aws

Panduan Administrasi

AWS Wickr

AWS Wickr: Panduan Administrasi

Table of Contents

Apa itu AWS Wickr?

AWS Wickr adalah layanan end-to-end terenkripsi yang membantu organisasi dan lembaga pemerintah untuk berkomunikasi dengan aman melalui dan mengelompokkan pesan, panggilan suara one-to-one dan video, berbagi file, berbagi layar, dan banyak lagi. Wickr dapat membantu pelanggan mengatasi kewajiban penyimpanan data yang terkait dengan aplikasi perpesanan tingkat konsumen, dan memfasilitasi kolaborasi dengan aman. Kontrol keamanan dan administratif tingkat lanjut membantu organisasi memenuhi persyaratan hukum dan peraturan, dan membangun solusi khusus untuk tantangan keamanan data.

Informasi dapat dicatat ke penyimpanan data pribadi yang dikendalikan pelanggan untuk tujuan retensi dan audit. Pengguna memiliki kontrol administratif yang komprehensif atas data, yang mencakup pengaturan izin, mengonfigurasi opsi pesan singkat, dan mendefinisikan grup keamanan. Wickr terintegrasi dengan layanan tambahan seperti Active Directory (AD), single sign-on (SSO) dengan OpenID Connect (OIDC), dan banyak lagi. Anda dapat dengan cepat membuat dan mengelola jaringan Wickr melalui Konsol Manajemen AWS, dan mengotomatiskan alur kerja dengan aman menggunakan bot Wickr. Untuk memulai, lihat Menyiapkan AWS Wickr.

Topik

Fitur Wickr

Keamanan dan privasi yang ditingkatkan

Wickr menggunakan enkripsi Advanced Encryption Standard (AES) end-to-end 256-bit untuk setiap fitur. Komunikasi dienkripsi secara lokal di perangkat pengguna, dan tetap tidak dapat diuraikan dalam perjalanan ke siapa pun selain pengirim dan penerima. Setiap pesan, panggilan, dan file dienkripsi dengan kunci acak baru, dan tidak seorang pun kecuali penerima yang dituju (bahkan tidak AWS) dapat mendekripsi mereka. Apakah mereka berbagi data sensitif dan diatur, mendiskusikan masalah hukum atau SDM, atau bahkan melakukan operasi militer taktis, pelanggan menggunakan Wickr untuk berkomunikasi ketika keamanan dan privasi adalah yang terpenting.

Retensi data

Fitur administratif yang fleksibel dirancang tidak hanya untuk melindungi informasi sensitif, tetapi untuk menyimpan data sebagaimana diperlukan untuk kewajiban kepatuhan, penahanan hukum, dan tujuan audit. Pesan dan file dapat diarsipkan di penyimpanan data yang aman dan dikendalikan pelanggan.

Akses yang fleksibel

Pengguna memiliki akses multi-perangkat (seluler, desktop) dan kemampuan untuk berfungsi di lingkungan bandwidth rendah, termasuk terputus dan komunikasi. out-of-band

Kontrol administratif

Pengguna memiliki kontrol administratif yang komprehensif atas data, yang mencakup pengaturan izin, mengonfigurasi opsi pesan singkat yang bertanggung jawab, dan mendefinisikan grup keamanan.

Integrasi dan bot yang kuat

Wickr terintegrasi dengan layanan tambahan seperti Active Directory, single sign-on (SSO) dengan OpenID Connect (OIDC), dan banyak lagi. Pelanggan dapat dengan cepat membuat dan mengelola jaringan Wickr melalui Konsol Manajemen AWS, dan mengotomatiskan alur kerja dengan aman dengan Wickr Bots.

Berikut ini adalah rincian penawaran kolaborasi Wickr:

- 1:1 dan pesan grup: Mengobrol dengan aman dengan tim Anda di kamar dengan hingga 500 anggota
- Panggilan audio dan video: Mengadakan panggilan konferensi dengan hingga 70 orang
- Berbagi layar dan penyiaran: Hadir dengan hingga 500 peserta
- Berbagi dan menyimpan file: Transfer file hingga 5 GBs dengan penyimpanan tak terbatas
- Ephemeral: Kontrol kedaluwarsa dan pengatur waktu burn-on-read
- Federasi global: Terhubung dengan pengguna Wickr di luar jaringan Anda

Ketersediaan wilayah

Wickr tersedia di AS Timur (Virginia N.), Asia Pasifik (Malaysia), Asia Pasifik (Singapura), Asia Pasifik (Sydney), Asia Pasifik (Tokyo), Kanada (Tengah), Eropa (Frankfurt), Eropa (London), Eropa

(Stockholm), dan Eropa (Zurich). Wilayah AWS Wickr juga tersedia di Wilayah AWS GovCloud (AS-Barat). Setiap Wilayah berisi beberapa Availability Zone, yang secara fisik terpisah tetapi terhubung oleh koneksi jaringan pribadi, latensi rendah, bandwidth tinggi, dan redundan. Availability Zone ini digunakan untuk memberikan peningkatan ketersediaan, toleransi kesalahan, dan latensi yang diminimalkan.

Untuk mempelajari selengkapnya Wilayah AWS, lihat Menentukan Wilayah AWS akun mana yang dapat digunakan di Referensi Umum AWS. Untuk informasi selengkapnya tentang jumlah Availability Zone yang tersedia di setiap Wilayah, lihat Infrastruktur AWS Global.

Mengakses Wickr

Administrator mengakses Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/ Sebelum Anda mulai menggunakan Wickr Anda harus menyelesaikan Menyiapkan AWS Wickr dan Memulai AWS Wickr panduan.

Pengguna akhir mengakses Wickr melalui klien Wickr. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS Wickr.

Harga

Wickr tersedia dalam berbagai rencana untuk individu, tim kecil, dan bisnis besar. Untuk informasi selengkapnya, lihat Harga AWS Wickr.

Dokumentasi pengguna akhir Wickr

Jika Anda adalah pengguna akhir klien Wickr dan perlu mengakses dokumentasinya, lihat Panduan Pengguna AWS Wickr.

Menyiapkan AWS Wickr

Jika Anda adalah AWS pelanggan baru, selesaikan prasyarat penyiapan yang tercantum di halaman ini sebelum Anda mulai menggunakan AWS Wickr. Untuk prosedur penyiapan ini, Anda menggunakan layanan AWS Identity and Access Management (IAM). Untuk informasi selengkapnya tentang IAM, lihat Panduan Pengguna IAM.

Topik

Mendaftar untuk AWS

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

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/pendaftaran.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon atau pesan teks dan memasukkan kode verifikasi pada keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

Mmebuat pengguna IAM

Untuk membuat pengguna administrator, pilih salah satu opsi berikut.

Pilih salah satu cara untuk mengelola administrator Anda	Untuk	Oleh	Anda juga bisa
Di Pusat Identitas IAM (Direkomendasikan)	Gunakan kredensi jangka pendek untuk mengakses. AWS Ini sejalan dengan praktik terbaik keamanan. Untuk informasi tentang praktik terbaik, lihat Praktik terbaik keamanan di IAM di Panduan Pengguna IAM.	Mengikuti petunjuk di Memulai di Panduan AWS IAM Identity Center Pengguna.	Konfigurasikan akses terprogram dengan Mengonfigurasi AWS CLI yang akan digunakan AWS IAM Identity Center dalam AWS Command Line Interface Panduan Pengguna.
Di IAM (Tidak direkomen dasikan)	Gunakan kredensi jangka panjang untuk mengakses. AWS	Mengikuti petunjuk dalam Membuat pengguna admin IAM pertama Anda dan grup pengguna di Panduan Pengguna IAM.	Konfigurasikan akses terprogram dengan Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

> **Note**
>
> Anda juga dapat menetapkan kebijakan `AWSWickrFullAccess` terkelola untuk memberikan izin administratif penuh ke layanan Wickr. Untuk informasi selengkapnya, lihat AWS kebijakan terkelola: AWSWickr FullAccess.

Apa selanjutnya

Anda menyelesaikan langkah-langkah pengaturan prasyarat. Untuk mulai mengkonfigurasi Wickr, lihat. Mulai menggunakan

Memulai AWS Wickr

Dalam panduan ini, kami menunjukkan kepada Anda cara memulai dengan Wickr dengan membuat jaringan, mengonfigurasi jaringan Anda, dan membuat pengguna.

Topik

Prasyarat

Sebelum Anda mulai, pastikan untuk menyelesaikan prasyarat berikut jika Anda belum melakukannya:

- Mendaftar untuk Amazon Web Services (AWS). Untuk informasi selengkapnya, lihat Menyiapkan AWS Wickr.
- Pastikan Anda memiliki izin yang diperlukan untuk mengelola Wickr. Untuk informasi selengkapnya, lihat AWS kebijakan terkelola: AWSWickr FullAccess.
- Pastikan Anda mengizinkan daftar port dan domain yang sesuai untuk Wickr. Untuk informasi selengkapnya, lihat Port dan domain untuk memungkinkan daftar untuk jaringan Wickr Anda.

Langkah 1: Buat jaringan

Anda dapat membuat jaringan Wickr.

Selesaikan prosedur berikut untuk membuat jaringan Wickr untuk akun Anda.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/

> **Note**
>
> Jika Anda belum pernah membuat jaringan Wickr sebelumnya, Anda akan melihat halaman informasi untuk layanan Wickr. Setelah Anda membuat satu atau lebih jaringan

Wickr, Anda akan melihat halaman Jaringan, yang berisi tampilan daftar semua jaringan Wickr yang telah Anda buat.

2. Pilih Buat jaringan.
3. Masukkan nama untuk jaringan Anda di kotak teks Nama jaringan. Pilih nama yang akan dikenali oleh anggota organisasi Anda, seperti nama perusahaan Anda atau nama tim Anda.
4. Pilih rencana. Anda dapat memilih salah satu paket jaringan Wickr berikut:

   - Standar — Untuk tim bisnis kecil dan besar yang membutuhkan kontrol administratif dan fleksibilitas.
   - Uji Coba Gratis Premium atau Premium — Untuk bisnis yang memerlukan batas fitur tertinggi, kontrol administratif terperinci, dan retensi data.

   Administrator memiliki opsi untuk memilih uji coba gratis premium, yang tersedia hingga 30 pengguna dan berlangsung selama tiga bulan. Untuk AWS WickrGov, opsi uji coba gratis premium memungkinkan hingga 50 pengguna dan juga bertahan selama tiga bulan. Selama masa uji coba gratis premium, administrator dapat meningkatkan atau menurunkan versi ke paket Premium atau Standar.

   Untuk informasi selengkapnya tentang paket dan harga Wickr yang tersedia, lihat halaman harga Wickr.
5. (Opsional) Pilih Tambahkan tag baru untuk menambahkan tag ke jaringan Anda. Tag terdiri dari pasangan nilai kunci. Tag dapat digunakan untuk mencari dan memfilter sumber daya atau melacak AWS biaya Anda. Untuk informasi selengkapnya, lihat Tag jaringan.
6. Pilih Buat Jaringan.

   Anda diarahkan ke halaman Jaringan Konsol Manajemen AWS untuk Wickr, dan jaringan baru tercantum di halaman.

Langkah 2: Konfigurasikan jaringan Anda

Selesaikan prosedur berikut untuk mengakses Wickr, di mana Anda dapat menambahkan pengguna, menambahkan grup keamanan, mengkonfigurasi SSO, mengonfigurasi retensi data, dan pengaturan jaringan tambahan. Konsol Manajemen AWS

1. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.

Anda dialihkan ke Konsol Admin Wickr untuk jaringan yang dipilih.

2. Opsi manajemen pengguna berikut tersedia. Untuk informasi selengkapnya tentang mengonfigurasi setelan ini, lihatKelola jaringan AWS Wickr Anda.

   - Grup Keamanan — Kelola grup keamanan dan pengaturannya, seperti kebijakan kompleksitas kata sandi, preferensi pesan, fitur panggilan, fitur keamanan, dan federasi eksternal. Untuk informasi selengkapnya, lihat Grup keamanan untuk AWS Wickr.
   - Konfigurasi Single Sign-on (SSO) - Konfigurasikan SSO dan lihat alamat titik akhir untuk jaringan Wickr Anda. Wickr mendukung penyedia SSO yang hanya menggunakan OpenID Connect (OIDC). Penyedia yang menggunakan Security Assertion Markup Language (SALL) tidak didukung. Untuk informasi selengkapnya, lihat Konfigurasi masuk tunggal untuk AWS Wickr.

Langkah 3: Buat dan undang pengguna

Anda dapat membuat pengguna di jaringan Wickr Anda menggunakan metode berikut:

- Single sign-on — Jika Anda mengonfigurasi SSO, Anda dapat mengundang pengguna dengan membagikan ID perusahaan Wickr Anda. Pengguna akhir mendaftar untuk Wickr menggunakan ID perusahaan yang disediakan dan alamat email kantor mereka. Untuk informasi selengkapnya, lihat Konfigurasi masuk tunggal untuk AWS Wickr.
- Undangan - Anda dapat secara manual membuat pengguna di Konsol Manajemen AWS for Wickr dan memiliki undangan email yang dikirim kepada mereka. Pengguna akhir dapat mendaftar untuk Wickr dengan memilih tautan di email.

> **Note**
>
> Anda juga dapat mengaktifkan pengguna tamu untuk jaringan Wickr Anda. Untuk informasi selengkapnya, lihat Pengguna tamu di jaringan AWS Wickr

Lengkapi prosedur berikut untuk membuat atau mengundang pengguna.

> **Note**
>
> Administrator juga dianggap pengguna dan harus mengundang diri mereka ke jaringan SSO atau non-SSO Wickr.

Untuk membuat pengguna Wickr dan mengirim undangan dengan SSO:

Tulis dan kirim email ke pengguna SSO yang harus mendaftar untuk Wickr. Sertakan informasi berikut di email Anda:

- ID perusahaan Wickr Anda. Anda menentukan ID perusahaan untuk jaringan Wickr Anda ketika Anda mengkonfigurasi SSO. Untuk informasi selengkapnya, lihat Konfigurasikan SSO di AWS Wickr.
- Alamat email yang harus mereka gunakan untuk mendaftar.
- URL untuk mengunduh klien Wickr. Pengguna dapat mengunduh klien Wickr dari halaman unduhan AWS Wickr saat mengunduh/. https://aws.amazon.com/wickr/

> **Note**
>
> Jika Anda membuat jaringan Wickr Anda di AWS GovCloud (US-Barat), instruksikan pengguna Anda untuk mengunduh dan menginstal klien. WickrGov Untuk semua AWS Wilayah lainnya, instruksikan pengguna Anda untuk mengunduh dan menginstal klien Wickr standar. Untuk informasi selengkapnya AWS WickrGov, lihat AWS WickrGovdi Panduan AWS GovCloud (US) Pengguna.

Saat pengguna mendaftar untuk jaringan Wickr Anda, mereka ditambahkan ke direktori tim Wickr dengan status aktif.

Untuk membuat pengguna Wickr secara manual dan mengirim undangan:

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.

   Kau dialihkan ke jaringan Wickr. Di jaringan Wickr, Anda dapat menambahkan pengguna, menambahkan grup keamanan, mengonfigurasi SSO, mengonfigurasi retensi data, dan menyesuaikan pengaturan tambahan.

3. Di panel navigasi, pilih Manajemen pengguna.
4. Pada halaman Manajemen pengguna, di bawah tab Direktori tim, pilih Undang pengguna.

   Anda juga dapat mengundang pengguna secara massal dengan memilih panah tarik-turun di sebelah Undang pengguna. Pada halaman mengundang pengguna Massal, pilih Unduh templat untuk mengunduh templat CSV yang dapat Anda edit dan unggah dengan daftar pengguna Anda.
5. Masukkan nama depan, nama belakang, kode negara, nomor telepon, dan alamat email pengguna. Alamat email adalah satu-satunya bidang yang diperlukan. Pastikan untuk memilih grup keamanan yang sesuai untuk pengguna.
6. Pilih Undang.

   Wickr mengirimkan email undangan ke alamat yang Anda tentukan untuk pengguna. Email tersebut menyediakan tautan unduhan untuk aplikasi klien Wickr, dan tautan untuk mendaftar ke Wickr. Untuk informasi selengkapnya tentang tampilan pengalaman pengguna akhir ini, lihat Mengunduh aplikasi Wickr dan menerima undangan Anda di Panduan Pengguna AWS Wickr.

   Saat pengguna mendaftar untuk Wickr menggunakan tautan di email, status mereka di direktori tim Wickr akan berubah dari Tertunda menjadi Aktif.

Langkah selanjutnya

Anda menyelesaikan langkah-langkah memulai. Untuk mengelola Wickr, lihat berikut ini:

- Kelola jaringan AWS Wickr Anda
- Kelola pengguna di AWS Wickr

Kelola jaringan AWS Wickr Anda

Dalam Konsol Manajemen AWS untuk Wickr Anda dapat mengelola nama jaringan Wickr Anda, grup keamanan, konfigurasi SSO, dan pengaturan retensi data.

Topik

Detail jaringan untuk AWS Wickr

Anda dapat mengedit nama jaringan Wickr Anda dan melihat ID jaringan Anda di bagian Detail jaringan Konsol Manajemen AWS untuk Wickr.

Topik

Lihat detail jaringan di AWS Wickr

Anda dapat melihat detail jaringan Wickr Anda, termasuk nama jaringan dan ID jaringan Anda.

Selesaikan prosedur berikut untuk melihat profil jaringan dan ID jaringan Wickr Anda.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, temukan jaringan yang ingin Anda lihat.
3. Di sisi kanan jaringan yang ingin Anda lihat, pilih ikon elipsis vertikal (tiga titik), lalu pilih Lihat detail.

   Halaman beranda Jaringan menampilkan nama jaringan Wickr dan ID jaringan Anda di bagian Detail Jaringan. Anda dapat menggunakan ID jaringan untuk mengkonfigurasi federasi.

Edit nama jaringan di AWS Wickr

Anda dapat mengedit nama jaringan Wickr Anda.

Selesaikan prosedur berikut untuk mengedit nama jaringan Wickr Anda.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke Konsol Admin Wickr untuk jaringan tersebut.
3. Di halaman beranda Jaringan, di bagian Detail jaringan, pilih Edit.
4. Masukkan nama jaringan baru Anda ke dalam kotak teks Nama Jaringan.
5. Pilih Simpan untuk menyimpan nama jaringan baru Anda.

Hapus jaringan di AWS Wickr

Anda dapat menghapus jaringan AWS Wickr Anda.

> **Note**
>
> Jika Anda menghapus jaringan uji coba gratis premium, Anda tidak akan dapat membuat yang lain.

Untuk menghapus jaringan Wickr Anda di halaman beranda Networks, selesaikan prosedur berikut.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, temukan jaringan yang ingin Anda hapus.
3. Di sisi kanan jaringan yang ingin Anda hapus, pilih ikon elipsis vertikal (tiga titik), lalu pilih Hapus jaringan.

4. Ketik konfirmasi di jendela pop-up, lalu pilih Hapus.

   Diperlukan beberapa menit untuk menghapus jaringan.

Untuk menghapus jaringan Wickr Anda saat berada di jaringan, selesaikan prosedur berikut.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih jaringan yang ingin Anda hapus.
3. Di dekat sudut kanan atas halaman beranda Jaringan, pilih Hapus jaringan.
4. Ketik konfirmasi di jendela pop-up, lalu pilih Hapus.

   Diperlukan beberapa menit untuk menghapus jaringan.

> **Note**
>
> Data yang disimpan oleh konfigurasi penyimpanan data Anda (jika diaktifkan) tidak akan dihapus ketika Anda menghapus jaringan Anda. Untuk informasi selengkapnya, lihat Retensi data untuk AWS Wickr.

Grup keamanan untuk AWS Wickr

Di bagian Grup Keamanan Konsol Manajemen AWS untuk Wickr, Anda dapat mengelola grup keamanan dan pengaturannya, seperti kebijakan kompleksitas kata sandi, preferensi pesan, fitur panggilan, fitur keamanan, dan federasi jaringan.

Topik

Lihat grup keamanan di AWS Wickr

Anda dapat melihat detail grup keamanan Wickr Anda.

Selesaikan prosedur berikut untuk melihat grup keamanan.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Pada panel navigasi, pilih Grup keamanan.

   Halaman grup Keamanan menampilkan grup keamanan Wickr Anda saat ini dan memberi Anda opsi untuk membuat grup baru.

   Pada halaman Grup keamanan, pilih grup keamanan yang ingin Anda lihat. Halaman akan menampilkan detail saat ini untuk grup keamanan tersebut.

Buat grup keamanan di AWS Wickr

Anda dapat membuat grup keamanan Wickr baru.

Selesaikan prosedur berikut untuk membuat grup keamanan.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Pada panel navigasi, pilih Grup keamanan.
4. Pada halaman Grup keamanan, pilih Buat grup keamanan untuk membuat grup keamanan baru.

   > **Note**
   >
   > Grup keamanan baru dengan nama default secara otomatis ditambahkan ke daftar grup keamanan.

5. Pada halaman Buat grup keamanan, masukkan nama grup keamanan Anda.
6. Pilih Buat grup keamanan.

   Untuk informasi selengkapnya tentang mengedit grup keamanan baru, lihatMengedit grup keamanan di AWS Wickr.

Mengedit grup keamanan di AWS Wickr

Anda dapat mengedit detail grup keamanan Wickr Anda.

Selesaikan prosedur berikut untuk mengedit grup keamanan.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Pada panel navigasi, pilih Grup keamanan.
4. Pilih nama grup keamanan yang ingin Anda edit.

   Halaman detail grup keamanan menampilkan pengaturan untuk grup keamanan di tab yang berbeda.
5. Tab berikut dan pengaturan yang sesuai tersedia:

   - Detail grup keamanan - Pilih Edit di bagian Detail grup keamanan untuk mengedit nama.
   - Pesan — Kelola fitur pesan untuk anggota grup.
     - B urn-on-read — Mengontrol nilai maksimum yang dapat ditetapkan pengguna untuk pengatur waktu mereka di burn-on-read klien Wickr mereka. Untuk informasi selengkapnya, lihat Mengatur kedaluwarsa pesan dan membakar timer di klien Wickr.
     - Timer kedaluwarsa - Mengontrol nilai maksimum yang dapat diatur pengguna untuk pengatur waktu kedaluwarsa pesan mereka di klien Wickr mereka. Untuk informasi selengkapnya, lihat Mengatur kedaluwarsa pesan dan membakar timer di klien Wickr.
     - Penerusan pesan — Mengontrol apakah pengguna dapat meneruskan pesan di klien Wickr mereka. Untuk informasi selengkapnya, lihat Meneruskan pesan di klien Wickr.
     - Respons cepat - Tetapkan daftar respons cepat bagi pengguna untuk merespons pesan.
     - Intensitas shredder aman — Konfigurasikan seberapa sering kontrol penghancur aman berjalan untuk pengguna. Untuk informasi selengkapnya, lihat Pesan.
   - Panggilan - Kelola fitur panggilan untuk anggota grup.
     - Aktifkan panggilan audio - Pengguna dapat memulai panggilan audio.
     - Aktifkan panggilan video dan berbagi layar - Pengguna dapat memulai panggilan video atau berbagi layar selama panggilan.
     - Panggilan TCP — Mengaktifkan (atau memaksa) panggilan TCP biasanya digunakan ketika port UDP VoIP standar tidak diizinkan oleh departemen TI atau keamanan organisasi. Jika panggilan TCP dinonaktifkan, dan port UDP tidak tersedia untuk digunakan, klien Wickr akan mencoba UDP terlebih dahulu dan mundur ke TCP.
   - Media dan tautan - Kelola pengaturan yang terkait dengan media dan tautan untuk anggota grup.

Ukuran unduhan file - Pilih Transfer kualitas terbaik untuk memungkinkan pengguna mentransfer file dan lampiran dalam bentuk terenkripsi aslinya. Jika Anda memilih transfer bandwidth rendah, lampiran file yang dikirim oleh pengguna di Wickr akan dikompresi oleh layanan transfer file Wickr.

- Lokasi - Mengelola pengaturan berbagi lokasi untuk anggota grup.

