관리 설명서

AWS Wickr

AWS Wickr: 관리 설명서

Table of Contents

AWS Wickr란 무엇입니까?

AWS Wickr는 조직과 정부 기관이 일대일 및 그룹 메시지, 음성 및 영상 통화, 파일 공유, 화면 공유 등을 통해 안전하게 통신할 수 있도록 지원하는 종단 간 암호화 서비스입니다. Wickr는 고객이 소비자용 메시징 앱과 관련된 데이터 보존 의무를 극복하고 협업을 안전하게 촉진하도록 지원할 수 있습니다. 고급 보안 및 관리 제어를 통해 조직은 법률 및 규제 요구 사항을 충족하고 데이터 보안 문제에 대한 맞춤형 솔루션을 구축할 수 있습니다.

보존 및 감사 목적으로 고객이 제어하는 개인 데이터 스토어에 정보를 기록할 수 있습니다. 사용자는 권한 설정, 임시 메시징 옵션 구성, 보안 그룹 정의 등 데이터에 대한 포괄적인 관리 제어를 할 수 있습니다. Wickr는 액티브 디렉터리(AD), OpenID Connect(OIDC)를 가진 Single Sign-On(SSO) 등과 같은 추가 서비스와 통합됩니다. 를 통해 Wickr 네트워크를 빠르게 생성 및 관리하고 Wickr 봇을 사용하여 워크플로를 AWS Management Console안전하게 자동화할 수 있습니다. 시작하려면 AWS Wickr에 대한 설정 섹션을 참조하십시오.

주제

- Wickr의 기능
- 리전별 가용성
- Wickr에 액세싱
- 가격 책정
- Wickr 최종 사용자 설명서

Wickr의 기능

향상된 보안 및 개인정보 보호

Wickr는 모든 기능에 대해 256비트 고급 암호화 표준(AES) 종단 간 암호화를 사용합니다. 통신은 사용자 디바이스에서 로컬로 암호화되며 발신자와 수신자를 제외한 다른 사람이 전송하는 동안에는 해독할 수 없습니다. 모든 메시지, 호출 및 파일은 새 임의 키로 암호화되며 의도한 수신자(짝수 아님 AWS) 외에는 아무도 복호화할 수 없습니다. 민감하고 규제된 데이터를 공유하든, 법률 또는 HR 문제를 논의하든, 심지어 전술적 군사 작전을 수행하든, 고객은 보안과 개인 정보 보호가 가장 중요할 때 Wickr를 사용하여 통신합니다.

데이터 보존

유연한 관리 기능은 민감한 정보를 보호할 뿐만 아니라 규정 준수 의무, 법적 보존 및 감사 목적에 필요한 만큼 데이터를 보관하도록 설계되었습니다. 메시지와 파일은 고객이 제어하는 안전한 데이터 스토어에 보관할 수 있습니다.

유연한 액세스

사용자는 다중 디바이스(모바일, 데스크톱)에 액세스할 수 있으며 연결이 끊긴 통신 및 대역외 통신을 비롯한 저대역폭 환경에서 기능할 수 있습니다.

관리 제어

사용자는 권한 설정, 임시 메시징 옵션 구성, 보안 그룹 정의 등 데이터에 대한 포괄적인 관리 제어를 할 수 있습니다.

강력한 통합 및 봇

Wickr는 Active Directory, OpenID Connect(OIDC)를 통한 Single Sign-On(SSO) 등과 같은 추가 서비스와 통합됩니다. 고객은를 통해 Wickr 네트워크를 빠르게 생성 및 관리하고 Wickr 봇을 사용하여 워크플로를 AWS Management Console안전하게 자동화할 수 있습니다.

다음은 Wickr 협업 상품의 세부 내용입니다.

- 1:1 및 그룹 메시지: 최대 500명의 구성원이 있는 룸에서 팀과 안전하게 채팅
- 음성 및 영상 통화: 최대 70명과 컨퍼런스 콜 진행
- 화면 공유 및 방송: 최대 500명의 참가자와 프레젠테이션 진행
- 파일 공유 및 저장: 무제한 저장으로 최대 5GB까지 파일 전송
- 임시: 만료 및 번온리드 타이머 제어
- 글로벌 페더레이션: 네트워크 외부의 Wickr 사용자와 연결

리전별 가용성

Wickr는 미국 동부(버지니아 북부), 아시아 태평양(말레이시아), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 아시아 태평양(도쿄), 캐나다(중부), 유럽(프랑크푸르트), 유럽(런던), 유럽(스톡홀름) 및 유럽(취리히)에서 사용할 수 있습니다 AWS 리전. Wickr는 AWS GovCloud(미국 서부) 리전에서도 사용할 수 있습니다. 각 리전에는 물리적으로 분리되어 있지만 프라이빗, 저지연, 고대역폭 및 중복 네트워크 연결로 연결되는 여러 가용 영역이 포함되어 있습니다. 이러한 가용 영역은 향상된 가용성, 내결함성 및 지연 시간 최소화를 제공하는 데 사용됩니다.

자세한 내용은에서 계정에서 사용할 수 있는 지정을 AWS 리전참조하세요AWS 일반 참조. AWS 리전 각 리전에서 사용 가능한 가용 영역 수에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

Wickr에 액세싱

관리자는 https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr에 액세스합니다. Wickr 사용을 시작하기 전에 먼저 AWS Wickr에 대한 설정 및 AWS Wickr 사용 시작하기 안내서를 작성해야 합니다.

최종 사용자는 Wickr 클라이언트를 통해 Wickr에 액세스합니다. 자세한 내용은 AWS Wickr 사용 설명서를 참조하십시오.

가격 책정

Wickr는 개인, 소규모 팀 및 대기업을 위해 다양한 요금제로 제공됩니다. 자세한 내용은 AWS Wickr 요금 책정을 참조하십시오.

Wickr 최종 사용자 설명서

Wickr 클라이언트의 최종 사용자이고 해당 설명서에 액세스해야 하는 경우 AWS Wickr 사용 설명서를 참조하십시오.

AWS Wickr에 대한 설정

신규 AWS 고객인 경우 AWS Wickr 사용을 시작하기 전에이 페이지에 나열된 설정 사전 조건을 완료합니다. 이러한 설정 절차에서는 AWS Identity and Access Management (IAM) 서비스를 사용합니다. IAM에 대한 전체 내용은 IAM 사용 설명서를 참조하십시오.

주제

에 가입 AWS

이 없는 경우 다음 단계를 AWS 계정완료하여 생성합니다.

에 가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. 온라인 지시 사항을 따르세요.

   등록 절차 중 전화 또는 텍스트 메시지를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   에 가입하면 AWS 계정AWS 계정 루트 사용자이 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

IAM 사용자를 생성합니다.

다음 옵션 중 하나를 선택하여 관리 사용자를 생성합니다.

관리자를 관리하는 방법 한 가지 선택	목적	By	다른 방법
IAM Identity Center에서 (권장)	단기 보안 인증 정보를 사용하여 AWS에 액세스합니다. 이는 보안 모범 사례와 일치합니다. 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.	AWS IAM Identity Center 사용 설명서의 시작하기 지침을 따릅니다.	AWS Command Line Interface 사용 설명서에서 사용하도록 AWS CLI 를 구성 AWS IAM Identity Center하여 프로그래밍 방식 액세스를 구성합니다.
IAM에서 (권장되지 않음)	장기 보안 인증 정보를 사용하여 AWS에 액세스합니다.	IAM 사용 설명서의 첫 IAM 관리 사용자 및 사용자 그룹 만들기에 나온 지침을 따릅니다.	IAM 사용 설명서에 나온 IAM 사용자의 액세스 키 관리 단계를 수행하여 프로그래밍 방식 액세스를 구성합니다.

> **Note**
>
> `AWSWickrFullAccess`관리형 정책을 할당하여 Wickr 서비스에 전체 관리 권한을 부여할 수도 있습니다. 자세한 내용은 AWS 관리형 정책: AWSWickrFullAccess 섹션을 참조하십시오.

다음에 있는 것

사전 요구 사항 설정 단계를 완료했습니다. Wickr 구성을 시작하려면 을 참조하십시오. 시작하기

AWS Wickr 사용 시작하기

이 설명서에서는 네트워크를 생성하고, 네트워크를 구성하고, 사용자를 생성하여 Wickr로 시작하는 방법을 안내합니다.

주제

사전 조건

시작에 앞서 아직 완료하지 않았다면 반드시 사전 조건을 완료하십시오.

- Amazon Web Services(AWS) 가입. 자세한 내용은 AWS Wickr에 대한 설정 섹션을 참조하십시오.
- Wickr를 관리하는 데 필요한 권한이 있는지 확인합니다. 자세한 내용은 AWS 관리형 정책: AWSWickrFullAccess 섹션을 참조하십시오.
- Wickr에 적합한 포트 및 도메인 목록을 허용했는지 확인하십시오. 자세한 내용은 Wickr 네트워크에 대한 목록을 허용할 포트 및 도메인 섹션을 참조하십시오.

1단계: 네트워크 생성

Wickr 네트워크를 생성할 수 있습니다.

계정을 위해 Wickr 네트워크를 생성하려면 다음 절차를 완료하십시오.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.

   > **Note**
   >
   > 이전에 Wickr 네트워킹을 만든 적이 없다면 Wickr 서비스에 대한 정보 페이지를 볼 수 있습니다. 하나 이상의 Wickr 네트워크를 만들고 나면 생성한 모든 Wickr 네트워크의 목록 보기가 포함된 네트워크 페이지가 나타납니다.

2. 네트워크 만들기를 선택합니다.

3. 네트워크 이름 텍스트 상자에 네트워크 이름을 입력합니다. 회사 이름이나 팀 이름과 같이 조직 구성원이 알아볼 수 있는 이름을 선택합니다.
4. 계획을 선택하십시오. 다음 Wickr 네트워크 플랜 중 하나를 선택할 수 있습니다.

   - 표준 - 관리 제어 및 유연성이 필요한 소규모 및 대규모 비즈니스 팀을 위한 것입니다.
   - 프리미엄 또는 프리미엄 무료 평가판 - 가장 높은 기능 제한, 세분화된 관리 제어 및 데이터 보존이 필요한 기업용입니다.

   관리자는 최대 30명의 사용자가 사용할 수 있고 3개월 동안 지속되는 프리미엄 무료 평가판을 선택할 수 있습니다. For AWS WickrGov의 프리미엄 무료 평가판 옵션은 최대 50명의 사용자를 허용하며 3개월 동안 지속됩니다. 프리미엄 무료 평가판 기간 동안 관리자는 Premium 또는 Standard 플랜으로 업그레이드하거나 다운그레이드할 수 있습니다.

   사용 가능한 Wickr 계획 및 요금 정책에 대한 자세한 내용은 Wickr 요금 책정 페이지를 참조하십시오.
5. (선택 사항) 네트워크에 태그를 추가하려면 새 태그 추가를 선택합니다. 태그는 키-값 쌍으로 이루어져 있습니다. 태그를 사용하여 리소스를 검색 및 필터링하거나 사용자의 AWS 비용을 추적할 수 있습니다. 자세한 내용은 네트워크 태그를 참조하세요.
6. 네트워크 생성을 선택합니다.

   Wickr AWS Management Console 용의 네트워크 페이지로 리디렉션되고 새 네트워크가 페이지에 나열됩니다.

2단계: 사용자 네트워크 구성

사용자를 추가하고, 보안 그룹을 추가하고, SSO를 구성하고, 데이터 보존을 구성하고, 네트워크 설정을 추가할 수 있는 Wickr AWS Management Console 용에 액세스하려면 다음 절차를 완료하세요.

1. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.

   선택된 네트워크의 Wickr 관리 콘솔로 리디렉션됩니다.
2. 다음과 같은 사용자 관리 옵션을 사용할 수 있습니다. 이러한 설정을 구성하는 것에 대한 자세한 내용은 AWS Wickr 네트워크 관리 섹션을 참조하십시오.

   - 보안 그룹 — 비밀번호 복잡성 정책, 메시징 기본 설정, 통화 기능, 보안 기능 및 외부 페더레이션과 같은 보안 그룹 및 해당 설정을 관리합니다. 자세한 내용은 AWS Wickr의 보안 그룹 단원을 참조하십시오.

- SSO(Single Sign-On) 구성 - SSO를 구성하고 Wickr 네트워크의 엔드포인트 주소를 확인합니다. Wickr는 OpenID Connect(OIDC)를 사용하는 SSO 공급자만 지원합니다. Security Assertion Markup Language(SAML)를 사용하는 공급자는 지원되지 않습니다. 자세한 내용은 AWS Wickr에 대한 Single Sign-On 구성 섹션을 참조하십시오.

3단계: 사용자 생성 및 초대

다음 방법을 사용하여 Wickr 네트워크에 사용자를 생성할 수 있습니다.

- 싱글 사인온 — 싱글 사인온(SSO)을 구성하면 Wickr 회사 ID를 공유하여 사용자를 초대할 수 있습니다. 최종 사용자는 제공된 회사 ID와 회사 이메일 주소를 사용하여 Wickr에 등록합니다. 자세한 내용은 AWS Wickr에 대한 Single Sign-On 구성 섹션을 참조하십시오.
- 초대 — AWS Management Console for Wickr에서 수동으로 사용자를 생성하고 이메일 초대장을 보내도록 할 수 있습니다. 최종 사용자는 이메일에서 링크를 선택하여 Wickr에 등록할 수 있습니다.

> **Note**
>
> Wickr 네트워크에서 게스트 사용자를 활성화할 수도 있습니다. 자세한 내용은 AWS Wickr 네트워크의 게스트 사용자 섹션을 참조하세요.

사용자를 생성하거나 초대하려면 다음 절차를 완료하십시오.

> **Note**
>
> 관리자 역시 사용자로 간주되므로 SSO 또는 비 SSO Wickr 네트워크에 그 자신을 초대해야 합니다.

Wickr 사용자를 생성하고 SSO로 초대를 보내려면:

Wickr에 등록해야 하는 SSO 사용자에게 이메일을 작성하여 보내십시오. 사용자의 이메일에 다음 정보를 포함합니다.

- 사용자의 Wickr 회사 ID. 사용자가 SSO를 구성할 때 Wickr 네트워크의 회사 ID를 지정합니다. 자세한 내용은 AWS Wickr에서 SSO 구성 섹션을 참조하십시오.
- 가입할 때 사용해야 하는 이메일 주소.

- Wickr 클라이언트를 다운로드할 URL입니다. 사용자는 https://aws.amazon.com/wickr/download/의 Wickr 다운로드 페이지에서 AWS Wickr 클라이언트를 다운로드할 수 있습니다.

> **Note**
>
> Wickr 네트워크를 in AWS GovCloud(미국 서부)에서 생성한 경우 사용자에게 WickrGov 클라이언트를 다운로드하고 설치하도록 지시합니다. 다른 모든 AWS 리전의 경우 사용자에게 표준 Wickr 클라이언트를 다운로드하고 설치하도록 지시합니다. AWS WickrGov에 대한 자세한 내용은 AWS GovCloud (US) 사용 설명서의 AWS WickrGov를 참조하세요.

사용자가 Wickr 네트워크에 등록하였으므로, 사용자는 Wickr 팀 디렉터리에 활성 상태로 추가됩니다.

Wickr 사용자를 수동으로 생성하고 초대장을 보내려면:

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.

   Wickr 네트워크로 리디렉션됩니다. Wickr 네트워크에서 사용자를 추가하고, 보안 그룹을 추가하고, SSO를 구성하고, 데이터 보존을 구성하고, 추가 설정을 조정할 수 있습니다.
3. 탐색 창에서 사용자 관리를 선택합니다.
4. 사용자 관리 페이지의 팀 디렉터리 탭에서 사용자 초대를 선택합니다.

   사용자 초대 옆의 드롭다운 화살표를 선택하여 사용자를 대량으로 초대할 수도 있습니다. 사용자 대량 초대 페이지에서 템플릿 다운로드를 선택하여 사용자 목록과 함께 편집하고 업로드할 수 있는 CSV 템플릿을 다운로드합니다.
5. 사용자의 이름, 성, 국가 코드, 전화번호 및 이메일 주소를 입력합니다. 이메일 주소는 유일한 필수 필드입니다. 반드시 사용자에게 적합한 보안 그룹을 선택해야 합니다.
6. 초대를 선택합니다.

   Wickr는 사용자가 지정한 주소로 초대 이메일을 보냅니다. 이메일은 Wickr 클라이언트 애플리케이션의 다운로드 링크와 Wickr 등록용 링크를 제공합니다. 이러한 최종 사용자 경험이 어떤 모습인지에 대한 자세한 내용은 AWS Wickr 사용 설명서의 Wickr 앱 다운로드 및 초대 수락을 참조하십시오.

   사용자가 이메일에 있는 링크를 사용하여 Wickr에 등록함에 따라 Wickr 팀 디렉토리에서의 사용자 상태가 보류 중에서 활성으로 변경됩니다.

다음 단계

시작하기 단계를 마쳤습니다. Wickr를 관리하려면 다음을 참조하세요.

- AWS Wickr 네트워크 관리
- AWS Wickr에서 사용자 관리

AWS Wickr 네트워크 관리

AWS Management Console for Wickr에서 Wickr 네트워크 이름, 보안 그룹, SSO 구성 및 데이터 보존 설정을 관리할 수 있습니다.

주제

AWS Wickr의 네트워크 세부 정보

Wickr용의 네트워크 세부 정보 섹션에서 Wickr 네트워크의 이름을 편집하고 네트워크 ID AWS Management Console 를 볼 수 있습니다.

주제

AWS Wickr에서 네트워크 세부 정보 보기

네트워크 이름 및 네트워크 ID를 포함하여 Wickr 네트워크의 세부 정보를 볼 수 있습니다.

Wickr 네트워크 프로필 및 네트워크 ID를 보려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 보려는 네트워크를 찾습니다.
3. 보려는 네트워크의 오른쪽에서 세로 줄임표 아이콘(점 3개)을 선택한 다음 세부 정보 보기를 선택합니다.

   네트워크 홈 페이지에는 네트워크 세부 정보 섹션에 Wickr 네트워크 이름과 네트워크 ID가 표시됩니다. 네트워크 ID를 사용하여 페더레이션을 구성할 수 있습니다.

AWS Wickr에서 네트워크 이름 편집

Wickr 네트워크의 이름을 편집할 수 있습니다.

Wickr 네트워크 이름을 편집하려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크의 Wickr 관리 콘솔로 이동합니다.
3. 네트워크 홈 페이지의 네트워크 세부 정보 섹션에서 편집을 선택합니다.
4. 네트워크 이름 텍스트 상자에 네트워크 이름을 입력합니다.
5. 저장을 선택하여 새 네트워크 이름을 저장합니다.

AWS Wickr에서 네트워크 삭제

AWS Wickr 네트워크를 삭제할 수 있습니다.

> **Note**
>
> 프리미엄 무료 평가판 네트워크를 삭제하면 다른 네트워크를 생성할 수 없습니다.

네트워크 홈 페이지에서 Wickr 네트워크를 삭제하려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 삭제할 네트워크를 찾습니다.
3. 삭제할 네트워크의 오른쪽에서 세로 줄임표 아이콘(점 3개)을 선택한 다음 네트워크 삭제를 선택합니다.
4. 팝업 창에 confirm을 입력한 다음 삭제를 선택합니다.

네트워크를 삭제하는 데 몇 분 정도 걸릴 수 있습니다.

네트워크에 있는 동안 Wickr 네트워크를 삭제하려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 삭제할 네트워크를 선택합니다.
3. 네트워크 홈 페이지의 오른쪽 상단 모서리 근처에서 네트워크 삭제를 선택합니다.
4. 팝업 창에 confirm을 입력한 다음 삭제를 선택합니다.

   네트워크를 삭제하는 데 몇 분 정도 걸릴 수 있습니다.

> **Note**
>
> 네트워크를 삭제해도 데이터 보존 구성에서 보존한 데이터(활성화된 경우)는 삭제되지 않습니다. 자세한 내용은 AWS Wickr의 데이터 보존을 참조하세요.

AWS Wickr의 보안 그룹

Wickr AWS Management Console 용의 보안 그룹 섹션에서 암호 복잡성 정책, 메시징 기본 설정, 호출 기능, 보안 기능 및 네트워크 페더레이션과 같은 보안 그룹 및 해당 설정을 관리할 수 있습니다.

주제

- AWS Wickr에서 보안 그룹 보기
- AWS Wickr에서 보안 그룹 생성
- AWS Wickr에서 보안 그룹 편집
- AWS Wickr에서 보안 그룹 삭제

AWS Wickr에서 보안 그룹 보기

Wickr 보안 그룹의 세부 정보를 볼 수 있습니다.

보안 그룹을 보려면 다음 절차를 완료하십시오.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.

3. 탐색 창에서 Security groups를 선택합니다.

   보안 그룹 페이지에는 현재 Wickr 보안 그룹이 표시되고 새 그룹을 생성할 수 있는 옵션이 제공됩니다.

   보안 그룹 페이지에서 보려는 보안 그룹을 선택합니다. 페이지에는 해당 보안 그룹에 대한 현재 세부 정보가 표시됩니다.

AWS Wickr에서 보안 그룹 생성

새 Wickr 보안 그룹을 생성할 수 있습니다.

보안 그룹을 만들려면 다음 절차를 완료하십시오.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 Security groups를 선택합니다.
4. 보안 그룹 페이지에서 보안 그룹 생성을 선택하여 새 보안 그룹을 생성합니다.

   > **Note**
   >
   > 기본 이름을 사용하는 새 보안 그룹이 보안 그룹 목록에 자동으로 추가됩니다.

5. 보안 그룹 생성 페이지에서 보안 그룹의 이름을 입력합니다.
6. 보안 그룹 생성을 선택합니다.

   새 보안 그룹 편집에 대한 자세한 내용은 AWS Wickr에서 보안 그룹 편집 단원을 참조하십시오.

AWS Wickr에서 보안 그룹 편집

Wickr 보안 그룹의 세부 정보를 편집할 수 있습니다.

보안 그룹을 편집하려면 다음 절차를 완료하십시오.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 Security groups를 선택합니다.
4. 편집할 보안 그룹의 이름을 선택합니다.

보안 그룹 세부 정보 페이지에는 보안 그룹의 설정이 다른 탭에 표시됩니다.

5. 다음 탭과 해당 설정을 사용할 수 있습니다.

- 보안 그룹 세부 정보 - 보안 그룹 세부 정보 섹션에서 편집을 선택하여 이름을 편집합니다.
- 메시징 - 그룹 구성원의 메시징 기능을 관리합니다.
  - Burn-on-read 사용자가 Wickr 클라이언트에서 burn-on-read 타이머에 설정할 수 있는 최대값을 제어합니다. 자세한 내용은 Wickr 클라이언트에서 메시지 만료 및 연소 타이머 설정을 참조하세요.
  - 만료 타이머 - 사용자가 Wickr 클라이언트에서 메시지 만료 타이머에 설정할 수 있는 최대값을 제어합니다. 자세한 내용은 Wickr 클라이언트에서 메시지 만료 및 연소 타이머 설정을 참조하세요.
  - 메시지 전달 - 사용자가 Wickr 클라이언트에서 메시지를 전달할 수 있는지 여부를 제어합니다. 자세한 내용은 Wickr 클라이언트에서 메시지 전달을 참조하세요.
  - 빠른 응답 - 사용자가 메시지에 응답할 수 있는 빠른 응답 목록을 설정합니다.
  - 보안 파쇄기 강도 - 보안 파쇄기 제어가 사용자에 대해 실행되는 빈도를 구성합니다. 자세한 내용은 메시징을 참조하세요.
- 통화 — 그룹 구성원의 통화 기능을 관리합니다.
  - 오디오 통화 활성화 - 사용자가 오디오 통화를 시작할 수 있습니다.
  - 영상 통화 및 화면 공유 활성화 - 사용자가 영상 통화를 시작하거나 통화 중에 화면을 공유할 수 있습니다.
  - TCP 호출 - TCP 호출 활성화(또는 강제)는 일반적으로 조직의 IT 또는 보안 부서에서 표준 VoIP UDP 포트를 허용하지 않을 때 사용됩니다. TCP 호출이 비활성화되어 있고 UDP 포트를 사용할 수 없는 경우 Wickr 클라이언트는 먼저 UDP를 시도하고 TCP로 폴백합니다.
- 미디어 및 링크 - 그룹 멤버의 미디어 및 링크와 관련된 설정을 관리합니다.

  파일 다운로드 크기 - 사용자가 원래 암호화된 형식으로 파일과 첨부 파일을 전송할 수 있도록 최상의 품질 전송을 선택합니다. 대역폭 전송 부족을 선택하면 Wickr에서 사용자가 보낸 파일 첨부 파일이 Wickr 파일 전송 서비스에 의해 압축됩니다.
- 위치 - 그룹 멤버의 위치 공유 설정을 관리합니다.

