam tabel berikut, lihat [Tabel tindakan](#).

Tindakan	Deskripsi	Tingkat akses	Jenis sumber daya (*diperlukan)	Kunci syarat	Tindakan bergantung
CreateDeviceInstance	Berikan izin untuk membuat instance perangkat	Tulis		<a href="#">aws:RequestTag/\${TagKey}</a>  <a href="#">aws:TagKeys</a>	
GetDeviceInstance	Berikan izin untuk mendapatkan informasi tentang instance perangkat	Baca	perangkat-instance*		
ListDeviceInstances	Berikan izin untuk mencantumkan instance perangkat	Baca			
UpdateDeviceInstance	Berikan izin untuk memperbaiki instance perangkat	Tulis	perangkat-instance*		
DeleteDeviceInstance	Berikan izin untuk menghapus instance perangkat	Tulis	perangkat-instance*		
CreateDeviceActivationQRCode	Berikan izin untuk membuat kode QR untuk mengaktifkan perangkat pada instance perangkat	Tulis	perangkat-instance*		
DeleteAssociatedDevice	Berikan izin untuk menghapus asosiasi antara perangkat dan instans perangkat	Tulis	perangkat-instance*		

Tindakan	Deskripsi	Tingkat akses	Jenis sumber daya (*diperlukan)	Kunci syarat	Tindakan bergantung
RebootDevice	Berikan izin untuk me-reboot perangkat	Tulis	perangkat-instance*		
CreateDeviceInstanceConfiguration	Berikan izin untuk membuat konfigurasi instance perangkat	Tulis			
GetDeviceInstanceConfiguration	Berikan izin untuk mendapatkan informasi tentang konfigurasi instance perangkat	Baca	konfigurasi*		
CreateSite	Berikan izin untuk membuat situs	Tulis		<a href="#">aws:RequestTag/\${TagKey}</a> <a href="#">aws:TagKeys</a>	
DeleteSite	Berikan izin untuk menghapus instance perangkat	Tulis	situs*		
GetSite	Memberikan izin untuk mendapatkan informasi tentang situs	Baca	situs*		
ListSites	Berikan izin untuk membuat daftar situs	Baca			
GetSiteAddress	Berikan izin untuk mendapatkan informasi tentang alamat situs	Baca	situs*		

Tindakan	Deskripsi	Tingkat akses	Jenis sumber daya (*diperlukan)	Kunci syarat	Tindakan bergantung
UpdateSite	Memberikan izin untuk memperbarui situs	Tulis	situs*		
UpdateSiteAddress	Berikan izin untuk memperbarui alamat situs	Tulis	situs*		
CreateDeviceConfigurationTemplate	Berikan izin untuk membuat instance perangkat	Tulis		<a href="#">aws:RequestTag/\${TagKey}</a> <a href="#">aws:TagKeys</a>	
DeleteDeviceConfigurationTemplate	Berikan izin untuk menghapus templat konfigurasi perangkat	Tulis	device-configuration-template*		
GetDeviceConfigurationTemplate	Berikan izin untuk mendapatkan informasi tentang templat konfigurasi perangkat	Baca	device-configuration-template*		
ListDeviceConfigurationTemplates	Berikan izin untuk membuat daftar templat konfigurasi perangkat	Baca			
UpdateDeviceConfigurationTemplate	Berikan izin untuk memperbaiki templat konfigurasi perangkat	Tulis	device-configuration-template*		

Tindakan	Deskripsi	Tingkat akses	Jenis sumber daya (*diperlukan)	Kunci syarat	Tindakan bergantung
TagResource	Memberikan izin untuk menandai sumber daya	Penandaan	perangkat -contoh, situs, device-configuration-template	<a href="#">aws:RequestTag/\${TagKey}</a>  <a href="#">aws:TagKeys</a>	
UntagResource	Memberikan izin untuk menghapus tag sumber daya	Penandaan	perangkat -contoh, situs, device-configuration-template	<a href="#">aws:TagKeys</a>	
ListTagForResource	Memberikan izin untuk mencantumkan tag untuk sumber daya	Baca			

## Jenis sumber daya yang ditentukan oleh Amazon One Enterprise

Jenis sumber daya berikut ditentukan oleh layanan ini dan dapat digunakan dalam elemen `Resource` pernyataan kebijakan izin IAM. Setiap tindakan dalam [Tabel tindakan](#) mengidentifikasi jenis sumber daya yang dapat ditentukan dengan tindakan tersebut. Jenis sumber daya juga dapat menentukan kunci kondisi mana yang dapat Anda sertakan dalam kebijakan. Tombol-tombol ini ditampilkan di kolom terakhir dari tabel Jenis sumber daya. Untuk detail tentang kolom dalam tabel berikut, lihat [Tabel tipe sumber daya](#).

