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 AWS Management Console, 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 pada 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 AWS Management Console, 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 5GB dengan penyimpanan tak terbatas
- Ephemeral: Kontrol kedaluwarsa dan pengatur waktu burn-on-read
- Federasi global: Terhubung dengan pengguna Wickr di luar jaringan Anda

> **Note**
>
> Jaringan Wickr di AWS GovCloud (AS-Barat) hanya dapat difederasi dengan jaringan Wickr lainnya di (AS-Barat). AWS GovCloud

Mengakses Wickr

Wickr tersedia di AS Timur (Virginia N.), Kanada (Tengah), Eropa (London), Asia Pasifik (Sydney), Eropa (Frankfurt), Eropa (Stockholm), Asia Pasifik (Singapura), dan Asia Pasifik (Tokyo). Wilayah AWS Wickr juga tersedia seperti WickrGov di AWS GovCloud (AS-Barat). Wilayah AWS

Administrator mengakses AWS Management Console 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.

> **Note**
>
> Layanan Wickr tidak memiliki antarmuka pemrograman aplikasi (API).

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

Daftar untuk AWS

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

Untuk mendaftar Akun AWS

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

   Anda akan diminta untuk menerima panggilan telepon dan memasukkan kode verifikasi pada keypad telepon sebagai bagian dari prosedur pendaftaran.

   Saat Anda mendaftar Akun AWS, Pengguna root akun AWS akan dibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya dalam akun. Sebagai praktik terbaik keamanan, tetapkan akses administratif ke pengguna administratif, dan hanya gunakan 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 InterfacePanduan 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: AWSWickrFullAccess.

Apa selanjutnya

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

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: AWSWickrFullAccess.
- Pastikan Anda mengizinkan daftar port dan domain yang sesuai untuk Wickr. Untuk informasi selengkapnya, lihat Port dan domain untuk mengizinkan daftar.

Langkah 1: Buat jaringan

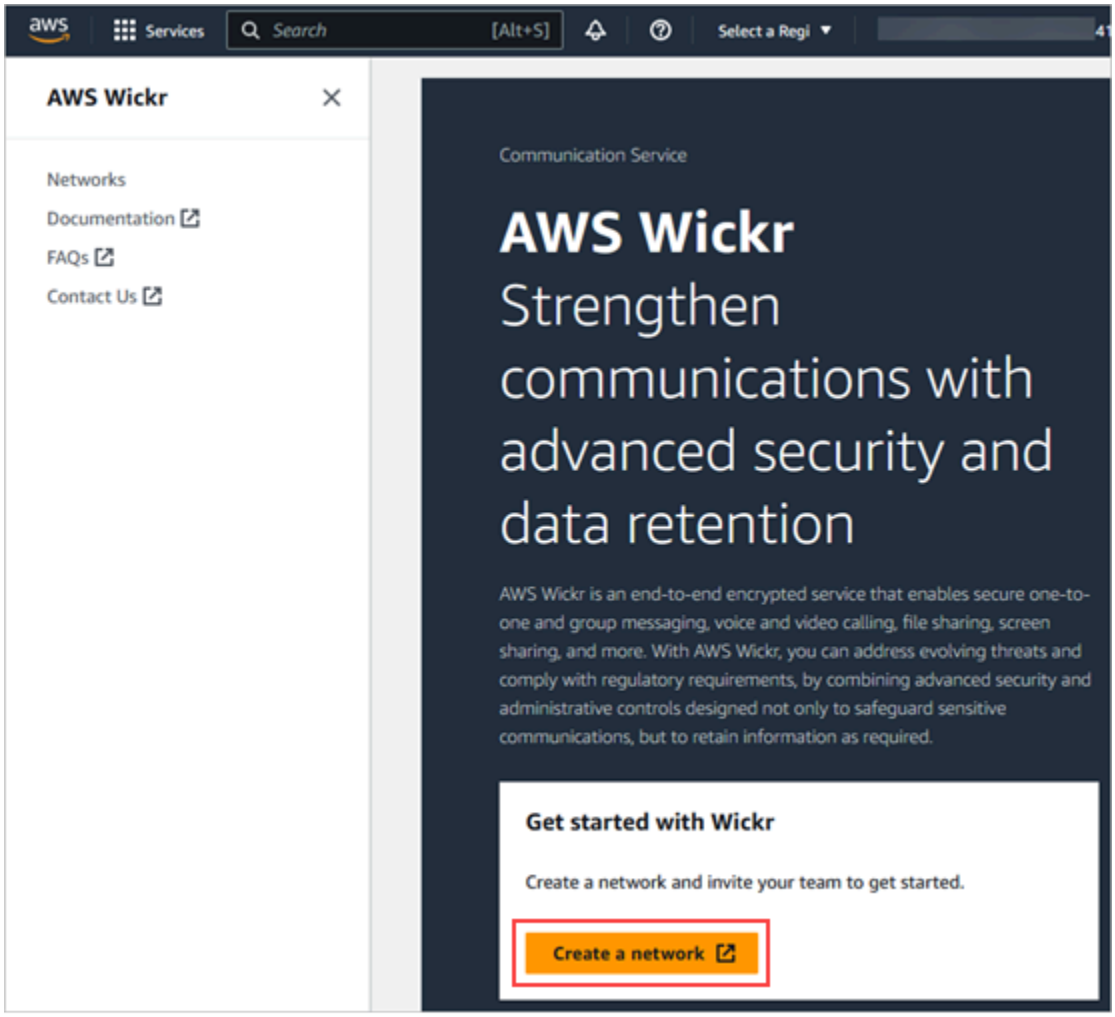
Selesaikan prosedur berikut untuk membuat jaringan Wickr untuk akun Anda.

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.

> **Note**
>
> Jika Anda belum 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 dapat memilih opsi uji coba gratis premium, yang tersedia hingga 30 pengguna dan berlangsung selama tiga bulan. Penawaran ini terbuka untuk uji coba baru, bebas warisan, dan paket standar. Administrator dapat meningkatkan atau menurunkan versi ke paket Premium atau Standar selama periode uji coba gratis premium.

Untuk informasi selengkapnya tentang paket dan harga Wickr yang tersedia, lihat halaman harga Wickr.

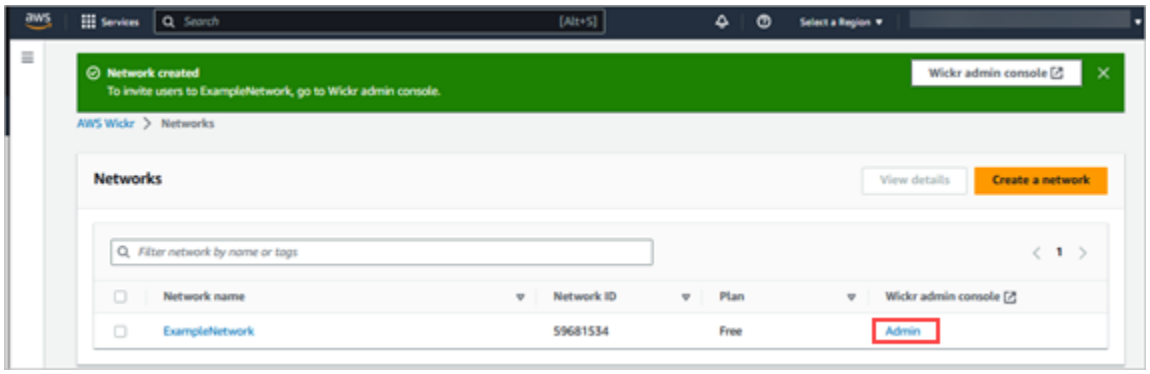
5. (Opsional) Pilih Tambahkan tag baru untuk menambahkan tag ke jaringan Anda. Tag terdiri dari pasangan nilai kunci. Tag dapat digunakan untuk mencari dan memfilter sumber daya atau melacak AWS biaya Anda. Untuk informasi selengkapnya, lihat Mengelola tag jaringan.
6. Pilih Buat Jaringan.

   Anda diarahkan ke halaman Jaringan AWS Management Console untuk Wickr, dan jaringan baru tercantum di halaman.

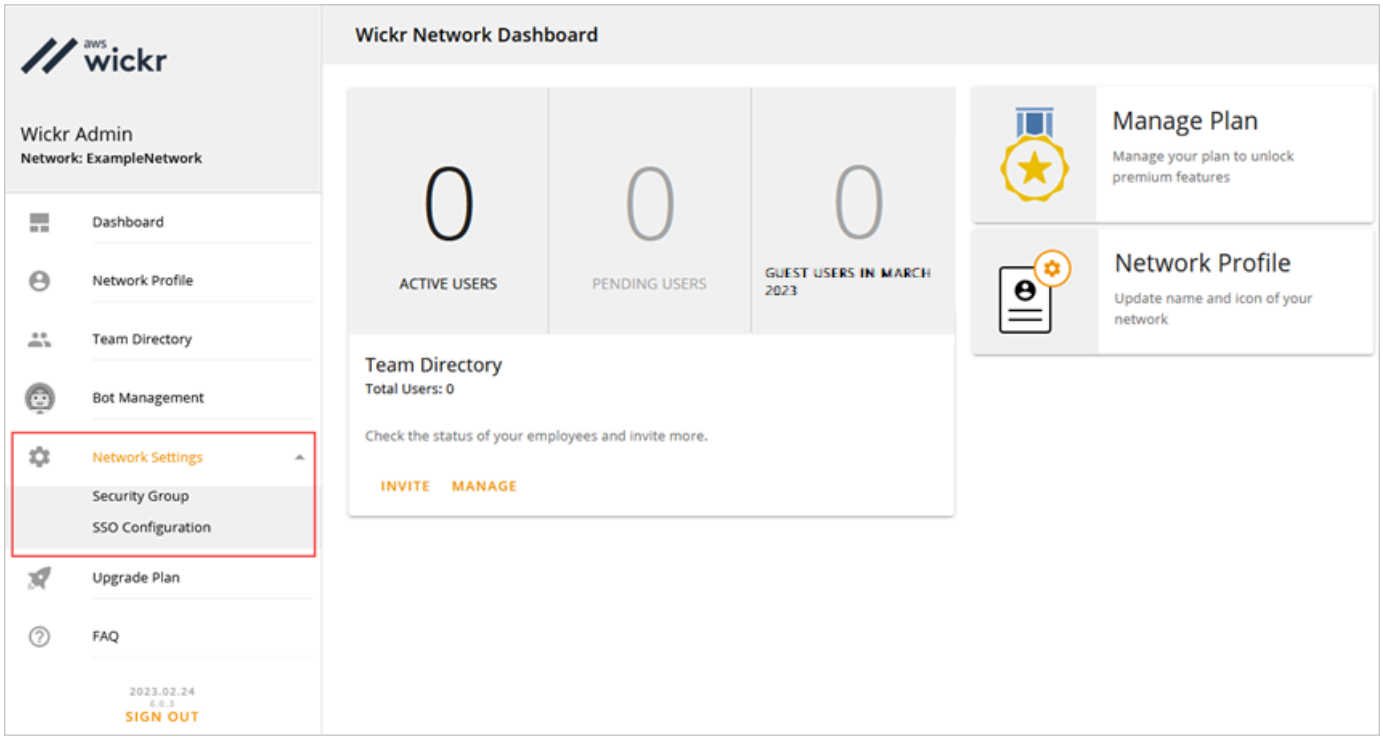
Langkah 2: Konfigurasikan jaringan Anda

Selesaikan prosedur berikut untuk mengakses Konsol Admin Wickr, tempat Anda dapat menambahkan pengguna, menambahkan grup keamanan, mengonfigurasi SSO, mengonfigurasi retensi data, dan pengaturan jaringan tambahan.

1. Pada halaman Jaringan, pilih tautan Admin, untuk menavigasi ke Konsol Admin Wickr untuk jaringan tersebut.



   Anda dialihkan ke Konsol Admin Wickr untuk jaringan yang dipilih.
2. Di panel navigasi Konsol Admin Wickr, pilih Pengaturan Jaringan.



Opsi pengaturan jaringan 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.
- Konfigurasi 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.

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.

- Undangan - Anda dapat secara manual membuat pengguna di AWS Management Console 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. Fitur pengguna tamu saat ini dalam pratinjau. Lihat informasi yang lebih lengkap di Pengguna tamu

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.

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.
- Alamat email yang harus mereka gunakan untuk mendaftar.
- URL untuk mengunduh klien Wickr. Pengguna dapat mengunduh klien Wickr dari halaman unduhan AWS Wickr di https://aws.amazon.com/wickr/download/.

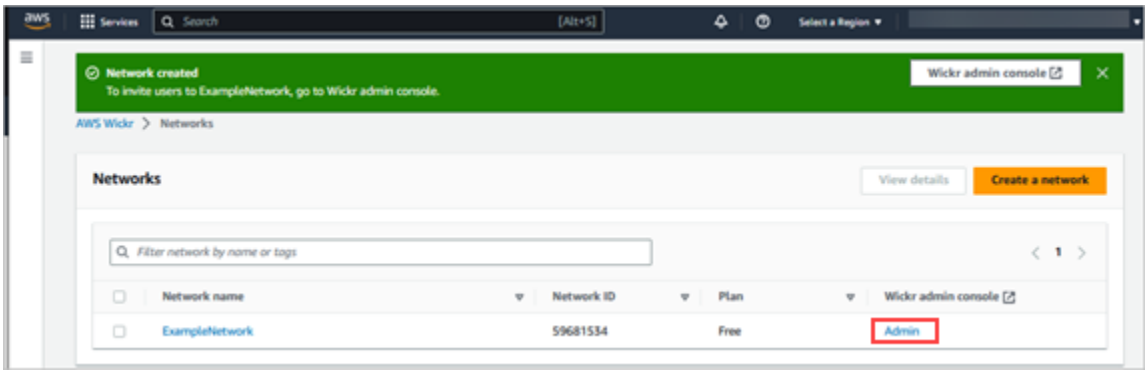
> **Note**
>
> Jika Anda membuat jaringan Wickr Anda di AWS GovCloud (US-Barat), instruksikan pengguna Anda untuk mengunduh dan menginstal klien. WickrGov Untuk semua AWS Wilayah lainnya, instruksikan pengguna Anda untuk mengunduh dan menginstal klien Wickr standar. Untuk informasi selengkapnya AWS WickrGov,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

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

Non-SSO

Untuk membuat pengguna Wickr secara manual dan mengirim undangan:

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Pada halaman Jaringan, pilih tautan Admin, untuk menavigasi ke Konsol Admin Wickr untuk jaringan tersebut.

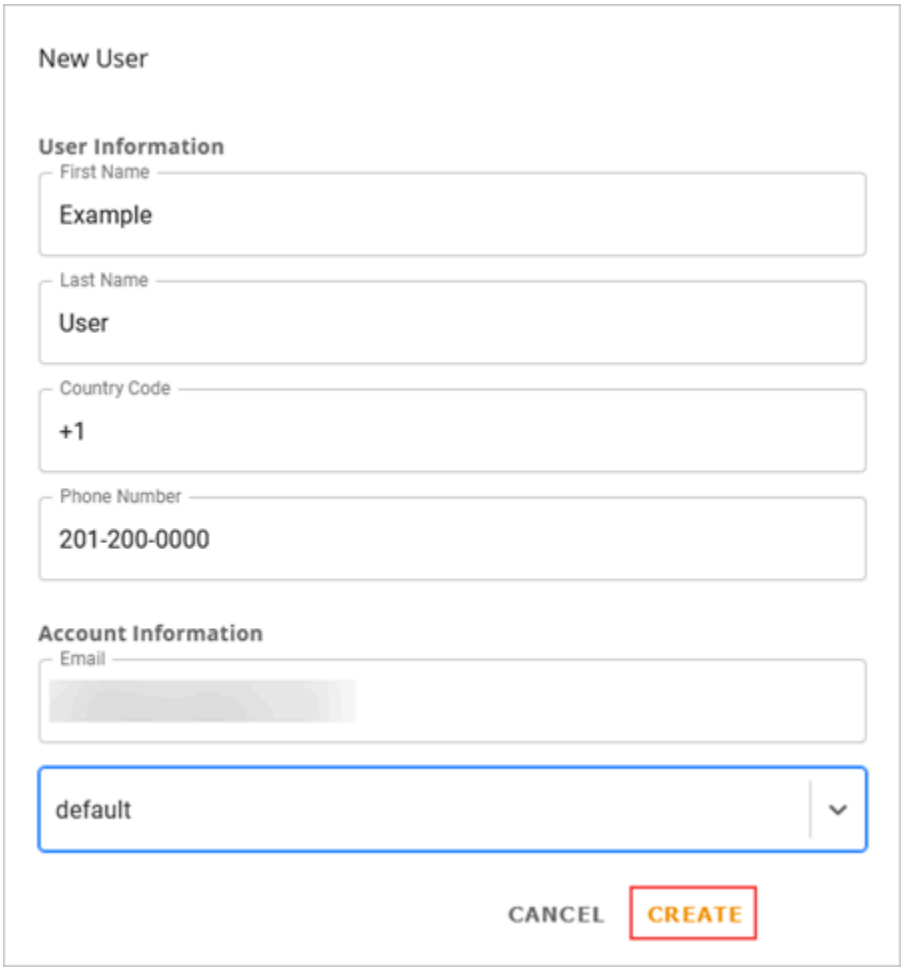


Halaman Jaringan.