  위치 공유 - 사용자는 GPS 지원 디바이스를 사용하여 위치를 공유할 수 있습니다. 이 기능은 디바이스의 운영 체제 기본값을 기반으로 시각적 맵을 표시합니다. 사용자는 맵 보기를 비활성화하고 대신 GPS 좌표가 포함된 링크를 공유할 수 있습니다.
- 보안 - 그룹에 대한 추가 보안 기능을 구성합니다.

    - 계정 탈취 보호 활성화 - 사용자가 계정에 새 디바이스를 추가할 때 2단계 인증을 적용합니다. 새 디바이스를 확인하기 위해 사용자는 이전 디바이스에서 Wickr 코드를 생성하거나 이메일 확인을 수행할 수 있습니다. 이는 AWS Wickr 계정에 대한 무단 액세스를 방지하기 위한 추가 보안 계층입니다.
    - 항상 재인증 활성화 - 애플리케이션을 다시 시작할 때 사용자가 항상 재인증하도록 합니다.
    - 마스터 복구 키 - 계정이 생성될 때 마스터 복구 키를 생성합니다. 다른 디바이스를 사용할 수 없는 경우 사용자는 계정에 새 디바이스 추가를 승인할 수 있습니다.
- 알림 및 가시성 - 그룹 구성원에 대한 알림의 메시지 미리 보기와 같은 알림 및 가시성 설정을 구성합니다.
- Wickr 오픈 액세스 - 그룹 멤버에 대한 Wickr 오픈 액세스 설정을 구성합니다.
    - Wickr 오픈 액세스 활성화 - Wickr 오픈 액세스를 활성화하면 트래픽을 위장하여 제한 및 모니터링되는 네트워크의 데이터를 보호합니다. 지리적 위치에 따라 Wickr 오픈 액세스는 트래픽 난독화를 위한 최상의 경로와 프로토콜을 제공하는 다양한 글로벌 프록시 서버에 연결됩니다.
    - Wickr 오픈 액세스 강제 적용 - 모든 디바이스에서 Wickr 오픈 액세스를 자동으로 활성화하고 적용합니다.
- 페더레이션 - 사용자가 다른 Wickr 네트워크와 통신할 수 있는 기능을 제어합니다.
    - 로컬 페더레이션 - 동일한 리전 내 다른 네트워크의 AWS 사용자와 페더레이션할 수 있는 기능입니다. 예를 들어 캐나다(중부) 리전에 AWS 로컬 페더레이션이 활성화된 두 개의 네트워크가 있는 경우 서로 통신할 수 있습니다.
    - 글로벌 페더레이션 - Wickr Enterprise 사용자 또는 다른 리전에 속한 다른 네트워크의 AWS 사용자와 페더레이션할 수 있는 기능입니다. 예를 들어 캐나다(중부) 리전의 Wickr 네트워크에 AWS 있는 사용자와 유럽(런던) 리전의 AWS 네트워크에 있는 사용자는 두 네트워크에 대해 글로벌 페더레이션이 켜져 있을 때 서로 통신할 수 있습니다.
    - 제한된 페더레이션 - 사용자가 페더레이션할 수 있는 특정 AWS Wickr 또는 Wickr Enterprise 네트워크를 나열할 수 있습니다. 구성된 경우 사용자는 나열된 허용 네트워크의 외부 사용자와만 통신할 수 있습니다. 두 네트워크 모두 제한된 페더레이션을 사용하려면 서로 목록을 허용해야 합니다.

      게스트 페더레이션에 대한 자세한 내용은 AWS Wickr 네트워크에서 게스트 사용자 활성화 또는 비활성화를 참조하세요.
- ATAK 플러그인 구성 - ATAK 활성화에 대한 자세한 내용은 ATAK란 무엇입니까?를 참조하세요.

6. 저장을 선택하여 보안 그룹 세부 정보에 대한 편집 내용을 저장합니다.

AWS Wickr에서 보안 그룹 삭제

Wickr 보안 그룹을 삭제할 수 있습니다.

보안 그룹을 삭제하려면 다음 절차를 완료하십시오.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 Security groups를 선택합니다.
4. 보안 그룹 페이지에서 삭제할 보안 그룹을 찾습니다.
5. 삭제할 보안 그룹의 오른쪽에서 세로 줄임표 아이콘(점 3개)을 선택한 다음 삭제를 선택합니다.
6. 팝업 창에 confirm을 입력한 다음 삭제를 선택합니다.

   사용자를 할당한 보안 그룹을 삭제하면 해당 사용자가 기본 보안 그룹에 자동으로 추가됩니다. 사용자에게 할당된 보안 그룹을 수정하려면 AWS Wickr 네트워크에서 사용자 편집을 참조하십시오.

AWS Wickr에 대한 Single Sign-On 구성

Wickr AWS Management Console 용에서 Single Sign-On 시스템을 사용하여 인증하도록 Wickr를 구성할 수 있습니다. SSO는 적절한 다중 인증(MFA) 시스템과 함께 사용할 경우 추가 보안 계층을 제공합니다. Wickr는 OpenID Connect(OIDC)를 사용하는 SSO 공급자만 지원합니다. Security Assertion Markup Language(SAML)를 사용하는 공급자는 지원되지 않습니다.

주제

- AWS Wickr에서 SSO 세부 정보 보기
- AWS Wickr에서 SSO 구성
- 토큰 새로고침 유예 기간

AWS Wickr에서 SSO 세부 정보 보기

Wickr 네트워크 및 네트워크 엔드포인트에 대한 Single Sign-On 구성의 세부 정보를 볼 수 있습니다.

Wickr 네트워크(있는 경우)의 현재 SSO 구성을 보려면 다음 절차를 완료하십시오.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.

3. 탐색 창에서 사용자 관리를 선택합니다.

   사용자 관리 페이지의 Single Sign-On 섹션에는 Wickr 네트워크 엔드포인트와 현재 SSO 구성이 표시됩니다.

AWS Wickr에서 SSO 구성

Wickr 네트워크에 대한 보안 액세스를 보장하기 위해 현재 Single Sign-On 구성을 설정할 수 있습니다. 이 프로세스에 도움이 되는 자세한 가이드가 제공됩니다.

> **Important**
>
> - SSO를 구성할 때 Wickr 네트워크의 회사 ID를 지정합니다. 이 회사 ID를 기록해야 합니다. 초대 이메일을 보낼 때 최종 사용자에게 제공해야 합니다. 최종 사용자는 Wickr 네트워크에 등록할 때 회사 ID를 지정해야 합니다.
> - 2025년 9월에 AWS Wickr는 향상된 보안 SSO 연결 시스템을 도입했습니다. 이러한 보안 개선 사항을 활용하려면 SSO를 사용하는 조직이 2026년 3월 9일까지 새 리디렉션 URI로 마이그레이션해야 합니다. 마이그레이션 지침은 AWS Wickr용 새 SSO 리디렉션 URI로 마이그레이션 AWS re:Post 문서를 참조하세요. https://repost.aws/articles/ARwG2sEMHkShKNn77mc8pc8Q/migrating-to-the-new-sso-redirect-uri-for-aws-wickr

SSO 구성에 대한 자세한 내용은 다음 가이드를 참조하세요.

- Microsoft Entra(Azure AD)를 사용한 AWS Wickr Single Sign-On(SSO) 설정
- Okta를 사용한 AWS Wickr Single Sign-On(SSO) 설정
- Amazon Cognito를 사용한 AWS Wickr Single Sign-On(SSO) 설정

Microsoft Entra(Azure AD) Single Sign-On을 사용하여 AWS Wickr 구성

AWS Wickr는 Microsoft Entra(Azure AD)를 자격 증명 공급자로 사용하도록 구성할 수 있습니다. 이렇게 하려면 Microsoft Entra와 AWS Wickr 관리자 콘솔 모두에서 다음 절차를 완료합니다.

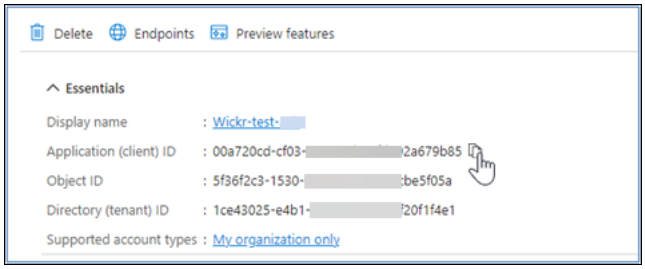
> **Warning**
>
> 네트워크에서 SSO가 활성화되면 활성 사용자가 Wickr에서 로그아웃하고 SSO 공급자를 사용하여 다시 인증하도록 강제합니다.

1단계: AWS Wickr를 Microsoft Entra의 애플리케이션으로 등록

다음 절차를 완료하여 AWS Wickr를 Microsoft Entra의 애플리케이션으로 등록합니다.

> **Note**
>
> 자세한 스크린샷 및 문제 해결은 Microsoft Entra 설명서를 참조하세요. 자세한 내용은 Microsoft 자격 증명 플랫폼에 애플리케이션 등록을 참조하세요.

1. 탐색 창에서 애플리케이션을 선택한 다음 앱 등록을 선택합니다.
2. 앱 등록 페이지에서 애플리케이션 등록을 선택한 다음 애플리케이션 이름을 입력합니다.
3. 이 조직 디렉터리에서만 계정을 선택합니다(기본 디렉터리만 - 단일 테넌트).
4. 리디렉션 URI에서 웹을 선택한 다음 AWS Wickr Admin 콘솔의 SSO 구성 설정에서 사용할 수 있는 리디렉션 URI를 입력합니다.
5. 등록을 선택합니다.
6. 등록 후 생성된 애플리케이션(클라이언트) ID를 복사/저장합니다.



7. 엔드포인트 탭을 선택하여 다음 사항을 기록해 둡니다.

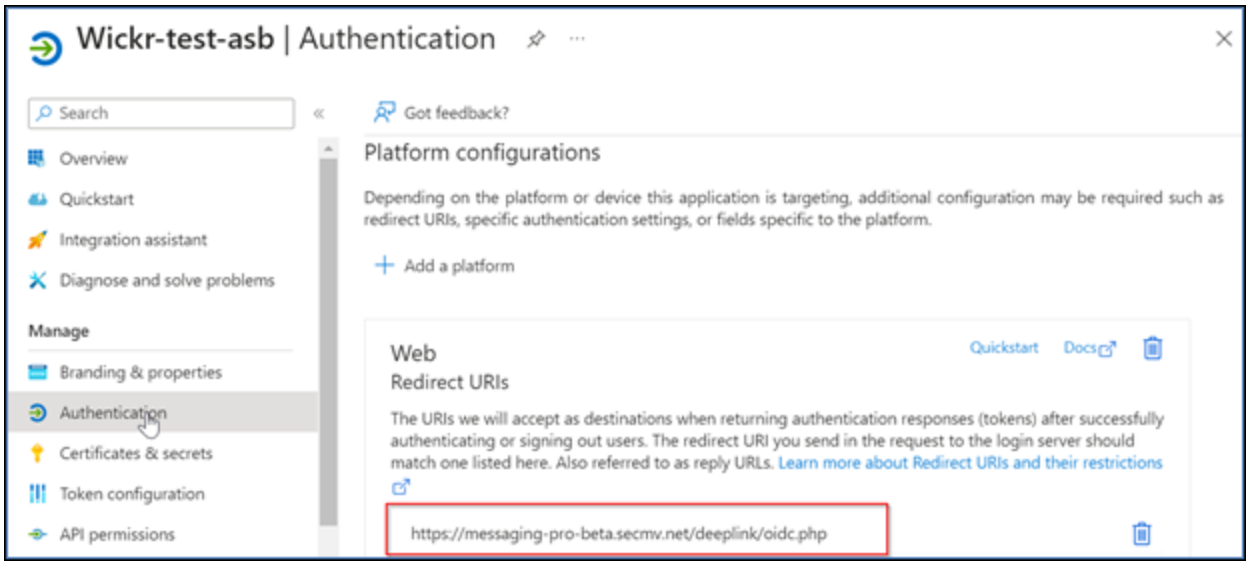
   1. Oauth 2.0 권한 부여 엔드포인트(v2): 예: `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/oauth2/v2.0/authorize`
   2. 이 값을 편집하여 'oauth2/' 및 'authorize'를 제거합니다. 예: 고정 URL은 다음과 같습니다. `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`

3. 이를 SSO 발급자라고 합니다.

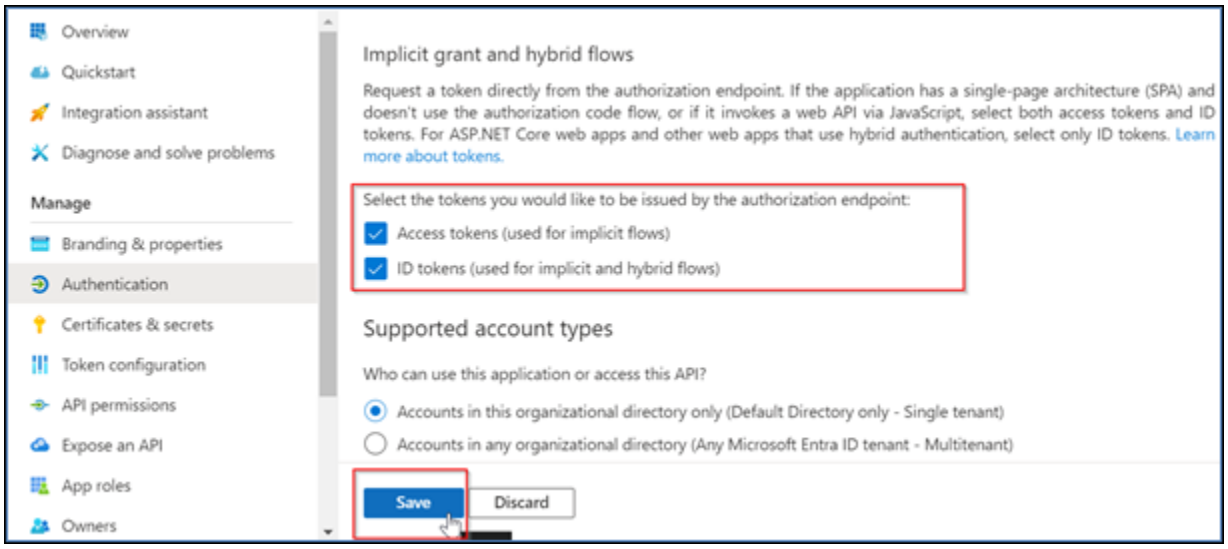
2단계: 인증 설정

Microsoft Entra에서 인증을 설정하려면 다음 절차를 완료하세요.

1. 탐색 창에서 인증을 선택합니다.
2. 인증 페이지에서 웹 리디렉션 URI가 이전에 입력한 것과 동일한지 확인합니다(AWS Wickr를 애플리케이션으로 등록).



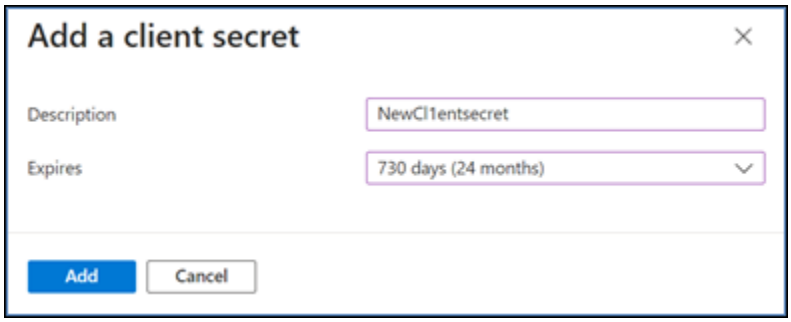
3. 암시적 흐름에 사용되는 액세스 토큰과 암시적 및 하이브리드 흐름에 사용되는 ID 토큰을 선택합니다.
4. 저장을 선택합니다.



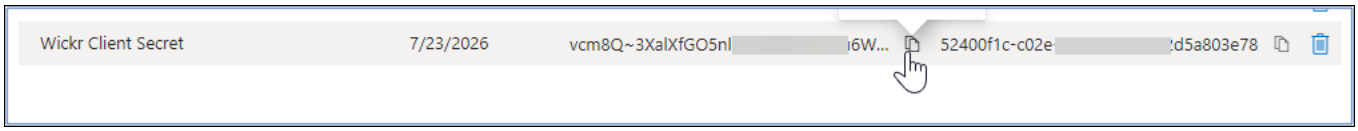
3단계: 인증서 및 보안 암호 설정

Microsoft Entra에서 인증서와 보안 암호를 설정하려면 다음 절차를 완료하세요.

1. 탐색 창에서 인증서 및 보안 암호를 선택합니다.
2. 인증서 및 보안 암호 페이지에서 클라이언트 보안 암호 탭을 선택합니다.
3. 클라이언트 보안 암호 탭에서 새 클라이언트 보안 암호를 선택합니다.
4. 설명을 입력하고 보안 암호의 만료 기간을 선택합니다.
5. 추가를 선택합니다.



6. 인증서를 생성한 후 클라이언트 보안 암호 값을 복사합니다.



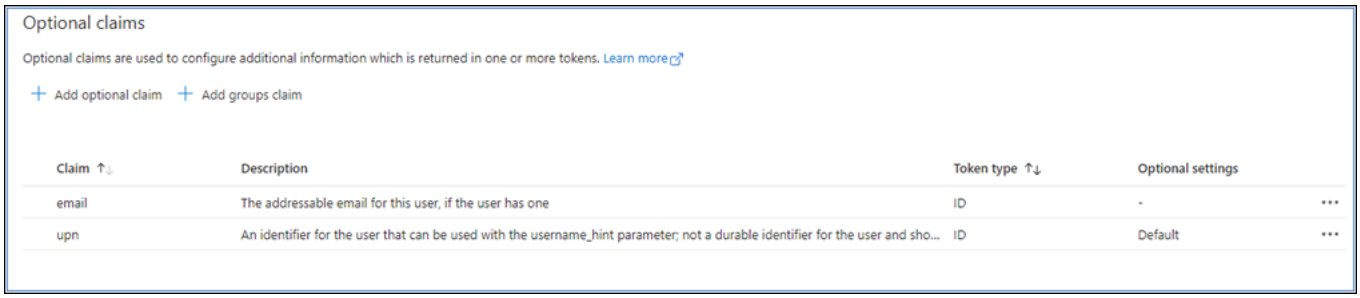
> **Note**
>
> 클라이언트 애플리케이션 코드에는 클라이언트 보안 암호 값(보안 암호 ID 아님)이 필요합니다. 이 페이지를 나간 후 보안 암호 값을 보거나 복사하지 못할 수 있습니다. 지금 복사하지 않으면 다시 돌아가서 새 클라이언트 암호를 생성해야 합니다.

4단계: 토큰 구성 설정

Microsoft Entra에서 토큰 구성을 설정하려면 다음 절차를 완료하세요.

1. 탐색 창에서 토큰 구성을 선택합니다.
2. 토큰 구성 페이지에서 선택적 클레임 추가를 선택합니다.
3. 선택적 클레임에서 토큰 유형을 ID로 선택합니다.
4. ID를 선택한 후 클레임에서 이메일 및 upn을 선택합니다.

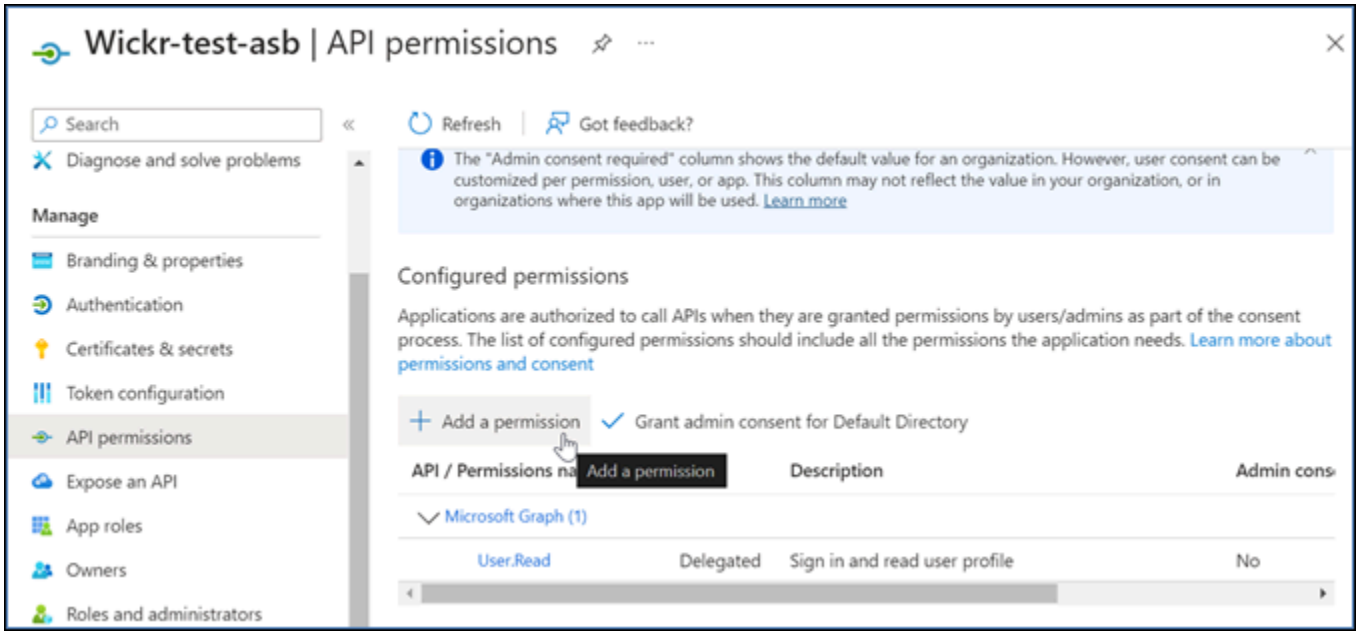
5. 추가를 선택합니다.



5단계: API 권한 설정

Microsoft Entra에서 API 권한을 설정하려면 다음 절차를 완료하세요.

1. 탐색 창에서 API 권한(API Permissions)을 선택합니다.
2. API 권한 페이지에서 권한 추가를 선택합니다.



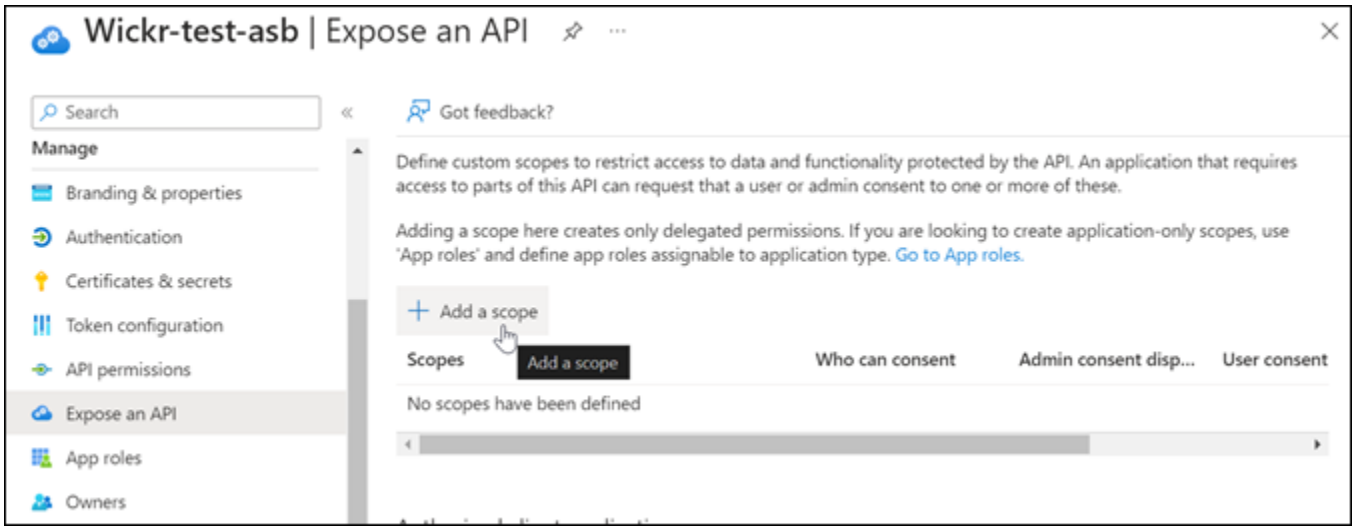
3. Microsoft 그래프를 선택한 다음 위임된 권한을 선택합니다.
4. 이메일 , offline_access, openid, 프로필의 확인란을 선택합니다.
5. 권한 추가를 선택합니다.

