aws

Panduan Pengguna

Amazon Satu

Amazon Satu: Panduan Pengguna

Table of Contents

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

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

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. Konfigurasikan 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

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

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 dalam suatu 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 — AWS Management Console 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 AWS Management Console, 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.comdi/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.comdi/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.comdi/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 lencana, berikan pengaturan konfigurasi yang menentukan tata letak format lencana 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.

Konfigurasikan instance perangkat untuk aktivasi

Setelah instance perangkat dibuat, Anda mengonfigurasi instance perangkat dengan templat konfigurasi yang dibuat sebelumnya (lihatBuat templat konfigurasi), atau Anda dapat menambahkan konfigurasi secara manual.

Untuk mengonfigurasi instance perangkat untuk aktivasi

1. Buka konsol Amazon One https://console.aws.amazon.comdi/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 Konfigurasikan
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, lihatBuat 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 Konfigurasikan

    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 lencana, berikan pengaturan konfigurasi yang menentukan tata letak format lencana 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 Konfigurasikan

6. Di bawah tabel Instance Tidak Aktif, status Instance akan ditampilkan.

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 AWS Management Console untuk mendapatkan kode QR aktivasi perangkat.

Topik

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.

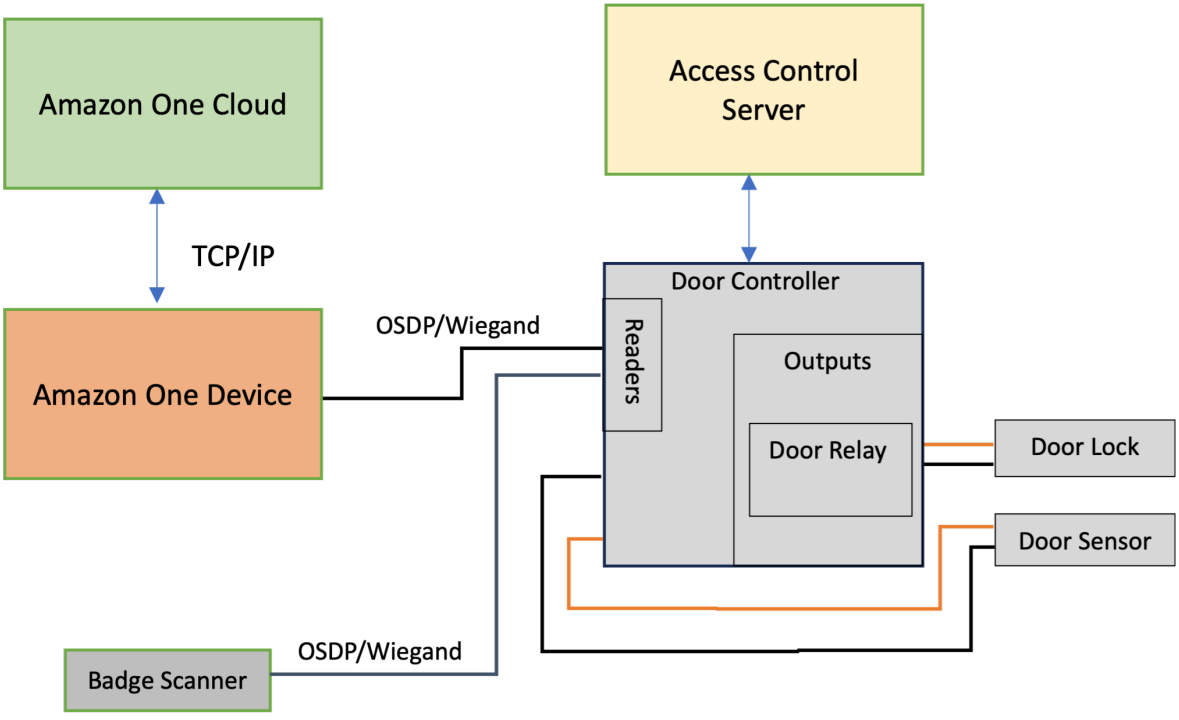
Kebutuhan daya

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

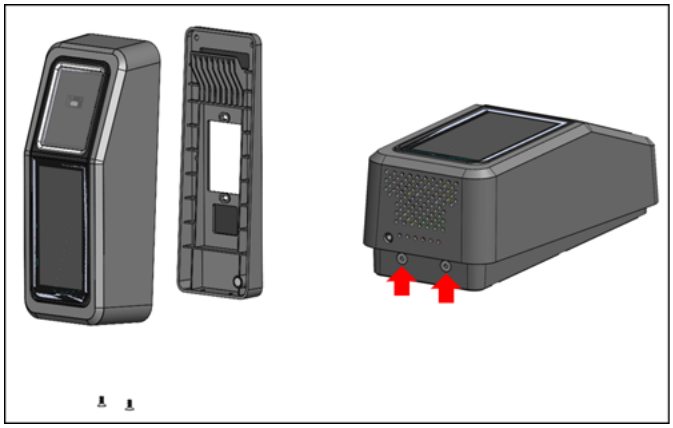
Termasuk dengan perangkat Amazon One yang dapat dipasang di dinding

- 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 kemasannya.
2. Pisahkan pelat pemasangan dari perangkat Amazon One Anda dengan melepas dua sekrup keamanan Torx bawah.