Anda diarahkan ke Konsol Admin Wickr untuk jaringan tertentu. Di Konsol Admin Wickr, Anda dapat menambahkan pengguna, menambahkan grup keamanan, mengonfigurasi SSO, mengonfigurasi penyimpanan data, dan pengaturan tambahan untuk jaringan tertentu yang Anda pilih.

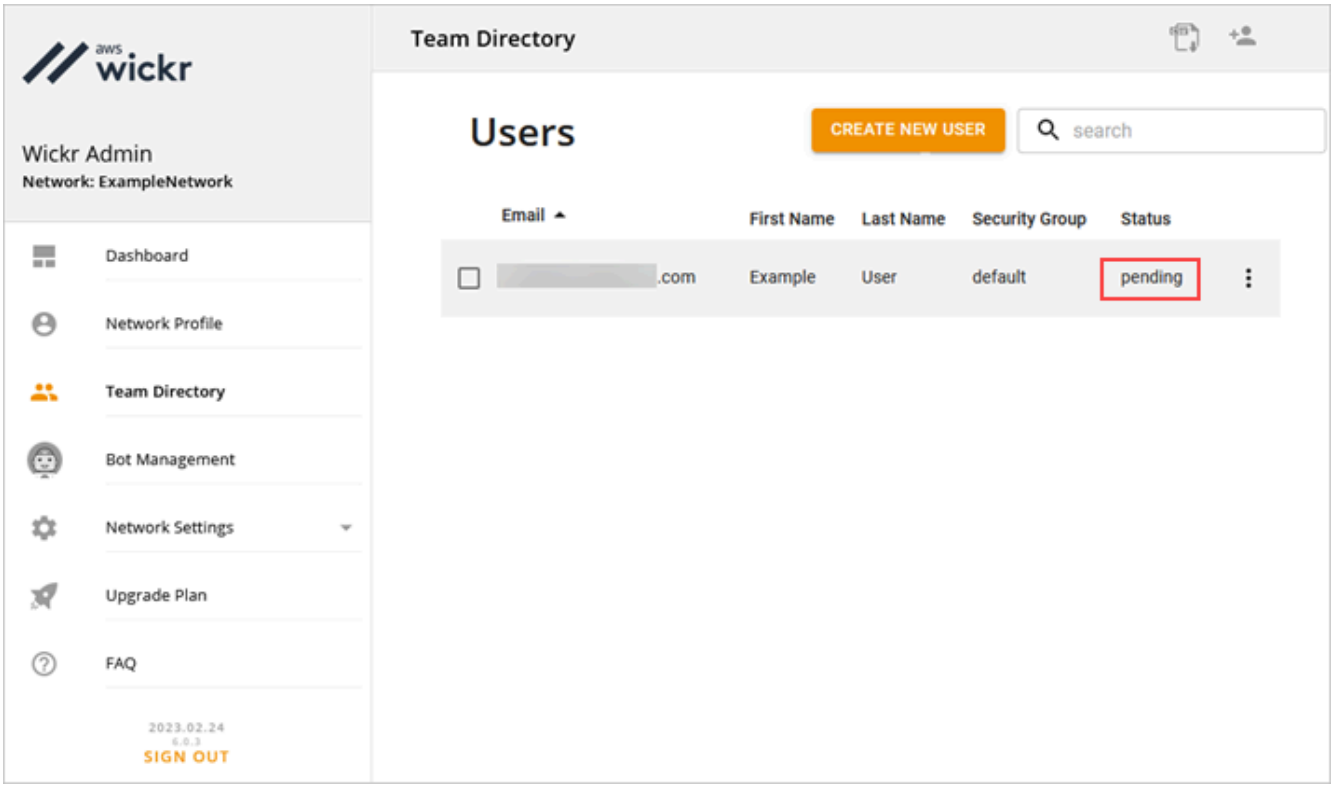
3. Di panel navigasi Konsol Admin Wickr, pilih Pengguna, lalu pilih Direktori Tim.

   Di halaman Pengguna, Anda dapat menambahkan pengguna individual dengan memilih Buat pengguna baru. Anda juga dapat menambahkan pengguna secara massal dengan memilih ikon Tambah pengguna di panel navigasi atas. Pilih ikon Unduh CSV untuk mengunduh templat CSV yang dapat Anda edit dan unggah dengan daftar pengguna Anda.
4. 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.
5. Pilih Buat.



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 panduan berikut:

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

Transfer Wickr Pro ke AWS Wickr

> **Note**
>
> Wickr Pro akan dihentikan pada 27 Maret 2024.

Dalam panduan ini, kami menunjukkan cara Anda mentransfer dari Wickr Pro dan mulai menggunakan AWS Wickr.

Ikuti langkah-langkah dalam panduan ini jika Anda memiliki jaringan Wickr Pro yang ada, tetapi JANGAN memilikinya. Akun AWS Silakan hubungi dukungan pada langkah apa pun jika Anda membutuhkan bantuan.

Jika organisasi Anda sudah memiliki AWS akun, lengkapi formulir Migrasi dari Wickr Pro ke AWS Wickr dan dukungan AWS Wickr akan membantu Anda.

Anda akan memerlukan Akun AWS ID untuk mengelola jaringan AWS Wickr Anda sebagai file. Layanan AWSUntuk informasi selengkapnya tentang apa Akun AWS itu, dan cara mengelola akun, lihat Panduan Referensi ManajemenAWS Akun.

Topik

Langkah 1: Buat AWS akun

Selesaikan prosedur berikut untuk membuat AWS akun.

1. Jika organisasi Anda tidak memiliki ID Akun AWS yang ada, Anda dapat memulai dengan membuat ID AWS akun mandiri. Beberapa hal penting yang Anda perlukan untuk ini:

   - Kartu kredit/debit untuk penagihan
   - Alamat email yang dapat diakses oleh grup (Direkomendasikan, tidak wajib)
   - Pilih AWS Support rencana. Untuk informasi selengkapnya, lihat Mengubah AWS Support Paket.

   > **Note**
   >
   > Anda selalu dapat mengubah AWS Support rencana Anda saat Anda mempelajari lebih lanjut tentang kebutuhan Anda.

2. Siapkan akses administratif melalui IAM sebagai praktik terbaik keamanan (opsional tetapi disarankan). Untuk informasi selengkapnya, lihat AWS Identity and Access Management. Untuk

petunjuk lebih spesifik tentang akses administratif AWS Wickr, lihat kebijakanAWS terkelola:. AWSWickrFullAccess

3. Setelah Anda menyelesaikan langkah-langkah sebelumnya, Anda akan dapat masuk ke AWS Management Console untuk menemukan Akun AWS ID 12 digit Anda di bawah nama akun Anda.

Langkah 2: Ambil ID jaringan Wickr Anda

Selesaikan prosedur berikut untuk mengambil ID jaringan Wickr Anda.

1. Masuk ke konsol admin Wickr Anda saat ini, dan pilih jaringan yang ingin Anda migrasikan, lalu pilih Profil Jaringan.
2. Halaman Profil Jaringan menampilkan ID jaringan Anda dan merupakan ID numerik 8 digit.

Langkah 3: Kirim permintaan

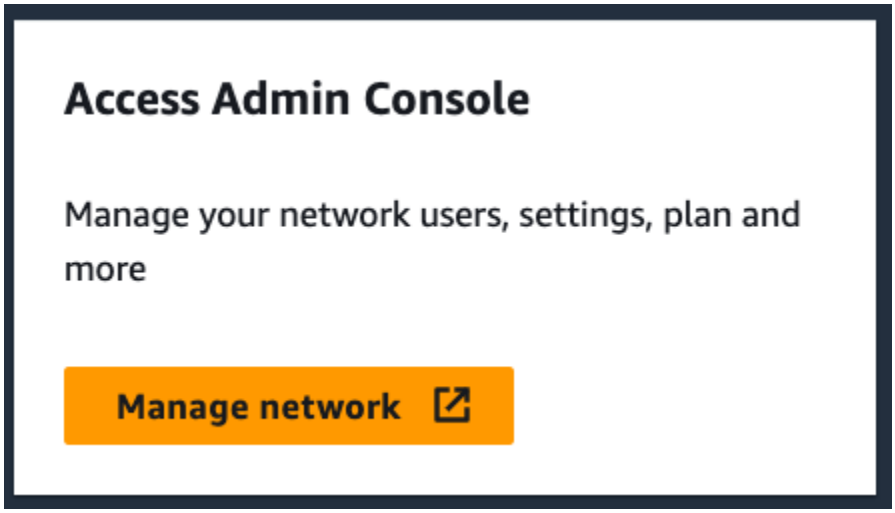
Sekarang setelah Anda memiliki Akun AWS ID dan ID jaringan Wickr Pro, Anda harus melengkapi formulir Migrasi dari Wickr Pro ke AWS Wickr.

Ketika selesai, biasanya dalam 14 hari, perwakilan dukungan AWS Wickr akan menghubungi Anda untuk mengonfirmasi bahwa jaringan Wickr Anda telah ditambahkan ke jaringan Anda. Akun AWS

Langkah 4: Masuk ke AWS Konsol Anda

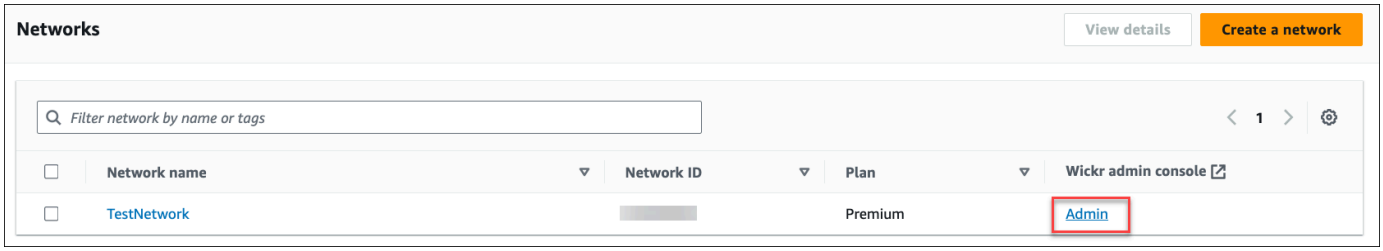
> **Note**
>
> Ikuti langkah-langkah ini SETELAH Anda menerima konfirmasi bahwa jaringan Wickr Pro Anda telah ditambahkan ke jaringan Anda. Akun AWS

1. Anda dapat masuk ke AWS konsol sebagai pengguna root ATAU dengan pengguna IAM yang sebelumnya Anda (seperti yang disarankan) dibuat di Langkah 2 untuk AWS Wickr.
2. Arahkan ke layanan AWS Wickr Anda. Anda dapat melakukan ini dari menu Layanan atau dengan mencari AWS Wickr di bilah pencarian.
3. Pada halaman AWS Wickr, pilih Kelola jaringan untuk mengakses daftar jaringan Wickr Anda.



Tombol Kelola jaringan.

4. Pada halaman Jaringan, di bawah kolom konsol admin Wickr, pilih tautan Admin di sebelah kanan nama Jaringan yang diinginkan.



Tautan konsol admin.

5. Transfer sudah selesai! Anda akan melihat dasbor jaringan Wickr Anda.

Penagihan untuk jaringan Anda sekarang akan ditransfer ke Anda Akun AWS. Biarkan hingga 3 hari kerja untuk dukungan untuk menghubungi dengan konfirmasi. Setelah menerima konfirmasi, Anda dapat melihat dan membayar tagihan Anda melalui AWS konsol.

Kelola jaringan AWS Wickr Anda

Di bagian Pengaturan Jaringan AWS Management Console untuk Wickr Anda dapat mengelola nama jaringan Wickr Anda, grup keamanan, konfigurasi SSO, dan pengaturan penyimpanan data.

Topik

Profil jaringan

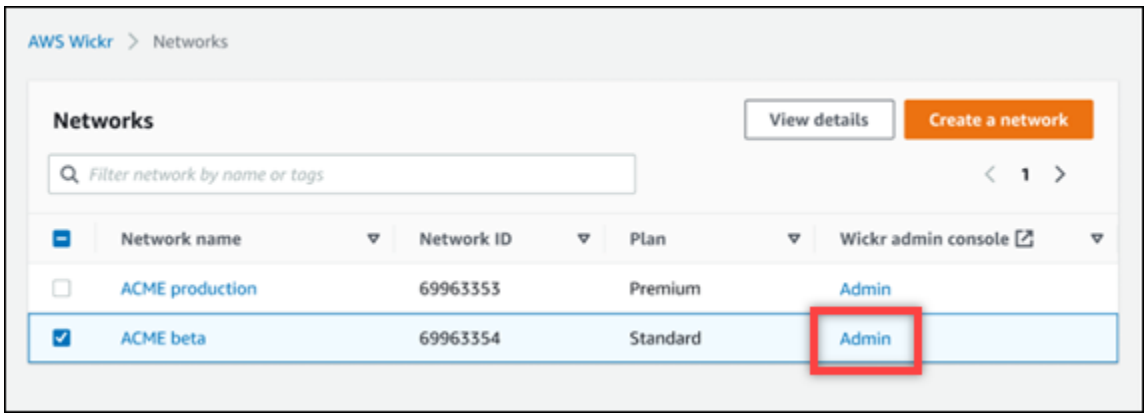
Anda dapat mengedit nama jaringan Wickr Anda dan melihat ID jaringan Anda di bagian Profil Jaringan AWS Management Console untuk Wickr.

Topik

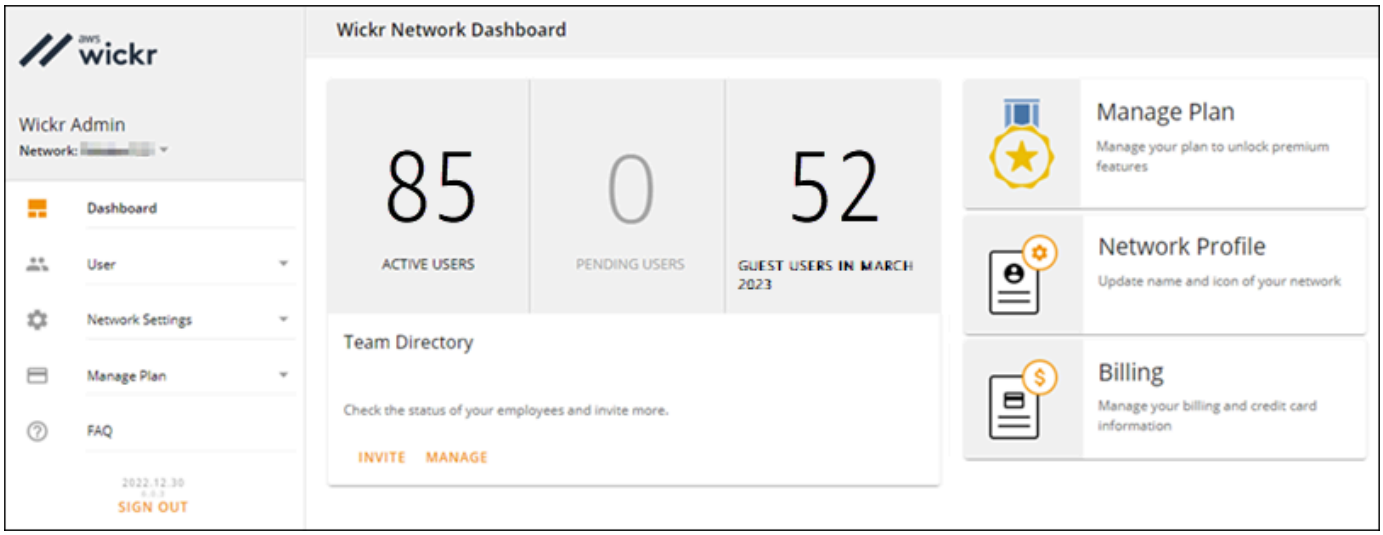
Lihat profil jaringan

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

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Pada halaman Jaringan, pilih tautan Admin, untuk menavigasi ke Konsol Admin Wickr untuk jaringan tersebut.



Anda diarahkan ke Konsol Admin Wickr untuk jaringan tertentu.



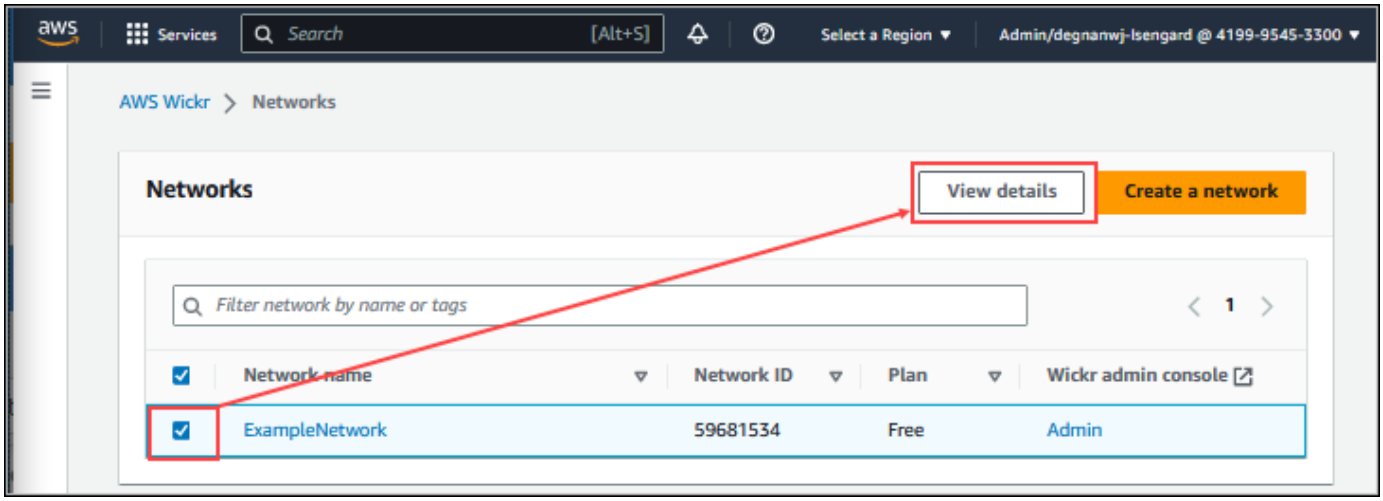
3. Di panel navigasi Konsol Admin Wickr, pilih Pengaturan Jaringan, lalu pilih Profil Jaringan.