  Berbagi lokasi - Pengguna dapat berbagi lokasi mereka menggunakan perangkat berkemampuan GPS. Fitur ini menampilkan peta visual berdasarkan default sistem operasi perangkat. Pengguna memiliki opsi untuk menonaktifkan tampilan peta dan membagikan tautan yang berisi koordinat GPS mereka sebagai gantinya.

- Keamanan — Konfigurasikan fitur keamanan tambahan untuk grup.
  - Aktifkan perlindungan pengambilalihan akun — Terapkan autentikasi dua faktor saat pengguna menambahkan perangkat baru ke akun mereka. Untuk memverifikasi perangkat baru, pengguna dapat membuat kode Wickr dari perangkat lama mereka, atau melakukan verifikasi email. Ini adalah lapisan keamanan tambahan untuk mencegah akses tidak sah ke akun AWS Wickr.
  - Aktifkan selalu autentikasi ulang - Memaksa pengguna untuk selalu mengautentikasi ulang saat memasuki kembali aplikasi.
  - Kunci pemulihan master - Membuat kunci pemulihan Master saat akun dibuat. Pengguna dapat menyetujui penambahan perangkat baru ke akun mereka jika tidak ada perangkat lain yang tersedia.
- Pemberitahuan dan visibilitas — Konfigurasikan pengaturan notifikasi dan visibilitas seperti pratinjau pesan di notifikasi untuk anggota grup.
- Akses terbuka Wickr - Konfigurasikan pengaturan akses terbuka Wickr untuk anggota grup.
  - Aktifkan akses terbuka Wickr — Mengaktifkan akses terbuka Wickr akan menyamarkan lalu lintas untuk melindungi data pada jaringan yang dibatasi dan dipantau. Berdasarkan lokasi geografis, akses terbuka Wickr akan terhubung ke berbagai server proxy global yang menyediakan jalur dan protokol terbaik untuk pengaburan lalu lintas.
  - Memaksa akses terbuka Wickr - Secara otomatis mengaktifkan dan memberlakukan akses terbuka Wickr di semua perangkat.
- Federasi — Kontrol kemampuan pengguna Anda untuk berkomunikasi dengan jaringan Wickr lainnya.
  - Federasi lokal — Kemampuan untuk berfederasi dengan AWS pengguna di jaringan lain dalam wilayah yang sama. Misalnya, jika ada dua jaringan di Wilayah AWS Kanada

(Tengah) dengan federasi lokal diaktifkan, mereka akan dapat berkomunikasi satu sama lain.

- Federasi global — Kemampuan untuk berfederasi dengan pengguna Wickr Enterprise atau AWS pengguna di jaringan berbeda yang termasuk dalam wilayah lain. Misalnya, pengguna di jaringan Wickr di Wilayah AWS Kanada (Tengah), dan pengguna dalam jaringan di Wilayah AWS Eropa (London) akan dapat berkomunikasi satu sama lain ketika federasi global diaktifkan untuk kedua jaringan.
- Federasi terbatas — Izinkan daftar jaringan AWS Wickr atau Wickr Enterprise tertentu yang dapat difederasi oleh pengguna. Ketika dikonfigurasi, pengguna hanya dapat berkomunikasi dengan pengguna eksternal di mengizinkan jaringan yang terdaftar. Kedua jaringan harus mengizinkan daftar satu sama lain untuk menggunakan federasi terbatas.

  Untuk informasi tentang federasi tamu, lihat Mengaktifkan atau menonaktifkan pengguna tamu di jaringan AWS Wickr.

- Konfigurasi plugin ATAK - Untuk informasi selengkapnya tentang mengaktifkan ATAK, lihat Apa itu ATAK? .

6. Pilih Simpan untuk menyimpan pengeditan yang Anda buat ke detail grup keamanan.

Menghapus grup keamanan di AWS Wickr

Anda dapat menghapus grup keamanan Wickr Anda.

Selesaikan prosedur berikut untuk menghapus grup keamanan.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Pada panel navigasi, pilih Grup keamanan.
4. Pada halaman Grup keamanan, temukan grup keamanan yang ingin Anda hapus.
5. Di sisi kanan grup keamanan yang ingin Anda hapus, pilih ikon elipsis vertikal (tiga titik), lalu pilih Hapus.
6. Ketik konfirmasi di jendela pop-up, lalu pilih Hapus.

   Saat Anda menghapus grup keamanan yang telah menetapkan pengguna, pengguna tersebut secara otomatis ditambahkan ke grup keamanan default. Untuk mengubah grup keamanan yang ditetapkan untuk pengguna, lihatMengedit pengguna di jaringan AWS Wickr.

Konfigurasi masuk tunggal untuk AWS Wickr

Dalam Konsol Manajemen AWS untuk Wickr, Anda dapat mengonfigurasi Wickr untuk menggunakan sistem masuk tunggal untuk mengautentikasi. SSO menyediakan lapisan keamanan tambahan saat dipasangkan dengan sistem otentikasi multi-faktor (MFA) yang sesuai. Wickr mendukung penyedia SSO yang hanya menggunakan OpenID Connect (OIDC). Penyedia yang menggunakan Security Assertion Markup Language (SALL) tidak didukung.

Topik

Lihat detail SSO di AWS Wickr

Anda dapat melihat detail konfigurasi masuk tunggal untuk jaringan Wickr Anda dan titik akhir jaringan.

Selesaikan prosedur berikut untuk melihat konfigurasi masuk tunggal saat ini untuk jaringan Wickr Anda, jika ada.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Di panel navigasi, pilih Manajemen Pengguna.

   Pada halaman Manajemen Pengguna, bagian Single Sign-on menampilkan titik akhir jaringan Wickr Anda dan konfigurasi SSO saat ini.

Konfigurasikan SSO di AWS Wickr

Untuk memastikan akses aman ke jaringan Wickr Anda, Anda dapat mengatur konfigurasi masuk tunggal Anda saat ini. Panduan terperinci tersedia untuk membantu Anda dalam proses ini.

Important

- Ketika Anda mengkonfigurasi SSO, Anda menentukan ID perusahaan untuk jaringan Wickr Anda. Pastikan untuk mencatat ID perusahaan ini. Anda harus memberikannya kepada

pengguna akhir Anda saat mengirim email undangan. Pengguna akhir harus menentukan ID perusahaan ketika mereka mendaftar untuk jaringan Wickr Anda.

- Pada bulan September 2025, AWS Wickr memperkenalkan sistem koneksi SSO yang lebih baik dan lebih aman. Untuk memanfaatkan peningkatan keamanan ini, organisasi yang menggunakan SSO harus bermigrasi ke URI pengalihan baru sebelum 09 Maret 2026. Untuk petunjuk migrasi, lihat AWS re:Post artikel berikut: Migrasi ke URI Pengalihan SSO Baru untuk AWS Wickr.

Untuk informasi selengkapnya tentang mengonfigurasi SSO, lihat panduan berikut:

- Penyiapan AWS Wickr Single Sign-on (SSO) dengan Microsoft Entra (Azure AD)
- Penyiapan AWS Wickr Single Sign-on (SSO) dengan Okta
- Penyiapan AWS Wickr Single Sign-on (SSO) dengan Amazon Cognito

Konfigurasikan AWS Wickr dengan sistem masuk tunggal Microsoft Entra (Azure AD)

AWS Wickr dapat dikonfigurasi untuk menggunakan Microsoft Entra (Azure AD) sebagai penyedia identitas. Untuk melakukannya, selesaikan prosedur berikut di Microsoft Entra dan konsol admin AWS Wickr.

Warning

Setelah SSO diaktifkan pada jaringan itu akan menandatangani pengguna aktif keluar dari Wickr dan memaksa mereka untuk mengautentikasi ulang menggunakan penyedia SSO.

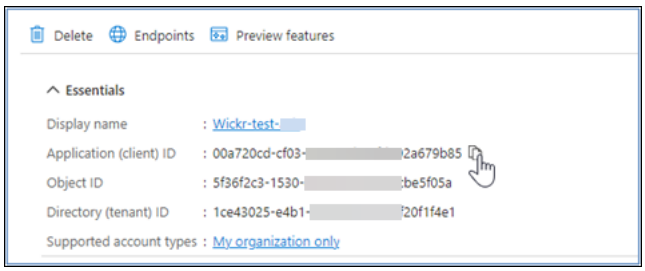
Langkah 1: Daftarkan AWS Wickr sebagai aplikasi di Microsoft Entra

Lengkapi prosedur berikut untuk mendaftarkan AWS Wickr sebagai aplikasi di Microsoft Entra.

Note

Lihat dokumentasi Microsoft Entra untuk tangkapan layar terperinci dan pemecahan masalah. Untuk informasi selengkapnya, lihat Mendaftarkan aplikasi dengan platform identitas Microsoft

1. Di panel navigasi, pilih Aplikasi dan kemudian pilih Pendaftaran Aplikasi.
2. Pada halaman Pendaftaran Aplikasi, pilih Daftarkan aplikasi, lalu masukkan nama aplikasi.
3. Pilih Akun di direktori organisasi ini saja (Hanya Direktori Default - Penyewa tunggal).
4. Di bawah Redirect URI, pilih Web, lalu masukkan URI pengalihan yang tersedia di pengaturan konfigurasi SSO di konsol Admin Wickr AWS
5. PilihPendaftaran.
6. Setelah pendaftaran, copy/save ID Aplikasi (Klien) dihasilkan.

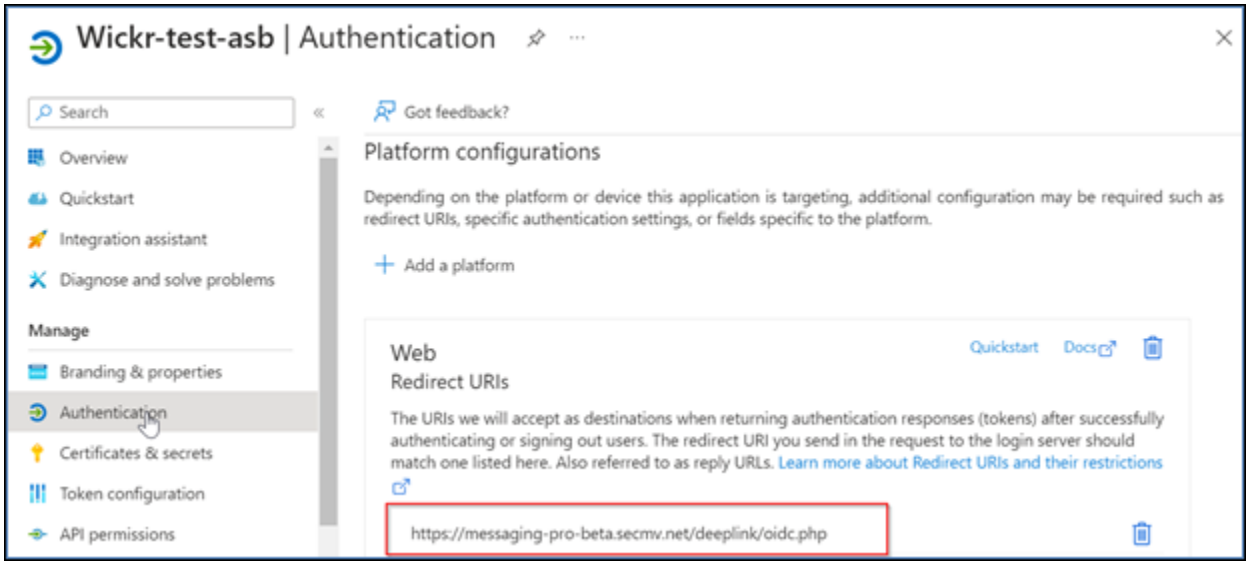


7. Pilih tab Endpoints untuk membuat catatan berikut:
    1. Titik akhir otorisasi Oauth 2.0 (v2): Misalnya: `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/oauth2/v2.0/authorize`
    2. Edit nilai ini untuk menghapus 'oauth2/” dan “otorisasi”. Misalnya URL tetap akan terlihat seperti ini: `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`
    3. Ini akan direferensikan sebagai Emiten SSO.

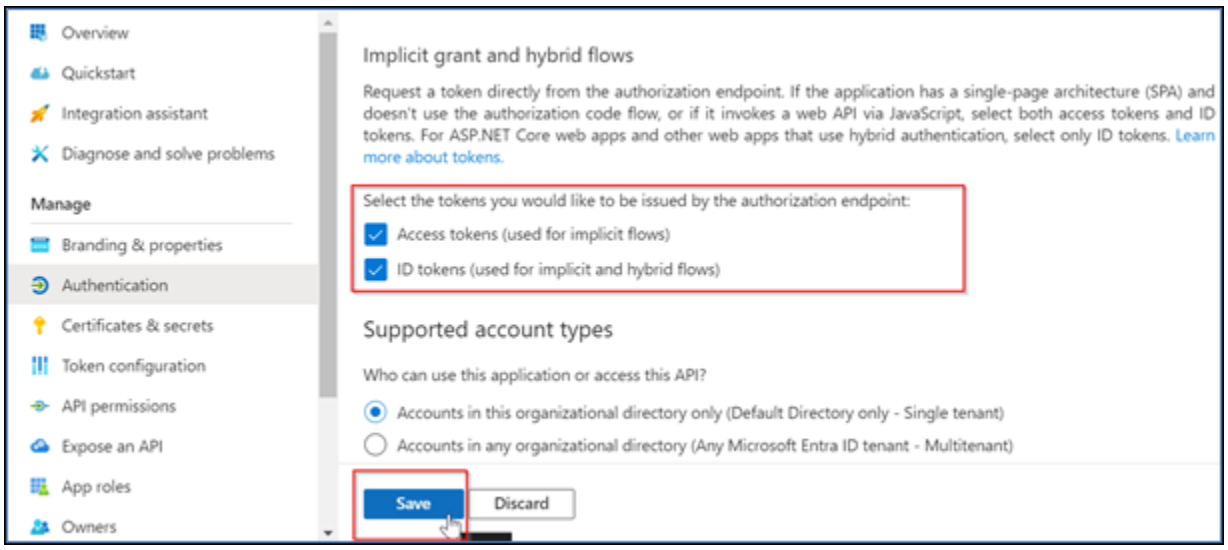
Langkah 2: Setup otentikasi

Selesaikan prosedur berikut untuk mengatur otentikasi di Microsoft Entra.

1. Di panel navigasi, pilih Otentikasi.
2. Pada halaman Otentikasi, pastikan URI Pengalihan Web sama dengan yang dimasukkan sebelumnya (dalam Daftar AWS Wickr sebagai Aplikasi).



3. Pilih Access token yang digunakan untuk aliran implisit dan token ID yang digunakan untuk aliran implisit dan hybrid.
4. Pilih Simpan.

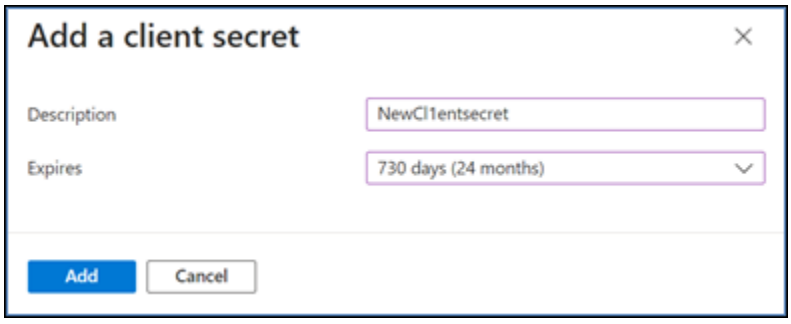


Langkah 3: Siapkan sertifikat dan rahasia

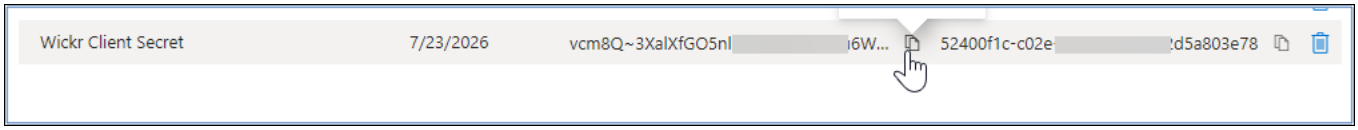
Selesaikan prosedur berikut untuk mengatur sertifikat dan rahasia di Microsoft Entra.

1. Di panel navigasi, pilih Sertifikat & rahasia.
2. Pada halaman Sertifikat & Rahasia, pilih tab Rahasia klien.
3. Di bawah tab Rahasia klien, pilih Rahasia klien baru.
4. Masukkan deskripsi dan pilih periode kedaluwarsa untuk rahasia tersebut.

5. Pilih Tambahkan.



6. Setelah sertifikat dibuat, salin nilai rahasia Klien.

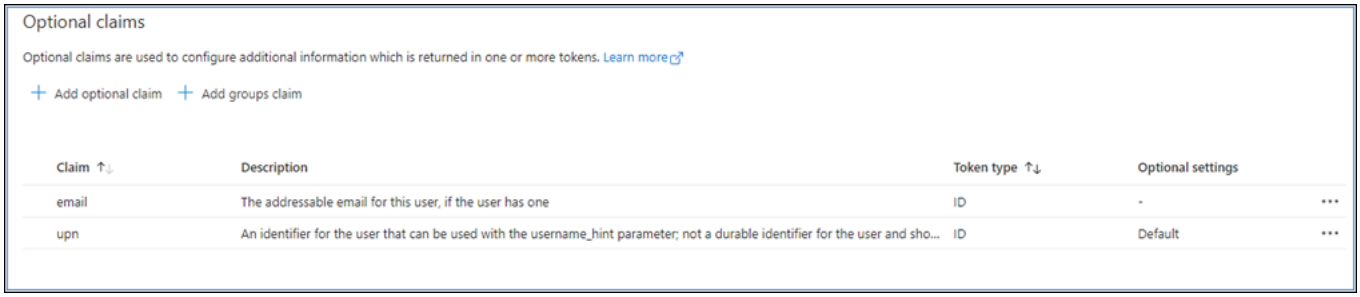


> **Note**
>
> Nilai rahasia klien (bukan ID Rahasia) akan diperlukan untuk kode aplikasi klien Anda. Anda mungkin tidak dapat melihat atau menyalin nilai rahasia setelah meninggalkan halaman ini. Jika Anda tidak menyalinnya sekarang, Anda harus kembali untuk membuat rahasia klien baru.

Langkah 4: Pengaturan konfigurasi token

Selesaikan prosedur berikut untuk mengatur konfigurasi token di Microsoft Entra.

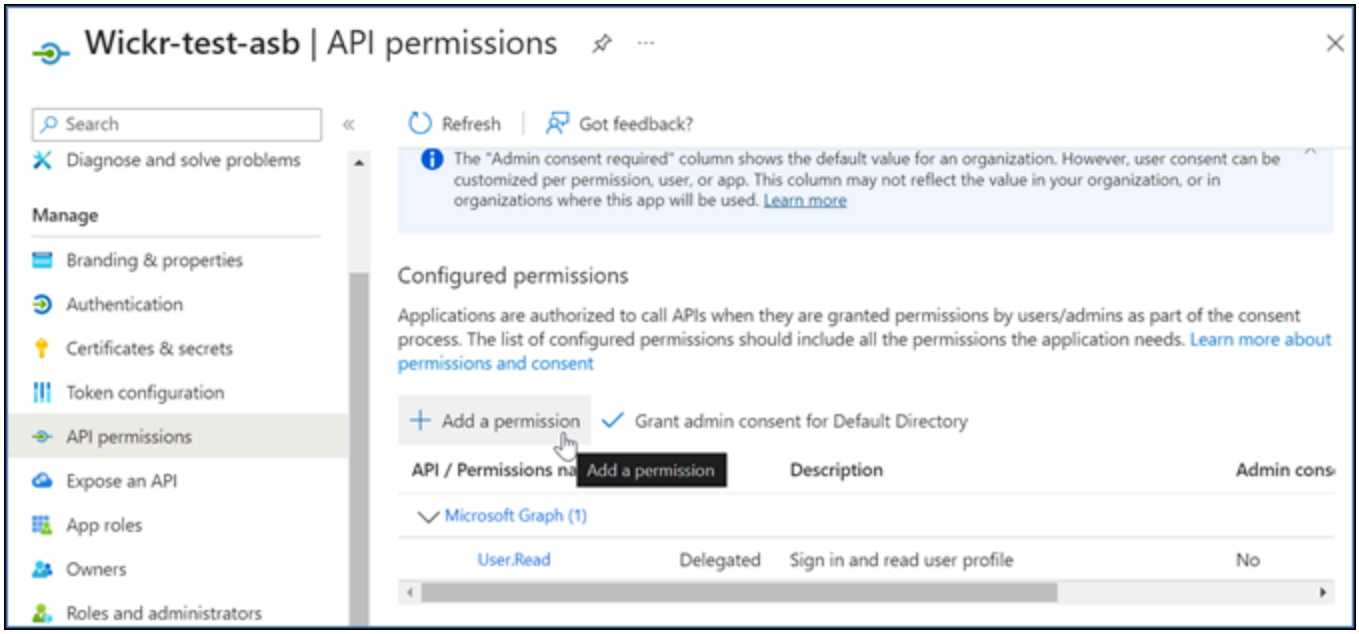
1. Di panel navigasi, pilih konfigurasi Token.
2. Pada halaman konfigurasi Token, pilih Tambahkan klaim opsional.
3. Di bawah Klaim opsional, pilih jenis Token sebagai ID.
4. Setelah memilih ID, di bawah Klaim, pilih email dan upn.
5. Pilih Tambahkan.



Langkah 5: Siapkan izin API

Selesaikan prosedur berikut untuk mengatur izin API di Microsoft Entra.

1. Di panel navigasi, pilih izin API.
2. Pada halaman izin API, pilih Tambahkan izin.

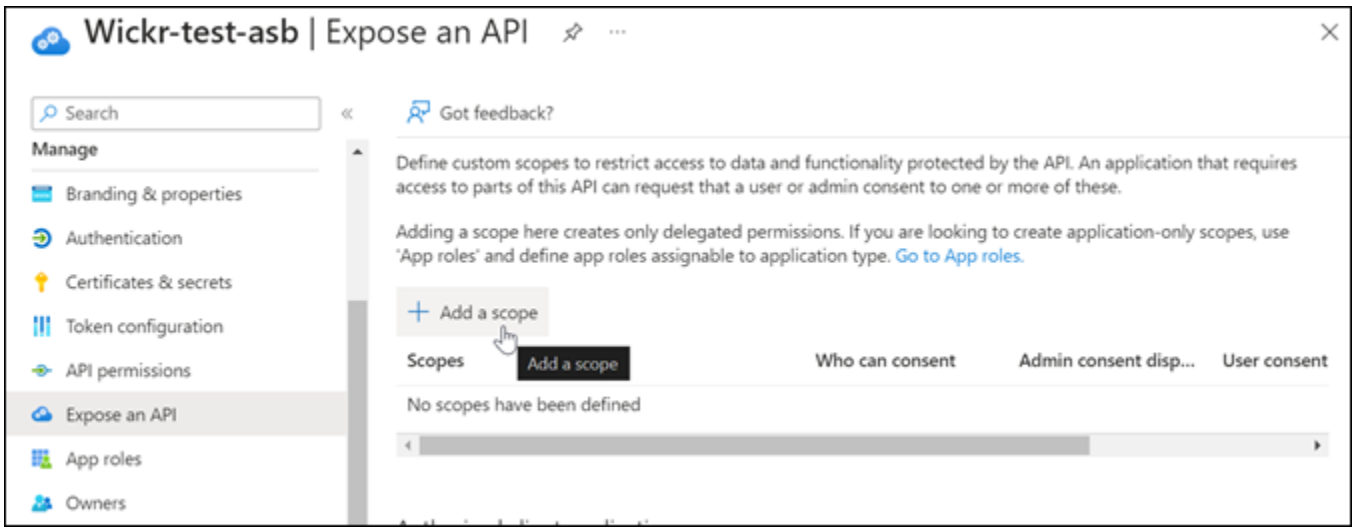


3. Pilih Microsoft Graph dan kemudian pilih Izin Delegasi.
4. Pilih kotak centang untuk email, offline_access, openid, profil.
5. Pilih Tambahkan izin.