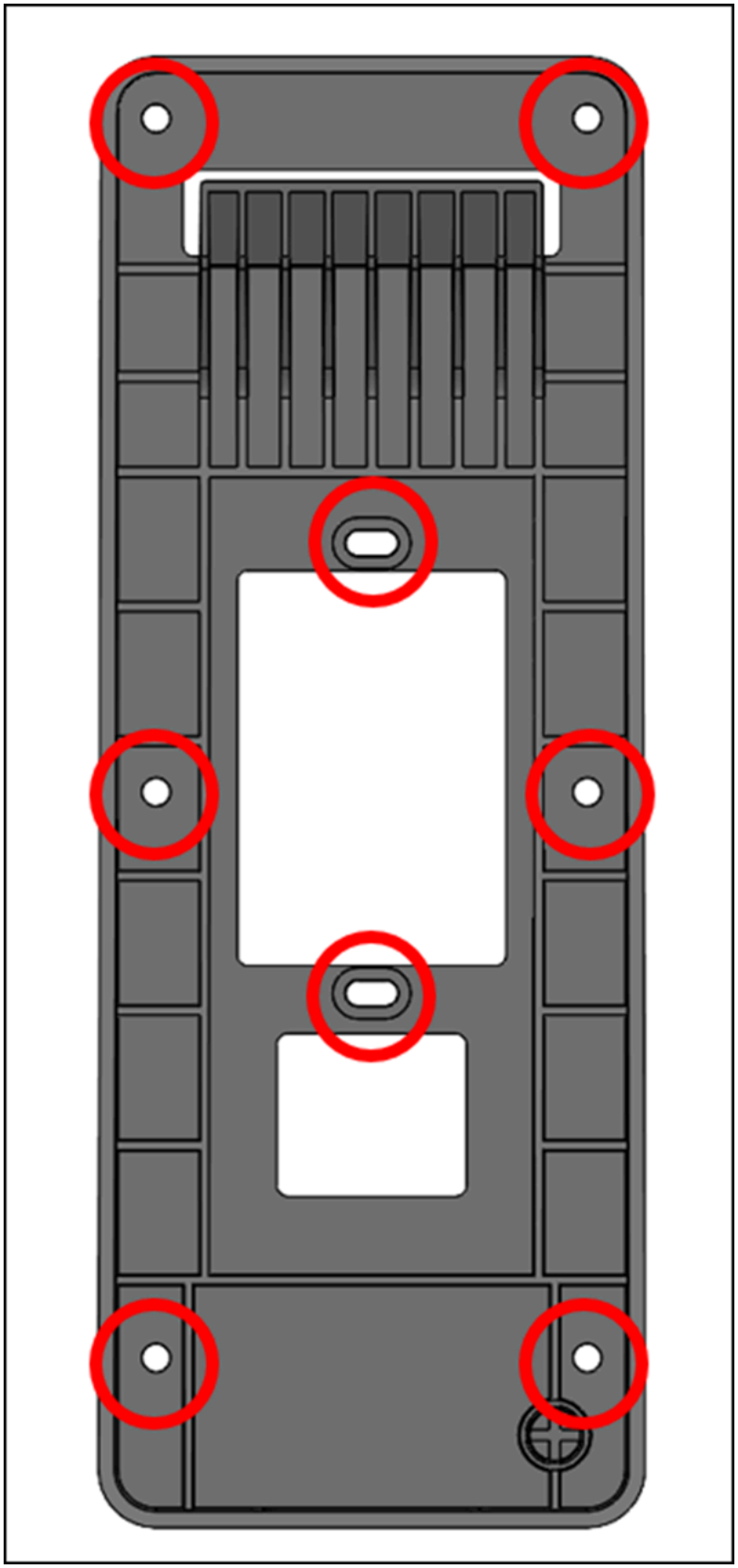


3. Posisikan pelat pemasangan di dinding di lokasi yang diinginkan. Gunakan braket sebagai templat untuk menandai enam lubang sekrup luar seperti yang ditunjukkan pada gambar berikut.

   (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 menahan pelat pemasangan ke dinding.

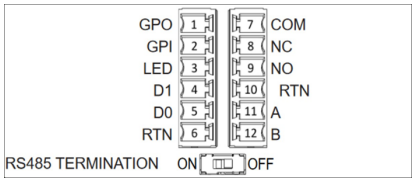
Untuk menghubungkan perangkat Amazon One yang dapat dipasang di dinding

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	

Pin	Koneksi	Deskripsi	Gunakan
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
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/ Jam	OSDP D1 - Kawat putih

Pin	Koneksi	Deskripsi	Gunakan	
12	B	RS485_B/D0/ Data	OSDP D0 - Kawat hijau	

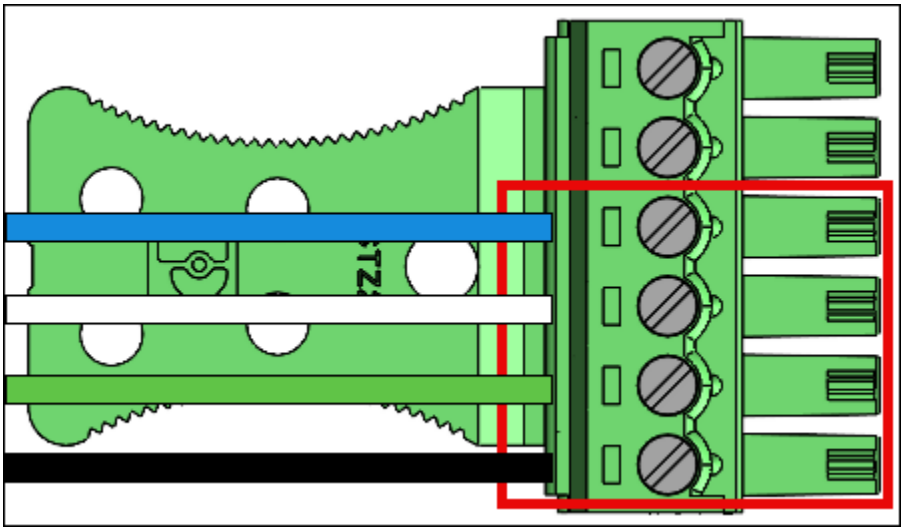
2. Saat memasang kawat, lepaskan 3mm-5mm dari ujung kawat.
3. Masukkan ujung kabel yang dilucuti ke posisi terminal yang diinginkan.
4. Dengan menggunakan obeng pipih, putar sekrup retensi terminal searah jarum jam untuk menjepit kabel sampai pas. Jangan terlalu kencangkan.
5. Setelah diikat, tarik kabel 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. Tangan kencangkan sekrup. Jangan terlalu kencangkan.

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

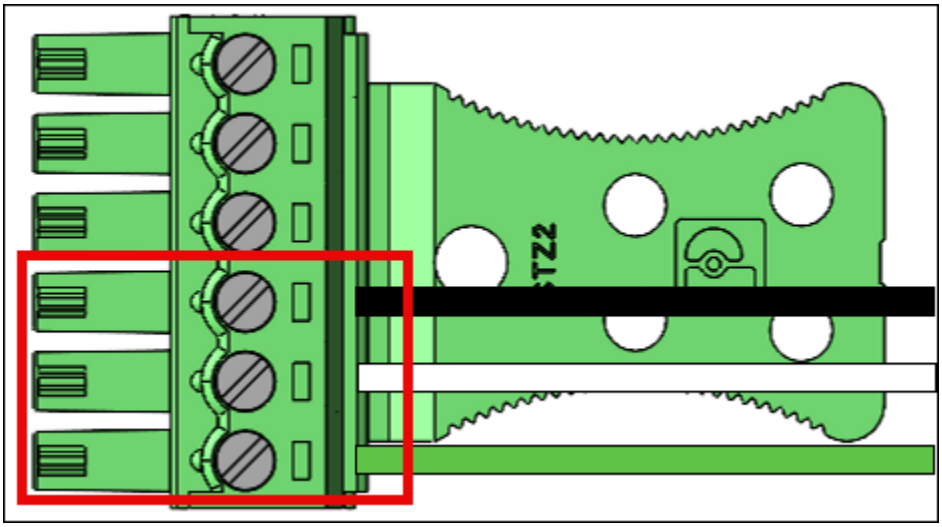
Pin	Koneksi	Deskripsi	Gunakan
3	DIPIMPIN	LED Wiegand	Masukan LED Wiegand - Opsional (5V TTL)
4	D1	Wiegand D1	Keluaran Wiegand D1 (5V TTL)
5	D0	Wiegand D0	Keluaran Wiegand D0 (5V TTL)
6	RTN	Sinyal kembali	Referensi Wiegand GND

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).