   Halaman Profil Jaringan menampilkan nama jaringan Wickr dan ID jaringan Anda. Anda dapat menggunakan ID jaringan untuk mengkonfigurasi federasi.

Edit nama jaringan

Selesaikan prosedur berikut untuk mengedit nama jaringan Wickr Anda.

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Pilih Kelola jaringan.
3. Pada halaman Jaringan, pilih kotak centang di sebelah nama jaringan yang ingin Anda edit, lalu pilih Lihat detail.



4. Di bagian Ikhtisar jaringan, pilih Edit.
5. Masukkan nama jaringan baru Anda ke dalam kotak teks Nama Jaringan.
6. Pilih Simpan perubahan untuk menyimpan nama jaringan baru Anda.

Grup keamanan

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

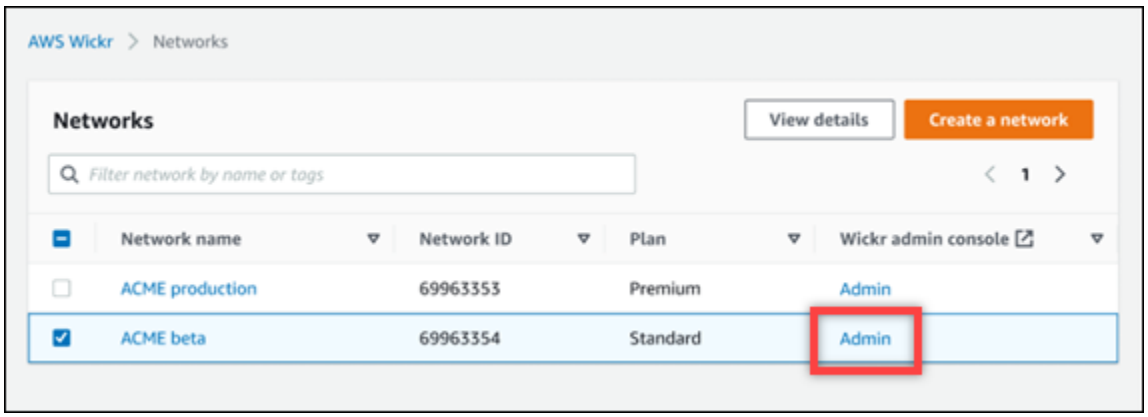
Topik

- Lihat grup keamanan
- Membuat grup keamanan
- Mengedit grup keamanan
- Menghapus grup keamanan

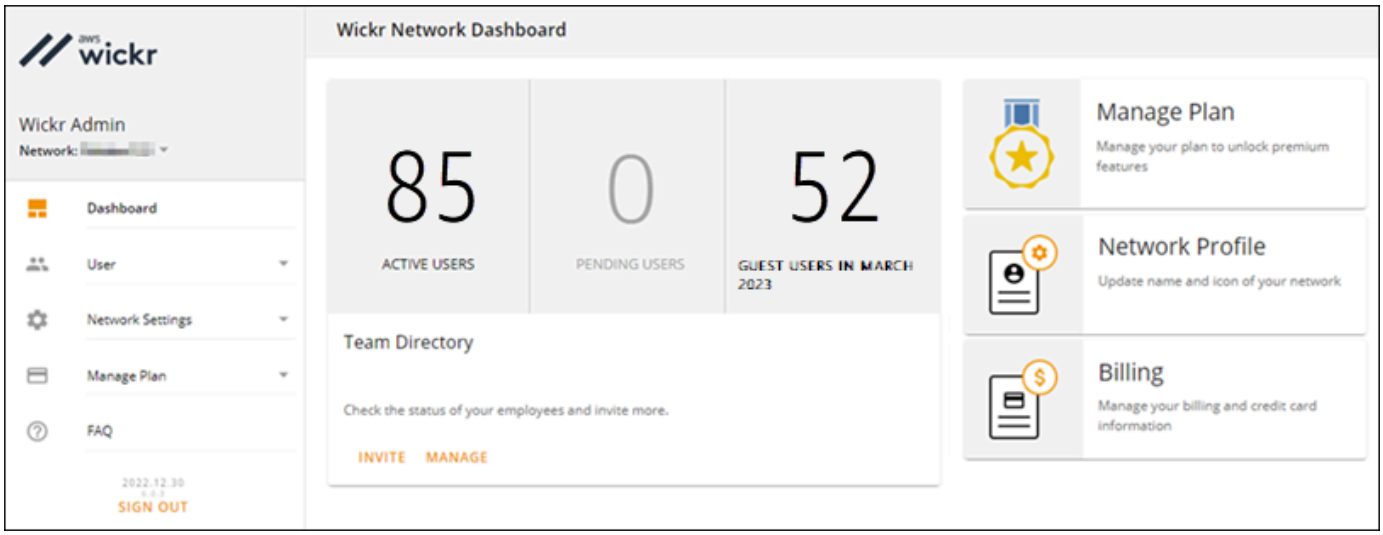
Lihat grup keamanan

Selesaikan prosedur berikut untuk melihat grup keamanan.

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Pada halaman Jaringan, pilih tautan Admin, untuk menavigasi ke Konsol Admin Wickr untuk jaringan tersebut.



Anda diarahkan ke Konsol Admin Wickr untuk jaringan tertentu.



3. Di panel navigasi Konsol Admin Wickr, pilih Pengaturan Jaringan, lalu pilih Grup Keamanan.

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

Membuat grup keamanan

Selesaikan prosedur berikut untuk membuat grup keamanan.

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Pada halaman Jaringan, pilih tautan Admin, untuk menavigasi ke Konsol Admin Wickr untuk jaringan tersebut.

   Anda diarahkan ke Konsol Admin Wickr untuk jaringan tertentu.
3. Di panel navigasi Konsol Admin Wickr, pilih Pengaturan Jaringan, lalu pilih Grup Keamanan.

4. Pilih Grup baru untuk membuat grup keamanan baru.

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

   Untuk informasi selengkapnya tentang mengedit grup keamanan baru, lihatMengedit grup keamanan.

Mengedit grup keamanan

Selesaikan prosedur berikut untuk mengedit grup keamanan.

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Pada halaman Jaringan, pilih tautan Admin, untuk menavigasi ke Konsol Admin Wickr untuk jaringan tersebut.

   Anda diarahkan ke Konsol Admin Wickr untuk jaringan tertentu.
3. Di panel navigasi Konsol Admin Wickr, pilih Pengaturan Jaringan, lalu pilih Grup Keamanan.
4. Pilih Detail di samping 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:

   - Nama grup keamanan - Pilih ikon pensil di sebelah nama grup untuk mengedit nama.
   - Umum — Edit konfigurasi dasar grup.
   - Pesan — Kelola fitur pesan untuk anggota grup.
   - Panggilan - Kelola fitur panggilan untuk anggota grup.
   - Keamanan — Konfigurasikan fitur keamanan tambahan untuk grup.
   - Federasi — Kemampuan untuk berkomunikasi antar jaringan. Ini dapat dikonfigurasi di konsol Admin untuk jaringan di tingkat grup keamanan. AWS Wickr memiliki 2 jenis federasi - Lokal dan Global.
     - Federasi Lokal — Kemampuan untuk berfederasi dengan pengguna AWS di jaringan lain dalam wilayah yang sama. Misalnya, jika ada dua jaringan di Kanada dengan federasi lokal diaktifkan, mereka akan dapat berkomunikasi satu sama lain.

- Federasi Global — Kemampuan untuk berfederasi dengan pengguna Enterprise atau AWS pengguna di jaringan berbeda yang termasuk dalam wilayah lain. Misalnya, jika ada pengguna di jaringan di wilayah Kanada dan pengguna di jaringan di wilayah London, dan federasi Global diaktifkan untuk kedua jaringan, mereka akan dapat berkomunikasi satu sama lain.
- Federasi Terbatas — Kemampuan untuk berfederasi dengan jaringan tertentu (Enterprise atau AWS) milik wilayah yang berbeda. Admin dapat mengizinkan daftar jaringan tertentu yang dapat difederasi oleh pengguna mereka. Setelah pembatasan, pengguna hanya dapat berkomunikasi dengan pengguna di jaringan yang diizinkan. Kedua jaringan harus mengizinkan satu sama lain dari pengaturan grup keamanan di tab federasi untuk menggunakan federasi terbatas.

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

Menghapus grup keamanan

Selesaikan prosedur berikut untuk menghapus grup keamanan.

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Pada halaman Jaringan, pilih tautan Admin, untuk menavigasi ke Konsol Admin Wickr untuk jaringan tersebut.

   Anda diarahkan ke Konsol Admin Wickr untuk jaringan tertentu.
3. Di panel navigasi Konsol Admin Wickr, pilih Pengaturan Jaringan, lalu pilih Grup Keamanan.
4. Pilih ikon elipsis vertikal di sebelah nama grup keamanan yang ingin Anda hapus.
5. Pilih Hapus untuk menghapus grup keamanan.

   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, lihatEdit pengguna.

Konfigurasi masuk tunggal

Di bagian Konfigurasi SSO AWS Management Console 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.

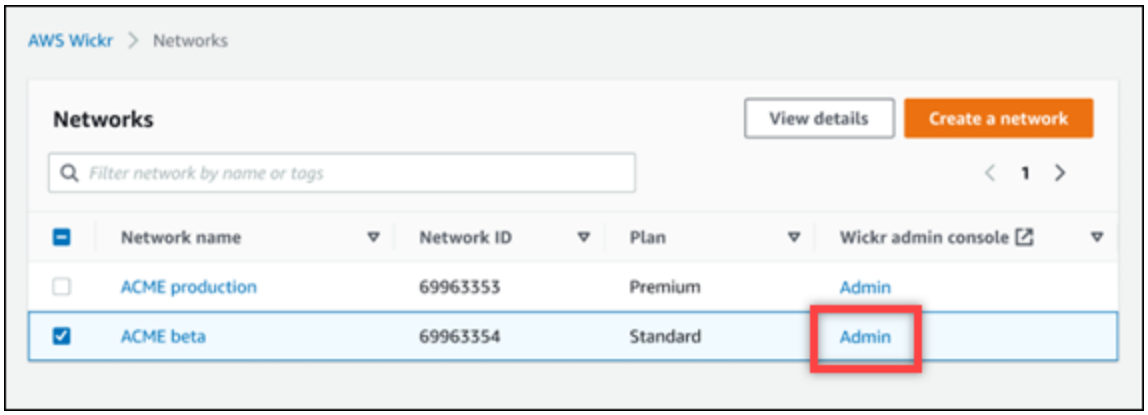
Wickr mendukung penyedia SSO yang hanya menggunakan OpenID Connect (OIDC). Penyedia yang menggunakan Security Assertion Markup Language (SALL) tidak didukung.

Topik

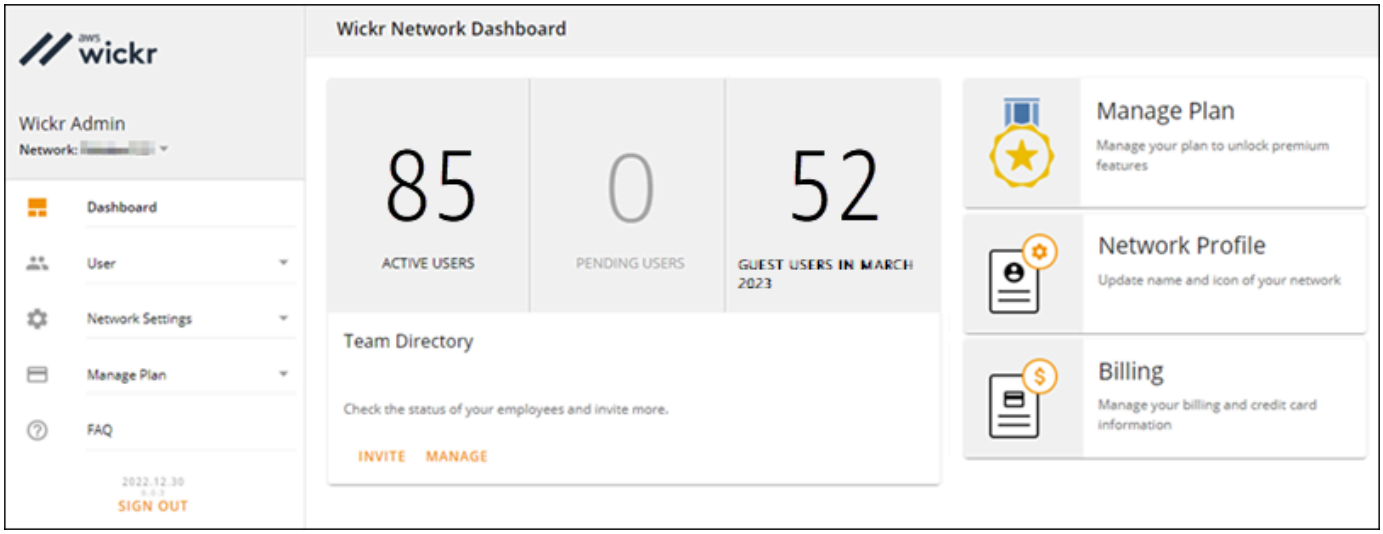
Lihat detail SSO

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

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Pada halaman Jaringan, pilih tautan Admin, untuk menavigasi ke Konsol Admin Wickr untuk jaringan tersebut.



Anda diarahkan ke Konsol Admin Wickr untuk jaringan tertentu.



3. Di panel navigasi Konsol Admin Wickr, pilih Pengaturan Jaringan, lalu pilih Konfigurasi SSO.

   Halaman Single Sign-on & LDAP Configuration menampilkan endpoint jaringan Wickr Anda dan konfigurasi SSO saat ini.

Konfigurasikan SSO

Untuk informasi selengkapnya tentang mengonfigurasi SSO, lihat panduan berikut di Pusat Bantuan Wickr:

> **Important**
>
> Ketika Anda mengkonfigurasi SSO, Anda menentukan ID perusahaan untuk jaringan Wickr Anda. Pastikan untuk menuliskan ID perusahaan untuk jaringan Wickr Anda. Anda harus memberikannya kepada pengguna akhir Anda saat mengirim email undangan. Pengguna akhir harus menentukan ID perusahaan ketika mereka mendaftar untuk jaringan Wickr Anda.

- Konfigurasikan sistem masuk tunggal Azure AD
- Konfigurasikan sistem masuk tunggal Okta

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.

Kelola tag jaringan

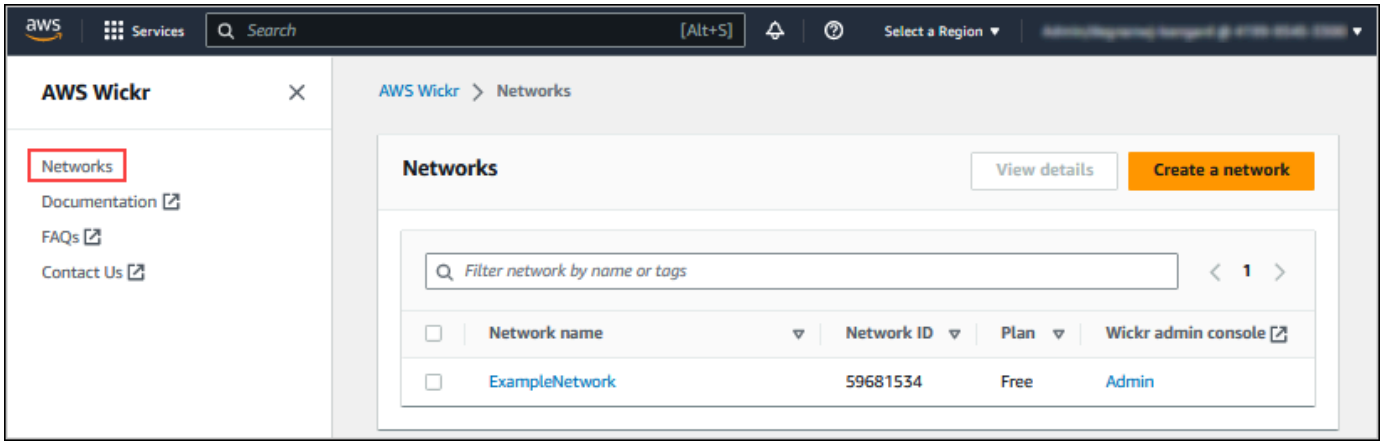
Anda dapat menerapkan tag ke jaringan Wickr. Anda kemudian dapat menggunakan tag tersebut untuk mencari dan memfilter jaringan Wickr Anda atau melacak biaya Anda AWS . Anda dapat mengonfigurasi tag jaringan di halaman ikhtisar Jaringan AWS Management Console untuk Wickr.

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.