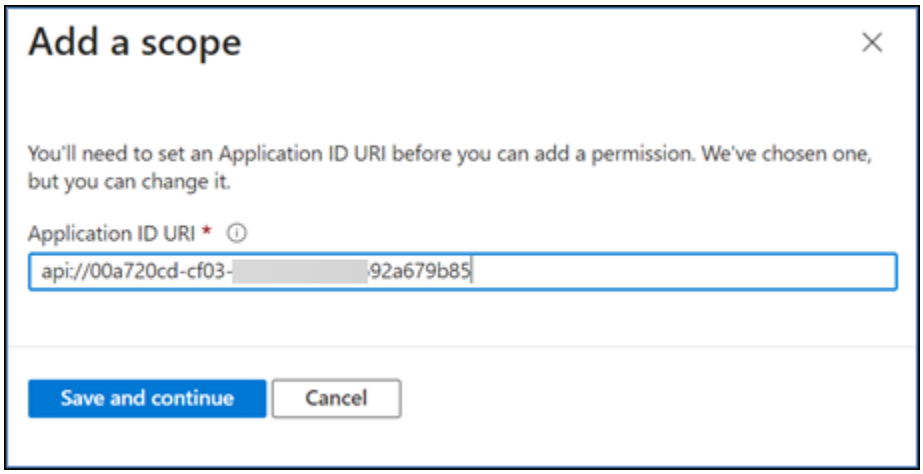
Langkah 6: Mengekspos API

Selesaikan prosedur berikut untuk mengekspos API untuk masing-masing dari 4 cakupan di Microsoft Entra.

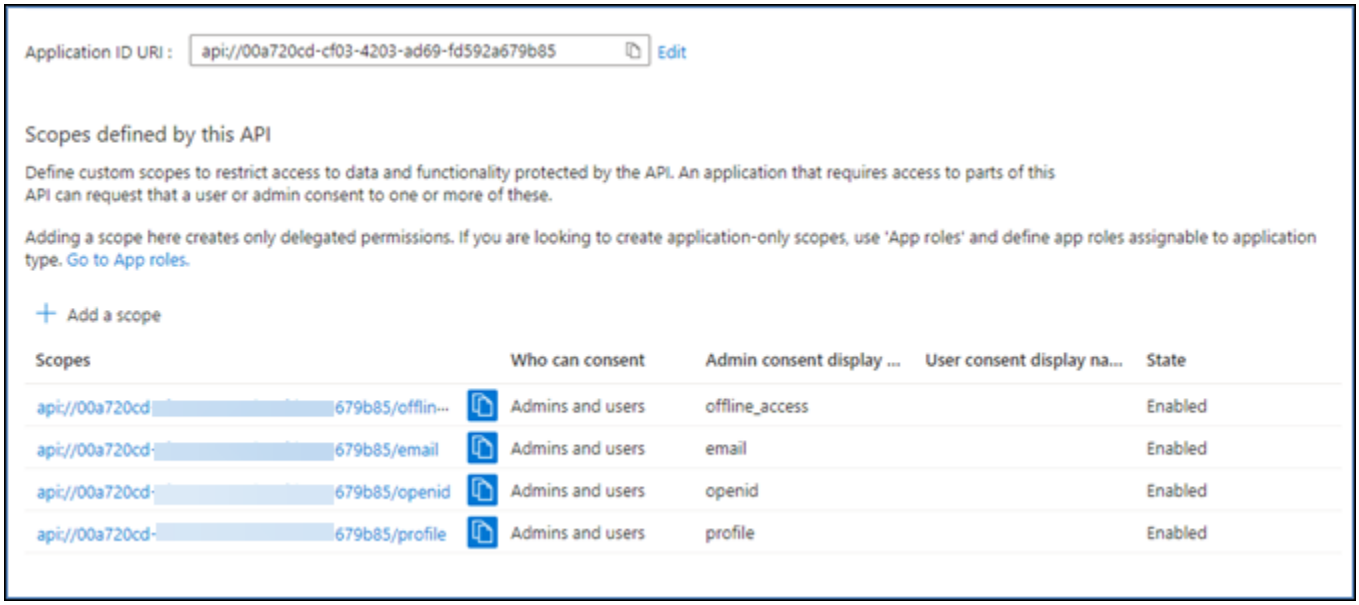
1. Di panel navigasi, pilih Expose an API.
2. Pada halaman Expose an API, pilih Add a scope.



URI ID Aplikasi harus diisi secara otomatis, dan ID yang mengikuti URI harus cocok dengan ID Aplikasi (dibuat di Register AWS Wickr sebagai aplikasi).



3. Jangan pilih Save and continue (Simpan dan lanjutkan).
4. Pilih tag Admin dan pengguna, lalu masukkan nama lingkup sebagai offline_access.
5. Pilih Status, lalu pilih Aktifkan.
6. Pilih Tambahkan ruang lingkup.
7. Ulangi langkah 1—6 dari bagian ini untuk menambahkan cakupan berikut: email, openid, dan profil.



8. Di bawah Aplikasi klien resmi, pilih Tambahkan aplikasi klien.
9. Pilih keempat cakupan yang dibuat pada langkah sebelumnya.
10. Masukkan atau verifikasi ID Aplikasi (klien).
11. Pilih Tambahkan aplikasi.

Langkah 7: Konfigurasi AWS Wickr SSO

Selesaikan prosedur konfigurasi berikut di konsol AWS Wickr.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Di panel navigasi, pilih Manajemen pengguna, lalu pilih Konfigurasi SSO.
4. Masukkan detail berikut:

   - Penerbit — Ini adalah titik akhir yang telah dimodifikasi sebelumnya (Misalnya). `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`
   - ID Klien - Ini adalah ID Aplikasi (klien) dari panel Ikhtisar.
   - Rahasia klien (opsional) - Ini adalah rahasia Klien dari panel Sertifikat & rahasia.
   - Cakupan — Ini adalah nama cakupan yang diekspos pada panel Expose an API. Masukkan email, profil, offline_access, dan openid.
   - Lingkup nama pengguna khusus (opsional) - Masukkan upn.

- ID Perusahaan — Ini bisa menjadi nilai teks unik termasuk karakter alfanumerik dan garis bawah. Frasa ini adalah apa yang akan dimasukkan pengguna Anda saat mendaftar di perangkat baru.

Bidang lainnya bersifat opsional.

5. Pilih Berikutnya.
6. Verifikasi detail di halaman Tinjau dan simpan, lalu pilih Simpan perubahan.

Konfigurasi SSO selesai. Untuk memverifikasi, Anda sekarang dapat menambahkan pengguna ke aplikasi di Microsoft Entra, dan login dengan pengguna menggunakan SSO dan ID Perusahaan.

Untuk informasi selengkapnya tentang cara mengundang dan menghubungkan pengguna, lihat Membuat dan mengundang pengguna.

Pemecahan masalah

Berikut ini adalah masalah umum yang mungkin Anda temui dan saran untuk menyelesaikannya.

- Tes SSO Connection gagal atau tidak responsif:
  - Pastikan Penerbit SSO dikonfigurasi seperti yang diharapkan.
  - Pastikan bidang yang diperlukan di SSO Configurated diatur seperti yang diharapkan.
- Tes koneksi berhasil, tetapi pengguna tidak dapat masuk:
  - Pastikan pengguna ditambahkan ke aplikasi Wickr yang Anda daftarkan di Microsoft Entra.
  - Pastikan pengguna menggunakan ID perusahaan yang benar, termasuk awalan. Misalnya UE1 - DemoNetwork W_DrQTVA.
  - Rahasia Klien mungkin tidak disetel dengan benar dalam Konfigurasi AWS Wickr SSO. Atur ulang dengan membuat rahasia Klien lain di Microsoft Entra dan atur rahasia Klien baru di Wickr SSO Configuration.

Masa tenggang untuk penyegaran token

Kadang-kadang, mungkin ada contoh di mana penyedia identitas mengalami pemadaman sementara atau diperpanjang, yang dapat menyebabkan pengguna Anda keluar secara tidak terduga karena token penyegaran yang gagal untuk sesi klien mereka. Untuk mencegah masalah ini, Anda dapat menetapkan masa tenggang yang memungkinkan pengguna Anda tetap masuk meskipun token penyegaran klien mereka gagal selama pemadaman tersebut.

Berikut adalah opsi yang tersedia untuk masa tenggang:

- Tidak ada masa tenggang (default): Pengguna akan keluar segera setelah kegagalan token refresh.
- Masa tenggang 30 menit: Pengguna dapat tetap masuk hingga 30 menit setelah kegagalan token refresh.
- Masa tenggang 60 menit: Pengguna dapat tetap masuk hingga 60 menit setelah kegagalan token refresh.

Tag jaringan untuk AWS Wickr

Anda dapat menerapkan tag ke jaringan Wickr. Anda kemudian dapat menggunakan tag tersebut untuk mencari dan memfilter jaringan Wickr Anda atau melacak biaya Anda AWS . Anda dapat mengonfigurasi tag jaringan di halaman beranda Jaringan Konsol Manajemen AWS untuk Wickr.

Tag adalah pasangan kunci-nilai yang diterapkan ke sumber daya untuk menyimpan metadata tentang sumber daya tersebut. Setiap tag adalah label yang terdiri dari kunci dan nilai. Untuk informasi selengkapnya tentang tag, lihat juga Apa itu tag? dan Menandai kasus penggunaan.

Topik

Kelola tag jaringan di AWS Wickr

Anda dapat mengelola tag jaringan untuk jaringan Wickr Anda.

Selesaikan prosedur berikut untuk mengelola tag jaringan untuk jaringan Wickr Anda.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Di halaman beranda Jaringan, di bagian Tag, pilih Kelola tag.
4. Pada halaman Kelola tag, Anda dapat menyelesaikan salah satu opsi berikut:

- Tambahkan tag baru - Masukkan tag baru dalam bentuk kunci dan pasangan nilai. Pilih Tambahkan tag baru untuk menambahkan beberapa pasangan nilai kunci. Tag peka huruf besar/kecil. Untuk informasi selengkapnya, lihat Tambahkan tag jaringan di AWS Wickr.
- Edit tag yang ada — Pilih kunci atau nilai teks untuk tag yang ada, lalu masukkan modifikasi ke dalam kotak teks. Untuk informasi selengkapnya, lihat Mengedit tag jaringan di AWS Wickr.
- Hapus tag yang ada — Pilih tombol Hapus yang tercantum di sebelah tag yang ingin Anda hapus. Untuk informasi selengkapnya, lihat Menghapus tag jaringan di AWS Wickr.

Tambahkan tag jaringan di AWS Wickr

Anda dapat menambahkan tag jaringan ke jaringan Wickr Anda.

Selesaikan prosedur berikut untuk menambahkan tag ke jaringan Wickr Anda. Untuk informasi selengkapnya tentang mengelola tag, lihatKelola tag jaringan di AWS Wickr.

1. Di halaman beranda Jaringan, di bagian Tag, pilih Tambahkan tag baru.
2. Pada halaman Kelola tag, pilih Tambahkan tag baru.
3. Di bidang Kunci dan Nilai kosong yang muncul, masukkan kunci dan nilai tag baru.
4. Pilih Simpan perubahan untuk menyimpan tag baru.

Mengedit tag jaringan di AWS Wickr

Anda dapat mengedit tag jaringan ke jaringan Wickr Anda.

Selesaikan prosedur berikut untuk mengedit tag yang terkait dengan jaringan Wickr Anda. Untuk informasi selengkapnya tentang mengelola tag, lihatKelola tag jaringan di AWS Wickr.

1. Pada halaman Kelola tag, edit nilai tag.

   > **Note**
   >
   > Anda tidak dapat mengedit kunci tag. Sebagai gantinya, hapus pasangan kunci dan nilai, dan tambahkan tag baru menggunakan kunci baru.

2. Pilih Simpan perubahan untuk menyimpan hasil edit Anda.

Menghapus tag jaringan di AWS Wickr

Anda dapat menghapus tag jaringan ke jaringan Wickr Anda.

Selesaikan prosedur berikut untuk menghapus tag dari jaringan Wickr Anda. Untuk informasi selengkapnya tentang mengelola tag, lihatKelola tag jaringan di AWS Wickr.

1. Pada halaman Kelola tag, pilih Hapus untuk tag yang ingin Anda hapus.
2. Pilih Simpan perubahan untuk menyimpan hasil edit Anda.

Baca tanda terima untuk AWS Wickr

Tanda terima baca untuk AWS Wickr adalah notifikasi yang dikirim ke pengirim untuk ditampilkan saat pesan mereka telah dibaca. Tanda terima ini tersedia dalam one-on-one percakapan. Tanda centang tunggal akan muncul untuk pesan terkirim, dan lingkaran padat dengan tanda centang akan muncul untuk pesan yang dibaca. Untuk melihat tanda terima baca pada pesan selama percakapan eksternal, kedua jaringan harus mengaktifkan tanda terima baca.

Administrator dapat mengaktifkan atau menonaktifkan tanda terima baca di panel administrator. Pengaturan ini akan diterapkan ke seluruh jaringan.

Selesaikan prosedur berikut untuk mengaktifkan atau menonaktifkan tanda terima baca.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Di panel navigasi, pilih Kebijakan jaringan.
4. Pada halaman Kebijakan jaringan, di bagian Pesan, pilih Edit.
5. Pilih kotak centang untuk Aktifkan atau Nonaktifkan tanda terima baca.
6. Pilih Simpan perubahan.

Kelola paket jaringan untuk AWS Wickr

Dalam Konsol Manajemen AWS for Wickr, Anda dapat mengelola rencana jaringan Anda berdasarkan kebutuhan bisnis Anda.

Untuk mengelola rencana jaringan Anda, selesaikan prosedur berikut.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Di halaman beranda Jaringan, di bagian Detail jaringan, pilih Edit.
4. Pada halaman Edit detail jaringan, pilih paket jaringan yang Anda inginkan. Anda dapat memodifikasi paket jaringan Anda saat ini dengan memilih salah satu dari berikut ini:

   - Standar — Untuk tim bisnis kecil dan besar yang membutuhkan kontrol administratif dan fleksibilitas.
   - Uji Coba Gratis Premium atau Premium — Untuk bisnis yang memerlukan batas fitur tertinggi, kontrol administratif terperinci, dan retensi data.

     Administrator memiliki opsi untuk memilih uji coba gratis premium, yang tersedia hingga 30 pengguna dan berlangsung selama tiga bulan. Untuk AWS WickrGov, opsi uji coba gratis premium memungkinkan hingga 50 pengguna dan juga bertahan selama tiga bulan. Penawaran ini terbuka untuk paket baru dan standar. Selama masa uji coba gratis premium, administrator dapat meningkatkan atau menurunkan versi ke paket Premium atau Standar

     > **Note**
     >
     > Untuk menghentikan penggunaan dan penagihan di jaringan Anda, hapus semua pengguna, termasuk pengguna yang ditangguhkan dari jaringan Anda.

Batasan uji coba gratis premium

Batasan berikut berlaku untuk uji coba gratis premium:

- Jika paket pernah terdaftar dalam uji coba gratis premium sebelumnya, itu tidak akan memenuhi syarat untuk uji coba lain.
- Hanya satu jaringan untuk setiap AWS akun yang dapat didaftarkan dalam uji coba gratis premium.
- Fitur pengguna tamu tidak tersedia selama uji coba gratis premium.
- Jika jaringan standar memiliki lebih dari 30 pengguna (lebih dari 50 pengguna untuk AWS WickrGov), tidak akan mungkin untuk meningkatkan ke uji coba gratis premium.

Retensi data untuk AWS Wickr

AWS Wickr Penyimpanan data dapat mempertahankan semua percakapan dalam jaringan. Ini termasuk percakapan pesan langsung dan percakapan di Grup atau Ruangan antara anggota dalam jaringan (internal) dan orang-orang dengan tim lain (eksternal) dengan siapa jaringan Anda digabungkan. Penyimpanan data hanya tersedia untuk pengguna paket AWS Wickr Premium dan pelanggan perusahaan yang memilih untuk retensi data. Untuk informasi selengkapnya tentang paket Premium, lihat Harga Wickr

Ketika administrator jaringan mengonfigurasi dan mengaktifkan penyimpanan data untuk jaringan mereka, semua pesan dan file yang dibagikan di jaringan mereka dipertahankan sesuai dengan kebijakan kepatuhan organisasi. Output file.txt ini dapat diakses oleh administrator jaringan di lokasi eksternal (misalnya: penyimpanan lokal, bucket Amazon S3, atau penyimpanan lainnya sesuai pilihan pengguna), dari mana mereka dapat dianalisis, dihapus, atau ditransfer.

> **Note**
>
> Wickr tidak pernah mengakses pesan dan file Anda. Oleh karena itu, Anda bertanggung jawab untuk mengonfigurasi sistem retensi data.

Topik

Lihat detail retensi data di AWS Wickr

Selesaikan prosedur berikut untuk melihat detail penyimpanan data untuk jaringan Wickr Anda. Anda juga dapat mengaktifkan atau menonaktifkan retensi data untuk jaringan Wickr Anda.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Di panel navigasi, pilih Kebijakan jaringan.

4. Halaman Kebijakan Jaringan menampilkan langkah-langkah untuk mengatur retensi data, dan opsi untuk mengaktifkan atau menonaktifkan fitur retensi data. Untuk informasi selengkapnya tentang mengonfigurasi retensi data, lihatKonfigurasikan retensi data untuk AWS Wickr.

> **Note**
>
> Ketika retensi data diaktifkan, pesan Retensi Data Dihidupkan akan terlihat oleh semua pengguna di jaringan Anda yang memberi tahu mereka tentang jaringan yang mendukung retensi.

Konfigurasikan retensi data untuk AWS Wickr

Untuk mengonfigurasi retensi data untuk jaringan AWS Wickr, Anda harus menerapkan image bot Docker penyimpanan data ke container di host, seperti komputer lokal atau instans di Amazon Elastic Compute Cloud (Amazon EC2). Setelah bot di-deploy, Anda dapat mengonfigurasinya untuk menyimpan data secara lokal atau di bucket Amazon Simple Storage Service (Amazon S3). Anda juga dapat mengonfigurasi bot retensi data untuk menggunakan AWS layanan lain seperti AWS Secrets Manager (Secrets Manager), Amazon CloudWatch (CloudWatch), Amazon Simple Notification Service (Amazon SNS), AWS Key Management Service dan ().AWS KMS Topik berikut menjelaskan cara mengkonfigurasi dan menjalankan bot retensi data untuk jaringan Wickr Anda.

Topik

Prasyarat untuk mengonfigurasi retensi data untuk AWS Wickr

Sebelum memulai, Anda harus mendapatkan nama bot retensi data (diberi label sebagai Nama Pengguna) dan kata sandi awal dari Konsol Manajemen AWS untuk Wickr. Anda harus menentukan kedua nilai ini saat pertama kali memulai bot retensi data. Anda juga harus mengaktifkan retensi data di konsol. Untuk informasi selengkapnya, lihat Lihat detail retensi data di AWS Wickr.

Kata sandi untuk bot retensi data di AWS Wickr

Pertama kali Anda memulai bot retensi data, Anda menentukan kata sandi awal menggunakan salah satu opsi berikut:

- Variabel `WICKRIO_BOT_PASSWORD` lingkungan. Variabel lingkungan bot retensi data diuraikan di Variabel lingkungan untuk mengonfigurasi bot retensi data di AWS Wickr bagian nanti dalam panduan ini.
- Nilai kata sandi di Secrets Manager diidentifikasi oleh variabel `AWS_SECRET_NAME` lingkungan. Nilai Secrets Manager untuk bot retensi data diuraikan di Nilai Secrets Manager untuk AWS Wickr bagian nanti dalam panduan ini.
- Masukkan kata sandi saat diminta oleh bot retensi data. Anda harus menjalankan bot retensi data dengan akses TTY interaktif menggunakan `-ti` opsi.

Kata sandi baru akan dihasilkan saat Anda mengonfigurasi bot retensi data untuk pertama kalinya. Jika Anda perlu menginstal ulang bot retensi data, Anda menggunakan kata sandi yang dihasilkan. Kata sandi awal tidak valid setelah instalasi awal bot retensi data.

Kata sandi yang baru dihasilkan akan ditampilkan seperti yang ditunjukkan pada contoh berikut.

> **Important**
>
> Simpan sandi di tempat yang aman. Jika Anda kehilangan kata sandi, Anda tidak akan dapat menginstal ulang bot retensi data. Jangan bagikan kata sandi ini. Ini memberikan kemampuan untuk memulai retensi data untuk jaringan Wickr Anda.

```
************************************************************
**** GENERATED PASSWORD
**** DO NOT LOSE THIS PASSWORD, YOU WILL NEED TO ENTER IT EVERY TIME
**** TO START THE BOT
```

```
"HuEXAMPLERAW4lGgEXAMPLEn"
****************************************************************
```

Opsi penyimpanan untuk jaringan AWS Wickr

Setelah retensi data diaktifkan dan bot retensi data dikonfigurasi untuk jaringan Wickr Anda, itu akan menangkap semua pesan dan file yang dikirim dalam jaringan Anda. Pesan disimpan dalam file yang terbatas pada ukuran atau batas waktu tertentu yang dapat dikonfigurasi menggunakan variabel lingkungan. Untuk informasi selengkapnya, lihat Variabel lingkungan untuk mengonfigurasi bot retensi data di AWS Wickr.

Anda dapat mengonfigurasi salah satu opsi berikut untuk menyimpan data ini:

- Simpan semua pesan dan file yang diambil secara lokal. Ini adalah pilihan default. Anda bertanggung jawab untuk memindahkan file lokal ke sistem lain untuk penyimpanan jangka panjang, dan memastikan disk host tidak kehabisan memori atau ruang.
- Simpan semua pesan dan file yang diambil dalam bucket Amazon S3. Bot retensi data akan menyimpan semua pesan dan file yang didekripsi ke bucket Amazon S3 yang Anda tentukan. Pesan dan file yang diambil dihapus dari mesin host setelah berhasil disimpan ke ember.
- Simpan semua pesan dan file yang diambil yang dienkripsi dalam bucket Amazon S3. Bot retensi data akan mengenkripsi ulang semua pesan dan file yang diambil menggunakan kunci yang Anda berikan dan menyimpannya ke bucket Amazon S3 yang Anda tentukan. Pesan dan file yang diambil dihapus dari mesin host setelah berhasil dienkripsi ulang dan disimpan ke ember. Anda akan memerlukan perangkat lunak untuk mendekripsi pesan dan file.

  Untuk informasi selengkapnya tentang membuat bucket Amazon S3 untuk digunakan dengan bot retensi data, lihat Membuat bucket di Panduan Pengguna Amazon S3

Variabel lingkungan untuk mengonfigurasi bot retensi data di AWS Wickr

Anda dapat menggunakan variabel lingkungan berikut untuk mengonfigurasi bot retensi data. Anda mengatur variabel lingkungan ini menggunakan `-e` opsi saat Anda menjalankan image bot Docker retensi data. Untuk informasi selengkapnya, lihat Mulai bot retensi data untuk jaringan Wickr Anda.

> **Note**
>
> Variabel lingkungan ini opsional kecuali ditentukan lain.

Gunakan variabel lingkungan berikut untuk menentukan kredensi bot retensi data:

- `WICKRIO_BOT_NAME`— Nama bot retensi data. Variabel ini diperlukan saat Anda menjalankan image bot Docker retensi data.
- `WICKRIO_BOT_PASSWORD`— Kata sandi awal untuk bot retensi data. Untuk informasi selengkapnya, lihat Prasyarat untuk mengonfigurasi retensi data untuk AWS Wickr. Variabel ini diperlukan jika Anda tidak berencana untuk memulai bot retensi data dengan prompt kata sandi atau Anda tidak berencana menggunakan Secrets Manager untuk menyimpan kredenal bot retensi data.