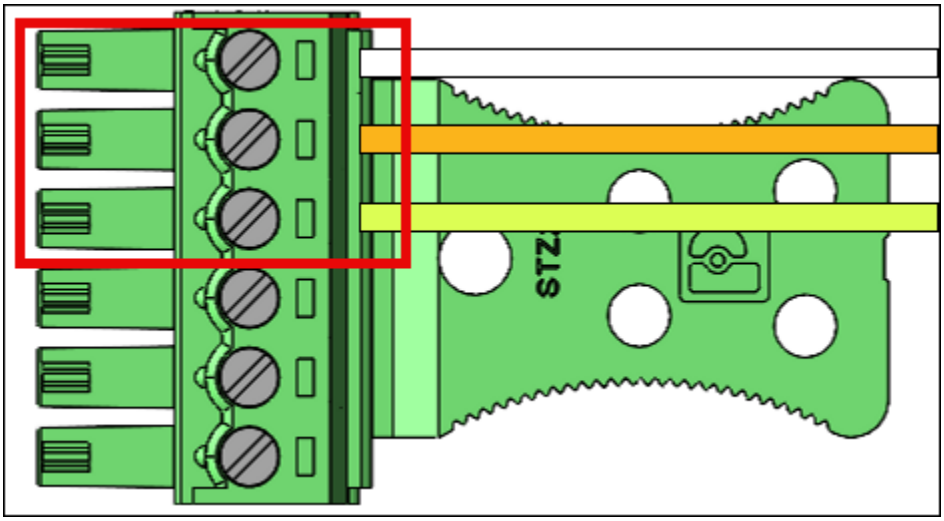


RS485 kabel

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

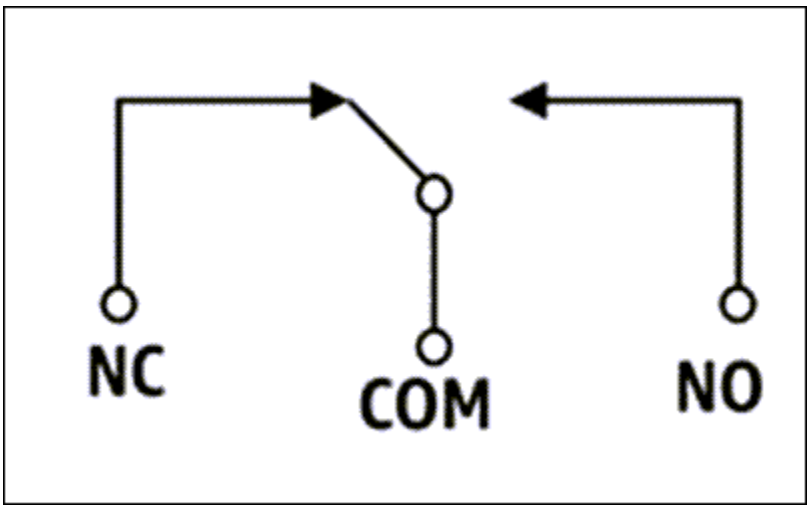
Koneksi relai

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



Kabel relai

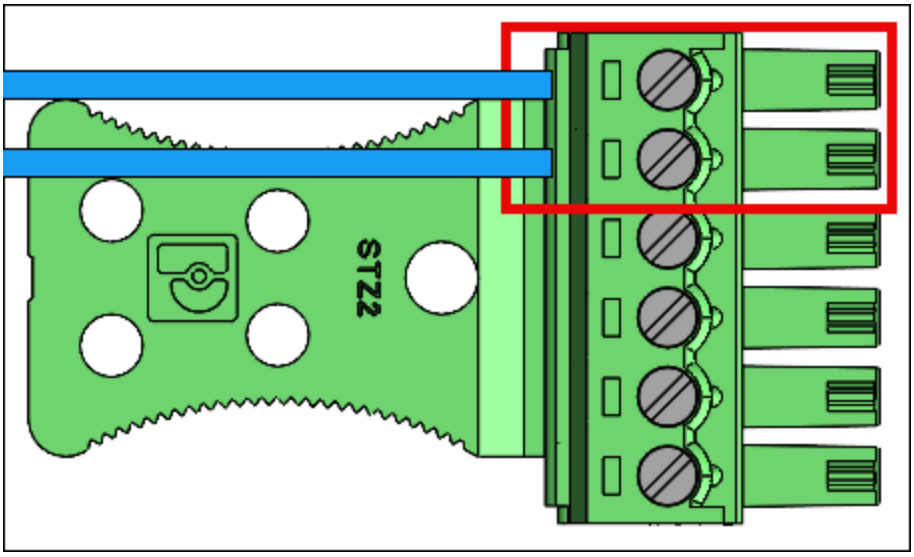
Pin	Koneksi	Deskripsi	Gunakan	
7	COM	Relay umum	Relai kontak Umum - Kabel putih	
8	NC	Relay biasanya ditutup	Relai kontak biasanya tertutup - Kawat oranye	
9	TIDAK	Relay biasanya terbuka	Relai kontak biasanya terbuka - Kabel kuning	



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

Koneksi input/output digital

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



Kabel input/output 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)	

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

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

Menginstal perangkat Amazon One 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 I/O Hub

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

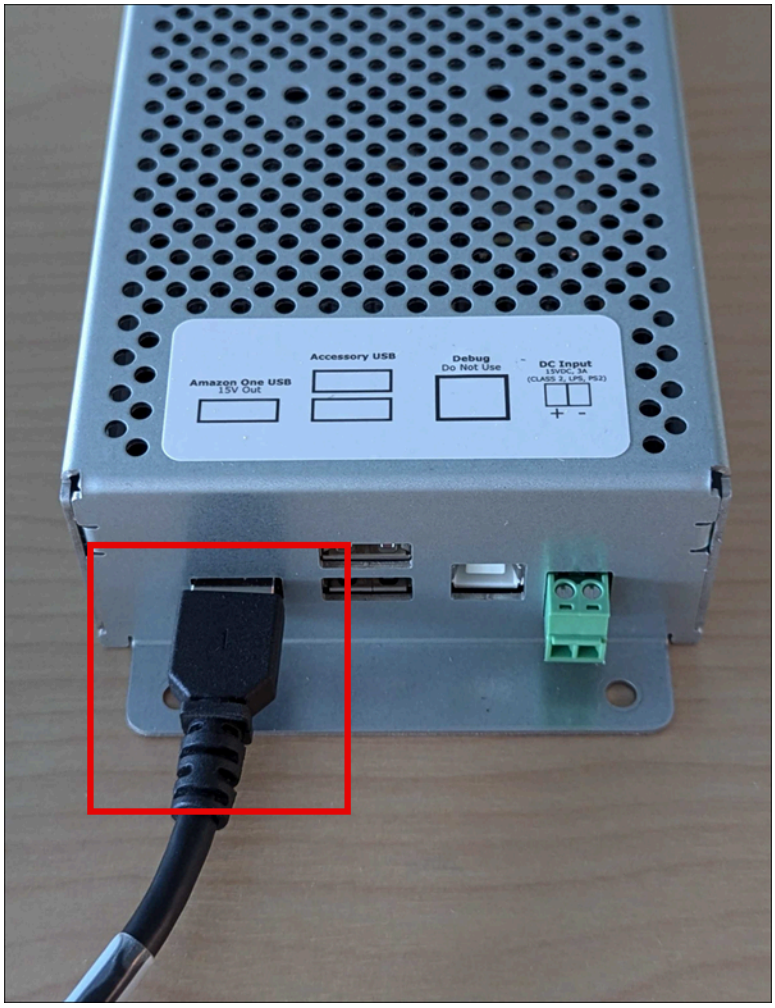
Termasuk dengan perangkat Amazon One dengan I/O Hub