6단계: API 노출

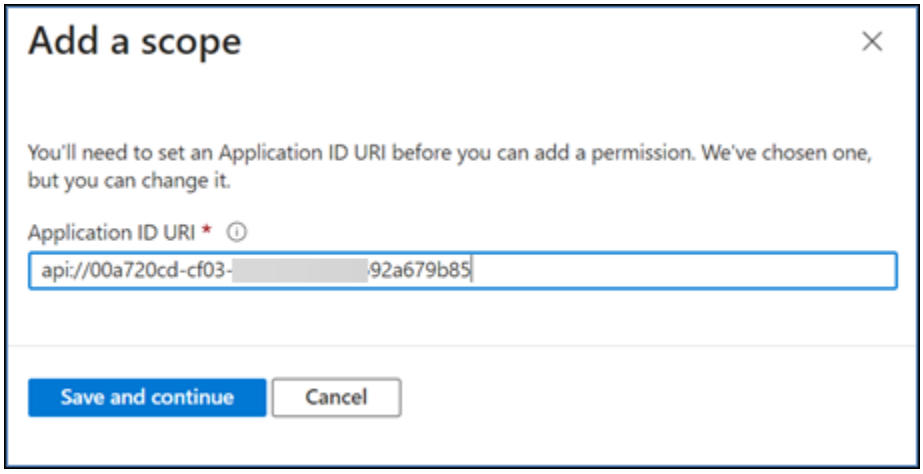
다음 절차를 완료하여 Microsoft Entra의 4개 범위 각각에 대한 API를 노출합니다.

1. 탐색 창에서 API 노출을 선택합니다.

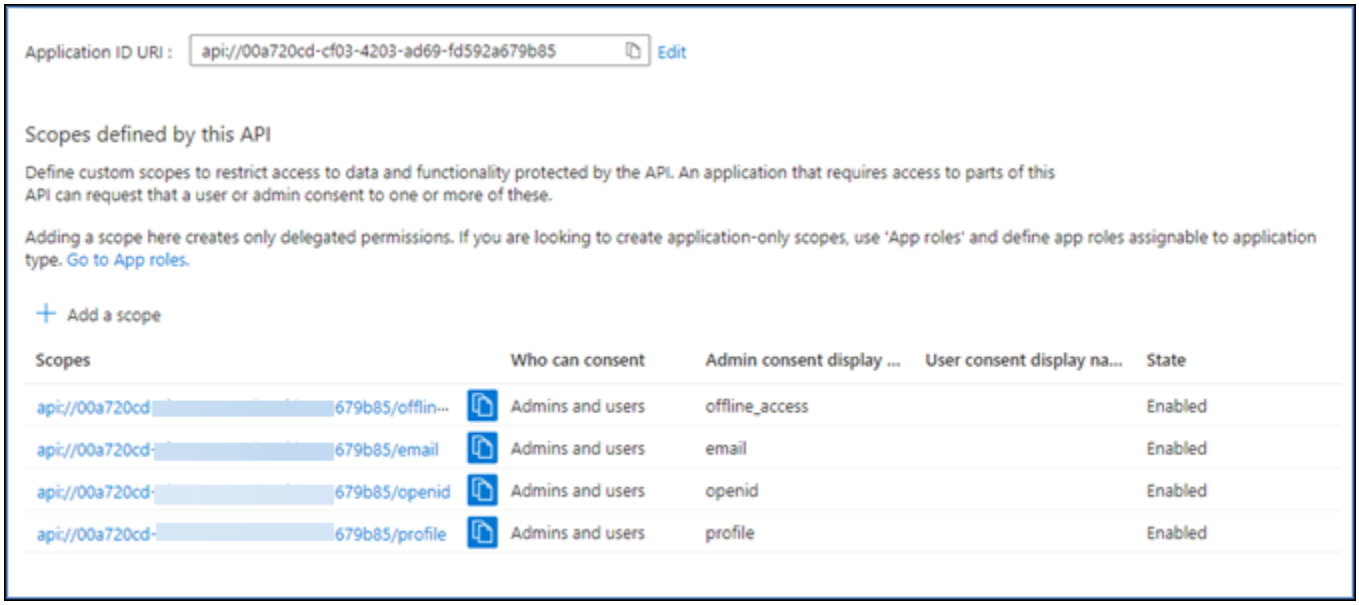
2. API 노출 페이지에서 범위 추가를 선택합니다.



애플리케이션 ID URI는 자동으로 채워지고 URI 뒤에 오는 ID는 애플리케이션 ID(AWS Wickr를 애플리케이션으로 등록에서 생성됨)와 일치해야 합니다.



3. [Save and continue]를 선택합니다.
4. 관리자 및 사용자 태그를 선택한 다음 범위 이름을 offline_access로 입력합니다.
5. 상태를 선택한 다음 활성화를 선택합니다.
6. 범위 추가를 선택합니다.
7. 이 섹션의 1~6단계를 반복하여 이메일, openid 및 프로필 범위를 추가합니다.



8. 승인된 클라이언트 애플리케이션에서 클라이언트 애플리케이션 추가를 선택합니다.
9. 이전 단계에서 생성된 네 가지 범위를 모두 선택합니다.
10. 애플리케이션(클라이언트) ID를 입력하거나 확인합니다.
11. 애플리케이션 추가를 선택합니다.

7단계: AWS Wickr SSO 구성

AWS Wickr 콘솔에서 다음 구성 절차를 완료합니다.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 사용자 관리를 선택한 다음 SSO 구성을 선택합니다.
4. 다음 세부 정보를 입력합니다.

   - 발급자 - 이전에 수정된 엔드포인트입니다(예: `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`).
   - 클라이언트 ID - 개요 창의 애플리케이션(클라이언트) ID입니다.
   - 클라이언트 보안 암호(선택 사항) - 인증서 및 보안 암호 창의 클라이언트 보안 암호입니다.
   - 범위 - API 노출 창에 표시되는 범위 이름입니다. 이메일, 프로필, offline_access 및 openid를 입력합니다.
   - 사용자 지정 사용자 이름 범위(선택 사항) - upn을 입력합니다.

- 회사 ID - 영숫자 및 밑줄 문자를 포함한 고유한 텍스트 값일 수 있습니다. 이 문구는 사용자가 새 디바이스에 등록할 때 입력할 문구입니다.

  다른 필드는 선택 사항입니다.

5. 다음을 선택합니다.
6. 검토 및 저장 페이지에서 세부 정보를 확인한 다음 변경 사항 저장을 선택합니다.

SSO 구성이 완료되었습니다. 확인을 위해 이제 Microsoft Entra의 애플리케이션에 사용자를 추가하고 SSO 및 회사 ID를 사용하여 사용자로 로그인할 수 있습니다.

사용자를 초대하고 온보딩하는 방법에 대한 자세한 내용은 사용자 생성 및 초대를 참조하세요.

문제 해결

다음은 발생할 수 있는 일반적인 문제와 이를 해결하기 위한 제안 사항입니다.

- SSO 연결 테스트가 실패하거나 응답하지 않습니다.
  - SSO 발급자가 예상대로 구성되어 있는지 확인합니다.
  - SSO 구성됨의 필수 필드가 예상대로 설정되어 있는지 확인합니다.
- 연결 테스트에 성공했지만 사용자가 로그인할 수 없습니다.
  - Microsoft Entra에 등록한 Wickr 애플리케이션에 사용자가 추가되었는지 확인합니다.
  - 사용자가 접두사를 포함하여 올바른 회사 ID를 사용하고 있는지 확인합니다. 예: UE1-DemoNetworkW_drqtva.
  - AWS Wickr SSO 구성에서 클라이언트 보안 암호가 올바르게 설정되지 않을 수 있습니다. Microsoft Entra에서 다른 클라이언트 보안 암호를 생성하여 다시 설정하고 Wickr SSO 구성에서 새 클라이언트 보안 암호를 설정합니다.

토큰 새로고침 유예 기간

때때로 ID 공급자가 일시적 또는 장기간 중단에 직면할 수 있으며, 이로 인해 클라이언트 세션의 새로 고침 토큰 실패로 인해 사용자가 예기치 않게 로그아웃될 수 있습니다. 이 문제를 방지하려면 이러한 중단으로 인해 클라이언트 새로 고침 토큰이 실패하더라도 사용자가 로그인 상태를 유지할 수 있는 유예 기간을 설정할 수 있습니다.

유예 기간에 사용할 수 있는 옵션은 다음과 같습니다.

- 유예 기간 없음(기본값): 토큰 새로 고침 실패 후 사용자가 즉시 로그아웃됩니다.
- 30분 유예 기간: 사용자는 토큰 새로 고침 실패 후 최대 30분 동안 로그인 상태를 유지할 수 있습니다.
- 60분 유예 기간: 사용자는 토큰 새로 고침 실패 후 최대 60분 동안 로그인 상태를 유지할 수 있습니다.

AWS Wickr용 네트워크 태그

Wickr 네트워크에 태그를 적용할 수 있습니다. 그런 다음 이러한 태그를 사용하여 Wickr 네트워크를 검색 및 필터링하거나 AWS 비용을 추적할 수 있습니다. Wickr AWS Management Console 용의 네트워크 홈 페이지에서 네트워크 태그를 구성할 수 있습니다.

태그는 리소스에 대한 메타데이터를 보관하기 위해 리소스에 적용되는 키-값 쌍입니다. 각 태그는 키와 값으로 구성된 레이블입니다. 태그에 대한 자세한 내용은 태그란 무엇입니까?및 태깅 사용 사례를 참조하십시오.

주제

- AWS Wickr에서 네트워크 태그 관리
- AWS Wickr에 네트워크 태그 추가
- AWS Wickr에서 네트워크 태그 편집
- AWS Wickr에서 네트워크 태그 제거

AWS Wickr에서 네트워크 태그 관리

Wickr 네트워크의 네트워크 태그를 관리할 수 있습니다.

Wickr 네트워크의 네트워크 태그를 관리하려면 다음 절차를 완료하십시오.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 네트워크 홈 페이지의 태그 섹션에서 태그 관리를 선택합니다.
4. 태그 관리 페이지에서 다음 옵션 중 하나를 완료할 수 있습니다.

    - 새 태그 추가 - 키와 값 쌍의 형태로 새 태그를 입력합니다. 키 값 쌍을 여러 개 추가하려면 새 태그추가를 선택합니다. 태그는 대/소문자를 구분합니다. 자세한 내용은 AWS Wickr에 네트워크 태그 추가 단원을 참조하십시오.

- 기존 태그 편집 - 기존 태그의 키 또는 값 텍스트를 선택한 다음 텍스트 상자에 수정 내용을 입력합니다. 자세한 내용은 AWS Wickr에서 네트워크 태그 편집 단원을 참조하십시오.
- 기존 태그 제거 — 삭제하려는 태그 옆에 나열된 제거 버튼을 선택합니다. 자세한 내용은 AWS Wickr에서 네트워크 태그 제거 단원을 참조하십시오.

AWS Wickr에 네트워크 태그 추가

Wickr 네트워크에 네트워크 태그를 추가할 수 있습니다.

Wickr 네트워크에 태그를 추가하려면 다음 절차를 완료하십시오. 태그 관리에 대한 자세한 내용은 AWS Wickr에서 네트워크 태그 관리 섹션을 참고하십시오.

1. 네트워크 홈 페이지의 태그 섹션에서 새 태그 추가를 선택합니다.
2. 태그 관리 페이지에서 새 태그 추가를 선택합니다.
3. 나타난 빈 키 및 값 필드에 새 태그 키와 값을 입력합니다.
4. 변경 사항 저장을 선택하여 새 태그를 저장합니다.

AWS Wickr에서 네트워크 태그 편집

Wickr 네트워크에 대한 네트워크 태그를 편집할 수 있습니다.

Wickr 네트워크와 관련된 태그를 편집하려면 다음 절차를 완료하십시오. 태그 관리에 대한 자세한 내용은 AWS Wickr에서 네트워크 태그 관리 섹션을 참고하십시오.

1. 태그 관리 페이지에서 태그 값을 편집합니다.

   > **Note**
   >
   > 태그의 키는 편집할 수 없습니다. 대신 키와 값 쌍을 제거하고 새 키를 사용하여 새 태그를 추가하십시오.

2. 변경 사항 저장을 선택하여 편집을 저장합니다.

AWS Wickr에서 네트워크 태그 제거

Wickr 네트워크에 대한 네트워크 태그를 제거할 수 있습니다.

Wickr 네트워크에서 태그를 제거하려면 다음 절차를 완료하십시오. 태그 관리에 대한 자세한 내용은 AWS Wickr에서 네트워크 태그 관리 섹션을 참고하십시오.

1. 태그 관리 페이지에서 제거할 태그에 대해 제거를 선택합니다.
2. 변경 사항 저장을 선택하여 편집을 저장합니다.

AWS Wickr에 대한 읽기 영수증

AWS Wickr에 대한 읽기 수신은 메시지를 읽은 시간을 표시하기 위해 발신자에게 전송되는 알림입니다. 이러한 영수증은 one-on-one 대화에서 사용할 수 있습니다. 전송된 메시지에는 단일 확인 표시가 나타나고 읽기 메시지에는 확인 표시가 있는 원 모양이 나타납니다. 외부 대화 중에 메시지에 대한 읽기 수신을 보려면 두 네트워크 모두 읽기 수신을 활성화해야 합니다.

관리자는 관리자 패널에서 읽기 수신을 활성화하거나 비활성화할 수 있습니다. 이 설정은 전체 네트워크에 적용됩니다.

읽기 수신을 활성화하거나 비활성화하려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 네트워크 정책을 선택합니다.
4. 네트워크 정책 페이지의 메시징 섹션에서 편집을 선택합니다.
5. 읽기 수신 활성화 또는 비활성화 확인란을 선택합니다.
6. 변경 사항 저장을 선택합니다.

AWS Wickr의 네트워크 계획 관리

Wickr AWS Management Console 용 에서는 비즈니스 요구 사항에 따라 네트워크 계획을 관리할 수 있습니다.

네트워크 계획을 관리하려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 네트워크 홈 페이지의 네트워크 세부 정보 섹션에서 편집을 선택합니다.

4. 네트워크 세부 정보 편집 페이지에서 원하는 네트워크 계획을 선택합니다. 다음 중 하나를 선택하여 현재 네트워크 계획을 수정할 수 있습니다.

   - 표준 - 관리 제어 및 유연성이 필요한 소규모 및 대규모 비즈니스 팀을 위한 것입니다.
   - 프리미엄 또는 프리미엄 무료 평가판 - 가장 높은 기능 제한, 세분화된 관리 제어 및 데이터 보존이 필요한 기업용입니다.

     관리자는 최대 30명의 사용자가 사용할 수 있고 3개월 동안 지속되는 프리미엄 무료 평가판을 선택할 수 있습니다. WickrGov의 경우 AWS 프리미엄 무료 평가판 옵션은 최대 50명의 사용자를 허용하며 3개월 동안 지속됩니다. 이 제안은 신규 및 표준 플랜에 적용됩니다. 프리미엄 무료 평가판 기간 동안 관리자는 Premium 또는 Standard 플랜으로 업그레이드하거나 다운그레이드할 수 있습니다.

     > **Note**
     >
     > 네트워크에서 사용 및 결제를 중지하려면 네트워크에서 일시 중지된 사용자를 포함한 모든 사용자를 제거합니다.

프리미엄 무료 평가판 제한 사항

프리미엄 무료 평가판에는 다음과 같은 제한 사항이 적용됩니다.

- 플랜이 이전에 프리미엄 무료 평가판에 등록된 적이 있는 경우 다른 평가판을 사용할 수 없습니다.
- 프리미엄 무료 평가판에는 AWS 계정당 하나의 네트워크만 등록할 수 있습니다.
- 프리미엄 무료 평가판에서는 게스트 사용자 기능을 사용할 수 없습니다.
- 표준 네트워크에 30명 이상의 사용자(WickrGov의 AWS 경우 50명 이상의 사용자)가 있는 경우 프리미엄 무료 평가판으로 업그레이드할 수 없습니다.

AWS Wickr의 데이터 보존

AWS Wickr 데이터 보존은 네트워크의 모든 대화를 유지할 수 있습니다. 여기에는 네트워크 내(내부) 구성원과 네트워크가 페더레이션된 다른 팀(외부 과의 그룹 또는 룸 내 대화와 다이렉트 메시지 대화가 포함됩니다. 데이터 보존은 데이터 보존을 선택한 AWS Wickr Premium 플랜 사용자 및 엔터프라이즈 고객만 사용할 수 있습니다. 프리미엄 플랜에 대한 자세한 내용은 Wickr 요금 책정을 참조하십시오.

네트워크 관리자가 네트워크에 대한 데이터 보존을 구성하고 활성화하면 네트워크에서 공유되는 모든 메시지와 파일은 조직의 규정 준수 정책에 따라 보관됩니다. 이러한 .txt 파일 출력은 네트워크 관리자가 외부 위치(예: 로컬 스토리지, Amazon S3 버킷 또는 사용자의 선택에 따른 기타 스토리지)에서 액세스할 수 있으며, 여기서 분석, 삭제 또는 전송할 수 있습니다.

> **Note**
>
> Wickr는 메시지와 파일에 절대 액세스하지 않습니다. 따라서 데이터 보존 시스템을 구성하는 것은 사용자의 책임입니다.

주제

AWS Wickr에서 데이터 보존 세부 정보 보기

Wickr 네트워크의 데이터 보존 세부 정보를 보려면 다음 절차를 완료하십시오. Wickr 네트워크에 대한 데이터 보존을 활성화하거나 비활성화할 수도 있습니다.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 네트워크 정책을 선택합니다.
4. 네트워크 정책 페이지에는 데이터 보존 설정 단계와 데이터 보존 기능을 활성화 또는 비활성화하는 옵션이 표시됩니다. 데이터 보존 구성에 대한 자세한 내용은 AWS Wickr의 데이터 보존 구성 단원을 참조하십시오.

> **Note**
>
> 데이터 보존이 활성화되면 네트워크의 모든 사용자에게 보존 지원 네트워크를 알리는 데이터 보존 켜짐 메시지가 표시됩니다.

AWS Wickr의 데이터 보존 구성

AWS Wickr 네트워크에 대한 데이터 보존을 구성하려면 데이터 보존 봇 Docker 이미지를 로컬 컴퓨터 또는 Amazon Elastic Compute Cloud(Amazon EC2)의 인스턴스와 같은 호스트의 컨테이너에 배포해야 합니다. 봇이 배포된 후, 데이터를 로컬에 저장하거나 Amazon Simple Storage Service(S3) 버킷에 저장하도록 구성할 수 있습니다. (Secrets Manager), Amazon CloudWatch AWS Secrets Manager (CloudWatch), Amazon Simple Notification Service(Amazon SNS) 및 AWS Key Management Service ()와 같은 다른 AWS 서비스를 사용하도록 데이터 보존 봇을 구성할 수도 있습니다AWS KMS. 다음 주제에서는 Wickr 네트워크용 데이터 보존 봇을 구성하고 실행하는 방법을 설명합니다.

주제

AWS Wickr에 대한 데이터 보존을 구성하기 위한 사전 조건

시작하기 전에 Wickr AWS Management Console 용에서 데이터 보존 봇 이름(사용자 이름으로 레이블 지정)과 초기 암호를 가져와야 합니다. 데이터 보존 봇을 처음 시작할 때는 이 두 값을 모두 지정해야 합니다. 또한 콘솔에서 데이터 보존을 활성화해야 합니다. 자세한 내용은 AWS Wickr에서 데이터 보존 세부 정보 보기 단원을 참조하십시오.

AWS Wickr의 데이터 보존 봇 암호

데이터 보존 봇을 처음 시작할 때는 다음 옵션 중 하나를 사용하여 초기 암호를 지정합니다.

- `WICKRIO_BOT_PASSWORD` 환경 변수. 데이터 보존 봇 환경 변수는 이 설명서의 뒷부분에 있는 AWS Wickr에서 데이터 보존 봇을 구성하기 위한 환경 변수 섹션에 요약되어 있습니다.
- Secrets Manager의 암호 값은 `AWS_SECRET_NAME`환경 변수에 의해 식별됩니다. 데이터 보존 봇에 대한 Secrets Manager 값은 이 설명서의 뒷부분에 있는 AWS Wickr의 Secrets Manager 값 섹션에 요약되어 있습니다.

- 데이터 보존 봇에서 프롬프트가 표시되면 암호를 입력합니다. `-ti`옵션을 사용하여 대화형 TTY 액세스로 데이터 보존 봇을 실행해야 합니다.

데이터 보존 봇을 처음 구성할 때 새 암호가 생성됩니다. 데이터 보존 봇을 다시 설치해야 하는 경우 생성된 암호를 사용합니다. 데이터 보존 봇을 처음 설치한 후에는 초기 암호가 유효하지 않습니다.

새로 생성된 암호가 다음 예와 같이 표시됩니다.

> **Important**
>
> 암호를 안전한 장소에 저장합니다. 암호를 분실하면 데이터 보존 봇을 다시 설치할 수 없습니다. 이 암호를 공유하지 마십시오. Wickr 네트워크의 데이터 보존을 시작할 수 있는 기능을 제공합니다.

```
**********************************************************************
**** GENERATED PASSWORD
**** DO NOT LOSE THIS PASSWORD, YOU WILL NEED TO ENTER IT EVERY TIME
**** TO START THE BOT
 "HuEXAMPLERAW4lGgEXAMPLEn"
 **********************************************************************
```

AWS Wickr 네트워크의 스토리지 옵션

데이터 보존이 활성화되고 데이터 보존 봇이 Wickr 네트워크에 맞게 구성되면 네트워크 내에서 전송되는 모든 메시지와 파일을 캡처합니다. 메시지는 환경 변수를 사용하여 구성할 수 있는 특정 크기 또는 시간제한으로 제한되는 파일에 저장됩니다. 자세한 내용은 AWS Wickr에서 데이터 보존 봇을 구성하기 위한 환경 변수 섹션을 참조하십시오.

이 데이터를 저장하기 위해 다음 옵션 중 하나를 구성할 수 있습니다.

- 캡처된 모든 메시지와 파일을 로컬에 저장합니다. 이 항목이 기본 옵션입니다. 장기 스토리지를 위해 로컬 파일을 다른 시스템으로 이동하고 호스트 디스크의 메모리 또는 스페이스가 부족하지 않은지 확인하는 것은 사용자의 책임입니다.
- 캡처한 모든 메시지와 파일을 Amazon S3 버킷에 저장합니다. 데이터 보존 봇은 복호화된 모든 메시지와 파일을 지정한 Amazon S3 버킷에 저장합니다. 캡처된 메시지와 파일은 버킷에 성공적으로 저장되면 호스트 머신에서 제거됩니다.

- 캡처한 모든 메시지와 파일을 암호화하여 Amazon S3 버킷에 저장합니다. 데이터 보존 봇은 사용자가 제공한 키를 사용하여 캡처한 모든 메시지와 파일을 다시 암호화하고 지정한 Amazon S3 버킷에 저장합니다. 캡처된 메시지와 파일은 성공적으로 재암호화되어 버킷에 저장되면 호스트 머신에서 제거됩니다. 메시지와 파일을 해독하려면 소프트웨어가 필요합니다.

  Amazon S3 버킷을 생성하여 데이터 보존 봇을 가지고 사용하는 것에 대한 자세한 내용은 Amazon S3 사용 설명서의 버킷 생성을 참조하십시오.

AWS Wickr에서 데이터 보존 봇을 구성하기 위한 환경 변수

다음 환경 변수를 사용하여 데이터 보존 봇을 구성할 수 있습니다. 데이터 보존 봇 Docker 이미지를 실행할 때 `-e` 옵션을 사용하여 이러한 환경 변수를 설정합니다. 자세한 내용은 Wickr 네트워크의 데이터 보존 봇 시작 섹션을 참조하십시오.

> **Note**
>
> 달리 지정하지 않는 한 이러한 환경 변수는 선택 사항입니다.

다음 환경 변수를 사용하여 데이터 보존 봇 자격 증명을 지정하십시오.

- `WICKRIO_BOT_NAME`— 데이터 보존 봇의 이름. 이 변수는 데이터 보존 봇 Docker 이미지를 실행할 때 필요합니다.
- `WICKRIO_BOT_PASSWORD`— 데이터 보존 봇의 초기 암호입니다. 자세한 내용은 AWS Wickr에 대한 데이터 보존을 구성하기 위한 사전 조건 섹션을 참조하십시오. 암호 프롬프트로 데이터 보존 봇을 시작하지 않거나 Secrets Manager를 사용하여 데이터 보존 봇 자격 증명을 저장할 계획이 없는 경우 이 변수가 필요합니다.

다음 환경 변수를 사용하여 기본 데이터 보존 스트리밍 기능을 구성합니다.

- `WICKRIO_COMP_MESGDEST`— 메시지가 스트리밍될 디렉터리의 경로 이름입니다. 기본값은 `/tmp/<botname>/compliance/messages`입니다.
- `WICKRIO_COMP_FILEDEST`— 파일을 스트리밍될 디렉터리의 경로 이름입니다. 기본값은 `/tmp/<botname>/compliance/attachments`입니다.
- `WICKRIO_COMP_BASENAME`— 수신된 메시지 파일의 기본 이름입니다. 기본값은 `receivedMessages`입니다.