Jenis sumber daya	ARN	Kunci syarat
Device Instance	arn:aws:one: <i>region:accountID</i> :device-instance/ <i>deviceInstanceId</i>	<a href="#">aws:ResourceTag/\${TagKey}</a>
Device Instance Configuration	arn:aws:one: <i>region:accountID</i> :device-instance/ <i>deviceInstanceId</i> /configuration/ <i>version</i>	
Site	arn:aws:one: <i>region:accountID</i> :site/ <i>siteId</i>	<a href="#">aws:ResourceTag/\${TagKey}</a>
Device Configuration Template	arn:aws:one: <i>region:accountID</i> :device-configuration-template/ <i>templateId</i>	<a href="#">aws:ResourceTag/\${TagKey}</a>

## Kunci kondisi untuk Amazon One Enterprise

Amazon One Enterprise mendefinisikan kunci kondisi berikut yang dapat digunakan dalam Condition elemen kebijakan IAM. Anda dapat menggunakan kunci ini untuk menyempurnakan syarat lebih lanjut saat pernyataan kebijakan berlaku. Untuk detail tentang kolom dalam tabel berikut, lihat [Tabel tombol kondisi](#).

Untuk melihat kunci kondisi global yang tersedia untuk semua layanan, lihat [Kunci kondisi global yang tersedia](#).

Kunci syarat	Deskripsi	Tipe
aws:RequestTag/\${TagKey}	Memfilter akses dengan tag dari permintaan	String
aws:ResourceTag/\${TagKey}	Memfilter akses dengan tag yang terkait dengan sumber daya	String
aws:TagKeys	Memfilter akses dengan kunci tag dari permintaan	ArrayOfString

## Validasi kepatuhan untuk Amazon One Enterprise

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat [Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS](#) dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat [Program AWS Kepatuhan Program AWS](#) .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat [Mengunduh Laporan di AWS Artifact](#) .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. Untuk informasi selengkapnya tentang tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS, lihat [Dokumentasi AWS Keamanan](#).

# Memantau Amazon One Enterprise

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja Amazon One Enterprise dan AWS solusi Anda yang lain. AWS menyediakan alat pemantauan berikut untuk menonton Amazon One Enterprise, melaporkan ketika ada sesuatu yang salah, dan mengambil tindakan otomatis bila perlu:

- Amazon EventBridge dapat digunakan untuk mengotomatiskan AWS layanan Anda dan merespons secara otomatis peristiwa sistem, seperti masalah ketersediaan aplikasi atau perubahan sumber daya. Acara dari AWS layanan dikirimkan ke EventBridge dalam waktu dekat. Anda dapat menuliskan aturan sederhana untuk menunjukkan peristiwa mana yang sesuai kepentingan Anda, dan tindakan otomatis mana yang diambil ketika suatu peristiwa sesuai dengan suatu aturan. Untuk informasi selengkapnya, lihat [Panduan EventBridge Pengguna Amazon](#).
- AWS CloudTrail menangkap panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama AWS akun Anda dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk informasi selengkapnya, silakan lihat [Panduan Pengguna AWS CloudTrail](#).

## Memantau peristiwa Amazon One Enterprise di Amazon EventBridge

Anda dapat memantau peristiwa Amazon One Enterprise di EventBridge, yang mengirimkan aliran data waktu nyata dari aplikasi, aplikasi software-as-a-service (SaaS), dan layanan Anda sendiri. AWS EventBridge merutekan data tersebut ke target seperti AWS Lambda dan Amazon Simple Notification Service. Peristiwa ini memberikan aliran peristiwa sistem yang mendekati waktu nyata yang menggambarkan perubahan AWS sumber daya.

## Berlangganan acara Amazon One Enterprise

Acara perubahan status perangkat dan profil pengguna Amazon One dipublikasikan menggunakan EventBridge, dan dapat diaktifkan di EventBridge konsol dengan membuat aturan baru. Meskipun acara tidak dipesan, mereka memiliki stempel waktu yang memungkinkan Anda untuk mengonsumsi data. Peristiwa dipancarkan atas dasar [upaya terbaik](#).

## Untuk berlangganan acara Amazon One Enterprise

1. Masuk ke konsol AWS Anda di <https://console.aws.amazon.com/events/>.
2. Buka EventBridge konsol di <https://console.aws.amazon.com/events/>.
3. Di panel navigasi, di bawah Bus, pilih Aturan.
4. Pilih Buat aturan.
5. Pada halaman detail aturan Default, tetapkan nama ke aturan.
6. Pilih Aturan dengan pola peristiwa, lalu pilih Berikutnya.
7. Pada halaman pola acara Build, di bawah Sumber acara, verifikasi bahwa AWS peristiwa atau acara EventBridge mitra dipilih.
8. Di bawah Contoh jenis peristiwa, pilih AWS Events.
9. Untuk metode Creation, pilih Custom pattern.
10. Di bagian Pola acara, tambahkan JSON dengan sumber peristiwa sebagai aws : one dan tipe detail yang diperlukan:

```
"
  source": ["aws.one"],
  "detail-type": ["New Successful Enrollment",
    "New Successful Un-enrollment",
    "Unsuccessful Enrollment",
    "Unsuccessful Un-enrollment",
    "Successful Recognition",
    "Unsuccessful Recognition",
    "New Alert(s) Detected",
    "Some Alert(s) Cleared"]
}
```

Anda dapat memilih jenis detail yang diperlukan dari daftar di atas dan menghapus apa yang tidak diperlukan.