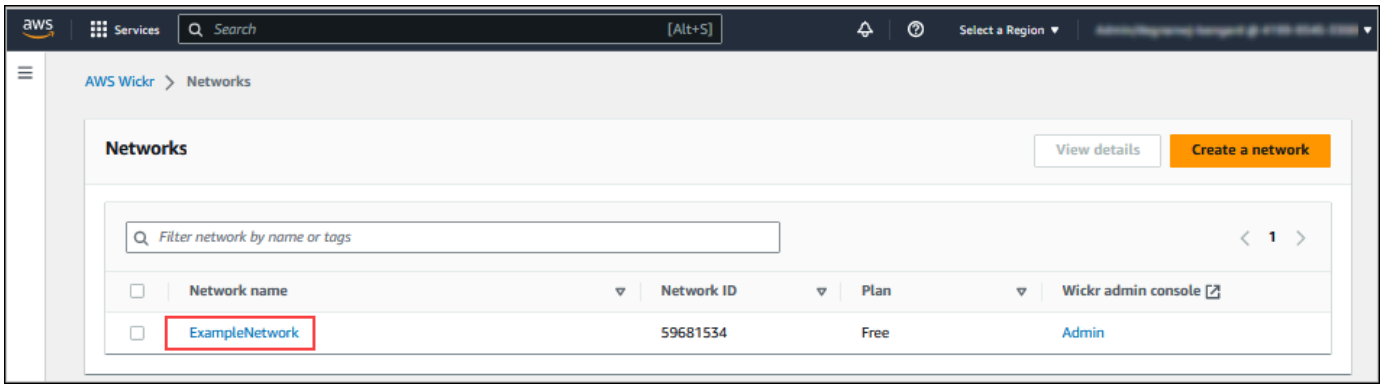
Kelola tag jaringan

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

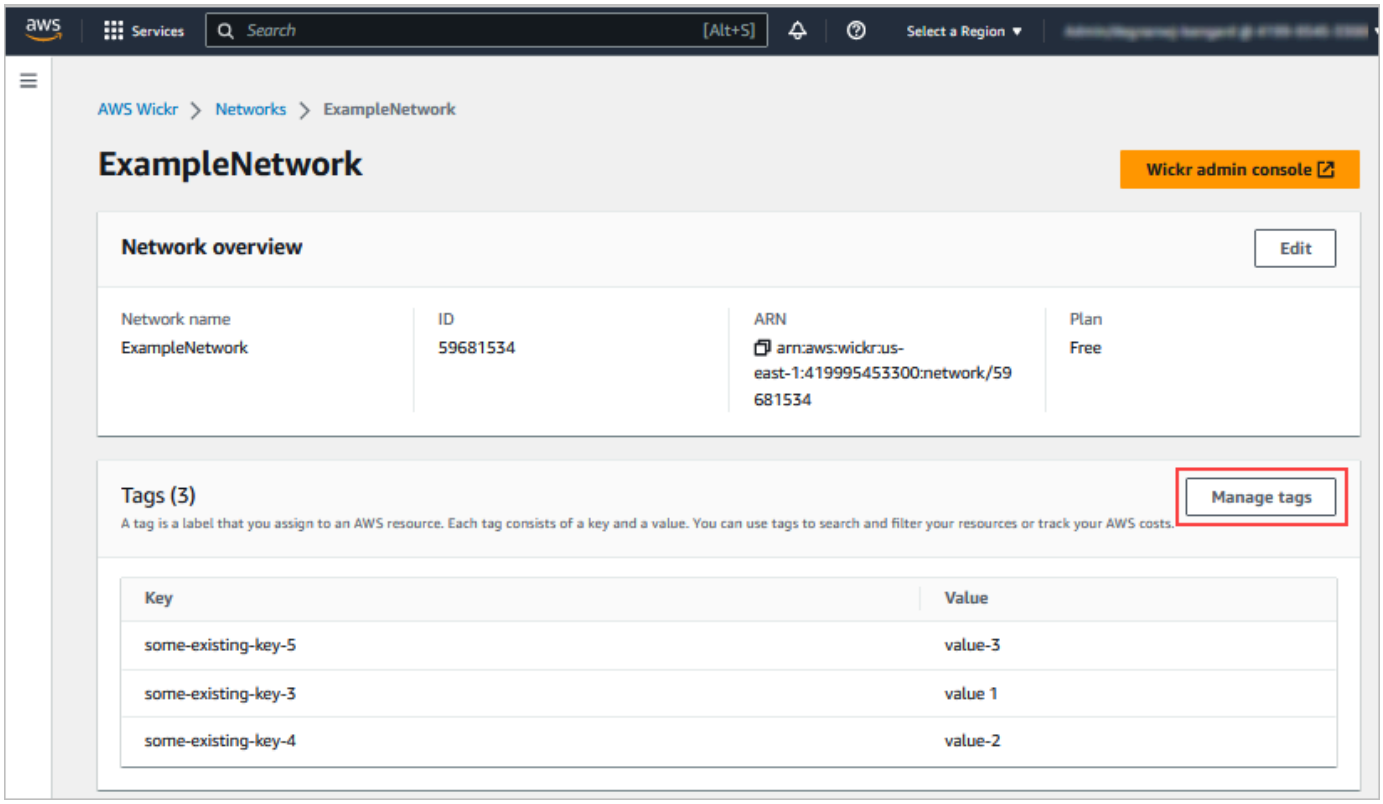
1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Pilih Jaringan dari panel navigasi AWS Management Console untuk Wickr.



3. Pada halaman Jaringan pilih nama jaringan yang ingin Anda kelola tag.



4. Di halaman Ikhtisar jaringan, pilih Kelola tag.



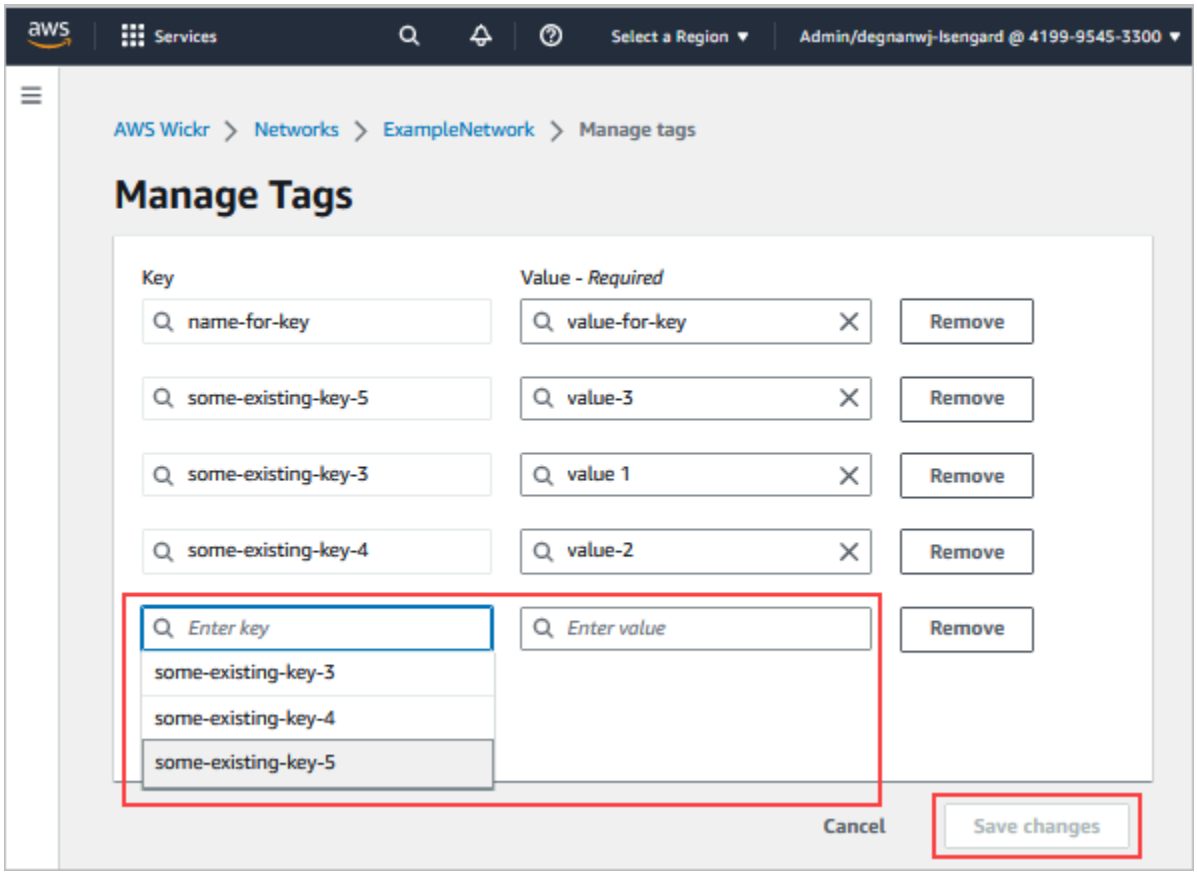
5. Pada halaman Kelola Tag, Anda dapat menyelesaikan salah satu opsi berikut:

   - 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.
   - 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.
   - Hapus tag yang ada — Pilih tombol Hapus yang tercantum di sebelah tag yang ingin Anda hapus. Untuk informasi selengkapnya, lihat Hapus tag jaringan.

Tambahkan tag jaringan

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

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

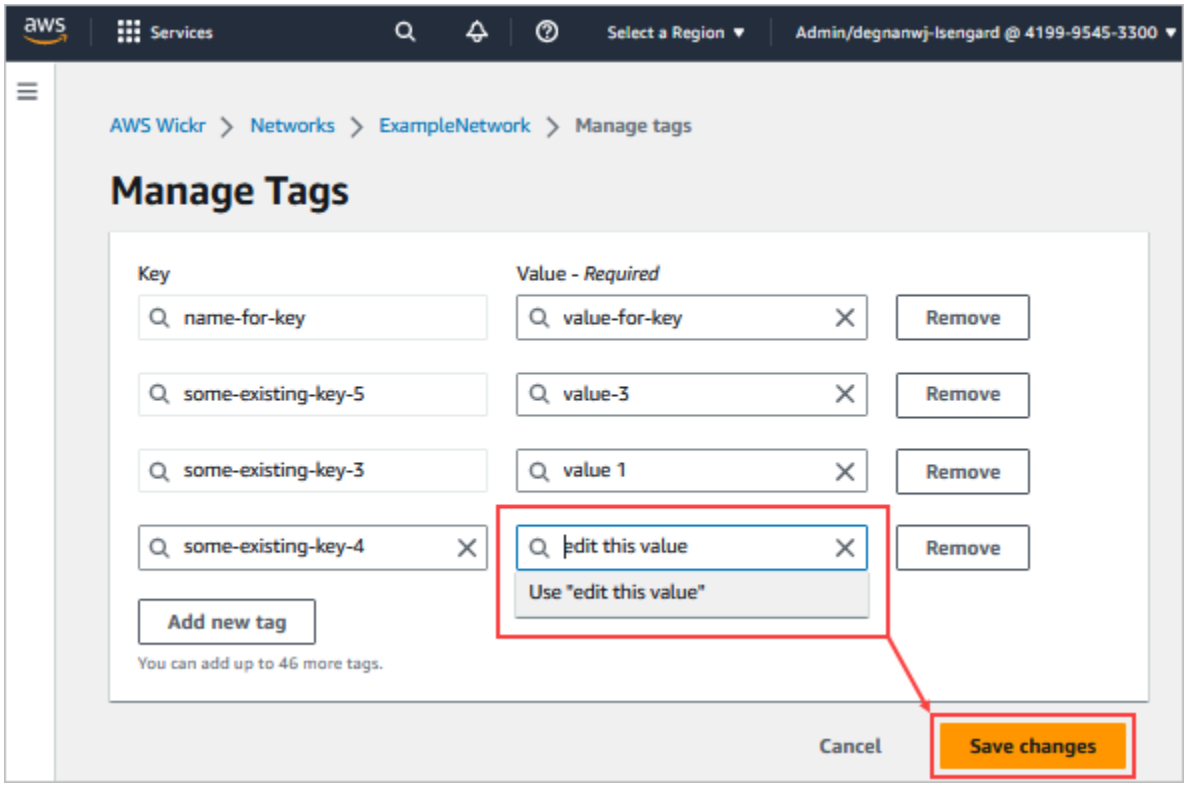


Mengedit tag jaringan

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

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.

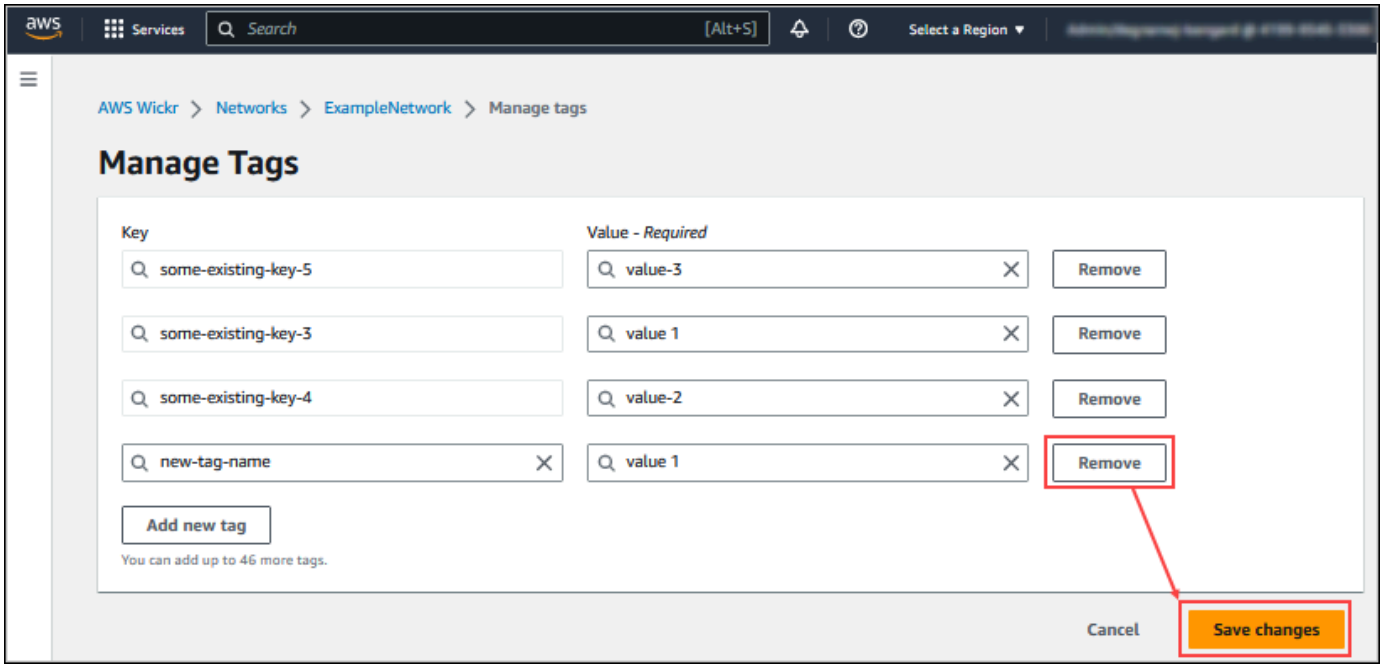


2. Pilih Simpan perubahan untuk menyimpan hasil edit Anda.

Hapus tag jaringan

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

1. Pada halaman Kelola tag, pilih Hapus untuk tag yang ingin Anda hapus.



2. Pilih Simpan perubahan untuk menyimpan hasil edit Anda.

Kelola paket jaringan

Di bagian Kelola Rencana AWS Management Console untuk Wickr, Anda dapat mengelola rencana jaringan Anda berdasarkan kebutuhan bisnis Anda.

Untuk mengelola rencana jaringan Anda, selesaikan prosedur berikut.

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Di panel navigasi Konsol Admin Wickr, pilih Kelola Paket, lalu pilih Paket Saya.
3. Pada halaman Paket Saya, 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 dapat memilih opsi uji coba gratis premium, yang tersedia hingga 30 pengguna dan berlangsung selama tiga bulan. Penawaran ini terbuka untuk uji coba baru, bebas warisan, dan paket standar. Administrator dapat meningkatkan atau menurunkan versi ke paket Premium atau Standar selama periode uji coba gratis premium.

> **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, tidak mungkin untuk meningkatkan ke uji coba gratis premium.

Retensi data

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.

