관리 설명서

AWS Wickr

AWS Wickr: 관리 설명서

Table of Contents

AWS Wickr란 무엇입니까?

AWS Wickr는 조직 및 정부 기관이 그룹 메시징, 음성 및 화상 통화, 파일 공유, 화면 공유 등을 통해 one-to-one 안전하게 통신할 수 있도록 지원하는 end-to-end 암호화된 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 SSO(Single Sign-On) 등과 같은 추가 서비스와 통합됩니다. 를 통해 Wickr 네트워크를 빠르게 생성 및 관리하고 Wickr 봇을 사용하여 워크플로를 안전하게 자동화할 수 있습니다. AWS Management Console시작하려면 AWS Wickr에 대한 설정 섹션을 참조하세요.

주제

- Wickr의 기능
- Wickr에 액세싱
- 요금
- Wickr 최종 사용자 설명서

Wickr의 기능

향상된 보안 및 개인정보 보호

Wickr는 모든 기능에 256비트 고급 암호화 표준 (AES) 암호화를 사용합니다. end-to-end 통신은 사용자 디바이스에서 로컬로 암호화되며 발신자와 수신자를 제외한 다른 사람이 전송하는 동안에는 해독할 수 없습니다. 모든 메시지, 통화, 파일은 새로운 무작위 키로 암호화되며, 수신자 외에는 누구도 암호를 해독할 수 AWS없습니다. 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 장치 (모바일, 데스크톱) 에 액세스할 수 있으며 연결이 끊긴 환경 및 통신을 포함하여 대역폭이 낮은 환경에서도 기능할 수 있습니다. out-of-band

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 SSO(Single Sign-On) 등과 같은 추가 서비스와 통합됩니다. 고객은 를 통해 Wickr 네트워크를 빠르게 생성 및 관리하고 Wickr Bot을 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 타이머를 제어합니다. burn-on-read
- 글로벌 페더레이션: 네트워크 외부의 Wickr 사용자와 연결

> **Note**
>
> (미국 서부) 의 Wickr 네트워크는 AWS GovCloud (미국 서부) 의 다른 Wickr 네트워크와만 페더레이션할 수 있습니다. AWS GovCloud

Wickr에 액세싱

Wickr는 미국 동부 (버지니아 북부), 캐나다 (중부), 유럽 (런던), 아시아 태평양 (시드니), 유럽 (프랑크푸르트), 유럽 (스톡홀름), 아시아 태평양 (싱가포르) 및 아시아 태평양 (도쿄) 에서 사용할 수 있습니다. AWS 리전 Wickr는 (미국 서부) 에서처럼 사용할 수도 있습니다. WickrGov AWS GovCloud AWS 리전

관리자는 https://console.aws.amazon.com/wickr/ 에서 AWS Management Console Wickr용 Wickr에 액세스할 수 있습니다. Wickr 사용을 시작하기 전에 먼저 AWS Wickr에 대한 설정 및 AWS Wickr 사용 시작하기 안내서를 작성해야 합니다.

> **Note**
>
> Wickr 서비스에는 애플리케이션 프로그래밍 인터페이스(API)가 없습니다.

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

요금

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 고객의 경우 AWS Wickr 사용을 시작하기 전에 이 페이지에 나열된 설정 사전 조건을 완료합니다. 이러한 설정 절차에는(AWS Identity and Access ManagementIAM) 서비스를 사용합니다. IAM에 대한 전체 내용은 IAM 사용 설명서를 참조하십시오.

주제

- 에 가입AWS
- IAM 사용자를 생성합니다.
- 다음에 있는 것

에 가입AWS

AWS 계정이 없는 경우 다음 절차에 따라 계정을 생성하세요.

AWS 계정에 가입하려면

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

   가입 절차 중 전화를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   AWS 계정에 가입하면 AWS 계정 루트 사용자이(가) 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스및 리소스에 액세스하는 권한이 있습니다. 보안 모범 사례는 관리 사용자에게 관리자 액세스 권한을 할당하고, 루트 사용자만 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 따르세요.	AWS Command Line Interface 사용 설명서의 AWS IAM Identity Center 사용할 AWS CLI 구성을 통해 프로그래밍 방식의 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 설명은 AWS 관리형 정책: AWSWickrFullAccess 섹션을 참조하세요.

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

필수 조건

시작에 앞서 아직 완료하지 않았다면 반드시 사전 조건을 완료하십시오.

- Amazon Web Services(AWS) 가입 자세한 설명은 AWS Wickr에 대한 설정 섹션을 참조하세요.
- Wickr를 관리하는 데 필요한 권한이 있는지 확인합니다. 자세한 설명은 AWS 관리형 정책: AWSWickrFullAccess 섹션을 참조하세요.
- Wickr에 적합한 포트 및 도메인 목록을 허용했는지 확인하세요. 자세한 설명은 허용할 포트 및 도메인 목록 섹션을 참조하세요.

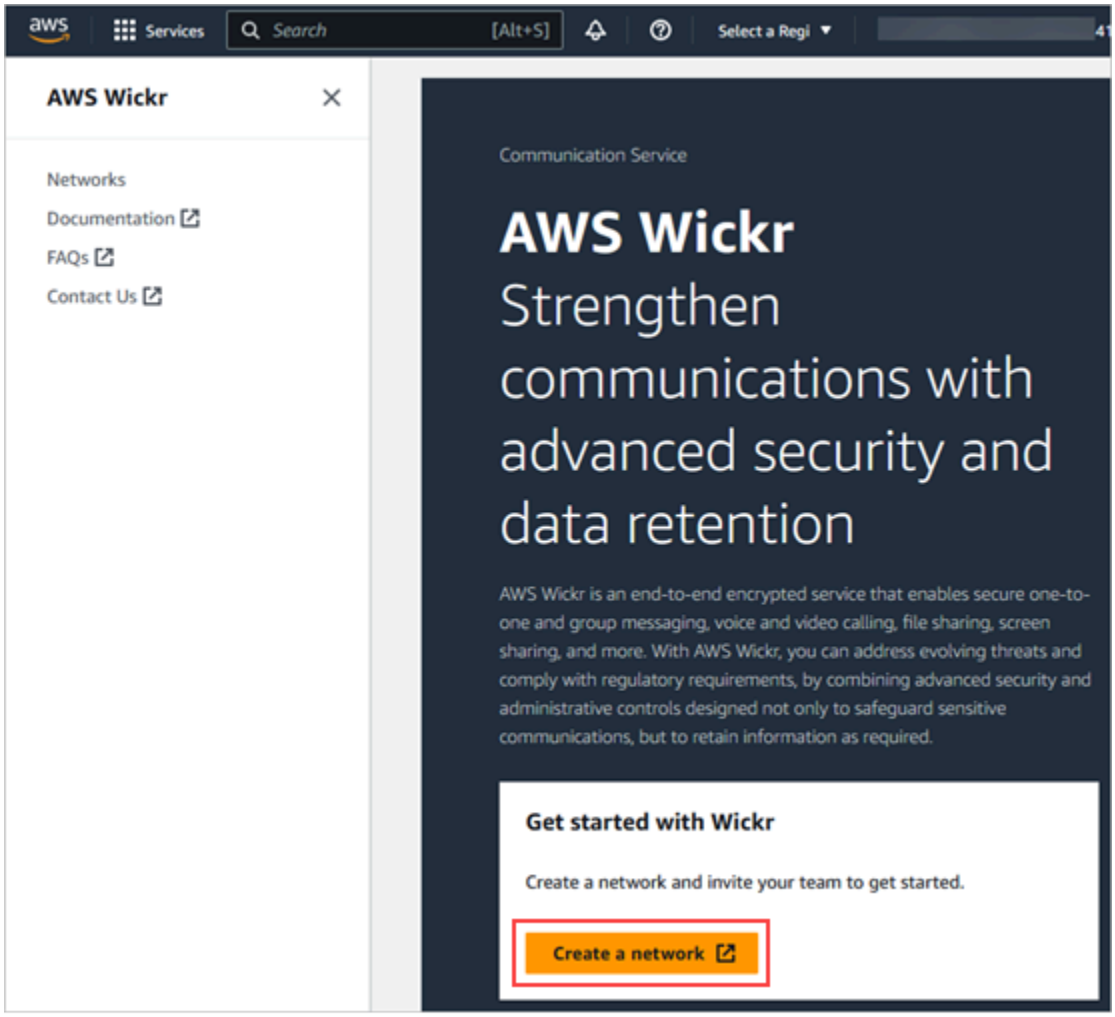
1단계: 네트워크 생성

계정을 위해 Wickr 네트워크를 생성하려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ 에서 AWS Management Console 위커 앱을 여세요.

> **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 선택하세요. 다음 Wickr 네트워크 플랜 중 하나를 선택할 수 있습니다.

   - 표준 — 관리 제어 및 유연성이 필요한 중소기업 및 대기업 팀에 적합합니다.
   - 프리미엄 또는 프리미엄 무료 평가판 — 최고의 기능 제한, 세분화된 관리 제어 및 데이터 보존이 필요한 비즈니스에 적합합니다.

   관리자는 최대 30명의 사용자가 사용할 수 있고 3개월 동안 사용할 수 있는 프리미엄 무료 평가판 옵션을 선택할 수 있습니다. 이 오퍼는 레거시가 없는 새로운 평가판 및 표준 요금제에서 사용할 수 있습니다. 관리자는 프리미엄 무료 평가판 기간 동안 Premium 또는 Standard 요금제로 업그레이드하거나 다운그레이드할 수 있습니다.

사용 가능한 Wickr 계획 및 요금 정책에 대한 자세한 내용은 Wickr 요금 책정 페이지를 참조하세요.

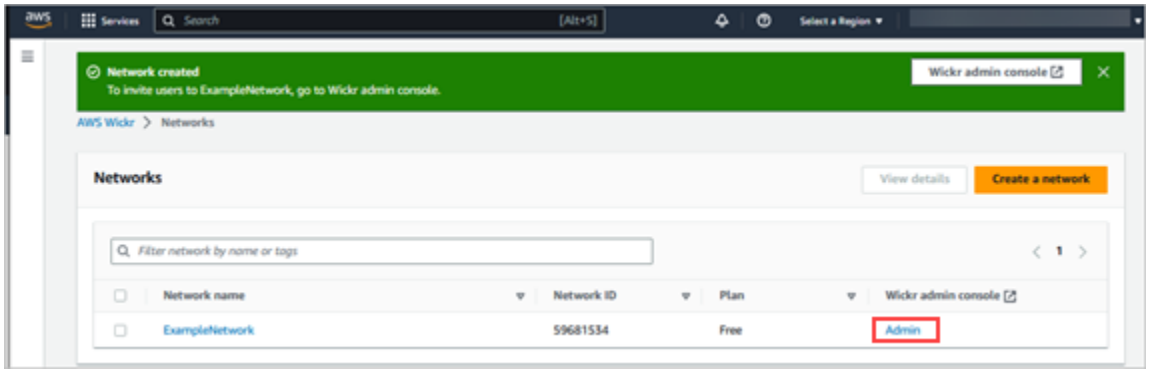
5. (선택 사항) 네트워크에 태그를 추가하려면 새 태그 추가를 선택합니다. 태그는 키-값 쌍으로 이루어져 있습니다. 태그를 사용하여 리소스를 검색 및 필터링하거나 사용자의 AWS 비용을 추적할 수 있습니다. 자세한 내용은 네트워크 태그 관리를 참조하세요.
6. 네트워크 생성을 선택합니다.

   AWS Management Console for Wickr의 네트워크 페이지로 리디렉션되고 페이지에 새 네트워크가 나열됩니다.

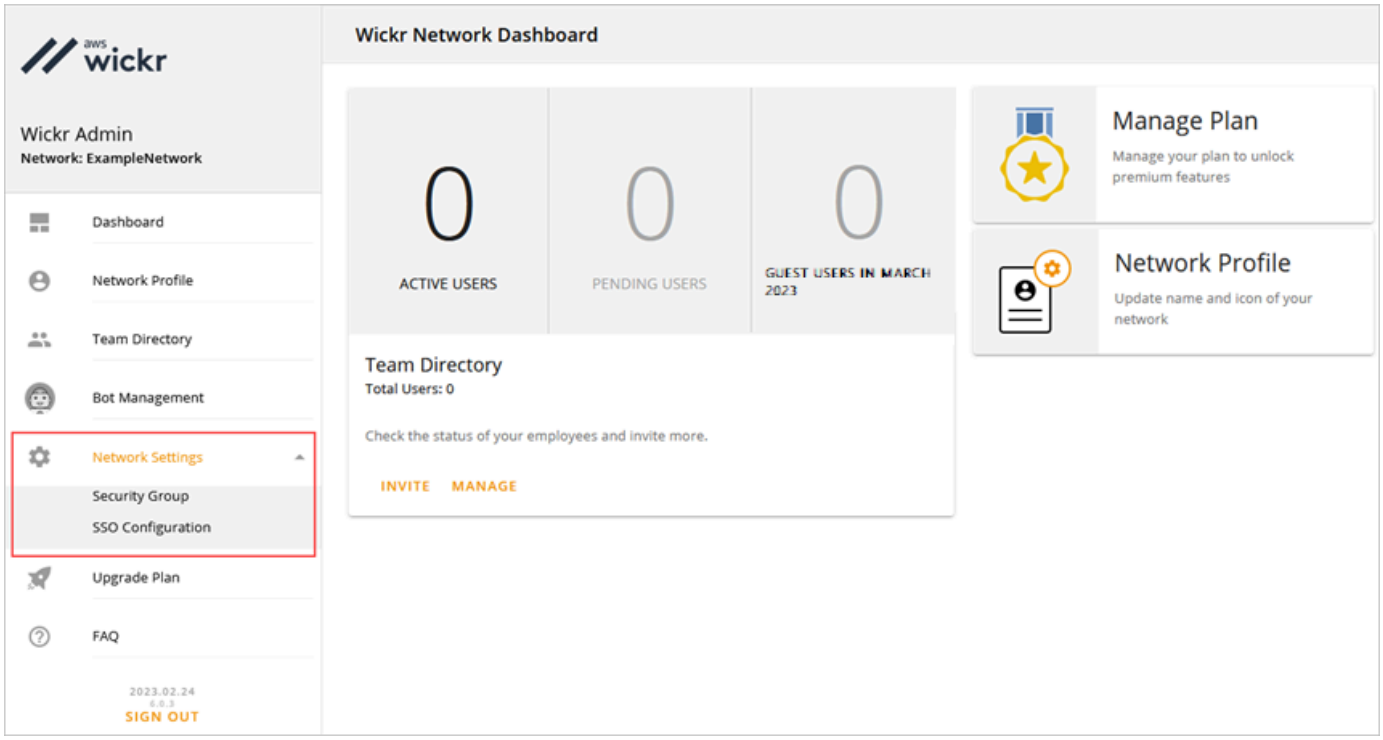
2단계: 사용자의 네트워크 구성

다음 절차를 완료하여 Wickr Admin Console에 액세스하여 사용자 추가, 보안 그룹 추가, SSO 구성, 데이터 보존 구성 및 추가 네트워크 설정을 수행할 수 있습니다.

1. 네트워크 페이지에서 관리자 링크를 선택하여 해당 네트워크의 Wickr 관리 콘솔로 이동합니다.



   선택된 네트워크의 Wickr 관리 콘솔로 리디렉션됩니다.
2. Wickr 관리 콘솔의 탐색 창에서 Network Settings을 선택한 다음 보안 그룹을 선택합니다.



다음과 같은 네트워크 설정 옵션을 사용할 수 있습니다. 이러한 설정을 구성하는 것에 대한 자세한 내용은 AWS Wickr 네트워크 관리 섹션을 참조하세요.

- 보안 그룹 — 비밀번호 복잡성 정책, 메시징 기본 설정, 통화 기능, 보안 기능 및 외부 페더레이션과 같은 보안 그룹 및 해당 설정을 관리합니다. 자세한 설명은 보안 그룹 섹션을 참조하세요.
- SSO 구성 - SSO를 구성하고 Wickr 네트워크의 엔드포인트 주소를 확인합니다. Wickr는 OpenID Connect(OIDC)를 사용하는 SSO 공급자만을 지원합니다. Security Assertion Markup Language(SAML)를 사용하는 공급자는 지원되지 않습니다. 자세한 설명은 Single Sign-On 구성 섹션을 참조하세요.

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 설명은 Single Sign-On 구성 섹션을 참조하세요.
- 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. 게스트 사용자 기능은 현재 미리 보기 중입니다. 자세한 정보는 게스트 사용자섹션을 참조하세요.

사용자를 생성하거나 초대하려면 다음 절차를 완료하세요.

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

SSO

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 설명은 SSO 구성. 섹션을 참조하세요.
- 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.

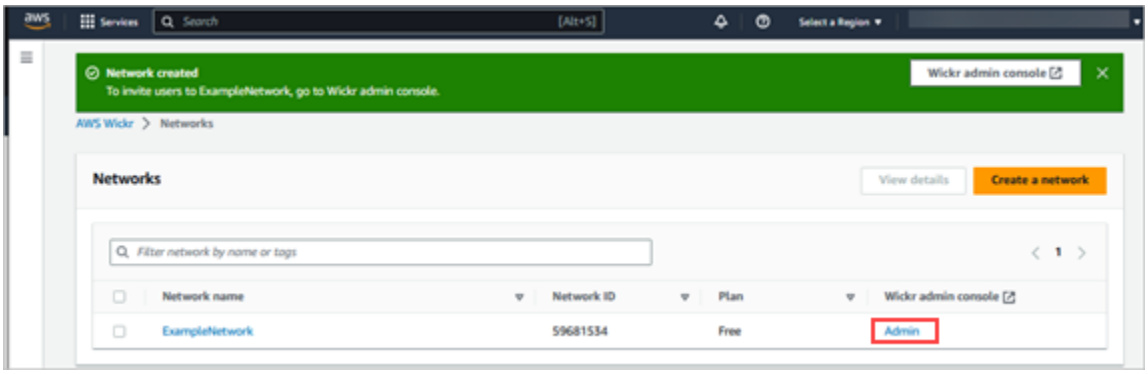
  > **Note**
  >
  > AWS GovCloud (미국 서부) 에서 Wickr 네트워크를 만든 경우 사용자에게 클라이언트를 다운로드하고 설치하도록 안내하십시오. WickrGov 다른 모든 AWS 지역의 경우 사용자에게 표준 Wickr 클라이언트를 다운로드하고 설치하도록 안내하십시오. 에 대한 자세한 내용은 사용 AWS WickrGov 설명서를 참조하십시오 AWS WickrGov.AWS GovCloud (US)

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

Non-SSO

Wickr 사용자를 수동으로 생성하고 초대장을 보내려면:

1. https://console.aws.amazon.com/wickr/ 에서 AWS Management Console 위커용 앱을 여십시오.
2. 네트워크 페이지에서 관리 링크를 선택하여 해당 네트워크의 Wickr 관리 콘솔로 이동합니다.



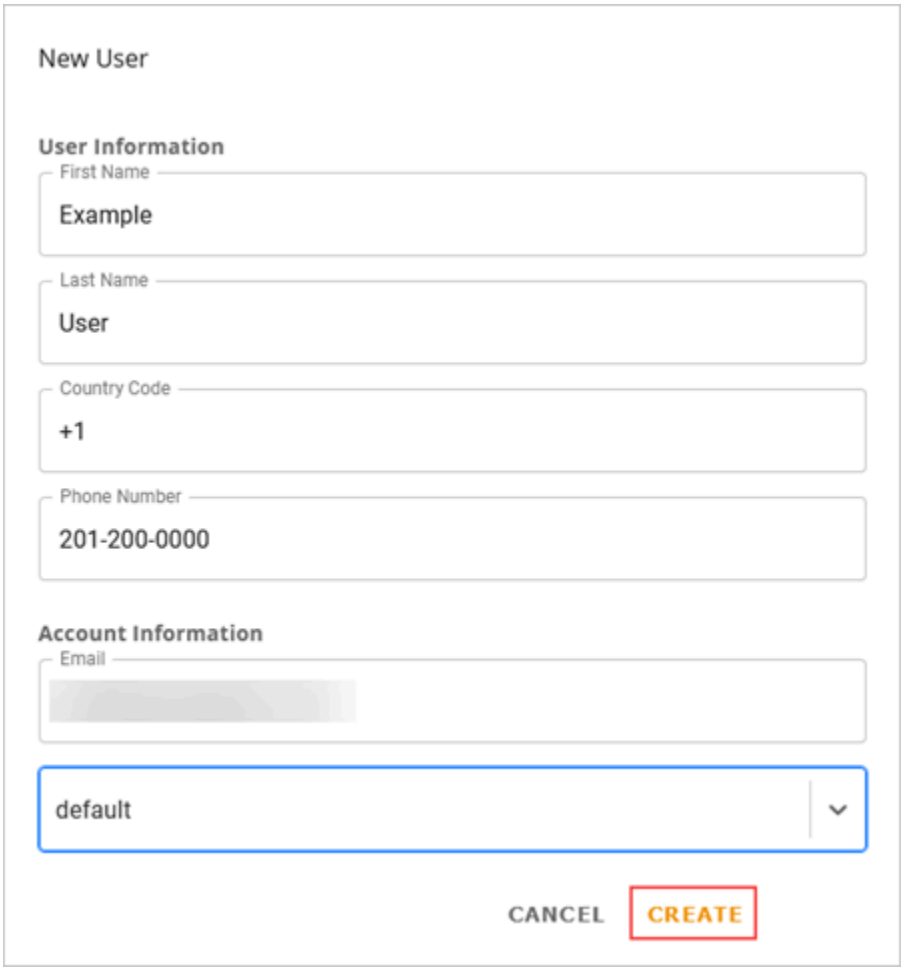
네트워크 페이지.