Gunakan variabel lingkungan berikut untuk mengonfigurasi kemampuan streaming retensi data default:

- `WICKRIO_COMP_MESGDEST`— Nama jalur ke direktori tempat pesan akan dialirkan. Nilai default-nya adalah `/tmp/<botname>/compliance/messages`.
- `WICKRIO_COMP_FILEDEST`— Nama jalur ke direktori tempat file akan dialirkan. Nilai default-nya adalah `/tmp/<botname>/compliance/attachments`.
- `WICKRIO_COMP_BASENAME`— Nama dasar untuk file pesan yang diterima. Nilai default-nya adalah `receivedMessages`.
- `WICKRIO_COMP_FILESIZE`— Ukuran file maksimum untuk file pesan yang diterima dalam kibibyte (KiB). File baru dimulai ketika ukuran maksimal tercapai. Nilai defaultnya adalah`1000000000`, seperti pada 1024 GiB.
- `WICKRIO_COMP_TIMEROTATE`— Jumlah waktu, dalam hitungan menit, di mana bot retensi data akan memasukkan pesan yang diterima ke dalam file pesan yang diterima. File baru dimulai ketika batas waktu tercapai. Anda hanya dapat menggunakan ukuran file atau waktu untuk membatasi ukuran file pesan yang diterima. Nilai defaultnya adalah`0`, seperti tanpa batas.

Gunakan variabel lingkungan berikut untuk menentukan default yang AWS Region akan digunakan.

- `AWS_DEFAULT_REGION`— Default AWS Region untuk digunakan untuk AWS layanan seperti Secrets Manager (tidak digunakan untuk Amazon S3 atau AWS KMS). `us-east-1`Wilayah digunakan secara default jika variabel lingkungan ini tidak didefinisikan.

Gunakan variabel lingkungan berikut untuk menentukan rahasia Secrets Manager yang akan digunakan saat Anda memilih untuk menggunakan Secrets Manager untuk menyimpan kredensi bot

retensi data dan informasi AWS layanan. Untuk informasi selengkapnya tentang nilai yang dapat Anda simpan di Secrets Manager lihatNilai Secrets Manager untuk AWS Wickr.

- `AWS_SECRET_NAME`— Nama rahasia Secrets Manager yang berisi kredensil dan informasi AWS layanan yang dibutuhkan oleh bot retensi data.
- `AWS_SECRET_REGION`— AWS Region AWS Rahasianya terletak di. Jika Anda menggunakan AWS rahasia dan nilai ini tidak ditentukan `AWS_DEFAULT_REGION` nilainya akan digunakan.

> **Note**
>
> Anda dapat menyimpan semua variabel lingkungan berikut sebagai nilai di Secrets Manager. Jika Anda memilih untuk menggunakan Secrets Manager, dan Anda menyimpan nilai-nilai ini di sana, maka Anda tidak perlu menentukannya sebagai variabel lingkungan saat Anda menjalankan image bot Docker retensi data. Anda hanya perlu menentukan variabel `AWS_SECRET_NAME` lingkungan yang dijelaskan sebelumnya dalam panduan ini. Untuk informasi selengkapnya, lihat Nilai Secrets Manager untuk AWS Wickr.

Gunakan variabel lingkungan berikut untuk menentukan bucket Amazon S3 saat Anda memilih untuk menyimpan pesan dan file ke bucket.

- `WICKRIO_S3_BUCKET_NAME`— Nama bucket Amazon S3 tempat pesan dan file akan disimpan.
- `WICKRIO_S3_REGION`— AWS Wilayah bucket Amazon S3 tempat pesan dan file akan disimpan.
- `WICKRIO_S3_FOLDER_NAME`— Nama folder opsional di bucket Amazon S3 tempat pesan dan file akan disimpan. Nama folder ini akan didahului dengan kunci untuk pesan dan file yang disimpan ke bucket Amazon S3.

Gunakan variabel lingkungan berikut untuk menentukan AWS KMS detail saat Anda memilih untuk menggunakan enkripsi sisi klien untuk mengenkripsi ulang file saat menyimpannya ke bucket Amazon S3.

- `WICKRIO_KMS_MSTRKEY_ARN`— Nama Sumber Daya Amazon (ARN) dari kunci AWS KMS master yang digunakan untuk mengenkripsi ulang file pesan dan file pada bot retensi data sebelum disimpan ke bucket Amazon S3.
- `WICKRIO_KMS_REGION`— AWS Wilayah tempat kunci AWS KMS utama berada.

Gunakan variabel lingkungan berikut untuk menentukan detail Amazon SNS saat Anda memilih untuk mengirim peristiwa penyimpanan data ke topik Amazon SNS. Peristiwa yang dikirim termasuk startup, shutdown, serta kondisi kesalahan.

- `WICKRIO_SNS_TOPIC_ARN`— ARN dari topik Amazon SNS yang ingin Anda kirimkan ke acara penyimpanan data.

Gunakan variabel lingkungan berikut untuk mengirim metrik retensi data ke CloudWatch. Jika ditentukan, metrik akan dihasilkan setiap 60 detik.

- `WICKRIO_METRICS_TYPE`— Tetapkan nilai variabel lingkungan ini `cloudwatch` untuk mengirim metrik ke CloudWatch.

Nilai Secrets Manager untuk AWS Wickr

Anda dapat menggunakan Secrets Manager untuk menyimpan kredensi bot retensi data dan informasi AWS layanan. Untuk informasi selengkapnya tentang membuat rahasia Secrets Manager, lihat Membuat AWS Secrets Manager rahasia di Panduan Pengguna Secrets Manager.

Rahasia Secrets Manager dapat memiliki nilai-nilai berikut:

- `password`— Kata sandi bot retensi data.
- `s3_bucket_name`— Nama bucket Amazon S3 tempat pesan dan file akan disimpan. Jika tidak diatur, streaming file default akan digunakan.
- `s3_region`— AWS Wilayah bucket Amazon S3 tempat pesan dan file akan disimpan.
- `s3_folder_name`— Nama folder opsional di bucket Amazon S3 tempat pesan dan file akan disimpan. Nama folder ini akan didahului dengan kunci untuk pesan dan file yang disimpan ke bucket Amazon S3.
- `kms_master_key_arn`— ARN dari kunci AWS KMS master digunakan untuk mengenkripsi ulang file pesan dan file pada bot retensi data sebelum disimpan ke bucket Amazon S3.
- `kms_region`— AWS Wilayah tempat kunci AWS KMS utama berada.
- `sns_topic_arn`— ARN dari topik Amazon SNS yang ingin Anda kirimkan ke acara penyimpanan data.

Kebijakan IAM untuk menggunakan penyimpanan data dengan layanan AWS

Jika Anda berencana untuk menggunakan AWS layanan lain dengan bot retensi data Wickr, Anda harus memastikan host memiliki peran dan kebijakan AWS Identity and Access Management (IAM) yang sesuai untuk mengaksesnya. Anda dapat mengonfigurasi bot retensi data untuk menggunakan Secrets Manager, Amazon S3, Amazon SNS CloudWatch, dan. AWS KMS Kebijakan IAM berikut memungkinkan akses ke tindakan spesifik untuk layanan ini.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "secretsmanager:GetSecretValue",
                "sns:Publish",
                "cloudwatch:PutMetricData",
                "kms:GenerateDataKey"
            ],
            "Resource": "*"
        }
    ]
}
```

Anda dapat membuat kebijakan IAM yang lebih ketat dengan mengidentifikasi objek tertentu untuk setiap layanan yang ingin Anda izinkan untuk diakses oleh container di host Anda. Hapus tindakan untuk AWS layanan yang tidak ingin Anda gunakan. Misalnya, jika Anda bermaksud hanya menggunakan bucket Amazon S3, gunakan kebijakan berikut, yang menghapus, `sns:Publish`kms:GenerateDataKey, `secretsmanager:GetSecretValue` `cloudwatch:PutMetricData` dan tindakan.

JSON

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

```
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "*"
        }
    ]
}
```

Jika Anda menggunakan instans Amazon Elastic Compute Cloud (Amazon EC2) untuk meng-host bot penyimpanan data Anda, buat peran IAM menggunakan kasus umum Amazon EC2 dan tetapkan kebijakan menggunakan definisi kebijakan dari atas.

Mulai bot retensi data untuk jaringan Wickr Anda

Sebelum Anda menjalankan bot retensi data, Anda harus menentukan bagaimana Anda ingin mengkonfigurasinya. Jika Anda berencana untuk menjalankan bot pada host yang:

- Tidak akan memiliki akses ke AWS layanan, maka pilihan Anda terbatas. Dalam hal ini Anda akan menggunakan opsi streaming pesan default. Anda harus memutuskan apakah Anda ingin membatasi ukuran file pesan yang diambil ke ukuran atau interval waktu tertentu. Untuk informasi selengkapnya, lihat Variabel lingkungan untuk mengonfigurasi bot retensi data di AWS Wickr.
- Akan memiliki akses ke AWS layanan, maka Anda harus membuat rahasia Secrets Manager untuk menyimpan kredensi bot, dan detail konfigurasi AWS layanan. Setelah AWS layanan dikonfigurasi, Anda dapat melanjutkan untuk memulai image bot penyimpanan data Docker. Untuk informasi selengkapnya tentang detail yang dapat Anda simpan di rahasia Secrets Manager, lihat Nilai Secrets Manager untuk AWS Wickr

Bagian berikut menunjukkan contoh perintah untuk menjalankan image bot penyimpanan data Docker. Di setiap perintah contoh, ganti nilai contoh berikut dengan milik Anda sendiri:

- *compliance_1234567890_bot*dengan nama bot retensi data Anda.
- *password*dengan kata sandi untuk bot retensi data Anda.
- *wickr/data/retention/bot*dengan nama rahasia Secrets Manager Anda untuk digunakan dengan bot retensi data Anda.
- *bucket-name*dengan nama bucket Amazon S3 tempat pesan dan file akan disimpan.

- *folder-name*dengan nama folder di bucket Amazon S3 tempat pesan dan file akan disimpan.
- *us-east-1*dengan AWS Wilayah sumber daya yang Anda tentukan. Misalnya, Wilayah kunci AWS KMS master atau Wilayah bucket Amazon S3.
- *arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-a617-abababababab*dengan Nama Sumber Daya Amazon (ARN) dari kunci AWS KMS master Anda untuk digunakan untuk mengenkripsi ulang file dan file pesan.

Mulai bot dengan variabel lingkungan kata sandi (tidak ada AWS layanan)

Perintah Docker berikut memulai bot retensi data. Kata sandi ditentukan menggunakan variabel `WICKRIO_BOT_PASSWORD` lingkungan. Bot mulai menggunakan streaming file default, dan menggunakan nilai default yang ditentukan di Variabel lingkungan untuk mengonfigurasi bot retensi data di AWS Wickr bagian panduan ini.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
wickr/bot-compliance-cloud:latest
```

Mulai bot dengan prompt kata sandi (tidak ada AWS layanan)

Perintah Docker berikut memulai bot retensi data. Kata sandi dimasukkan saat diminta oleh bot retensi data. Ini akan mulai menggunakan streaming file default menggunakan nilai default yang ditentukan di Variabel lingkungan untuk mengonfigurasi bot retensi data di AWS Wickr bagian panduan ini.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
wickr/bot-compliance-cloud:latest

docker attach compliance_1234567890_bot
.
.
.
Enter the password:************
Re-enter the password:************
```

Jalankan bot menggunakan `-ti` opsi untuk menerima prompt kata sandi. Anda juga harus menjalankan `docker attach` *<container ID or container name>* perintah segera setelah memulai image docker sehingga Anda mendapatkan prompt kata sandi. Anda harus menjalankan kedua perintah ini dalam skrip. Jika Anda melampirkan ke gambar docker dan tidak melihat prompt, tekan Enter dan Anda akan melihat prompt.

Mulai bot dengan rotasi file pesan 15 menit (tidak ada AWS layanan)

Perintah Docker berikut memulai bot retensi data menggunakan variabel lingkungan. Ini juga mengonfigurasinya untuk memutar file pesan yang diterima menjadi 15 menit.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
-e WICKRIO_COMP_TIMEROTATE=15 \
wickr/bot-compliance-cloud:latest
```

Mulai bot dan tentukan kata sandi awal dengan Secrets Manager

Anda dapat menggunakan Secrets Manager untuk mengidentifikasi kata sandi bot retensi data. Saat Anda memulai bot retensi data, Anda perlu mengatur variabel lingkungan yang menentukan Secrets Manager tempat informasi ini disimpan.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e AWS_SECRET_NAME='wickrpro/alpha/new-3-bot' \
wickr/bot-compliance-cloud:latest
```

`wickrpro/compliance/compliance_1234567890_bot`Rahasia memiliki nilai rahasia berikut di dalamnya, ditampilkan sebagai plaintext.

```
{
    "password":"password"
}
```

Mulai bot dan konfigurasikan Amazon S3 dengan Secrets Manager

Anda dapat menggunakan Secrets Manager untuk meng-host kredensi, dan informasi bucket Amazon S3. Saat Anda memulai bot retensi data, Anda perlu mengatur variabel lingkungan yang menentukan Secrets Manager tempat informasi ini disimpan.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
 -e AWS_SECRET_NAME='wickrpro/alpha/compliance_1234567890_bot' \
wickr/bot-compliance-cloud:latest
```

`wickrpro/compliance/compliance_1234567890_bot`Rahasia memiliki nilai rahasia berikut di dalamnya, ditampilkan sebagai plaintext.

```
{
    "password":"password",
    "s3_bucket_name":"bucket-name",
    "s3_region":"us-east-1",
    "s3_folder_name":"folder-name"
}
```

Pesan dan file yang diterima oleh bot akan dimasukkan ke dalam `bot-compliance` ember di folder bernama`network1234567890`.

Mulai bot dan konfigurasikan Amazon S3 dan AWS KMS dengan Secrets Manager

Anda dapat menggunakan Secrets Manager untuk meng-host kredensi, bucket Amazon S3, AWS KMS dan informasi kunci master. Saat Anda memulai bot retensi data, Anda perlu mengatur variabel lingkungan yang menentukan Secrets Manager tempat informasi ini disimpan.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
 -e AWS_SECRET_NAME='wickrpro/alpha/compliance_1234567890_bot' \
wickr/bot-compliance-cloud:latest
```

`wickrpro/compliance/compliance_1234567890_bot`Rahasia memiliki nilai rahasia berikut di dalamnya, ditampilkan sebagai plaintext.

```
{
    "password":"password",
    "s3_bucket_name":"bucket-name",
    "s3_region":"us-east-1",
    "s3_folder_name":"folder-name",
    "kms_master_key_arn":"arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-a617-abababababab",
    "kms_region":"us-east-1"
}
```

Pesan dan file yang diterima oleh bot akan dienkripsi menggunakan kunci KMS yang diidentifikasi oleh nilai ARN, kemudian dimasukkan ke dalam ember “kepatuhan bot” di folder bernama “network1234567890”. Pastikan Anda memiliki pengaturan kebijakan IAM yang sesuai.

Mulai bot dan konfigurasikan Amazon S3 menggunakan variabel lingkungan

Jika Anda tidak ingin menggunakan Secrets Manager untuk meng-host kredensi bot retensi data, Anda dapat memulai image bot Docker retensi data dengan variabel lingkungan berikut. Anda harus mengidentifikasi nama bot retensi data menggunakan variabel `WICKRIO_BOT_NAME` lingkungan.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
-e WICKRIO_S3_BUCKET_NAME='bot-compliance' \
-e WICKRIO_S3_FOLDER_NAME='network1234567890' \
-e WICKRIO_S3_REGION='us-east-1' \
wickr/bot-compliance-cloud:latest
```

Anda dapat menggunakan nilai lingkungan untuk mengidentifikasi kredensional bot retensi data, informasi tentang bucket Amazon S3, dan informasi konfigurasi untuk streaming file default.

Hentikan bot retensi data untuk jaringan Wickr Anda

Perangkat lunak yang berjalan pada bot retensi data akan menangkap `SIGTERM` sinyal dan mematikan dengan anggun. Gunakan `docker stop` *<container ID or container name>* perintah, seperti yang ditunjukkan pada contoh berikut, untuk mengeluarkan `SIGTERM` perintah ke image bot penyimpanan data Docker.

```
docker stop compliance_1234567890_bot
```

Dapatkan log retensi data untuk jaringan Wickr Anda

Perangkat lunak yang berjalan pada gambar Docker bot retensi data akan menghasilkan file log di `/tmp/<botname>/logs` direktori. Mereka akan memutar hingga maksimal 5 file. Anda bisa mendapatkan log dengan menjalankan perintah berikut.

```
docker logs <botname>
```

Contoh:

```
docker logs compliance_1234567890_bot
```

Metrik dan peristiwa retensi data untuk jaringan Wickr Anda

Berikut ini adalah metrik Amazon CloudWatch (CloudWatch) dan peristiwa Simple Notification Service Amazon (Amazon SNS) yang saat ini didukung oleh versi 5.116 dari bot retensi data AWS Wickr.

Topik

- CloudWatch metrik untuk jaringan Wickr Anda
- Acara Amazon SNS untuk jaringan Wickr Anda

CloudWatch metrik untuk jaringan Wickr Anda

Metrik dihasilkan oleh bot dalam interval 1 menit dan dikirimkan ke CloudWatch layanan yang terkait dengan akun tempat image bot Docker penyimpanan data berjalan.

Berikut ini adalah metrik yang ada yang didukung oleh bot retensi data.

Metrik	Deskripsi
Pesan_Rx	Pesan diterima.
Pesan_Rx_Gagal	Kegagalan untuk memproses pesan yang diterima.
Messages_Saved	Pesan disimpan ke file pesan yang diterima.

Metrik	Deskripsi
Messages_Saved_Failed	Kegagalan untuk menyimpan pesan ke file pesan yang diterima.
Files_Saved	File yang diterima.
Files_Saved_Bytes	Jumlah byte untuk file yang diterima.
Files_Saved_Failed	Kegagalan untuk menyimpan file.
Kredensial Masuk	Login (biasanya ini akan menjadi 1 untuk setiap interval).
Login_Failures	Kegagalan untuk login (biasanya ini akan menjadi 1 untuk setiap interval).
S3_Post_Errors	Kesalahan saat memposting file pesan dan file ke bucket Amazon S3.
Watchdog_Failures	Kegagalan pengawas.
Watchdog_Warnings	Peringatan Watchdog.

Metrik dihasilkan untuk dikonsumsi oleh CloudWatch. Namespace yang digunakan untuk bot adalah. `WickrIO` Setiap metrik memiliki berbagai dimensi. Berikut ini adalah daftar dimensi yang diposting dengan metrik di atas.

Dimensi	Nilai
Id	Nama pengguna bot.
Perangkat	Deskripsi perangkat atau contoh bot tertentu. Berguna jika Anda menjalankan beberapa perangkat bot atau instance.
Produk	Produk untuk bot. Bisa `WickrPro_` atau `WickrEnterprise_` dengan`Alpha`,`Beta`, atau `Production` ditambahkan.

Dimensi	Nilai
BotType	Jenis bot. Dilabeli sebagai Kepatuhan untuk bot kepatuhan.
Jaringan	ID dari jaringan terkait.

Acara Amazon SNS untuk jaringan Wickr Anda

Peristiwa berikut diposting ke topik Amazon SNS yang ditentukan oleh nilai Amazon Resource Name (ARN) yang diidentifikasi menggunakan variabel `WICKRIO_SNS_TOPIC_ARN` lingkungan atau nilai rahasia Secrets Manager`sns_topic_arn`. Untuk informasi selengkapnya, lihat Variabel lingkungan untuk mengonfigurasi bot retensi data di AWS Wickr dan Nilai Secrets Manager untuk AWS Wickr.

Peristiwa yang dihasilkan oleh bot retensi data dikirim sebagai string JSON. Nilai-nilai berikut disertakan dalam peristiwa pada versi 5.116 dari bot retensi data.

Nama	Nilai
ComplianceBot	Nama pengguna bot retensi data.
DataTime	Tanggal dan waktu ketika peristiwa itu terjadi.
pesawat	Deskripsi perangkat atau instance bot tertentu. Berguna jika Anda menjalankan beberapa instance bot.
DockerImage	Gambar Docker yang terkait dengan bot.
DockerTag	Tag atau versi gambar Docker.
pesan	Pesan acara. Untuk informasi lebih lanjut, lihat Peristiwa kritis dan Peristiwa normal.
notificationType	Nilai ini akan menjadi`Bot Event`.
kepelikan	Tingkat keparahan acara. Bisa `normal` atau`critical`.

Anda harus berlangganan topik Amazon SNS sehingga Anda dapat menerima acara. Jika Anda berlangganan menggunakan alamat email, email akan dikirimkan kepada Anda yang berisi informasi yang mirip dengan contoh berikut.

```
{
"complianceBot": "compliance_1234567890_bot",
 "dateTime": "2022-10-12T13:05:39",
 "device": "Desktop 1234567890ab",
 "dockerImage": "wickr/bot-compliance-cloud",
 "dockerTag": "5.116.13.01",
 "message": "Logged in",
 "notificationType": "Bot Event",
 "severity": "normal"
}
```

Peristiwa kritis

Peristiwa ini akan menyebabkan bot berhenti atau memulai ulang. Jumlah restart terbatas untuk menghindari menyebabkan masalah lain.

Kegagalan login

Berikut ini adalah kemungkinan peristiwa yang dapat dihasilkan ketika bot gagal masuk. Setiap pesan akan menunjukkan alasan kegagalan login.

Tipe peristiwa	Pesan peristiwa
failedlogin	Kredensi buruk. Periksa kata sandinya.
failedlogin	Pengguna tidak ditemukan.
failedlogin	Akun atau perangkat ditangguhkan.
penyediaan	Pengguna keluar dari perintah.
penyediaan	Kata sandi yang buruk untuk `config.wickr` file.
penyediaan	Tidak dapat membaca `config.wickr` file.
failedlogin	Semua login gagal.

Tipe peristiwa	Pesan peristiwa
failedlogin	Pengguna baru tetapi database sudah ada.

Peristiwa yang lebih kritis

Tipe peristiwa	Pesan peristiwa
Akun yang Ditangguhkan	Wickr IOClient Main:: slotAdminUser Tangguhkan: kode (% 1): alasan:% 2”
BotDevice Ditangguhkan	Perangkat ditangguhkan!
WatchDog	SwitchBoard Sistem mati selama lebih dari < *N* > menit
Kegagalan S3	Gagal meletakkan file < *file-name* ≫ di bucket S3. Kesalahan: < *AWS-error* >
Kunci Fallback	SERVER SUBMIITED FALLBACK KEY: Bukan kunci fallback aktif klien yang diakui. Silakan kirimkan log ke rekayasa desktop.

Peristiwa normal

Berikut ini adalah peristiwa yang memperingatkan Anda tentang kejadian operasi normal. Terlalu banyak kejadian dari jenis peristiwa ini dalam jangka waktu tertentu dapat memprihatinkan.

Perangkat ditambahkan ke akun

Acara ini dihasilkan ketika perangkat baru ditambahkan ke akun bot retensi data. Dalam beberapa keadaan, ini bisa menjadi indikasi penting bahwa seseorang telah membuat instance bot retensi data. Berikut ini adalah pesan untuk acara ini.

```
A device has been added to this account!
```

Bot masuk

Peristiwa ini dihasilkan ketika bot telah berhasil masuk. Berikut ini adalah pesan untuk acara ini.

```
Logged in
```

Mematikan

Acara ini dihasilkan saat bot dimatikan. Jika pengguna tidak secara eksplisit memulai ini, itu bisa menjadi indikasi masalah. Berikut ini adalah pesan untuk acara ini.

```
Shutting down
```

Pembaruan tersedia

Peristiwa ini dihasilkan ketika bot retensi data dimulai dan mengidentifikasi bahwa ada versi yang lebih baru dari gambar Docker terkait yang tersedia. Acara ini dihasilkan saat bot dimulai, dan setiap hari. Acara ini mencakup bidang `versions` array yang mengidentifikasi versi baru yang tersedia. Berikut ini adalah contoh seperti apa acara ini.

```
{
  "complianceBot": "compliance_1234567890_bot",
  "dateTime": "2022-10-12T13:05:55",
  "device": "Desktop 1234567890ab",
  "dockerImage": "wickr/bot-compliance-cloud",
  "dockerTag": "5.116.13.01",
  "message": "There are updates available",
  "notificationType": "Bot Event",
  "severity": "normal",
  "versions": [
    "5.116.10.01"
  ]
}
```

Apa itu ATAK?