- Konektor blok terminal 2x 6 posisi
- Konektor steker DC
- 72 “kabel daya/data

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

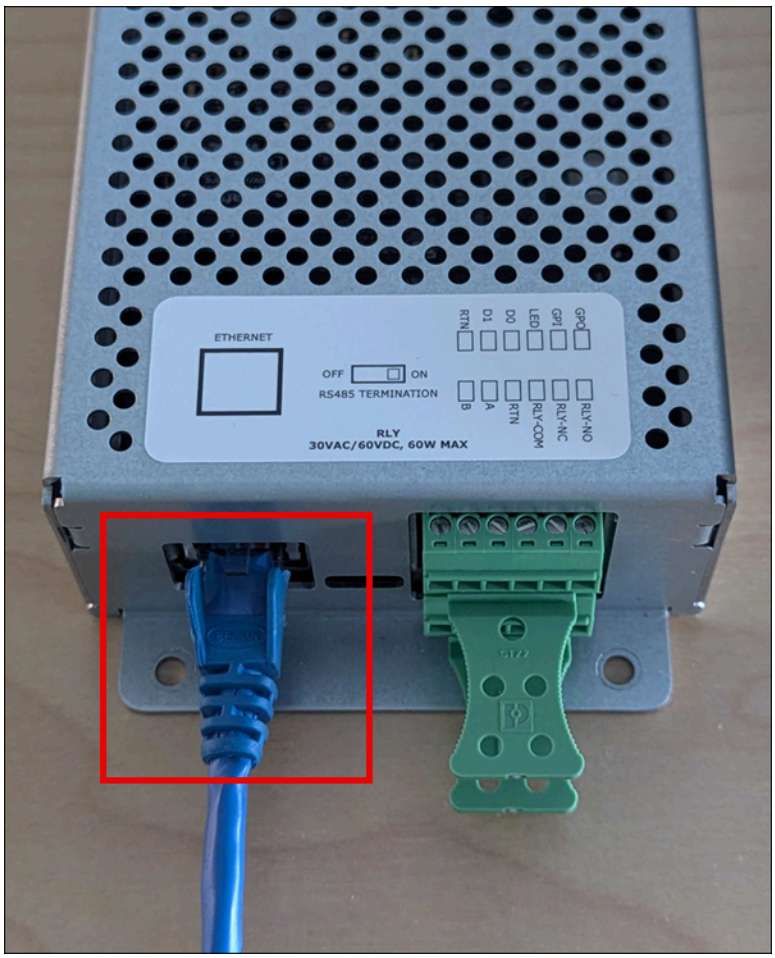
Untuk menginstal hub I/O untuk perangkat Amazon One Anda

1. Hapus perangkat Amazon One Anda dengan I/O Hub dari kemasannya.
2. Amankan hub I/O di lokasi yang diinginkan.
3. Colokkan kabel USB Amazon One ke port hub I/O.



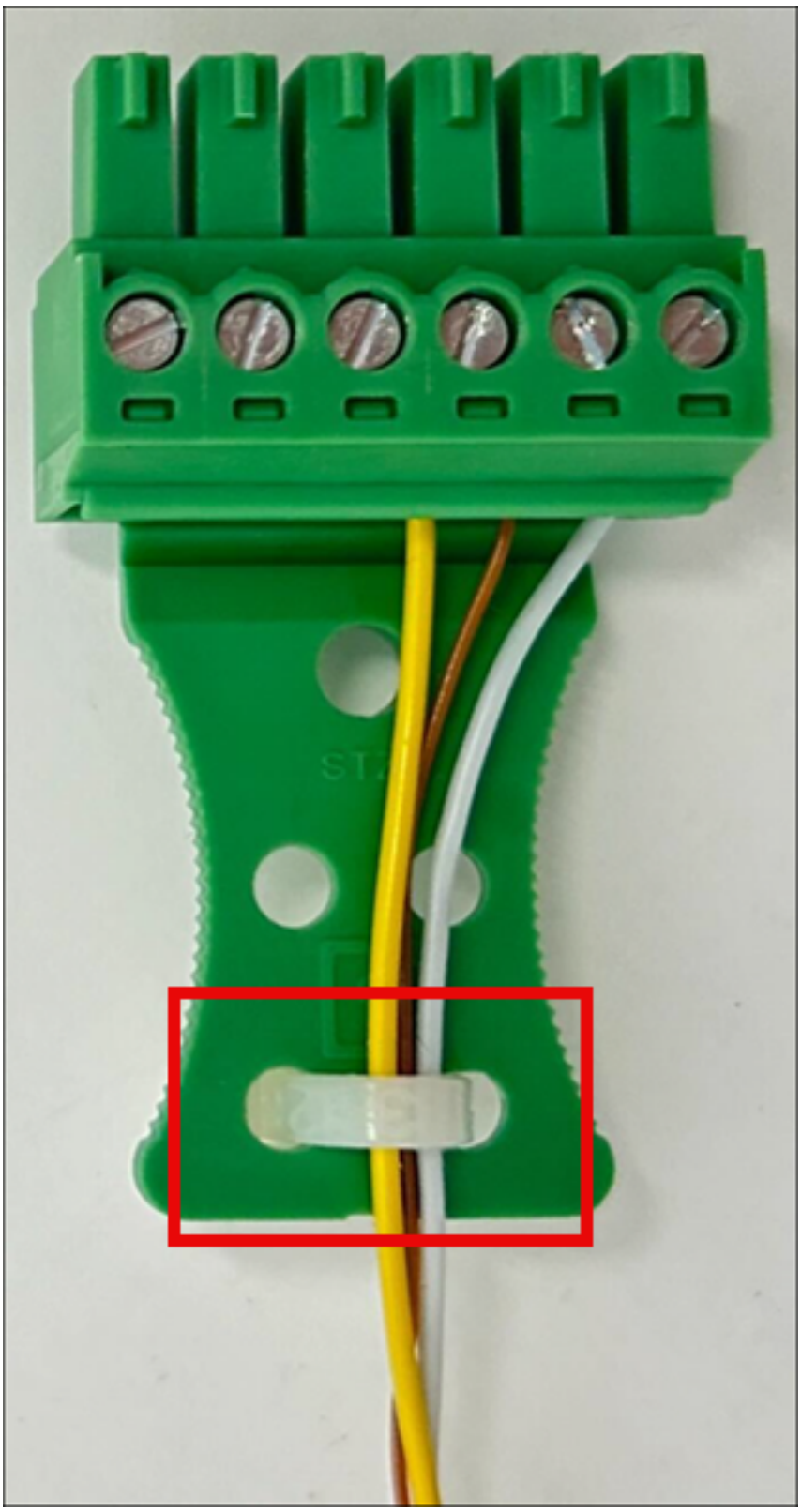
4. Untuk daya POE++, colokkan kabel Ethernet dari sumber POE++ ke port hub I/O.

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



Untuk menghubungkan hub I/O untuk perangkat Amazon One Anda

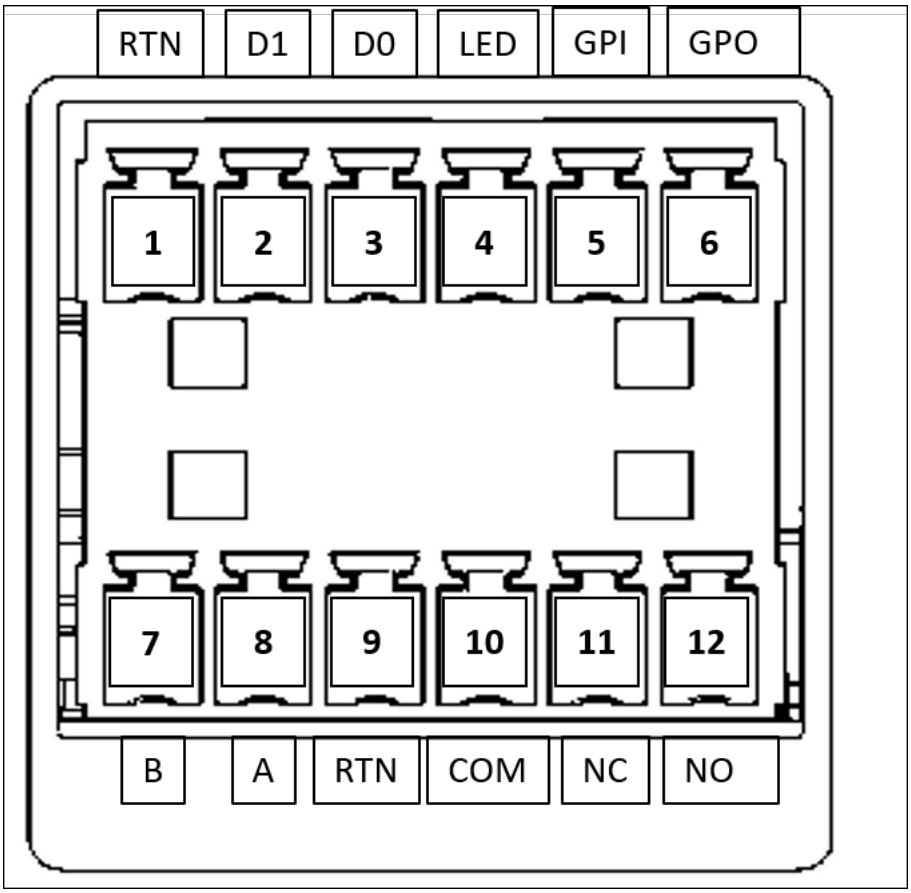
- Pasang loop tetes untuk menghindari cairan yang tidak sengaja mengalir ke kabel dan masuk ke hub I/O.
- Pasang penjepit pelepas regangan untuk melindungi kabel dari kerusakan atau stres, seperti yang ditunjukkan pada gambar berikut.