특정 네트워크의 Wickr 관리 콘솔로 리디렉션됩니다. Wickr 관리 콘솔에서, 사용자 추가, 보안 그룹 추가, SSO 구성, 데이터 보존 및 선택한 특정 네트워크에 대한 추가 설정을 구성할 수 있습니다.

3. Wickr 관리 콘솔의 탐색 창에서, 사용자를 선택한 다음 팀 디렉터리를 선택합니다.

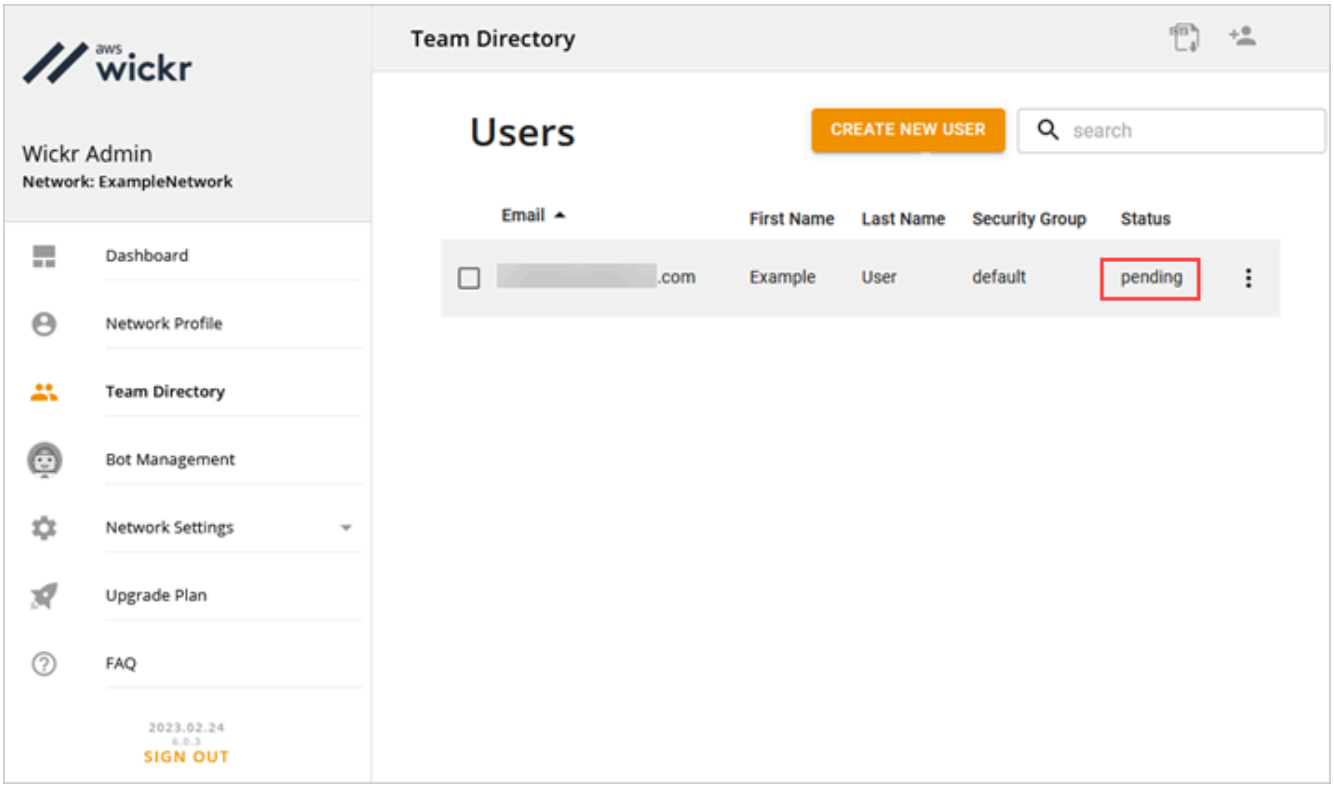
   사용자 페이지에서 새 사용자 생성을 선택하여 개별 사용자를 추가할 수 있습니다. 상단 탐색 창에서 사용자 추가 아이콘을 선택하여 사용자를 일괄로 추가할 수도 있습니다. CSV 다운로드 아이콘을 선택하여 사용자 목록과 함께 편집하고 업로드할 수 있는 CSV 템플릿을 다운로드합니다.

4. 사용자의 이름, 성, 국가 코드, 전화번호 및 이메일 주소를 입력합니다. 이메일 주소는 유일한 필수 필드입니다. 반드시 사용자에게 적합한 보안 그룹을 선택해야 합니다.
5. 생성을 선택하세요.



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 다음 가이드를 참조하세요.

- AWS Wickr 네트워크 관리
- AWS Wickr에서 사용자 관리

Wickr Pro를 AWS Wickr로 이전

> **Note**
>
> 위커 프로는 2024년 3월 27일에 단종될 예정입니다.

이 설명서에서는 Wickr Pro에서 이전하고 AWS Wickr를 시작하는 방법을 안내합니다.

기존 Wickr Pro 네트워크가 있지만 아직 없는 경우 이 가이드의 단계를 따르십시오. AWS 계정 도움이 필요한 어떤 단계에서든 지원팀에 문의하세요.

조직에 이미 AWS 계정이 있는 경우 Wickr Pro에서 AWS Wickr로 마이그레이션 양식을 작성하면 AWS Wickr 지원팀에서 도움을 받을 수 있습니다.

AWS Wickr 네트워크를 a로 관리하려면 AWS 계정 ID가 필요합니다. AWS 서비스계정이란 무엇이며 계정을 AWS 계정 관리하는 방법에 대한 자세한 내용은 AWS 계정 관리 참조 안내서를 참조하십시오.

주제

1단계: AWS 계정 생성

AWS 계정을 만들려면 다음 절차를 완료하세요.

1. 조직에 기존 AWS 계정 ID가 없는 경우 먼저 독립형 AWS 계정 ID를 생성할 수 있습니다. 이를 위해 필요한 몇 가지 주요 사항은 다음과 같습니다.

   - 청구용 신용/직불카드
   - 그룹이 액세스할 수 있는 이메일 주소(권장, 필수는 아님)
   - AWS Support 플랜을 선택합니다. 자세한 내용은 AWS Support 플랜 변경을 참조하세요.

   > **Note**
   >
   > 필요에 대해 자세히 알아보면 언제든지 AWS Support 플랜을 변경할 수 있습니다.

2. IAM을 통한 관리 액세스를 보안 모범 사례로 설정합니다(선택 사항이지만 권장됨). 자세한 내용은 AWS 보안 인증 및 액세스 관리를 참조하십시오. AWS Wickr 관리 액세스에 대한 자세한 지침은 AWS 관리형 정책을 참조하십시오. AWSWickrFullAccess
3. 이전 단계를 완료하면 에 로그인하여 계정 이름으로 12자리 AWS 계정 ID를 찾을 수 있습니다. AWS Management Console

2단계: Wickr 네트워크 ID 검색

Wickr 네트워크 ID를 검색하려면 다음 절차를 완료하세요.

1. 현재 Wickr 관리 콘솔에 로그인하고 마이그레이션하려는 네트워크를 선택한 다음 네트워크 프로필을 선택합니다.
2. 네트워크 프로필 페이지에는 네트워크 ID가 표시되며 8자리 숫자 ID입니다.

3단계: 요청 제출

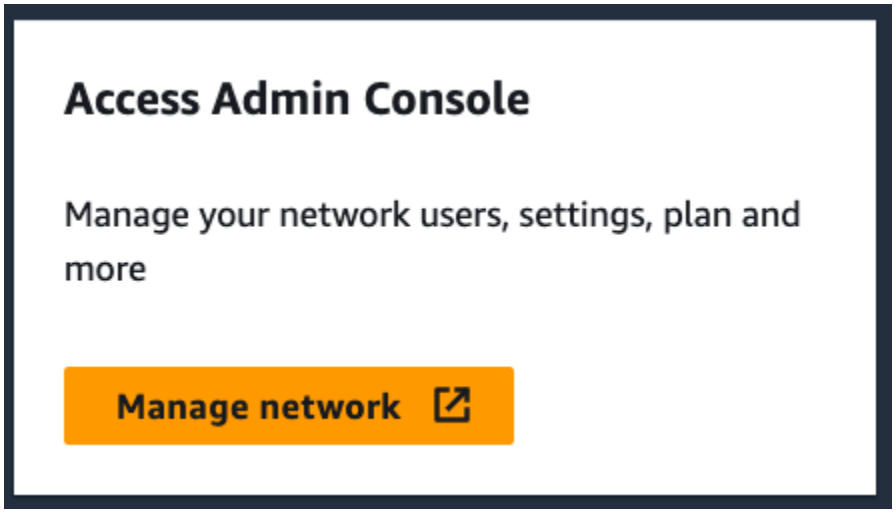
이제 AWS 계정 ID와 Wickr Pro 네트워크 ID를 얻었으므로 Wickr Pro에서 AWS Wickr로 마이그레이션 양식을 작성해야 합니다.

작업이 완료되면 일반적으로 14일 이내에 AWS Wickr 지원 담당자가 연락하여 Wickr 네트워크가 사용자의 AWS 계정에 추가되었는지 확인합니다.

4단계: 콘솔에 로그인 AWS

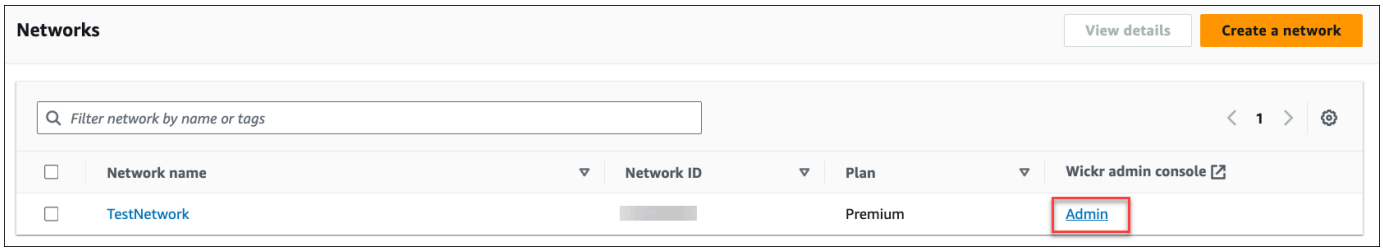
> **Note**
>
> Wickr Pro 네트워크가 사용자 네트워크에 추가되었다는 확인을 받은 후 다음 단계를 따르세요 AWS 계정.

1. 루트 사용자 또는 이전에 AWS Wickr용 2단계에서 생성한 (권장) IAM 사용자로 AWS 콘솔에 로그인할 수 있습니다.
2. AWS Wickr 서비스로 이동하십시오. 서비스 메뉴에서 또는 검색 창에서 AWS Wickr를 검색하여 이 작업을 수행할 수 있습니다.
3. AWS Wickr 페이지에서 네트워크 관리를 선택하여 Wickr 네트워크 목록에 액세스합니다.



네트워크 관리 버튼.

4. 네트워크 페이지의 Wickr 관리 콘솔 열에서 원하는 네트워크 이름 오른쪽에 있는 관리자 링크를 선택합니다.



관리 콘솔 링크.

5. 이제 전송이 완료되었습니다! Wickr 네트워크 대시보드가 보일 것입니다.

이제 네트워크에 대한 청구가 사용자 AWS 계정으로 이전됩니다. 지원팀이 확인 연락을 드릴 때까지 영업일 기준 최대 3일이 소요될 수 있습니다. 확인을 받은 후 콘솔을 통해 청구서를 확인하고 결제할 수 있습니다. AWS

AWS Wickr 네트워크 관리

AWS Management Console Wickr용 네트워크 설정 섹션에서 Wickr 네트워크 이름, 보안 그룹, SSO 구성 및 데이터 보존 설정을 관리할 수 있습니다.

주제

네트워크 프로필

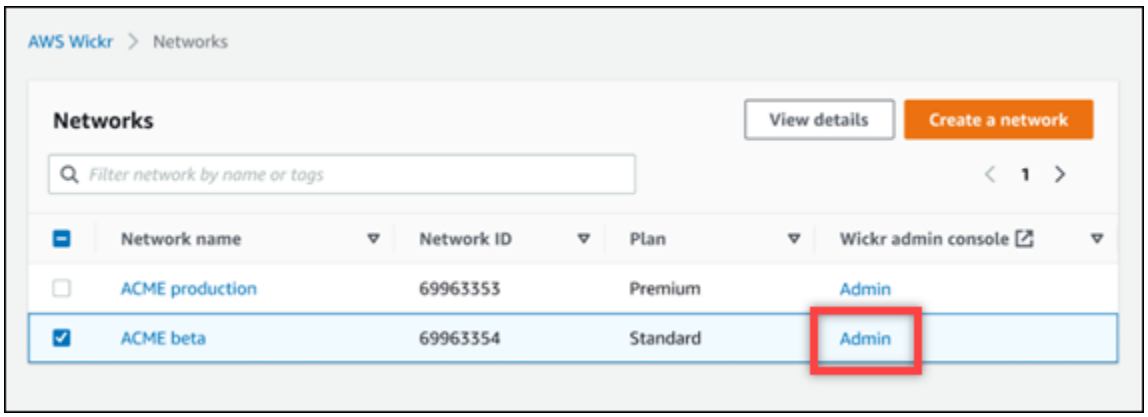
Wickr용 네트워크 프로필 섹션에서 Wickr 네트워크 이름을 편집하고 네트워크 ID를 볼 수 있습니다. AWS Management Console

주제

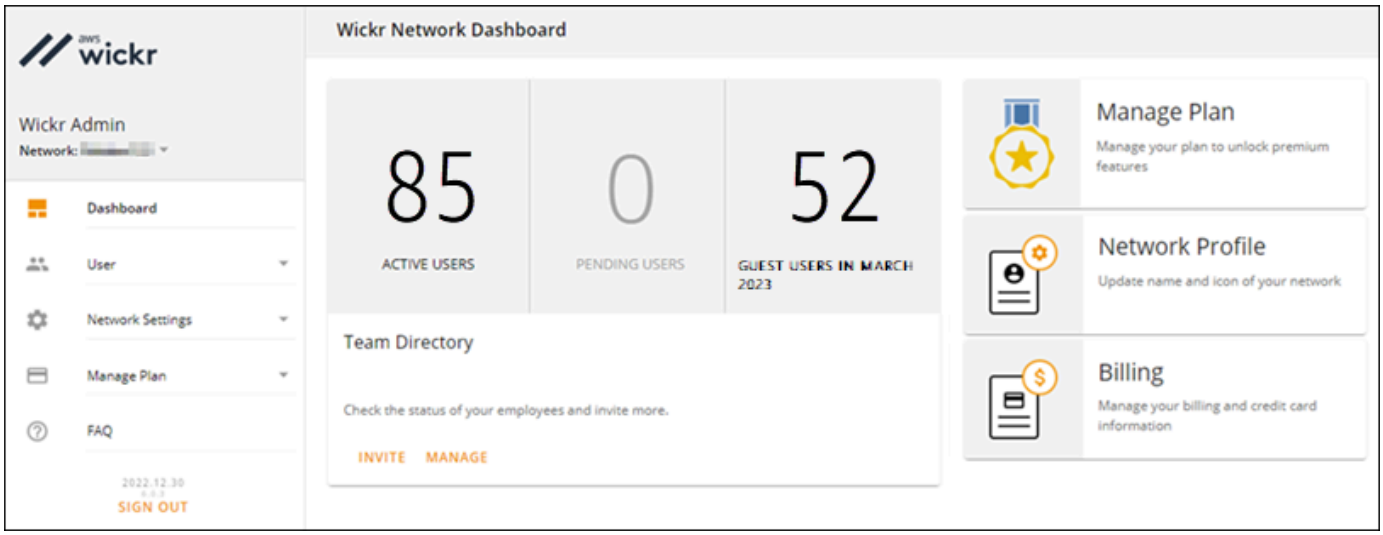
네트워크 프로필 보기

Wickr 네트워크 프로필 및 네트워크 ID를 보려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ 에서 AWS Management Console 위커용 앱을 여십시오.
2. 네트워크 페이지에서 관리 링크를 선택하여 해당 네트워크의 Wickr 관리 콘솔로 이동합니다.



특정 네트워크의 Wickr 관리 콘솔로 리디렉션됩니다.



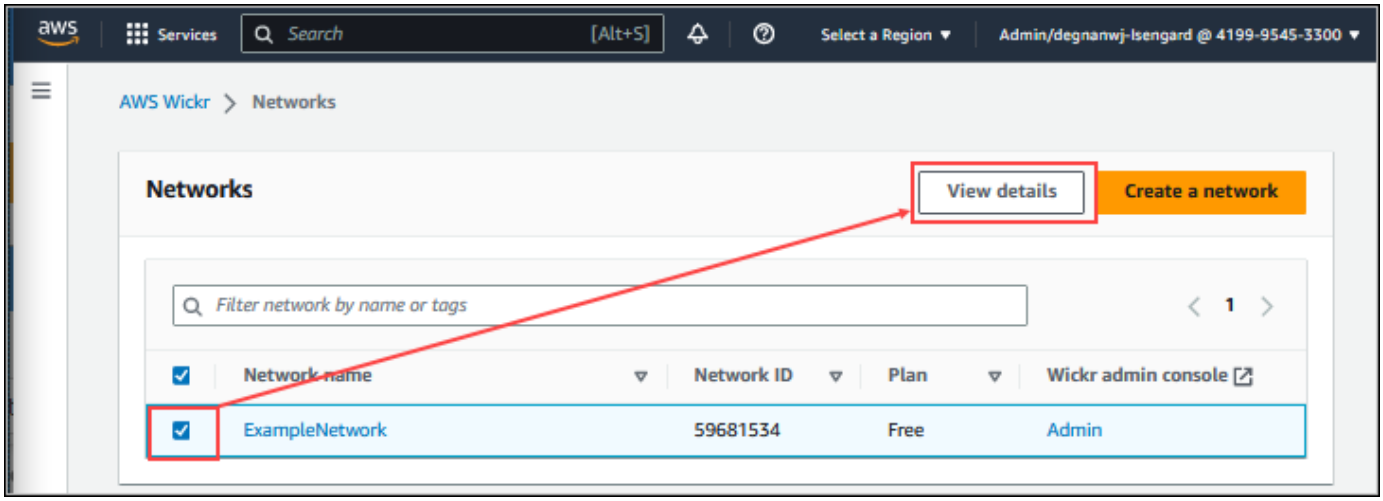
3. Wickr 관리 콘솔의 탐색 창에서 네트워크 설정을 선택한 다음 네트워크 프로필을 선택합니다.

   네트워크 프로필 페이지에는 Wickr 네트워크 이름과 네트워크 ID가 표시됩니다. 네트워크 ID를 사용하여 페더레이션을 구성할 수 있습니다.

네트워크 이름 편집

Wickr 네트워크 이름을 편집하려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ 에서 포 AWS Management Console 위커를 여세요.
2. 네트워크 관리를 선택합니다.
3. 네트워크 페이지에서 편집할 네트워크 이름 옆의 확인란을 선택한 다음 세부 정보 보기를 선택합니다.



4. 네트워크 개요 섹션에서 편집을 선택합니다.
5. 네트워크 이름 텍스트 상자에 네트워크 이름을 입력합니다.
6. 변경 내용 저장을 선택하여 이 네트워크 이름을 저장합니다.