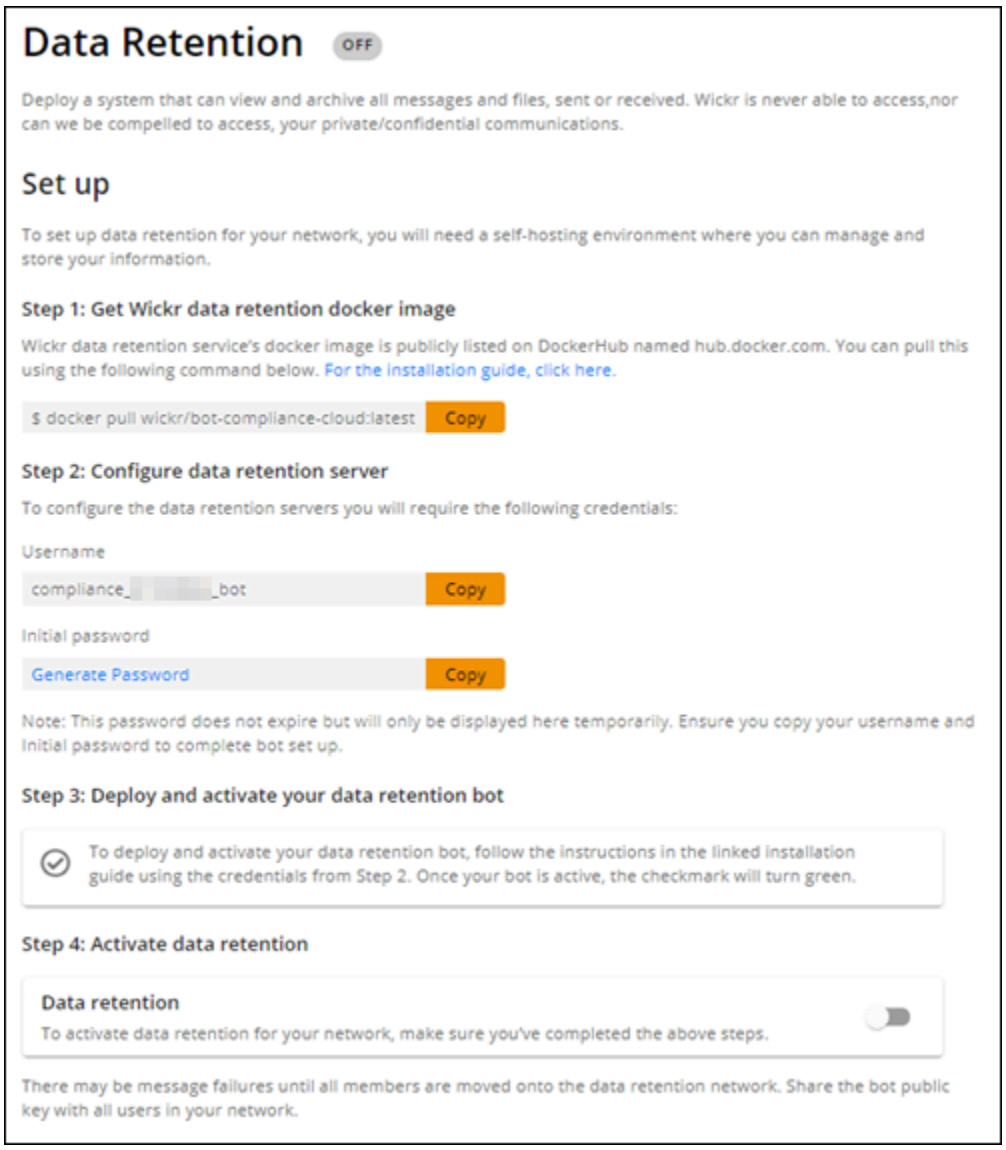
Topik

Lihat detail retensi data

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 AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Pilih Kelola jaringan.
3. Di panel navigasi Konsol Admin Wickr, pilih Pengaturan Jaringan, lalu pilih Retensi Data.

   Halaman Penyimpanan Data menampilkan langkah-langkah untuk mengatur retensi data, dan opsi untuk mengaktifkan atau menonaktifkan fitur penyimpanan data. Untuk informasi selengkapnya tentang mengonfigurasi retensi data, lihatKonfigurasikan retensi data.



> **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 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

Sebelum memulai, Anda harus mendapatkan nama bot retensi data (diberi label sebagai Nama Pengguna) dan kata sandi awal dari AWS Management Console 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.

Kata sandi

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-variabel lingkungan 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 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

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-variabel lingkungan.

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-variabel lingkungan

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.

> **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. 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 Wilayah AWS akan digunakan.

- `AWS_DEFAULT_REGION`— Default Wilayah AWS untuk digunakan untuk AWS layanan seperti Secrets Manager (tidak digunakan untuk Amazon S3 atauAWS KMS). `us-east-1`Region 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.

- `AWS_SECRET_NAME`— Nama rahasia Secrets Manager yang berisi kredensil dan informasi AWS layanan yang dibutuhkan oleh bot retensi data.
- `AWS_SECRET_REGION`— Wilayah AWS 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.

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

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.

```
{
    "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.

```
{
    "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

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-variabel lingkungan.
- 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