- `WICKRIO_COMP_FILESIZE`— 받은 메시지의 최대 파일 크기는 키비바이트(KiB)입니다. 최대 크기에 도달하면 새 파일이 시작됩니다. 기본값은 `1000000000`이고, 1024GiB에서와 같습니다.
- `WICKRIO_COMP_TIMEROTATE`— 데이터 보존 봇이 수신된 메시지를 수신된 메시지 파일에 저장하는 시간의 합계(분). 시간제한에 도달하면 새 파일이 시작됩니다. 사용자는 파일 크기 또는 시간만 사용하여 받은 메시지 파일의 크기를 제한할 수 있습니다. 기본값은 `0`이고 제한은 없습니다.

다음 환경 변수를 사용하여 AWS 리전 사용할 기본값을 정의합니다.

- `AWS_DEFAULT_REGION` - Secrets Manager와 같은 AWS 서비스에 AWS 리전 사용할 기본값입니다(Amazon S3 또는 에는 사용되지 않음 AWS KMS). 이 환경 변수가 정의되지 않은 경우 기본적으로 `us-east-1` 리전이 사용됩니다.

다음 환경 변수를 사용하여 Secrets Manager를 사용하여 데이터 보존 봇 보안 인증 및 AWS 서비스 정보를 저장하도록 선택할 때 사용할 Secrets Manager 보안 암호를 지정합니다. Secrets Manager에 저장할 수 있는 값에 대한 자세한 내용은 AWS Wickr의 Secrets Manager 값을 참조하십시오.

- `AWS_SECRET_NAME` - 데이터 보존 봇에 필요한 자격 증명 및 AWS 서비스 정보가 포함된 Secrets Manager 보안 암호의 이름입니다.
- `AWS_SECRET_REGION` - AWS 보안 AWS 리전 암호가 있는 입니다. AWS 보안 암호를 사용 중이고 이 값이 정의되지 않은 경우 `AWS_DEFAULT_REGION` 값이 사용됩니다.

> **Note**
>
> 다음 환경 변수를 모두 Secrets Manager에 값으로 저장할 수 있습니다. Secrets Manager를 사용하기로 선택하고 이 값을 저장하면 데이터 보존 봇 Docker 이미지를 실행할 때 환경 변수로 지정할 필요가 없습니다. 이 설명서의 앞부분에서 설명한 `AWS_SECRET_NAME` 환경 변수만 지정하면 됩니다. 자세한 내용은 AWS Wickr의 Secrets Manager 값 섹션을 참조하십시오.

메시지와 파일을 버킷에 저장하도록 선택할 경우 다음 환경 변수를 사용하여 Amazon S3 버킷을 지정합니다.

- `WICKRIO_S3_BUCKET_NAME`— 메시지와 파일이 저장되는 Amazon S3 버킷의 이름.
- `WICKRIO_S3_REGION` - 메시지와 파일이 저장될 Amazon S3 버킷의 AWS 리전입니다.
- `WICKRIO_S3_FOLDER_NAME`— 메시지 및 파일이 저장되는 Amazon S3 버킷의 선택 가능 폴더 이름입니다. 이 폴더 이름 앞에는 Amazon S3 버킷에 저장된 메시지 및 파일의 키가 표시됩니다.

다음 환경 변수를 사용하여 Amazon S3 버킷에 파일을 저장할 때 클라이언트 측 암호화를 사용하여 파일을 다시 암호화하도록 선택할 때 AWS KMS 세부 정보를 지정합니다.

- `WICKRIO_KMS_MSTRKEY_ARN` - Amazon S3 버킷에 저장되기 전에 데이터 보존 봇의 메시지 파일과 파일을 다시 암호화하는 데 사용되는 AWS KMS 마스터 키의 Amazon 리소스 이름(ARN)입니다. Amazon S3
- `WICKRIO_KMS_REGION` - 마스터 키가 AWS KMS 위치한 AWS 리전입니다.

Amazon SNS 주제에 데이터 보존 이벤트를 전송하도록 선택한 경우, 다음 환경 변수를 사용하여 Amazon SNS 세부 정보를 지정합니다. 전송된 이벤트에는 시작, 종료 및 오류 상태가 포함됩니다.

- `WICKRIO_SNS_TOPIC_ARN`— 데이터 보존 이벤트를 전송할 Amazon SNS 주제의 ARN입니다.

다음 환경 변수를 사용하여 데이터 보존 지표를 CloudWatch에 전송합니다. 지정된 경우 지표는 60초마다 생성됩니다.

- `WICKRIO_METRICS_TYPE`— CloudWatch로 지표를 전송하려면 이 환경 변수의 값을 `cloudwatch`로 설정합니다.

AWS Wickr의 Secrets Manager 값

Secrets Manager를 사용하여 데이터 보존 봇 자격 증명 및 AWS 서비스 정보를 저장할 수 있습니다. Secrets Manager 보안 암호 생성에 대한 자세한 내용은 Secrets Manager 사용 설명서의 보안 AWS Secrets Manager 암호 생성을 참조하세요.

Secrets Manager 보안 암호는 다음과 같은 값을 가질 수 있습니다.

- `password`— 데이터 보존 봇 암호.
- `s3_bucket_name`— 메시지와 파일이 저장되는 Amazon S3 버킷의 이름. 설정하지 않으면 기본 파일 스트리밍이 사용됩니다.
- `s3_region` - 메시지와 파일이 저장될 Amazon S3 버킷의 AWS 리전입니다.
- `s3_folder_name`— 메시지 및 파일이 저장되는 Amazon S3 버킷의 선택 가능 폴더 이름입니다. 이 폴더 이름 앞에는 Amazon S3 버킷에 저장된 메시지 및 파일의 키가 표시됩니다.
- `kms_master_key_arn` - Amazon S3 버킷에 저장되기 전에 데이터 보존 봇의 메시지 파일과 파일을 다시 암호화하는 데 사용되는 AWS KMS 마스터 키의 ARN입니다.
- `kms_region` - AWS KMS 마스터 키가 위치한 AWS 리전입니다.

- `sns_topic_arn`— 데이터 보존 이벤트를 전송할 Amazon SNS 주제의 ARN입니다.

AWS 서비스와 함께 데이터 보존을 사용하는 IAM 정책

Wickr 데이터 보존 봇과 함께 다른 AWS 서비스를 사용하려는 경우 호스트에 액세스하기 위한 적절한 AWS Identity and Access Management (IAM) 역할과 정책이 있는지 확인해야 합니다. Secrets Manager, Amazon S3, CloudWatch, Amazon SNS 및를 사용하도록 데이터 보존 봇을 구성할 수 있습니다 AWS KMS. 다음 IAM 정책은 이러한 서비스에 대한 특정 작업에 대한 액세스를 허용합니다.

JSON

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

사용자는 호스트의 컨테이너가 액세스하도록 허용하려는 각 서비스의 특정 객체를 식별하여 보다 엄격한 IAM 정책을 만들 수 있습니다. 사용하지 않을 AWS 서비스에 대한 작업을 제거합니다. 예를 들어, Amazon S3 버킷만 사용하려는 경우, `secretsmanager:GetSecretValue` `sns:Publishkms:GenerateDataKey`, 및 `cloudwatch:PutMetricData` 작업을 제거하는 다음 정책을 사용하십시오.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "*"
        }
    ]
}
```

Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 사용하여 데이터 보존 봇을 호스팅하는 경우, Amazon EC2의 일반적인 사례를 사용하는 IAM 역할을 생성하고 위의 정책 정의를 사용하여 정책을 할당하십시오.

Wickr 네트워크의 데이터 보존 봇 시작

데이터 보존 봇을 실행하기 전에 원하는 구성 방법을 결정해야 합니다. 다음과 같은 호스트에서 봇을 실행하려는 경우,

- AWS 서비스에 액세스할 수 없는 경우 옵션이 제한됩니다. 이 경우 기본 메시지 스트리밍 옵션을 사용하게 됩니다. 캡처된 메시지 파일의 크기를 특정 크기 또는 시간 간격으로 제한할지 여부를 결정해야 합니다. 자세한 내용은 AWS Wickr에서 데이터 보존 봇을 구성하기 위한 환경 변수 단원을 참조하십시오.
- AWS 서비스에 액세스할 수 있게 되면 Secrets Manager 보안 암호를 생성하여 봇 자격 증명과 AWS 서비스 구성 세부 정보를 저장해야 합니다. AWS 서비스를 구성한 후, 데이터 보존 봇 Docker 이미지를 시작할 수 있습니다. Secrets Manager 보안 암호에 저장할 수 있는 세부 정보에 대한 자세한 내용은 AWS Wickr의 Secrets Manager 값을 참조하십시오.

다음 섹션에서는 데이터 보존 봇 Docker 이미지를 실행하는 예제 명령을 보여줍니다. 각 예제 명령에서, 다음 예제 값을 사용자 자신의 값으로 바꿉니다.

- *compliance_1234567890_bot*과 데이터 보존 봇의 이름.
- *password*과 데이터 보존 봇의 암호.
- 데이터 보존 봇과 함께 사용할 *wickr/data/retention/bot*과 Secrets Manager 보안 암호의 이름.
- *bucket-name*과 메시지 및 파일이 저장되는 Amazon S3 버킷의 이름.

- *folder-name*과 메시지 및 파일이 저장되는 Amazon S3 버킷의 폴더 이름.
- *us-east-1*를 지정하려는 리소스의 AWS 리전으로 바꿉니다. 예를 들어 AWS KMS 마스터 키의 리전 또는 Amazon S3 버킷의 리전입니다.
- *arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-a617-abababababab*를 메시지 파일 및 파일을 다시 암호화하는 데 사용할 AWS KMS 마스터 키의 Amazon 리소스 이름(ARN)으로 바꿉니다.

암호 환경 변수로 봇 시작(AWS 서비스 없음)

다음 Docker 명령은 데이터 보존 봇을 시작합니다. 암호는 WICKRIO_BOT_PASSWORD 환경 변수를 사용하여 지정됩니다. 봇은 기본 파일 스트리밍을 사용하고 이 설명서의 AWS Wickr에서 데이터 보존 봇을 구성하기 위한 환경 변수 섹션에 정의된 기본값을 사용하여 시작합니다.

```
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
```

암호 프롬프트로 봇 시작(AWS 서비스 없음)

다음 Docker 명령은 데이터 보존 봇을 시작합니다. 데이터 보존 봇에서 암호를 묻는 메시지가 표시되면 암호를 입력합니다. 이 설명서의 AWS Wickr에서 데이터 보존 봇을 구성하기 위한 환경 변수 섹션에 정의된 기본값을 사용하여 기본 파일 스트리밍을 사용하기 시작합니다.

```
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:************
```

-ti 옵션을 사용하여 봇을 실행하면 암호 프롬프트를 받을 수 있습니다. 또한 도커 이미지를 시작한 후 즉시 docker attach *<container ID or container name>* 명령을 실행하여 암호 프롬프트

가 표시되도록 해야 합니다. 이 두 명령은 모두 스크립트로 실행해야 합니다. 도커 이미지에 연결했는데 메시지가 표시되지 않는 경우 입력 키를 누르면 프롬프트가 표시됩니다.

15분 메시지 파일 교체로 봇 시작(AWS 서비스 없음)

다음 Docker 명령은 환경 변수를 사용하여 데이터 보존 봇을 시작합니다. 또한 수신된 메시지 파일을 15분 단위로 회전하도록 구성합니다.

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

봇을 시작하고 Secrets Manager를 사용하여 초기 암호를 지정합니다.

사용자는 Secrets Manager를 사용하여 데이터 보존 봇의 암호를 식별할 수 있습니다. 데이터 보존 봇을 시작할 때는 이 정보가 저장되는 Secrets Manager를 지정하는 환경 변수를 설정해야 합니다.

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

`wickrpro/compliance/compliance_1234567890_bot` 보안 암호에는 일반 텍스트로 보이는, 그 안에 표시된 다음과 같은 보안 암호 값이 있습니다.

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

봇을 시작하고 Secrets Manager를 사용하여 Amazon S3를 구성합니다.

사용자는 Secrets Manager를 사용하여 자격 증명과 Amazon S3 버킷 정보를 호스팅할 수 있습니다. 데이터 보존 봇을 시작할 때는 이 정보가 저장되는 Secrets Manager를 지정하는 환경 변수를 설정해야 합니다.

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

wickrpro/compliance/compliance_1234567890_bot 보안 암호에는 일반 텍스트로 보이는, 그 안에 표시된 다음과 같은 보안 암호 값이 있습니다.

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

봇이 수신한 메시지와 파일은 network1234567890이름이 지정된 폴더의 bot-compliance 버킷에 저장됩니다.

봇을 시작하고 Secrets Manager를 AWS KMS 사용하여 Amazon S3 및 구성

Secrets Manager를 사용하여 자격 증명, Amazon S3 버킷 및 AWS KMS 마스터 키 정보를 호스팅할 수 있습니다. 데이터 보존 봇을 시작할 때는 이 정보가 저장되는 Secrets Manager를 지정하는 환경 변수를 설정해야 합니다.

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

wickrpro/compliance/compliance_1234567890_bot 보안 암호에는 일반 텍스트로 보이는, 그 안에 표시된 다음과 같은 보안 암호 값이 있습니다.

```
{
    "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"
}
```

봇이 수신한 메시지와 파일은 ARN 값으로 식별되는 KMS 키를 사용하여 암호화된 다음 “network1234567890"이라는 폴더에 있는 “봇 규정 준수” 버킷에 저장됩니다. 적절한 IAM 정책 설정이 있는지 확인하십시오.

봇을 시작하고 환경 변수를 사용하여 Amazon S3를 구성합니다.

Secrets Manager를 사용하여 데이터 보존 봇 자격 증명을 호스팅하지 않으려면 다음 환경 변수를 사용하여 데이터 보존 봇 Docker 이미지를 시작할 수 있습니다. WICKRIO_BOT_NAME환경 변수를 사용하여 데이터 보존 봇의 이름을 식별해야 합니다.

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

환경 값을 사용하여 데이터 보존 봇의 자격 증명, Amazon S3 버킷에 대한 정보, 기본 파일 스트리밍을 위한 구성 정보를 식별할 수 있습니다.

Wickr 네트워크의 데이터 보존 봇 중지

데이터 보존 봇에서 실행되는 소프트웨어는 SIGTERM 신호를 캡쳐하고 정상적으로 종료됩니다. 다음 예제와 같이 `docker stop <container ID or container name>` 명령을 사용하여 데이터 보존 봇 Docker 이미지에 SIGTERM 명령을 내립니다.

```
docker stop compliance_1234567890_bot
```

Wickr 네트워크의 데이터 보존 로그 가져오기

데이터 보존 봇 도커 이미지에서 실행되는 소프트웨어는 /tmp/<botname>/logs디렉터리의 로그 파일에 출력됩니다. 파일은 최대 5개 파일로 회전합니다. 다음 명령을 실행하여 로그를 가질 수 있습니다.

```
docker logs <botname>
```

예제:

```
docker logs compliance_1234567890_bot
```

Wickr 네트워크의 데이터 보존 지표 및 이벤트

다음은 AWS Wickr 데이터 보존 봇 5.116 버전에서 현재 지원하는 Amazon CloudWatch 지표와 Amazon Simple Notification Service(SNS) 이벤트입니다.

주제

Wickr 네트워크에 대한 CloudWatch 지표

지표는 봇이 1분 간격으로 생성되어 데이터 보존 봇 도커 이미지가 실행되는 계정과 연결된 CloudWatch 서비스에 전송됩니다.

다음은 데이터 보존 봇이 지원하는 기존 지표입니다.

지표	설명
Messages_Rx	메시지 수신됨
메시지_Rx_실패함	수신된 메시지를 처리하지 못했습니다.
메시지_저장됨	받은 메시지 파일에 메시지가 저장되었습니다.
메시지_저장_실패	받은 메시지 파일에 메시지를 저장하지 못했습니다.
파일_저장됨	파일을 받았습니다.
파일_저장_바이트	받은 파일의 바이트 수
파일_저장_실패	파일 저장 실패.

지표	설명
로그인	로그인(일반적으로 각 간격마다 1회입니다).
로그인_실패	로그인 실패(일반적으로 각 간격마다 1회씩 발생)
S3_Post_Errors	Amazon S3 버킷에 메시지 파일 및 파일을 게시하는 중 오류가 발생했습니다.
Watchdog_실패	Watchdog 장애
Watchdog_경고	Watchdog 경고

지표는 CloudWatch에서 사용할 수 있도록 생성됩니다. 봇에 사용되는 네임스페이스는 `WickrIO`입니다. 각 지표에는 차원 배열이 있습니다. 다음은 위 지표와 함께 게시된 측정기준 목록입니다.

측정 기준	값
Id	봇의 사용자 이름입니다.
장치	특정 봇 기기 또는 인스턴스에 대한 설명. 여러 봇 기기 또는 인스턴스를 실행하는 경우 유용합니다.
제품	봇을 위한 제품입니다. `WickrPro_` 또는 `WickrEnterprise_` 에 `Alpha`, `Beta`, 또는 `Production` 가 붙을 수 있습니다.
BotType	봇 유형. 규정 준수스 봇의 경우 규정 준수로 분류됩니다.
Network	연결된 네트워크의 ID.

Wickr 네트워크에 대한 Amazon SNS 이벤트

다음 이벤트는 `WICKRIO_SNS_TOPIC_ARN`환경 변수 또는 Secrets Manager `sns_topic_arn` 비밀 값을 사용하여 식별된 Amazon 리소스 이름(ARN) 값으로 정의된 Amazon SNS 주제에 게시됩니다.

자세한 정보는 AWS Wickr에서 데이터 보존 봇을 구성하기 위한 환경 변수및 AWS Wickr의 Secrets Manager 값 섹션을 참조하십시오.

데이터 보존 봇에서 생성된 이벤트는 JSON 문자열로 전송됩니다. 데이터 보존 봇 5.116 버전부터 이벤트에 포함된 값은 다음과 같습니다.

이름	값
complianceBot	데이터 보존 봇의 사용자 이름.
dataTime	이벤트가 발생한 날짜와 시간.
디바이스	특정 봇 디바이스 또는 인스턴스에 대한 설명. 여러 봇 인스턴스를 실행하는 경우 유용합니다.
dockerImage	봇과 관련된 도커 이미지.
dockerTag	도커 이미지의 태그 또는 버전입니다.
message	이벤트 메시지 자세한 내용은 중요 이벤트 및 일반 이벤트 단원을 참조하십시오.
notificationType	이 값은 `Bot Event` 입니다.
severity	이벤트의 심각도. 가능한 값은 `normal` 또는 `critical`입니다.

이벤트를 받으려면 Amazon SNS 주제를 구독해야 합니다. 이메일 주소를 사용하여 구독하는 경우 다음 예제와 유사한 정보가 포함된 이메일이 전송됩니다.

```
{
"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"
}
```

중요 이벤트

이러한 이벤트로 인해 봇이 중지되거나 다시 시작됩니다. 다른 문제가 발생하지 않도록 재시작 횟수를 제한합니다.

로그인 실패

봇이 로그인하지 못할 때 생성될 수 있는 이벤트는 다음과 같습니다. 각 메시지에는 로그인 실패 이유가 표시됩니다.

이벤트 유형	이벤트 메시지
failedlogin	보안 인증이 잘못되었습니다. 비밀번호를 확인합니다.
failedlogin	사용자를 찾을 수 없습니다.
failedlogin	계정 또는 기기가 일시 중지되었습니다.
provisioning	사용자가 명령을 종료합니다.
provisioning	`config.wickr` 파일의 비밀번호가 잘못되었습니다.
provisioning	`config.wickr` 파일을 읽을 수 없습니다.
failedlogin	로그인이 모두 실패했습니다.
failedlogin	새 사용자이지만 데이터베이스가 이미 있습니다.

더 중요한 이벤트

이벤트 유형	이벤트 메시지
일시 중지된 계정	WickrIOClientMain::slotAdminUserSuspend: code(%1): reason: %2“
BotDevice Suspended	기기가 일시 중지되었습니다!

이벤트 유형	이벤트 메시지
WatchDog	SwitchBoard 시스템이 <*N*> 분 이상 다운되었습니다.
S3 실패	S3 버킷에 파일 <*file-name* >을 넣지 못했습니다. *##: <AWS-error* >
Fallback Key	서버에서 제출한 폴백 키: 인식된 클라이언트 활성 폴백 키가 아닙니다. 데스크탑 엔지니어링에 로그를 제출하십시오.

일반 이벤트

다음은 정상 작동 발생에 대해 경고하는 이벤트입니다. 특정 기간 내에 이러한 유형의 이벤트가 너무 많이 발생하는 것은 우려의 원인이 될 수 있습니다.

계정에 추가된 기기

이 이벤트는 새 기기가 데이터 보존 봇 계정에 추가될 때 생성됩니다. 경우에 따라 이는 누군가가 데이터 보존 봇의 인스턴스를 생성했다는 중요한 표시일 수 있습니다. 다음은 이 이벤트의 메시지입니다.

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

봇이 로그인

이 이벤트는 봇이 성공적으로 로그인했을 때 생성됩니다. 다음은 이 이벤트의 메시지입니다.

```
Logged in
```

시스템 종료

이 이벤트는 봇이 종료될 때 생성됩니다. 사용자가 이를 명시적으로 시작하지 않았다면 문제가 있다는 신호일 수 있습니다. 다음은 이 이벤트의 메시지입니다.

```
Shutting down
```

업데이트 사용 가능

이 이벤트는 데이터 보존 봇이 시작될 때 생성되며 관련 도커 이미지의 최신 버전을 사용할 수 있음을 식별합니다. 이 이벤트는 봇이 시작될 때 매일 생성됩니다. 이 이벤트에는 사용 가능한 새 버전을 식별하는 `versions`배열 필드가 포함됩니다. 다음은 이 이벤트의 모습에 대한 예시입니다.