11. Pilih Berikutnya.
12. Pada halaman Pilih target, pilih target pilihan Anda, yang mencakup fungsi Lambda, antrian SQS, atau topik SNS. Untuk informasi tentang mengonfigurasi target, lihat [EventBridge Target Amazon](#).

Misalnya, untuk melihat kapan seseorang masuk, pilih “Pengakuan Sukses”. Kemudian lihat detail acara (diberikan dalam Lampiran) untuk melihat siapa yang masuk.

Untuk menyelesaikan alur kerja Anda, Anda dapat menjalankan API eksternal atau target lain.

13. Secara opsional, Anda dapat mengonfigurasi tag.
14. Pada halaman Tinjau dan buat, pilih Buat aturan. Untuk informasi selengkapnya tentang mengonfigurasi aturan, lihat [EventBridgeaturan](#) di Panduan EventBridge Pengguna.

## Jenis peristiwa perubahan status perangkat

Peristiwa perubahan status perangkat dihasilkan di JSON. Untuk setiap jenis acara, gumpalan JSON dikirim ke target pilihan Anda, seperti yang dikonfigurasi dalam aturan. Jenis detail berikut tersedia:

### Beberapa Peringatan Dihapus

Perangkat melewati satu atau lebih pemeriksaan kesehatan.

### Peringatan Baru Terdeteksi

Perangkat gagal satu atau lebih pemeriksaan kesehatan.

### sumber daya

Berisi daftar DeviceInstance arn tempat peristiwa Perubahan Status Perangkat dipublikasikan.

### data

#### ClearedAlerts

- Merupakan pemeriksaan kesehatan yang sebelumnya gagal DeviceInstance.
- Terdiri dari StatusCode untuk jenis alert dan timestamp ReporteDat.
- Kemungkinan nilai StatusCode:, NetworkDisconnected USBDisconnected

#### CurrentAlerts

- Merupakan status DeviceInstance saat ini.
- Terdiri dari StatusCode untuk jenis alert dan timestamp ReporteDat.
- Kemungkinan nilai StatusCode:, NetworkDisconnected USBDisconnected

#### Newalerts

- Merupakan pemeriksaan kesehatan DeviceInstance yang baru gagal.

- Terdiri dari StatusCode untuk jenis alert dan timestamp ReporteDat.
  - Kemungkinan nilai StatusCode: NetworkDisconnected USBDisconnected
- currentAlertsCount
- Hitungan pemeriksaan kesehatan yang saat ini gagal dengan DeviceInstance.
- assetTagId
- Perangkat assetTagId yang terkait dengan DeviceInstance.
- deviceInstanceName
- Nama DeviceInstance tempat Peristiwa Status Perangkat diterbitkan.
- SiteName
- Nama situs tempat DeviceInstance hadir.
- SitEArn
- Arn untuk situs tempat DeviceInstance hadir.

## Jenis acara profil pengguna

Jenis detail acara terkait profil Pengguna adalah:

### Pendaftaran Baru yang Sukses

Ketika pengguna berhasil mendaftar.

### Pendaftaran PBB Baru yang Berhasil

Ketika pengguna berhasil tidak terdaftar.

### Pendaftaran yang Tidak Berhasil

Ketika pengguna gagal mendaftar.

### Pendaftaran PBB yang tidak berhasil

Ketika pengguna gagal membatalkan pendaftaran.

### Pengakuan Sukses

Ketika pengguna memindai palm untuk otentikasi berhasil.

### Pengakuan yang Tidak Berhasil

Ketika pengenalan pemindaian telapak tangan gagal.

## sumber daya

Berisi daftar profil pengguna arn tempat acara profil pengguna diterbitkan.

### data

#### accountId

- AWS Akun yang relevan untuk perangkat yang memulai permintaan.

#### RequestSource

- Ini adalah deviceId perangkat yang memulai permintaan.

#### dibuatTimeStamps

- Waktu acara sedang dibuat.

#### UserStatus

- Status pengguna saat ini.
- Nilai yang mungkin: AKTIF, DIHAPUS

#### AssociateDid

- Id terkait pengguna, misalnya id lencana.

#### akal budi

- Nilai ini akan hadir untuk acara yang gagal. Ini berisi alasan mengapa acara itu tidak berhasil.

## Contoh acara

Contoh berikut menunjukkan acara untuk Amazon One Enterprise.