보안 그룹

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

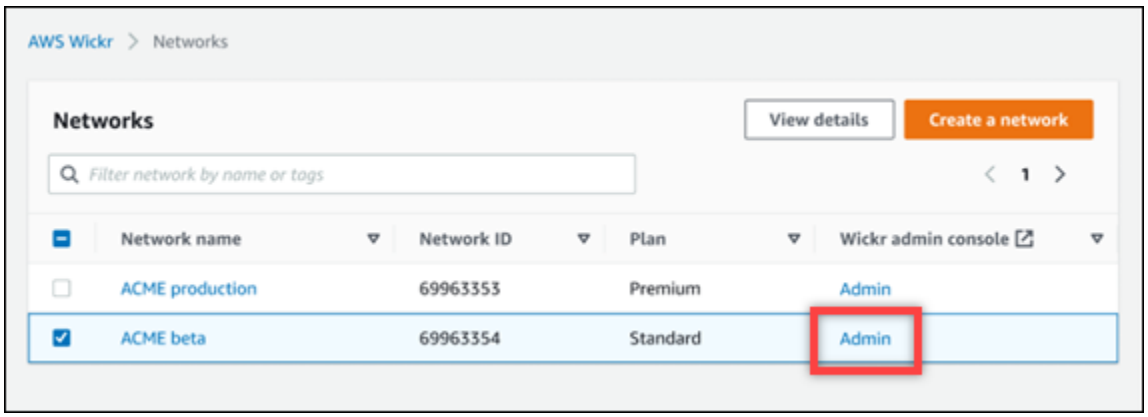
주제

- 보안 그룹 보기
- 보안 그룹 생성
- 보안 그룹 편집
- 보안 그룹 삭제

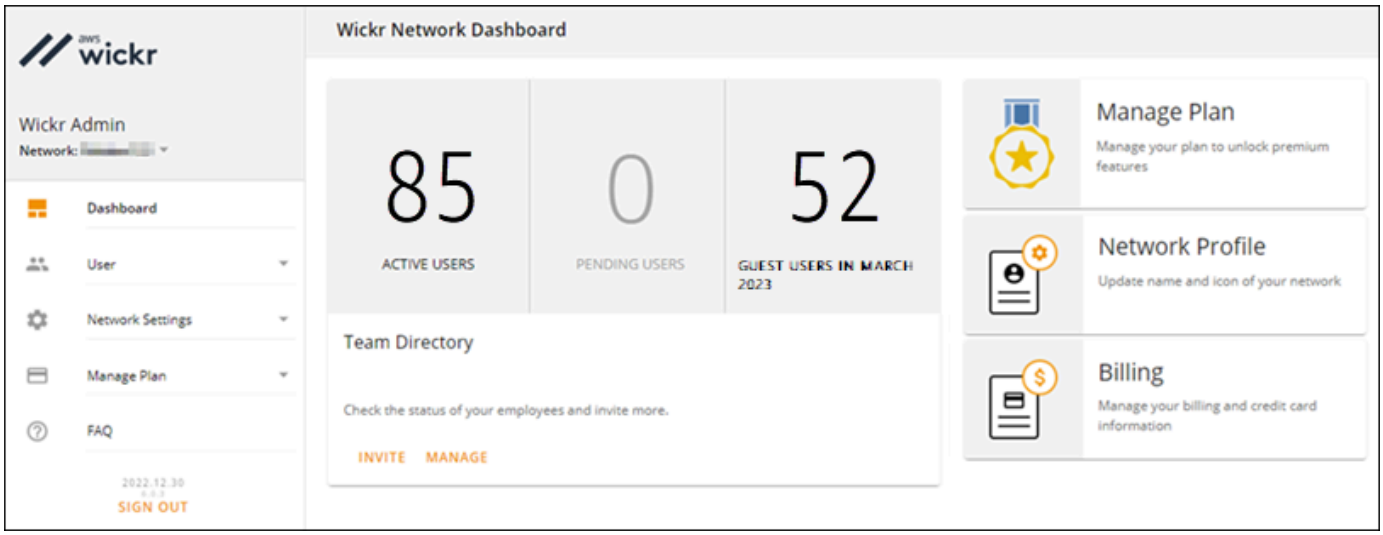
보안 그룹 보기

보안 그룹을 보려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ 에서 AWS Management Console Wickr용 앱을 여십시오.
2. 네트워크 페이지에서 관리 링크를 선택하여 해당 네트워크의 Wickr 관리 콘솔로 이동합니다.



특정 네트워크의 Wickr 관리 콘솔로 리디렉션됩니다.



3. Wickr 관리 콘솔의 탐색 창에서 네트워크 설정을 선택한 다음 보안 그룹을 선택합니다.

   보안 그룹 페이지에는 현재 Wickr 보안 그룹이 표시되며 해당 세부 정보를 보거나 새 그룹을 만들 수 있는 옵션이 제공됩니다.

보안 그룹 생성

보안 그룹을 만들려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ 에서 포 AWS Management Console 위커를 여세요.
2. 네트워크 페이지에서 관리 링크를 선택하여 해당 네트워크의 Wickr 관리 콘솔로 이동합니다.

   특정 네트워크의 Wickr 관리 콘솔로 리디렉션됩니다.
3. Wickr 관리 콘솔의 탐색 창에서 네트워크 설정을 선택한 다음 보안 그룹을 선택합니다.

4. 새 보안 그룹을 생성하려면 새 그룹을 선택합니다.

   기본 이름을 사용하는 새 보안 그룹이 보안 그룹 목록에 자동으로 추가됩니다.

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

보안 그룹 편집

보안 그룹을 편집하려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ 에서 포 AWS Management Console 위커를 여세요.
2. 네트워크 페이지에서 관리 링크를 선택하여 해당 네트워크의 Wickr 관리 콘솔로 이동합니다.

   특정 네트워크의 Wickr 관리 콘솔로 리디렉션됩니다.
3. Wickr 관리 콘솔의 탐색 창에서 네트워크 설정을 선택한 다음 보안 그룹을 선택합니다.
4. 편집하려는 보안 그룹 이름 옆에 있는 세부 정보를 선택합니다.

   보안 그룹 세부 정보 페이지에는 보안 그룹에 대한 설정이 여러 탭에 표시됩니다.
5. 다음 탭과 해당 설정을 사용할 수 있습니다.

   - 보안 그룹 이름 — 그룹 이름 옆에 있는 연필 아이콘을 선택하여 이름을 편집합니다.
   - 일반 - 그룹의 기본 구성을 편집합니다.
   - 메시징 - 그룹 구성원의 메시징 기능을 관리합니다.
   - 통화 — 그룹 구성원의 통화 기능을 관리합니다.
   - 보안 - 그룹에 대한 추가 보안 기능을 구성합니다.
   - 페더레이션 - 네트워크 간 통신 기능. 이는 보안 그룹 수준의 네트워크에 대한 관리 콘솔에서 구성할 수 있습니다. AWS Wickr에는 로컬 및 글로벌이라는 2개 유형의 페더레이션이 있습니다.
     - 로컬 페더레이션 — 동일한 지역 내 다른 네트워크의 AWS 사용자와 페더레이션할 수 있는 기능. 예를 들어, 캐나다에 로컬 페더레이션이 활성화된 두 개의 네트워크가 있는 경우 두 네트워크는 서로 통신할 수 있습니다.
     - 글로벌 페더레이션 — 기업 사용자 또는 다른 지역에 속한 다른 네트워크의 AWS 사용자와 페더레이션할 수 있는 기능입니다. 예를 들어 캐나다 지역의 네트워크에 사용자가 있고 런던 지역의 네트워크에 사용자가 있는데 두 네트워크 모두에 글로벌 페더레이션이 켜져 있는 경우 두 네트워크 모두 서로 통신할 수 있습니다.
     - 제한적 페더레이션 — 다른 지역에 속한 특정 네트워크 (엔터프라이즈 또는 AWS) 와 페더레이션할 수 있는 기능입니다. 관리자는 사용자가 페더레이션할 수 있는 특정 네트워크를 허용

목록에 추가할 수 있습니다. 제한 이후 사용자는 허용 목록에 있는 네트워크의 사용자와만 통신할 수 있습니다. 제한된 페더레이션을 사용하려면 두 네트워크 모두 페더레이션 탭의 보안 그룹 설정에서 서로를 허용 목록에 추가해야 합니다.

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

보안 그룹 삭제

보안 그룹을 삭제하려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ 에서 AWS Management Console Wickr용 앱을 여십시오.
2. 네트워크 페이지에서 관리 링크를 선택하여 해당 네트워크의 Wickr 관리 콘솔로 이동합니다.

   특정 네트워크의 Wickr 관리 콘솔로 리디렉션됩니다.
3. Wickr 관리 콘솔의 탐색 창에서 네트워크 설정을 선택한 다음 보안 그룹을 선택합니다.
4. 삭제할 보안 그룹 이름 옆에 있는 세로 줄임표 아이콘을 선택합니다.
5. 제거를 선택하여 보안 그룹을 삭제합니다.

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

Single Sign-On 구성

AWS Management Console for Wickr의 SSO 구성 섹션에서 싱글 사인온 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.

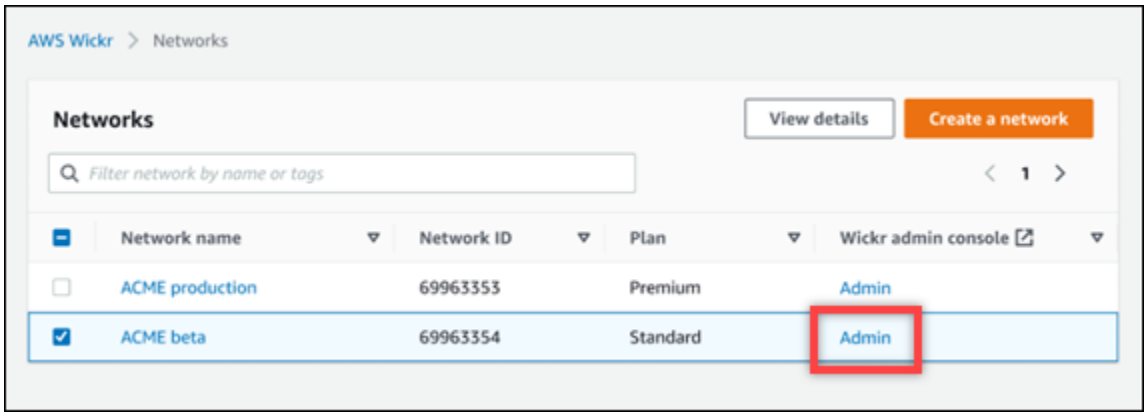
주제

- SSO 세부 정보 보기
- SSO 구성.
- 토큰 새로고침 유예 기간

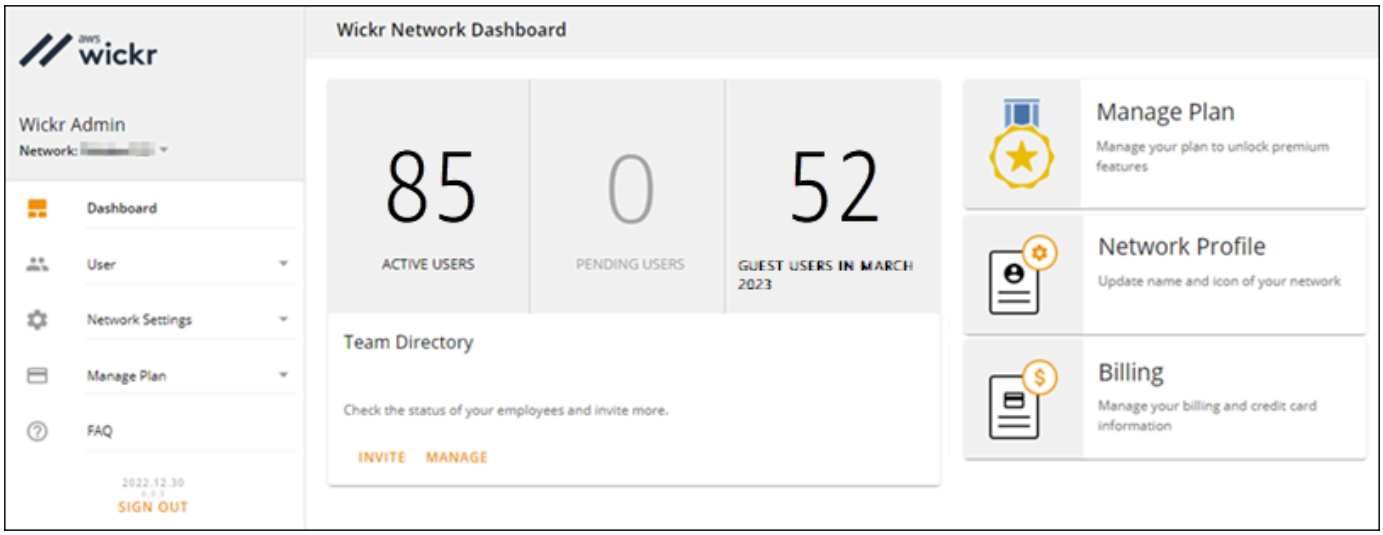
SSO 세부 정보 보기

Wickr 네트워크의 현재 SSO 구성(있는 경우)을 보려면 다음 절차를 완료하세요. Wickr 네트워크의 네트워크 엔드포인트를 볼 수도 있습니다.

1. AWS Management Console https://console.aws.amazon.com/wickr/ 에서 위커용 앱을 여십시오.
2. 네트워크 페이지에서 관리 링크를 선택하여 해당 네트워크의 Wickr 관리 콘솔로 이동합니다.



특정 네트워크의 Wickr 관리 콘솔로 리디렉션됩니다.



3. Wickr 관리 콘솔의 탐색 창에서 네트워크 설정을 선택한 다음 SSO 구성을 선택합니다.

   싱글 사인온 및 LDAP 구성 페이지에는 Wickr 네트워크 엔드포인트와 현재 SSO 구성이 표시됩니다.

SSO 구성.

SSO 구성에 대한 자세한 내용은 Wickr 도움말 센터의 다음 설명서를 참조하십시오.

> **Important**
>
> SSO를 구성할 때 Wickr 네트워크의 회사 ID를 지정합니다. Wickr 네트워크의 회사 ID를 기록해 두어야 합니다. 초대 이메일을 보낼 때 최종 사용자에게 제공해야 합니다. 최종 사용자는 Wickr 네트워크에 등록할 때 회사 ID를 지정해야 합니다.

- Azure AD Single Sign-On 구성
- Okta 싱글 사인온 구성

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.

네트워크 태그 관리

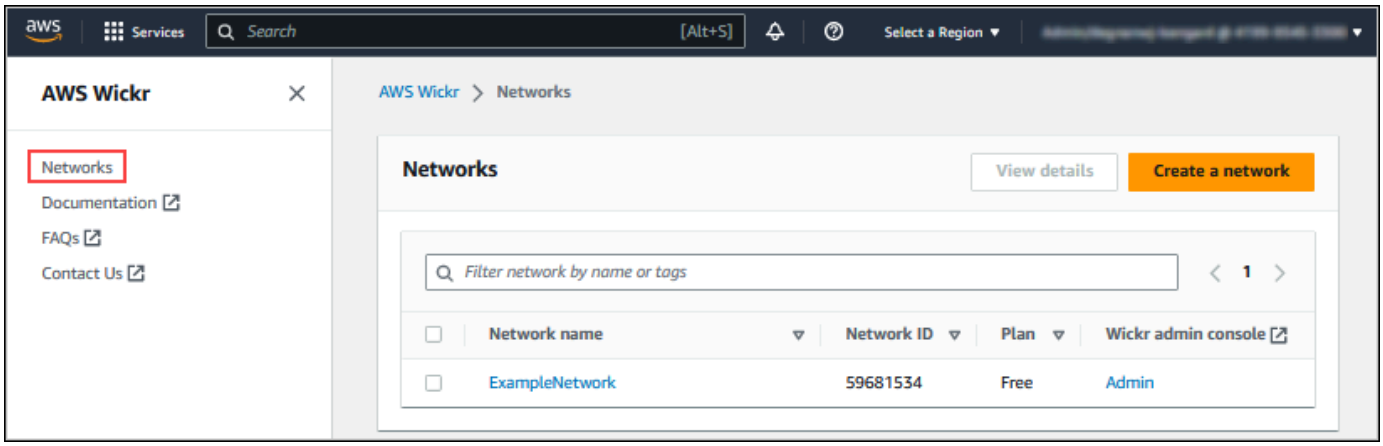
Wickr 네트워크에 태그를 적용할 수 있습니다. 그런 다음 해당 태그를 사용하여 Wickr 네트워크를 검색 및 필터링하거나 비용을 추적할 수 있습니다. AWS AWS Management Console for Wickr의 네트워크 개요 페이지에서 네트워크 태그를 구성할 수 있습니다.

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.

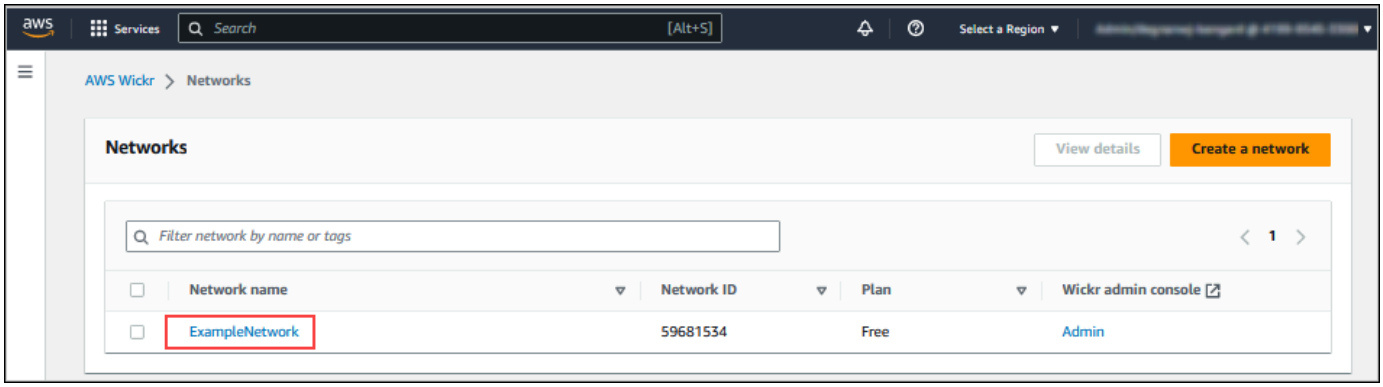
네트워크 태그 관리

Wickr 네트워크의 네트워크 태그를 관리하려면 다음 절차를 완료하세요.

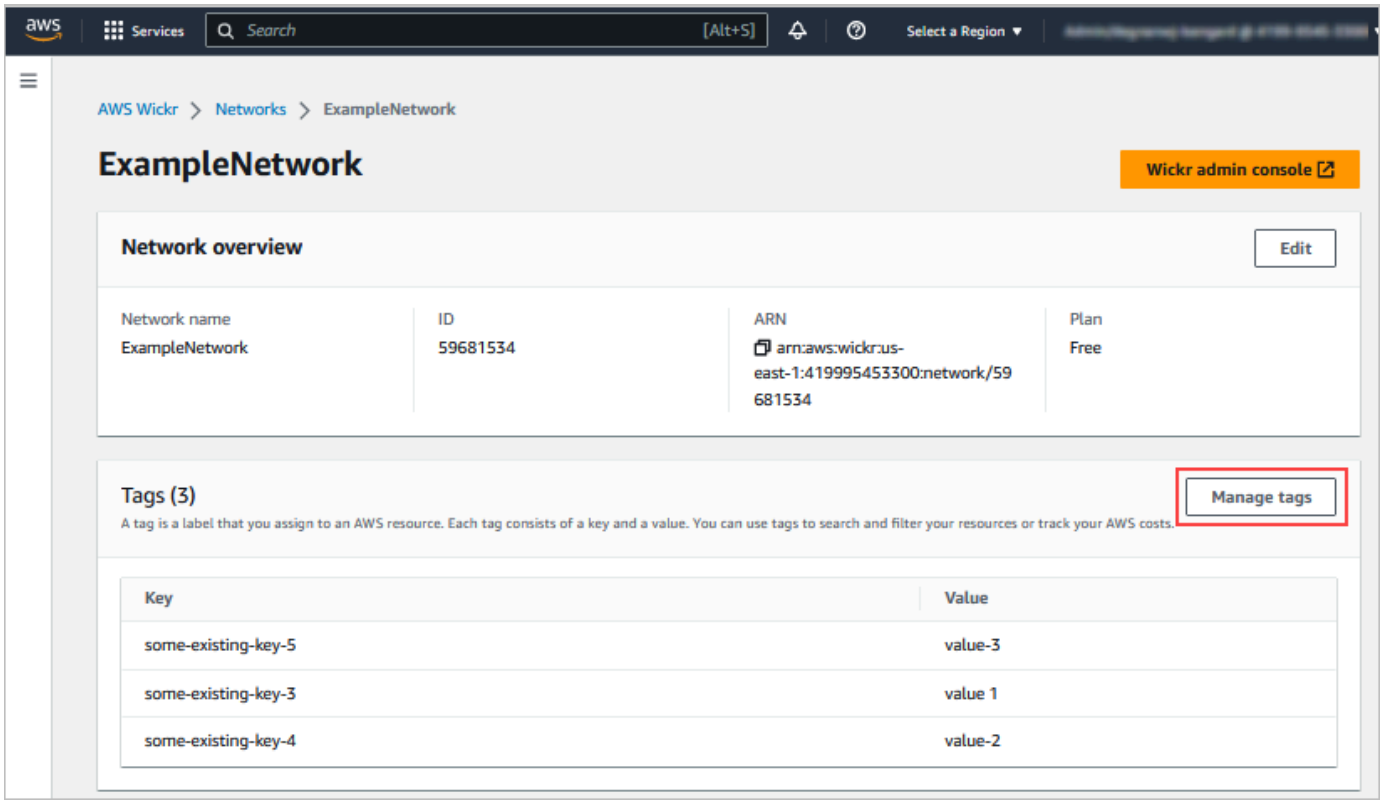
1. https://console.aws.amazon.com/wickr/ 에서 AWS Management Console 위커용 앱을 여십시오.
2. AWS Management Console for Wickr의 탐색 창에서 네트워크를 선택합니다.



3. Networks 페이지에서 태그를 관리할 네트워크 이름을 선택합니다.



4. 네트워크 개요 페이지에서 태그 관리를 선택합니다.