Android Team Awareness Kit (ATAK) —atau Android Tactical Assault Kit (juga ATAK) untuk penggunaan militer—adalah infrastruktur geospasial ponsel pintar dan aplikasi kesadaran situasional yang memungkinkan kolaborasi aman atas geografi. Meskipun awalnya dirancang untuk digunakan di zona pertempuran, ATAK telah disesuaikan agar sesuai dengan misi lembaga lokal, negara bagian, dan federal.

Topik

Aktifkan ATAK di Dasbor Jaringan Wickr

AWS Wickr mendukung banyak agensi yang menggunakan Android Tactical Assault Kit (ATAK). Namun, sampai sekarang, operator ATAK yang menggunakan Wickr harus meninggalkan aplikasi untuk melakukannya. Untuk membantu mengurangi gangguan dan risiko operasional, Wickr telah mengembangkan plugin yang meningkatkan ATAK dengan fitur komunikasi yang aman. Dengan plugin Wickr untuk ATAK, pengguna dapat mengirim pesan, berkolaborasi, dan mentransfer file di Wickr dalam aplikasi ATAK. Ini menghilangkan gangguan, dan kompleksitas konfigurasi dengan fitur obrolan ATAK.

Aktifkan ATAK di Dasbor Jaringan Wickr

Selesaikan prosedur berikut untuk mengaktifkan ATAK di Dasbor Jaringan Wickr.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Pada panel navigasi, pilih Grup keamanan.
4. Pada halaman Grup keamanan, pilih grup keamanan yang diinginkan yang ingin Anda aktifkan ATAK.
5. Pada tab Integrasi, di bagian plugin ATAK, pilih Edit.
6. Pada halaman plugin Edit ATAK, pilih kotak centang Aktifkan plugin ATAK.
7. Pilih Tambah paket baru
8. Masukkan nama paket di kotak teks Paket. Anda dapat memasukkan salah satu nilai berikut tergantung pada versi ATAK yang akan dipasang dan digunakan pengguna Anda:

- `com.atakmap.app.civ`— Masukkan nilai ini ke dalam kotak teks Paket jika pengguna akhir Wickr Anda akan menginstal dan menggunakan versi sipil aplikasi ATAK di perangkat Android mereka.
- `com.atakmap.app.mil`— Masukkan nilai ini ke dalam kotak teks Paket jika pengguna akhir Wickr Anda akan menginstal dan menggunakan versi militer aplikasi ATAK di perangkat Android mereka.

9. Pilih Simpan.

   ATAK sekarang diaktifkan untuk Jaringan Wickr yang dipilih, dan Grup Keamanan yang dipilih. Anda harus meminta pengguna Android di grup keamanan tempat Anda mengaktifkan fungsionalitas ATAK untuk menginstal plugin Wickr untuk ATAK. Untuk informasi selengkapnya, lihat Menginstal dan memasangkan plugin Wickr ATAK.

Informasi tambahan tentang ATAK

Untuk informasi selengkapnya tentang plugin Wickr untuk ATAK, lihat berikut ini:

- Ikhtisar Plugin Wickr ATAK
- Informasi Plugin Wickr ATAK Tambahan

Instal dan pasangkan plugin Wickr untuk ATAK

Android Team Awareness Kit (ATAK) adalah solusi Android yang digunakan oleh militer AS, negara bagian, dan lembaga pemerintah yang memerlukan kemampuan kesadaran situasional untuk perencanaan misi, pelaksanaan, dan respons insiden. ATAK memiliki arsitektur plugin yang memungkinkan pengembang untuk menambahkan fungsionalitas. Ini memungkinkan pengguna untuk menavigasi menggunakan GPS dan data peta geospasial yang dilapisi dengan kesadaran situasional waktu nyata dari peristiwa yang sedang berlangsung. Dalam dokumen ini, kami menunjukkan kepada Anda cara menginstal plugin Wickr untuk ATAK pada perangkat Android dan memasangkannya dengan klien Wickr. Ini memungkinkan Anda untuk mengirim pesan dan berkolaborasi di Wickr tanpa keluar dari aplikasi ATAK.

Instal plugin Wickr untuk ATAK

Selesaikan prosedur berikut untuk menginstal plugin Wickr untuk ATAK di perangkat Android.

1. Buka Google Play store, dan instal plugin Wickr untuk ATAK.
2. Buka aplikasi ATAK di perangkat Android Anda.
3. Di aplikasi ATAK, pilih ikon menu () di kanan atas layar, lalu pilih Plugin.
4. Pilih Impor.
5. Pada pop-up Pilih Jenis Impor, pilih SD Lokal dan arahkan ke tempat Anda menyimpan plugin Wickr untuk file ATAK .apk.
6. Pilih file plugin dan ikuti petunjuk untuk menginstalnya.

> **Note**
>
> Jika Anda diminta untuk mengirim file plugin untuk pemindaian, pilih No.

7. Aplikasi ATAK akan menanyakan apakah Anda ingin memuat plugin. Pilih OK.

Plugin Wickr untuk ATAK sekarang diinstal. Lanjutkan ke bagian Pasangkan ATAK berikut dengan Wickr untuk menyelesaikan proses.

Pasangkan ATAK dengan Wickr

Selesaikan prosedur berikut untuk memasangkan aplikasi ATAK dengan Wickr setelah Anda berhasil menginstal plugin Wickr untuk ATAK.

1. Di aplikasi ATAK, pilih ikon menu () di kanan atas layar, lalu pilih Plugin Wickr.
2. Pilih Pair Wickr.

   Prompt pemberitahuan akan muncul meminta Anda untuk meninjau izin untuk plugin Wickr untuk ATAK. Jika prompt notifikasi tidak muncul, buka klien Wickr dan buka Pengaturan, lalu Aplikasi Terhubung. Anda akan melihat plugin di bawah bagian Pending layar.
3. Pilih Setujui untuk dipasangkan.
4. Pilih tombol Open Wickr ATAK Plugin untuk kembali ke aplikasi ATAK.

Anda sekarang telah berhasil memasangkan plugin ATAK dan Wickr, dan dapat menggunakan plugin untuk mengirim pesan dan berkolaborasi menggunakan Wickr tanpa keluar dari aplikasi ATAK.

Lepaskan Plugin Wickr untuk ATAK

Anda dapat memutuskan pasangan plugin Wickr untuk ATAK.

Selesaikan prosedur berikut untuk memutuskan pasangan plugin ATAK dengan Wickr.

1. Di aplikasi asli, pilih Pengaturan, lalu pilih Aplikasi Terhubung.
2. Pada layar Aplikasi Terhubung, pilih Plugin Wickr ATAK.
3. Pada Plugin Wickr ATAK layar, pilih Hapus di bagian bawah layar.

   Anda sekarang telah berhasil memutuskan pasangan plugin Wickr untuk ATAK.

Panggil dan terima panggilan di ATAK

Anda dapat menghubungi dan menerima panggilan di plugin Wickr untuk ATAK.

Selesaikan prosedur berikut untuk menghubungi dan menerima panggilan.

1. Buka jendela obrolan.
2. Dalam tampilan Peta, pilih ikon untuk pengguna yang ingin Anda panggil.
3. Pilih ikon telepon di kanan atas layar.
4. Setelah terhubung, Anda dapat kembali ke tampilan plugin ATAK dan menerima panggilan.

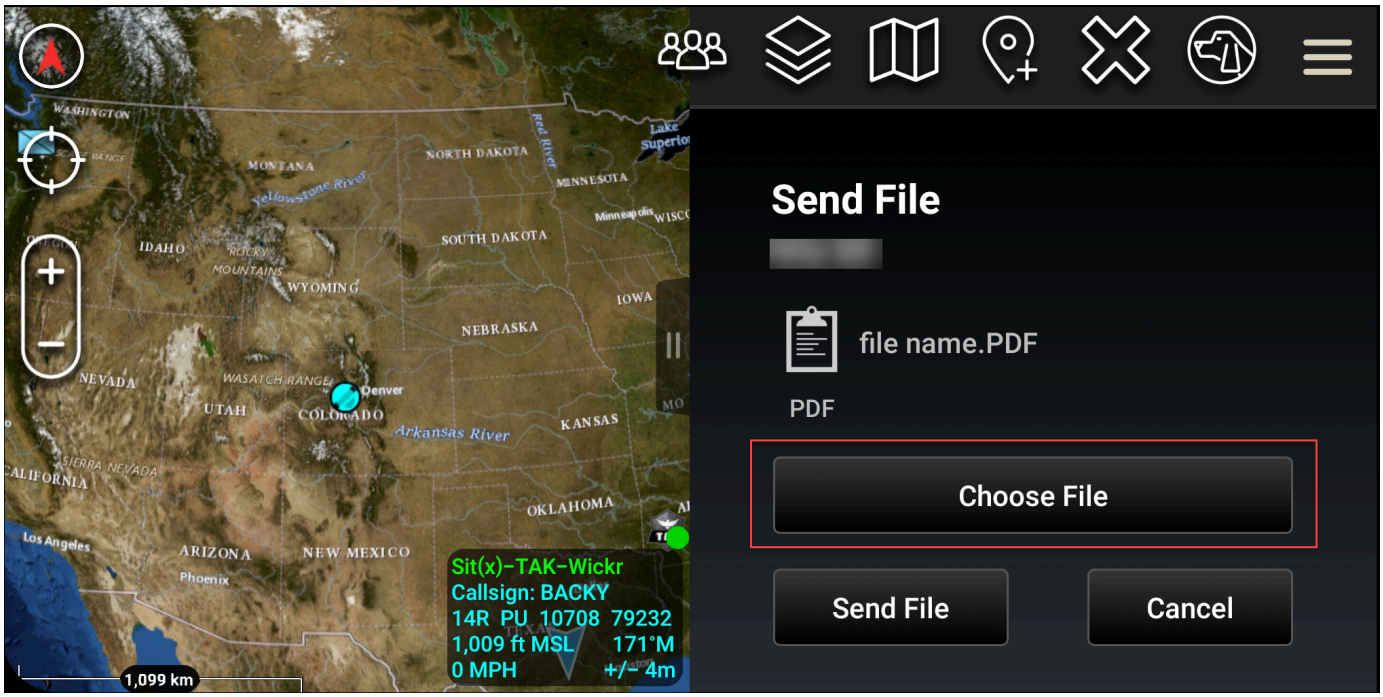
Kirim file di ATAK

Anda dapat mengirim file di plugin Wickr untuk ATAK.

Selesaikan prosedur berikut untuk mengirim file.

1. Buka jendela obrolan.
2. Dalam tampilan Peta, cari pengguna yang ingin Anda kirimi file.
3. Ketika Anda menemukan pengguna yang ingin Anda kirim file, pilih nama mereka.

4. Pada layar Kirim File, pilih Pilih File, lalu arahkan ke file yang ingin Anda kirim.



5. Di jendela browser, pilih file yang diinginkan.
6. Pada layar Kirim File, pilih Kirim File.

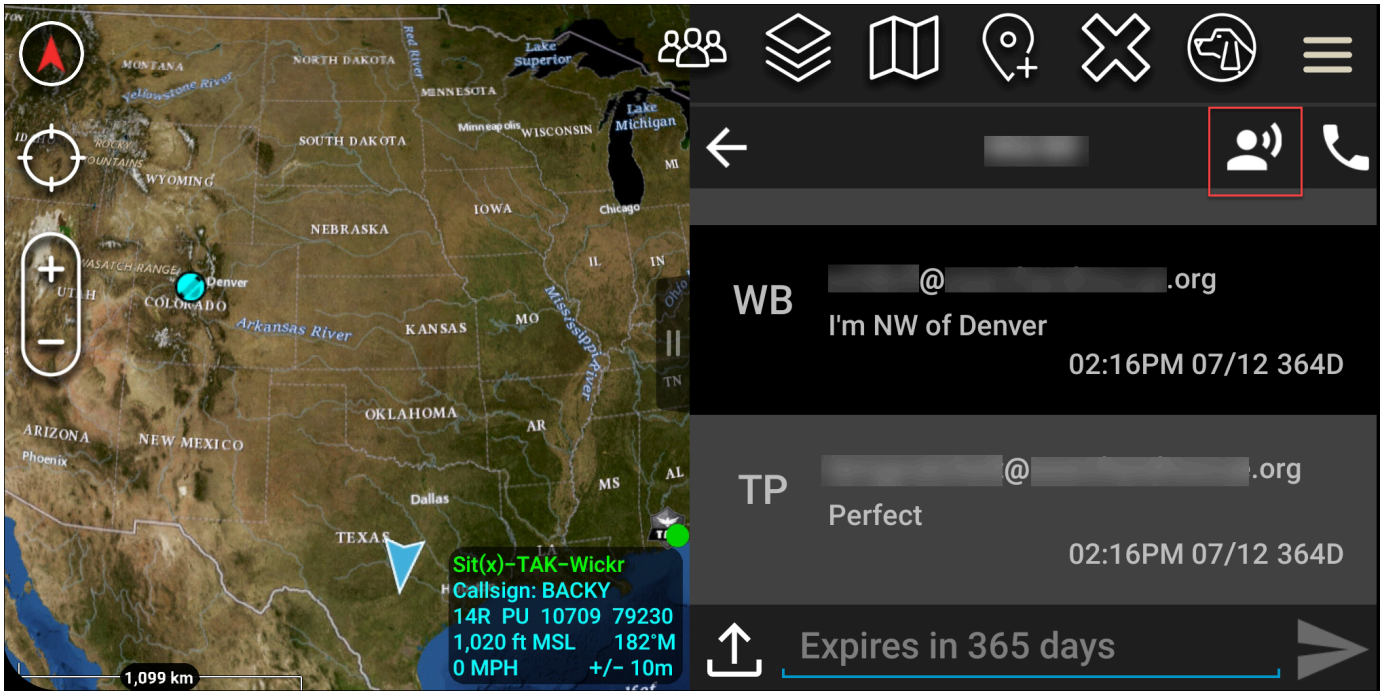
   Ikon unduhan ditampilkan, yang menunjukkan file yang Anda pilih sedang diunduh.

Mengirim pesan suara aman (Push-to-talk) di ATAK

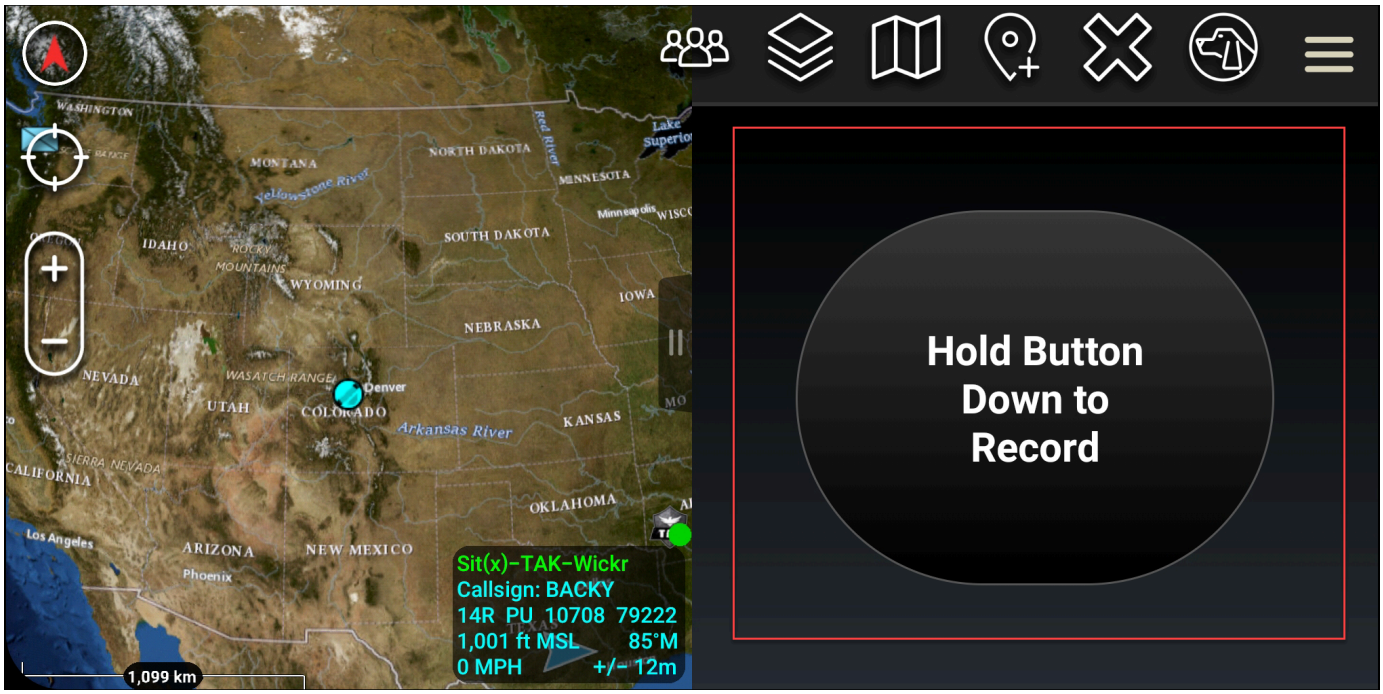
Anda dapat mengirim pesan suara aman (Push-to-talk) di plugin Wickr untuk ATAK.

Selesaikan prosedur berikut untuk mengirim pesan suara yang aman.

1. Buka jendela obrolan.
2. Pilih Push-to-Talk ikon di bagian atas layar, ditunjukkan oleh ikon seseorang yang berbicara.



3. Pilih dan tahan Tombol Tahan Turun untuk Merekam tombol.



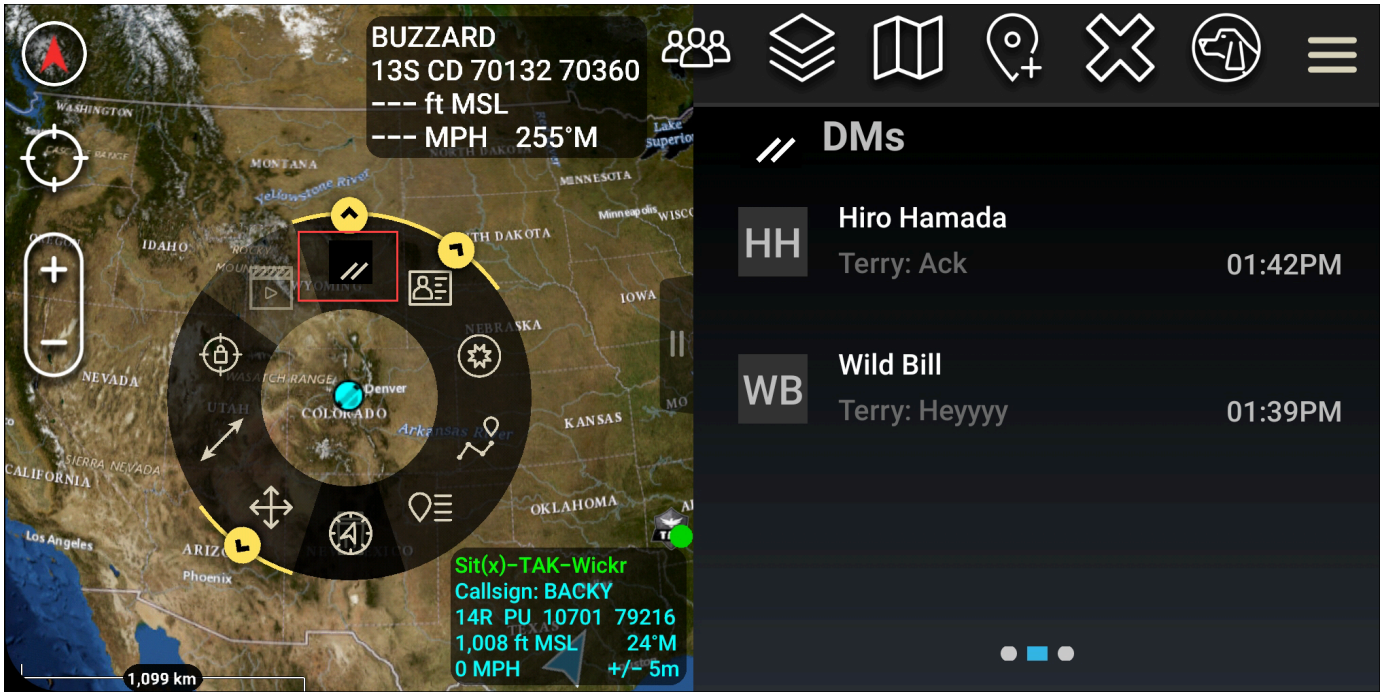
4. Rekam pesan Anda.
5. Setelah Anda merekam pesan Anda, lepaskan tombol untuk mengirim.

Pinwheel (Akses Cepat) untuk ATAK

Fitur pinwheel atau akses cepat digunakan untuk one-one-one percakapan atau pesan langsung.

Selesaikan prosedur berikut untuk menggunakan kincir.

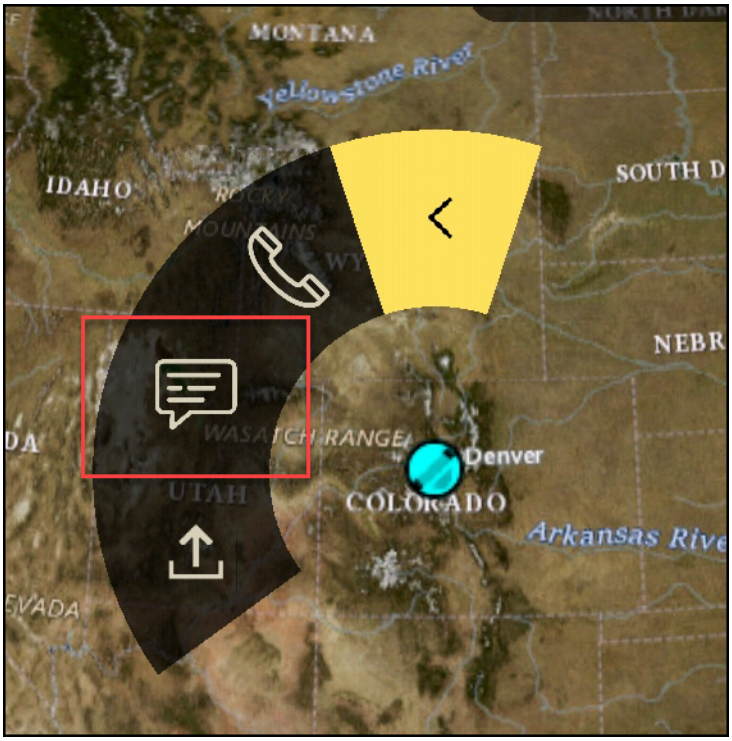
1. Buka tampilan layar terpisah dari peta ATAK dan plugin Wickr untuk ATAK secara bersamaan. Peta menampilkan rekan tim atau aset Anda pada tampilan peta.
2. Pilih ikon pengguna untuk membuka kincir.
3. Pilih ikon Wickr untuk melihat opsi yang tersedia untuk pengguna yang dipilih.