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

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

Koneksi

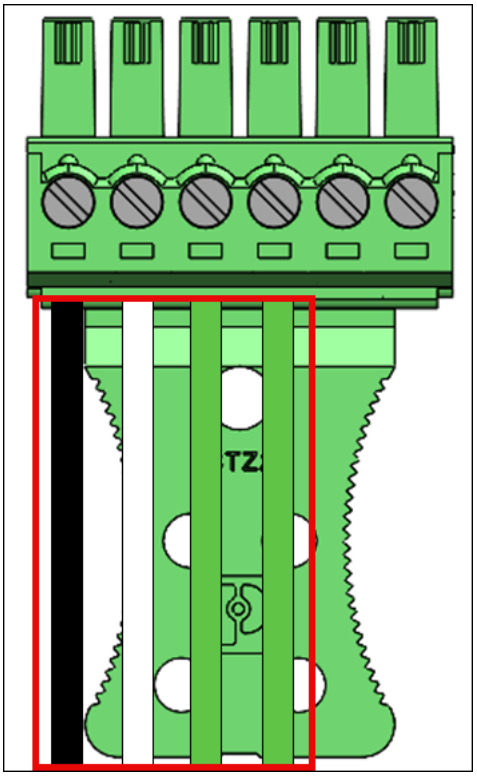


Pin	Koneksi	Deskripsi	Gunakan
1	RTN	Sinyal kembali	Tanah Wiegand - Kawat hitam
2	D1	Wiegand D1	Wiegand Data 1 - Kabel putih
3	D0	Wiegand D0	Data Wiegand 0 — Kabel hijau
4	DIPIMPIN	LED Wiegand	Wiegand LED - Opsional

Pin	Koneksi	Deskripsi	Gunakan	
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/ Jam	OSDP D1 - Kawat putih	
9	RTN	Sinyal kembali	Pengembalian OSDP - Kabel hitam	
10	COM	Relay Umum	Relai kontak umum - Kabel putih	
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).

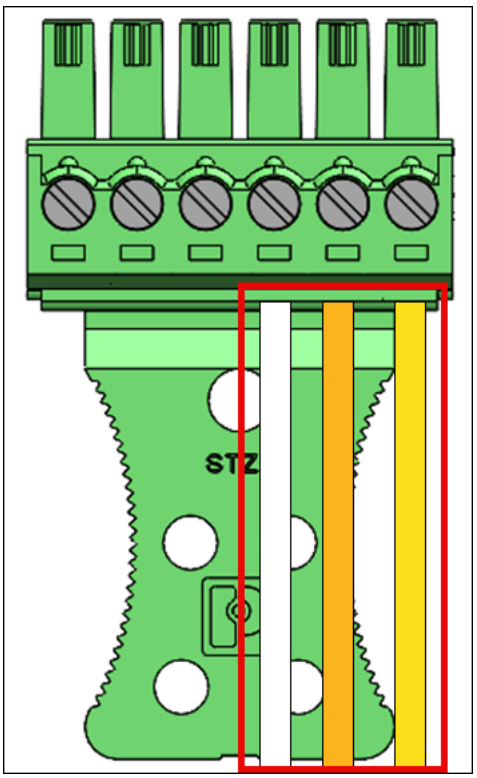
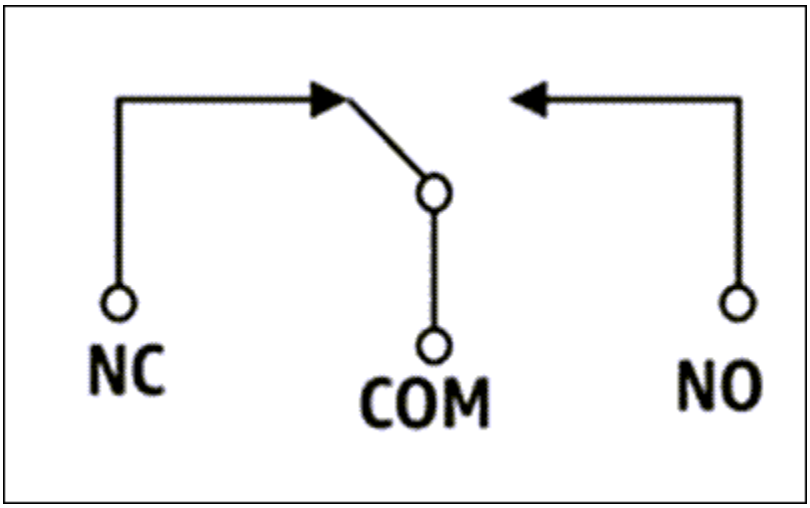


Diagram relai

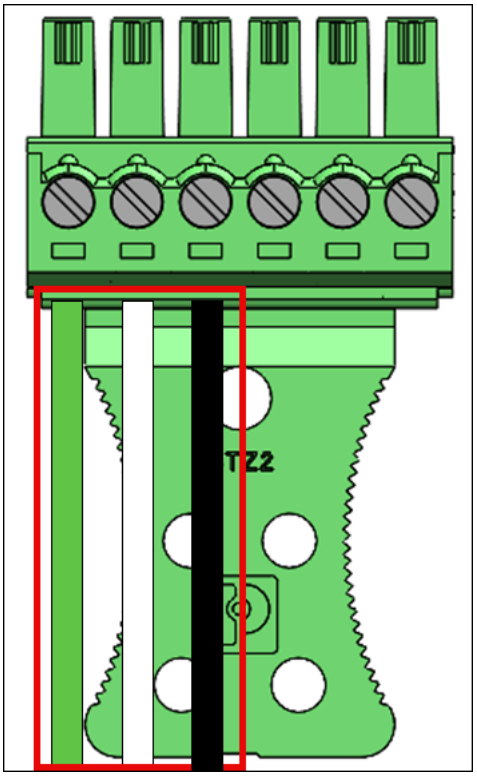


Relai harus dioperasikan sesuai dengan peringkat keselamatan yang ditentukan 30VAC/60VDC, 60W Max.