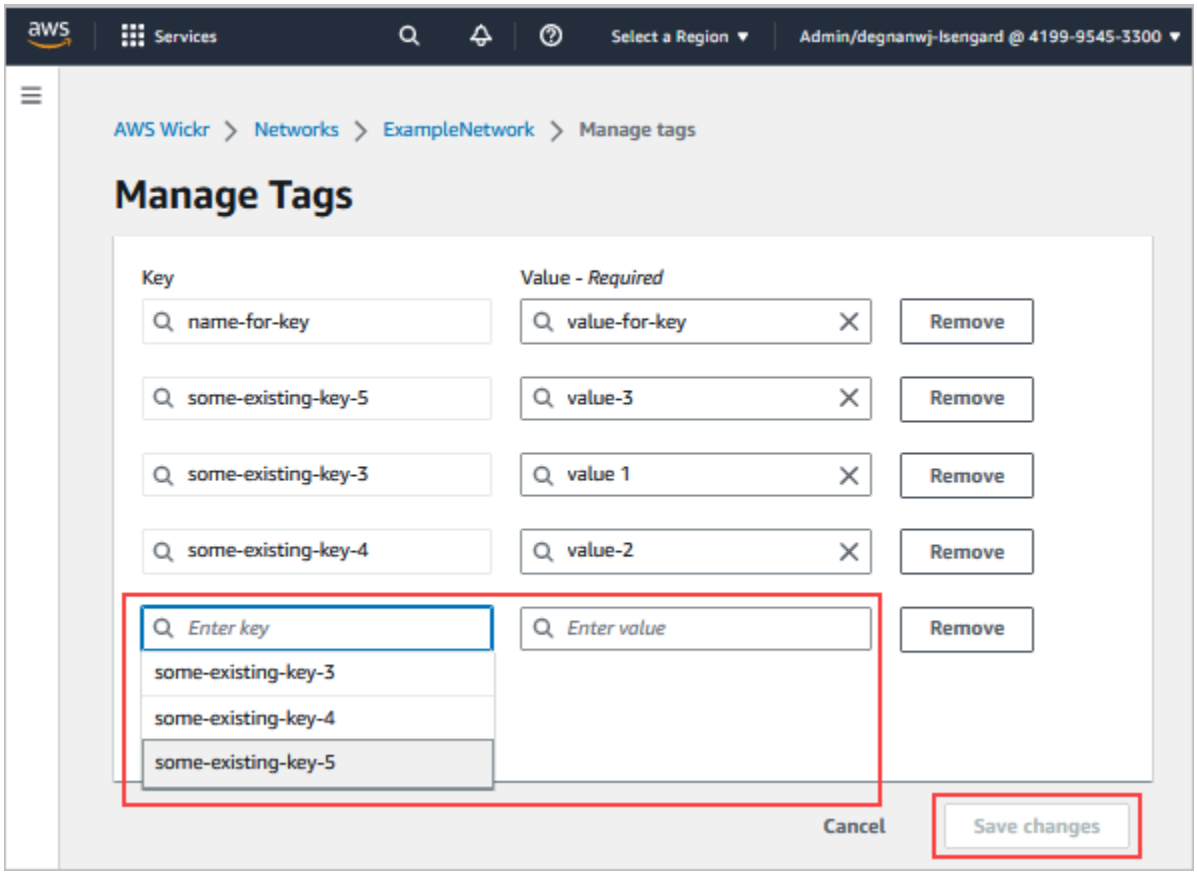
5. 태그 관리 페이지에서 다음 옵션 중 하나를 완료할 수 있습니다.

   - 새 태그 추가 - 키와 값 쌍의 형태로 새 태그를 입력합니다. 키 값 쌍을 여러 개 추가하려면 새 태그추가를 선택합니다. 태그는 대/소문자를 구분합니다. 자세한 정보는 네트워크 태그 추가을 참조하세요.
   - 기존 태그 편집 - 기존 태그의 키 또는 값 텍스트를 선택한 다음 텍스트 상자에 수정 내용을 입력합니다. 자세한 정보는 네트워크 태그 편집을 참조하세요.
   - 기존 태그 제거 — 삭제하려는 태그 옆에 나열된 제거 버튼을 선택합니다. 자세한 정보는 네트워크 태그 제거을 참조하세요.

네트워크 태그 추가

Wickr 네트워크에 태그를 추가하려면 다음 절차를 완료하세요. 태그 관리에 대한 자세한 내용은 네트워크 태그 관리 섹션을 참고하세요.

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

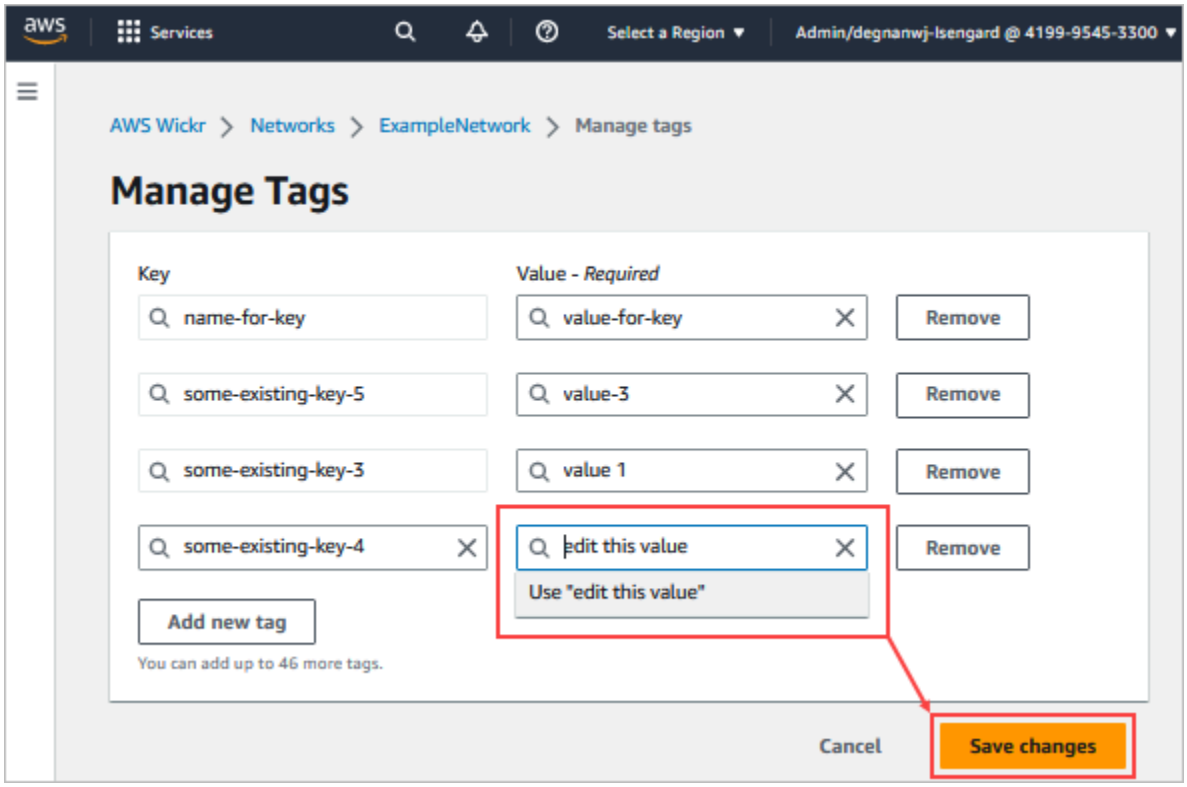


네트워크 태그 편집

Wickr 네트워크와 관련된 태그를 편집하려면 다음 절차를 완료하세요. 태그 관리에 대한 자세한 내용은 네트워크 태그 관리 섹션을 참고하세요.

1. 태그 관리 페이지에서 태그 값을 편집합니다.

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

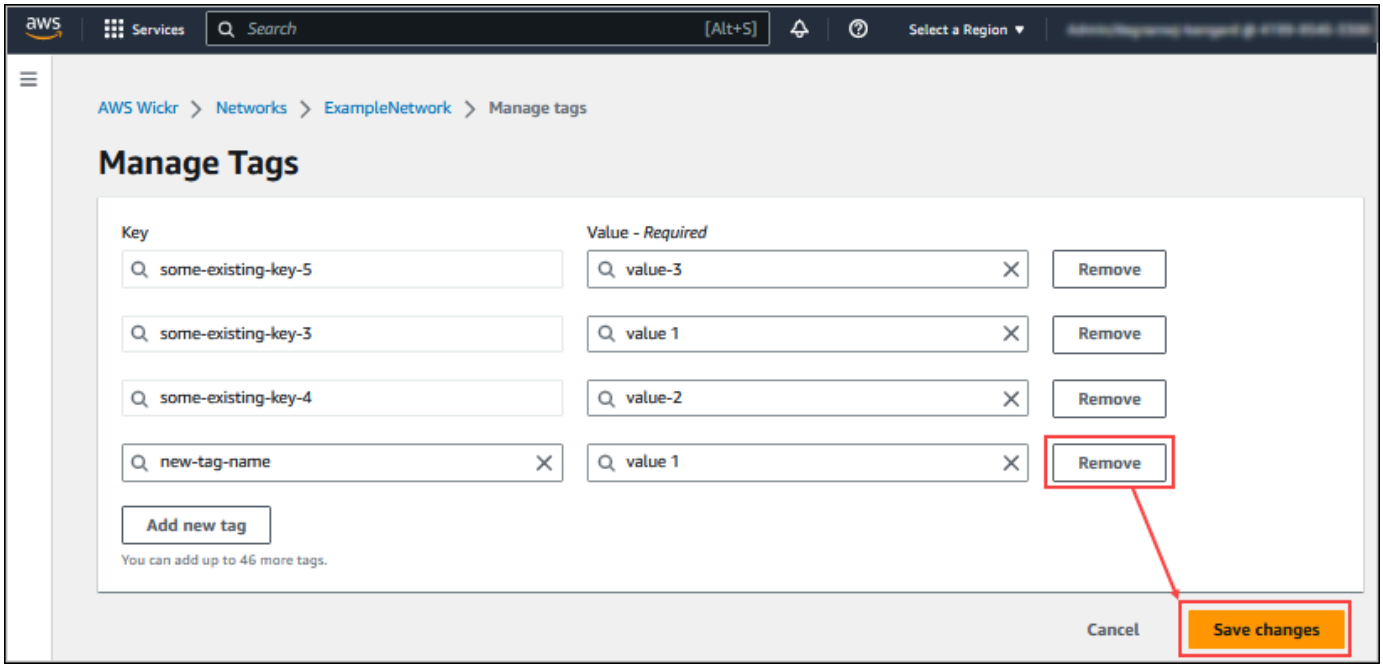


2. 변경 사항 저장을 선택하여 편집을 저장합니다.

네트워크 태그 제거

Wickr 네트워크에서 태그를 제거하려면 다음 절차를 완료하세요. 태그 관리에 대한 자세한 내용은 네트워크 태그 관리 섹션을 참고하세요.

1. 태그 관리 페이지에서 제거할 태그에 대해 제거를 선택합니다.



2. 변경 사항 저장을 선택하여 편집을 저장합니다.

네트워크 플랜 관리

AWS Management Console for Wickr의 플랜 관리 섹션에서 비즈니스 요구 사항에 따라 네트워크 플랜을 관리할 수 있습니다.

네트워크 요금제를 관리하려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ 에서 AWS Management Console 위커 앱을 여십시오.
2. Wickr 관리 콘솔의 탐색 창에서 플랜 관리를 선택한 다음 내 플랜을 선택합니다.
3. 내 플랜 페이지에서 원하는 네트워크 요금제를 선택합니다. 다음 중 하나를 선택하여 현재 네트워크 요금제를 수정할 수 있습니다.

   - 표준 — 관리 제어 및 유연성이 필요한 중소기업 및 대기업 팀에 적합합니다.
   - 프리미엄 또는 프리미엄 무료 평가판 — 최고의 기능 제한, 세분화된 관리 제어 및 데이터 보존이 필요한 비즈니스에 적합합니다.

     관리자는 최대 30명의 사용자가 사용할 수 있고 3개월 동안 사용할 수 있는 프리미엄 무료 평가판 옵션을 선택할 수 있습니다. 이 오퍼는 레거시가 없는 새로운 평가판 및 표준 요금제에서 사용할 수 있습니다. 관리자는 프리미엄 무료 평가판 기간 동안 Premium 또는 Standard 요금제로 업그레이드하거나 다운그레이드할 수 있습니다.

> **Note**
>
> 네트워크에서 사용 및 청구를 중지하려면 정지된 사용자를 포함하여 네트워크에서 모든 사용자를 제거하세요.

프리미엄 무료 평가판 한도

프리미엄 무료 평가판에는 다음과 같은 제한 사항이 적용됩니다.

- 이전에 프리미엄 무료 평가판에 등록한 적이 있는 플랜은 다른 평가판을 사용할 수 없습니다.
- AWS 계정당 하나의 네트워크만 프리미엄 무료 평가판에 등록할 수 있습니다.
- 프리미엄 무료 평가판 기간에는 게스트 사용자 기능을 사용할 수 없습니다.
- 표준 네트워크의 사용자가 30명 이상인 경우 프리미엄 무료 평가판으로 업그레이드할 수 없습니다.

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

- 데이터 보존 세부 정보 보기

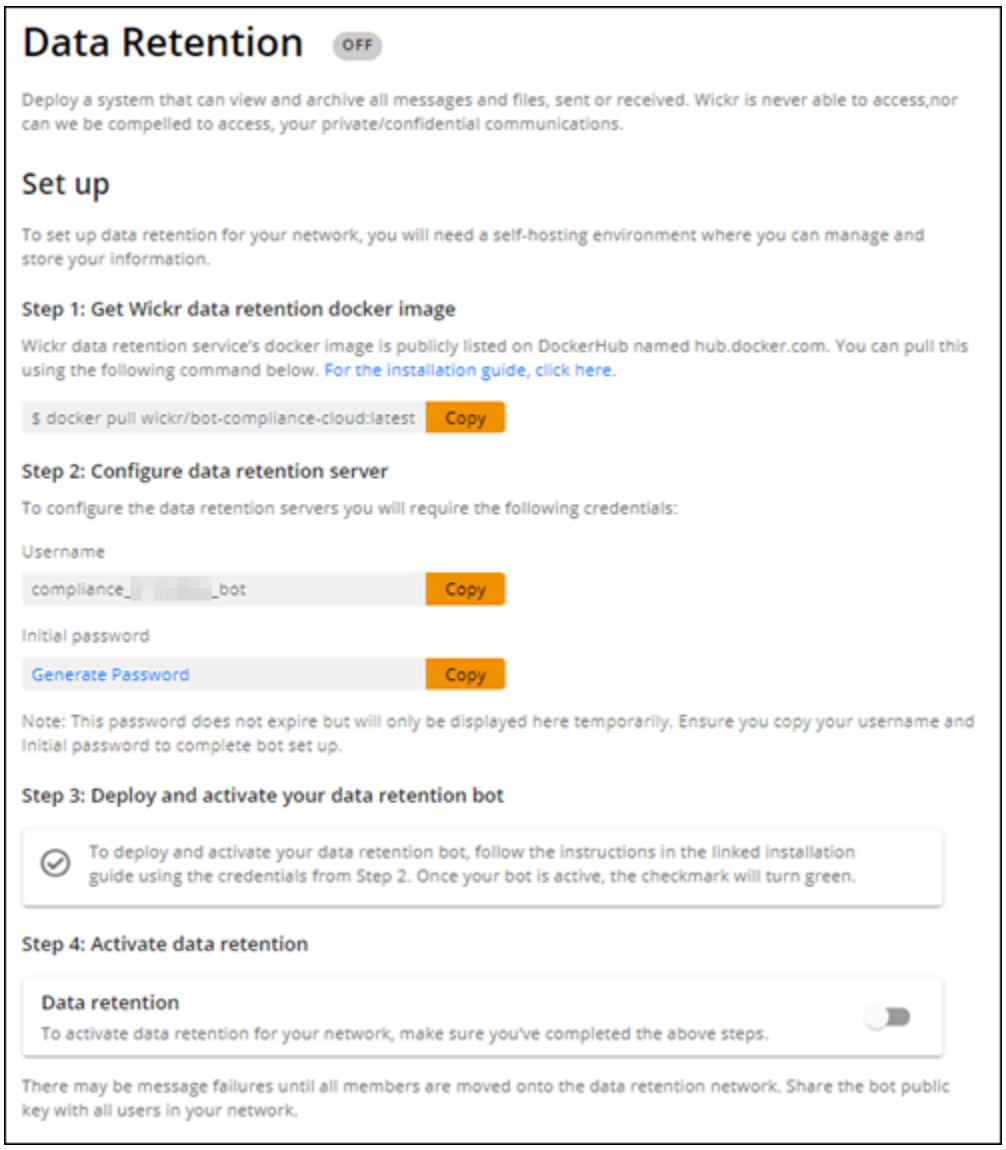
- 데이터 보존 구성
- 데이터 보존 로그 가져오기
- 데이터 보존 지표 및 이벤트

데이터 보존 세부 정보 보기

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

1. https://console.aws.amazon.com/wickr/ 에서 AWS Management Console Wickr용 앱을 여십시오.
2. 네트워크 관리를 선택합니다.
3. Wickr 관리 콘솔의 탐색 창에서 네트워크 설정을 선택한 다음 데이터 보존을 선택합니다.

   데이터 보존 페이지에는 데이터 보존 설정 단계와 데이터 보존 기능을 활성화하거나 비활성화하는 옵션이 표시됩니다. 데이터 보존 구성에 대한 자세한 내용은 데이터 보존 구성 단원을 참조하십시오.



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

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) 버킷

에 저장하도록 구성할 수 있습니다. 또한 (Secrets Manager), 아마존 AWS Secrets Manager (), 아마존 심플 알림 서비스 CloudWatch (Amazon SNSCloudWatch), () AWS Key Management Service 와 AWS KMS 같은 다른 AWS 서비스를 사용하도록 데이터 보존 봇을 구성할 수 있습니다. 다음 주제에서는 Wickr 네트워크용 데이터 보존 봇을 구성하고 실행하는 방법을 설명합니다.

주제

데이터 보존 구성을 위한 필요 조건

시작하기 전에 데이터 보존 봇 이름(사용자 이름으로 레이블됨)과 Wickr용 AWS Management Console에서 초기 암호를 가져와야 합니다. 데이터 보존 봇을 처음 시작할 때는 이 두 값을 모두 지정해야 합니다. 또한 콘솔에서 데이터 보존을 활성화해야 합니다. 자세한 설명은 데이터 보존 세부 정보 보기 섹션을 참조하세요.

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 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 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 마세요. 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"
 **********************************************************************
```

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 설명은 환경 변수 섹션을 참조하세요.

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 참조하세요.

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 설명은 데이터 보존 봇 시작 섹션을 참조하세요.

> **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 설명은 데이터 보존 구성을 위한 필요 조건 섹션을 참조하세요. 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. 기본 값은 `/tmp/<botname>/compliance/messages`입니다.
- `WICKRIO_COMP_FILEDEST`— 파일을 스트리밍될 디렉터리의 경로 이름입니다. 기본 값은 `/tmp/<botname>/compliance/attachments`입니다.
- `WICKRIO_COMP_BASENAME`— 수신된 메시지 파일의 기본 이름입니다. 기본 값은 `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 사용할 기본값 AWS 리전을 정의하십시오.

- AWS_DEFAULT_REGION— 기본적으로 AWS 리전가 Secrets Manager와 같은 AWS서비스를 위해 사용됩니다 (Amazon S3 또는 AWS KMS에는 사용되지 않음). 이 환경 변수가 정의되지 않은 경우 기본적으로 us-east-1 리전이 사용됩니다.

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

- AWS_SECRET_NAME— 데이터 보존 봇에 필요한 자격 증명과 AWS 서비스 정보가 포함된 Secrets Manager 보안 암호의 이름입니다.
- AWS_SECRET_REGION— AWS 리전는 AWS 보안 암호가 있는 위치입니다. AWS 보안 암호를 사용하고 있고 이 값이 정의되지 않은 경우 해당 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 설명은 Secrets Manager 값 섹션을 참조하세요.

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 저장되는 Amazon S3 버킷의 AWS리전입니다.
- 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.

Amazon S3 버킷에 파일을 저장할 때 클라이언트측 암호화를 사용하여 파일을 다시 암호화하도록 선택하는 경우, 다음 환경 변수를 사용하여 AWS KMS 세부 정보를 지정합니다.

- WICKRIO_KMS_MSTRKEY_ARN— Amazon S3 버킷에 저장하기 전에, 데이터 보존 봇에 있는 메시지 파일 및 파일을 다시 암호화하는 데 사용되는 AWS KMS 마스터 키의 Amazon 리소스 이름(ARN)
- WICKRIO_KMS_REGION— AWS KMS 마스터 키가 위치한 AWS 리전.

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 로 CloudWatch 전송하십시오. 지정된 경우 지표는 60초마다 생성됩니다.

- `WICKRIO_METRICS_TYPE`— 메트릭을 전송할 이 환경 변수의 값을 로 설정합니다 CloudWatch. `cloudwatch`

Secrets Manager 값

Secrets Manager를 사용하여 데이터 보존 봇 자격 증명과 AWS 서비스 정보를 저장할 수 있습니다. Secrets Manager 보안 암호를 생성하는 방법에 대한 자세한 내용은 Secrets Manager 사용 설명서의 AWS Secrets Manager 보안 암호 생성을 참조하십시오.

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 저장되는 Amazon S3 버킷의 AWS리전입니다.
- `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 저장하기 전에 데이터 보존 봇에 있는 메시지 파일 및 파일을 다시 암호화하는 데 사용되는 AWS KMS 마스터 키의 ARN.
- `kms_region`— AWS KMS 마스터 키가 위치한 AWS 리전.
- `sns_topic_arn`— 데이터 보존 이벤트를 전송할 Amazon SNS 주제의 ARN입니다.

AWS 서비스와 함께 데이터 보존을 사용하기 위한 IAM 정책

Wickr 데이터 보존 봇과 함께 다른 AWS 서비스를 사용하려는 경우, 호스트에 해당 서비스에 액세스할 수 있는 적절한 AWS Identity and Access Management (IAM) 역할과 정책이 있는지 확인해야 합니다. Secrets Manager, Amazon S3 CloudWatch, Amazon SNS 등을 사용하도록 데이터 보존 봇을 구성할

수 AWS KMS 있습니다. 다음 IAM 정책은 이러한 서비스에 대한 특정 작업에 대한 액세스를 허용합니다.