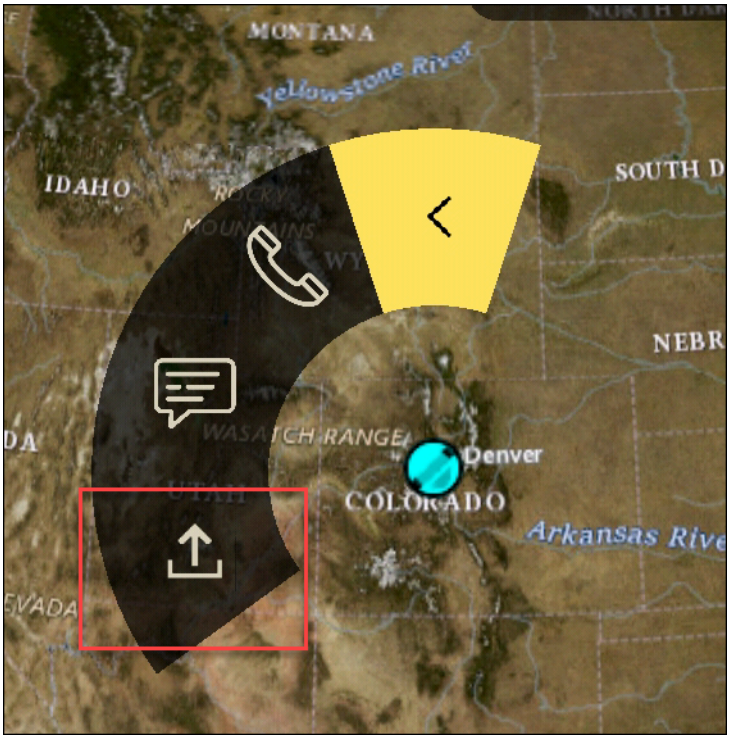
4. Pada kincir, pilih salah satu ikon berikut:

   - Telepon: Pilih untuk menelepon.

- Pesan: Pilih untuk mengobrol.



- Kirim file: Pilih untuk mengirim file.



Navigasi untuk ATAK

UI plugin berisi tiga tampilan plugin yang ditunjukkan oleh bentuk biru dan putih di kanan bawah layar. Geser ke kiri dan kanan untuk menavigasi di antara tampilan.

- Tampilan kontak: Buat grup pesan langsung atau percakapan ruangan.
- DMs view: Buat one-to-one percakapan. Fungsionalitas obrolan berfungsi seperti di aplikasi asli Wickr. Fungsionalitas ini memungkinkan Anda untuk tetap berada di tampilan Peta dan berkomunikasi dengan orang lain di plugin.
- Tampilan kamar: Kamar yang ada di aplikasi asli di-porting. Apa pun yang dilakukan di plugin tercermin dalam aplikasi asli Wickr.

> **Note**
>
> Fungsi tertentu, seperti menghapus ruangan, hanya dapat dilakukan di aplikasi asli dan secara langsung untuk mencegah modifikasi yang tidak diinginkan oleh pengguna dan gangguan yang disebabkan oleh peralatan lapangan.

Port dan domain untuk memungkinkan daftar untuk jaringan Wickr Anda

Izinkan daftar port berikut untuk memastikan Wickr berfungsi dengan benar:

Pelabuhan

- Port TCP 443 (untuk pesan dan lampiran)
- Port UDP 16384-16584 (untuk menelepon)

Domain dan alamat untuk daftar yang diizinkan menurut Wilayah

Jika Anda perlu mengizinkan daftar semua kemungkinan domain panggilan dan alamat IP server, lihat daftar potensi CIDRs berdasarkan Wilayah berikut. Periksa daftar ini secara berkala, karena dapat berubah.

> **Note**
>
> Email pendaftaran dan verifikasi dikirim dari `no-reply@amazonaws.com` dan`donotreply@wickr.email`.

AS Timur (Virginia Utara)

Domain:	• gw-pro-prod.wickr.com • api.messaging. wickr.us-east-1.amazonaws.com • ingress.prod.calling.wickr.com
Memanggil alamat CIDR:	• 44.211.195.0/27 • 44.213.83.32/28
Memanggil alamat IP:	• 44.211.195.0 • 44.211.195.1 • 44.211.195.2 • 44.211.195.3

- 44.211.195.4
- 44.211.195.5
- 44.211.195.6
- 44.211.195.7
- 44.211.195.8
- 44.211.195.9
- 44.211.195.10
- 44.211.195.11
- 44.211.195.12
- 44.211.195.13
- 44.211.195.14
- 44.211.195.15
- 44.211.195.16
- 44.211.195.17
- 44.211.195.18
- 44.211.195.19
- 44.211.195.20
- 44.211.195.21
- 44.211.195.22
- 44.211.195.23
- 44.211.195.24
- 44.211.195.25
- 44.211.195.26
- 44.211.195.27
- 44.211.195.28
- 44.211.195.29
- 44.211.195.30
- 44.211.195.31
- 44.213.83.32
- 44.213.83.33

	• 44.213.83.34 • 44.213.83.35 • 44.213.83.36 • 44.213.83.37 • 44.213.83.38 • 44.213.83.39 • 44.213.83.40 • 44.213.83.41 • 44.213.83.42 • 44.213.83.43 • 44.213.83.44 • 44.213.83.45 • 44.213.83.46 • 44.213.83.47

Asia Pasifik (Malaysia)

Domain:	• gw-pro-prod.wickr.com • api.messaging. wickr.ap-southeast-5.amazonaws.com • ingress.prod.calling. wickr.ap-southeast-5.amazonaws.com
Memanggil alamat CIDR:	• 43.216.226.160/28
Memanggil alamat IP:	• 43.216.226.160 • 43.216.226.161 • 43.216.226.162 • 43.216.226.163 • 43.216.226.164 • 43.216.226.165 • 43.216.226.166

	• 43.216.226.167 • 43.216.226.168 • 43.216.226.169 • 43.216.226.170 • 43.216.226.171 • 43.216.226.172 • 43.216.226.173 • 43.216.226.174 • 43.216.226.175

Asia Pasifik (Singapura)

Domain:	• gw-pro-prod.wickr.com • api.messaging. wickr.ap-southeast-1.amazonaws.com • ingress.prod.calling. wickr.ap-southeast-1.amazonaws.com
Memanggil alamat CIDR:	• 47.129.23.144/28
Memanggil alamat IP:	• 47.129.23.144 • 47.129.23.145 • 47.129.23.146 • 47.129.23.147 • 47.129.23.148 • 47.129.23.149 • 47.129.23.150 • 47.129.23.151 • 47.129.23.152 • 47.129.23.153 • 47.129.23.154 • 47.129.23.155

	• 47.129.23.156 • 47.129.23.157 • 47.129.23.158 • 47.129.23.159

Asia Pasifik (Sydney)

Domain:	• gw-pro-prod.wickr.com • api.messaging. wickr.ap-southeast-2.amazonaws.com • ingress.prod.calling. wickr.ap-southeast-2.amazonaws.com
Memanggil alamat CIDR:	• 3.27.180.208/28
Memanggil alamat IP:	• 3.27.180.208 • 3.27.180.209 • 3.27.180.210 • 3.27.180.211 • 3.27.180.212 • 3.27.180.213 • 3.27.180.214 • 3.27.180.215 • 3.27.180.216 • 3.27.180.217 • 3.27.180.218 • 3.27.180.219 • 3.27.180.220 • 3.27.180.221 • 3.27.180.222 • 3.27.180.223

Asia Pasifik (Tokyo)

Domain:	• gw-pro-prod.wickr.com • api.messaging. wickr.ap-northeast-1.amazonaws.com • ingress.prod.calling. wickr.ap-northeast-1.amazonaws.com
Memanggil alamat CIDR:	• 57.181.142.240/28
Memanggil alamat IP:	• 57.181.142.240 • 57.181.142.241 • 57.181.142.242 • 57.181.142.243 • 57.181.142.244 • 57.181.142.245 • 57.181.142.246 • 57.181.142.247 • 57.181.142.248 • 57.181.142.249 • 57.181.142.250 • 57.181.142.251 • 57.181.142.252 • 57.181.142.253 • 57.181.142.254 • 57.181.142.255

Kanada (Pusat)

Domain:	• gw-pro-prod.wickr.com • api.messaging. wickr.ca-central-1.amazonaws.com

	• ingress.prod.calling. wickr.ca-central-1 .amazonaws.com
Memanggil alamat CIDR:	• 15.156.152.96/28
Memanggil alamat IP:	• 15.156.152.96 • 15.156.152.97 • 15.156.152.98 • 15.156.152.99 • 15.156.152.100 • 15.156.152.101 • 15.156.152.102 • 15.156.152.103 • 15.156.152.104 • 15.156.152.105 • 15.156.152.106 • 15.156.152.107 • 15.156.152.108 • 15.156.152.109 • 15.156.152.110 • 15.156.152.111

Eropa (Frankfurt)

Domain:	• gw-pro-prod.wickr.com • api.messaging. wickr.eu-central-1.amazonaw s.com • ingress.prod.calling. wickr.eu-central-1 .amazonaws.com
Memanggil alamat CIDR:	• 3.78.252.32/28
Memanggil alamat IP:	• 3.78.252.32

	• 3.78.252.33 • 3.78.252.34 • 3.78.252.35 • 3.78.252.36 • 3.78.252.37 • 3.78.252.38 • 3.78.252.39 • 3.78.252.40 • 3.78.252.41 • 3.78.252.42 • 3.78.252.43 • 3.78.252.44 • 3.78.252.45 • 3.78.252.46 • 3.78.252.47

Alamat IP perpesanan:	• 3.163.236.183 • 3.163.238.183 • 3.163.251.183 • 3.163.232.183 • 3.163.241.183 • 3.163.245.183 • 3.163.248.183 • 3.163.234.183 • 3.163.237.183 • 3.163.243.183 • 3.163.247.183 • 3.163.240.183 • 3.163.242.183 • 3.163.244.183 • 3.163.246.183 • 3.163.249.183 • 3.163.252.183 • 3.163.235.183 • 3.163.250.183 • 3.163.239.183 • 3.163.233.183

Eropa (London)

Domain:	• gw-pro-prod.wickr.com • api.messaging. wickr.eu-west-2.amazonaws.com • ingress.prod.calling. wickr.eu-west-2.amazonaws.com
Memanggil alamat CIDR:	• 13.43.91.48/28

Memanggil alamat IP:	• 13.43.91.48 • 13.43.91.49 • 13.43.91.50 • 13.43.91.51 • 13.43.91.52 • 13.43.91.53 • 13.43.91.54 • 13.43.91.55 • 13.43.91.56 • 13.43.91.57 • 13.43.91.58 • 13.43.91.59 • 13.43.91.60 • 13.43.91.61 • 13.43.91.62 • 13.43.91.63

Eropa (Stockholm)

Domain:	• gw-pro-prod.wickr.com • api.messaging. wickr.eu-north-1.amazonaws.com • ingress.prod.calling. wickr.eu-north-1.amazonaws.com
Memanggil alamat CIDR:	• 13.60.1.64/28
Memanggil alamat IP:	• 13.60.1.64 • 13.60.1.65 • 13.60.1.66 • 13.60.1.67 • 13.60.1.68

	• 13.60.1.69 • 13.60.1.70 • 13.60.1.71 • 13.60.1.72 • 13.60.1.73 • 13.60.1.74 • 13.60.1.75 • 13.60.1.76 • 13.60.1.77 • 13.60.1.78 • 13.60.1.79

Europe (Zurich)

Domain:	• gw-pro-prod.wickr.com • api.messaging. wickr.eu-central-2.amazonaws.com • ingress.prod.calling. wickr.eu-central-2 .amazonaws.com
Memanggil alamat CIDR:	• 16.63.106.224/28
Memanggil alamat IP:	• 16.63.106.224 • 16.63.106.225 • 16.63.106.226 • 16.63.106.227 • 16.63.106.228 • 16.63.106.229 • 16.63.106.230 • 16.63.106.231 • 16.63.106.232 • 16.63.106.233

	• 16.63.106.234 • 16.63.106.235 • 16.63.106.236 • 16.63.106.237 • 16.63.106.238 • 16.63.106.239

AWS GovCloud (AS-Barat)

Domain:	• gw-pro-prod.wickr.com • api.messaging.wickr. us-gov-west-1.amazonaws.com • ingress-prod-calling.wickr. us-gov-west-1.amazonaws.com • s3. us-gov-west-1.amazonaws.com • s3-fips. us-gov-west-1.amazonaws.com • s3.amazonaws.com • daftar.wickr. us-gov-west-1.amazonaws.com • admin.wickr. us-gov-west-1.amazonaws.com • admin.messaging.wickr. us-gov-west-1.amazonaws.com • kognito-identitas. us-gov-west-1.amazonaws.com • kinesis. us-gov-west-1.amazonaws.com
Memanggil alamat CIDR:	• 3.30.186.208/28 • 3.31.11.216/29
Memanggil alamat IP:	• 3.30.186.208 • 3.30.186.209 • 3.30.186.210 • 3.30.186.211

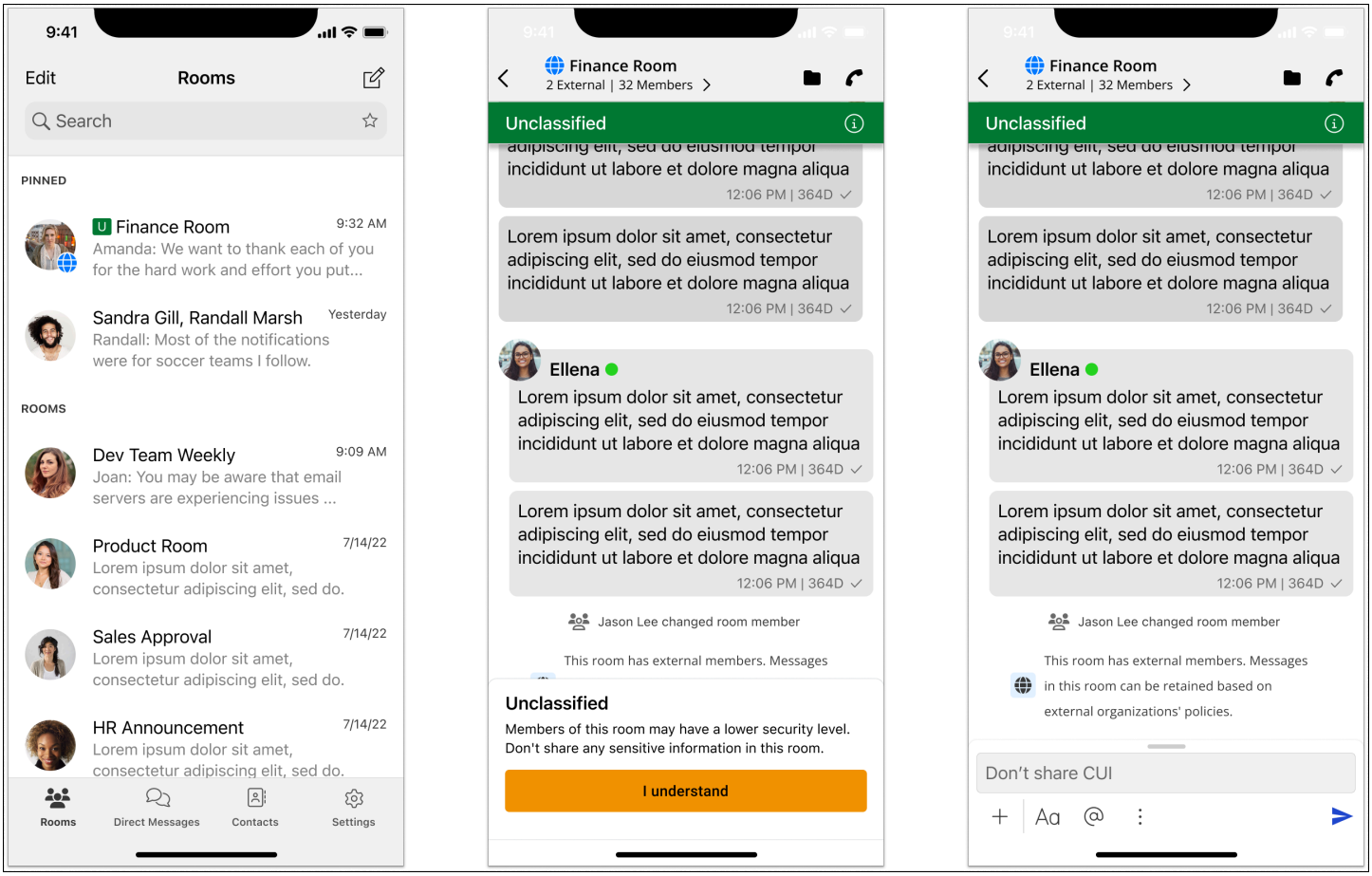
- 3.30.186.212
- 3.30.186.213
- 3.30.186.214
- 3.30.186.215
- 3.30.186.216
- 3.30.186.217
- 3.30.186.218
- 3.30.186.219
- 3.30.186.220
- 3.30.186.221
- 3.30.186.222
- 3.30.186.223
- 3.31.11.216
- 3.31.11.217
- 3.31.11.218
- 3.31.11.219
- 3.31.11.220
- 3.31.11.221
- 3.31.11.222
- 3.31.11.223

GovCloud klasifikasi lintas batas dan federasi

AWS Wickr menawarkan WickrGov klien yang disesuaikan untuk pengguna. GovCloud GovCloud Federasi memungkinkan komunikasi antara GovCloud pengguna dan pengguna komersial. Fitur klasifikasi lintas batas memungkinkan perubahan antarmuka pengguna untuk percakapan bagi GovCloud pengguna. Sebagai GovCloud pengguna, Anda harus mematuhi pedoman ketat mengenai klasifikasi yang ditetapkan pemerintah. Ketika GovCloud pengguna terlibat dalam percakapan dengan pengguna komersial (Enterprise, AWS Wickr, pengguna Tamu), mereka akan melihat peringatan tidak diklasifikasikan berikut ditampilkan:

- Tag U di daftar kamar

- Pengakuan yang tidak diklasifikasikan di layar pesan
- Spanduk yang tidak diklasifikasikan di atas percakapan



> **Note**
>
> Peringatan ini hanya akan ditampilkan ketika GovCloud pengguna sedang dalam percakapan atau bagian dari ruangan dengan pengguna eksternal. Mereka akan hilang jika pengguna eksternal meninggalkan percakapan. Tidak ada peringatan yang akan ditampilkan dalam percakapan antar GovCloud pengguna.

Pratinjau file untuk AWS Wickr

Organizations yang menggunakan tingkat Wickr Premium (termasuk uji coba gratis Premium), sekarang dapat mengelola izin pengunduhan file di tingkat grup keamanan.

Unduhan file diaktifkan secara default di grup keamanan. Administrator dapat mengaktifkan atau menonaktifkan unduhan file melalui panel administrator. Pengaturan ini diterapkan ke seluruh jaringan Wickr.

Untuk mengaktifkan atau menonaktifkan unduhan file, selesaikan prosedur berikut.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Pada panel navigasi, pilih Grup keamanan.
4. Pilih nama grup keamanan yang ingin Anda edit.

   Halaman detail grup keamanan menampilkan pengaturan untuk grup keamanan di tab yang berbeda.
5. Di bawah tab Pesan, di bagian Media dan tautan, pilih Edit.
6. Pada halaman Edit media dan tautan, centang atau hapus centang opsi Unduhan file.
7. Pilih Simpan perubahan.

Saat unduhan file diaktifkan untuk grup keamanan, pengguna dapat mengunduh file yang dibagikan dalam pesan langsung dan ruangan. Jika unduhan dinonaktifkan, mereka hanya dapat melihat pratinjau file-file ini dan mengunggah ke tab File, tetapi tidak dapat mengunduhnya. Pengguna juga dibatasi untuk mengambil tangkapan layar; upaya akan menghasilkan layar hitam.

> **Note**
>
> Ketika unduhan File dinonaktifkan, semua pengguna dalam grup keamanan itu harus menggunakan Wickr versi 6.54 ke atas agar pengaturan file ini diterapkan.

> **Note**
>
> Di ruangan di mana pengguna dari jaringan yang berbeda (karena federasi) dan grup keamanan hadir, kemampuan setiap pengguna untuk melihat pratinjau atau mengunduh file didasarkan pada pengaturan grup keamanan khusus mereka. Akibatnya, beberapa pengguna dapat mengunduh file di ruangan sementara yang lain hanya dapat mempratinjaunya.

Kelola pengguna di AWS Wickr

Di bagian Manajemen pengguna Konsol Manajemen AWS untuk Wickr Anda dapat melihat pengguna dan bot Wickr saat ini, dan memodifikasi detailnya.

Topik

Direktori tim di jaringan AWS Wickr

Anda dapat melihat pengguna Wickr saat ini dan memodifikasi detailnya di bagian Manajemen pengguna Konsol Manajemen AWS untuk Wickr.

Topik

Lihat pengguna di jaringan AWS Wickr

Anda dapat melihat detail pengguna yang terdaftar di jaringan Wickr Anda.

Selesaikan prosedur berikut untuk melihat pengguna yang terdaftar di jaringan Wickr Anda.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Di panel navigasi, pilih Manajemen pengguna.

   Tab Direktori Tim menampilkan pengguna yang terdaftar ke jaringan Wickr Anda, termasuk nama, alamat email, grup keamanan yang ditetapkan, dan status saat ini. Untuk pengguna saat

ini, Anda dapat melihat perangkat mereka, mengedit detailnya, menangguhkan, menghapus, dan mengalihkannya ke jaringan Wickr lain.

Mengundang pengguna di jaringan AWS Wickr

Anda dapat mengundang pengguna di jaringan Wickr Anda.

Selesaikan prosedur berikut untuk mengundang pengguna di jaringan Wickr Anda.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Di panel navigasi, pilih Manajemen pengguna.
4. Di tab Direktori tim, pilih Undang pengguna.
5. Pada halaman Undang pengguna, masukkan alamat email dan grup keamanan pengguna. Alamat email dan grup keamanan adalah satu-satunya bidang yang diperlukan. Pastikan untuk memilih grup keamanan yang sesuai untuk pengguna. Wickr akan mengirim email undangan ke alamat yang Anda tentukan untuk pengguna.
6. Pilih Undang pengguna.

   Email dikirim ke pengguna. Email tersebut menyediakan tautan unduhan untuk aplikasi klien Wickr, dan tautan untuk mendaftar ke Wickr. Saat pengguna mendaftar untuk Wickr menggunakan tautan di email, status mereka di direktori tim Wickr akan berubah dari Tertunda menjadi Aktif.

Mengedit pengguna di jaringan AWS Wickr

Anda dapat mengedit pengguna di jaringan Wickr Anda.

Selesaikan prosedur berikut untuk mengedit pengguna.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Di panel navigasi, pilih Manajemen pengguna.
4. Di tab Direktori tim, pilih ikon elipsis vertikal (tiga titik) dari pengguna yang ingin Anda edit.
5. Pilih Edit.
6. Edit informasi pengguna, lalu pilih Simpan perubahan.

Menghapus pengguna di jaringan AWS Wickr

Anda dapat menghapus pengguna di jaringan Wickr Anda.

Selesaikan prosedur berikut untuk menghapus pengguna.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Di panel navigasi, pilih Manajemen pengguna.
4. Di tab Direktori tim, pilih ikon elipsis vertikal (tiga titik) dari pengguna yang ingin Anda hapus.
5. Pilih Hapus untuk menghapus pengguna.

   Saat Anda menghapus pengguna, pengguna tersebut tidak lagi dapat masuk ke jaringan Wickr Anda di klien Wickr.
6. Di jendela pop-up, pilih Hapus.

Hapus pengguna secara massal di jaringan AWS Wickr

Anda dapat menghapus pengguna jaringan Wickr secara massal di bagian Manajemen pengguna di Konsol Manajemen AWS untuk Wickr.

> **Note**
>
> Opsi untuk menghapus pengguna secara massal hanya berlaku ketika SSO tidak diaktifkan.

Untuk menghapus pengguna jaringan Wickr Anda secara massal menggunakan templat CSV, selesaikan prosedur berikut.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Di panel navigasi, pilih Manajemen pengguna.
4. Tab Direktori Tim menampilkan pengguna yang terdaftar ke jaringan Wickr Anda.
5. Di tab Direktori tim, pilih Kelola pengguna, lalu pilih Hapus massal.
6. Pada halaman Hapus pengguna massal, unduh contoh template CSV. Untuk mengunduh templat sampel, pilih Unduh templat.

7. Lengkapi template dengan menambahkan email pengguna yang ingin Anda hapus secara massal dari jaringan Anda.
8. Unggah template CSV yang sudah selesai. Anda dapat menarik dan melepas file ke dalam kotak unggah, atau pilih pilih file.
9. Pilih kotak centang, saya mengerti bahwa menghapus pengguna tidak dapat dibalik.
10. Pilih Hapus pengguna.