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-variabel lingkungan 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-variabel lingkungan 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 \
-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 \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e AWS_SECRET_NAME='wickr/data/retention/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 \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
 -e AWS_SECRET_NAME='wickr/data/retention/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 \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
 -e AWS_SECRET_NAME='wickr/data/retention/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 \
-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='bucket-name' \
-e WICKRIO_S3_FOLDER_NAME='folder-name' \
-e WICKRIO_S3_REGION='us-east-1' \
wickr/bot-compliance-cloud:latest
```

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

Hentikan bot retensi data

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

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

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
- Acara Amazon SNS

CloudWatch metrik

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.

Metrik	Deskripsi
Messages_Saved	Pesan disimpan ke file pesan yang diterima.
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.

Dimensi	Nilai
Produk	Produk untuk bot. Bisa `WickrPro_` atau `WickrEnterprise_` dengan`Alpha`,`Beta`, atau `Production` ditambahkan.
BotType	Jenis bot. Dilabeli sebagai Kepatuhan untuk bot kepatuhan.
Jaringan	ID dari jaringan terkait.

Acara Amazon SNS

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`. Lihat informasi yang lebih lengkap di Variabel-variabel lingkungan dan Nilai Secrets Manager.

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`.

Nama	Nilai
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.

Jenis peristiwa	Pesan peristiwa
failedlogin	Kredensyal buruk. Periksa kata sandinya.
failedlogin	Pengguna tidak ditemukan.
failedlogin	Akun atau perangkat ditangguhkan.
penyediaan	Pengguna keluar dari perintah.

Jenis peristiwa	Pesan peristiwa
penyediaan	Kata sandi yang buruk untuk `config.wickr` file.
penyediaan	Tidak dapat membaca `config.wickr` file.
failedlogin	Semua login gagal.
failedlogin	Pengguna baru tetapi database sudah ada.

Peristiwa yang lebih kritis

Jenis peristiwa	Pesan kejadian
Akun yang Ditangguhkan	WickRioClientMain:: 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

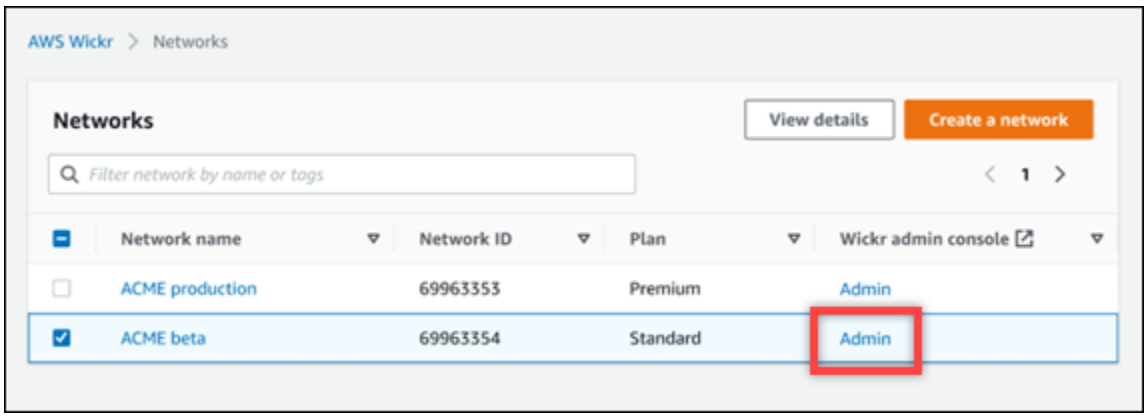
Aktifkan ATAK di Dasbor Jaringan Wickr

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.

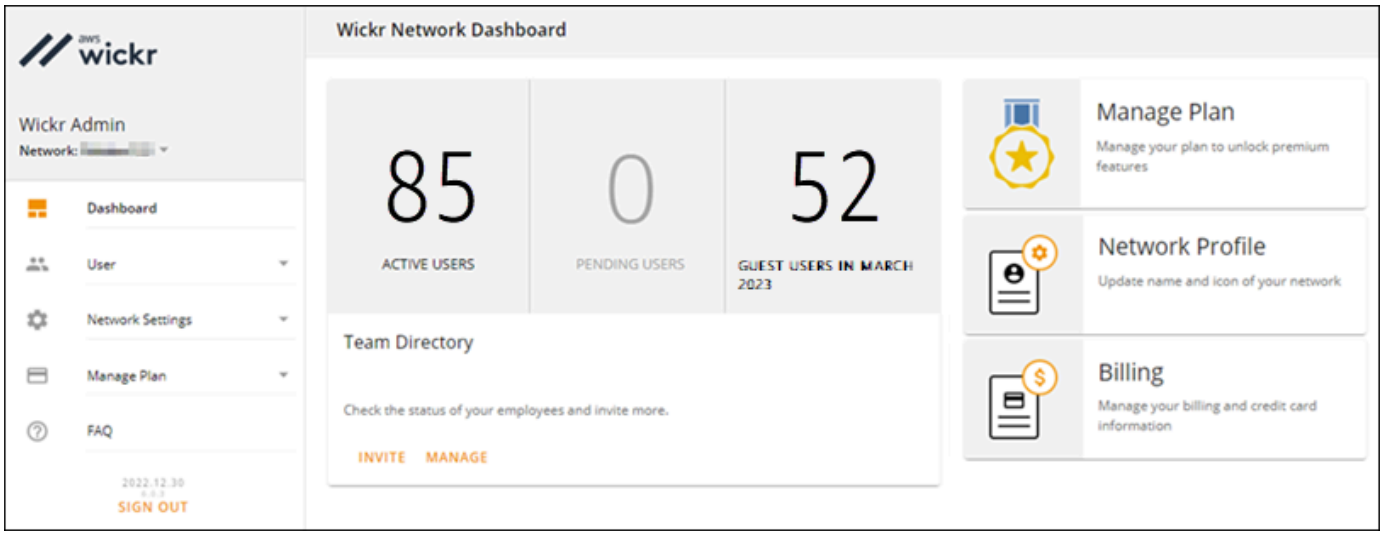
Aktifkan ATAK di Dasbor Jaringan Wickr

Selesaikan prosedur berikut untuk mengaktifkan ATAK di Dasbor Jaringan Wickr.

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Pada halaman Jaringan, pilih tautan Admin, untuk menavigasi ke Konsol Admin Wickr untuk jaringan tersebut.



Anda diarahkan ke Konsol Admin Wickr untuk jaringan tertentu.



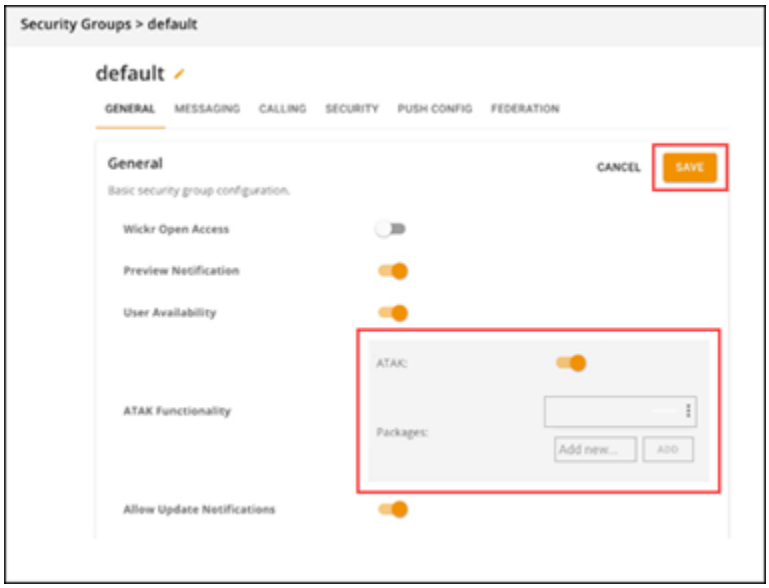
3. Di panel navigasi Konsol Admin Wickr, pilih Pengaturan Jaringan, lalu pilih Grup Keamanan.
4. Pilih Detail di samping grup keamanan yang diinginkan yang ingin Anda aktifkan ATAK.
5. Di tab Umum, pilih Edit.
6. Di bagian Fungsionalitas ATAK:

    a. 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.

b. Geser sakelar ATAK ke kanan untuk mengaktifkan fungsionalitas.

c. 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.

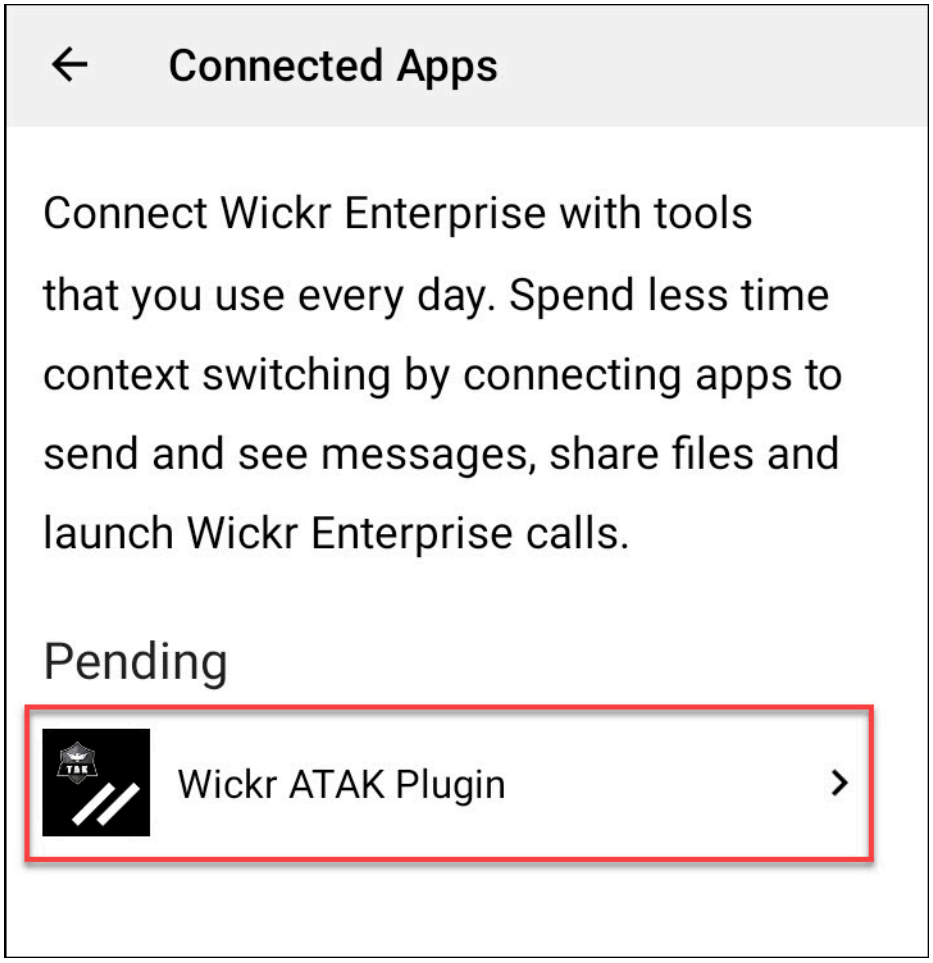
Pasangkan ATAK dengan Wickr

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

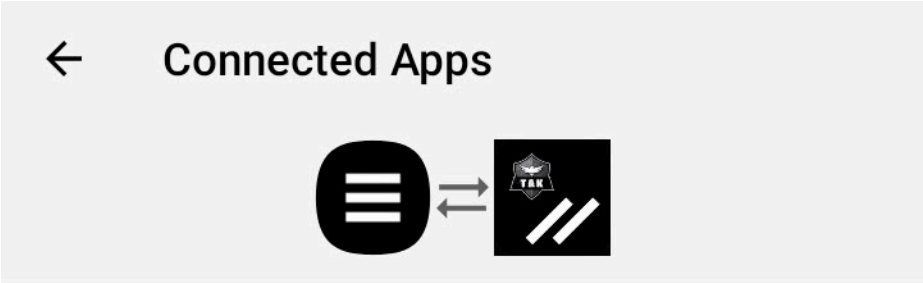
1. Di aplikasi ATAK, pilih ikon menu () di kanan atas layar, lalu pilih Plugin Wickr.

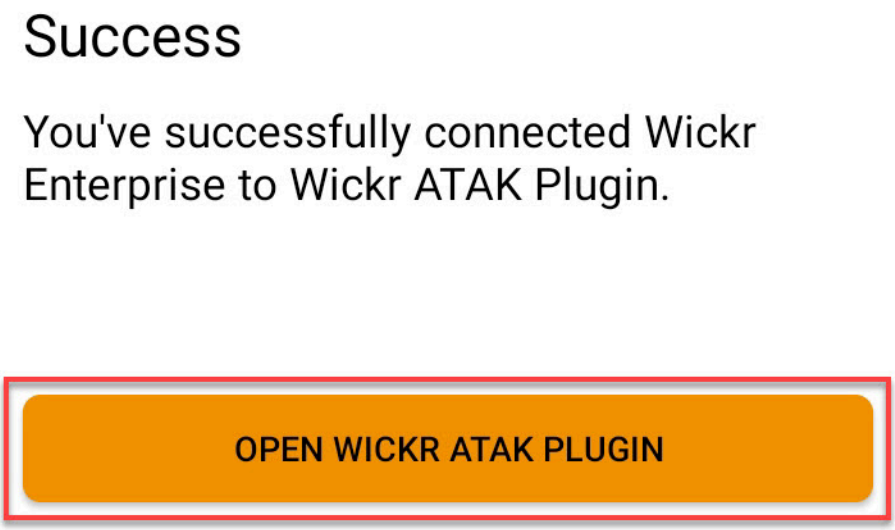
2. Pilih Pair Wickr.

   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.



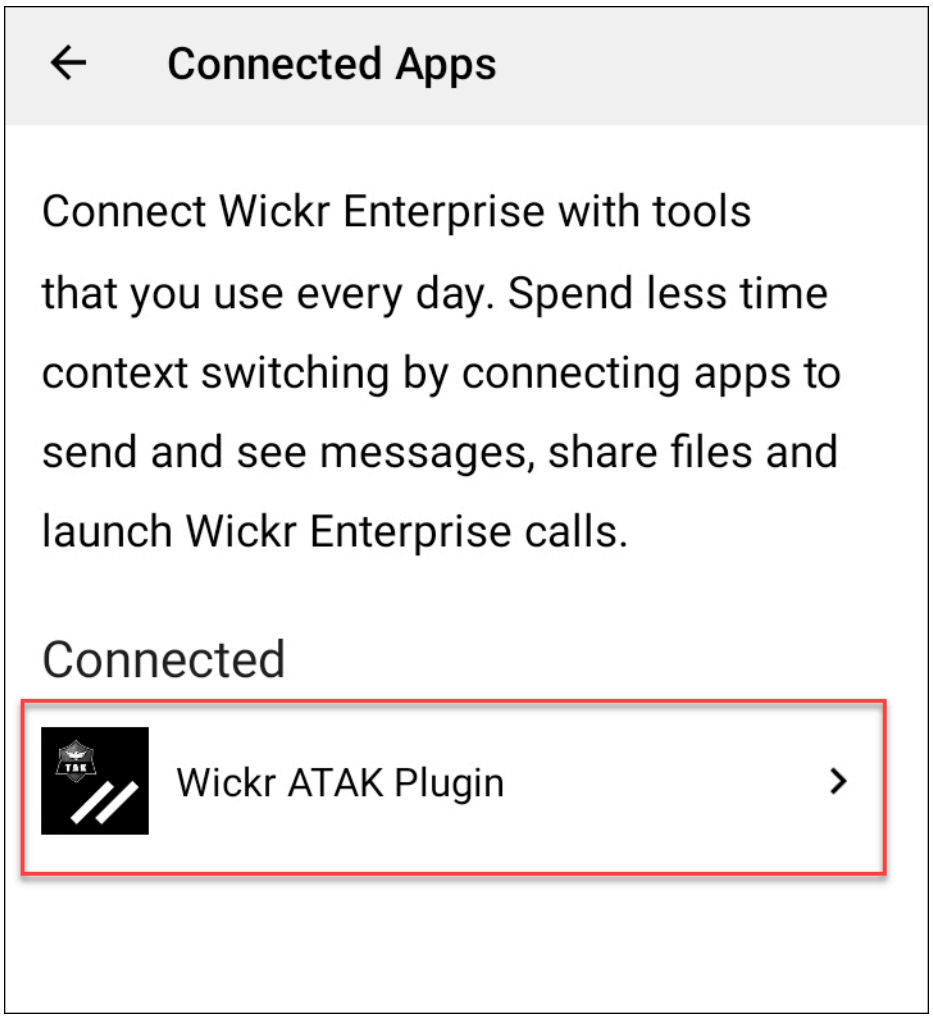


Anda sekarang telah berhasil memasangkan plugin ATAK dan Wickr, dan dapat menggunakan plugin untuk mengirim pesan dan berkolaborasi menggunakan Wickr tanpa keluar dari aplikasi ATAK.

Putuskan pasangan ATAK dengan Wickr

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.

   Layar konfirmasi menampilkan bahwa Anda tidak lagi menggunakan API. Anda sekarang telah berhasil memutuskan pasangan plugin ATAK.

Panggil dan terima panggilan

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

Selesaikan prosedur berikut untuk menghubungi dan menerima panggilan.

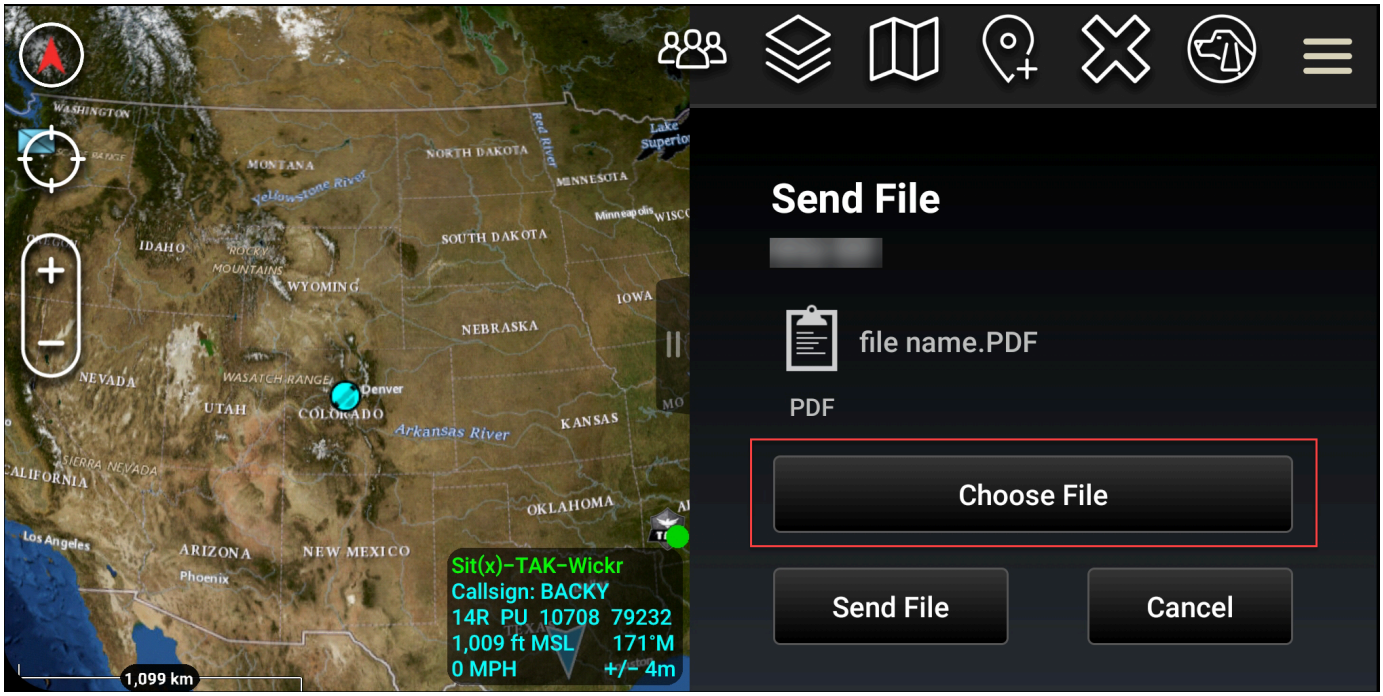
1. Buka jendela obrolan.
2. Dalam tampilan Peta, pilih ikon untuk pengguna yang ingin Anda panggil.
3. Pilih ikon telepon di kanan atas layar.
4. Setelah terhubung, Anda dapat kembali ke tampilan plugin ATAK dan menerima panggilan.

Kirim file

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.

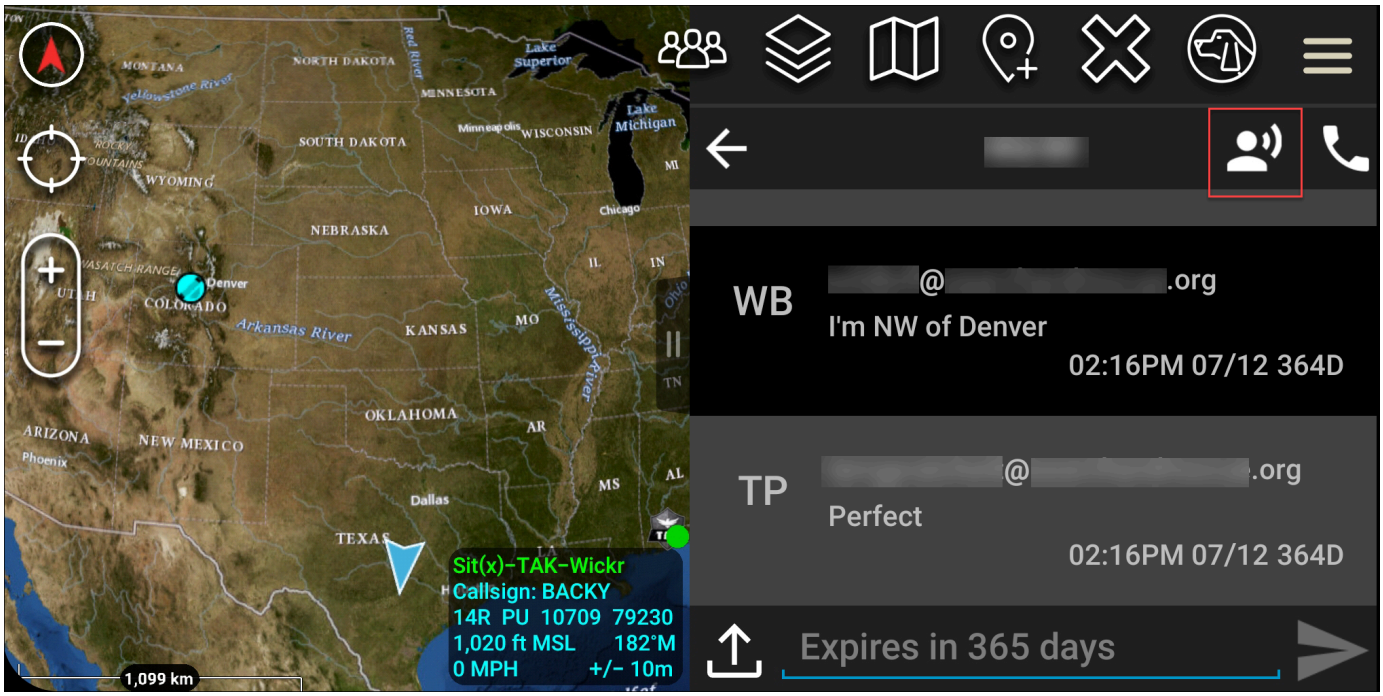
Mengirim pesan suara aman (Push-to-talk)

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

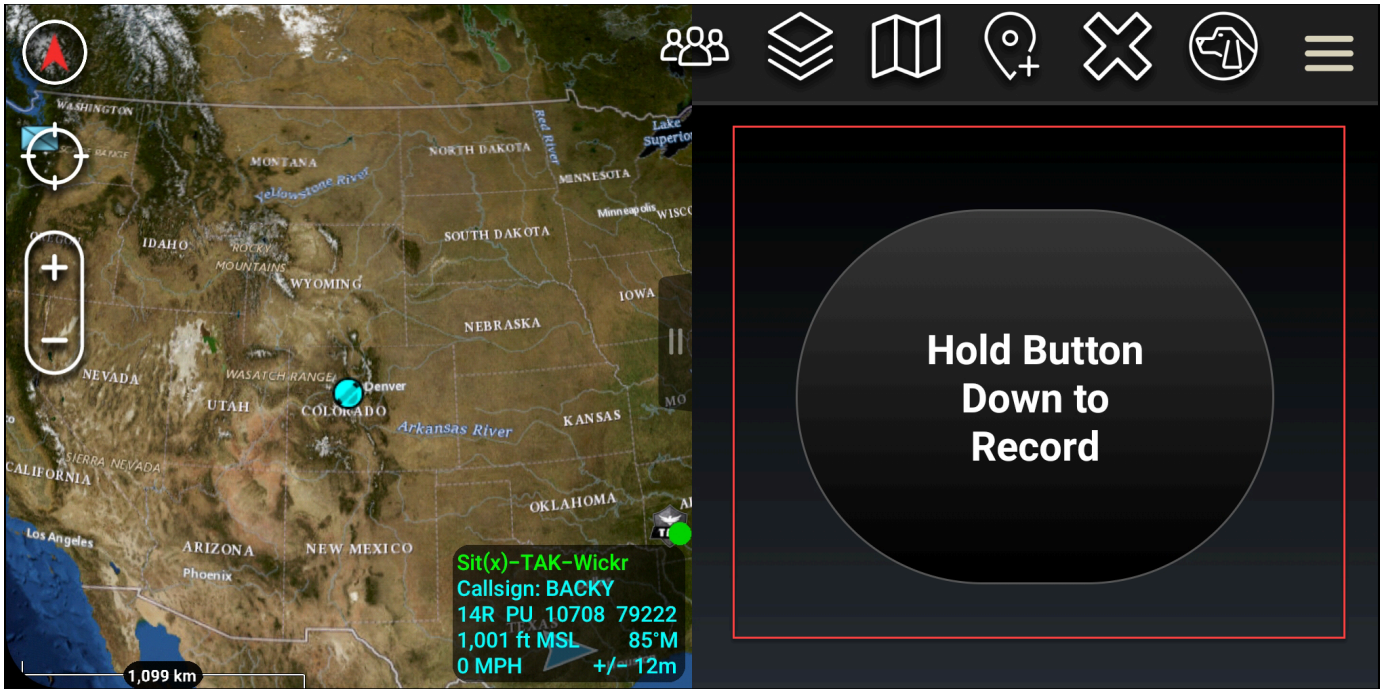
Selesaikan prosedur berikut untuk mengirim pesan suara yang aman.

1. Buka jendela obrolan.

2. Pilih ikon Push-to-Talk di bagian atas layar, yang ditunjukkan oleh ikon orang yang berbicara.



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



4. Rekam pesan Anda.

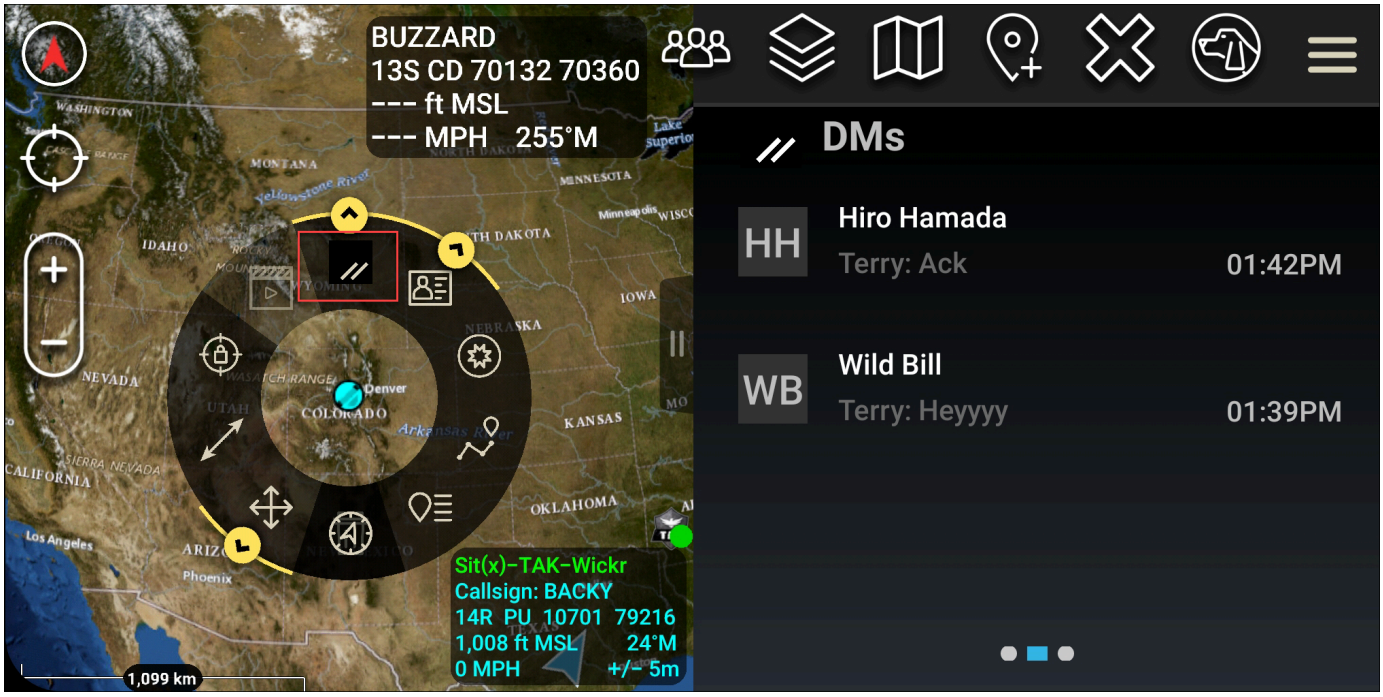
5. Setelah Anda merekam pesan Anda, lepaskan tombol untuk mengirim.

Pinwheel (Akses Cepat)

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

Selesaikan prosedur berikut untuk menggunakan kincir.

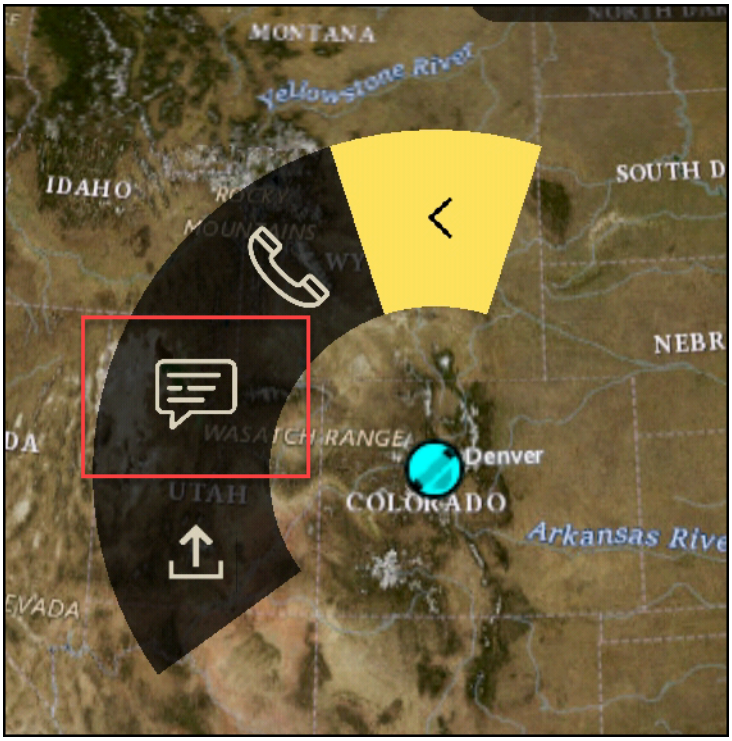
1. Buka tampilan layar terpisah dari peta ATAK dan plugin Wickr untuk ATAK secara bersamaan. Peta menampilkan rekan tim atau aset Anda pada tampilan peta.
2. Pilih ikon pengguna untuk membuka kincir.
3. Pilih ikon Wickr untuk melihat opsi yang tersedia untuk pengguna yang dipilih.



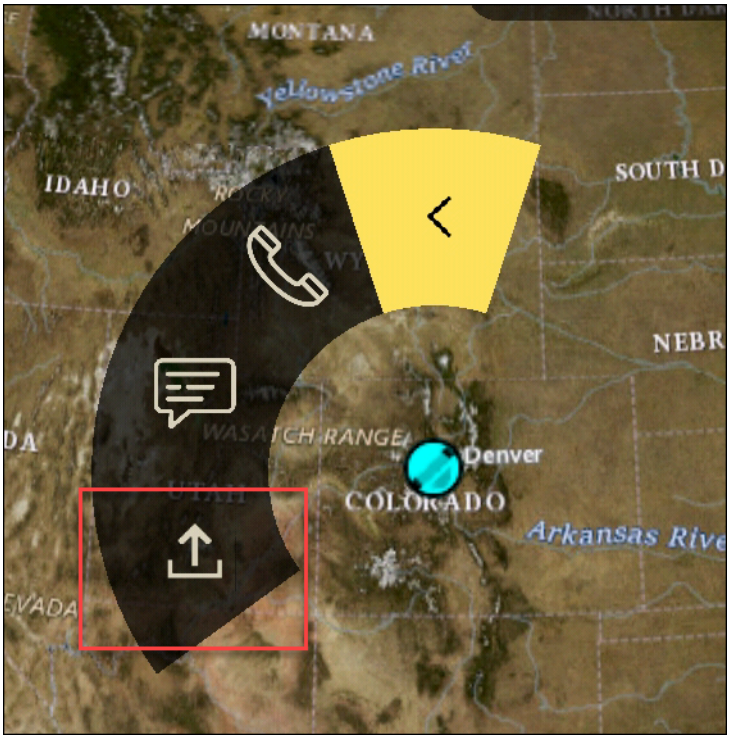
4. Pada kincir, pilih salah satu ikon berikut:

   - Telepon: Pilih untuk menelepon.

- Pesan: Pilih untuk mengobrol.



- Kirim file: Pilih untuk mengirim file.



Navigasi

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.
- Tampilan DM: 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 mengizinkan daftar

Izinkan daftar port dan domain berikut untuk memastikan Wickr berfungsi dengan benar:

Pelabuhan

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

Domain Regional

- Eropa (Frankfurt): api.messaging. wickr.eu-central-1.amazonaws.com
- AS Timur (Virginia Utara): gw-pro-prod .wickr.com, api.messaging. wickr.us-east-1.amazonaws.com
- Eropa (London): api.messaging. wickr.eu-west-2.amazonaws.com
- Asia Pasifik (Sydney): api.messaging. wickr.ap-southeast-2.amazonaws.com
- Kanada (Tengah): api.messaging. wickr.ca-central-1.amazonaws.com
- AWS GovCloud (AS-Barat): api.messaging.wickr. us-gov-west-1.amazonaws.com

Email pendaftaran dan verifikasi dikirim dari donotreply@wickr.email.

Jika Anda perlu mengizinkan daftar semua alamat IP server panggilan yang mungkin, Anda harus AllowlistWickrmengunduh.txt dari kemungkinan CIDR dan memeriksanya secara berkala karena dapat berubah.

Kelola pengguna di AWS Wickr

Di bagian Pengguna AWS Management Console untuk Wickr Anda dapat melihat pengguna dan bot Wickr saat ini, dan memodifikasi detailnya.

Topik

Direktori tim

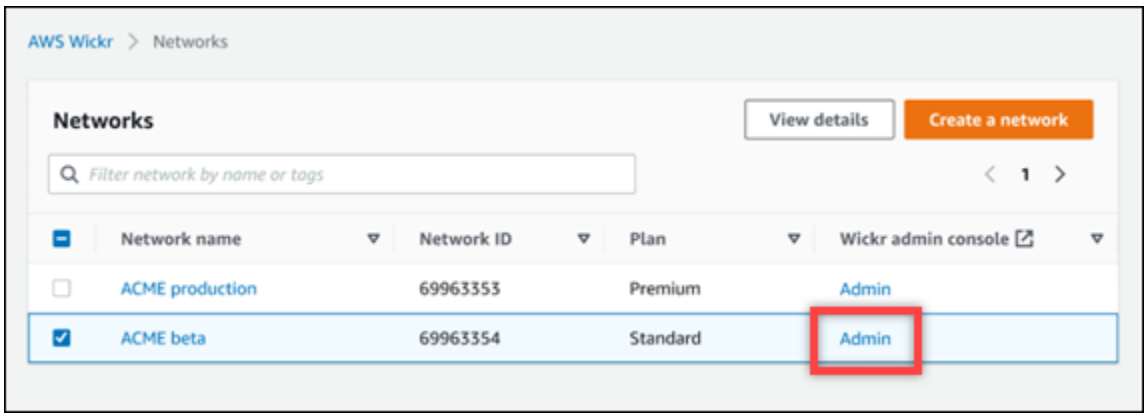
Anda dapat melihat pengguna Wickr saat ini dan memodifikasi detailnya di bagian Pengguna AWS Management Console untuk Wickr.

Topik

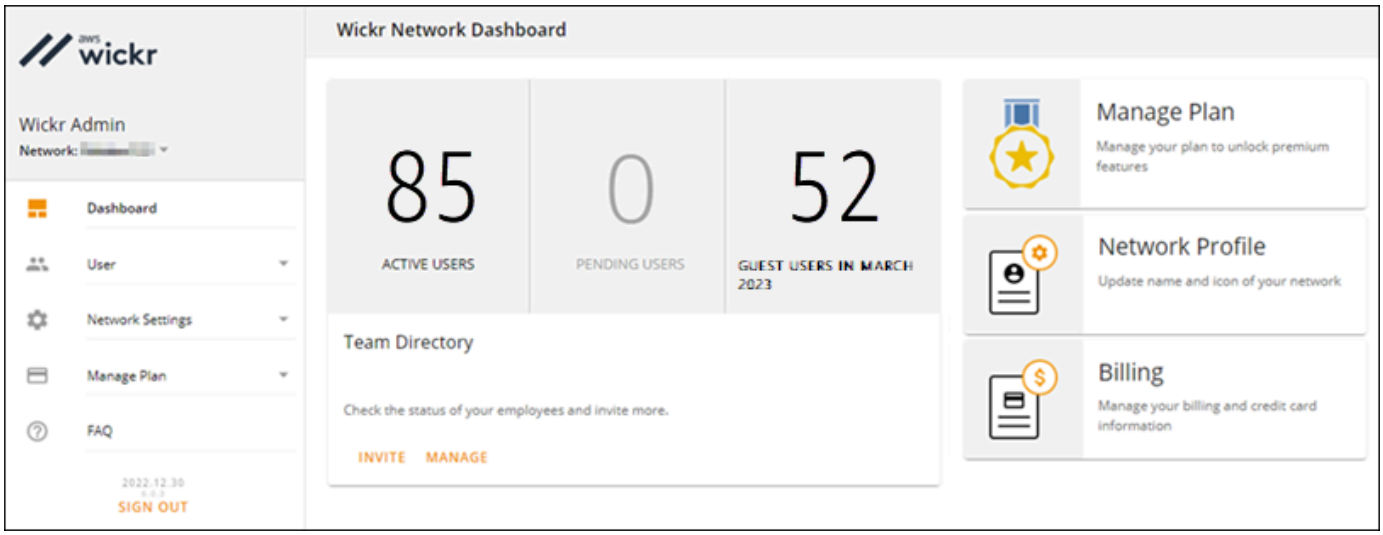
Lihat pengguna

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

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Pada halaman Jaringan, pilih tautan Admin, untuk menavigasi ke Konsol Admin Wickr untuk jaringan tersebut.



Anda diarahkan ke Konsol Admin Wickr untuk jaringan tertentu.



3. Di panel navigasi Konsol Admin Wickr, pilih Pengguna, lalu pilih Direktori Tim.

   Halaman 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.

Buat pengguna

Selesaikan prosedur berikut untuk membuat pengguna.

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Pada halaman Jaringan, pilih tautan Admin, untuk menavigasi ke Konsol Admin Wickr untuk jaringan tersebut.

Anda diarahkan ke Konsol Admin Wickr untuk jaringan tertentu.

3. Di panel navigasi Konsol Admin Wickr, pilih Pengguna, lalu pilih Direktori Tim.
4. Pilih Buat pengguna baru.
5. Dalam formulir yang muncul, 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. Wickr akan mengirim email undangan ke alamat yang Anda tentukan untuk pengguna.
6. Pilih Buat.

   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.

Edit pengguna

Selesaikan prosedur berikut untuk mengedit pengguna.

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Pada halaman Jaringan, pilih tautan Admin, untuk menavigasi ke Konsol Admin Wickr untuk jaringan tersebut.

   Anda diarahkan ke Konsol Admin Wickr untuk jaringan tertentu.
3. Di panel navigasi Konsol Admin Wickr, pilih Pengguna, lalu pilih Direktori Tim.
4. Pilih ikon elipsis vertikal di sebelah nama pengguna yang ingin Anda hapus.
5. Anda dapat memilih salah satu opsi berikut:

   - Perangkat — Lihat perangkat yang telah dikonfigurasi pengguna dengan klien Wickr.
   - Edit — Edit detail pengguna, seperti nama, kode negara, nomor telepon (opsional), dan grup keamanan yang ditetapkan.
   - Tangguhkan — Tangguhkan pengguna sehingga mereka 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.
   - Hapus — Hapus pengguna dari jaringan Wickr Anda.

Hapus pengguna

Selesaikan prosedur berikut untuk menghapus pengguna.

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Pada halaman Jaringan, pilih tautan Admin, untuk menavigasi ke Konsol Admin Wickr untuk jaringan tersebut.

   Anda diarahkan ke Konsol Admin Wickr untuk jaringan tertentu.
3. Di panel navigasi Konsol Admin Wickr, pilih Pengguna, lalu pilih Direktori Tim.
4. Pilih ikon elipsis vertikal di sebelah nama 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.

Hapus pengguna secara massal

Anda dapat menghapus secara massal dan menangguhkan pengguna jaringan Wickr secara massal di bagian Pengguna Konsol Admin Wickr untuk Wickr.

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

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Di panel navigasi Konsol Admin Wickr, pilih Pengguna, lalu pilih Direktori Tim.

   Halaman Direktori Tim menampilkan pengguna yang terdaftar ke jaringan Wickr Anda.
3. Pada halaman Direktori Tim, pilih Kelola Pengguna.
4. Pada jendela pop-up Kelola Pengguna, pilih Hapus Pengguna.
5. Unduh contoh template CSV. Untuk mengunduh templat sampel, pilih Unduh Template.
6. Lengkapi template dengan menambahkan email pengguna yang ingin Anda hapus massal dari jaringan Anda.
7. Unggah template CSV yang sudah selesai. Anda dapat menarik dan melepas file ke dalam kotak unggah, atau pilih pilih file.
8. Pilih kotak centang, saya mengakui bahwa menghapus pengguna tidak dapat dibalik.

9. 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 AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Di panel navigasi Konsol Admin Wickr, pilih Pengguna, lalu pilih Direktori Tim.

   Halaman Direktori Tim menampilkan pengguna yang terdaftar ke jaringan Wickr Anda.
3. Pilih ikon unduhan CSV di pojok kanan atas halaman Direktori Tim.
4. Setelah Anda mengunduh templat CSV direktori tim, hapus baris pengguna yang tidak perlu dihapus.
5. Pada halaman Direktori Tim, pilih Kelola Pengguna.
6. Pada jendela pop-up Kelola Pengguna, pilih Hapus Pengguna.
7. Unggah templat CSV direktori tim. Anda dapat menarik dan melepas file ke dalam kotak unggah, atau pilih pilih file.