```
{
    "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 제거하십시오. 예를 들어, Amazon S3 버킷만 사용하려는 경우, `secretsmanager:GetSecretValue` `sns:Publishkms:GenerateDataKey`, 및 `cloudwatch:PutMetricData` 작업을 제거하는 다음 정책을 사용하십시오.

```
{
    "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.

데이터 보존 봇 시작

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

- AWS 서비스에 액세스할 수 없게 되면 옵션이 제한됩니다. 이 경우 기본 메시지 스트리밍 옵션을 사용하게 됩니다. 캡처된 메시지 파일의 크기를 특정 크기 또는 시간 간격으로 제한할지 여부를 결정해야 합니다. 자세한 설명은 환경 변수 섹션을 참조하세요.
- AWS 서비스에 액세스할 수 있게 되면, Secrets Manager 보안 암호를 만들어 봇 보안 인증과 AWS 서비스 구성 세부 사항을 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 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*과 지정한 리소스의 AWS 리전. 예: AWS KMS 마스터 키의 리전 또는 Amazon S3 버킷의 리전.
- *arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-a617-abababababab*와 메시지 파일 및 파일을 재암호화하는 데 사용할 AWS KMS 마스터 키의 Amazon 리소스 이름(ARN).

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 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(AWS서비스 없음)

다음 Docker 명령은 데이터 보존 봇을 시작합니다. 데이터 보존 봇에서 암호를 묻는 메시지가 표시되면 암호를 입력합니다. 이 설명서의 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 docker 이미지를 시작한 후 즉시 docker attach *<container ID or container name>* 명령을 실행하여 암호 프롬프트가 표시되도록 해야 합니다. 이 두 명령은 모두 스크립트로 실행해야 합니다. docker 이미지에 연결했는데 메시지가 표시되지 않는 경우 입력 키를 누르면 프롬프트가 표시됩니다.

15분 메시지 파일 로테이션(AWS서비스 없음)으로 봇을 시작합니다.

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 \
-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 \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e AWS_SECRET_NAME='wickr/data/retention/bot' \
wickr/bot-compliance-cloud:latest
```

`wickrpro/compliance/compliance_1234567890_bot` 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 \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
 -e AWS_SECRET_NAME='wickr/data/retention/bot' \
wickr/bot-compliance-cloud:latest
```

`wickrpro/compliance/compliance_1234567890_bot` 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.

Secrets Manager를 사용하여 봇을 시작하고 Amazon S3와 AWS KMS를 구성합니다.

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 \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
 -e AWS_SECRET_NAME='wickr/data/retention/bot' \
wickr/bot-compliance-cloud:latest
```

wickrpro/compliance/compliance_1234567890_bot 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 \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
-e WICKRIO_S3_BUCKET_NAME='bucket-name' \
-e WICKRIO_S3_FOLDER_NAME='folder-name' \
-e WICKRIO_S3_REGION='us-east-1' \
wickr/bot-compliance-cloud:latest
```

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

데이터 보존 봇을 중지하십시오.

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
```

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
```

데이터 보존 지표 및 이벤트

다음은 현재 AWS Wickr 데이터 보존 봇 5.116 버전에서 지원하는 Amazon CloudWatch (CloudWatch) 지표와 아마존 심플 알림 서비스 (Amazon SNS) 이벤트입니다.

주제

- CloudWatch 메트릭스

- Amazon SNS 이벤트

CloudWatch 메트릭스

메트릭은 봇이 1분 간격으로 생성하여 데이터 보존 봇 Docker 이미지가 실행되는 계정과 연결된 CloudWatch 서비스로 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.
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

사용할 지표가 생성됩니다. CloudWatch 봇에 사용되는 네임스페이스는 `WickrIO`입니다. 각 지표에는 차원 배열이 있습니다. 다음은 위 지표와 함께 게시된 측정기준 목록입니다.

측정기준	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.
네트워크	연결된 네트워크의 ID.

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 환경 변수및 Secrets Manager 값 섹션을 참조하세요.

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.

이름	값
message	이벤트 메시지 자세한 내용은 중요 이벤트 및 일반 이벤트 단원을 참조하세요.
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 예와 유사한 정보가 포함된 이메일이 발송됩니다.

```
{
"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.

이벤트 유형	이벤트 메시지
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:: slotAdminUser 일시 중지: 코드 (%1): 이유: %2”
BotDevice 일시 중지됨	기기가 일시 중지되었습니다!
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

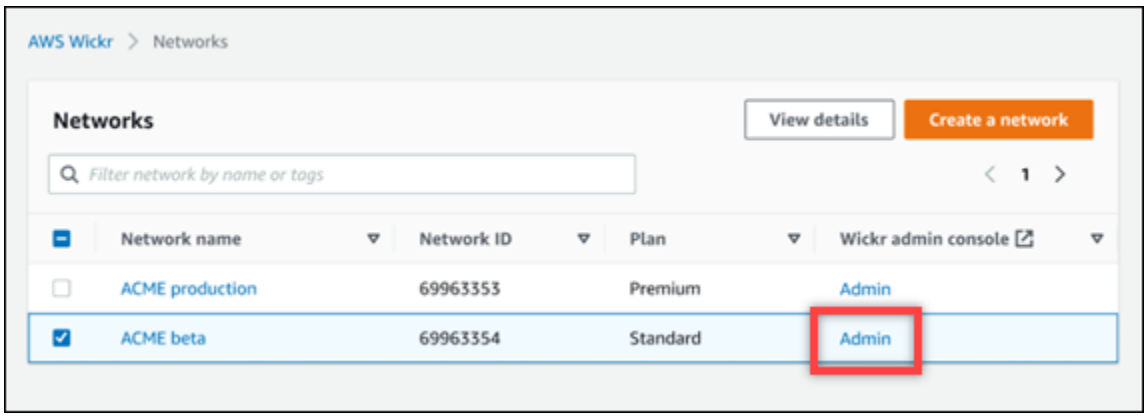
Wickr 네트워크 대시보드에서 ATAK 활성화

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.

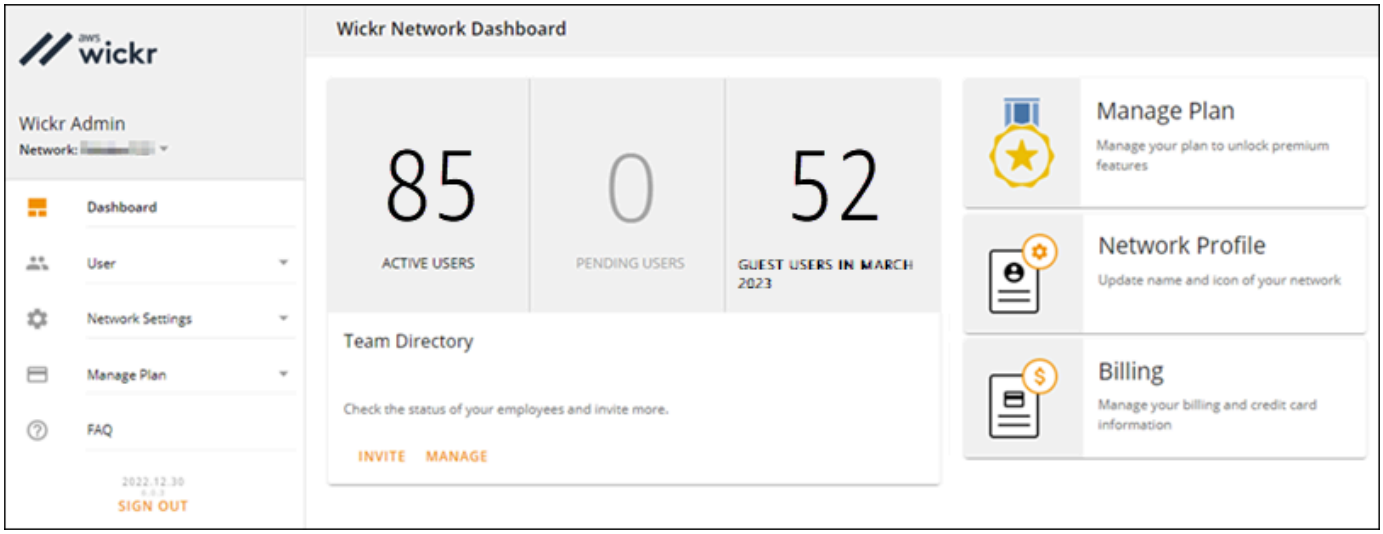
Wickr 네트워크 대시보드에서 ATAK 활성화

Wickr Network Dashboard에서 ATAK를 활성화하려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/에서 Wickr용 AWS Management Console을 여십시오.
2. 네트워크 페이지에서 관리 링크를 선택하여 해당 네트워크의 Wickr 관리 콘솔로 이동합니다.



특정 네트워크의 Wickr 관리 콘솔로 리디렉션됩니다.



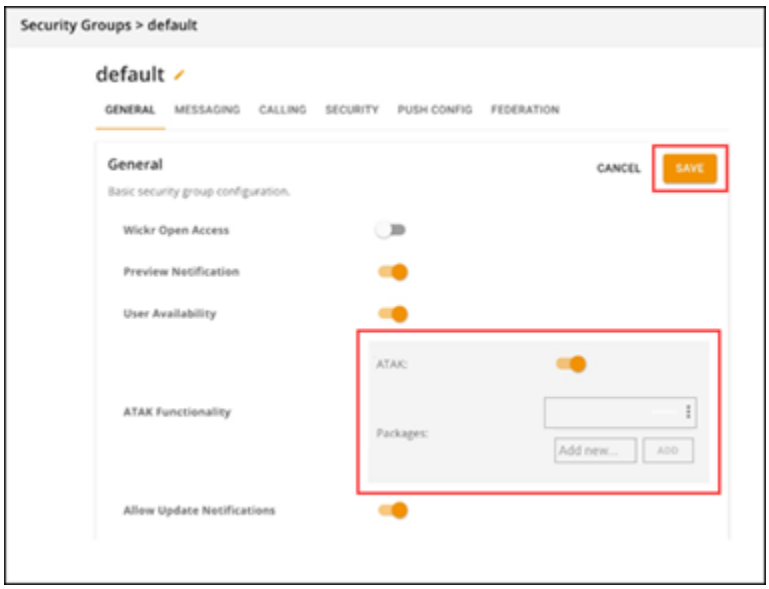
3. Wickr 관리 콘솔의 탐색 창에서 네트워크 설정을 선택한 다음 보안 그룹을 선택합니다.
4. ATAK를 활성화할 보안 그룹 옆의 세부 정보 를 선택합니다.
5. General 탭에서 Edit를 선택합니다.
6. ATAK 기능 섹션에서:

   a. 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.

   b. ATAK 토글을 오른쪽으로 밀어 기능을 켜십시오.

   c. 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

안드로이드 디바이스에 ATAK용 Wickr 플러그인을 설치하려면 다음 절차를 완료하십시오.

1. 구글 플레이 스토어로 이동하여 ATAK용 Wickr 플러그인을 설치하세요.
2. 안드로이드 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 표시에 따라 설치합니다.

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

7. ATAK 애플리케이션은 플러그인을 로드할지 여부를 물을 것입니다. 확인을 선택합니다.

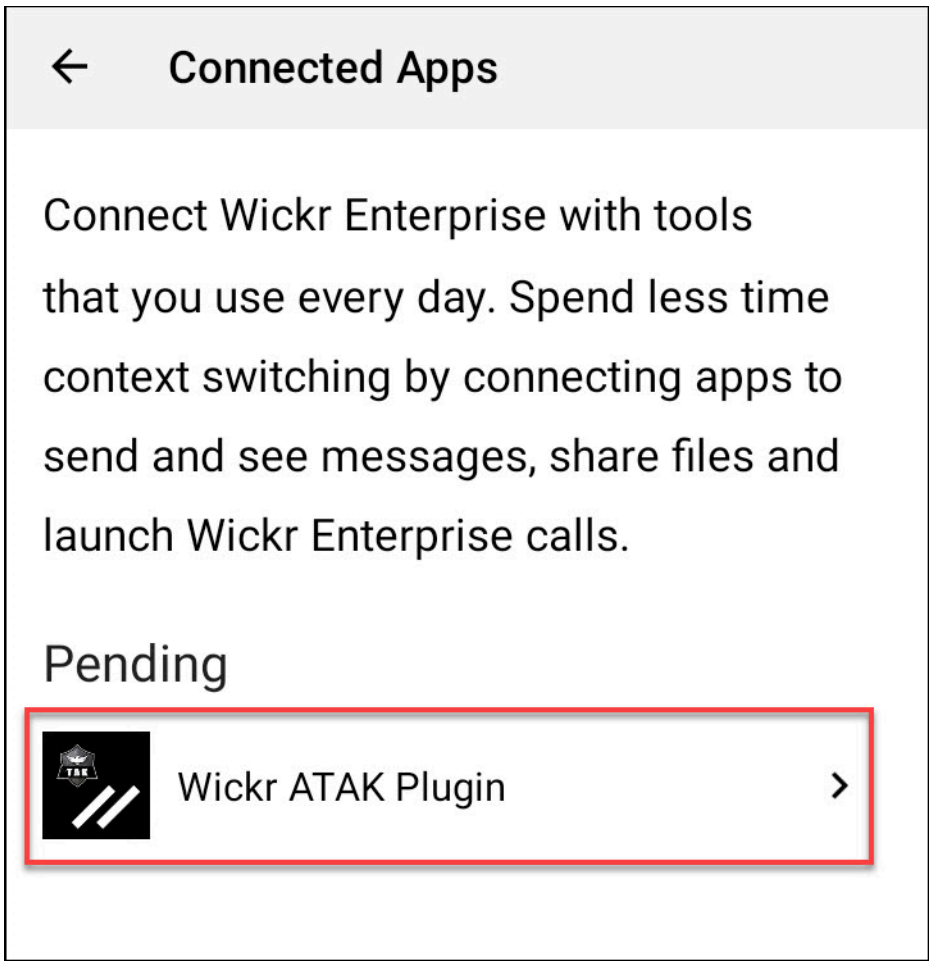
이제 ATAK용 Wickr 플러그인이 설치되었습니다. Wickr로 ATAK 페어링 섹션을 계속 진행하여 프로세스를 완료하십시오.

ATAK와 Wickr를 페어링하십시오.

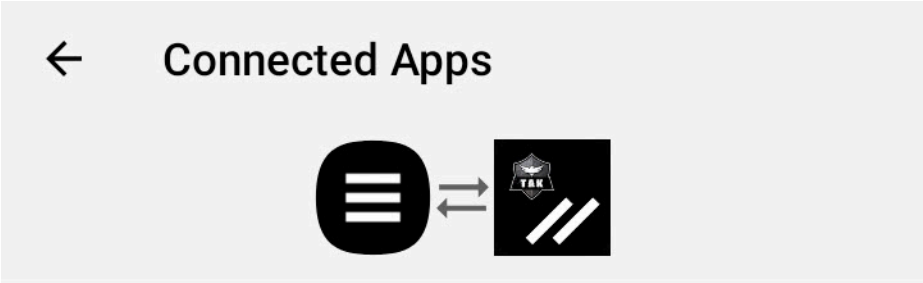
ATAK용 Wickr 플러그인을 성공적으로 설치한 후 다음 절차를 완료하여 ATAK 응용 프로그램을 Wickr와 페어링하십시오.

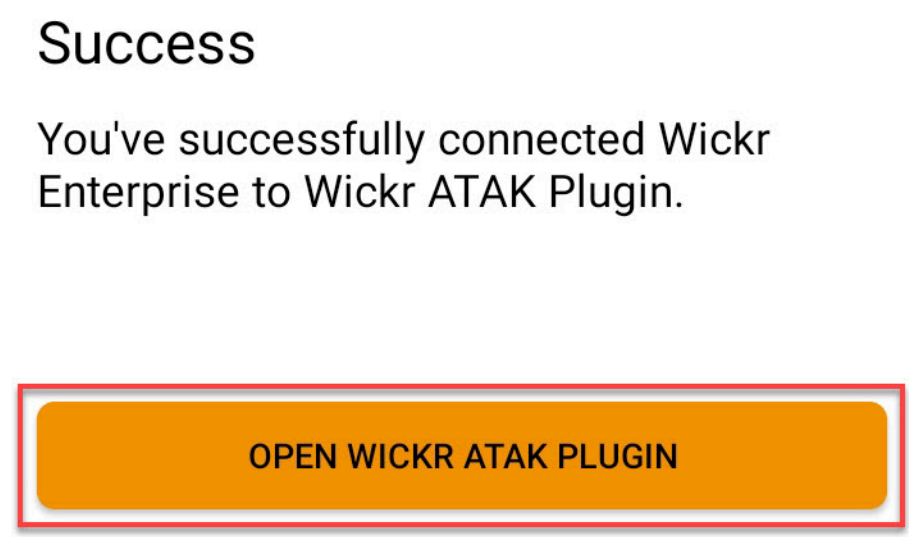
1. ATAK 애플리케이션에서, 화면 오른쪽 상단의 메뉴 아이콘 ()을 선택하고 Wickr 플러그인을 선택합니다.
2. Wicker 페어링을 선택합니다.

   ATAK용 Wickr 플러그인의 권한을 검토하라는 알림 메시지가 나타납니다. 알림 메시지가 나타나지 않으면, Wickr 클라이언트를 열고 설정으로 이동한 다음 연결된 앱으로 이동합니다. 다음 예제와 같이 화면의 보류 중 섹션에 플러그인이 표시되어야 합니다.



3. 승인을 선택하여 페어링하십시오.
4. Wickr ATAK 플러그인 열기 버튼을 선택하여 ATAK 애플리케이션으로 돌아가십시오.



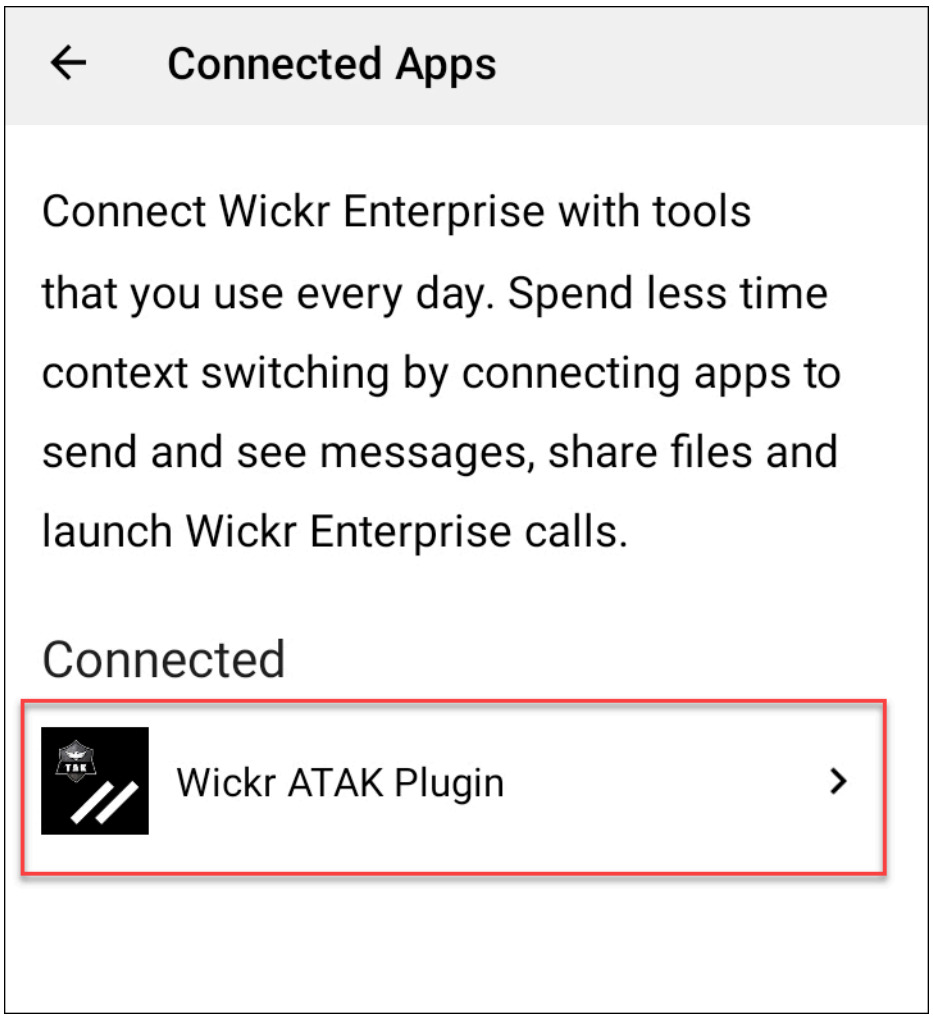


이제 ATAK 플러그인과 Wickr가 성공적으로 페어링되었으며 ATAK 애플리케이션을 종료하지 않고도 플러그인을 사용하여 Wickr를 사용하여 메시지를 보내고 협업할 수 있습니다.