> **Note**
>
> Tindakan ini akan segera mulai menghapus pengguna dan mungkin memakan waktu beberapa menit. Pengguna yang dihapus tidak akan lagi dapat masuk ke jaringan Wickr Anda di klien Wickr.

Untuk menghapus pengguna jaringan Wickr Anda secara massal dengan mengunduh CSV direktori tim Anda, selesaikan prosedur berikut.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Di panel navigasi, pilih Manajemen pengguna.
4. Tab Direktori Tim menampilkan pengguna yang terdaftar ke jaringan Wickr Anda.
5. Di tab Direktori tim, pilih Kelola pengguna, lalu pilih Unduh sebagai CSV.
6. Setelah Anda mengunduh templat CSV direktori tim, hapus baris pengguna yang tidak perlu dihapus.
7. Di tab Direktori tim, pilih Kelola pengguna, lalu pilih Hapus massal.
8. Pada halaman Hapus pengguna massal, unggah templat CSV direktori tim. Anda dapat menarik dan melepas file ke dalam kotak unggah, atau pilih Pilih file.
9. Pilih kotak centang, saya mengerti bahwa menghapus pengguna tidak dapat dibalik.
10. Pilih Hapus pengguna.

> **Note**
>
> Tindakan ini akan segera mulai menghapus pengguna dan mungkin memakan waktu beberapa menit. Pengguna yang dihapus tidak akan lagi dapat masuk ke jaringan Wickr Anda di klien Wickr.

Menangguhkan pengguna secara massal di jaringan AWS Wickr

Anda dapat menangguhkan pengguna jaringan Wickr secara massal di bagian Manajemen pengguna di untuk Wickr. Konsol Manajemen AWS

> **Note**
>
> Opsi untuk menangguhkan pengguna secara massal hanya berlaku ketika SSO tidak diaktifkan.

Untuk menangguhkan pengguna jaringan Wickr Anda secara massal, selesaikan prosedur berikut.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Di panel navigasi, pilih Manajemen pengguna.
4. Tab Direktori Tim menampilkan pengguna yang terdaftar ke jaringan Wickr Anda.
5. Di tab Direktori tim, pilih Kelola pengguna, lalu pilih Penangguhan massal.
6. Pada halaman Bulk menangguhkan pengguna, unduh contoh template CSV. Untuk mengunduh templat sampel, pilih Unduh templat.
7. Lengkapi template dengan menambahkan email pengguna yang ingin ditangguhkan secara massal dari jaringan Anda.
8. Unggah template CSV yang sudah selesai. Anda dapat menarik dan melepas file ke dalam kotak unggah, atau pilih pilih file.
9. Pilih Tangguhkan pengguna.

> **Note**
>
> Tindakan ini akan segera mulai menangguhkan pengguna dan mungkin memakan waktu beberapa menit. Pengguna yang ditangguhkan tidak dapat masuk ke jaringan Wickr Anda di klien Wickr. Ketika Anda menangguhkan pengguna yang saat ini masuk ke jaringan Wickr Anda di klien, pengguna tersebut secara otomatis keluar.

Pengguna tamu di jaringan AWS Wickr

Fitur pengguna tamu Wickr memungkinkan pengguna tamu individu untuk masuk ke klien Wickr dan berkolaborasi dengan pengguna jaringan Wickr. Administrator Wickr dapat mengaktifkan atau menonaktifkan pengguna tamu untuk jaringan Wickr mereka.

Setelah fitur diaktifkan, pengguna tamu yang diundang ke jaringan Wickr Anda dapat berinteraksi dengan pengguna di jaringan Wickr Anda. Biaya akan dikenakan untuk fitur pengguna tamu Anda Akun AWS . Untuk informasi selengkapnya tentang harga untuk fitur pengguna tamu, lihat halaman harga Wickr di bawah Pengaya Harga.

Topik

Mengaktifkan atau menonaktifkan pengguna tamu di jaringan AWS Wickr

Anda dapat mengaktifkan atau menonaktifkan pengguna tamu di jaringan Wickr Anda.

Selesaikan prosedur berikut untuk mengaktifkan atau menonaktifkan pengguna tamu untuk jaringan Wickr Anda.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.

3. Pada panel navigasi, pilih Grup keamanan.
4. Pilih nama untuk grup keamanan tertentu.

> **Note**
>
> Anda dapat mengaktifkan pengguna tamu hanya untuk grup keamanan individual. Untuk mengaktifkan pengguna tamu untuk semua grup keamanan di jaringan Wickr Anda, Anda harus mengaktifkan fitur untuk setiap grup keamanan di jaringan Anda.

5. Pilih tab Federasi di grup keamanan.
6. Ada dua lokasi di mana opsi untuk mengaktifkan pengguna tamu tersedia:
   - Federasi lokal - Untuk jaringan di AS Timur (Virginia Utara), pilih Edit di bagian federasi lokal halaman.
   - Federasi global - Untuk semua jaringan lain di wilayah lain, pilih Edit di bagian Federasi global halaman.
7. Pada halaman Edit federasi, pilih Aktifkan federasi.
8. Pilih Simpan perubahan untuk menyimpan perubahan dan membuatnya efektif untuk grup keamanan.

   Pengguna terdaftar di grup keamanan tertentu di jaringan Wickr Anda sekarang dapat berinteraksi dengan pengguna tamu. Untuk informasi selengkapnya, lihat Pengguna tamu di Panduan Pengguna Wickr.

Lihat jumlah pengguna tamu di jaringan AWS Wickr

Anda dapat melihat jumlah pengguna tamu di jaringan Wickr Anda.

Selesaikan prosedur berikut untuk melihat jumlah pengguna tamu untuk jaringan Wickr Anda.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Di panel navigasi, pilih Manajemen pengguna.

   Halaman manajemen pengguna, menampilkan hitungan pengguna tamu di jaringan Wickr Anda.

Lihat penggunaan bulanan di jaringan AWS Wickr

Anda dapat melihat jumlah pengguna tamu yang telah berkomunikasi dengan jaringan Anda selama periode penagihan.

Selesaikan prosedur berikut untuk melihat penggunaan bulanan Anda untuk jaringan Wickr Anda.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Di panel navigasi, pilih Manajemen pengguna.
4. Pilih tab Pengguna tamu.

   Tab Pengguna tamu menampilkan penggunaan bulanan pengguna tamu.

   > **Note**
   >
   > Data penagihan tamu diperbarui setiap 24 jam.

Lihat pengguna tamu di jaringan AWS Wickr

Anda dapat melihat pengguna tamu yang telah berkomunikasi dengan pengguna jaringan selama periode penagihan tertentu.

Selesaikan prosedur berikut untuk melihat pengguna tamu yang berkomunikasi dengan pengguna jaringan selama periode penagihan tertentu.

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Di panel navigasi, pilih Manajemen pengguna.
4. Pilih tab Pengguna tamu.

   Tab Pengguna tamu menampilkan pengguna tamu di jaringan Anda.

Memblokir pengguna tamu di jaringan AWS Wickr

Anda dapat memblokir dan membuka blokir pengguna tamu di jaringan Wickr Anda. Pengguna yang diblokir tidak dapat berkomunikasi dengan siapa pun di jaringan Anda.

Untuk memblokir pengguna tamu

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Di panel navigasi, pilih Manajemen pengguna.
4. Pilih tab Pengguna tamu.

   Tab Pengguna tamu menampilkan pengguna tamu di jaringan Anda.
5. Di bagian Pengguna Tamu, temukan email pengguna tamu yang ingin Anda blokir.
6. Di sisi kanan nama pengguna tamu, pilih tiga titik, dan pilih Blokir pengguna tamu.
7. Pilih Blokir pada jendela pop-up.
8. Untuk melihat daftar pengguna yang diblokir di jaringan Wickr Anda, pilih menu tarik-turun Status, lalu pilih Diblokir.

Untuk membuka blokir pengguna tamu

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Di panel navigasi, pilih Manajemen pengguna.
4. Pilih tab Pengguna tamu.

   Tab Pengguna tamu menampilkan pengguna tamu di jaringan Anda.
5. Pilih menu tarik-turun Status, lalu pilih Diblokir.
6. Di bagian Diblokir, temukan email pengguna tamu yang ingin Anda buka blokir.
7. Di sisi kanan nama pengguna tamu, pilih tiga titik, dan pilih Buka blokir pengguna.
8. Pilih Buka blokir di jendela pop-up.

Keamanan di AWS Wickr

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

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

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku untuk AWS Wickr, lihat AWS Layanan dalam Lingkup oleh AWS Layanan Program Kepatuhan dalam Lingkup oleh Program .
- 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 Wickr. Topik berikut menunjukkan cara mengkonfigurasi Wickr untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Wickr Anda.

Topik

Perlindungan data di AWS Wickr

Model tanggung jawab AWS bersama model tanggung berlaku untuk perlindungan data di AWS Wickr. 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 kredensil dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

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

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk ketika Anda bekerja dengan Wickr 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.

Manajemen identitas dan akses untuk AWS Wickr

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 Wickr. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

Audiens untuk AWS Wickr

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

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

Mengautentikasi dengan identitas AWS Wickr

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

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

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

Akun AWS pengguna root

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

Identitas terfederasi

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

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

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

Pengguna dan grup IAM

Pengguna IAM adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk

informasi selengkapnya, lihat Mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredensi sementara di Panduan Pengguna IAM.

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

Peran IAM

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

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

Mengelola akses menggunakan kebijakan untuk AWS Wickr

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

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

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

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh

identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan dalam Panduan Pengguna IAM.

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

Kebijakan berbasis sumber daya

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

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

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 batas izin untuk suatu entitas. Izin yang dihasilkan adalah persimpangan antara kebijakan berbasis identitas milik entitas dan batas 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 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.

AWS kebijakan terkelola untuk AWS Wickr

Untuk menambahkan izin ke pengguna, grup, dan peran, lebih mudah menggunakan kebijakan AWS terkelola daripada menulis kebijakan sendiri. Dibutuhkan waktu dan keahlian untuk membuat kebijakan yang dikelola pelanggan IAM yang hanya memberi tim Anda izin yang mereka butuhkan. Untuk memulai dengan cepat, Anda dapat menggunakan kebijakan AWS terkelola kami. Kebijakan ini mencakup kasus penggunaan umum dan tersedia di Akun AWS Anda. Untuk informasi selengkapnya tentang kebijakan AWS AWS terkelola, lihat kebijakan terkelola di Panduan Pengguna IAM.

Layanan AWS memelihara dan memperbarui kebijakan AWS terkelola. Anda tidak dapat mengubah izin dalam kebijakan AWS terkelola. Layanan terkadang menambahkan izin tambahan ke kebijakan yang dikelola AWS untuk mendukung fitur-fitur baru. Jenis pembaruan ini akan memengaruhi semua identitas (pengguna, grup, dan peran) di mana kebijakan tersebut dilampirkan. Layanan kemungkinan besar akan memperbarui kebijakan yang dikelola AWS saat ada fitur baru yang diluncurkan atau saat ada operasi baru yang tersedia. Layanan tidak menghapus izin dari kebijakan AWS terkelola, sehingga pembaruan kebijakan tidak akan merusak izin yang ada.

AWS kebijakan terkelola: AWSWickr FullAccess

Anda dapat melampirkan kebijakan `AWSWickrFullAccess` ke identitas IAM Anda. Kebijakan ini memberikan izin administratif penuh ke layanan Wickr, termasuk Konsol Manajemen AWS untuk

Wickr di. Konsol Manajemen AWSUntuk informasi selengkapnya tentang melampirkan kebijakan ke identitas, lihat Menambahkan dan menghapus izin identitas IAM di Panduan Pengguna.AWS Identity and Access Management

Detail izin

Kebijakan ini mencakup izin berikut.

- `wickr`— Memberikan izin administratif penuh ke layanan Wickr.

JSON

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

Pembaruan Wickr ke AWS kebijakan terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Wickr sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman riwayat Dokumen Wickr.

Ubah	Deskripsi	Date
AWSWickrFullAccess – Kebijakan baru	Wickr menambahkan kebijakan baru yang memberikan izin administr atif penuh ke layanan Wickr, termasuk konsol administrator Wickr di. Konsol Manajemen AWS	28 November 2022

Ubah	Deskripsi	Date
Wickr mulai melacak perubahan	Wickr mulai melacak perubahan untuk kebijakan yang AWS dikelola.	28 November 2022

Bagaimana AWS Wickr bekerja dengan IAM

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

Fitur IAM yang dapat Anda gunakan dengan AWS Wickr

Fitur IAM	Dukungan Wickr
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Tidak
Kunci kondisi kebijakan	Tidak
ACLs	Tidak
ABAC (tanda dalam kebijakan)	Tidak
Kredensial sementara	Tidak
Izin principal	Tidak
Peran layanan	Tidak
Peran terkait layanan	Tidak

Untuk mendapatkan tampilan tingkat tinggi tentang bagaimana Wickr dan AWS layanan lainnya bekerja dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk Wickr

Mendukung kebijakan berbasis identitas: Ya

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

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

Contoh kebijakan berbasis identitas untuk Wickr

Untuk melihat contoh kebijakan berbasis identitas Wickr, lihat. Contoh kebijakan berbasis identitas untuk AWS Wickr

Kebijakan berbasis sumber daya dalam Wickr

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan principal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

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

Tindakan kebijakan untuk Wickr

Mendukung tindakan kebijakan: Ya

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

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

Untuk melihat daftar tindakan Wickr, lihat Tindakan yang Ditentukan oleh AWS Wickr di Referensi Otorisasi Layanan.

Tindakan kebijakan di Wickr menggunakan awalan berikut sebelum tindakan:

```
wickr
```

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

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

Untuk melihat contoh kebijakan berbasis identitas Wickr, lihat. Contoh kebijakan berbasis identitas untuk AWS Wickr

Sumber daya kebijakan untuk Wickr

Mendukung sumber daya kebijakan: Tidak

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

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

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

Untuk melihat daftar jenis sumber daya Wickr dan jenisnya ARNs, lihat Sumber Daya yang Ditentukan oleh AWS Wickr di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang Ditentukan oleh AWS Wickr.

Untuk melihat contoh kebijakan berbasis identitas Wickr, lihat. Contoh kebijakan berbasis identitas untuk AWS Wickr

Kunci kondisi kebijakan untuk Wickr

Mendukung kunci kondisi kebijakan khusus layanan: Tidak

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

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

Untuk melihat daftar kunci kondisi Wickr, lihat Kunci Kondisi untuk AWS Wickr di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang Ditentukan oleh AWS Wickr.

Untuk melihat contoh kebijakan berbasis identitas Wickr, lihat. Contoh kebijakan berbasis identitas untuk AWS Wickr

ACLs di Wickr

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 Wickr

Mendukung ABAC (tag dalam kebijakan): Tidak

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

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

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

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

Menggunakan kredensil sementara dengan Wickr

Mendukung kredensi sementara: Tidak

Kredensi sementara menyediakan akses jangka pendek ke AWS sumber daya dan secara otomatis dibuat saat Anda menggunakan federasi atau beralih peran. 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 dan Layanan AWS yang berfungsi dengan IAM dalam Panduan Pengguna IAM.

Izin utama lintas layanan untuk Wickr

Mendukung sesi akses maju (FAS): Tidak

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

Peran layanan untuk Wickr

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 Wickr. Edit peran layanan hanya ketika Wickr memberikan panduan untuk melakukannya.

Peran terkait layanan untuk Wickr

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 AWS Wickr

Secara default, pengguna IAM baru tidak memiliki izin untuk melakukan apa pun. Administrator IAM harus membuat dan menetapkan kebijakan IAM yang memberikan izin kepada pengguna untuk mengelola layanan AWS Wickr. Berikut adalah contoh kebijakan izin.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wickr:CreateAdminSession",
                "wickr:ListNetworks"
            ],
            "Resource": "*"
        }
    ]
}
```

Kebijakan contoh ini memberi pengguna izin untuk mencantumkan jaringan Wickr menggunakan Wickr for Wickr. Konsol Manajemen AWS Untuk mempelajari lebih lanjut tentang elemen-elemen dalam pernyataan kebijakan IAM, lihat Kebijakan berbasis identitas untuk Wickr. Untuk mempelajari cara membuat kebijakan IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan di tab JSON dalam Panduan Pengguna IAM.

Anda juga dapat membuat kebijakan IAM untuk memungkinkan pengguna mengakses tindakan API tertentu. Akses ke tindakan API dikelola secara terpisah dari konsol AWS Wickr. Di bawah ini adalah contoh kebijakan yang memberikan akses hanya-baca ke tindakan API tertentu. Untuk informasi selengkapnya tentang tindakan API, lihat Selamat datang di Referensi AWS Wickr API.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "WickrAPIReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "wickr:ListNetworks",
                "wickr:ListUsers",
                "wickr:GetNetworkSettings",
                "wickr:GetNetwork",
                "wickr:GetUser",
                "wickr:ListTagsForResource"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

Topik

- Praktik terbaik kebijakan
- Menggunakan Konsol Manajemen AWS untuk Wickr
- Mengizinkan pengguna melihat izin mereka sendiri

Praktik terbaik kebijakan

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

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti

CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.

- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan dengan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Amankan akses API dengan MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM dalam Panduan Pengguna IAM.

Menggunakan Konsol Manajemen AWS untuk Wickr

Lampirkan kebijakan `AWSWickrFullAccess` AWS terkelola ke identitas IAM Anda untuk memberi mereka izin administratif penuh ke layanan Wickr, termasuk konsol administrator Wickr di. Konsol Manajemen AWS Untuk informasi selengkapnya, lihat AWS kebijakan terkelola: AWSWickr FullAccess.

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": "*"
        }
    ]
}
```

Memecahkan masalah identitas dan akses AWS Wickr

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

Topik

- Saya tidak berwenang untuk melakukan tindakan administratif di Konsol Manajemen AWS for Wickr

Saya tidak berwenang untuk melakukan tindakan administratif di Konsol Manajemen AWS for Wickr

Jika Konsol Manajemen AWS for Wickr memberi tahu Anda bahwa Anda tidak berwenang untuk melakukan suatu tindakan, maka Anda harus menghubungi administrator Anda untuk mendapatkan bantuan. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Contoh kesalahan berikut terjadi ketika pengguna `mateojackson` IAM mencoba menggunakan untuk Wickr Konsol Manajemen AWS untuk membuat, mengelola, atau melihat jaringan Wickr di Konsol Manajemen AWS untuk Wickr tetapi tidak memiliki izin dan. `wickr:CreateAdminSession` `wickr:ListNetworks`

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 wickr:ListNetworks
```

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk memungkinkannya mengakses Konsol Manajemen AWS untuk Wickr menggunakan dan tindakan. `wickr:CreateAdminSession` `wickr:ListNetworks` Untuk informasi selengkapnya, lihat Contoh kebijakan berbasis identitas untuk AWS Wickr dan AWS kebijakan terkelola: AWSWickr FullAccess.

Validasi kepatuhan

Untuk daftar AWS layanan dalam lingkup program kepatuhan tertentu, lihat AWS Layanan dalam Lingkup oleh AWS Layanan Program Kepatuhan . 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 Wickr ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan Panduan Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar yang berfokus pada keamanan dan kepatuhan. AWS
- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.

- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config; menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub CSPM— AWS Layanan ini memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS yang membantu Anda memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik.

Ketahanan di AWS Wickr

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur AWS Global.

Selain infrastruktur AWS global, Wickr menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan cadangan Anda. Untuk informasi selengkapnya, lihat Retensi data untuk AWS Wickr.

AWS PrivateLink untuk AWS Wickr

Dengan AWS PrivateLink AWS Wickr, Anda dapat membuat koneksi pribadi antara Virtual Private Cloud (VPC) dan subset titik akhir di AWS Wickr dengan menggunakan titik akhir VPC antarmuka. Endpoint VPC antarmuka didukung oleh AWS PrivateLink, sebuah AWS teknologi yang dapat Anda gunakan untuk mengakses layanan yang berjalan AWS dengan menggunakan alamat IP pribadi.

Untuk klien seluler atau perangkat lokal lainnya, gunakan VPN untuk menghubungkan perangkat Anda ke VPC untuk konektivitas pribadi ujung ke ujung. Untuk informasi selengkapnya, lihat Dokumentasi AWS Virtual Private Network.

Untuk informasi selengkapnya tentang AWS PrivateLink dan AWS VPC, lihat Apa itu? AWS PrivateLink dalam AWS PrivateLink Panduan dan Apa itu AWS VPC? di Panduan Pengguna Amazon Virtual Private Cloud.

Layanan AWS Wickr yang Didukung

Dukungan layanan AWS Wickr berikut: AWS PrivateLink

Layanan	Format Titik Akhir
AWS Wickr Admin	`com.amazonaws.` *`your-region`* `.wickr-admin`
Pesan AWS Wickr	`com.amazonaws.` *`your-region`* `.wickr-messaging`
AWS Wickr Panggilan	`com.amazonaws.` *`your-region`* `.wickr-calling`

Semua titik akhir VPC Wickr saat ini memerlukan Nama DNS Pribadi untuk diaktifkan. Untuk informasi selengkapnya, lihat Mengaktifkan nama DNS pribadi.

Titik Akhir VPC Wickr mendukung FIPS di wilayah di mana titik akhir Wickr publik mendukung FIPS. Untuk informasi selengkapnya, lihat Standar Pemrosesan Informasi Federal.

Saat Ini Tidak Didukung

- Kebijakan titik akhir VPC untuk titik akhir Pesan dan Panggilan
- Titik akhir Perpesanan dan Panggilan tidak tersedia di`us-east-1`.

Topik

Prasyarat

Sebelum membuat titik akhir VPC, pastikan Anda memiliki prasyarat berikut:

1. Konfigurasi VPC: VPC yang dikonfigurasi dengan benar dengan subnet di beberapa Availability Zone
2. Grup Keamanan: Grup keamanan yang sesuai yang memungkinkan lalu lintas HTTPS (port 443)
3. Resolusi DNS: Nama host DNS dan resolusi DNS diaktifkan di VPC
4. Izin IAM: Izin yang diperlukan untuk membuat dan mengelola titik akhir VPC

Buat VPC endpoint

Anda dapat membuat titik akhir VPC untuk AWS Wickr Admin, Messaging, dan Calling.

Selesaikan prosedur berikut untuk membuat titik akhir VPC menggunakan Console. AWS

Langkah 1: Arahkan ke Konsol VPC

1. Masuk ke Konsol VPC Amazon.
2. Pada panel navigasi kiri, pilih Titik Akhir.
3. Pilih Buat Titik Akhir.

Langkah 2: Konfigurasikan Pengaturan Titik Akhir

1. Di bawah Kategori Layanan, pilih AWS layanan.
2. Di bawah Nama Layanan, cari `wickr` dan pilih layanan yang sesuai:
   - Untuk Admin: `com.amazonaws.`*`your-region`*`.wickr-admin`
   - Untuk Pesan: `com.amazonaws.`*`your-region`*`.wickr-messaging`
   - Untuk Menelepon: `com.amazonaws.`*`your-region`*`.wickr-calling`

Langkah 3: Konfigurasi Jaringan

1. Di bawah VPC, pilih VPC target Anda.
2. Di bawah Subnet, pilih subnet di beberapa Availability Zone untuk ketersediaan tinggi.
3. Di bawah Aktifkan nama DNS pribadi, pilih kotak centang. Ini memungkinkan dukungan untuk nama DNS pribadi.
4. Di bawah Grup Keamanan, pilih atau buat grup keamanan yang ingin Anda kaitkan dengan antarmuka jaringan titik akhir.

Langkah 4: Buat Endpoint

1. Tinjau konfigurasi Anda.
2. Secara opsional, Anda dapat menambah atau menghapus tag. Tag adalah pasangan nama-nilai yang Anda gunakan untuk mengasosiasikan dengan titik akhir Anda.
3. Pilih Buat Titik Akhir.

Selesaikan prosedur berikut untuk membuat titik akhir VPC menggunakan. AWS CLI

1. Periksa ketersediaan layanan di wilayah Anda:

   Periksa ketersediaan Admin Wickr

   ```
   aws ec2 describe-vpc-endpoint-services --service-names com.amazonaws.your-region.wickr-admin
   ```

   Periksa ketersediaan Pesan Wickr

   ```
   aws ec2 describe-vpc-endpoint-services --service-names com.amazonaws.your-region.wickr-messaging
   ```

   Periksa ketersediaan Panggilan Wickr

   ```
   aws ec2 describe-vpc-endpoint-services --service-names com.amazonaws.your-region.wickr-calling
   ```

2. Buat titik akhir VPC.

   Titik Akhir Admin Wickr:

   ```
   aws ec2 create-vpc-endpoint \
     --vpc-endpoint-type Interface \
     --service-name com.amazonaws.your-region.wickr-admin \
     --subnet-ids subnet-12345678 subnet-87654321 subnet-11223344 \
     --vpc-id vpc-12345678 \
     --security-group-ids sg-12345678 \
     --private-dns-enabled \
   ```

Titik Akhir Pesan Wickr