```
{
  "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"
  ]
}
```

ATAK란 무엇입니까?

Android 팀 인식 키트 (ATAK) 또는 군용 Android 전술 공격 키트(ATAK)는 스마트폰 지리공간 인프라 및 상황 인식 애플리케이션으로, 지리 전반에 걸쳐 안전한 협업을 가능하게 합니다. ATAK는 처음에는 전투 지역에서 사용하도록 설계되었지만 지역, 주 및 연방 기관의 임무에 맞게 조정되었습니다.

주제

- Wickr 네트워크 대시보드에서 ATAK 활성화
- ATAK에 대한 추가 정보
- ATAK용 Wickr 플러그인 설치 및 페어링
- ATAK용 Wickr 플러그인 페어링 해제
- ATAK에서 전화 걸기 및 받기
- ATAK로 파일 전송
- ATAK로 보안 음성 메시지(Push-to-talk) 전송
- ATAK용 핀 휠(빠른 액세스)
- ATAK 탐색

Wickr 네트워크 대시보드에서 ATAK 활성화

AWS Wickr는 Android Tactical Assault Kit(ATAK)를 사용하는 많은 기관을 지원합니다. 하지만 지금까지 Wickr를 사용하는 ATAK 운영자는 이를 위해 애플리케이션을 종료해야 했습니다. 운영 중단과 운영 위험을 줄이기 위해 Wickr는 보안 통신 기능으로 ATAK를 강화하는 플러그인을 개발했습니다. ATAK용 Wickr 플러그인을 사용하여 ATAK 애플리케이션 내에서 Wickr에서 메시지를 보내고, 협업하고, 파일을 전송할 수 있습니다. 이를 통해 ATAK의 채팅 기능을 통해 구성이 중단되거나 복잡하지 않습니다.

Wickr 네트워크 대시보드에서 ATAK 활성화

Wickr Network Dashboard에서 ATAK를 활성화하려면 다음 절차를 완료하십시오.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 Security groups를 선택합니다.
4. 보안 그룹 페이지에서 ATAK를 활성화하려는 보안 그룹을 선택합니다.
5. 통합 탭의 ATAK 플러그인 섹션에서 편집을 선택합니다.
6. ATAK 플러그인 편집 페이지에서 ATAK 플러그인 활성화 확인란을 선택합니다.
7. 새 패키지 추가를 선택합니다.
8. 패키지 텍스트 상자에 패키지 이름을 입력합니다. 사용자가 설치하고 사용할 ATAK 버전에 따라 다음 값 중 하나를 입력할 수 있습니다.

   - `com.atakmap.app.civ`— Wickr 최종 사용자가 Android 장치에 ATAK 애플리케이션의 민간 버전을 설치하고 사용하려는 경우 패키지 텍스트 상자에 이 값을 입력합니다.
   - `com.atakmap.app.mil`— Wickr 최종 사용자가 Android 장치에 ATAK 애플리케이션의 군용 버전을 설치하고 사용하려는 경우 패키지 텍스트 상자에 이 값을 입력합니다.
9. 저장을 선택합니다.

   이제 선택한 Wickr 네트워크와 선택한 보안 그룹에 대해 ATAK가 활성화되었습니다. ATAK 기능을 활성화한 보안 그룹의 Android 사용자에게 ATAK용 Wickr 플러그인을 설치하도록 요청해야 합니다. 자세한 내용은 Wickr ATAK 플러그인 설치 및 페어링하기를 참조하십시오.

ATAK에 대한 추가 정보

ATAK용 Wickr 플러그인에 대한 자세한 내용은 다음을 참조하십시오.

- Wickr ATAK 플러그인 개요

- 추가 Wickr ATAK 플러그인 정보

ATAK용 Wickr 플러그인 설치 및 페어링

Android 팀 인식 키트(ATAK)는 임무 계획, 실행 및 사고 대응을 위한 상황 인식 기능이 필요한 미군, 주 및 정부 기관에서 사용하는 Android 솔루션입니다. ATAK에는 개발자가 기능을 추가할 수 있는 플러그인 아키텍처가 있습니다. 이를 통해 사용자는 진행 중인 이벤트에 대한 실시간 상황 인식과 함께 GPS 및 지리공간 지도 데이터를 사용하여 탐색할 수 있습니다. 이 문서에서는 Android 디바이스에 ATAK용 Wickr 플러그인을 설치하고 이를 Wickr 클라이언트와 페어링하는 방법을 보여줍니다. 이렇게 하면 ATAK 애플리케이션을 종료하지 않고도 Wickr에서 메시지를 보내고 협업할 수 있습니다.

ATAK용 플러그인을 설치

Android 디바이스에 ATAK용 Wickr 플러그인을 설치하려면 다음 절차를 완료하십시오.

1. 구글 플레이 스토어로 이동하여 ATAK용 Wickr 플러그인을 설치하십시오.
2. Android 디바이스에서 ATAK 애플리케이션을 엽니다.
3. ATAK 애플리케이션에서 화면 오른쪽 상단의 메뉴 아이콘 ()을 선택하고 플러그인을 선택합니다.
4. 가져오기를 선택합니다.
5. 가져오기 유형 선택 팝업에서 로컬 SD를 선택하고 ATAK 파일용 Wickr 플러그인을 저장한 위치로 이동합니다.
6. 플러그인 파일을 선택하고 프롬프트에 따라 설치합니다.

   > **Note**
   >
   > 스캔할 플러그인 파일을 보내라는 메시지가 표시되면 아니요를 선택합니다.

7. ATAK 애플리케이션에 플러그인을 로드할지 여부를 묻는 메시지가 표시됩니다. 확인을 선택합니다.

이제 ATAK용 Wickr 플러그인이 설치되었습니다. Wickr로 ATAK 페어링 섹션을 계속 진행하여 프로세스를 완료하십시오.

ATAK와 Wickr 페어링

ATAK용 Wickr 플러그인을 성공적으로 설치한 후 다음 절차를 완료하여 ATAK 응용 프로그램을 Wickr와 페어링하십시오.

1. ATAK 애플리케이션에서, 화면 오른쪽 상단의 메뉴 아이콘 ()을 선택하고 Wickr 플러그인을 선택합니다.
2. Wicker 페어링을 선택합니다.

   ATAK용 Wickr 플러그인의 권한을 검토하라는 알림 메시지가 나타납니다. 알림 프롬프트가 나타나지 않으면, Wickr 클라이언트를 열고 설정으로 이동한 다음 연결된 앱으로 이동합니다. 다음 예제와 같이 화면의 보류 중 섹션에 플러그인이 표시되어야 합니다.
3. 승인을 선택하여 페어링합니다.
4. Wickr ATAK 플러그인 열기 버튼을 선택하여 ATAK 애플리케이션으로 돌아갑니다.

   이제 ATAK 플러그인과 Wickr가 성공적으로 페어링되었으며 ATAK 애플리케이션을 종료하지 않고도 플러그인을 사용하여 Wickr를 사용하여 메시지를 보내고 협업할 수 있습니다.

ATAK용 Wickr 플러그인 페어링 해제

ATAK용 Wickr 플러그인의 페어링을 해제할 수 있습니다.

Wickr와 ATAK 플러그인의 페어링을 해제하려면 다음 절차를 완료하세요.

1. 네이티브 앱에서 설정을 선택한 다음 연결된 앱을 선택합니다.
2. 연결된 앱 화면에서 Wickr ATAK 플러그인을 선택합니다.
3. Wickr ATAK 플러그인 화면에서 화면 하단의 제거를 선택합니다.

   이제 ATAK용 Wickr 플러그인의 페어링을 해제했습니다.

ATAK에서 전화 걸기 및 받기

ATAK용 Wickr 플러그인에서 전화를 걸거나 받을 수 있습니다.

전화를 걸고 받으려면 다음 절차를 완료하세요.

1. 채팅 창을 엽니다.

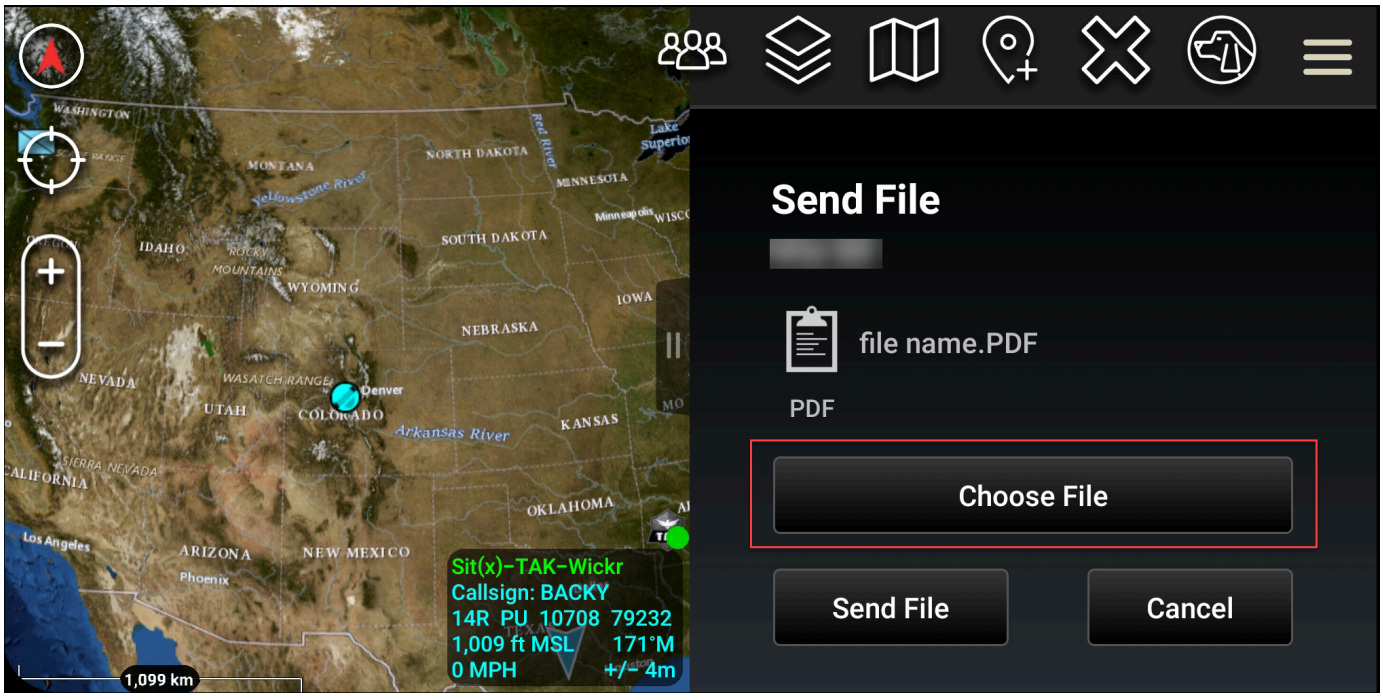
2. 맵 뷰에서 통화할 사용자의 아이콘을 선택합니다.
3. 화면 오른쪽 위에 있는 전화 아이콘을 선택합니다.
4. 연결되면 ATAK 플러그인 보기로 돌아가 전화를 받을 수 있습니다.

ATAK로 파일 전송

ATAK용 Wickr 플러그인에서 파일을 보낼 수 있습니다.

파일을 보내려면 다음 절차를 완료하세요.

1. 채팅 창을 엽니다.
2. 맵 보기에서 파일을 받을 사용자를 검색합니다.
3. 파일을 받을 사용자를 찾으면 해당 이름을 선택합니다.
4. 파일 전송 화면에서 파일 선택을 선택한 다음 보낼 파일을 찾습니다.



5. 브라우저 창에서 원하는 파일을 선택합니다.
6. 파일 전송 화면에서 파일 전송을 선택합니다.

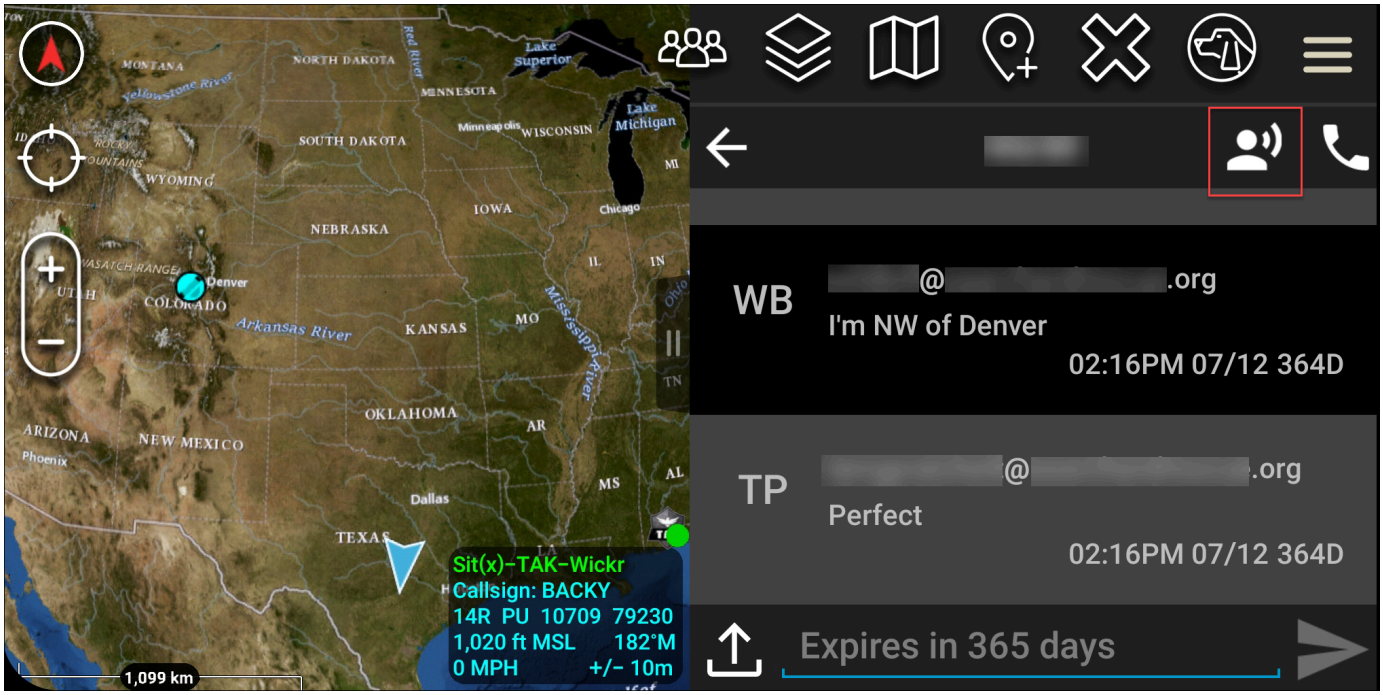
   선택한 파일이 다운로드되고 있음을 나타내는 다운로드 아이콘이 표시됩니다.

ATAK로 보안 음성 메시지(Push-to-talk) 전송

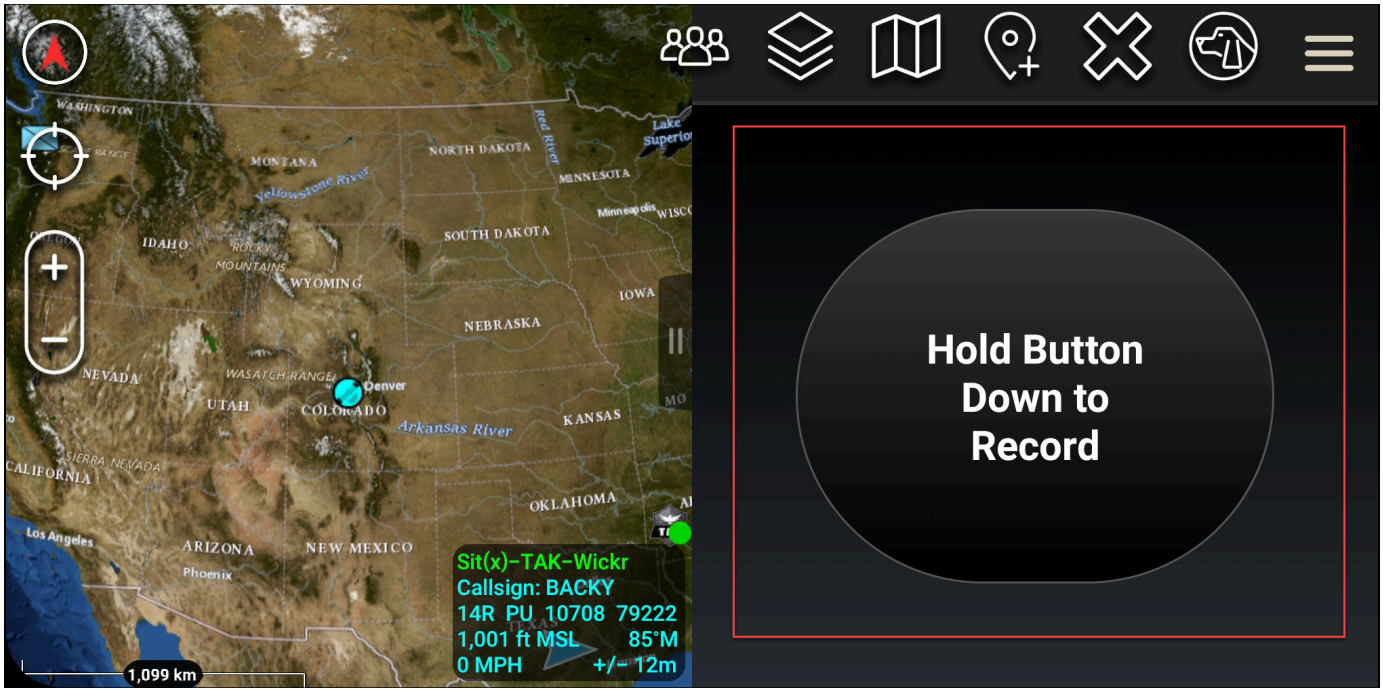
ATAK용 Wickr 플러그인에서 보안 음성 메시지(푸시-투-토크)를 보낼 수 있습니다.

보안 음성 메시지를 보내려면 다음 절차를 완료합니다.

1. 채팅 창을 엽니다.
2. 화면 상단에서 말하는 사람 아이콘으로 표시된 푸시-투-토크 아이콘을 선택합니다.



3. 길게 눌러 녹음하기 버튼을 선택하고 길게 누릅니다.



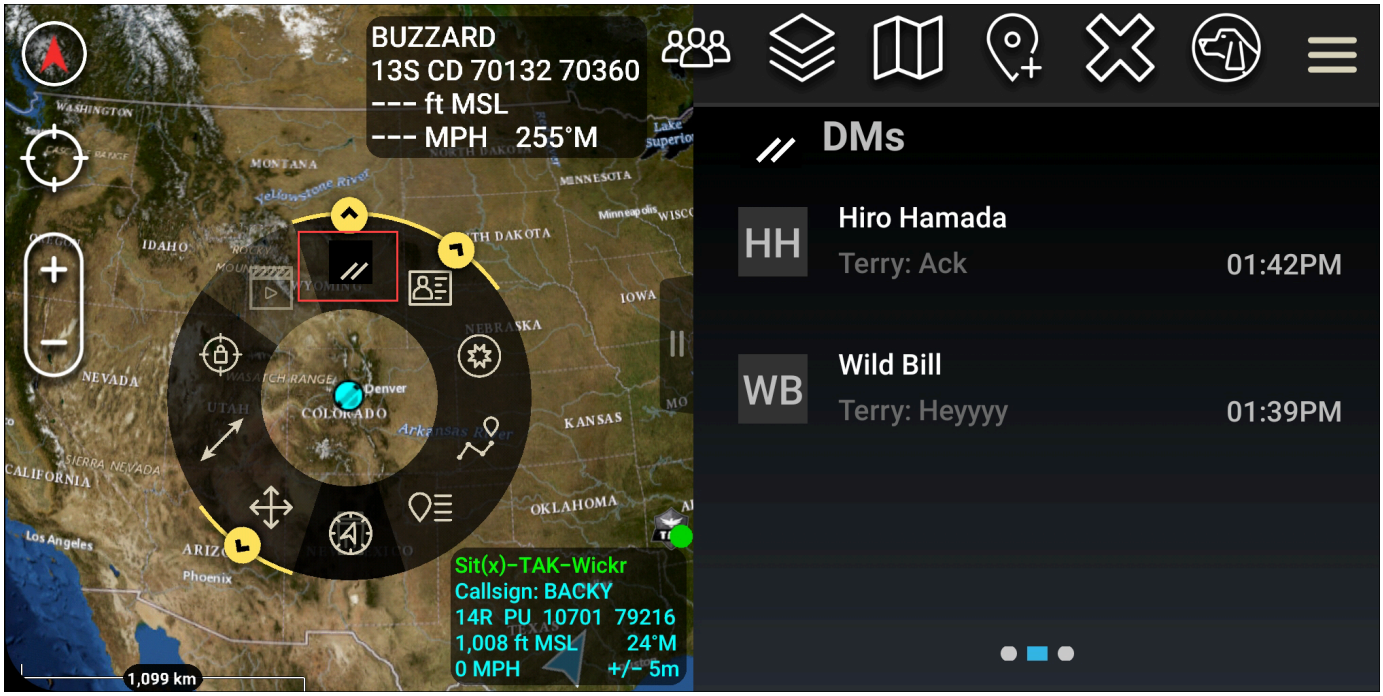
4. 메시지를 녹음하세요.
5. 메시지를 녹음한 후 버튼을 놓으면 메시지를 보낼 수 있습니다.

ATAK용 핀 휠(빠른 액세스)

바람개비 또는 퀵 액세스 기능은 일대일 대화나 다이렉트 메시지에 사용됩니다.

바람개비를 사용하려면 다음 절차를 완료합니다.

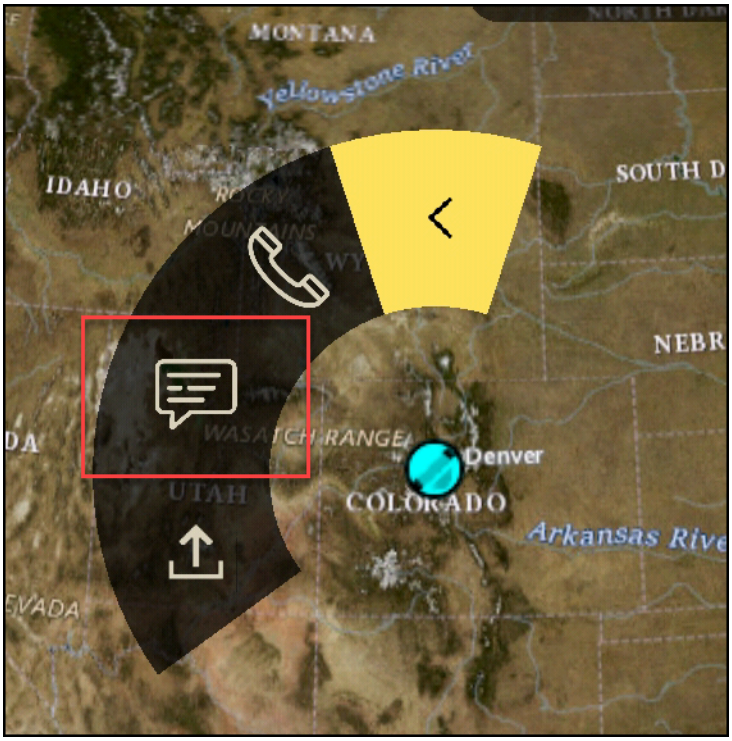
1. ATAK 맵의 분할 화면 보기와 Wickr for ATAK 플러그인을 동시에 엽니다. 맵 보기에는 팀원이나 자산이 표시됩니다.
2. 사용자 아이콘을 선택하여 바람개비를 엽니다.
3. 선택한 사용자가 사용할 수 있는 옵션을 보려면 Wickr 아이콘을 선택합니다.



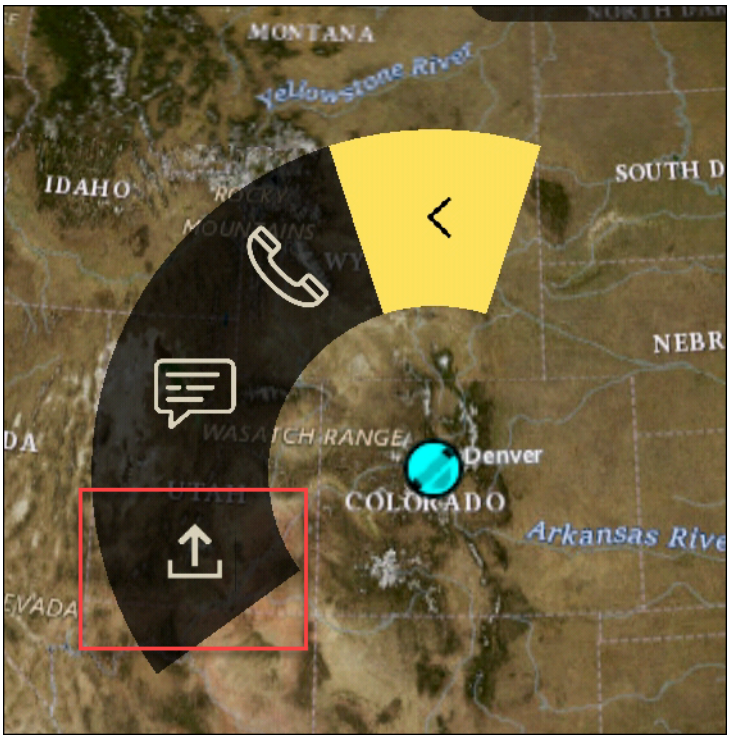
4. 바람개비에서 다음 아이콘 중 하나를 선택합니다.

   - 전화: 통화할 때 선택합니다.

   - 메시지: 채팅할 때 선택합니다.



- 파일 전송: 파일을 보낼 때 선택합니다.



ATAK 탐색

플러그인 UI에는 화면 오른쪽 하단에 파란색과 흰색 모양으로 표시되는 세 개의 플러그인 보기가 포함되어 있습니다. 왼쪽과 오른쪽으로 스와이프하여 보기를 선택할 수 있습니다.

- 연락처 보기: 다이렉트 메시지 그룹 또는 룸 대화를 만들 때 사용합니다.
- DM 보기: 일대일 대화를 만들 때 사용합니다. 채팅 기능은 Wickr 네이티브 앱에 있는 것처럼 작동합니다. 이 기능을 사용하면 맵 보기에 머물면서 플러그인에서 다른 사람들과 소통할 수 있습니다.
- 룸 보기: 네이티브 앱의 기존 룸이 포팅됩니다. 플러그인에서 수행한 모든 작업은 Wickr 네이티브 앱에 반영됩니다.

> **Note**
>
> 룸 삭제와 같은 특정 기능은 사용자의 의도하지 않은 수정과 현장 장비로 인한 간섭을 방지하기 위해 네이티브 앱 및 개인적으로만 수행할 수 있습니다.

Wickr 네트워크에 대한 목록을 허용할 포트 및 도메인

Wickr가 올바르게 작동하는지 확인하려면 다음 포트를 허용하십시오.

포트

- TCP 포트 443(메시지 및 첨부 파일용)
- UDP 포트 16384-16584(통화용)

리전별로 허용 목록에 추가할 도메인 및 주소

가능한 모든 호출 도메인 및 서버 IP 주소를 허용해야 하는 경우 다음 리전별 잠재적 CIDRs. 이 목록은 변경될 수 있으므로 주기적으로 확인하세요.

> **Note**
>
> 등록 및 확인 이메일은 `no-reply@amazonaws.com` 및에서 전송됩니다`donotreply@wickr.email`.

미국 동부(버지니아 북부)

도메인:	• gw-pro-prod.wickr.com • api.messaging.wickr.us-east-1.amazonaws.com • ingress.prod.calling.wickr.com
CIDR 주소 호출:	• 44.211.195.0/27 • 44.213.83.32/28
IP 주소 호출:	• 44.211.195.0 • 44.211.195.1 • 44.211.195.2 • 44.211.195.3 • 44.211.195.4 • 44.211.195.5 • 44.211.195.6 • 44.211.195.7 • 44.211.195.8 • 44.211.195.9 • 44.211.195.10 • 44.211.195.11 • 44.211.195.12 • 44.211.195.13 • 44.211.195.14 • 44.211.195.15 • 44.211.195.16 • 44.211.195.17 • 44.211.195.18 • 44.211.195.19 • 44.211.195.20 • 44.211.195.21

	• 44.211.195.22 • 44.211.195.23 • 44.211.195.24 • 44.211.195.25 • 44.211.195.26 • 44.211.195.27 • 44.211.195.28 • 44.211.195.29 • 44.211.195.30 • 44.211.195.31 • 44.213.83.32 • 44.213.83.33 • 44.213.83.34 • 44.213.83.35 • 44.213.83.36 • 44.213.83.37 • 44.213.83.38 • 44.213.83.39 • 44.213.83.40 • 44.213.83.41 • 44.213.83.42 • 44.213.83.43 • 44.213.83.44 • 44.213.83.45 • 44.213.83.46 • 44.213.83.47

아시아 태평양(말레이시아)

도메인:	• gw-pro-prod.wickr.com

	• api.messaging.wickr.ap-southeast-5.amazonaws.com • ingress.prod.calling.wickr.ap-southeast-5.amazonaws.com
CIDR 주소 호출:	• 43.216.226.160/28
IP 주소 호출:	• 43.216.226.160 • 43.216.226.161 • 43.216.226.162 • 43.216.226.163 • 43.216.226.164 • 43.216.226.165 • 43.216.226.166 • 43.216.226.167 • 43.216.226.168 • 43.216.226.169 • 43.216.226.170 • 43.216.226.171 • 43.216.226.172 • 43.216.226.173 • 43.216.226.174 • 43.216.226.175

아시아 태평양(싱가포르)

도메인:	• gw-pro-prod.wickr.com • api.messaging.wickr.ap-southeast-1.amazonaws.com • ingress.prod.calling.wickr.ap-southeast-1.amazonaws.com
CIDR 주소 호출:	• 47.129.23.144/28

IP 주소 호출:	• 47.129.23.144 • 47.129.23.145 • 47.129.23.146 • 47.129.23.147 • 47.129.23.148 • 47.129.23.149 • 47.129.23.150 • 47.129.23.151 • 47.129.23.152 • 47.129.23.153 • 47.129.23.154 • 47.129.23.155 • 47.129.23.156 • 47.129.23.157 • 47.129.23.158 • 47.129.23.159

아시아 태평양(시드니)

도메인:	• gw-pro-prod.wickr.com • api.messaging.wickr.ap-southeast-2.amazonaws.com • ingress.prod.calling.wickr.ap-southeast-2.amazonaws.com
CIDR 주소 호출:	• 3.27.180.208/28
IP 주소 호출:	• 3.27.180.208 • 3.27.180.209 • 3.27.180.210 • 3.27.180.211 • 3.27.180.212

	• 3.27.180.213 • 3.27.180.214 • 3.27.180.215 • 3.27.180.216 • 3.27.180.217 • 3.27.180.218 • 3.27.180.219 • 3.27.180.220 • 3.27.180.221 • 3.27.180.222 • 3.27.180.223

아시아 태평양(도쿄)

도메인:	• gw-pro-prod.wickr.com • api.messaging.wickr.ap-northeast-1.amazonaws.com • ingress.prod.calling.wickr.ap-northeast-1.amazonaws.com
CIDR 주소 호출:	• 57.181.142.240/28
IP 주소 호출:	• 57.181.142.240 • 57.181.142.241 • 57.181.142.242 • 57.181.142.243 • 57.181.142.244 • 57.181.142.245 • 57.181.142.246 • 57.181.142.247 • 57.181.142.248 • 57.181.142.249

	• 57.181.142.250 • 57.181.142.251 • 57.181.142.252 • 57.181.142.253 • 57.181.142.254 • 57.181.142.255

캐나다(중부)

도메인:	• gw-pro-prod.wickr.com • api.messaging.wickr.ca-central-1.amazonaws.com • ingress.prod.calling.wickr.ca-central-1.amazonaws.com
CIDR 주소 호출:	• 15.156.152.96/28
IP 주소 호출:	• 15.156.152.96 • 15.156.152.97 • 15.156.152.98 • 15.156.152.99 • 15.156.152.100 • 15.156.152.101 • 15.156.152.102 • 15.156.152.103 • 15.156.152.104 • 15.156.152.105 • 15.156.152.106 • 15.156.152.107 • 15.156.152.108 • 15.156.152.109 • 15.156.152.110

	• 15.156.152.111

유럽(프랑크푸르트)

도메인:	• gw-pro-prod.wickr.com • api.messaging.wickr.eu-central-1.amazonaws.com • ingress.prod.calling.wickr.eu-central-1.amazonaws.com
CIDR 주소 호출:	• 3.78.252.32/28
IP 주소 호출:	• 3.78.252.32 • 3.78.252.33 • 3.78.252.34 • 3.78.252.35 • 3.78.252.36 • 3.78.252.37 • 3.78.252.38 • 3.78.252.39 • 3.78.252.40 • 3.78.252.41 • 3.78.252.42 • 3.78.252.43 • 3.78.252.44 • 3.78.252.45 • 3.78.252.46 • 3.78.252.47
메시징 IP 주소:	• 3.163.236.183 • 3.163.238.183 • 3.163.251.183 • 3.163.232.183

	• 3.163.241.183 • 3.163.245.183 • 3.163.248.183 • 3.163.234.183 • 3.163.237.183 • 3.163.243.183 • 3.163.247.183 • 3.163.240.183 • 3.163.242.183 • 3.163.244.183 • 3.163.246.183 • 3.163.249.183 • 3.163.252.183 • 3.163.235.183 • 3.163.250.183 • 3.163.239.183 • 3.163.233.183

유럽(런던)

도메인:	• gw-pro-prod.wickr.com • api.messaging.wickr.eu-west-2.amazonaws.com • ingress.prod.calling.wickr.eu-west-2.amazonaws.com
CIDR 주소 호출:	• 13.43.91.48/28
IP 주소 호출:	• 13.43.91.48 • 13.43.91.49 • 13.43.91.50 • 13.43.91.51

	• 13.43.91.52 • 13.43.91.53 • 13.43.91.54 • 13.43.91.55 • 13.43.91.56 • 13.43.91.57 • 13.43.91.58 • 13.43.91.59 • 13.43.91.60 • 13.43.91.61 • 13.43.91.62 • 13.43.91.63

유럽(스톡홀름)

도메인:	• gw-pro-prod.wickr.com • api.messaging.wickr.eu-north-1.amazonaws.com • ingress.prod.calling.wickr.eu-north-1.amazonaws.com
CIDR 주소 호출:	• 13.60.1.64/28
IP 주소 호출:	• 13.60.1.64 • 13.60.1.65 • 13.60.1.66 • 13.60.1.67 • 13.60.1.68 • 13.60.1.69 • 13.60.1.70 • 13.60.1.71 • 13.60.1.72

	• 13.60.1.73 • 13.60.1.74 • 13.60.1.75 • 13.60.1.76 • 13.60.1.77 • 13.60.1.78 • 13.60.1.79

유럽(취리히)

도메인:	• gw-pro-prod.wickr.com • api.messaging.wickr.eu-central-2.amazonaws.com • ingress.prod.calling.wickr.eu-central-2.amazonaws.com
CIDR 주소 호출:	• 16.63.106.224/28
IP 주소 호출:	• 16.63.106.224 • 16.63.106.225 • 16.63.106.226 • 16.63.106.227 • 16.63.106.228 • 16.63.106.229 • 16.63.106.230 • 16.63.106.231 • 16.63.106.232 • 16.63.106.233 • 16.63.106.234 • 16.63.106.235 • 16.63.106.236 • 16.63.106.237

	• 16.63.106.238 • 16.63.106.239

AWS GovCloud(미국 서부)

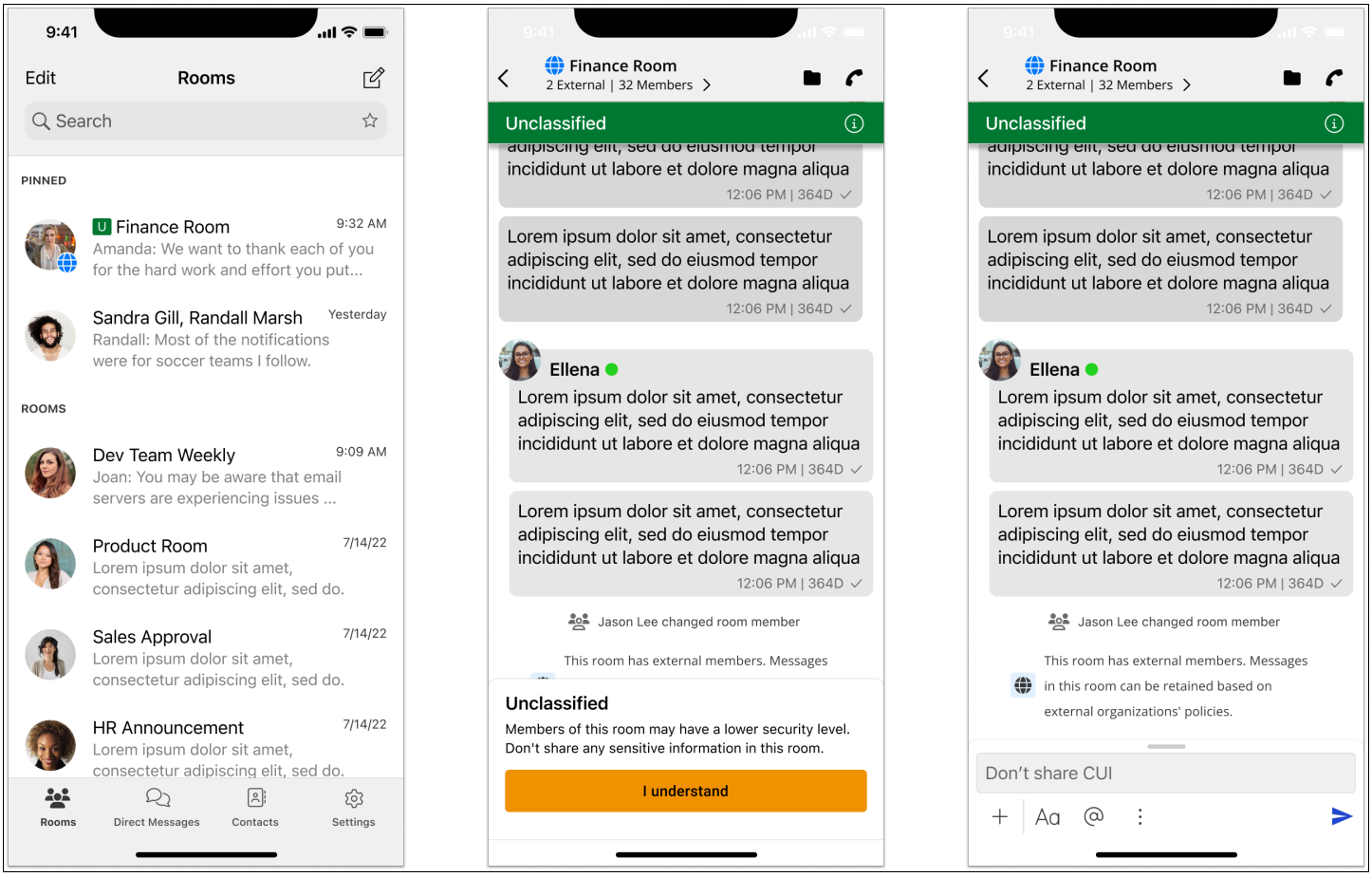
도메인:	• gw-pro-prod.wickr.com • api.messaging.wickr.us-gov-west-1.amazonaws.com • ingress-prod-calling.wickr.us-gov-west-1.amazonaws.com • s3.us-gov-west-1.amazonaws.com • s3-fips.us-gov-west-1.amazonaws.com • s3.amazonaws.com • register.wickr.us-gov-west-1.amazonaws.com • admin.wickr.us-gov-west-1.amazonaws.com • admin.messaging.wickr.us-gov-west-1.amazonaws.com • cognito-identity.us-gov-west-1.amazonaws.com • kinesis.us-gov-west-1.amazonaws.com
CIDR 주소 호출:	• 3.30.186.208/28 • 3.31.11.216/29
IP 주소 호출:	• 3.30.186.208 • 3.30.186.209 • 3.30.186.210 • 3.30.186.211 • 3.30.186.212 • 3.30.186.213 • 3.30.186.214

	• 3.30.186.215 • 3.30.186.216 • 3.30.186.217 • 3.30.186.218 • 3.30.186.219 • 3.30.186.220 • 3.30.186.221 • 3.30.186.222 • 3.30.186.223 • 3.31.11.216 • 3.31.11.217 • 3.31.11.218 • 3.31.11.219 • 3.31.11.220 • 3.31.11.221 • 3.31.11.222 • 3.31.11.223

GovCloud 교차 경계 분류 및 페더레이션

AWS Wickr는 GovCloud 사용자에 맞게 조정된 WickrGov 클라이언트를 제공합니다. GovCloud 페더레이션은 GovCloud 사용자와 상용 사용자 간의 통신을 허용합니다. 교차 경계 분류 기능을 사용하면 GovCloud 사용자의 대화에 대한 사용자 인터페이스 변경이 가능합니다. GovCloud 사용자는 정부에서 정의한 분류와 관련된 엄격한 지침을 준수해야 합니다. GovCloud 사용자가 상용 사용자(엔터프라이즈, AWS Wickr, 게스트 사용자)와 대화하는 경우 다음과 같은 분류되지 않은 경고가 표시됩니다.

- 방 목록의 U 태그
- 메시지 화면의 분류되지 않은 승인
- 대화 상단의 분류되지 않은 배너



> **Note**
>
> 이러한 경고는 GovCloud 사용자가 외부 사용자와 대화 중이거나 회의실에 있는 경우에만 표시됩니다. 외부 사용자가 대화를 종료하면 사라집니다. GovCloud 사용자 간의 대화에는 경고가 표시되지 않습니다.

AWS Wickr용 파일 미리 보기

Wickr Premium 티어(프리미엄 무료 평가판 포함)를 사용하는 조직은 이제 보안 그룹 수준에서 파일 다운로드 권한을 관리할 수 있습니다.

파일 다운로드는 보안 그룹에서 기본적으로 활성화됩니다. 관리자는 관리자 패널을 통해 파일 다운로드를 활성화하거나 비활성화할 수 있습니다. 이 설정은 전체 Wickr 네트워크에 적용됩니다.

파일 다운로드를 활성화하거나 비활성화하려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.

2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 Security groups를 선택합니다.
4. 편집할 보안 그룹의 이름을 선택합니다.

   보안 그룹 세부 정보 페이지에는 보안 그룹의 설정이 다른 탭에 표시됩니다.
5. 메시징 탭의 미디어 및 링크 섹션에서 편집을 선택합니다.
6. 미디어 및 링크 편집 페이지에서 파일 다운로드 옵션을 선택하거나 선택 취소합니다.
7. 변경 사항 저장을 선택합니다.

보안 그룹에 대해 파일 다운로드가 활성화되면 사용자는 다이렉트 메시지 및 방에서 공유된 파일을 다운로드할 수 있습니다. 다운로드가 비활성화된 경우 이러한 파일을 미리 보고 파일 탭에 업로드할 수만 있지만 다운로드할 수는 없습니다. 또한 사용자는 스크린샷을 찍을 수 없습니다. 시도하면 검은색 화면이 나타납니다.

> **Note**
>
> 파일 다운로드가 비활성화되면이 파일 설정이 적용되려면 해당 보안 그룹의 모든 사용자가 Wickr 버전 6.54 이상이어야 합니다.

> **Note**
>
> 다른 네트워크(페더레이션으로 인해) 및 보안 그룹의 사용자가 있는 방에서는 각 사용자가 파일을 미리 보거나 다운로드할 수 있는 기능이 특정 보안 그룹 설정을 기반으로 합니다. 따라서 일부 사용자는 룸에서 파일을 다운로드할 수 있고 다른 사용자는 미리 보기만 할 수 있습니다.

AWS Wickr에서 사용자 관리

Wickr AWS Management Console 용의 사용자 관리 섹션에서 현재 Wickr 사용자 및 봇을 보고 세부 정보를 수정할 수 있습니다.

주제

AWS Wickr 네트워크의 팀 디렉터리