8. Pilih kotak centang, saya mengakui bahwa menghapus pengguna tidak dapat dibalik.
9. 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

Anda dapat menangguhkan pengguna jaringan Wickr secara massal di bagian Pengguna Konsol Admin Wickr untuk Wickr.

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

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Di panel navigasi Konsol Admin Wickr, pilih Pengguna, lalu pilih Direktori Tim.

   Halaman Direktori Tim menampilkan pengguna yang terdaftar ke jaringan Wickr Anda.
3. Pada halaman Direktori Tim, pilih Kelola Pengguna.
4. Pada jendela pop-up Kelola Pengguna, pilih Tangguhkan Pengguna.
5. Unduh contoh template CSV. Untuk mengunduh templat sampel, pilih Unduh Template.
6. Lengkapi template dengan menambahkan email pengguna yang ingin ditangguhkan secara massal dari jaringan Anda.
7. Unggah template CSV yang sudah selesai. Anda dapat menarik dan melepas file ke dalam kotak unggah, atau pilih pilih file.
8. Setelah Anda mengunggah file CSV, 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

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 di halaman Grup Keamanan konsol admin Wickr.

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

AndaAkun AWS. Untuk informasi selengkapnya tentang harga untuk fitur pengguna tamu, lihat halaman harga Wickr di bawah Pengaya Harga.

Topik

Mengaktifkan atau menonaktifkan pengguna tamu

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

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Pada halaman Jaringan, pilih tautan Admin, untuk menavigasi ke Konsol Admin Wickr untuk jaringan tersebut.

   Anda diarahkan ke Konsol Admin Wickr untuk jaringan tertentu.
3. Di panel navigasi Konsol Admin Wickr, pilih Pengaturan Jaringan, lalu pilih Grup Keamanan.
4. Pilih Detail 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 halaman detail grup keamanan.
6. Ada dua lokasi di mana sakelar untuk mengizinkan pengguna tamu akan tersedia:

   - Federasi Lokal - Untuk jaringan di AS Timur (Virginia Utara), pilih Edit di sebelah bagian Federasi Lokal halaman.
   - Federasi Global - Untuk semua jaringan lain di wilayah lain, pilih Edit di sebelah bagian Federasi Global pada halaman.

7. Pilih Izinkan pengguna tamu untuk mengaktifkan pengguna tamu untuk grup keamanan, atau batalkan pilihan untuk menonaktifkannya.
8. Pilih Simpan 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.

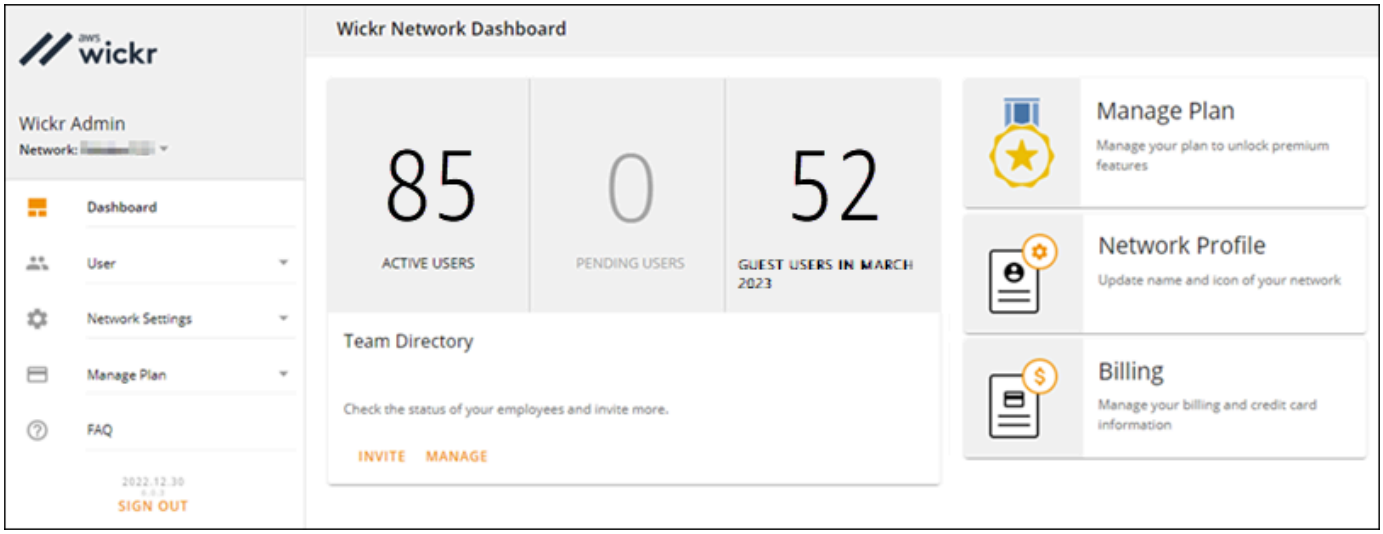
> **Note**
>
> Fitur pengguna tamu Wickr tidak tersedia di AWS GovCloud (US) West () AWS WickrGov.

Lihat jumlah pengguna tamu

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

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Pada halaman Jaringan, pilih tautan Admin, untuk menavigasi ke Konsol Admin Wickr untuk jaringan tersebut.

   Anda diarahkan ke Konsol Admin Wickr untuk jaringan tertentu. Halaman Dasbor menampilkan jumlah pengguna tamu di jaringan Wickr Anda seperti yang ditunjukkan pada contoh berikut.



Lihat penggunaan bulanan

Anda dapat melihat jumlah pengguna tamu yang telah berkomunikasi dengan jaringan Anda selama periode penagihan. Untuk melihat penggunaan bulanan Anda, selesaikan langkah-langkah berikut.

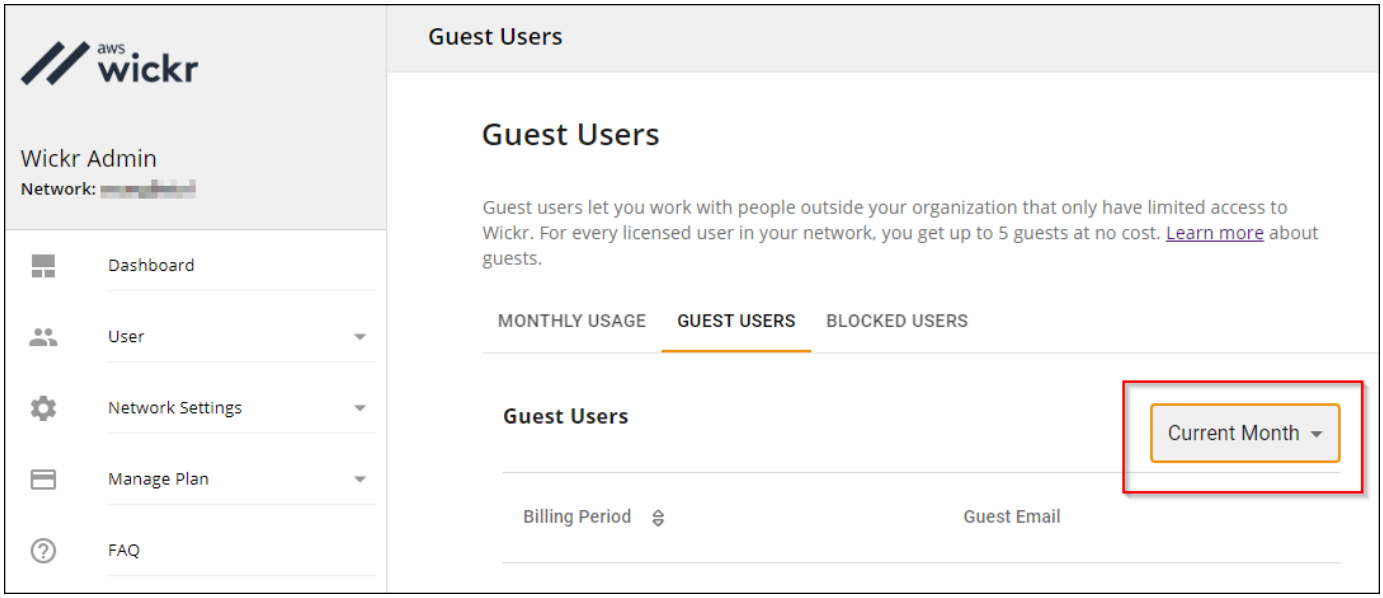
1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Pada halaman Jaringan, pilih tautan Admin, untuk menavigasi ke Konsol Admin Wickr untuk jaringan tersebut.
3. Di panel navigasi Konsol Admin Wickr, pilih Pengguna, lalu pilih Pengguna Tamu.
4. Pada halaman Pengguna Tamu, pilih bagian Penggunaan Bulanan.

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

Lihat pengguna tamu

Anda dapat melihat daftar pengguna tamu yang telah berkomunikasi dengan pengguna jaringan selama periode penagihan tertentu. Untuk melihat pengguna tamu Anda, selesaikan langkah-langkah berikut.

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Pada halaman Jaringan, pilih tautan Admin, untuk menavigasi ke Konsol Admin Wickr untuk jaringan tersebut.
3. Di panel navigasi Konsol Admin Wickr, pilih Pengguna, lalu pilih Pengguna Tamu.
4. Pada halaman Pengguna Tamu, pilih bagian Pengguna Tamu.
5. Untuk melihat pengguna tamu untuk bulan tertentu, pilih bulan yang sesuai dari menu tarik-turun.



Memblokir pengguna tamu

Pengguna yang diblokir tidak dapat berkomunikasi dengan siapa pun di jaringan Anda.

Untuk memblokir pengguna tamu

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. Pada halaman Jaringan, pilih tautan Admin, untuk menavigasi ke Konsol Admin Wickr untuk jaringan tersebut.
3. Di panel navigasi Konsol Admin Wickr, pilih Pengguna, lalu pilih Pengguna Tamu.
4. Pada halaman Pengguna Tamu, pilih bagian Pengguna Tamu.
5. Bagian Pengguna Tamu menunjukkan pengguna tamu yang telah berkomunikasi di jaringan Wickr Anda.
6. Di bagian Pengguna Tamu, temukan email pengguna tamu yang ingin Anda blokir.
7. Di sisi kanan nama pengguna tamu, pilih tiga titik, dan pilih Blokir.
8. Pilih Blokir pada jendela pop-up.
9. Untuk melihat daftar pengguna yang diblokir di jaringan Wickr Anda, pilih bagian Pengguna yang Diblokir.

Untuk membuka blokir pengguna tamu

1. Buka AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.

2. Pada halaman Jaringan, pilih tautan Admin, untuk menavigasi ke Konsol Admin Wickr untuk jaringan tersebut.
3. Di panel navigasi Konsol Admin Wickr, pilih Pengguna, lalu pilih Pengguna Tamu.
4. Pada halaman Pengguna Tamu, pilih bagian Pengguna yang Diblokir.
5. Bagian Pengguna yang Diblokir menunjukkan pengguna tamu yang diblokir di jaringan Wickr Anda.
6. Di bagian Pengguna yang Diblokir, temukan email pengguna tamu yang ingin Anda buka blokir.
7. Di sisi kanan nama pengguna tamu, pilih tiga titik, dan pilih Buka blokir.
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 sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Wickr atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. 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

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

Pengguna layanan — Jika Anda menggunakan layanan Wickr untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Wickr untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Wickr, lihat. Memecahkan masalah identitas dan akses AWS Wickr

Administrator layanan — Jika Anda bertanggung jawab atas sumber daya Wickr di perusahaan Anda, Anda mungkin memiliki akses penuh ke Wickr. Tugas Anda adalah menentukan fitur dan sumber daya Wickr mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan

permintaan kepada administrator IAM Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Wickr, lihat. Bagaimana AWS Wickr bekerja dengan IAM

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

Mengautentikasi dengan identitas

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

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

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

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

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

Akun AWS pengguna root

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

Identitas terfederasi

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

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

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

Pengguna dan grup IAM

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

Grup IAM adalah identitas yang menentukan kumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin untuk beberapa pengguna sekaligus. Grup membuat izin lebih mudah dikelola untuk sekelompok besar pengguna. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

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

Peran IAM

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

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna gabungan – Untuk menetapkan izin ke sebuah identitas gabungan, Anda dapat membuat peran dan menentukan izin untuk peran tersebut. Saat identitas terfederasi mengautentikasi, identitas tersebut akan dikaitkan dengan peran dan diberi izin yang ditentukan oleh peran tersebut. Untuk informasi tentang peran-peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika Anda menggunakan Pusat Identitas IAM, Anda perlu mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM mengorelasikan izin yang diatur ke peran dalam IAM. Untuk informasi tentang rangkaian izin, lihat Rangkaian izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (pengguna utama tepercaya) dengan akun berbeda untuk mengakses sumber daya yang ada di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya

(alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.

- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Sebagai contoh, ketika Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Saat Anda menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian memulai tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat permintaan FAS, lihat Teruskan sesi akses.
  - Peran layanan – Peran layanan adalah peran IAM yang diambil oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan dapat menggunakan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat Kapan harus membuat peran IAM (bukan pengguna) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

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

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

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

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk operasi. Sebagai contoh, anggap saja Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

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

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan terkelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang

dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan inline, lihat Memilih 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. 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 yang dilampiri kebijakan tersebut, kebijakan ini menentukan jenis tindakan yang dapat dilakukan oleh pengguna utama tertentu di sumber daya tersebut dan apa ketentuannya. Anda harus menentukan pengguna utama dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

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

Daftar kontrol akses (ACL)

Daftar kontrol akses (ACL) mengendalikan pengguna utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL sama dengan kebijakan berbasis sumber daya, meskipun tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, silakan lihat Gambaran umum daftar kontrol akses (ACL) di Panduan Developer Layanan Penyimpanan Ringkas Amazon.

Tipe kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Tipe-tipe kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda berdasarkan tipe kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan di mana Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM (pengguna 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 secara eksplisit terhadap salah satu kebijakan ini akan mengesampingkan izin tersebut. 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 teruskan sebagai parameter saat Anda membuat sesi sementara secara terprogram untuk peran atau pengguna gabungan. 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 membatalkan izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Beberapa jenis kebijakan

Ketika beberapa jenis kebijakan berlaku untuk sebuah 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: AWSWickrFullAccess

Anda dapat melampirkan kebijakan `AWSWickrFullAccess` ke identitas IAM Anda. Kebijakan ini memberikan izin administratif penuh ke layanan Wickr, termasuk AWS Management Console untuk Wickr di. AWS Management ConsoleUntuk 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.