### Topik

- [Status kesehatan perangkat berubah menjadi sehat](#)
- [Status kesehatan perangkat berubah menjadi kritis](#)
- [Konektivitas perangkat diubah menjadi online](#)
- [Konektivitas perangkat diubah menjadi offline](#)

## Status kesehatan perangkat berubah menjadi sehat

Perangkat melewati semua pemeriksaan kesehatan.

```
{
  "version": "0",
  "id": "51e022b4-7ce6-34e0-264b-370948fc1123",
  "detail-type": "Some Alert(s) Cleared",
  "source": "aws.one",
  "account": "123456789012",
  "time": "2025-07-17T19:32:42Z",
  "region": "us-east-1",
  "resources":
  [
    "arn:aws:one:us-east-1:123456789012:deviceInstance/F5JRte5Jz21Tqx"
  ],
  "detail":
  {
    "version": "1.0.0",
    "data":
    {
      "clearedAlerts":
      [
        {
          "statusCode": "USBDisconnected",
          "reportedAt": "Thu Jul 17 19:32:42 UTC 2025"
        }
      ],
      "currentAlerts":
      [],
      "currentAlertsCount": 0,
      "assetTagId": "0000123456",
      "deviceInstanceName": "device_name",
      "siteName": "site_name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    }
  }
}
```

## Status kesehatan perangkat berubah menjadi kritis

Perangkat gagal satu atau lebih pemeriksaan kesehatan.

```
{
  "version": "0",
  "id": "07af4893-ef9f-965a-d245-3f0c8bd3c123",
  "detail-type": "New Alert(s) Detected",
```

```
"source": "aws.one",
"account": "123456789012",
"time": "2025-07-17T19:26:58Z",
"region": "us-east-1",
"resources":
[
  "arn:aws:one:us-east-1:123456789012:deviceInstance/12345678901234"
],
"detail":
{
  "version": "1.0.0",
  "data":
  {
    "newAlerts":
    [
      {
        "statusCode": "USBDisconnected",
        "reportedAt": "Thu Jul 17 19:26:58 UTC 2025"
      }
    ],
    "currentAlerts":
    [
      {
        "statusCode": "USBDisconnected",
        "reportedAt": "Thu Jul 17 19:26:58 UTC 2025"
      }
    ],
    "currentAlertsCount": 1,
    "assetTagId": "0000123456",
    "deviceInstanceName": "device_name",
    "siteName": "site_name",
    "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
  }
}
}
```

## Konektivitas perangkat diubah menjadi online

Perangkat sekarang terhubung ke internet.

```
{
  "version": "0",
  "id": "e6ecea28-dd60-5061-29f8-dfbc902f4123",
```

```

"detail-type": "Some Alert(s) Cleared",
"source": "aws.one",
"account": "123456789012",
"time": "2025-07-17T18:28:23Z",
"region": "us-east-1",
"resources":
[
  "arn:aws:one:us-east-1:123456789012:deviceInstance/12345678901234"
],
"detail":
{
  "version": "1.0.0",
  "data":
  {
    "clearedAlerts":
    [
      {
        "statusCode": "NetworkDisconnected",
        "reportedAt": "Thu Jul 17 18:28:23 UTC 2025"
      }
    ],
    "currentAlerts":
    [],
    "currentAlertsCount": 0,
    "assetTagId": "0000123456",
    "deviceInstanceName": "device_name",
    "siteName": "site_name",
    "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
  }
}
}

```

## Konektivitas perangkat diubah menjadi offline

Perangkat tidak lagi terhubung ke internet.

```

{
  "version": "0",
  "id": "e6ecea28-dd60-5061-29f8-dfbc902f4123",
  "detail-type": "New Alert(s) Detected",
  "source": "aws.one",
  "account": "123456789012",
  "time": "2025-07-17T18:28:23Z",

```

```
"region": "us-east-1",
"resources":
[
  "arn:aws:one:us-east-1:123456789012:deviceInstance/12345678901234"
],
"detail":
{
  "version": "1.0.0",
  "data":
  {
    "newAlerts":
    [
      {
        "statusCode": "NetworkDisconnected",
        "reportedAt": "Thu Jul 17 18:28:23 UTC 2025"
      }
    ],
    "currentAlerts":
    [
      {
        "statusCode": "NetworkDisconnected",
        "reportedAt": "Thu Jul 17 18:28:23 UTC 2025"
      }
    ],
    "currentAlertsCount": 1,
    "assetTagId": "0000123456",
    "deviceInstanceName": "device_name",
    "siteName": "site_name",
    "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
  }
}
}
```

## Mencatat panggilan API Amazon One Enterprise menggunakan AWS CloudTrail

Amazon One Enterprise terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Amazon One Enterprise. CloudTrail menangkap semua panggilan API untuk Amazon One Enterprise sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari konsol Amazon One Enterprise dan panggilan kode ke operasi Amazon One Enterprise API. Jika Anda membuat jejak, Anda dapat mengaktifkan

pengiriman CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk Amazon One Enterprise. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk Amazon One Enterprise, alamat IP dari mana permintaan itu dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat [Panduan AWS CloudTrail Pengguna](#).

## Informasi Amazon One Enterprise di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di Amazon One Enterprise, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS. Untuk informasi selengkapnya, lihat [Melihat peristiwa dengan Riwayat CloudTrail acara](#).