```
aws ec2 create-vpc-endpoint \
  --vpc-endpoint-type Interface \
  --service-name com.amazonaws.your-region.wickr-messaging \
  --subnet-ids subnet-12345678 subnet-87654321 subnet-11223344 \
  --vpc-id vpc-12345678 \
  --security-group-ids sg-12345678 \
  --private-dns-enabled \
```

Titik Akhir Panggilan Wickr

```
aws ec2 create-vpc-endpoint \
  --vpc-endpoint-type Interface \
  --service-name com.amazonaws.your-region.wickr-calling \
  --subnet-ids subnet-12345678 subnet-87654321 subnet-11223344 \
  --vpc-id vpc-12345678 \
  --security-group-ids sg-12345678 \
  --private-dns-enabled \
```

Batasan

Fitur-fitur berikut tidak didukung melalui AWS PrivateLink dan memerlukan konektivitas internet:

- Akses Terbuka Wickr (WOA)
- Pembaruan Aplikasi Klien
  - Aplikasi Seluler (iOS/Android)
    - Sumber: App Store/Google Play Store
    - Persyaratan: Diperlukan akses internet
  - Aplikasi Desktop
    - Windows/Mac: Menggunakan titik akhir S3 global (tidak kompatibel) AWS PrivateLink
    - Linux: Menggunakan Snap Store (membutuhkan akses internet)
- Debugging dan Telemetri
  - Laporan kerusakan

    - Metrik debug
    - Tautan analitik sisi klien
- Pemberitahuan Push Seluler

  Layanan ini memerlukan konektivitas internet dan tidak dapat menggunakan AWS PrivateLink:

  - Pemberitahuan Push Apple
    - Persyaratan: Akses internet langsung
    - Pelabuhan: 443, 2195, 2196, 5223
    - Referensi: Dokumentasi Dukungan Apple
  - Pemberitahuan Google/Android
    - Persyaratan: Akses Firebase Cloud Messaging
    - Referensi: Dokumentasi Firebase
- AWS Wickr Console saat ini tidak didukung untuk Akses Pribadi. Untuk informasi selengkapnya, lihat Didukung Wilayah AWS, konsol layanan, dan fitur untuk Akses Pribadi.

Versi klien minimum yang diperlukan untuk AWS PrivateLink

Versi klien berikut telah divalidasi dengan AWS PrivateLink:

- iOS 6.64 (jika berlaku)
- Android 6.60 (jika berlaku)
- Klien desktop 6.60
- Bot 6.60

Fitur yang membutuhkan konfigurasi tambahan

Bot Wickr

- Persyaratan: Infrastruktur yang dikelola pelanggan
- Tindakan: Konfigurasikan jalur jaringan untuk dependensi bot
- Pertimbangan: Pastikan bot dapat mencapai AWS layanan yang diperlukan melalui titik akhir VPC

Unduhan File

- Konektivitas S3: Diperlukan untuk operasi file (kecuali wilayah Frankfurt)
- Solusi: Buat titik akhir gateway VPC S3
- Referensi: AWS PrivateLink untuk Amazon S3

Keamanan Infrastruktur di AWS Wickr

Sebagai layanan terkelola, AWS Wickr dilindungi oleh prosedur keamanan jaringan AWS global yang dijelaskan dalam whitepaper Amazon Web Services: Tinjauan Proses Keamanan.

Analisis konfigurasi dan kerentanan di AWS Wickr

Konfigurasi dan kontrol TI adalah tanggung jawab bersama antara AWS dan Anda, pelanggan kami. Untuk informasi selengkapnya, lihat model tanggung jawab AWS bersama.

Adalah tanggung jawab Anda untuk mengonfigurasi Wickr sesuai dengan spesifikasi dan pedoman, untuk secara berkala menginstruksikan pengguna Anda untuk mengunduh versi terbaru klien Wickr, untuk memastikan Anda menjalankan versi terbaru dari bot retensi data Wickr, dan untuk memantau penggunaan Wickr oleh pengguna Anda.

Praktik terbaik keamanan untuk AWS Wickr

Wickr menyediakan sejumlah fitur keamanan untuk dipertimbangkan saat Anda mengembangkan dan menerapkan kebijakan keamanan Anda sendiri. Praktik terbaik berikut adalah pedoman umum dan tidak mewakili solusi keamanan yang lengkap. Karena praktik terbaik ini mungkin tidak sesuai atau tidak memadai untuk lingkungan Anda, perlakukan itu sebagai pertimbangan yang bermanfaat, bukan sebagai resep.

Untuk mencegah potensi peristiwa keamanan yang terkait dengan penggunaan Wickr oleh Anda, ikuti praktik terbaik berikut ini:

- Terapkan akses hak istimewa paling sedikit dan buat peran khusus yang akan digunakan untuk tindakan Wickr. Gunakan template IAM untuk membuat peran. Untuk informasi selengkapnya, lihat AWS kebijakan terkelola untuk AWS Wickr.
- Akses Konsol Manajemen AWS untuk Wickr dengan mengautentikasi ke yang pertama. Konsol Manajemen AWS Jangan bagikan kredenal konsol pribadi Anda. Siapa pun di internet dapat menjelajah ke konsol, tetapi mereka tidak dapat masuk atau memulai sesi kecuali mereka memiliki kredensil yang valid ke konsol.

Pemantauan AWS Wickr

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

- 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, silakan lihat Panduan Pengguna AWS CloudTrail. Untuk informasi selengkapnya tentang pencatatan panggilan API Wickr menggunakan CloudTrail, lihat. Pencatatan panggilan AWS Wickr API menggunakan AWS CloudTrail

Pencatatan panggilan AWS Wickr API menggunakan AWS CloudTrail

AWS Wickr terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Wickr. CloudTrail menangkap semua panggilan API untuk Wickr sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari Konsol Manajemen AWS untuk Wickr dan panggilan kode ke operasi API Wickr. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk Wickr. 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 Wickr, 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 Wickr di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di Wickr, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan acara AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di Akun AWS Anda. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan Riwayat CloudTrail acara.

Untuk catatan acara yang sedang berlangsung di Anda Akun AWS, termasuk acara untuk Wickr, 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 Wickr dicatat oleh. CloudTrail Misalnya, panggilan ke`CreateAdminSession`, dan `ListNetworks` tindakan menghasilkan entri dalam file CloudTrail log.

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

- Apakah permintaan itu dibuat dengan 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 berkas log Wickr

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 `CreateAdminSession` tindakan.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T07:53:17Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-10T08:19:24Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "CreateAdminSession",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "networkId": 56019692
    },
    "responseElements": {
        "sessionCookie": "***",
        "sessionNonce": "***"
    },
    "requestID": "39ed0e6f-36e9-460d-8a6e-f24be0ec11c5",
    "eventID": "98ccb633-0e6c-4325-8996-35c3043022ac",
    "readOnly": false,
```

```
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `CreateNetwork` tindakan.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T07:53:17Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-10T07:54:09Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "CreateNetwork",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "networkName": "BOT_Network",
        "accessLevel": "3000"
    },
    "responseElements": null,
```

```
    "requestID": "b83c0b6e-73ae-45b6-8c85-9910f64d33a1",
    "eventID": "551277bb-87e0-4e66-b2a0-3cc1eff303f3",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `ListNetworks` tindakan.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T12:19:39Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-10T12:29:32Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "ListNetworks",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
```

```
    "requestID": "b9800ba8-541a-43d1-9c8e-efd94d5f2115",
    "eventID": "5fbc83d7-771b-457d-9329-f85163a6a428",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `UpdateNetworkdetails` tindakan.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T22:42:15Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-08T22:42:58Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "UpdateNetworkDetails",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
```

```
        "networkName": "CloudTrailTest1",
        "networkId": <network-id>
    },
    "responseElements": null,
    "requestID": "abced980-23c7-4de1-b3e3-56aaf0e1fdbb",
    "eventID": "a4dc3391-bdce-487d-b9b0-6f76cedbb198",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `TagResource` tindakan.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T22:42:15Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-08T23:06:04Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
```

```
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "resource-arn": "<arn>",
        "tags": {
            "some-existing-key-3": "value 1"
        }
    },
    "responseElements": null,
    "requestID": "4ff210e1-f69c-4058-8ac3-633fed546983",
    "eventID": "26147035-8130-4841-b908-4537845fac6a",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `ListTagsForResource` tindakan.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<access-key-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T18:50:37Z",
                "mfaAuthenticated": "false"
            }
        }
```

```
    },
    "eventTime": "2023-03-08T18:50:37Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "ListTagsForResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "axios/0.27.2",
    "errorCode": "AccessDenied",
    "requestParameters": {
        "resource-arn": "<arn>"
    },
    "responseElements": {
        "message": "User: <arn> is not authorized to perform: wickr:ListTagsForResource
 on resource: <arn> with an explicit deny"
    },
    "requestID": "c7488490-a987-4ca2-a686-b29d06db89ed",
    "eventID": "5699d5de-3c69-4fe8-b353-8ae62f249187",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

Dasbor analitik di AWS Wickr

Anda dapat menggunakan dasbor analitik untuk melihat bagaimana organisasi Anda menggunakan AWS Wickr. Prosedur berikut menjelaskan cara mengakses dasbor analitik dengan menggunakan konsol AWS Wickr.

Untuk mengakses dasbor analitik

1. Buka Konsol Manajemen AWS untuk Wickr di. https://console.aws.amazon.com/wickr/
2. Pada halaman Jaringan, pilih nama jaringan untuk menavigasi ke jaringan itu.
3. Di panel navigasi, pilih Analytics.

   Halaman Analytics menampilkan metrik untuk jaringan Anda di tab yang berbeda.

Pada halaman Analytics, Anda akan menemukan filter kerangka waktu di sudut kanan atas setiap tab. Filter ini berlaku untuk seluruh halaman. Selain itu, di sudut kanan atas setiap tab, Anda dapat mengekspor titik data untuk rentang waktu yang dipilih dengan memilih opsi Ekspor yang tersedia.

> **Note**
>
> Waktu yang dipilih adalah dalam UTC (Universal Time Coordinated).

Tab berikut tersedia:

- Ikhtisar menampilkan:
  - Terdaftar — Jumlah total pengguna terdaftar, termasuk pengguna aktif dan ditangguhkan di jaringan dalam waktu yang dipilih. Itu tidak termasuk pengguna yang tertunda atau diundang.
  - Pending — Jumlah total pengguna yang tertunda di jaringan dalam waktu yang dipilih.
  - Pendaftaran Pengguna - Grafik menampilkan jumlah total pengguna yang terdaftar dalam rentang waktu yang dipilih.
  - Perangkat — Jumlah perangkat tempat aplikasi aktif.
  - Versi Klien — Jumlah perangkat aktif yang dikategorikan berdasarkan versi klien mereka.

- Anggota menampilkan:
  - Status — Pengguna aktif di jaringan dalam jangka waktu yang dipilih.
  - Pengguna aktif -
    - Grafik menampilkan jumlah pengguna aktif dari waktu ke waktu dan dapat dikumpulkan berdasarkan harian, mingguan atau bulanan (dalam rentang waktu yang dipilih di atas).
    - Jumlah pengguna aktif dapat dipecah berdasarkan Platform, Versi Klien, atau Grup Keamanan. Jika grup keamanan dihapus, jumlah total akan ditampilkan sebagai Deleted#.

- Pesan menampilkan:
  - Pesan terkirim — Jumlah pesan unik yang dikirim oleh semua pengguna dan bot di jaringan dalam periode waktu yang dipilih.
  - Panggilan — Jumlah panggilan unik yang dilakukan oleh semua pengguna di jaringan.
  - File — Jumlah file yang dikirim oleh pengguna dalam jaringan (termasuk memo suara).

- Perangkat — Diagram lingkaran menampilkan jumlah perangkat aktif yang dikategorikan berdasarkan sistem operasinya.
- Versi Klien — Jumlah perangkat aktif yang dikategorikan berdasarkan versi klien mereka.

Riwayat dokumen

Tabel berikut menjelaskan rilis dokumentasi untuk Wickr.

Perubahan	Deskripsi	Tanggal
Pratinjau file sekarang tersedia	Administrator Wickr sekarang memiliki kemampuan untuk mengaktifkan atau menonaktifkan unduhan file. Untuk informasi selengkapnya, lihat Pratinjau file untuk AWS Wickr.	29 Mei 2025
Konsol administrator Wickr yang baru didesain ulang sekarang tersedia	Wickr telah meningkatkan konsol administrator Wickr untuk navigasi yang lebih baik dan peningkatan aksesibilitas bagi administrator.	13 Maret 2025
Wickr sekarang tersedia di Asia Pasifik (Malaysia) AWS Region	Wickr sekarang tersedia di Asia Pasifik (Malaysia). AWS Region Untuk informasi selengkapnya, lihat Ketersediaan regional.	November 20, 2024
Hapus jaringan sekarang tersedia	Administrator Wickr sekarang memiliki kemampuan untuk menghapus jaringan AWS Wickr. Untuk informasi selengkapnya, lihat Menghapus jaringan di AWS Wickr.	Oktober 4, 2024
Mengkonfigurasi AWS Wickr dengan Microsoft Entra (Azure AD) SSO sekarang tersedia	AWS Wickr dapat dikonfigurasi untuk menggunakan Microsoft Entra (Azure AD) sebagai	September 18, 2024

	penyedia identitas. Untuk informasi selengkapnya, lihat Mengonfigurasi AWS Wickr dengan sistem masuk tunggal Microsoft Entra (Azure AD).	
Wickr sekarang tersedia di Eropa (Zurich) AWS Region	Wickr sekarang tersedia di Eropa (Zurich). AWS Region Untuk informasi selengkapnya, lihat Ketersediaan regional.	Agustus 12, 2024
Klasifikasi dan federasi Lintas Batas sekarang tersedia	Fitur klasifikasi lintas batas memungkinkan perubahan antarmuka pengguna untuk percakapan bagi GovCloud pengguna. Untuk informasi lebih lanjut, lihat klasifikasi dan federasi GovCloud lintas batas.	Juni 25, 2024
Fitur tanda terima baca sekarang tersedia	Administrator Wickr sekarang dapat mengaktifkan atau menonaktifkan fitur tanda terima baca di Konsol Administrator. Untuk informasi selengkapnya, lihat Membaca tanda terima.	April 23, 2024

Federasi Global sekarang mendukung federasi terbatas dan administrator dapat melihat analisis penggunaan di Konsol Administrator	Federasi Global sekarang mendukung federasi terbatas. Ini berfungsi untuk jaringan Wickr di jaringan lain. Wilayah AWS Untuk informasi selengkapnya, lihat Grup keamanan. Selain itu, administrator sekarang dapat melihat analisis penggunaan mereka di dasbor Analytics di Konsol Admin. Untuk informasi selengkapnya, lihat dasbor Analytics.	Maret 28, 2024
Uji coba gratis tiga bulan untuk paket Premium AWS Wickr sekarang tersedia	Administrator Wickr sekarang dapat memilih paket Premium uji coba gratis tiga bulan untuk hingga 30 pengguna. Selama uji coba gratis, semua fitur paket Standar dan Premium tersedia, termasuk kontrol admin tak terbatas dan retensi data. Fitur pengguna tamu tidak tersedia selama uji coba gratis Premium. Untuk informasi selengkapnya, lihat Mengelola paket.	Februari 9, 2024

Fitur pengguna tamu umumnya tersedia dan lebih banyak kontrol administrator telah ditambahkan	Administrator Wickr sekarang dapat mengakses berbagai fitur baru, termasuk daftar pengguna tamu, kemampuan untuk menghapus atau menangguhkan pengguna secara massal, dan opsi untuk memblokir pengguna tamu agar tidak berkomunikasi di jaringan Wickr Anda. Untuk informasi selengkapnya, lihat Pengguna tamu.	8 November 2023
Wickr sekarang tersedia di Eropa (Frankfurt) AWS Region	Wickr sekarang tersedia di Eropa (Frankfurt). AWS Region Untuk informasi selengkapnya, lihat Ketersediaan regional.	26 Oktober 2023
Jaringan Wickr sekarang memiliki kemampuan untuk berfederasi Wilayah AWS	Jaringan Wickr sekarang memiliki kemampuan untuk berfederasi. Wilayah AWS Untuk informasi selengkapnya, lihat Grup keamanan.	September 29, 2023
Wickr sekarang tersedia di Eropa (London) AWS Region	Wickr sekarang tersedia di Eropa (London). AWS Region Untuk informasi selengkapnya, lihat Ketersediaan regional.	23 Agustus 2023
Wickr sekarang tersedia di Kanada (Tengah) AWS Region	Wickr sekarang tersedia di Kanada (Tengah). AWS Region Untuk informasi selengkapnya, lihat Ketersediaan regional.	3 Juli 2023

Fitur pengguna tamu sekarang tersedia untuk pratinjau	Pengguna tamu dapat masuk ke klien Wickr dan berkolaborasi dengan pengguna jaringan Wickr. Untuk informasi selengkapnya, lihat Pengguna tamu (pratinjau).	31 Mei 2023
AWS Wickr sekarang terintegrasi dengan AWS CloudTrail, dan sekarang tersedia di AWS GovCloud (AS-Barat) sebagai WickrGov	AWS Wickr sekarang terintegrasi dengan. AWS CloudTrail Untuk informasi selengkapnya, lihat Mencatat panggilan AWS Wickr API menggunakan. AWS CloudTrail Selain itu, Wickr sekarang tersedia di AWS GovCloud (AS-Barat) sebagai. WickrGov Untuk informasi selengkapnya, lihat AWS WickrGov di AWS GovCloud (US) Panduan Pengguna.	30 Maret 2023
Penandaan dan pembuatan beberapa jaringan	Penandaan sekarang didukung di AWS Wickr. Untuk informasi selengkapnya, lihat Tag jaringan. Beberapa jaringan sekarang dapat dibuat di Wickr. Untuk informasi selengkapnya, lihat Membuat jaringan.	7 Maret 2023
Rilis awal	Rilis awal Panduan Administrasi Wickr	28 November 2022

Catatan rilis

Untuk membantu Anda melacak pembaruan dan peningkatan yang sedang berlangsung pada Wickr, kami menerbitkan pemberitahuan rilis yang menjelaskan perubahan terbaru.

Agustus 2025

- Template email untuk AWS Wickr dan AWS WickrGov telah diperbarui untuk meningkatkan pengalaman orientasi pengguna. Alamat email pengirim telah berubah dari `donotreply@wickr.email` menjadi`no-reply@amazonaws.com`.

Mei 2025

- Pratinjau file sekarang tersedia. Ketika unduhan file dinonaktifkan oleh admin di konsol admin untuk grup keamanan, pengguna hanya akan dapat melihat daftar file yang didukung di tab Pesan dan File.

Maret 2025

- Konsol administrator Wickr yang didesain ulang sekarang tersedia.

Oktober 2024

- Wickr sekarang mendukung jaringan hapus. Untuk informasi selengkapnya, lihat Menghapus jaringan di AWS Wickr.

September 2024

- Administrator sekarang dapat mengonfigurasi AWS Wickr dengan sistem masuk tunggal Microsoft Entra (Azure AD). Untuk informasi selengkapnya, lihat Mengonfigurasi AWS Wickr dengan sistem masuk tunggal Microsoft Entra (Azure AD).

Agustus 2024

- Penyempurnaan
  - Wickr sekarang tersedia di Eropa (Zurich). AWS Region

Juni 2024

- Klasifikasi dan federasi Lintas Batas sekarang tersedia untuk GovCloud pengguna. Untuk informasi lebih lanjut, lihat klasifikasi dan federasi GovCloud lintas batas.

April 2024

- Wickr sekarang mendukung tanda terima baca. Untuk informasi selengkapnya, lihat Membaca tanda terima.

Maret 2024

- Federasi Global sekarang mendukung federasi terbatas, di mana federasi global hanya dapat diaktifkan untuk jaringan tertentu yang ditambahkan di bawah federasi terbatas. Ini berfungsi untuk jaringan Wickr di jaringan lain. Wilayah AWS Untuk informasi selengkapnya, lihat Grup keamanan.
- Administrator sekarang dapat melihat analisis penggunaan mereka di dasbor Analytics di Konsol Admin. Untuk informasi selengkapnya, lihat dasbor Analytics.

Februari 2024

- AWS Wickr sekarang menawarkan uji coba gratis tiga bulan paket Premium-nya untuk hingga 30 pengguna. Perubahan dan batasan meliputi:
  - Semua fitur paket Standar dan Premium seperti kontrol admin tak terbatas dan retensi data sekarang tersedia dalam uji coba gratis Premium. Fitur pengguna tamu tidak tersedia selama uji coba gratis Premium.
  - Uji coba gratis sebelumnya tidak lagi tersedia. Anda dapat meningkatkan uji coba Gratis atau paket Standar yang ada ke uji coba gratis Premium jika Anda belum menggunakan uji coba gratis Premium. Untuk informasi selengkapnya, lihat Mengelola paket.

November 2023

- Fitur pengguna tamu sekarang tersedia secara umum. Perubahan dan penambahan meliputi:
  - Kemampuan untuk melaporkan penyalahgunaan oleh pengguna Wickr lainnya.
  - Administrator dapat melihat daftar pengguna tamu yang berinteraksi dengan jaringan, dan jumlah penggunaan bulanan.
  - Administrator dapat memblokir pengguna tamu dari berkomunikasi dengan jaringan mereka.
  - Harga tambahan untuk pengguna tamu.

- Penyempurnaan kontrol admin
  - Kemampuan untuk delete/suspend pengguna massal.
  - Pengaturan SSO tambahan untuk mengonfigurasi masa tenggang untuk penyegaran token.

Oktober 2023

- Penyempurnaan
  - Wickr sekarang tersedia di Eropa (Frankfurt). AWS Region

September 2023

- Penyempurnaan
  - Jaringan Wickr sekarang memiliki kemampuan untuk berfederasi. Wilayah AWS Untuk informasi selengkapnya, lihat Grup keamanan.

Agustus 2023

- Penyempurnaan
  - Wickr sekarang tersedia di Eropa (London). AWS Region

Juli 2023

- Penyempurnaan

- Wickr sekarang tersedia di Kanada (Tengah). AWS Region

Mei 2023

- Penyempurnaan
  - Menambahkan dukungan untuk pengguna tamu. Untuk informasi selengkapnya, lihat Pengguna tamu di jaringan AWS Wickr.

Maret 2023

- Wickr sekarang terintegrasi dengan. AWS CloudTrail Untuk informasi selengkapnya, lihat Pencatatan panggilan AWS Wickr API menggunakan AWS CloudTrail.
- Wickr sekarang tersedia di AWS GovCloud (AS-Barat) sebagai. WickrGov Untuk informasi selengkapnya, lihat AWS WickrGov di AWS GovCloud (US) Panduan Pengguna.
- Wickr sekarang mendukung penandaan. Untuk informasi selengkapnya, lihat Tag jaringan untuk AWS Wickr. Beberapa jaringan sekarang dapat dibuat di Wickr. Untuk informasi selengkapnya, lihat Langkah 1: Buat jaringan.

Februari 2023

- Wickr sekarang mendukung Android Tactical Assault Kit (ATAK). Untuk informasi selengkapnya, lihat Aktifkan ATAK di Dasbor Jaringan Wickr.

Januari 2023

- Single sign-on (SSO) sekarang dapat dikonfigurasi pada semua paket, termasuk Uji Coba Gratis dan Standar.

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