```
{
    "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.

Perubahan	Deskripsi	Tanggal
AWSWickrFullAccess – Kebijakan baru	Wickr menambahkan kebijakan baru yang memberikan izin administr atif penuh ke layanan Wickr, termasuk konsol administrator Wickr di. AWS Management Console	28 November 2022
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 persyaratan kebijakan	Tidak
ACL	Tidak
ABAC (tanda dalam kebijakan)	Tidak
Kredensial sementara	Tidak
Izin pengguna utama	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 pengguna dan peran, di sumber daya mana, dan dengan ketentuan apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak, serta ketentuan terkait jenis tindakan yang diizinkan atau ditolak. Anda tidak dapat menentukan pengguna utama dalam kebijakan berbasis identitas karena kebijakan ini berlaku untuk pengguna atau peran yang dilampiri kebijakan. Untuk mempelajari semua elemen yang dapat digunakan 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 yang dilampiri kebijakan tersebut, kebijakan ini menentukan jenis tindakan yang dapat dilakukan oleh pengguna utama tertentu di sumber daya tersebut dan apa ketentuannya. Anda harus menentukan pengguna utama dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan seluruh akun atau entitas IAM di akun lain sebagai pengguna utama dalam kebijakan berbasis sumber daya. Menambahkan pengguna utama lintas akun ke kebijakan berbasis sumber daya bagian dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses

sumber daya. Izin diberikan dengan melampirkan kebijakan berbasis identitas ke entitas tersebut. Namun, jika kebijakan berbasis sumber daya memberikan akses kepada pengguna utama dalam akun yang sama, kebijakan berbasis identitas lainnya tidak diperlukan. Untuk informasi selengkapnya, lihat Perbedaan peran IAM dengan kebijakan berbasis sumber daya di 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, pengguna utama mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam suatu kebijakan untuk memberikan izin 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-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, pengguna utama mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek atau beberapa objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk mengindikasikan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

Untuk melihat daftar jenis sumber daya Wickr dan ARNnya, 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 spesifik layanan	Tidak

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

Elemen `Condition` (atau blok `Condition`) memungkinkan Anda menentukan kondisi di mana suatu pernyataan akan diterapkan. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi kondisional yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

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

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

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi 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

ACL di Wickr

Mendukung ACL	Tidak

Daftar kontrol akses (ACL) mengontrol pengguna utama (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL sama dengan kebijakan berbasis sumber daya, meskipun tidak menggunakan format dokumen kebijakan JSON.

ABAC dengan Wickr

Mendukung ABAC (tanda dalam kebijakan)	Tidak

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Pemberian tanda ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian, rancanglah kebijakan ABAC untuk mengizinkan operasi saat tag milik pengguna utama cocok dengan tag yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi di mana pengelolaan kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag di elemen kondisi dari kebijakan dengan 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 hanya untuk beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Apa itu ABAC? di Panduan Pengguna IAM. Untuk melihat tutorial terkait langkah-langkah penyiapan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) di Panduan Pengguna IAM.

Menggunakan kredensyal sementara dengan Wickr

Mendukung kredensial sementara	Tidak

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

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensil sementara. Anda juga akan membuat kredensial sementara secara otomatis saat

masuk ke konsol sebagai pengguna dan kemudian beralih peran. Untuk informasi selengkapnya tentang cara beralih peran, lihat Beralih peran (konsol) di Panduan Pengguna IAM.

Anda dapat membuat kredensyal sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensyal sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Izin utama lintas layanan untuk Wickr

Mendukung sesi akses maju (FAS)	Tidak

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

Peran layanan untuk Wickr

Mendukung peran layanan	Tidak

Peran layanan adalah sebuah 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 Membuat 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 dapat menggunakan 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 pengelolaan peran terkait layanan, lihat Layanan AWS yang berfungsi dengan IAM. Temukan sebuah 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.

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

Kebijakan contoh ini memberi pengguna izin untuk membuat, melihat, dan mengelola jaringan Wickr menggunakan for Wickr. AWS Management Console 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.

Topik

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Wickr di akun Anda. Tindakan ini dikenai biaya untuk Akun AWS Anda. 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 pekerjaan di 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 melakukan ini dengan menentukan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk menerapkan izin, lihat Kebijakan dan izin di IAM di Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Syarat di Panduan Pengguna IAM.
- Menggunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda guna memastikan izin yang aman dan berfungsi – 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 Analizer Akses IAM di 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 mewajibkan MFA saat operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA di Panduan Pengguna IAM.

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

Menggunakan AWS Management Console 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. AWS Management Console Untuk informasi selengkapnya, lihat AWS kebijakan terkelola: AWSWickrFullAccess.

Izinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan para 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 AWS Management Console for Wickr

Saya tidak berwenang untuk melakukan tindakan administratif di AWS Management Console for Wickr

Jika AWS Management Console 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 AWS Management Console untuk membuat, mengelola, atau melihat

jaringan Wickr di AWS Management Console 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 AWS Management Console untuk Wickr menggunakan dan tindakan. `wickr:CreateAdminSession` `wickr:ListNetworks` Lihat informasi yang lebih lengkap di Contoh kebijakan berbasis identitas untuk AWS Wickr dan AWS kebijakan terkelola: AWSWickrFullAccess.

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— 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.

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 AWS Management Console untuk Wickr dengan mengautentikasi ke yang pertama. AWS Management Console Jangan bagikan kredensyal 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 denganAWS 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 AWS Management Console 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 AndaAkun 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 partisi AWS 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 peristiwa atau entri log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut ini:

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

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 AWS Management Console untuk Wickr di https://console.aws.amazon.com/wickr/.
2. 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
Federasi Global sekarang mendukung federasi terbatas dan admin dapat melihat analisis penggunaan di Konsol Admin	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	Administrator Wickr sekarang dapat mengakses berbagai fitur baru, termasuk daftar	8 November 2023

banyak kontrol admin telah ditambahkan	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.	
Wickr sekarang tersedia di Eropa (Frankfurt) Wilayah AWS	Wickr sekarang tersedia di Eropa (Frankfurt). Wilayah AWS Untuk informasi lebih lanjut, lihat Mengakses Wickr.	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) Wilayah AWS	Wickr sekarang tersedia di Eropa (London). Wilayah AWS Untuk informasi lebih lanjut, lihat Mengakses Wickr.	23 Agustus 2023
Wickr sekarang tersedia di Kanada (Tengah) Wilayah AWS	Wickr sekarang tersedia di Kanada (Tengah). Wilayah AWS Untuk informasi lebih lanjut, lihat Mengakses Wickr.	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 WickrGovdi Panduan AWS GovCloud (US) Pengguna.	30 Maret 2023
Penandaan dan pembuatan beberapa jaringan	Penandaan sekarang didukung di AWS Wickr. Untuk informasi selengkapnya, lihat Mengelola 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.

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 menghapus/menangguhkan pengguna secara massal.
  - Pengaturan SSO tambahan untuk mengonfigurasi masa tenggang untuk penyegaran token.

Oktober 2023

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

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). Wilayah AWS

Juli 2023

- Penyempurnaan
  - Wickr sekarang tersedia di Kanada (Tengah). Wilayah AWS

Mei 2023

- Penyempurnaan
  - Menambahkan dukungan untuk pengguna tamu. Untuk informasi selengkapnya, lihat Pengguna tamu.

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 WickrGovdi Panduan AWS GovCloud (US) Pengguna.
- Wickr sekarang mendukung penandaan. Untuk informasi selengkapnya, lihat Kelola tag jaringan. 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.