Untuk catatan acara yang sedang berlangsung di Anda Akun AWS, termasuk acara untuk Amazon One Enterprise, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- [Gambaran umum untuk membuat jejak](#)
- [CloudTrail layanan dan integrasi yang didukung](#)
- [Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail](#)
- [Menerima file CloudTrail log dari beberapa wilayah](#) dan [Menerima file CloudTrail log dari beberapa akun](#)

Semua tindakan Amazon One Enterprise dicatat oleh CloudTrail dan didokumentasikan dalam file [Tindakan, sumber daya, dan kunci kondisi untuk Amazon One Enterprise](#). Misalnya, panggilan ke `ListSites`, `RebootDevice` dan `DeleteDeviceInstance` tindakan menghasilkan entri dalam file CloudTrail log.

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut ini:

- Apakah permintaan itu dibuat dengan kredensial pengguna root atau AWS Identity and Access Management (IAM).
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat [Elemen userIdentity CloudTrail](#).

## Memahami entri file log Amazon One Enterprise

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber mana pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan CreateSite tindakan.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDAKDBG0AT6C2EXAMPLE:J_D0E",
    "arn": "arn:aws:sts::123456789012:assumed-role/Admin/J_D0E",
    "accountId": "123456789012",
    "accessKeyId": "AKIALAVPULGA71EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDAKDBG0AT6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-10-11T06:28:04Z",
        "mfaAuthenticated": "false"
      }
    }
  }
}
```