Wickr AWS Management Console 용의 사용자 관리 섹션에서 현재 Wickr 사용자를 보고 세부 정보를 수정할 수 있습니다.

주제

AWS Wickr 네트워크의 사용자 보기

Wickr 네트워크에 등록된 사용자의 세부 정보를 볼 수 있습니다.

Wickr 네트워크에 등록된 사용자를 보려면 다음 절차를 완료하십시오.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 사용자 관리를 선택합니다.

   팀 디렉터리 탭에는 이름, 이메일 주소, 할당된 보안 그룹 및 현재 상태를 포함하여 Wickr 네트워크에 등록된 사용자가 표시됩니다. 현재 사용자의 경우 장치를 보고, 세부 정보를 편집하고, 일시 중지, 삭제하고, 다른 Wickr 네트워크로 전환할 수 있습니다.

AWS Wickr 네트워크에서 사용자 초대

Wickr 네트워크에서 사용자를 초대할 수 있습니다.

Wickr 네트워크에서 사용자를 초대하려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 사용자 관리를 선택합니다.
4. 팀 디렉터리 탭에서 사용자 초대를 선택합니다.
5. 사용자 초대 페이지에서 사용자의 이메일 주소와 보안 그룹을 입력합니다. 이메일 주소와 보안 그룹만 필수 필드입니다. 사용자에게 적합한 보안 그룹을 선택해야 합니다. Wickr는 사용자가 지정한 주소로 초대 이메일을 보냅니다.
6. 사용자 초대를 선택합니다.

   이메일이 사용자에게 전송됩니다. 이메일은 Wickr 클라이언트 애플리케이션의 다운로드 링크와 Wickr 등록용 링크를 제공합니다. 사용자가 이메일에 있는 링크를 사용하여 Wickr에 등록하면 Wickr 팀 디렉토리의 상태가 보류 중에서 활성으로 변경됩니다.

AWS Wickr 네트워크에서 사용자 편집

Wickr 네트워크에서 사용자를 편집할 수 있습니다.

사용자를 편집하려면 다음 절차를 완료하십시오.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 사용자 관리를 선택합니다.
4. 팀 디렉터리 탭에서 편집하려는 사용자의 세로 줄임표(점 3개) 아이콘을 선택합니다.
5. 편집을 선택합니다.
6. 사용자 정보를 편집한 다음 변경 사항 저장을 선택합니다.

AWS Wickr 네트워크에서 사용자 삭제

Wickr 네트워크에서 사용자를 삭제할 수 있습니다.

사용자를 삭제하려면 다음 절차를 완료하십시오.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 사용자 관리를 선택합니다.
4. 팀 디렉터리 탭에서 삭제할 사용자의 세로 줄임표(점 3개) 아이콘을 선택합니다.
5. 호스트를 삭제하려면 삭제를 선택합니다.

   사용자를 삭제하면 해당 사용자는 더 이상 Wickr 클라이언트에서 Wickr 네트워크에 로그인할 수 없습니다.
6. 팝업 창에서 삭제를 선택합니다.

AWS Wickr 네트워크의 사용자 대량 삭제

Wickr AWS Management Console 용의 사용자 관리 섹션에서 Wickr 네트워크 사용자를 대량 삭제할 수 있습니다.

> **Note**
>
> 사용자를 대량 삭제하는 옵션은 SSO가 활성화되지 않은 경우에만 적용됩니다.

CSV 템플릿을 사용하여 Wickr 네트워크 사용자를 대량 삭제하려면 다음 절차를 완료하십시오.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 사용자 관리를 선택합니다.
4. 팀 디렉터리 탭에는 Wickr 네트워크에 등록된 사용자가 표시됩니다.
5. 팀 디렉터리 탭에서 사용자 관리를 선택한 다음 대량 삭제를 선택합니다.
6. 사용자 대량 삭제 페이지에서 샘플 CSV 템플릿을 다운로드합니다. 샘플 템플릿을 다운로드하려면 템플릿 다운로드를 선택합니다.
7. 네트워크에서 대량 삭제하려는 사용자의 이메일을 추가하여 템플릿을 완료합니다.
8. 완성된 CSV 템플릿을 업로드합니다. 파일을 업로드 상자에 끌어다 놓거나 파일 선택을 선택할 수 있습니다.
9. 확인란을 선택합니다. 사용자 삭제는 되돌릴 수 없습니다.
10. 사용자 삭제를 선택합니다.

> **Note**
>
> 이 작업을 수행하면 사용자 삭제가 즉시 시작되며 몇 분 정도 걸릴 수 있습니다. 삭제된 사용자는 더 이상 Wickr 클라이언트에서 Wickr 네트워크에 로그인할 수 없습니다.

팀 디렉터리의 CSV를 다운로드하여 Wickr 네트워크 사용자를 대량 삭제하려면 다음 절차를 완료하십시오.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 사용자 관리를 선택합니다.
4. 팀 디렉터리 탭에는 Wickr 네트워크에 등록된 사용자가 표시됩니다.
5. 팀 디렉터리 탭에서 사용자 관리를 선택한 다음 CSV로 다운로드를 선택합니다.
6. 팀 디렉터리 CSV 템플릿을 다운로드한 후 삭제할 필요가 없는 사용자 행을 삭제하십시오.
7. 팀 디렉터리 탭에서 사용자 관리를 선택한 다음 대량 삭제를 선택합니다.
8. 사용자 대량 삭제 페이지에서 팀 디렉터리 CSV 템플릿을 업로드합니다. 파일을 업로드 상자로 끌어다 놓거나 파일 선택을 선택할 수 있습니다.
9. 확인란을 선택합니다. 사용자 삭제는 되돌릴 수 없습니다.
10. 사용자 삭제를 선택합니다.

> **Note**
>
> 이 작업을 수행하면 사용자 삭제가 즉시 시작되며 몇 분 정도 걸릴 수 있습니다. 삭제된 사용자는 더 이상 Wickr 클라이언트에서 Wickr 네트워크에 로그인할 수 없습니다.

AWS Wickr 네트워크의 사용자 대량 일시 중지

Wickr AWS Management Console 용의 사용자 관리 섹션에서 Wickr 네트워크 사용자를 대량 일시 중지할 수 있습니다.

> **Note**
>
> 사용자를 대량 일시 중지하는 옵션은 SSO가 활성화되지 않은 경우에만 적용됩니다.

CSV 템플릿을 사용하여 Wickr 네트워크 사용자를 대량 일시 중지하려면 다음 절차를 완료하십시오.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 사용자 관리를 선택합니다.
4. 팀 디렉터리 탭에는 Wickr 네트워크에 등록된 사용자가 표시됩니다.
5. 팀 디렉터리 탭에서 사용자 관리를 선택한 다음 대량 일시 중지를 선택합니다.
6. 사용자 대량 일시 중지 페이지에서 샘플 CSV 템플릿을 다운로드합니다. 샘플 템플릿을 다운로드하려면 템플릿 다운로드를 선택합니다.
7. 네트워크에서 대량으로 일시 중지하려는 사용자의 이메일을 추가하여 템플릿을 완성합니다.
8. 완성된 CSV 템플릿을 업로드합니다. 파일을 업로드 상자에 끌어다 놓거나 파일 선택을 선택할 수 있습니다.
9. 사용자 일시 중지를 선택합니다.

> **Note**
>
> 이 작업을 수행하면 즉각 사용자를 일시 중지하기 시작되며 몇 분 걸릴 수 있습니다. 일시 중지된 사용자는 Wickr 클라이언트의 Wickr 네트워크에 로그인할 수 없습니다. 클라이언트에서 Wickr 네트워크에 현재 로그인되어 있는 사용자를 일시 중단하면 해당 사용자는 자동으로 로그아웃됩니다.

AWS Wickr 네트워크의 게스트 사용자

Wickr 게스트 사용자 기능을 사용하면 개별 게스트 사용자가 Wickr 클라이언트에 로그인하여 Wickr 네트워크 사용자와 협업할 수 있습니다. Wickr 관리자는 Wickr 네트워크의 게스트 사용자를 활성화하거나 비활성화할 수 있습니다.

이 기능이 활성화되면, Wickr 네트워크에 초대된 게스트 사용자가 Wickr 네트워크의 사용자와 상호 작용할 수 있습니다. 게스트 사용자 기능에 AWS 계정 대한 요금이에 적용됩니다. 게스트 사용자 기능의 요금 책정에 대한 자세한 내용은 요금 책정 추가 기능의 Wickr 요금 책정 페이지를 참조하십시오.

주제

- AWS Wickr 네트워크에서 게스트 사용자 활성화 또는 비활성화
- AWS Wickr 네트워크에서 게스트 사용자 수 보기
- AWS Wickr 네트워크에서 월별 사용량 보기

- AWS Wickr 네트워크의 게스트 사용자 보기
- AWS Wickr 네트워크에서 게스트 사용자 차단

AWS Wickr 네트워크에서 게스트 사용자 활성화 또는 비활성화

Wickr 네트워크에서 게스트 사용자를 활성화하거나 비활성화할 수 있습니다.

Wickr 네트워크의 게스트 사용자를 활성화하거나 비활성화하려면 다음 절차를 완료하십시오.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 Security groups를 선택합니다.
4. 특정 보안 그룹의 이름을 선택합니다.

   > **Note**
   >
   > 개별 보안 그룹에서만 게스트 사용자를 활성화할 수 있습니다. Wickr 네트워크의 모든 보안 그룹에 게스트 사용자를 활성화하려면 네트워크의 각 보안 그룹에 대해 이 기능을 활성화해야 합니다.

5. 보안 그룹에서 연동 탭을 선택합니다.
6. 게스트 사용자를 활성화하는 옵션을 사용할 수 있는 두 가지 위치가 있습니다.

   - 로컬 페더레이션 - 미국 동부(버지니아 북부)의 네트워크에서 페이지의 로컬 페더레이션 섹션에서 편집을 선택합니다.
   - 글로벌 페더레이션 - 다른 리전의 다른 모든 네트워크의 경우 페이지의 글로벌 페더레이션 섹션에서 편집을 선택합니다.
7. 페더레이션 편집 페이지에서 페더레이션 활성화를 선택합니다.
8. 변경 사항 저장을 선택하여 변경 사항을 저장하고 보안 그룹에 적용되도록 합니다.

   이제 Wickr 네트워크의 특정 보안 그룹에 등록된 사용자가 게스트 사용자와 상호 작용할 수 있습니다. 자세한 내용은 Wickr 사용 설명서의 게스트 사용자를 참조하십시오.

AWS Wickr 네트워크에서 게스트 사용자 수 보기

Wickr 네트워크에서 게스트 사용자 수를 볼 수 있습니다.

Wickr 네트워크에 등록된 사용자를 보려면 다음 절차를 완료하십시오.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 사용자 관리를 선택합니다.

   사용자 관리 페이지에는 Wickr 네트워크의 게스트 사용자 수가 표시됩니다.

AWS Wickr 네트워크에서 월별 사용량 보기

청구 기간 동안 네트워크가 통신한 게스트 사용자 수를 볼 수 있습니다.

Wickr 네트워크의 월별 사용량을 보려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 사용자 관리를 선택합니다.
4. 게스트 사용자 탭을 선택합니다.

   게스트 사용자 탭에는 게스트 사용자의 월별 사용량이 표시됩니다.

> **Note**
>
> 게스트 청구 데이터는 24시간마다 업데이트됩니다.

AWS Wickr 네트워크의 게스트 사용자 보기

특정 결제 기간 동안 네트워크 사용자가 통신한 게스트 사용자를 볼 수 있습니다.

특정 결제 기간 동안 네트워크 사용자가 통신한 게스트 사용자를 보려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 사용자 관리를 선택합니다.
4. 게스트 사용자 탭을 선택합니다.

   게스트 사용자 탭에는 네트워크의 게스트 사용자가 표시됩니다.

AWS Wickr 네트워크에서 게스트 사용자 차단

Wickr 네트워크에서 게스트 사용자를 차단 및 차단 해제할 수 있습니다. 차단된 사용자는 네트워크에 있는 누구와도 통신할 수 없습니다.

게스트 사용자 차단

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 사용자 관리를 선택합니다.
4. 게스트 사용자 탭을 선택합니다.

   게스트 사용자 탭에는 네트워크의 게스트 사용자가 표시됩니다.
5. 게스트 사용자 섹션에서, 차단하려는 게스트 사용자의 이메일을 찾습니다.
6. 게스트 사용자 이름의 오른쪽에서 점 3개를 선택하고 게스트 사용자 차단을 선택합니다.
7. 팝업 창에서 차단을 선택합니다.
8. Wickr 네트워크에서 차단된 사용자 목록을 보려면 상태 드롭다운 메뉴를 선택한 다음 차단됨을 선택합니다.

게스트 사용자 차단 해제

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 사용자 관리를 선택합니다.
4. 게스트 사용자 탭을 선택합니다.

   게스트 사용자 탭에는 네트워크의 게스트 사용자가 표시됩니다.
5. 상태 드롭다운 메뉴를 선택한 다음 차단됨을 선택합니다.
6. 차단됨 섹션에서 차단을 해제하려는 게스트 사용자의 이메일을 찾습니다.
7. 게스트 사용자 이름의 오른쪽에서 점 3개를 선택하고 사용자 차단 해제를 선택합니다.
8. 팝업 창에서 차단 해제를 선택합니다.

AWS Wicker의 보안

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다 AWS 클라우드. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. AWS Wickr에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 AWS 제공 범위 내 서비스규정 준수 프로그램 .
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Wickr 사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표를 충족하도록 Wickr를 구성하는 방법을 보여줍니다. 또한 Wickr 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

주제

AWS Wickr의 데이터 보호

AWS 공동 책임 모델 AWS Wickr의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 이 인프라에 호스팅되는 콘텐츠에 대한 통제 권한을 유지할 책임이 있습니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 관한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM)를 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- 내부의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다.
- 명령줄 인터페이스 또는 API를 AWS 통해에 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 Wickr 또는 기타 AWS 서비스 에서 콘솔 AWS CLI, API 또는 AWS SDKs를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명을 URL에 포함해서는 안 됩니다.

AWS Wickr를 위한 자격 증명 및 액세스 관리

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 누가 Wickr 리소스를 사용하도록 인증되고

(로그인됨) 권한이 부여되는지(권한 가짐)를 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

AWS Wickr 대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 역할에 따라 다릅니다.

- 서비스 사용자 - 기능에 액세스할 수 없는 경우 관리자에게 권한 요청(참조AWS Wickr 자격 증명 및 액세스 문제 해결)
- 서비스 관리자 - 사용자 액세스 결정 및 권한 요청 제출(AWS Wickr가 IAM과 작동하는 방법 참조)
- IAM 관리자 - 액세스를 관리하기 위한 정책 작성(AWS Wickr에 대한 자격 증명 기반 정책 예제 참조)

AWS Wickr의 자격 증명으로 인증

인증은 자격 증명 자격 증명을 AWS 사용하여에 로그인하는 방법입니다. AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할을 수임하여 인증되어야 합니다.

AWS IAM Identity Center (IAM Identity Center), Single Sign-On 인증 또는 Google/Facebook 자격 증명과 같은 자격 증명 소스의 자격 증명을 사용하여 페더레이션 자격 증명으로 로그인할 수 있습니다. 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 AWS 계정에 로그인하는 방법 섹션을 참조하세요.

프로그래밍 방식 액세스를 위해는 요청에 암호화 방식으로 서명할 수 있는 SDK 및 CLI를 AWS 제공합니다. 자세한 내용은 IAM 사용 설명서의 API 요청용AWS Signature Version 4 섹션을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 AWS 계정 theroot 사용자라는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명이 필요한 작업은 IAM 사용 설명서의 루트 사용자 자격 증명이 필요한 작업 섹션을 참조하세요.

페더레이션 ID

가장 좋은 방법은 인간 사용자가 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 서비스 사용하여에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 디렉터리, 웹 자격 증명 공급자 또는 자격 증명 소스의 자격 증명을 AWS 서비스 사용하여 Directory Service 에 액세스하는 사용자입니다. 페더레이션 ID는 임시 자격 증명을 제공하는 역할을 수임합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center를 추천합니다. 자세한 정보는 AWS IAM Identity Center 사용 설명서의 What is IAM Identity Center?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 개인 또는 애플리케이션에 대한 특정 권한을 가진 ID입니다. 장기 자격 증명이 있는 IAM 사용자 대신 임시 자격 증명을 사용하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 사용하여에 액세스하도록 인간 사용자에게 요구하기를 참조하세요.

IAM 그룹은 IAM 사용자 모음을 지정하고 대규모 사용자 집합에 대한 관리 권한을 더 쉽게 만듭니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자 사용 사례 섹션을 참조하세요.

IAM 역할

IAM 역할은 임시 자격 증명을 제공하는 특정 권한이 있는 자격 증명입니다. 사용자에서 IAM 역할(콘솔)로 전환하거나 또는 API 작업을 호출하여 역할을 수임할 수 있습니다. AWS CLI AWS 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

IAM 역할은 페더레이션 사용자 액세스, 임시 IAM 사용자 권한, 교차 계정 액세스, 교차 서비스 액세스 및 Amazon EC2에서 실행되는 애플리케이션에 유용합니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

AWS Wickr에 대한 정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결될 때 권한을 정의합니다.는 보안 주체가 요청할 때 이러한 정책을 AWS 평가합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요 섹션을 참조하세요.

정책을 사용하여 관리자는 어떤 보안 주체가 어떤 리소스에 대해 어떤 조건에서 작업을 수행할 수 있는지 정의하여 누가 무엇을 액세스할 수 있는지 지정합니다.

기본적으로 사용자 및 역할에는 어떠한 권한도 없습니다. IAM 관리자는 IAM 정책을 생성하고 사용자가 수임할 수 있는 역할에 추가합니다. IAM 정책은 작업을 수행하기 위해 사용하는 방법과 관계없이 작업에 대한 권한을 정의합니다.

ID 기반 정책

ID 기반 정책은 ID(사용자, 사용자 그룹 또는 역할)에 연결하는 JSON 권한 정책 문서입니다. 이러한 정책은 자격 증명이 수행할 수 있는 작업, 대상 리소스 및 이에 관한 조건을 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책(단일 ID에 직접 포함) 또는 관리형 정책(여러 ID에 연결된 독립 실행형 정책)일 수 있습니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택 섹션을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 예를 들어 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

액세스 제어 목록(ACL)

액세스 제어 목록(ACL)은 어떤 위탁자(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Amazon S3 AWS WAF및 Amazon VPC는 ACLs. ACL에 관한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 액세스 제어 목록(ACL) 개요를 참조하세요.

기타 정책 타입

AWS 는 덜 일반적인 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 ID 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 엔터티에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 개체의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 보안 주체로 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 IAM 엔터티에 대한 권한 경계를 참조하십시오.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 ID 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

AWS AWS Wickr에 대한 관리형 정책

사용자, 그룹 및 역할에 권한을 추가하려면 직접 정책을 작성하는 것보다 AWS 관리형 정책을 사용하는 것이 더 쉽습니다. 팀에 필요한 권한만 제공하는 IAM 고객 관리형 정책을 생성하기 위해서는 시간과 전문 지식이 필요합니다. 빠르게 시작하려면 AWS 관리형 정책을 사용할 수 있습니다. 이 정책은 일반적인 사용 사례를 다루며 사용자의 AWS 계정에서 사용할 수 있습니다. AWS 관리형 정책에 대한 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

AWS 서비스 AWS 관리형 정책을 유지 관리하고 업데이트합니다. AWS 관리형 정책에서는 권한을 변경할 수 없습니다. 서비스에서 때때로 추가 권한을 AWS 관리형 정책에 추가하여 새로운 기능을 지원합니다. 이 유형의 업데이트는 정책이 연결된 모든 ID(사용자, 그룹 및 역할)에 적용됩니다. 서비스는 새로운 기능이 시작되거나 새 작업을 사용할 수 있을 때 AWS 관리형 정책에 업데이트됩니다. 서비스

는 AWS 관리형 정책에서 권한을 제거하지 않으므로 정책 업데이트로 인해 기존 권한이 손상되지 않습니다.

AWS 관리형 정책: AWSWickrFullAccess

`AWSWickrFullAccess` 정책을 IAM ID에 연결할 수 있습니다. 이 정책은 Wickr 서비스에 대한 모든 관리 권한을 부여합니다. 여기에는 AWS Management Console의 Wickr에 대한 AWS Management Console 도 포함됩니다. ID에 정책을 연결하는 방법에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 IAM ID 권한 추가 및 제거를 참조하십시오.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `wickr`— Wickr 서비스에 완전한 관리 권한을 부여합니다.

JSON

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

AWS 관리형 정책에 대한 Wickr 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후부터 Wickr의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 Wickr 문서 기록 페이지에서 RSS 피드를 구독하십시오.

변경	설명	Date
AWSWickrFullAccess — 새 정책	Wickr는 Wickr 서비스에 전체 관리 권한을 부여하는 새 정	2022년 11월 28일

변경	설명	Date
	책을 추가했습니다. 여기에는 AWS Management Console의 Wickr 관리자 콘솔도 포함됩니다.	
Wickr 변경 내용 추적 시작	Wickr는 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2022년 11월 28일

AWS Wickr가 IAM과 작동하는 방법

IAM을 사용하여 Wickr에 대한 액세스를 관리하기 전에 Wickr와 함께 사용할 수 있는 IAM 기능을 알아보십시오.

AWS Wickr와 함께 사용할 수 있는 IAM 기능

IAM 특성	Wickr 지원
자격 증명 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	아니요
정책 조건 키	아니요
ACL	아니요
ABAC(정책 내 태그)	아니요
임시 보안 인증	아니요
위탁자 권한	아니요
서비스 역할	아니요

IAM 특성	Wickr 지원
서비스 연결 역할	아니요

Wickr 및 기타 AWS 서비스에서 대부분의 IAM 기능을 사용하는 방법을 개괄적으로 알아보려면 IAM 사용 설명서의 AWS IAM으로 작업하는 서비스를 참조하세요.

Wickr에 대한 자격 증명 기반 정책

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. JSON 정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

Wickr에 대한 자격 증명 기반 정책 예제

Wickr 자격 증명 기반 정책의 예를 보려면 AWS Wickr에 대한 자격 증명 기반 정책 예제 단원을 참조하십시오.

Wickr 내 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는가 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM에서 교차 계정 리소스 액세스를 참조하세요.

Wickr를 위한 정책 작업

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

Wickr 작업 목록을 보려면 서비스 권한 부여 참조의 AWS Wickr가 정의한 작업를 참조하십시오.

Wickr의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
wickr
```