RS485 koneksi

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

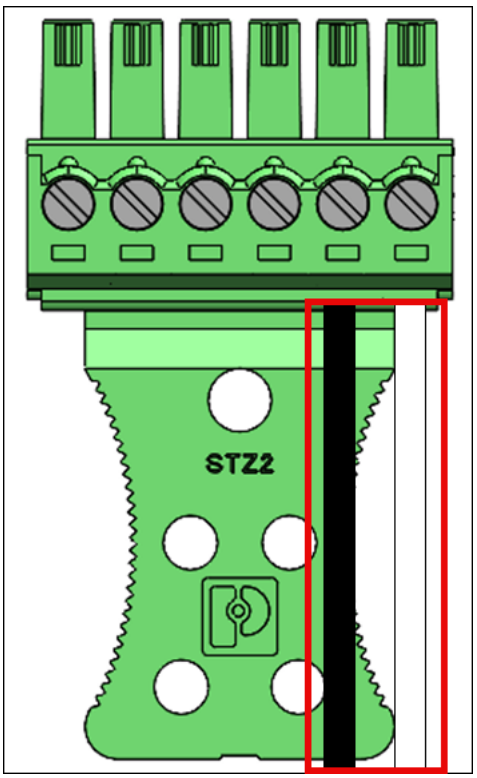
- Masukkan kabel hitam di Pin 9 (RTN).



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

Koneksi input/output digital

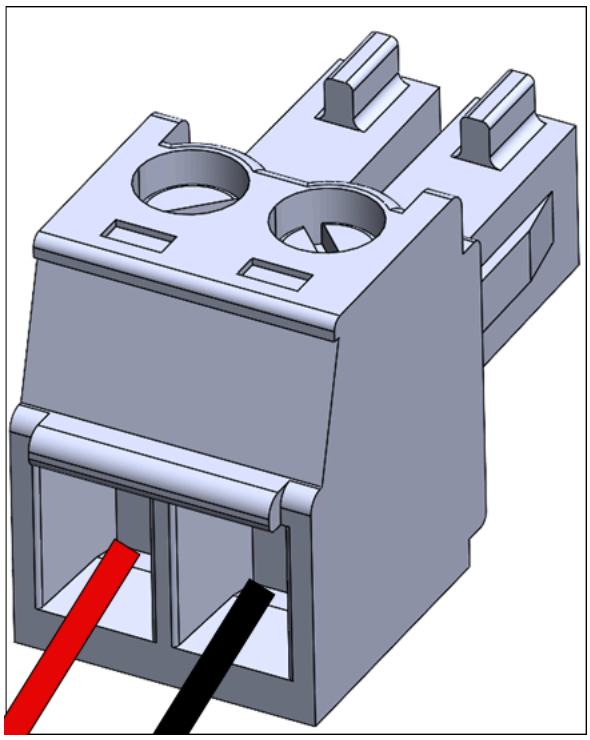
- Masukkan kabel hitam di Pin 5 (GPI).
- Masukkan kabel putih di Pin 6 (GPO).



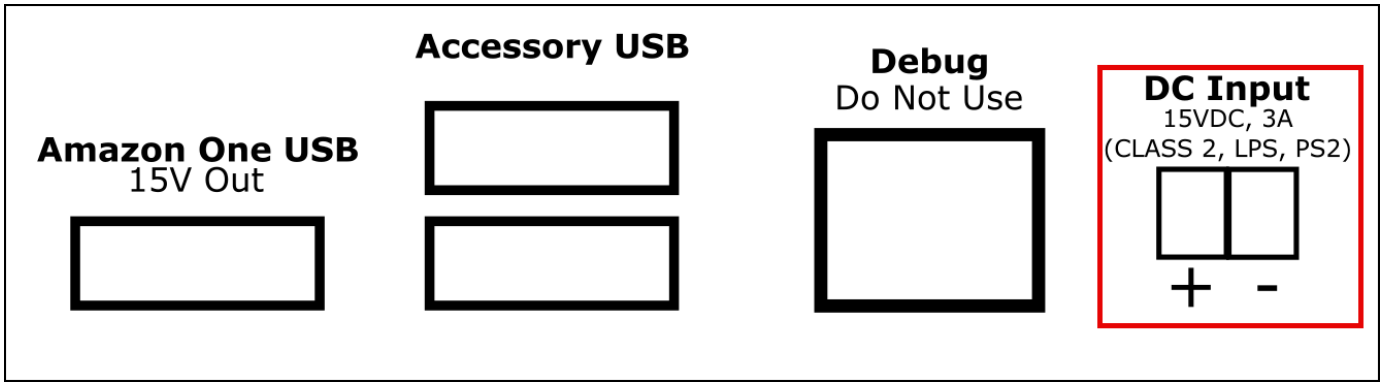
- Koneksi input/output digital harus dioperasikan seperti yang tercantum.

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 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.

   > **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, konfirmasikan 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

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

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 pengenal 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

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 periferal 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 celah/bukaan yang memperlihatkan komponen/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 hariand/or when the window is visually dirty (e.g., finger/hand prints/smudges). 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.

Manajemen Situs

Situs mewakili lokasi fisik tempat 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 instance perangkat

Prosedur berikut merinci cara melihat status instance perangkat Anda.

Untuk melihat status 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, 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 instance 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 (lihatKonfigurasikan instance perangkat untuk aktivasi). Kemudian, Anda dapat melalui proses aktivasi perangkat (lihatMengaktifkan 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 kredensil 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 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

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 kredensyal 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 sumber daya. AWS 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 diberi wewenang (memiliki izin) untuk menggunakan sumber daya Amazon One Enterprise. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Amazon One Enterprise.

Pengguna layanan - Jika Anda menggunakan layanan Amazon One Enterprise untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Amazon One Enterprise untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Amazon One Enterprise, lihatMemecahkan masalah identitas dan akses Amazon One.

Administrator layanan - Jika Anda bertanggung jawab atas sumber daya Amazon One Enterprise di perusahaan Anda, Anda mungkin memiliki akses penuh ke Amazon One Enterprise. Tugas Anda adalah menentukan fitur dan sumber daya Amazon One Enterprise mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Amazon One Enterprise, lihatBagaimana Amazon One Enterprise bekerja dengan IAM.

Administrator IAM - Jika Anda administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Amazon One Enterprise. Untuk melihat contoh kebijakan berbasis identitas Amazon One Enterprise yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas untuk Amazon One Enterprise

Mengautentikasi dengan identitas

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

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensil yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Guna mengetahui informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Autentikasi multi-faktor AWS di IAM dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensil yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apakah itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat meminta kelompok untuk menyebutkan IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk pengguna IAM dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Untuk mengambil peran IAM sementara AWS Management Console, Anda dapat beralih dari pengguna ke peran IAM (konsol). Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Metode untuk mengambil peran dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Buat peran untuk penyedia identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.
  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh 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.

  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. 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.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS permintaan API. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

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.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

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.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat Pilih antara kebijakan yang dikelola 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. 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 prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

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.

Daftar kontrol akses (ACLs)

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.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung. ACLs Untuk mempelajari selengkapnya ACLs, lihat Ringkasan daftar kontrol akses (ACL) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCPs) — SCPs adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam suatu organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organizations dan SCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.
- Kebijakan kontrol sumber daya (RCPs) — RCPs adalah kebijakan JSON yang dapat Anda gunakan untuk menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda tanpa memperbarui kebijakan IAM yang dilampirkan ke setiap sumber daya yang Anda miliki. RCP membatasi izin untuk sumber daya di akun anggota dan dapat memengaruhi izin efektif untuk identitas, termasuk Pengguna root akun AWS, terlepas dari apakah itu milik organisasi Anda. Untuk informasi selengkapnya tentang Organizations dan RCPs, termasuk daftar dukungan Layanan AWS tersebut RCPs, lihat Kebijakan kontrol sumber daya (RCPs) di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. 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
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Ya
ACLs	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Izin principal	Ya
Peran layanan	Tidak
Peran terkait layanan	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. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. 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 prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal 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 prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan

kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke principal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. 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. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar tindakan Amazon One Enterprise, lihatTindakan, 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. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, 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, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. 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.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi `AND` logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tanda yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat Elemen kebijakan IAM: variabel dan tanda dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. 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, lihatTindakan, 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. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tanda milik prinsipal cocok dengan tanda yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi saat manajemen kebijakan menjadi rumit.