```
  },
  "eventTime": "2023-10-11T07:19:09Z",
  "eventSource": "one.amazonaws.com",
  "eventName": "CreateSite",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "XXX.XXX.XXX.XXX",
  "userAgent": "userAgent",
  "requestParameters": {
    "name": "****",
    "description": "****",
    "address": {
      "addressLine1": "****",
      "addressLine2": "****",
      "addressLine3": "****",
      "city": "EXAMPLE_CITY",
      "postalCode": "12345",
      "countryCode": "EXAMPLE_COUNTRY",
      "stateOrRegion": "EXAMPLE_STATE"
    }
  },
  "clientToken": "abc12d34-567e-8910-1112-12fghi0jk131"
},
"responseElements": {
  "stateOrRegion": "EXAMPLE_STATE",
  "createdAtInMillis": 1697008749263,
  "city": "EXAMPLE_CITY",
  "countryCode": "EXAMPLE_COUNTRY",
  "deviceInstanceCount": 0,
  "postalCode": "12345",
  "name": "****",
  "description": "****",
  "siteId": " abCdefG12hijkl",
  "siteArn": "arn:aws:one:us-east-1:123456789012:site/abCdefG12hijkl",
  "tags": "****"
},
"requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
"eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management"
}
```

# Memecahkan Masalah Amazon One

Jika Anda memiliki masalah dengan Aplikasi Amazon One atau salah satu perangkat Amazon One Anda, gunakan saran ini untuk memecahkan masalah. Kemudian, jika Anda masih mengalami masalah, hubungi AWS Support.

## Topik

- [Memecahkan masalah identitas dan akses Amazon One](#)
- [Memecahkan Masalah Konsol Amazon One](#)
- [Memecahkan masalah perangkat Amazon One](#)

## Memecahkan masalah identitas dan akses Amazon One

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Amazon One Enterprise dan IAM.

## Topik

- [Saya tidak berwenang untuk melakukan tindakan di Amazon One](#)
- [Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Amazon One saya](#)

## Saya tidak berwenang untuk melakukan tindakan di Amazon One

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya `my-example-widget` rekaan, tetapi tidak memiliki izin `one:GetWidget` rekaan.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
one:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya `my-example-widget` dengan menggunakan tindakan `one:GetWidget`.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

## Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Amazon One saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Amazon One Enterprise mendukung fitur-fitur ini, lihat [Bagaimana Amazon One Enterprise bekerja dengan IAM](#).
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat [Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki](#) di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat [Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat [Menyediakan akses ke pengguna terautentikasi eksternal \(federasi identitas\)](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM](#).

## Memecahkan Masalah Konsol Amazon One

Jika Anda memiliki masalah dengan Aplikasi Amazon One atau salah satu perangkat Amazon One Anda, gunakan saran ini untuk memecahkan masalah. Kemudian, jika Anda masih mengalami masalah, hubungi AWS Support.

Topik

- [Saya tidak dapat membuat situs](#)
- [Saya tidak dapat membuat instance perangkat](#)

- [Saya tidak dapat membuat templat konfigurasi](#)
- [Saya tidak dapat membuat kode QR aktivasi](#)

## Saya tidak dapat membuat situs

- Hubungi administrator Amazon One Console untuk memberi Anda akses.
- Jika masalah berlanjut, hubungi AWS Support.

## Saya tidak dapat membuat instance perangkat

- Hubungi administrator Amazon One Console untuk memberi Anda akses.
- Jika masalah berlanjut, hubungi AWS Support.

## Saya tidak dapat membuat templat konfigurasi

- Hubungi administrator Amazon One Console untuk memberi Anda akses.
- Jika masalah berlanjut, hubungi AWS Support.

## Saya tidak dapat membuat kode QR aktivasi

- Hubungi administrator Amazon One Console untuk memberi Anda akses.
- Jika masalah berlanjut, hubungi AWS Support.

## Memecahkan masalah perangkat Amazon One

Jika Anda memiliki masalah dengan Amazon One Console atau salah satu Perangkat Amazon One Anda, gunakan saran ini untuk memecahkan masalah. Kemudian, jika Anda masih mengalami masalah, hubungi AWS Support.

### Topik

- [Layar kosong](#)
- [Saya tidak dapat terhubung ke Wi-Fi atau jaringan](#)
- [Mem-boot ulang perangkat dengan peringatan aktif](#)

- [Kesalahan sistem](#)
- [Kode QR tidak dikenali](#)
- [Tidak dapat membaca kode QR](#)
- [Beberapa kode QR terdeteksi](#)
- [Instans perangkat tidak ada](#)
- [Situs tidak ditemukan](#)
- [Kode Pos tidak cocok](#)
- [Gateway habis waktu](#)
- [Saya tidak dapat mengonfigurasi perangkat](#)
- [Perangkat dimulai ulang dengan pesan kesalahan dan kode kesalahan](#)