단일 문에서 여러 작업을 지정하려면 쉼표로 구분합니다.

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

Wickr 자격 증명 기반 정책의 예를 보려면 AWS Wickr에 대한 자격 증명 기반 정책 예제 단원을 참조하십시오.

Wickr 정책 리소스

정책 리소스 지원: 아니요

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

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

Wickr 리소스 유형 및 해당 ARN의 목록을 보려면, 서비스 권한 부여 참조의 AWS Wickr가 정의한 리소스를 참조하십시오. 각 리소스의 ARN에 어떤 작업을 지정할 수 있는지 알아보려면 AWS Wickr가 정의한 작업을 참조하십시오.

Wickr 자격 증명 기반 정책의 예를 보려면 AWS Wickr에 대한 자격 증명 기반 정책 예제 단원을 참조하십시오.

Wickr를 위한 정책 조건 키

서비스별 정책 조건 키 지원: 아니요

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소는 정의된 기준에 따라 문이 실행되는 시기를 지정합니다. 같음(equals) 또는 미만(less than)과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

Wickr 조건 키 목록을 보려면, 서비스 권한 부여 참조의 AWS Wickr를 위한 조건 키를 참조하십시오. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 AWS Wickr가 정의한 작업 단원을 참조하십시오.

Wickr 자격 증명 기반 정책의 예를 보려면 AWS Wickr에 대한 자격 증명 기반 정책 예제 단원을 참조하십시오.

Wickr의 ACL

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Wick와 함께 ABAC

ABAC 지원(정책의 태그): 아니요

속성 기반 액세스 제어(ABAC)는 태그라고 불리는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. IAM 엔터티 및 AWS 리소스에 태그를 연결한 다음 보안 주체의 태그가 리소스의 태그와 일치할 때 작업을 허용하는 ABAC 정책을 설계할 수 있습니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`또는 `aws:TagKeys`조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여를 통한 권한 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

Wickr에서 보안 인증 정보 사용

임시 자격 증명 지원: 아니요

임시 자격 증명은 AWS 리소스에 대한 단기 액세스를 제공하며 페더레이션 또는 전환 역할을 사용할 때 자동으로 생성됩니다. 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 것이 AWS 좋습니다. 자세한 내용은 IAM 사용 설명서의 IAM의 임시 보안 자격 증명 및 IAM으로 작업하는 AWS 서비스 섹션을 참조하세요.

Wickr의 서비스 간 보안 주요 권한

전달 액세스 세션(FAS) 지원: 아니요

전달 액세스 세션(FAS)은를 호출하는 보안 주체의 권한을 다운스트림 서비스에 대한 요청 AWS 서비스 과 AWS 서비스함께 사용합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

Wickr에 대한 서비스 역할

서비스 역할 지원: 아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스 AWS에 권한을 위임할 역할 생성을 참조하세요.

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 Wickr 기능이 중단될 수 있습니다. Wickr에서 관련 지침을 제공하는 경우에만 서비스 역할을 편집하십시오.

Wickr에 대한 서비스 연결 역할

서비스 연결 역할 지원: 아니요

서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하세요. 서비스 연결 역할 열에서 Yes가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예(Yes) 링크를 선택합니다.

AWS Wickr에 대한 자격 증명 기반 정책 예제

기본적으로 신규 IAM 사용자는 어떤 작업 권한도 없습니다. IAM 관리자는 사용자에게 AWS Wickr 서비스를 관리할 권한을 부여하는 IAM 정책을 생성하고 할당해야 합니다. 다음은 권한 정책의 예입니다.

JSON

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

이 샘플 정책은 사용자에게 AWS Management Console for Wickr를 사용하여 Wickr 네트워크를 나열할 수 있는 권한을 부여합니다. IAM 정책 명령문의 요소에 대해 자세히 알아보려면 Wickr에 대한 자격 증명 기반 정책 섹션을 참조하십시오. 이러한 예제 JSON 정책 문서를 사용하여 IAM 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 JSON 탭에서 정책 생성을 참조하십시오.

사용자가 특정 API 작업에 액세스할 수 있도록 허용하는 IAM 정책을 생성할 수도 있습니다. API 작업에 대한 액세스는 AWS Wickr 콘솔과 별도로 관리됩니다. 다음은 특정 API 작업에 대한 읽기 전용 액세

스 권한을 부여하는 정책의 예입니다. API 작업에 대한 자세한 내용은 AWS Wickr API 참조 시작을 참조하세요.

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

주제

- 정책 모범 사례
- Wickr AWS Management Console 용 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용

정책 모범 사례

자격 증명 기반 정책에 따라 계정에서 사용자가 계정에서 누군가가 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 사용자의 AWS 계정에 대한 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.

- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS 서비스와 같은 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 CloudFormation. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정켭니다. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

Wickr AWS Management Console 용 사용

`AWSWickrFullAccess` AWS 관리형 정책을 IAM 자격 증명에 연결하여의 Wickr 관리자 콘솔을 포함하여 Wickr 서비스에 대한 전체 관리 권한을 부여합니다 AWS Management Console. 자세한 내용은 AWS 관리형 정책: AWSWickrFullAccess 단원을 참조하십시오.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "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": "*"
        }
    ]
}
```

AWS Wickr 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 Wickr 및 IAM으로 작업할 때 마주칠 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다.

주제

- Wickr AWS Management Console 용에서 관리 작업을 수행할 권한이 없음

Wickr AWS Management Console 용에서 관리 작업을 수행할 권한이 없음

Wickr AWS Management Console 용에서 작업을 수행할 권한이 없다는 메시지가 표시되면 관리자에게 문의하여 도움을 받아야 합니다. 관리자는 로그인 보안 인증 정보를 제공한 사람입니다.

다음 예제 오류는 mateojackson IAM 사용자가 Wickr AWS Management Console 용를 사용하여 Wickr AWS Management Console 용에서 Wickr 네트워크를 생성, 관리 또는 보려고 하지만 wickr:CreateAdminSession 및 wickr:ListNetworks 권한이 없는 경우에 발생합니다.

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

이 경우 Mateo는 관리자에게 wickr:CreateAdminSession 및 wickr:ListNetworks 작업을 사용하여 Wickr AWS Management Console 용에 액세스할 수 있도록 정책을 업데이트하도록 요청합니다. 자세한 내용은 AWS Wickr에 대한 자격 증명 기반 정책 예제 및 AWS 관리형 정책: AWSWickrFullAccess 섹션을 참조하세요.

규정 준수 확인

특정 규정 준수 프로그램 범위의 AWS 서비스 목록은 규정 준수 프로그램 AWS 제공 범위 내 서비스규정 준수 프로그램 . 일반 정보는 AWS 규정 준수 프로그램.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 Downloading Reports inDownloading AWS Artifact을 참조하세요.

Wickr 사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 결정됩니다. AWS 에서는 규정 준수를 지원할 다음과 같은 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 -이 배포 가이드에서는 아키텍처 고려 사항에 대해 설명하고 보안 및 규정 준수 중심 기준 환경을 배포하기 위한 단계를 제공합니다 AWS.
- AWS 규정 준수 리소스 -이 워크북 및 가이드 모음은 산업 및 위치에 적용될 수 있습니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 - 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 AWS Config평가합니다.
- AWS Security Hub CSPM -이 AWS 서비스는 보안 업계 표준 및 모범 사례 준수 여부를 확인하는 데 도움이 AWS 되는 내 보안 상태에 대한 포괄적인 보기를 제공합니다.

AWS Wickr의 복원성

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다.는 지연 시간이 짧고 처리량이 많으며 중복성이 높은 네트워킹과 연결된 물리적으로 분리되고 격리된 여러 가용 영역을 AWS 리전 제공합니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케

이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

Wickr는 AWS 글로벌 인프라 외에도 데이터 복원력 및 백업 요구 사항을 지원하는 몇 가지 기능을 제공합니다. 자세한 내용은 AWS Wickr의 데이터 보존 단원을 참조하십시오.

AWS PrivateLink AWS Wickr용

AWS PrivateLink for AWS Wickr를 사용하면 인터페이스 VPC 엔드포인트를 사용하여 Virtual Private Cloud(VPC)와 AWS Wickr의 엔드포인트 하위 집합 간에 프라이빗 연결을 설정할 수 있습니다. 인터페이스 VPC 엔드포인트는 프라이빗 IP 주소를 AWS 사용하여에서 실행되는 서비스에 액세스하는 데 사용할 수 있는 AWS PrivateLink AWS 기술로 구동됩니다.

모바일 클라이언트 또는 기타 온프레미스 디바이스의 경우 VPN을 사용하여 엔드 투 엔드 프라이빗 연결을 위해 디바이스를 VPC에 연결합니다. 자세한 내용은 AWS Virtual Private Network 설명서를 참조하세요.

AWS PrivateLink 및 AWS VPC에 대한 자세한 내용은 AWS PrivateLink 가이드의 What is AWS PrivateLink? 및 Amazon Virtual Private Cloud 사용 설명서의 What is AWS VPC?를 참조하세요. Amazon Virtual Private Cloud

지원되는 AWS Wickr 서비스

다음 AWS Wickr 서비스가 지원합니다 AWS PrivateLink.

서비스	엔드포인트 형식	
AWS Wickr 관리자	`com.amazonaws.` *`your-region`* `.wickr-admin`	
AWS Wickr 메시징	`com.amazonaws.` *`your-region`* `.wickr-messaging`	
AWS Wickr 호출	`com.amazonaws.` *`your-region`* `.wickr-calling`	

현재 모든 Wickr VPC 엔드포인트에서 프라이빗 DNS 이름을 활성화해야 합니다. 자세한 내용은 프라이빗 DNS 이름 활성화를 참조하세요.

Wickr VPC 엔드포인트는 퍼블릭 Wickr 엔드포인트가 FIPS를 지원하는 리전에서 FIPS를 지원합니다. 자세한 내용은 연방 정보 처리 표준 단원을 참조하십시오.

현재 지원되지 않음

- 메시징 및 호출 엔드포인트에 대한 VPC 엔드포인트 정책
- 메시징 및 호출 엔드포인트는에서 사용할 수 없습니다`us-east-1`.

주제

사전 조건

VPC 엔드포인트를 생성하기 전에 다음 사전 조건이 있는지 확인합니다.

1. VPC 구성: 여러 가용 영역에 서브넷이 있는 올바르게 구성된 VPC
2. 보안 그룹: HTTPS 트래픽을 허용하는 적절한 보안 그룹(포트 443)
3. DNS 확인: VPC에서 활성화된 DNS 호스트 이름 및 DNS 확인
4. IAM 권한: VPC 엔드포인트를 생성하고 관리하는 데 필요한 권한

VPC 엔드포인트 생성

AWS Wickr Admin, Messaging 및 Calling에 대한 VPC 엔드포인트를 생성할 수 있습니다.

콘솔을 사용하여 AWS VPC 엔드포인트를 생성하려면 다음 절차를 완료하세요.

1단계: VPC 콘솔로 이동

1. Amazon VPC 콘솔에 로그인합니다.
2. 왼쪽 탐색 창에서 엔드포인트를 선택합니다.

3. 엔드포인트 생성을 선택합니다.

2단계: 엔드포인트 설정 구성

1. 서비스 범주에서 AWS 서비스를 선택합니다.
2. 서비스 이름에서 적절한 서비스를 검색wickr하고 선택합니다.
   - 관리자의 경우: `com.amazonaws.your-region.wickr-admin`
   - 메시징의 경우: `com.amazonaws.your-region.wickr-messaging`
   - 호출의 경우: `com.amazonaws.your-region.wickr-calling`

3단계: 네트워크 구성

1. VPC에서 대상 VPC를 선택합니다.
2. 서브넷에서 고가용성을 위해 여러 가용 영역의 서브넷을 선택합니다.
3. 프라이빗 DNS 이름 활성화에서 확인란을 선택합니다. 이를 통해 프라이빗 DNS 이름을 지원할 수 있습니다.
4. 보안 그룹에서 엔드포인트 네트워크 인터페이스와 연결할 보안 그룹을 선택하거나 생성합니다.

4단계: 엔드포인트 생성

1. 구성을 검토합니다.
2. 선택적으로 태그를 추가하거나 제거할 수 있습니다. 태그는 엔드포인트와 연결하는 데 사용하는 이름-값 페어입니다.
3. 엔드포인트 생성을 선택합니다.

를 사용하여 VPC 엔드포인트를 생성하려면 다음 절차를 완료하세요 AWS CLI.

1. 해당 리전의 서비스 가용성을 확인합니다.

   Wickr 관리자 가용성 확인

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

   Wickr 메시징 가용성 확인

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

Wickr Calling 가용성 확인

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

2. VPC 엔드포인트를 생성합니다.

Wickr 관리자 엔드포인트:

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

Wickr 메시징 엔드포인트

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

Wickr 호출 엔드포인트

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