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 kredensyal sementara dengan Amazon One Enterprise

Mendukung kredensial sementara: Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensyal sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensi sementara, lihat Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensil sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Beralih dari pengguna ke peran IAM (konsol) dalam Panduan Pengguna IAM.

Anda dapat membuat kredensyal sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensyal sementara tersebut untuk mengakses.

AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Izin utama lintas layanan untuk Amazon One Enterprise

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.

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. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM 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

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 AWS 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 Anda 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:ListGroupsForUser",
                "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.

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

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.

```
{
    "Version": "2012-10-17",
```

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

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

Tindakan API	Sumber daya
	arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
GetDeviceInstance	Instans Perangkat arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
UpdateDeviceInstance	Instans Perangkat arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
DeleteDeviceInstance	Instans Perangkat arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
CreateDeviceActivationQrCode	Instans Perangkat arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
DeleteAssociatedDevice	Instans Perangkat arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
RebootDevice	Instans Perangkat arn:aws:one ::device-instance/ *region:accountID deviceInstanceId*
CreateDeviceInstanceConfiguration	Konfigurasi Instans Perangkat arn:aws:one ::device-instance/ /configuration/ *region:accountID deviceInstanceId version*

Tindakan API	Sumber daya
GetDeviceInstanceConfiguration	Konfigurasi Instans Perangkat arn:aws:one ::device-instance/ /configuration/ *region:accountID deviceInstanceId version*
CreateSite	Situs arn:aws:one ::site/ *region:accountID siteId*
DeleteSite	Situs arn:aws:one ::site/ *region:accountID siteId*
GetSiteAddress	Situs arn:aws:one ::site/ *region:accountID siteId*
UpdateSite	Situs arn:aws:one ::site/ *region:accountID siteId*
UpdateSiteAddress	Situs arn:aws:one ::site/ *region:accountID siteId*
CreateDeviceConfigurationTemplate	Template Konfigurasi Perangkat arn:aws:one::/*region:accountID* device-configuration-template*templateId*
DeleteDeviceConfigurationTemplate	Template Konfigurasi Perangkat arn:aws:one::/*region:accountID* device-configuration-template*templateId*
GetDeviceConfigurationTemplate	Template Konfigurasi Perangkat arn:aws:one::/*region:accountID* device-configuration-template*templateId*

Tindakan API	Sumber daya
UpdateDeviceConfigurationTemplate	Template Konfigurasi Perangkat arn:aws:one::/*region:accountID* device-configuration-template*templateId*

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.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "VisualEditor0",
                "Effect": "Allow",
                "Action": [
                    "one:GetSite",
                    "one:GetSiteAddress"
                ],
                "Resource": [
                    "arn:aws:one:region:accountID:site/siteId"
                ]
            }
        ]
    }
```

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "one:DeleteSite",
```

```
                "one:UpdateSiteAddress"
              ],
            "Resource": "arn:aws:one:region:accountID:site/siteId"
          }
    ]
}
```

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.

```
{
 "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.

```
{
 "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.

```
{
 "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.

Perubahan	Deskripsi	Tanggal
Amazon One Enterprise ditambahkan AmazonOne MetricPublishAccess	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		aws:RequestTag/${TagKey} aws:TagKeys	
GetDeviceInstance	Berikan izin untuk mendapatkan informasi tentang instance perangkat	Baca	perangkat-instance*		
ListDeviceInstances	Berikan izin untuk mencantumkan instance perangkat	Baca			
UpdateDeviceInstance	Berikan izin untuk memperbarui 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		aws:RequestTag/${TagKey} aws:TagKeys	
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	Berikan izin untuk memperbarui situs	Tulis	situs*		
UpdateSiteAddress	Berikan izin untuk memperbarui alamat situs	Tulis	situs*		
CreateDeviceConfigurationTemplate	Berikan izin untuk membuat instance perangkat	Tulis		aws:RequestTag/${TagKey} aws:TagKeys	
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 memperbarui 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	aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Memberikan izin untuk menghapus tag sumber daya	Penandaan	perangkat-contoh, situs, device-configuration-template	aws:TagKeys	
ListTagForResources	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: region:accountID :device-instance/ deviceInstanceId`	aws:ResourceTag/${TagKey}
Device Instance Configuration	`arn:aws:one: region:accountID :device-instance/ deviceInstanceId /configuration/ version`	
Site	`arn:aws:one: region:accountID :site/siteId`	aws:ResourceTag/${TagKey}
Device Configuration Template	`arn:aws:one: region:accountID :device-configuration-template/ templateId`	aws:ResourceTag/${TagKey}

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	Jenis
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. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Kepatuhan dan Tata Kelola Keamanan – Panduan implementasi solusi ini membahas pertimbangan arsitektur serta memberikan langkah-langkah untuk menerapkan fitur keamanan dan kepatuhan.
- Referensi Layanan yang Memenuhi Syarat HIPAA — Daftar layanan yang memenuhi syarat HIPAA. Tidak semua memenuhi Layanan AWS syarat HIPAA.
- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas yang mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan

kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.

- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

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 CloudTrailmenangkap 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, 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 EventBridgemerutekan 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 mengkonsumsi 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"]
}
```

    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:

Status Kesehatan Perangkat Berubah Menjadi Sehat

Perangkat lulus semua pemeriksaan kesehatan.

Status Kesehatan Perangkat Berubah Menjadi Kritis

Perangkat gagal satu atau lebih pemeriksaan kesehatan.

Konektivitas Perangkat Berubah Menjadi Offline

Perangkat tidak terhubung ke internet.

Konektivitas Perangkat Berubah Menjadi Online

Perangkat terhubung ke internet.

sumber daya

Berisi daftar DeviceInstance arn tempat peristiwa Perubahan Status Perangkat dipublikasikan.

Metadata

SiteName

- Nama situs tempat DeviceInstance hadir.

SitEarn

- Arn untuk situs tempat DeviceInstance hadir.

data

Konektivitas Saat Ini

- Merupakan apakah DeviceInstance terhubung atau terputus dari internet.

- Nilai yang mungkin: TERHUBUNG, TERPUTUS

sebelumnyaKonektivitas

- Merupakan apakah DeviceInstance terhubung atau terputus dari internet sebelum acara.
- Nilai yang mungkin: TERHUBUNG, TERPUTUS

currentHealthStatus

- Merupakan apakah DeviceInstance telah lulus semua pemeriksaan kesehatan.
- Nilai yang mungkin: SEHAT, KRITIS

previousHealthStatus

- Merupakan apakah DeviceInstance lulus semua pemeriksaan kesehatan saat terakhir diperiksa.
- Nilai yang mungkin: SEHAT, KRITIS

assetTagId

- Perangkat assetTagId yang terkait dengan DeviceInstance.

deviceInstanceName

- Nama DeviceInstance tempat Peristiwa Status Perangkat diterbitkan.