- [Logo Amazon di layar perangkat tanpa aktivitas lebih lanjut](#)
- [Tidak tersedia untuk sementara](#)
- [Ada yang tidak beres di pihak kami](#)
- [Sementara keluar dari layanan](#)
- [Perangkat Amazon One mengalami kerusakan fisik](#)
- [Tidak dapat membaca telapak tangan](#)
- [Telapak tangan tidak dikenali](#)
- [Perangkat terkunci karena ketidakaktifan yang diperpanjang](#)
- [Perangkat terkunci karena peristiwa tamper](#)

## Layar kosong

Ini terjadi ketika perangkat tidak memiliki daya atau macet saat reboot.

Lakukan hal berikut untuk memecahkan masalah ini:

- Tunggu beberapa saat (kurang dari 30 detik) jika perangkat sedang reboot.
- Jika cincin lampu berdenyut saat perangkat kosong, tunggu hingga 30 detik.
- Periksa apakah kabel daya dicolokkan ke stopkontak serta kuat di bagian belakang perangkat Amazon One. Juga, periksa apakah kabelnya tidak rusak.
- Periksa sumber listriknya.

- Periksa apakah semua kabel terhubung dengan benar ke Amazon One dan hub USB.
- Reboot perangkat dari konsol.
- Jika me-reboot perangkat tidak memperbaiki masalah, cabut hub USB Amazon One dari catu daya, lalu colokkan kembali.
- Jika masalah berlanjut, hubungi AWS Support.

## Saya tidak dapat terhubung ke Wi-Fi atau jaringan

Ini terjadi ketika perangkat kehilangan konektivitas.

Lakukan hal berikut untuk memecahkan masalah ini:

- Jika terhubung ke Wi-Fi, gunakan perangkat lain untuk memeriksa apakah Wi-Fi muncul di jaringan yang tersedia.
- Periksa apakah router Wi-Fi dinyalakan dan dalam jangkauan.
- Perangkat akan terhubung kembali setelah jaringan pulih.
- Jika masalah berlanjut, hubungi dukungan AWS.

## Mem-boot ulang perangkat dengan peringatan aktif

Ketika Reboot diminta dari konsol, operasi menunggu hingga 15 menit hingga perangkat menerima perintah dan mencoba reboot, bahkan jika sedang offline atau menghadapi masalah jaringan.

Lakukan hal berikut untuk memecahkan masalah ini:

- Tunggu hingga reboot selesai.
- Jika masalah berlanjut, hubungi dukungan AWS.

## Kesalahan sistem

Ini terjadi karena kesalahan internal.

Lakukan hal berikut untuk memecahkan masalah ini:

- Pilih Mulai Ulang di layar untuk memulai ulang aplikasi.

- Setelah 2 kali mencoba, jika masalah tidak teratasi, hubungi AWS Support.

## Kode QR tidak dikenali

Ini terjadi karena kode QR yang tidak sah atau kode QR yang kedaluwarsa.

Lakukan hal berikut untuk memecahkan masalah ini:

- Pilih Coba lagi untuk menavigasi kembali ke layar kode QR.
- Buat kode QR baru di konsol AWS, lalu pindai kode QR yang valid.

## Tidak dapat membaca kode QR

Ini terjadi ketika aplikasi tidak dapat membaca kode QR.

Lakukan hal berikut untuk memecahkan masalah ini:

- Pilih Coba lagi untuk menavigasi kembali ke layar kode QR.
- Jika masalah berlanjut, batalkan alur kerja aktivasi dan mulai ulang.

## Beberapa kode QR terdeteksi

Ini terjadi ketika beberapa kode QR dipindai.

Lakukan hal berikut untuk memecahkan masalah ini:

- Pilih Coba lagi untuk menavigasi kembali ke layar kode QR.
- Pindai hanya satu kode QR yang valid pada satu waktu.

## Instans perangkat tidak ada

Ini terjadi ketika instance perangkat dihapus atau tidak ada di konsol AWS.

Lakukan hal berikut untuk memecahkan masalah ini:

- Pilih Coba lagi untuk menavigasi kembali ke layar kode QR.
- Periksa konsol AWS untuk mengetahui instans perangkat yang benar. Jika instance perangkat tidak ada, hubungi administrator Anda.

- Buat kode QR baru untuk instance perangkat itu, lalu pindai kode QR baru.

## Situs tidak ditemukan

Ini terjadi ketika situs dihapus atau tidak ada di konsol AWS.

Lakukan hal berikut untuk memecahkan masalah ini:

- Periksa konsol AWS untuk informasi situs. Jika situs tidak ada, hubungi administrator Anda.

## Kode Pos tidak cocok

Ini terjadi saat memasukkan Kode Pos yang berbeda dari yang dikonfigurasi untuk perangkat.

Lakukan hal berikut untuk memecahkan masalah ini:

- Pilih Coba lagi untuk menavigasi kembali ke layar Kode ZIP.
- Periksa apakah Anda memiliki Kode Pos situs yang benar.
- Jika masalah berlanjut, hubungi administrator Anda untuk memeriksa Kode Pos situs di konsol AWS.

## Gateway habis waktu

Hal ini terjadi ketika tidak ada respon dari gateway dalam waktu yang ditentukan.

Lakukan hal berikut untuk memecahkan masalah ini:

- Pilih Restart untuk me-restart aplikasi.
- Setelah dua kali mencoba, jika masalah tidak teratasi, hubungi AWS Support.

## Saya tidak dapat mengonfigurasi perangkat

Ini terjadi ketika operasi gagal menyimpan konfigurasi pada disk perangkat.

Lakukan hal berikut untuk memecahkan masalah ini:

- Pilih Restart untuk me-restart aplikasi.
- Setelah dua kali mencoba, jika masalah tidak teratasi, hubungi AWS Support.