```
  --private-dns-enabled \
```

제한 사항

다음 기능은를 통해 지원되지 않으며 인터넷 연결이 AWS PrivateLink 필요합니다.

- Wickr Open Access(WOA)
- 클라이언트 애플리케이션 업데이트
  - 모바일 앱(iOS/Android)
    - 소스: App Store/Google Play Store
    - 요구 사항: 인터넷 액세스 필요
  - 데스크톱 애플리케이션
    - Windows/Mac: 글로벌 S3 엔드포인트 사용(AWS PrivateLink 호환되지 않음)
    - Linux: Snap Store 사용(인터넷 액세스 필요)
- 디버깅 및 원격 측정
  - 충돌 보고서
  - 지표 디버그
  - 클라이언트 측 분석 링크
- 모바일 푸시 알림

  이러한 서비스는 인터넷 연결이 필요하며를 사용할 수 없습니다 AWS PrivateLink.
  - Apple 푸시 알림
    - 요구 사항: 직접 인터넷 액세스
    - 포트: 443, 2195, 2196, 5223
    - 참조: Apple Support 설명서
  - Google/Android 알림
    - 요구 사항: Firebase Cloud Messaging 액세스
    - 참조: Firebase 설명서
- AWS Wickr 콘솔은 현재 프라이빗 액세스에서 지원되지 않습니다. 자세한 내용은 지원되는 AWS 리전서비스 콘솔 및 프라이빗 액세스 기능을 참조하세요.

에 필요한 최소 클라이언트 버전 AWS PrivateLink

다음 클라이언트 버전은 AWS PrivateLink를 사용하여 검증되었습니다.

- iOS 6.64(해당하는 경우)
- Android 6.60(해당하는 경우)
- 데스크톱 클라이언트 6.60
- 봇 6.60

추가 구성이 필요한 기능

Wickr 봇

- 요구 사항: 고객 관리형 인프라
- 작업: 봇 종속성에 대한 네트워크 경로 구성
- 고려 사항: 봇이 VPC 엔드포인트를 통해 필요한 AWS 서비스에 도달할 수 있는지 확인

파일 다운로드

- S3 연결: 파일 작업에 필요(프랑크푸르트 리전 제외)
- 솔루션: S3 VPC 게이트웨이 엔드포인트 생성
- 참조: AWS PrivateLink Amazon S3용

AWS Wickr의 인프라 보안

관리형 서비스인 AWS Wickr는 Amazon Web Services: 보안 프로세스 개요 백서에 설명된 AWS 글로벌 네트워크 보안 절차로 보호됩니다.

AWS Wickr의 구성 및 취약성 분석

구성 및 IT 제어는 AWS 와 고객 간의 공동 책임입니다. 자세한 내용은 AWS 공동 책임 모델을 참조하세요.

사양 및 지침에 따라 Wickr를 구성하고, 사용자에게 최신 버전의 Wickr 클라이언트를 다운로드하도록 정기적으로 지시하고, 최신 버전의 Wickr 데이터 보존 봇을 실행하고, 사용자의 Wickr 사용을 모니터링하는 것은 사용자의 책임입니다.

AWS Wickr의 보안 모범 사례

Wickr는 사용자가 자체 보안 정책을 개발하고 구현할 때 고려해야 할 여러 보안 기능을 제공합니다. 다음 모범 사례는 일반적인 지침이며 완벽한 보안 솔루션을 나타내지는 않습니다. 이러한 모범 사례는 환경에 적절하지 않거나 충분하지 않을 수 있으므로 참고용으로만 사용해 주십시오.

Wickr 사용과 관련된 잠재적 보안 이벤트를 방지하려면, 다음 모범 사례를 따릅니다.

- 최소 권한 액세스를 구현하고 Wickr 작업에 사용할 특정 역할을 생성하십시오. IAM 템플릿을 사용하여 역할을 생성합니다. 자세한 내용은 AWS AWS Wickr에 대한 관리형 정책 단원을 참조하십시오.
- AWS Management Console 첫 번째에 인증하여 Wickr AWS Management Console 용에 액세스합니다. 개인용 콘솔 자격 증명을 공유하지 마십시오. 인터넷을 사용하는 모든 사용자는 콘솔을 탐색할 수 있지만 콘솔에 대한 유효한 자격 증명이 없으면 로그인하거나 세션을 시작할 수 없습니다.

AWS Wickr 모니터링

모니터링은 AWS Wickr 및 기타 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다.는 Wickr를 모니터링하고, 이상이 있을 때 보고하고, 필요한 경우 자동 조치를 취할 수 있도록 다음과 같은 모니터링 도구를 AWS 제공합니다.

- AWS CloudTrail는 AWS 계정에 의해 또는 계정을 대신하여 수행된 API 호출 및 관련 이벤트를 캡처하고 사용자가 지정한 Amazon S3 버킷에 로그 파일을 전송합니다. 호출한 사용자 및 계정 AWS, 호출이 수행된 소스 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오. CloudTrail을 사용하는 Wickr API 직접 호출에 대한 자세한 내용은 를 사용하여 AWS Wickr API 호출 로깅 AWS CloudTrail 섹션을 참조하십시오.

를 사용하여 AWS Wickr API 호출 로깅 AWS CloudTrail

AWS Wickr는 Wickr에서 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다. CloudTrail은 Wickr에 대한 모든 API 직접 호출을 이벤트로서 캡처합니다. 캡처되는 호출에는 Wickr에 AWS Management Console 대한의 호출과 Wickr API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하면, Wickr의 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 추적을 구성하지 않은 경우에도 이벤트 기록에서 CloudTrail 콘솔의 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 Wickr에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다. CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

CloudTrail의 Wickr 정보

CloudTrail은 계정을 생성할 AWS 계정 때에서 활성화됩니다. Wickr에서 활동이 발생하면 해당 활동이 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

Wickr에 대한 이벤트를 AWS 계정포함하여에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 트레일을 생성하면 기본적으로 모든 AWS 리전에 트레일이 적용됩니다. 추적은 AWS 파티션의 모든 리전에서 이벤트를 로깅하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 추가적으로, CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 받기 및 여러 계정에서 CloudTrail 로그 파일 받기

모든 Wickr 작업은 Amazon CloudTrail에서 로깅됩니다. 예를 들어, `CreateAdminSession` 직접 호출 및 `ListNetworks` 작업을 통해 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 관한 정보가 포함됩니다. ID 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부입니다.
- 역할 또는 페더레이션 사용자의 임시 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 요청이 다른 AWS 서비스에서 이루어졌는지 여부입니다.

자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.

Wickr 로그 파일 항목 이해하기

트레일이란 지정한 S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 `CreateAdminSession` 작업을 보여주는 CloudTrail 로그 항목이 나타냅니다.

```
{
    "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"
}
```

다음은 CreateNetwork 작업을 설명하는 CloudTrail 로그 항목을 보여 주는 예시입니다.

```
{
    "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"
}
```

다음은 `ListNetworks` 작업을 설명하는 CloudTrail 로그 항목을 보여 주는 예시입니다.

```
{
    "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"
}
```

다음은 UpdateNetworkdetails 작업을 설명하는 CloudTrail 로그 항목을 보여 주는 예시입니다.

```
{
    "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"
}
```

다음은 TagResource 작업을 설명하는 CloudTrail 로그 항목을 보여 주는 예시입니다.

```
{
    "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"
}
```

다음은 ListTagsForResource 작업을 보여주는 CloudTrail 로그 항목이 나타낸 예시입니다.

```
{
    "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"
}
```

AWS Wickr의 분석 대시보드

분석 대시보드를 사용하여 조직이 AWS Wickr를 어떻게 활용하고 있는지 확인할 수 있습니다. 다음 절차에서는 AWS Wickr 콘솔을 사용하여 분석 대시보드에 액세스하는 방법을 설명합니다.

분석 대시보드에 액세스하려면

1. https://console.aws.amazon.com/wickr/ AWS Management Console for Wickr를 엽니다.
2. 네트워크 페이지에서 네트워크 이름을 선택하여 해당 네트워크로 이동합니다.
3. 탐색 창에서 분석을 선택합니다.

   분석 페이지에는 네트워크에 대한 지표가 다른 탭에 표시됩니다.

분석 페이지에서 각 탭의 오른쪽 상단에 기간 필터가 있습니다. 이 필터는 전체 페이지에 적용됩니다. 또한 각 탭의 오른쪽 상단 모서리에서 사용 가능한 내보내기 옵션을 선택하여 선택한 시간 범위의 데이터 포인트를 내보낼 수 있습니다.

> **Note**
>
> 선택한 시간은 UTC(협정 세계시)입니다.

다음 탭을 사용할 수 있습니다.

- 개요가 표시됩니다.
  - 등록됨 - 선택한 시간 동안 네트워크의 활성 및 일시 중지된 사용자를 포함하여 등록된 총 사용자 수입니다. 보류 중이거나 초대된 사용자는 포함되지 않습니다.
  - 보류 중 - 선택한 시간 동안 네트워크의 보류 중인 총 사용자 수입니다.
  - 사용자 등록 - 그래프에는 선택한 시간 범위에 등록된 총 사용자 수가 표시됩니다.
  - 디바이스 - 앱이 활성화된 디바이스 수입니다.

  - 클라이언트 버전 - 클라이언트 버전별로 분류된 활성 디바이스 수입니다.

- 멤버는 다음을 표시합니다.
  - 상태 - 선택한 기간 내에 네트워크의 활성 사용자입니다.
  - 활성 사용자 -
    - 그래프에는 시간 경과에 따른 활성 사용자 수가 표시되며 일별, 주별 또는 월별(위에서 선택한 시간 범위 내)로 집계할 수 있습니다.
    - 활성 사용자 수는 플랫폼, 클라이언트 버전 또는 보안 그룹별로 분류할 수 있습니다. 보안 그룹이 삭제된 경우 총 개수는 삭제됨#으로 표시됩니다.

- 메시지가 표시됩니다.
  - 전송된 메시지 - 선택한 기간 동안 네트워크의 모든 사용자와 봇이 보낸 고유한 메시지 수입니다.
  - 호출 - 네트워크의 모든 사용자가 수행한 고유한 호출 수입니다.
  - 파일 - 네트워크의 사용자가 보낸 파일 수입니다(음성 메모 포함).
  - 디바이스 - 파이형 차트에는 운영 체제별로 분류된 활성 디바이스 수가 표시됩니다.
  - 클라이언트 버전 - 클라이언트 버전별로 분류된 활성 디바이스 수입니다.

문서 이력

다음 표에서는 Wickr에 대한 문서 릴리스를 소개합니다.

변경 사항	설명	날짜
이제 파일 미리 보기를 사용할 수 있습니다.	Wickr 관리자는 이제 파일 다운로드를 활성화하거나 비활성화할 수 있습니다. 자세한 내용은 AWS Wickr용 파일 미리 보기를 참조하세요.	2025년 5월 29일
이제 새로 재설계된 Wickr 관리자 콘솔을 사용할 수 있습니다.	Wickr는 더 나은 탐색과 관리자의 접근성을 위해 Wickr 관리자 콘솔을 개선했습니다.	2025년 3월 13일
이제 아시아 태평양(말레이시아)에서 Wickr를 사용할 수 있습니다. AWS 리전	이제 아시아 태평양(말레이시아)에서 Wickr를 사용할 수 있습니다 AWS 리전. 자세한 내용은 리전별 가용성을 참조하세요.	2024년 11월 20일
이제 네트워크 삭제를 사용할 수 있습니다.	Wickr 관리자는 이제 AWS Wickr 네트워크를 삭제할 수 있습니다. 자세한 내용은 AWS Wickr에서 네트워크 삭제를 참조하세요.	2024년 10월 4일
이제 Microsoft Entra(Azure AD) SSO를 사용하여 AWS Wickr를 구성할 수 있습니다.	AWS Wickr는 Microsoft Entra(Azure AD)를 자격 증명 공급자로 사용하도록 구성할 수 있습니다. 자세한 내용은 Microsoft Entra(Azure AD) Single Sign-On을 사용하여 AWS Wickr 구성을 참조하세요.	2024년 9월 18일

이제 유럽(취리히)에서 Wickr를 사용할 수 있습니다. AWS 리전	이제 유럽(취리히)에서 Wickr를 사용할 수 있습니다 AWS 리전. 자세한 내용은 리전별 가용성을 참조하세요.	2024년 8월 12일
이제 교차 경계 분류 및 페더레이션을 사용할 수 있습니다.	교차 경계 분류 기능을 사용하면 GovCloud 사용자의 대화에 대한 사용자 인터페이스 변경이 가능합니다. 자세한 내용은 GovCloud 교차 경계 분류 및 페더레이션을 참조하세요.	2024년 6월 25일
이제 읽기 수신 기능을 사용할 수 있습니다.	이제 Wickr 관리자는 관리자 콘솔에서 수신 읽기 기능을 활성화하거나 비활성화할 수 있습니다. 자세한 내용은 읽기 수신을 참조하세요.	2024년 4월 23일
Global Federation은 이제 제한된 페더레이션을 지원하며 관리자는 관리자 콘솔에서 사용 분석을 볼 수 있습니다.	Global Federation은 이제 제한된 페더레이션을 지원합니다. 이는 다른의 Wickr 네트워크에서 작동합니다 AWS 리전. 자세한 내용은 보안 그룹을 참조하십시오. 또한 관리자는 이제 관리자 콘솔의 분석 대시보드에서 사용 분석을 볼 수 있습니다. 자세한 내용은 분석 대시보드를 참조하세요.	2024년 3월 28일

이제 AWS Wickr Premium 플랜의 3개월 무료 평가판을 사용할 수 있습니다.	Wickr 관리자는 이제 최대 30명의 사용자를 위한 3개월 무료 평가판 Premium 플랜을 선택할 수 있습니다. 무료 평가판 기간 동안 무제한 관리자 제어 및 데이터 보존을 포함하여 모든 Standard 및 Premium 플랜 기능을 사용할 수 있습니다. 프리미엄 무료 평가판에서는 게스트 사용자 기능을 사용할 수 없습니다. 자세한 내용은 계획 관리를 참조하세요.	2024년 2월 9일
게스트 사용자 기능을 일반적으로 사용할 수 있으며 더 많은 관리자 제어가 추가되었습니다.	이제 Wickr 관리자는 게스트 사용자 목록, 사용자 대량 삭제 또는 일시 중지 기능, Wickr 네트워크에서 게스트 사용자의 통신을 차단하는 옵션 등 다양한 새 기능에 액세스할 수 있습니다. 자세한 내용은 게스트 사용자를 참조하십시오.	2023년 11월 8일
이제 유럽(프랑크푸르트)에서 Wickr를 사용할 수 있습니다. AWS 리전	이제 유럽(프랑크푸르트)에서 Wickr를 사용할 수 있습니다 AWS 리전. 자세한 내용은 리전별 가용성을 참조하세요.	2023년 10월 26일
Wickr 네트워크는 이제 AWS 리전	이제 Wickr 네트워크를 AWS 리전에 걸쳐서 페더레이션할 수 있습니다. 자세한 내용은 보안 그룹을 참조하십시오.	2023년 9월 29일
이제 유럽(런던)에서 Wickr를 사용할 수 있습니다. AWS 리전	이제 유럽(런던)에서 Wickr를 사용할 수 있습니다 AWS 리전. 자세한 내용은 리전별 가용성을 참조하세요.	2023년 8월 23일

이제 캐나다(중부)에서 Wickr를 사용할 수 있습니다. AWS 리전	이제 캐나다(중부)에서 Wickr를 사용할 수 있습니다 AWS 리전. 자세한 내용은 리전별 가용성을 참조하세요.	2023년 7월 3일
게스트 사용자 기능을 이제 미리 볼 수 있습니다.	게스트 사용자는 Wickr 클라이언트에 로그인하여 Wickr 네트워크 사용자와 협업할 수 있습니다. 자세한 내용은 게스트 사용자(미리보기) 섹션을 참조하십시오.	2023년 5월 31일
이제 AWS Wickr가와 통합되어 AWS CloudTrail Wickr AWS GovCloud(미국 서부)에서 WickrGov로 사용할 수 있습니다.	이제 AWS Wickr가와 통합되었습니다 AWS CloudTrail. 자세한 내용은 AWS CloudTrail을 사용하여 AWS Wickr API 직접 호출 로깅을 참조하십시오. 또한 이제 Wickr는 AWS GovCloud(미국 서부)에서 WickRGov로 사용할 수 있습니다. 자세한 내용을 알아보려면 AWS GovCloud (US) 사용 설명서의 AWS WickrGov를 참조하십시오.	2023년 3월 30일
태깅 및 다중 네트워크 생성	이제 AWS Wickr에서 태깅이 지원됩니다. 자세한 내용은 네트워크 태그를 참조하세요. 여러 네트워크를 이제 Wickr에서 만들 수 있습니다. 자세한 내용은 네트워크 생성을 참조하십시오.	2023년 3월 7일
최초 릴리스	Wickr 관리 설명서의 최초 릴리스	2022년 11월 28일

릴리스 노트

Wickr의 진행 중인 업데이트 및 개선 사항을 추적할 수 있도록 최근 변경 사항을 설명하는 릴리스 공지를 게시합니다.

2025년 8월

- 사용자 온보딩 환경을 개선하기 위해 AWS Wickr 및 AWS WickrGov용 이메일 템플릿이 업데이트되었습니다. 발신자 이메일 주소가에서 `donotreply@wickr.email`로 변경되었습니다`no-reply@amazonaws.com`.

2025년 5월

- 이제 파일 미리 보기를 사용할 수 있습니다. 관리자가 보안 그룹의 관리자 콘솔에서 파일 다운로드를 비활성화하면 사용자는 메시징 및 파일 탭에서만 지원되는 파일 목록을 볼 수 있습니다.

2025년 3월

- 이제 재설계된 Wickr 관리자 콘솔을 사용할 수 있습니다.

2024년 10월

- Wickr는 이제 네트워크 삭제를 지원합니다. 자세한 내용은 AWS Wickr에서 네트워크 삭제를 참조하세요.

2024년 9월

- 이제 관리자는 Microsoft Entra(Azure AD) Single Sign-On으로 AWS Wickr를 구성할 수 있습니다. 자세한 내용은 Microsoft Entra(Azure AD) Single Sign-On을 사용하여 AWS Wickr 구성을 참조하세요.

2024년 8월

- 개선 사항

- 이제 유럽(취리히)에서 Wickr를 사용할 수 있습니다 AWS 리전.

2024년 6월

- 이제 GovCloud 사용자가 경계 간 분류 및 페더레이션을 사용할 수 있습니다. 자세한 내용은 GovCloud 교차 경계 분류 및 페더레이션을 참조하세요.

2024년 4월

- Wickr는 이제 읽기 수신을 지원합니다. 자세한 내용은 읽기 수신을 참조하세요.

2024년 3월

- 글로벌 페더레이션은 이제 제한된 페더레이션을 지원하며, 여기서 글로벌 페더레이션은 제한된 페더레이션에 추가된 선택한 네트워크에 대해서만 활성화할 수 있습니다. 이는 다른의 Wickr 네트워크에서 작동합니다 AWS 리전. 자세한 내용은 보안 그룹을 참조하십시오.
- 이제 관리자는 관리자 콘솔의 분석 대시보드에서 사용 분석을 볼 수 있습니다. 자세한 내용은 분석 대시보드를 참조하세요.

2024년 2월

- AWS Wickr는 이제 최대 30명의 사용자에게 Premium 플랜의 3개월 무료 평가판을 제공합니다. 변경 사항 및 제한 사항은 다음과 같습니다.
  - 무제한 관리자 제어 및 데이터 보존과 같은 모든 Standard 및 Premium 플랜 기능을 이제 Premium 무료 평가판에서 사용할 수 있습니다. 프리미엄 무료 평가판에서는 게스트 사용자 기능을 사용할 수 없습니다.
  - 이전 무료 평가판은 더 이상 사용할 수 없습니다. Premium 무료 평가판을 아직 사용하지 않은 경우 기존 무료 평가판 또는 Standard 플랜을 Premium 무료 평가판으로 업그레이드할 수 있습니다. 자세한 내용은 계획 관리를 참조하세요.

2023년 11월

- 이제 게스트 사용자 기능을 정식으로 사용할 수 있습니다. 변경 및 추가 사항은 다음을 포함합니다.

  - 다른 Wickr 사용자의 악용 사례를 신고할 수 있습니다.
  - 관리자는 네트워크가 상호작용한 게스트 사용자 목록과 월별 사용량을 볼 수 있습니다.
  - 관리자는 게스트 사용자가 네트워크와 통신하지 못하도록 차단할 수 있습니다.
  - 게스트 사용자를 위한 추가 기능 요금 책정.

- 관리자 제어 개선 사항
  - 사용자 일괄 삭제/일시 중지 기능
  - 토큰 새로 고침의 유예 기간을 구성하기 위한 추가 SSO 설정.

2023년 10월

- 개선 사항
  - 이제 유럽(프랑크푸르트) AWS 리전에서 Wickr를 사용할 수 있습니다.

2023년 9월

- 개선 사항
  - 이제 Wickr 네트워크를 AWS 리전에 걸쳐서 페더레이션할 수 있습니다. 자세한 내용은 보안 그룹을 참조하십시오.

2023년 8월

- 개선 사항
  - 이제 유럽(런던) AWS 리전에서 Wickr를 사용할 수 있습니다.

2023년 7월

- 개선 사항
  - 이제 캐나다(중부) AWS 리전에서 Wickr를 사용할 수 있습니다.

2023년 5월

- 개선 사항
  - 게스트 사용자에 대한 지원이 추가되었습니다. 자세한 내용은 AWS Wickr 네트워크의 게스트 사용자 섹션을 참조하십시오.

2023년 3월

- 이제 Wickr가와 통합되었습니다 AWS CloudTrail. 자세한 내용은 를 사용하여 AWS Wickr API 호출 로깅 AWS CloudTrail 단원을 참조하십시오.
- 이제 Wickr를 AWS GovCloud(미국 서부)에서 WickrGov로 사용할 수 있습니다. 자세한 내용을 알아보려면 AWS GovCloud (US) 사용 설명서의 AWS WickrGov를 참조하십시오.
- 이제 Wickr에서 태그 지정을 지원합니다. 자세한 내용은 AWS Wickr용 네트워크 태그 단원을 참조하십시오. 여러 네트워크를 이제 Wickr에서 만들 수 있습니다. 자세한 내용은 1단계: 네트워크 생성 섹션을 참조하십시오.

2023년 2월

- Wickr는 이제 Android Tactical Assault Kit(ATAK)를 지원합니다. 자세한 내용은 Wickr 네트워크 대시보드에서 ATAK 활성화 섹션을 참조하십시오.

2023년 1월

- 이제 무료 평가판 및 표준을 포함한 모든 요금제에서 Single Sign-On(SSO)을 구성할 수 있습니다.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.