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 deviceInstanceId perangkat yang memulai permintaan.

dibuatTimeStamp

- 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 kesehatan dan status kesehatan instance perangkat berubah menjadi SEHAT dari status kesehatan KRITIS.


```
{
    "version": "0",
    "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
    "detail-type": "Device Health Status Changed To Healthy",
    "source": "aws.one",
    "account": "123456789012",
    "time": "2022-10-22T18:43:48Z",
    "region": "us-east-1",
    "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
    "detail": {
    "version": "1.0.0",
    "metadata": {
      "siteName": "Site name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    },
    "data": {
      "currentHealthStatus": "HEALTHY",
      "previousHealthStatus": "CRITICAL",
      "assetTagId": "0000195169",
      "deviceInstanceName": "Device name"
    }
  }
}
```


Status kesehatan perangkat berubah menjadi kritis

Perangkat gagal satu atau lebih pemeriksaan kesehatan dan status kesehatan instance perangkat berubah menjadi KRITIS dari SEHAT.


```
{
  "version": "0",
  "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
  "detail-type": "Device Health Status Changed To Critical",
```

```
  "source": "aws.one",
  "account": "123456789012",
  "time": "2022-10-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
  "detail": {
    "version": "1.0.0",
    "metadata": {
      "siteName": "Site name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    },
    "data": {
      "currentHealthStatus": "CRITICAL",
      "previousHealthStatus": "HEALTHY",
      "assetTagId": "0000195169",
      "deviceInstanceName": "Device name"
    }
  }
}
```

Konektivitas perangkat diubah menjadi online

Perangkat terhubung ke internet dan status konektivitas instance perangkat diubah menjadi CONNECTED dari DISCONNECTED.

```
{
  "version": "0",
  "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
  "detail-type": "Device Connectivity Changed To Online",
  "source": "aws.one",
  "account": "123456789012",
  "time": "2022-10-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
  "detail": {
    "version": "1.0.0",
    "metadata": {
      "siteName": "Site name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    },
    "data": {
      "currentConnectivity": "CONNECTED",
      "previousConnectivity": "DISCONNECTED",
```

```
      "assetTagId": "0000195169",
      "deviceInstanceName": "Device name"
    }
  }
}
```

Konektivitas perangkat diubah menjadi offline

Perangkat tidak terhubung ke internet dan status konektivitas instance perangkat diubah menjadi TERPUTUS dari TERHUBUNG.

```
{
  "version": "0",
  "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
  "detail-type": "Device Connectivity Changed To Offline",
  "source": "aws.one",
  "account": "123456789012",
  "time": "2022-10-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
  "detail": {
    "version": "1.0.0",
    "metadata": {
      "siteName": "Site name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    },
    "data": {
      "currentConnectivity": "DISCONNECTED",
      "previousConnectivity": "CONNECTED",
      "assetTagId": "0000195169",
      "deviceInstanceName": "Device name"
    }
  }
}
```

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 fileTindakan, 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 siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut ini:

- Apakah permintaan itu dibuat dengan kredenal 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 manapun 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": "AIDAKDBGOAT6C2EXAMPLE:J_DOE",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin/J_DOE",
        "accountId": "123456789012",
        "accessKeyId": "AKIALAVPULGA71EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAKDBGOAT6C2EXAMPLE",
                "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-8910-1112-12fghi0jk13l"
    },
    "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

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

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, lihatBagaimana 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 situs

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

Saya tidak dapat membuat instance perangkat

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

Saya tidak dapat membuat templat konfigurasi

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

Saya tidak dapat membuat kode QR aktivasi

- Hubungi administrator Amazon One Console Anda 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

- 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 perangkat/sistem host 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.

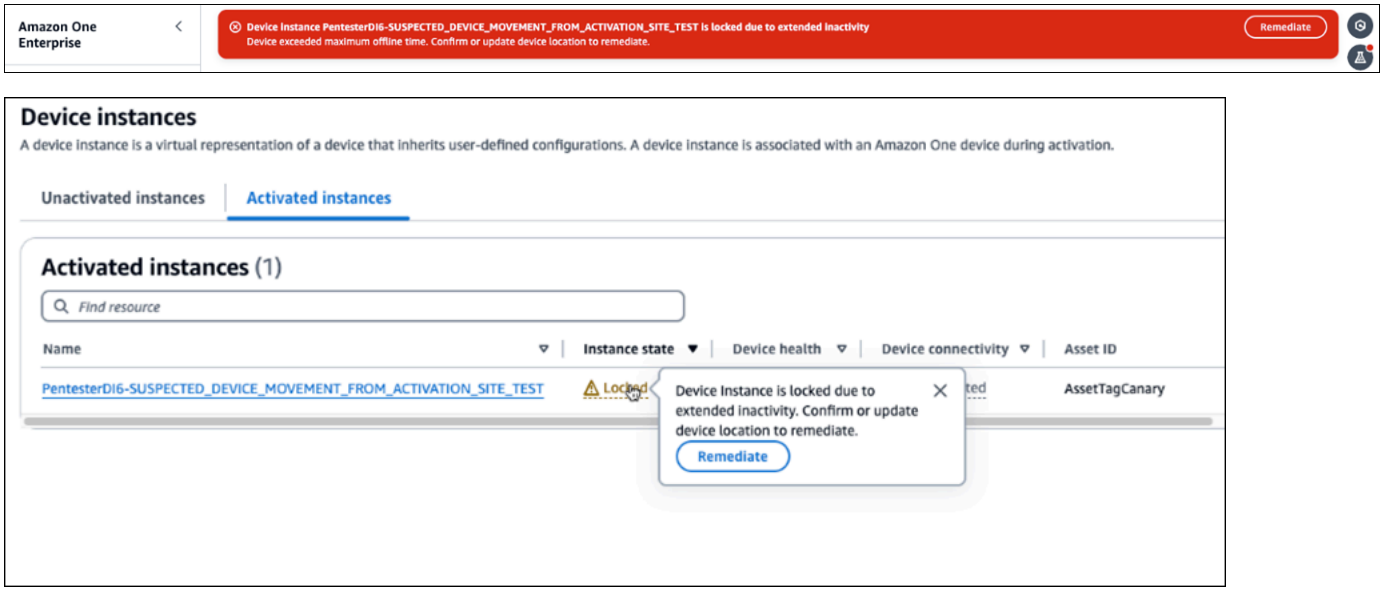
Perangkat terkunci karena ketidakaktifan yang diperpanjang

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
Perbarui	Menambahkan bagian Peran Tertaut Layanan	Februari 4, 2025
Perbarui	Ditambahkan: konten Skenario-driven	Oktober 10, 2024
Perbarui	Topik yang ditambahkan: Memecahkan masalah konsol Amazon One Enterprise	Oktober 10, 2024
Perbarui	Topik yang ditambahk an: Pemecahan masalah perangkat Amazon One Enterprise	Oktober 10, 2024
Perbarui	Bab yang ditambahkan: Menyiapkan Amazon One Enterprise	Oktober 10, 2024
Perbarui	Topik tambahan: Memelihara dan membersihkan perangkat Amazon One Enterprise	Oktober 10, 2024
Perbarui	Konten yang direorganisasi	Oktober 10, 2024
Perbarui	Topik yang ditambahkan: Menginstal perangkat Amazon One Enterprise I/O Hub untuk akses aman	Agustus 14, 2024

Perbarui	Topik tambahan: Memasang perangkat Amazon One Enterprise yang dapat dipasang di dinding	Juni 5, 2024
Rilis awal	Rilis awal Panduan Pengguna Amazon One Enterprise	27 November 2023

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