## Perangkat dimulai ulang dengan pesan kesalahan dan kode kesalahan

Lakukan hal berikut untuk memecahkan masalah ini:

- Pilih Restart, dan biarkan perangkat pulih.
- Jika perangkat tidak pulih, cabut hub USB dari catu daya dan sambungkan kembali.
- Jika masalah berlanjut, hubungi AWS Support.

## Logo Amazon di layar perangkat tanpa aktivitas lebih lanjut

Lakukan hal berikut untuk memecahkan masalah ini:

- Tunggu beberapa saat (kurang dari 30 detik) jika perangkat sedang reboot.
- Cabut hub USB dari catu daya dan sambungkan kembali.
- Jika masalah berlanjut, hubungi AWS Support.

## Tidak tersedia untuk sementara

Lakukan hal berikut untuk memecahkan masalah ini:

- Pastikan koneksi USB dengan host device/system aman.
- Putuskan sambungan dan sambungkan kembali semua kabel yang masuk ke hub USB.
- Jika masalah berlanjut, hubungi AWS Support.

## Ada yang tidak beres di pihak kami

Ini terjadi ketika ada kesalahan internal.

Lakukan hal berikut untuk memecahkan masalah ini:

1. Matikan perangkat.
2. Putuskan sambungan dari catu dayanya.
3. Tunggu 30 detik.
4. Colokkan perangkat kembali ke sumber listriknya.
5. Nyalakan perangkat.

6. Jika masalah berlanjut, hubungi AWS Support.

## Sementara keluar dari layanan

Ini terjadi ketika perangkat telah dipindahkan dari layanan oleh Amazon One.

Lakukan hal berikut untuk memecahkan masalah ini:

- Hubungi AWS Support.

## Perangkat Amazon One mengalami kerusakan fisik

Lakukan hal berikut untuk memecahkan masalah ini:

- Hubungi AWS Support untuk langkah selanjutnya, dan berikan detail sebanyak mungkin, seperti apa yang terjadi, kapan itu terjadi, dan mengapa hal itu terjadi.

## Tidak dapat membaca telapak tangan

Lakukan hal berikut untuk memecahkan masalah ini:

- Periksa kembali apakah perangkat Amazon One bebas dari goresan dan noda.
- Pastikan telapak tangan pelanggan bebas dari oklusi seperti perban, lengan baju, dan kotoran/minyak yang signifikan.
- Jika masalah berlanjut, dan perangkat tidak membaca telapak tangan apa pun, hubungi AWS Support.

## Telapak tangan tidak dikenali

Lakukan hal berikut untuk memecahkan masalah ini:

- Minta pelanggan mencoba menggunakan telapak tangan mereka yang lain.
- Pastikan pelanggan sudah terdaftar. Jika tidak, minta mereka mendaftar secara online atau di perangkat.
- Jika masalah berlanjut, dan perangkat tidak membaca kontak telapak tangan apa pun, hubungi AWS Support.

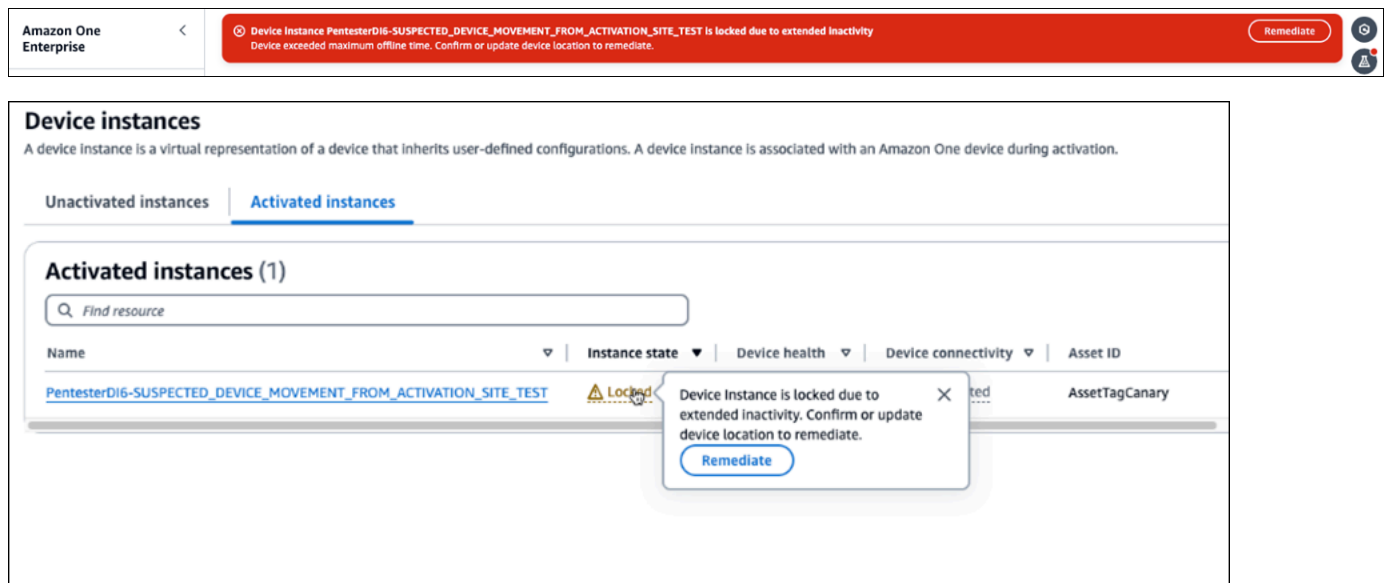
## Perangkat terkunci karena ketidakaktifan yang diperpanjang

Ketika perangkat mencurigai telah dipindahkan dari situs aktivasi, itu mengunci pengguna. Ini terjadi ketika perangkat melebihi maksimum 120 jam waktu offline.

Lakukan hal berikut untuk membuka kunci perangkat:

1. Masuk ke konsol AWS Anda, dan pilih instance perangkat.
2. Dari spanduk kesalahan di bagian atas halaman, pilih Remediate.

Opsional: Dari Instance yang diaktifkan, pilih Terkunci, dan pilih Remediate.



3. Jika perangkat masih di situs aktivasi asli, pilih Ya, perangkat ada di situs ini.
4. Jika perangkat berada di situs yang berbeda, pilih Tidak, perangkat berada di situs yang berbeda. Memilih Tidak menonaktifkan perangkat. Aktifkan perangkat di situs baru.

## Perangkat terkunci karena peristiwa tamper

Untuk alasan keamanan, perangkat Amazon One akan dikunci jika terjadi peristiwa tamper.

Lakukan hal berikut untuk memecahkan masalah ini:

- Hubungi AWS Support.

# Riwayat dokumen untuk Panduan Pengguna Amazon One Enterprise

Tabel berikut menjelaskan rilis dokumentasi untuk Amazon One Enterprise.

Perubahan	Deskripsi	Tanggal
<a href="#">Perbarui</a>	Menambahkan bagian Peran Tertaut Layanan	Februari 4, 2025
<a href="#">Perbarui</a>	Ditambahkan: konten Skenario-driven	Oktober 10, 2024
<a href="#">Perbarui</a>	Topik yang ditambahkan: Memecahkan masalah konsol Amazon One Enterprise	Oktober 10, 2024
<a href="#">Perbarui</a>	Topik yang ditambahkan: Pemecahan masalah perangkat Amazon One Enterprise	Oktober 10, 2024
<a href="#">Perbarui</a>	Bab yang ditambahkan: Menyiapkan Amazon One Enterprise	Oktober 10, 2024
<a href="#">Perbarui</a>	Topik tambahan: Memelihara dan membersihkan perangkat Amazon One Enterprise	Oktober 10, 2024
<a href="#">Perbarui</a>	Konten yang direorganisasi	Oktober 10, 2024
<a href="#">Perbarui</a>	Topik tambahan: Menginstal I/O Hub perangkat Amazon One Enterprise untuk akses aman	Agustus 14, 2024
<a href="#">Perbarui</a>	Topik tambahan: Memasang perangkat Amazon One	Juni 5, 2024

Enterprise yang dapat  
dipasang di dinding

[Rilis awal](#)

Rilis awal Panduan Pengguna 27 November 2023  
Amazon One Enterprise

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