ATAK 및 Wickr 페어링 해제

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.

   API를 더 이상 사용하지 않는다는 확인 화면이 표시됩니다. 이제 ATAK 플러그인의 페어링을 해제했습니다.

전화 걸기 및 받기

ATAK용 Wickr 플러그인에서 전화를 걸거나 받을 수 있습니다.

전화를 걸고 받으려면 다음 절차를 완료하세요.

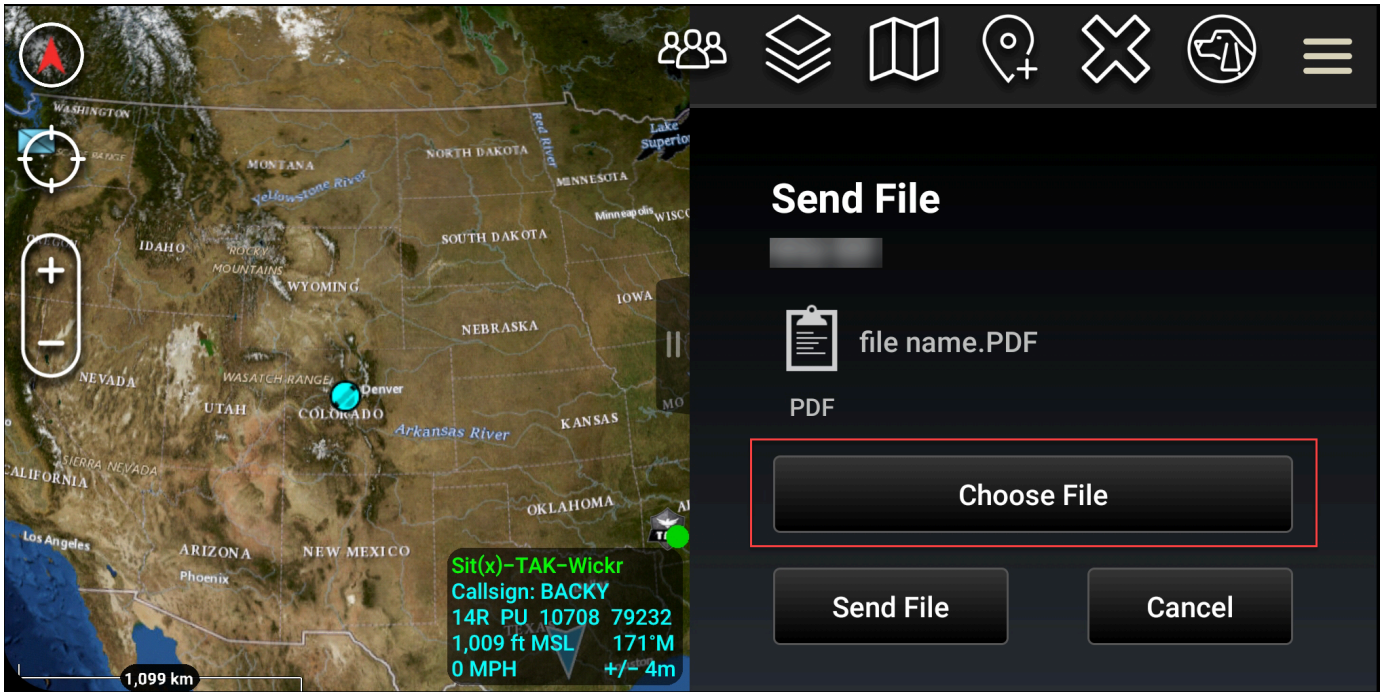
1. 채팅 창을 엽니다.
2. 맵 뷰에서 통화할 사용자의 아이콘을 선택합니다.
3. 화면 오른쪽 위에 있는 전화 아이콘을 선택합니다.
4. 연결되면 ATAK 플러그인 보기로 돌아가 전화를 받을 수 있습니다.

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.

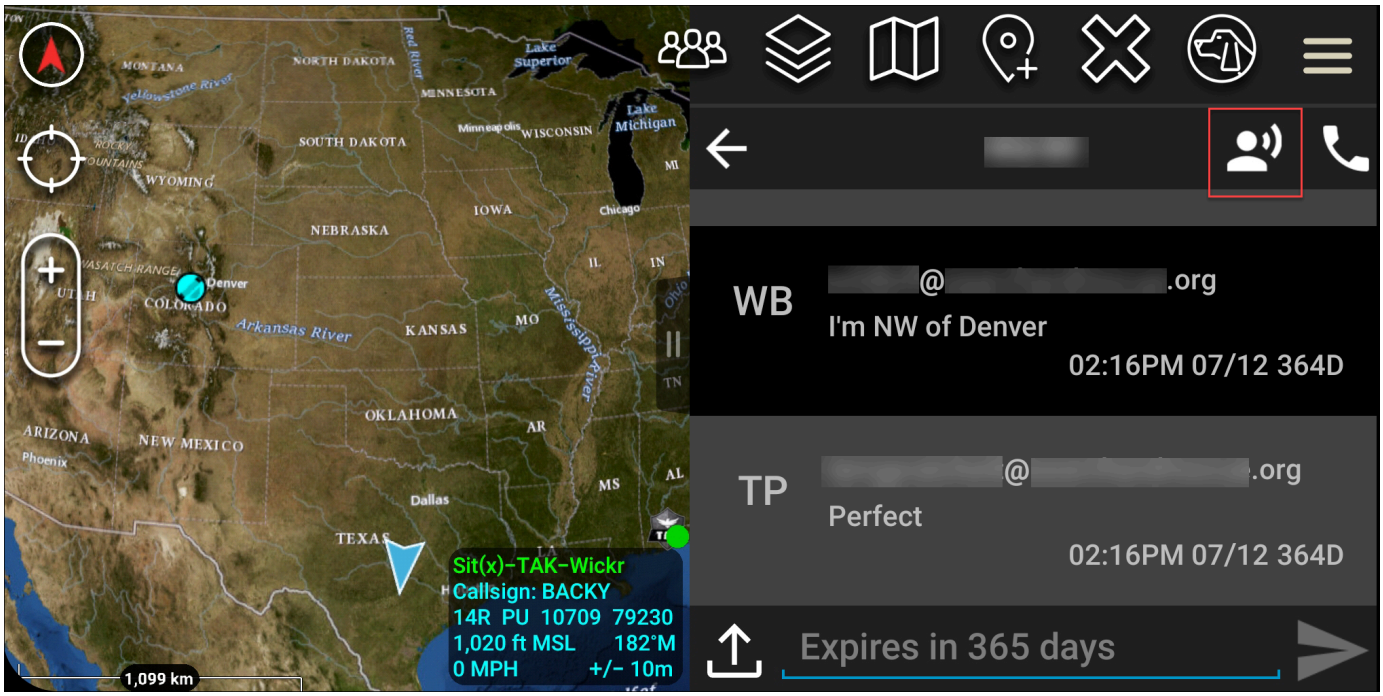
보안 음성 메시지 보내기 (Push-to-talk)

ATAK용 Wickr 플러그인에서 보안 음성 메시지 (Push-to-talk) 를 보낼 수 있습니다.

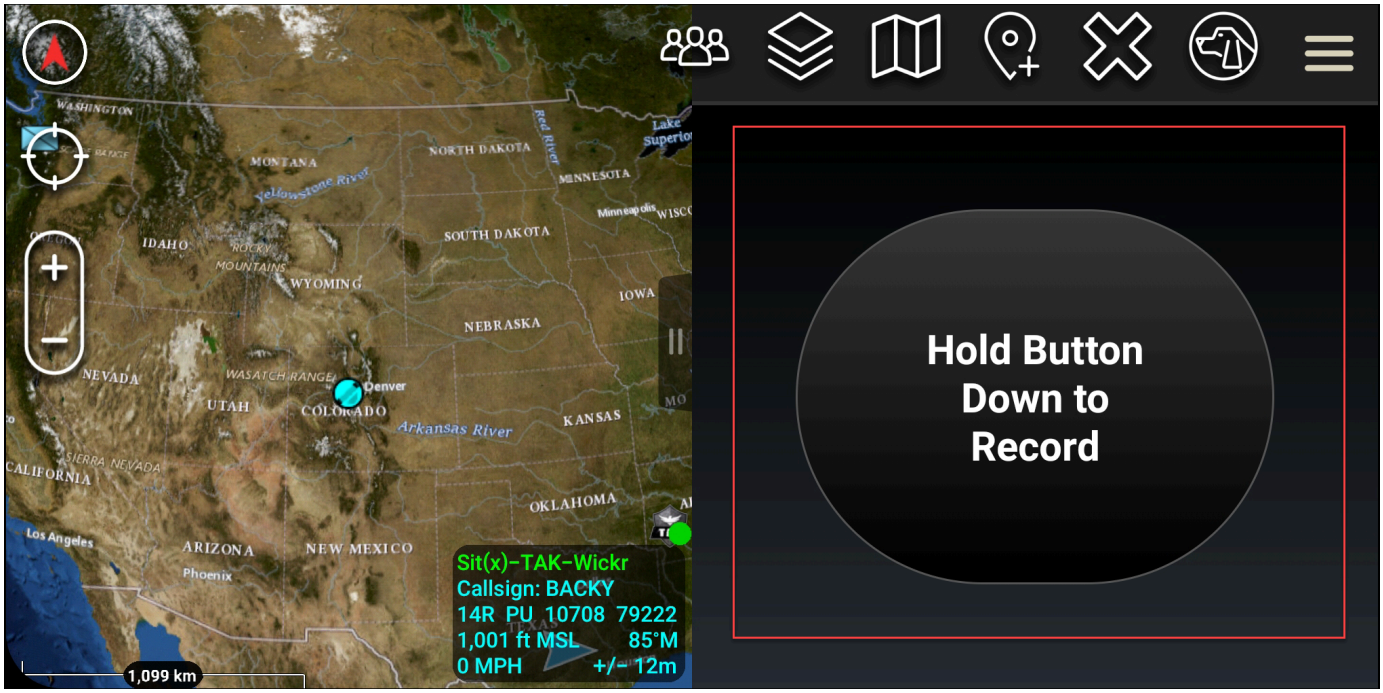
보안 음성 메시지를 보내려면 다음 절차를 완료합니다.

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.

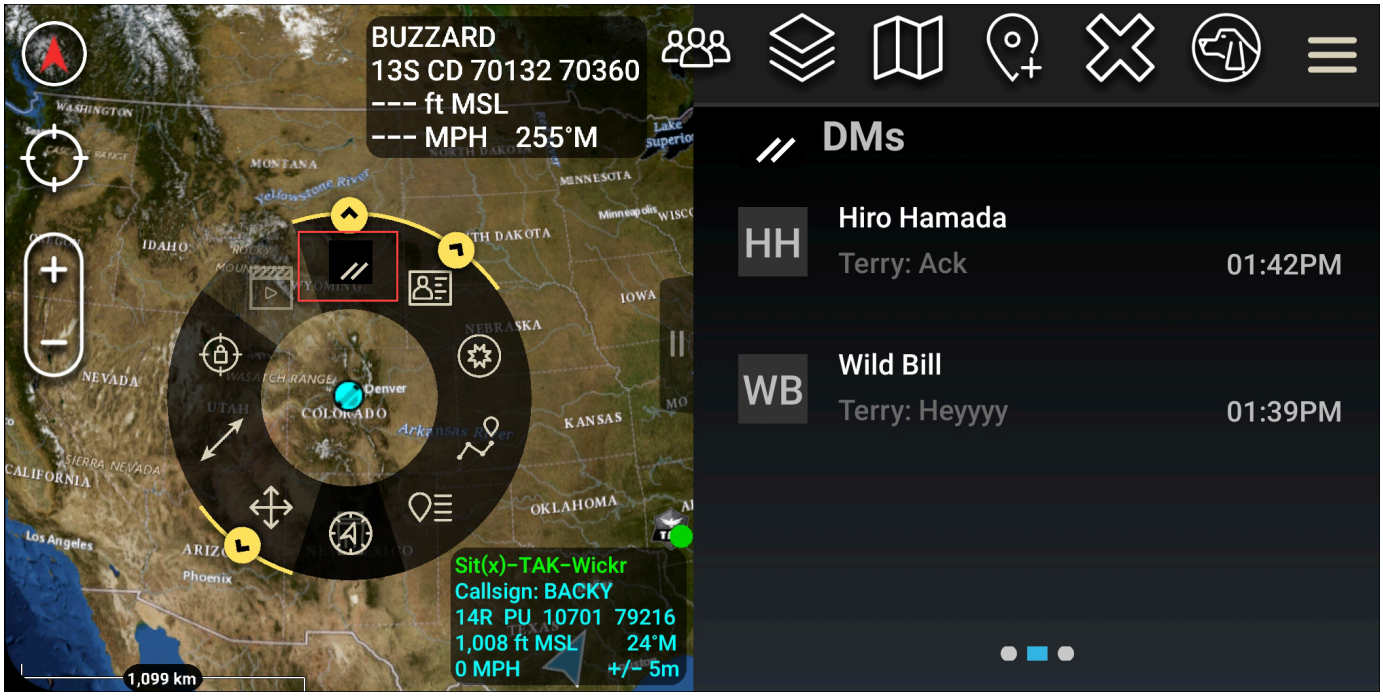
5. 메시지를 녹음한 후 버튼을 놓으면 메시지를 보낼 수 있습니다.

바람개비(퀵 액세스)

바람개비 또는 퀵 액세스 기능은 one-one-one 대화나 다이렉트 메시지에 사용됩니다.

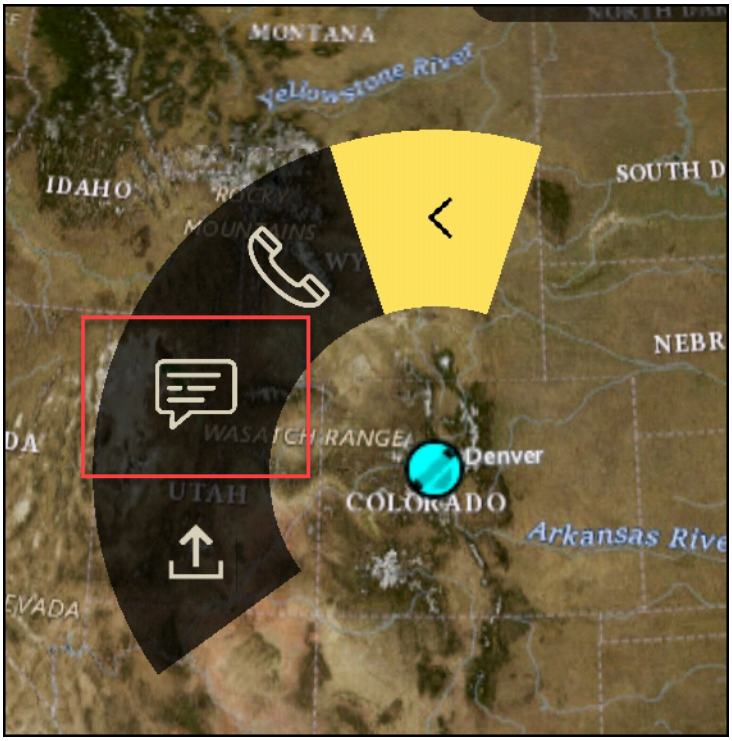
바람개비를 사용하려면 다음 절차를 완료합니다.

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.

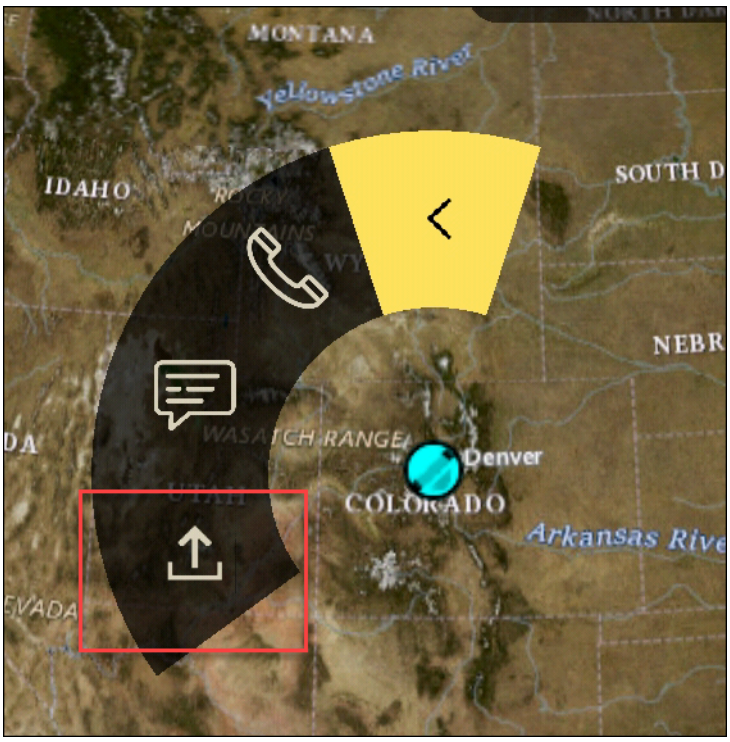


4. 바람개비에서 다음 아이콘 중 하나를 선택합니다.
   - 전화: 통화할 때 선택합니다.

- 메시지: 채팅할 때 선택합니다.



- 파일 전송: 파일을 보낼 때 선택합니다.



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: 대화 만들기. one-to-one 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.

허용할 포트 및 도메인 목록

Wickr가 올바르게 작동할 수 있도록 허용 목록에 다음 포트 및 도메인을 나열하십시오.

포트

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

지역 도메인

- 유럽(프랑크푸르트): api.messaging. wickr.eu-central-1.amazonaws.com
- 미국 동부 (버지니아 북부): gw-pro-prod .wickr.com, api.messaging. wickr.us-east-1.amazonaws.com
- 유럽(런던): api.messaging. wickr.eu-west-2.amazonaws.com
- 아시아 태평양(시드니): api.messaging. wickr.ap-southeast-2.amazonaws.com
- 캐나다(중부): api.messaging. wickr.ca-central-1.amazonaws.com
- AWS GovCloud (미국 서부): api.messaging.wickr. us-gov-west-1.amazonaws.com

등록 및 확인 이메일은 donotreply@wickr.email 에서 발송됩니다.

가능한 모든 호출 서버 IP 주소 목록을 허용해야 하는 경우 가능한 AllowlistWickrCIDR의.txt를 다운로드하여 정기적으로 확인해야 합니다. CIDR은 변경될 수 있기 때문입니다.

AWS Wickr에서 사용자 관리

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

주제

팀 디렉터리

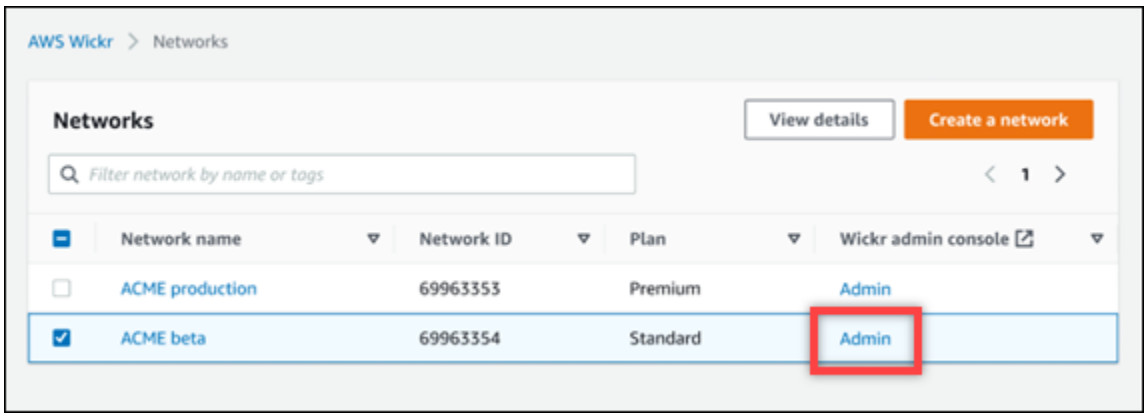
for Wickr의 사용자 섹션에서 현재 Wickr 사용자를 보고 세부 정보를 수정할 수 있습니다. AWS Management Console

주제

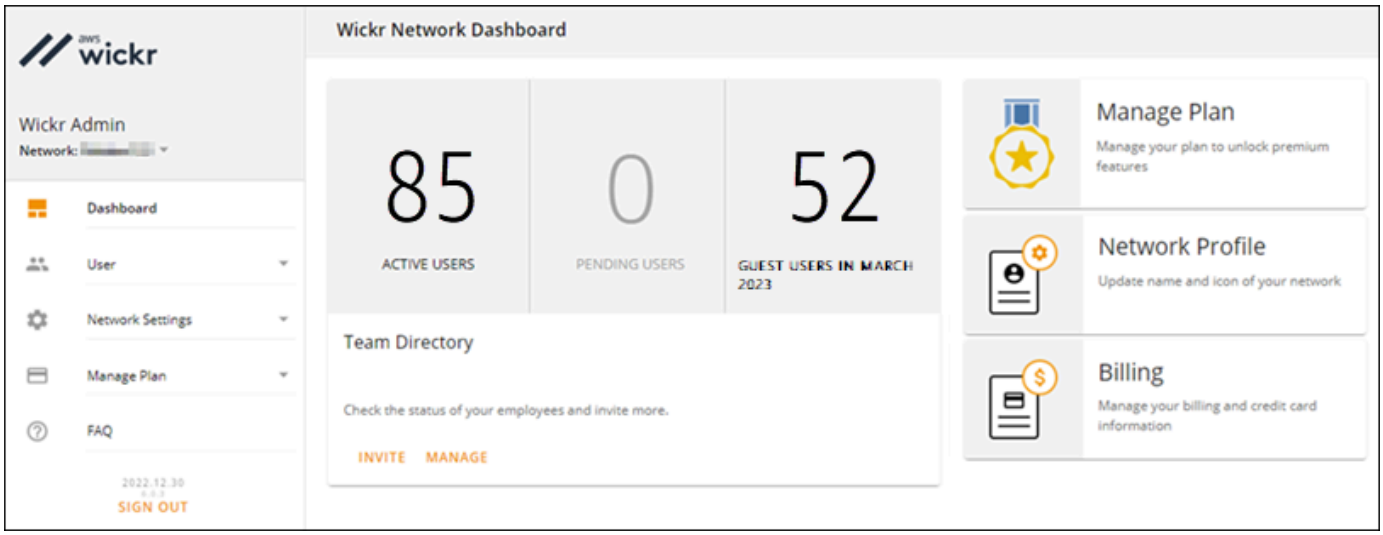
사용자 보기

Wickr 네트워크에 등록된 사용자를 보려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ 에서 AWS Management Console 위커용 위커를 여십시오.
2. 네트워크 페이지에서 관리 링크를 선택하여 해당 네트워크의 Wickr 관리 콘솔로 이동합니다.



특정 네트워크의 Wickr 관리 콘솔로 리디렉션됩니다.



3. Wickr 관리 콘솔의 탐색 창에서 사용자를 선택한 다음 팀 디렉터리를 선택합니다.

   팀 디렉터리 페이지에는 이름, 이메일 주소, 지정된 보안 그룹, 현재 상태 등 Wickr 네트워크에 등록된 사용자가 표시됩니다. 현재 사용자의 경우 장치를 보고, 세부 정보를 편집하고, 일시 중지, 삭제하고, 다른 Wickr 네트워크로 전환할 수 있습니다.

사용자 생성

사용자를 생성하려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ 에서 포 AWS Management Console 위커를 여세요.
2. 네트워크 페이지에서 관리 링크를 선택하여 해당 네트워크의 Wickr 관리 콘솔로 이동합니다.

   특정 네트워크의 Wickr 관리 콘솔로 리디렉션됩니다.
3. Wickr 관리 콘솔의 탐색 창에서 사용자를 선택한 다음 팀 디렉터리를 선택합니다.

4. 새 사용자 만들기를 선택합니다.
5. 표시되는 양식에 사용자의 이름, 성, 국가 코드, 전화번호, 이메일 주소를 입력합니다. 이메일 주소만 필수 필드입니다. 사용자에게 적합한 보안 그룹을 선택해야 합니다. Wickr는 사용자가 지정한 주소로 초대 이메일을 보냅니다.
6. 생성을 선택하세요.

   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.

사용자 편집

사용자를 편집하려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ 에서 포 AWS Management Console 위커를 여세요.
2. 네트워크 페이지에서 관리 링크를 선택하여 해당 네트워크의 Wickr 관리 콘솔로 이동합니다.

   특정 네트워크의 Wickr 관리 콘솔로 리디렉션됩니다.
3. Wickr 관리 콘솔의 탐색 창에서 사용자를 선택한 다음 팀 디렉터리를 선택합니다.
4. 삭제할 사용자 이름 옆에 있는 세로 줄임표 아이콘을 선택합니다.
5. 다음 옵션 중 하나를 선택할 수 있습니다.

   - 장치 - 사용자가 Wickr 클라이언트로 구성한 장치를 볼 수 있습니다.
   - 편집 - 이름, 국가 코드, 전화번호(선택 사항), 할당된 보안 그룹 등의 사용자 세부 정보를 편집합니다.
   - 일시 중지 - 사용자가 Wickr 클라이언트에서 Wickr 네트워크에 로그인할 수 없도록 사용자를 일시 중단합니다. 클라이언트에서 Wickr 네트워크에 현재 로그인되어 있는 사용자를 일시 중단하면 해당 사용자는 자동으로 로그아웃됩니다.
   - 삭제 - Wickr 네트워크에서 사용자를 삭제합니다.

사용자 삭제

사용자를 삭제하려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/ 에서 포 AWS Management Console 위커를 여세요.
2. 네트워크 페이지에서 관리 링크를 선택하여 해당 네트워크의 Wickr 관리 콘솔로 이동합니다.

특정 네트워크의 Wickr 관리 콘솔로 리디렉션됩니다.

3. Wickr 관리 콘솔의 탐색 창에서 사용자를 선택한 다음 팀 디렉터리를 선택합니다.
4. 삭제할 사용자 이름 옆에 있는 세로 줄임표 아이콘을 선택합니다.
5. 호스트를 삭제하려면 삭제를 선택합니다.

   사용자를 삭제하면 해당 사용자는 더 이상 Wickr 클라이언트에서 Wickr 네트워크에 로그인할 수 없습니다.

사용자 대량 삭제

Wickr용 Wickr 관리 콘솔의 사용자 섹션에서 Wickr 네트워크 사용자를 대량 삭제하고 대량 일시 중단할 수 있습니다.

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

1. https://console.aws.amazon.com/wickr/ 에서 포 AWS Management Console 위커를 여세요.
2. Wickr 관리 콘솔의 탐색 창에서 사용자를 선택한 다음 팀 디렉터리를 선택합니다.

   팀 디렉터리 페이지에는 Wickr 네트워크에 등록된 사용자가 표시됩니다.
3. 팀 디렉터리 페이지에서 사용자 관리를 선택합니다.
4. 사용자 관리 팝업 창에서 사용자 삭제를 선택합니다.
5. 모든 샘플 CSV 템플릿을 다운로드합니다. 샘플 템플릿을 다운로드하려면 템플릿 다운로드를 선택합니다.
6. 네트워크에서 대량 삭제하려는 사용자의 이메일을 추가하여 템플릿을 완성합니다.
7. 완성된 CSV 템플릿을 업로드합니다. 파일을 업로드 상자에 끌어다 놓거나 파일 선택을 선택할 수 있습니다.
8. 사용자를 삭제하면 되돌릴 수 없음을 인정합니다라는 확인란을 선택합니다.
9. 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 완료하세요.

1. https://console.aws.amazon.com/wickr/ 에서 포 AWS Management Console 위커를 여세요.
2. Wickr 관리 콘솔의 탐색 창에서 사용자를 선택한 다음 팀 디렉터리를 선택합니다.

   팀 디렉터리 페이지에는 Wickr 네트워크에 등록된 사용자가 표시됩니다.
3. 팀 디렉터리 페이지 오른쪽 상단에 있는 CSV 다운로드 아이콘을 선택합니다.
4. 팀 디렉터리 CSV 템플릿을 다운로드한 후 삭제할 필요가 없는 사용자 행을 삭제하세요.
5. 팀 디렉터리 페이지에서 사용자 관리를 선택합니다.
6. 사용자 관리 팝업 창에서 사용자 삭제를 선택합니다.
7. 팀 디렉터리 CSV 템플릿을 업로드하세요. 파일을 업로드 상자에 끌어다 놓거나 파일 선택을 선택할 수 있습니다.
8. 사용자를 삭제하면 되돌릴 수 없음을 인정합니다라는 확인란을 선택합니다.
9. 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.

사용자 대량 일시 중지

Wickr용 Wickr 관리 콘솔의 사용자 섹션에서 Wickr 네트워크 사용자를 대량 일시 중지할 수 있습니다.

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

1. https://console.aws.amazon.com/wickr/ 에서 포 AWS Management Console 위커를 여세요.
2. Wickr 관리 콘솔의 탐색 창에서 사용자를 선택한 다음 팀 디렉터리를 선택합니다.

   팀 디렉터리 페이지에는 Wickr 네트워크에 등록된 사용자가 표시됩니다.
3. 팀 디렉터리 페이지에서 사용자 관리를 선택합니다.
4. 사용자 관리 팝업 창에서 사용자 일시 중지를 선택합니다.
5. 모든 샘플 CSV 템플릿을 다운로드합니다. 샘플 템플릿을 다운로드하려면 템플릿 다운로드를 선택합니다.

6. 네트워크에서 대량으로 일시 중지하려는 사용자의 이메일을 추가하여 템플릿을 완성합니다.
7. 완성된 CSV 템플릿을 업로드합니다. 파일을 업로드 상자에 끌어다 놓거나 파일 선택을 선택할 수 있습니다.
8. CSV 파일을 업로드한 후 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.

게스트 사용자

Wickr 게스트 사용자 기능을 사용하면 개별 게스트 사용자가 Wickr 클라이언트에 로그인하여 Wickr 네트워크 사용자와 협업할 수 있습니다. Wickr 관리자는 Wickr 관리 콘솔의 보안 그룹 페이지에서 Wickr 네트워크에 대한 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 요금이 부과됩니다. 게스트 사용자 기능의 요금 책정에 대한 자세한 내용은 요금 책정 추가 기능의 Wickr 요금 책정 페이지를 참조하십시오.

주제

게스트 사용자 활성화 또는 비활성화

Wickr 네트워크의 게스트 사용자를 활성화하거나 비활성화하려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/에서 Wickr용AWS Management Console 을 여십시오.
2. 네트워크 페이지에서 관리 링크를 선택하여 해당 네트워크의 Wickr 관리 콘솔로 이동합니다.

특정 네트워크의 Wickr 관리 콘솔로 리디렉션됩니다.

3. Wickr 관리 콘솔의 탐색 창에서 네트워크 설정을 선택한 다음 보안 그룹을 선택합니다.
4. 특정 보안 그룹의 세부 정보를 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 그룹 세부 정보 페이지에서 페더레이션 탭을 선택합니다.
6. 게스트 사용자 허용 토글을 사용할 수 있는 위치는 두 곳입니다.

   - 로컬 페더레이션 - 미국 동부(버지니아 북부)에 있는 네트워크의 경우 페이지의 로컬 페더레이션 섹션 옆에 있는 편집을 선택합니다.
   - 글로벌 페더레이션 — 다른 지역에 있는 다른 모든 네트워크의 경우 페이지의 글로벌 페더레이션 섹션 옆에 있는 편집을 선택합니다.
7. 게스트 사용자 허용을 선택하여 보안 그룹의 게스트 사용자를 활성화하거나 선택을 해제하여 보안 그룹을 비활성화합니다.
8. 저장을 선택하여 변경 내용을 저장하고 보안 그룹에 적용합니다.

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

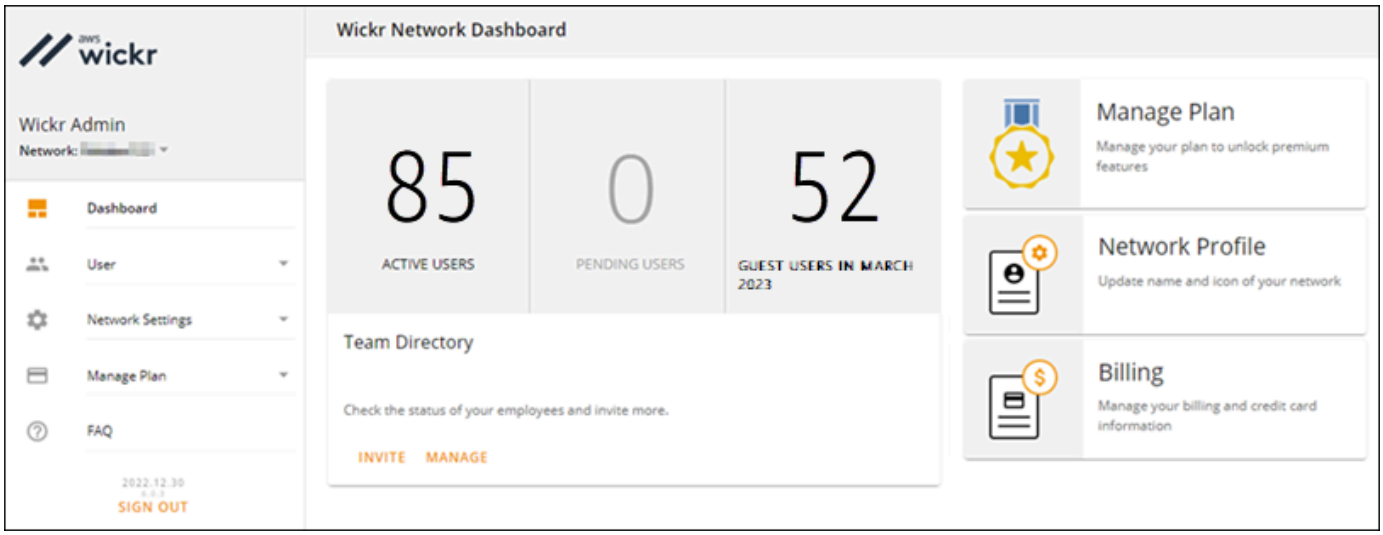
> **Note**
>
> AWS GovCloud (US)West () AWS WickrGov 에서는 Wickr 게스트 사용자 기능을 사용할 수 없습니다.

게스트 사용자 수 보기

Wickr 네트워크에 등록된 사용자를 보려면 다음 절차를 완료하세요.

1. https://console.aws.amazon.com/wickr/에서 Wickr용 AWS Management Console을 여십시오
2. 네트워크 페이지에서 관리자 링크를 선택하여 해당 네트워크의 Wickr 관리 콘솔로 이동합니다.

특정 네트워크의 Wickr 관리 콘솔로 리디렉션됩니다. 대시보드 페이지에는 다음 예와 같이 Wickr 네트워크의 게스트 사용자 수가 표시됩니다.



월별 사용량 보기

청구 기간 동안 네트워크가 통신한 게스트 사용자 수를 볼 수 있습니다. 월별 사용량을 보려면 다음 단계를 완료하세요.

1. https://console.aws.amazon.com/wickr/에서 Wickr용 AWS Management Console을 여십시오.
2. 네트워크 페이지에서 관리자 링크를 선택하여 해당 네트워크의 Wickr 관리 콘솔로 이동합니다.
3. Wickr 관리 콘솔의 탐색 창에서 사용자를 선택한 다음 게스트 사용자를 선택합니다.
4. 게스트 사용자 페이지에서 월간 사용량 섹션을 선택합니다.

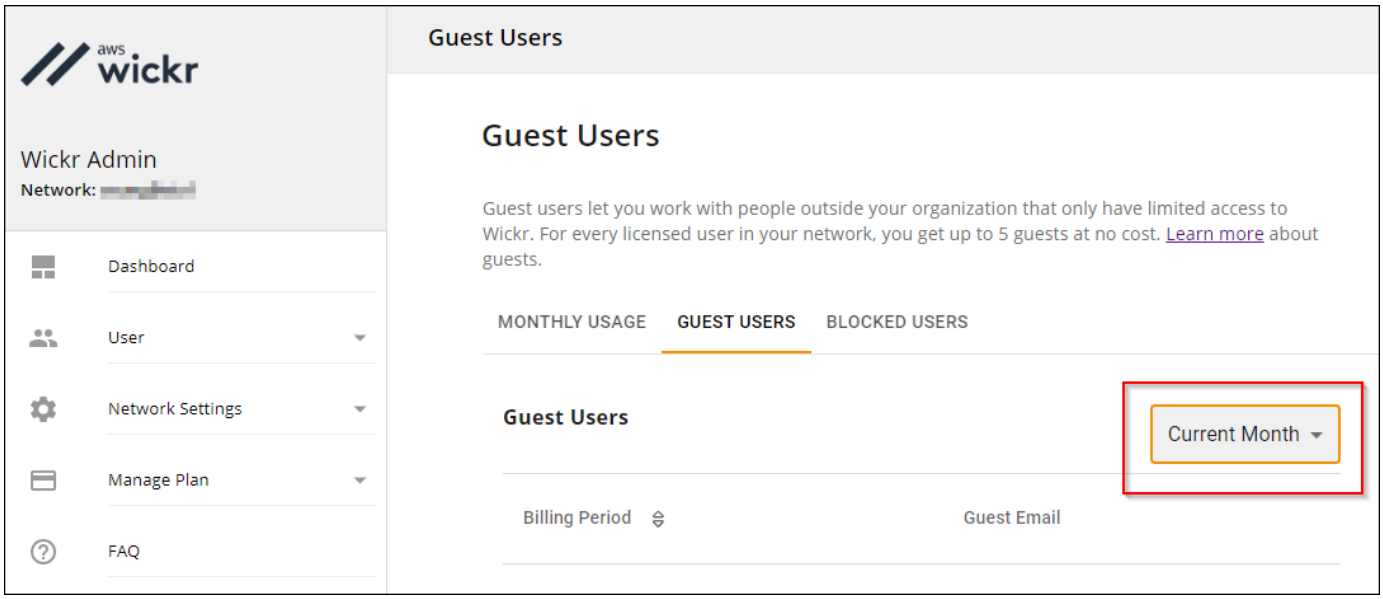
> **Note**
>
> 게스트 청구 데이터는 24시간마다 업데이트됩니다.

게스트 사용자 보기

특정 청구 기간 동안 네트워크 사용자가가 통신한 게스트 사용자 목록을 볼 수 있습니다. 게스트 사용자를 보려면 다음 단계를 완료하세요.

1. https://console.aws.amazon.com/wickr/에서 Wickr용 AWS Management Console을 여십시오.

2. 네트워크 페이지에서 관리자 링크를 선택하여 해당 네트워크의 Wickr 관리 콘솔로 이동합니다.
3. Wickr 관리 콘솔의 탐색 창에서 사용자를 선택한 다음 게스트 사용자를 선택합니다.
4. 게스트 사용자 페이지에서 게스트 사용자 섹션을 선택합니다.
5. 특정 월의 게스트 사용자를 보려면 드롭다운 메뉴에서 해당 월을 선택합니다.



게스트 사용자 차단

차단된 사용자는 네트워크에 있는 누구와도 통신할 수 없습니다.

게스트 사용자 차단

1. https://console.aws.amazon.com/wickr/에서 Wickr용 AWS Management Console을 여십시오.
2. 네트워크 페이지에서 관리자 링크를 선택하여 해당 네트워크의 Wickr 관리 콘솔로 이동합니다.
3. Wickr 관리 콘솔의 탐색 창에서 사용자를 선택한 다음 게스트 사용자를 선택합니다.
4. 게스트 사용자 페이지에서 게스트 사용자 섹션을 선택합니다.
5. 게스트 사용자 섹션에는 Wickr 네트워크에서 통신한 게스트 사용자가 표시됩니다.
6. 게스트 사용자 섹션에서, 차단하려는 게스트 사용자의 이메일을 찾습니다.
7. 게스트 사용자 이름 오른쪽에서 점 세 개를 선택하고 차단을 선택합니다.
8. 팝업 창에서 차단을 선택합니다.
9. Wickr 네트워크에서 차단된 사용자 목록을 보려면 차단된 사용자 섹션을 선택합니다.

게스트 사용자 차단 해제

1. https://console.aws.amazon.com/wickr/에서 Wickr용 AWS Management Console을 여십시오.
2. 네트워크 페이지에서 관리자 링크를 선택하여 해당 네트워크의 Wickr 관리 콘솔로 이동합니다.
3. Wickr 관리 콘솔의 탐색 창에서 사용자를 선택한 다음 게스트 사용자를 선택합니다.
4. 게스트 사용자 페이지에서 차단된 섹션을 선택합니다.
5. 차단된 사용자 섹션에는 Wickr 네트워크에서 차단된 게스트 사용자가 표시됩니다.
6. 게스트 사용자 섹션에서 차단하려는 게스트 사용자의 이메일을 찾습니다.
7. 게스트 사용자 이름 오른쪽에서 점 세 개를 선택하고 차단 해제를 선택합니다.
8. 팝업 창에서 차단 해제를 선택합니다.

AWS Wicker의 보안

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처를 활용할 수 있습니다.

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

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다 AWS 클라우드. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. AWS Wickr에 적용되는 규정 준수 프로그램에 대해 자세히 알아보려면 규정 준수 프로그램별 범위 내AWS 서비스 규정 준수 참조하십시오.
- 클라우드에서의 보안 — 사용하는 AWS 서비스에 따라 책임이 결정됩니다. 또한 귀하는 귀사의 데이터의 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 방법도 알아봅니다.

주제

AWS Wickr의 데이터 보호

AWS 공동 책임 모델 AWS Wickr의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로, AWS 는 모든 모델을 실행하는 글로벌 인프라를 보호할 책임이 있습니다. AWS 클라우드이 인프라에서 호스팅되는 콘텐츠에 대한 제어를 유지하는 것은 사용자의 책임입니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이

버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 AWS IAM Identity Center OR AWS Identity and Access Management (IAM) 을 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이 방식을 사용하면 각 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 리소스와 통신할 수 있습니다. AWS TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다. AWS CloudTrail
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.
- Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하여 Amazon S3에 저장된 민감한 데이터를 검색하고 보호합니다.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-2로 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용하십시오. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-2를 참조하십시오.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, API 또는 SDK를 AWS 서비스 사용하여 Wickr 또는 기타 작업을 수행하는 경우가 포함됩니다. AWS CLI AWS 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 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

AWS Wickr를 위한 자격 증명 및 액세스 관리

AWS Identity and Access Management (IAM) 은 관리자가 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 도구입니다. AWS IAM 관리자는 누가 Wickr 리소스를 사용하도록 인증되고(로그인됨) 권한이 부여되는지(권한 가짐)를 제어합니다. IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

주제

- 정책을 사용한 액세스 관리
- AWS AWS 위커에 대한 관리형 정책
- AWS Wickr가 IAM과 작동하는 방법
- AWS Wickr에 대한 자격 증명 기반 정책 예제
- AWS Wickr 자격 증명 및 액세스 문제 해결

고객

Wickr에서 수행하는 작업에 따라 사용 방법 AWS Identity and Access Management (IAM) 이 다릅니다.

서비스 사용자 - 사용자가 Wickr 서비스를 사용하여 작업을 수행하는 경우, 관리자는 필요한 자격 증명과 권한을 제공합니다. 더 많은 Wickr 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. Wickr의 기능에 액세스할 수 없는 경우, AWS Wickr 자격 증명 및 액세스 문제 해결 단원을 참조하세요.

서비스 관리자 - 회사에서 Wickr 리소스를 책임지고 있는 경우, Wickr에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Wickr 기능과 리소스를 결정합니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하십시오. 회사가 Wickr와 함께 IAM을 사용하는 방법에 대해 자세히 알아보려면, AWS Wickr가 IAM과 작동하는 방법 단원을 참조하세요.

IAM 관리자 - 사용자가 IAM 관리자라면 Wickr에 대한 액세스 권한 관리 정책 작성 방법에 관한 세부 사항을 알고 싶을 것입니다. IAM에서 사용할 수 있는 Wickr ID 기반 정책 예제를 보려면 단원을 AWS Wickr에 대한 자격 증명 기반 정책 예제을 참조하세요.

자격 증명을 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 연합형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 연합을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트 (SDK) 와 명령줄 인터페이스 (CLI) 를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하십시오.

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 태스크의 전체 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 태스크를 참조하세요.

연동 보안 인증

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS Directory Service페더레이션 ID에 AWS 계정액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 모든 사용자 및 애플리케이션에서 사용할 수 있습니다. AWS 계정 IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇입니까?를 참조하십시오.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한을 AWS 계정 가진 사용자 내 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 증명이 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명이 필요한 특정 사용 사

례가 있는 경우 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우 정기적으로 액세스 키 교체를 참조하십시오.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증 정보만 제공합니다. 자세한 정보는 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하십시오.

IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM 역할 사용을 참조하십시오.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다:

- 연합 사용자 액세스 - 연합 아이덴티티에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 연합 아이덴티티가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 타사 자격 증명 공급자의 역할 생성을 참조하세요. IAM Identity Center를 사용하는 경우 권한 집합을 구성합니다. 인증 후 아이덴티티가 액세스할 수 있는 항목을 통제하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 상관짓습니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하십시오.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 교차 계정 액세스를 위한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하십시오.
- 서비스 간 액세스 — 일부는 다른 AWS 서비스서비스의 기능을 AWS 서비스 사용합니다. 예컨대, 어떤 서비스에서 호출을 수행하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행

하거나 Amazon S3에 객체를 저장합니다. 서비스는 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.

- 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
- 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 역할을 생성하여 AWS 서비스에게 권한 위임을 참조하십시오.
- 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

- Amazon EC2에서 실행되는 애플리케이션 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증 정보를 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하십시오.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하십시오.

정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책의 권한이 요청 허용 또는 거부 여부를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 JSON 정책 개요를 참조하십시오.

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.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole`태스크를 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

보안 인증 기반 정책

보안 인증 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 보안 인증에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

자격 증명 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하십시오.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 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, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

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

액세스 제어 목록(ACL)

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 설명서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAF ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 안내서의 ACL(액세스 제어 목록) 개요를 참조하십시오.

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 자격 증명 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 자격 증명 기반 정책의 교집합과 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 세션 정책을 참조하십시오.

여러 정책 타입

여러 정책 타입이 요청에 적용되는 경우 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련된 경우 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하십시오.

AWS AWS 위커에 대한 관리형 정책

사용자, 그룹 및 역할에 권한을 추가하려면 정책을 직접 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 설명서의AWS 관리형 정책을 참조하십시오.

AWS 서비스 AWS 관리형 정책을 유지 관리하고 업데이트하십시오. AWS 관리형 정책에서는 권한을 변경할 수 없습니다. 서비스에서 때때로 추가 권한을 AWS 관리형 정책에 추가하여 새로운 기능을 지원합니다. 이 타입의 업데이트는 정책이 연결된 모든 보안 인증(사용자, 그룹 및 역할)에 적용됩니다.

서비스는 새로운 기능이 시작되거나 새 작업을 사용할 수 있을 때 AWS 관리형 정책에 업데이트됩니다. 서비스는 AWS 관리형 정책에서 권한을 제거하지 않으므로 정책 업데이트로 인해 기존 권한이 손상되지 않습니다.

AWS 관리형 정책: AWSWickrFullAccess

`AWSWickrFullAccess` 정책을 IAM 보안 인증에 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 참조하세요.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

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

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

관리형 정책에 대한 AWS Wickr 업데이트

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

변경 사항	설명	날짜
AWSWickrFullAccess - 새 정책	Wickr는 Wickr 서비스에 전체 관리 권한을 부여하는 새 정책을 추가했습니다. 여기에는 AWS Management Console의	2022년 11월 28일

변경 사항	설명	날짜
	Wickr 관리자 콘솔도 포함됩니다.	
Wickr 변경 내용 추적 시작	Wickr는 관리형 정책의 변경 사항을 추적하기 시작했습니다. AWS	2022년 11월 28일

AWS Wickr가 IAM과 작동하는 방법

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

AWS Wickr와 함께 사용할 수 있는 IAM 기능

IAM 특성	Wickr 지원
ID 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
보안 주체 권한	아니요
서비스 역할	아니요
서비스 연결 역할	아니요

Wickr 및 기타 AWS 서비스가 대부분의 IAM 기능과 어떻게 작동하는지 자세히 알아보려면 IAM 사용 설명서에서 IAM과 함께 작동하는AWS 서비스를 참조하십시오.

Wickr에 대한 자격 증명 기반 정책

ID 기반 정책 지원	예

자격 증명기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 태스크와 리소스 뿐만 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 자격 증명 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하십시오.

Wickr에 대한 자격 증명 기반 정책 예제

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

Wickr 내 리소스 기반 정책

리소스 기반 정책 지원	아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예는 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, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

크로스 계정 액세스를 활성화하려는 경우 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 보안 주체와 리소스가 다른 AWS 계정경

우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 개체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 개체에 자격 증명 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하십시오.

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 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

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

Wickr의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
wickr
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

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

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

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. 보고서에는 `Resource` 또는 `NotResource` 요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 작업을 수행할 수 있습니다.

작업 나열과 같이 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 참조하세요. 각 리소스의 ARN에 어떤 작업을 지정할 수 있는지 알아보려면 AWS Wickr가 정의한 작업을 참조하세요.

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

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` 요소(또는 `Condition`블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 적음 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 Condition요소를 지정하거나 단일 Condition요소에서 여러 키를 지정하는 경우 AWS 는 논리적 AND태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 OR 연산을 사용하여 조건을 AWS 평가합니다. 명령문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하십시오.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

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

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

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 설명서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Wick와 함께 ABAC

ABAC 지원(정책의 태그)	아니요

ABAC(속성 기반 액세스 제어)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 엔티티 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그를 기반으로 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 부분입니다.

ABAC에 대한 자세한 정보는 IAM 사용 설명서의 ABAC란 무엇인가요?를 참조하십시오. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하십시오.

Wickr에서 보안 인증 정보 사용

임시 보안 인증 정보 지원	아니요

임시 자격 증명을 사용하여 로그인하면 작동하지 AWS 서비스 않는 것도 있습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 IAM 사용 설명서의 IAM과AWS 서비스 연동되는 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증 정보를 자동으로 생성합니다. 역할 전환에 대한 자세한 정보는 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하십시오.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 자격 증명 섹션을 참조하십시오.

Wickr의 서비스 간 보안 주요 권한

전달 액세스 세션(FAS) 지원	아니요

IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하라는 요청과 결합하여 사용합니다. AWS 서비스 FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신

한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

Wickr에 대한 서비스 역할

서비스 역할 지원	아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 IAM role(IAM 역할)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 역할을 생성하여 AWS 서비스에게 권한 위임을 참조하십시오.

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

Wickr에 대한 서비스 연결 역할

서비스 연결 역할 지원	아니요

서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스 섹션을 참조하세요. Service-linked role(서비스 연결 역할) 열에서 Yes이(가) 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 Yes(네) 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.

```
{
```

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

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

주제

- 정책 모범 사례
- Wickr용 AWS Management Console 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. 자격 증명 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르십시오.

- AWS 관리형 정책을 시작하고 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 직무에 대한AWS 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 설명서의 IAM의 정책 및 권한을 참조하세요.

- Use conditions in IAM policies to further restrict access(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 생성할 수 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하십시오.
- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 권장 사항을 제공하여 안전하고 기능적인 정책을 생성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하세요.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 MFA 보호 API 액세스 구성을 참조하세요.

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

Wickr용 AWS Management Console 사용

`AWSWickrFullAccess` AWS 관리형 정책을 IAM ID에 연결하여 Wickr 서비스에 대한 전체 관리 권한을 부여하십시오. 여기에는 의 Wickr 관리자 콘솔도 포함됩니다. AWS Management Console자세한 정보는 AWS 관리형 정책: AWSWickrFullAccess을 참조하세요.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
```

```
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

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

- 저는 Wickr 앱에서 관리 작업을 수행할 권한이 없습니다. AWS Management Console

저는 Wickr 앱에서 관리 작업을 수행할 권한이 없습니다. AWS Management Console

Wickr AWS Management Console for Wickr에서 작업을 수행할 권한이 없다고 표시되면 관리자에게 도움을 요청해야 합니다. 관리자는 로그인 보안 인증 정보를 제공한 사람입니다.

다음 예제 오류는 mateojackson IAM 사용자가 AWS Management Console for Wickr에서 Wickr를 사용하여 Wickr 네트워크를 생성, 관리 또는 확인하려고 하지만 및 권한이 없는 AWS Management Console 경우 발생합니다. wickr:CreateAdminSession wickr:ListNetworks

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

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

규정 준수 확인

특정 규정 준수 프로그램 범위 내 AWS 서비스 목록은 규정 준수 프로그램별 범위 내AWS 서비스 규정 준수 참조하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

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 사항을 설명하고 보안 및 규정 준수에 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다. AWS
- AWS 규정 준수 리소스AWS — 이 통합 문서 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS Config 개발자 안내서의 규칙을 통한 리소스 평가 — AWS Config; 는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이 AWS 서비스는 보안 업계 표준 및 모범 사례를 준수하는지 확인하는 데 도움이 AWS 되는 내부 보안 상태를 종합적으로 보여줍니다.

AWS Wickr의 복원성

AWS 글로벌 인프라는 가용 영역을 중심으로 구축됩니다. AWS 리전 AWS 리전 물리적으로 분리되고 격리된 여러 가용 영역을 제공합니다. 이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹으로 연결됩니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

가용 영역에 대한 AWS 리전 자세한 내용은 글로벌 인프라를 참조하십시오AWS .

AWS 글로벌 인프라 외에도 Wickr는 데이터 복원력 및 백업 요구 사항을 지원하는 데 도움이 되는 여러 기능을 제공합니다. 자세한 정보는 데이터 보존을 참조하세요.

AWS Wickr의 인프라 보안

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

AWS Wickr의 구성 및 취약성 분석

구성 및 IT 제어는 귀하와 당사 고객 간의 AWS 공동 책임입니다. 자세한 내용은 AWS 공동 책임 모델을 참조하십시오.

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 정보는 AWS AWS 위커에 대한 관리형 정책을 참조하세요.

- 첫 번째 인증으로 AWS Management Console Wickr용 Wickr에 액세스하세요. AWS Management Console 개인용 콘솔 자격 증명을 공유하지 마세요. 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 있어 중요한 부분입니다. AWS Wickr를 관찰하고, 문제 발생 시 보고하고, 적절한 경우 자동 조치를 취할 수 있는 다음과 같은 모니터링 도구를 제공합니다.

- AWS CloudTrail계정에서 또는 AWS 계정을 대신하여 이루어진 API 호출 및 관련 이벤트를 캡처하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 어떤 사용자와 계정이 전화를 걸었는지 AWS, 어떤 소스 IP 주소에서 호출이 이루어졌는지, 언제 호출이 발생했는지 식별할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오. 를 사용하여 CloudTrail Wickr API 호출을 로깅하는 방법에 대한 자세한 내용은 을 참조하십시오. AWS CloudTrail를 사용하여 AWS Wickr API 호출 로깅

AWS CloudTrail를 사용하여 AWS Wickr API 호출 로깅

AWS Wickr는 Wickr에서 사용자AWS CloudTrail, 역할 또는 서비스가 수행한 작업의 기록을 제공하는 AWS 서비스와 통합되어 있습니다. CloudTrail Wickr에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 Wickr의 AWS Management Console에서 호출과 Wickr API 작업에 대한 호출이 포함됩니다. 트레일을 생성하면 Wickr에 대한 CloudTrail 이벤트를 포함하여 Amazon S3 버킷으로 이벤트를 지속적으로 전송할 수 있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 Wickr에 이루어진 요청, 요청이 이루어진 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다. 자세한 CloudTrail 내용은 AWS CloudTrail사용 설명서를 참조하십시오.

위커 정보는 CloudTrail

CloudTrail 계정을 만들 AWS 계정 때 활성화됩니다. Wickr에서 활동이 발생하면 해당 활동이 이벤트 기록의 다른 AWS 서비스 CloudTrail 이벤트와 함께 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 이벤트 기록으로 CloudTrail 이벤트 보기를 참조하십시오.

Wickr에 대한 이벤트를 포함하여 AWS 계정에 진행 중인 이벤트를 기록하려면 추적을 생성합니다. 트레일을 사용하면 CloudTrail Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 영역의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하세요.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

모든 Wickr 작업은 로그에 의해 기록됩니다. CloudTrail 예를 들어`CreateAdminSession`, 에 대한 호출 및 `ListNetworks` 작업은 CloudTrail 로그 파일에 항목을 생성합니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 보안 인증 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트로 했는지 아니면 AWS Identity and Access Management(IAM) 사용자 보안 인증 정보로 했는지
- 역할 또는 페더레이션 사용자에 대한 임시 보안 인증 정보를 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지.

자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.

Wickr 로그 파일 항목 이해하기

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함되어 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 `CreateAdminSession` 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
{
    "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"
}
```


다음 예제는 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다. `CreateNetwork`


```
{
    "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"
}
```

다음 예제는 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다. `ListNetworks`

```
{
    "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"
}
```


다음 예제는 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다. `UpdateNetworkdetails`


```
{
    "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"
}
```

다음 예제는 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다. TagResource

```
{
    "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"
}
```

다음 예제는 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다. `ListTagsForResource`

```
{
    "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"
}
```

애널리틱스 대시보드

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

분석 대시보드에 액세스하려면

1. https://console.aws.amazon.com/wickr/ 에서 AWS Management Console 위커용 앱을 여십시오.
2. 탐색 창에서 분석을 선택합니다.

   애널리틱스 페이지에는 네트워크에 대한 지표가 여러 탭에 표시됩니다.

애널리틱스 페이지의 각 탭의 오른쪽 상단 모서리에 기간 필터가 있습니다. 이 필터는 전체 페이지에 적용됩니다. 또한 각 탭의 오른쪽 상단에서 사용 가능한 내보내기 옵션을 선택하여 선택한 시간 범위의 데이터 포인트를 내보낼 수 있습니다.

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

다음과 같은 탭을 사용할 수 있습니다.

- 개요가 표시됩니다.
  - 등록 — 선택한 시간 동안 네트워크에서 활성 및 일시 중단된 사용자를 포함하여 등록된 총 사용자 수입니다. 대기 중이거나 초대된 사용자는 포함되지 않습니다.
  - 보류 중 — 선택한 시간 동안 네트워크에서 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 장치 수입니다.

- 구성원은 다음을 표시합니다.
  - 상태 — 선택한 기간 내에 네트워크에 있는 활성 사용자
  - 활성 사용자 —
    - 그래프는 시간 경과에 따른 활성 사용자 수를 표시하며 위에서 선택한 시간 범위 내에서 일별, 주별 또는 월별로 집계할 수 있습니다.
    - 활성 사용자 수는 플랫폼, 클라이언트 버전 또는 보안 그룹별로 분류할 수 있습니다. 보안 그룹이 삭제된 경우 총 수는 삭제된 횟수로 표시됩니다.

- 메시지는 다음과 같이 표시됩니다.
  - 보낸 메시지 — 선택한 기간 동안 네트워크상의 모든 사용자와 봇이 보낸 고유한 메시지 수입니다.
  - 통화 — 네트워크 내 모든 사용자가 수행한 고유 통화 수입니다.
  - 파일 — 네트워크에서 사용자가 보낸 파일 수 (음성 메모 포함).
  - 장치 - 원형 차트에는 운영 체제별로 분류된 활성 장치 수가 표시됩니다.
  - 클라이언트 버전 — 클라이언트 버전별로 분류된 활성 장치 수입니다.

문서 이력

다음 표에서는 Wickr에 대한 문서 릴리스를 소개합니다.

변경 사항	설명	날짜
글로벌 페더레이션은 이제 제한된 페더레이션을 지원하며 관리자는 관리 콘솔에서 사용 분석을 볼 수 있습니다.	글로벌 페더레이션은 이제 제한된 페더레이션을 지원합니다. 이는 다른 네트워크의 Wickr 네트워크에서도 작동합니다. AWS 리전자세한 내용은 보안 그룹을 참조하십시오. 또한 관리자는 이제 관리 콘솔의 애널리틱스 대시보드에서 사용량 분석을 볼 수 있습니다. 자세한 내용은 애널리틱스 대시보드를 참조하십시오.	2024년 3월 28일
이제 AWS Wickr 프리미엄 요금제의 3개월 무료 평가판을 사용할 수 있습니다.	Wickr 관리자는 이제 최대 30명의 사용자를 위한 3개월 무료 평가판 프리미엄 플랜을 선택할 수 있습니다. 무료 평가판 기간 동안 무제한 관리자 제어 및 데이터 보존을 포함한 모든 Standard 및 Premium 플랜 기능을 사용할 수 있습니다. 프리미엄 무료 평가판 기간에는 게스트 사용자 기능을 사용할 수 없습니다. 자세한 내용은 플랜 관리를 참조하십시오.	2024년 2월 9일
게스트 사용자 기능은 일반적으로 사용할 수 있으며 더 많은 관리자 제어 기능이 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 있습니	2023년 11월 8일

	다. 자세한 내용은 게스트 사용자를 참조하세요.	
이제 유럽 (프랑크푸르트) 에서 Wickr를 사용할 수 있습니다. AWS 리전	이제 유럽 (프랑크푸르트) 에서 Wickr를 사용할 수 있습니다. AWS 리전자세한 내용은 Wickr 액세스하기를 참조하십시오.	2023년 10월 26일
이제 Wickr 네트워크를 여러 곳으로 페더레이션할 수 있습니다. 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 리전자세한 내용은 Wickr 액세스하기를 참조하십시오.	2023년 8월 23일
이제 캐나다 (중부) 에서 Wickr를 사용할 수 있습니다. AWS 리전	이제 캐나다 (중부) 에서 Wickr를 사용할 수 있습니다. AWS 리전자세한 내용은 Wickr 액세스하기를 참조하십시오.	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 참조하세요.	2023년 5월 31일

AWS Wickr는 이제 다음과 통합되어 AWS CloudTrailAWS GovCloud (미국 서부) 에서 사용할 수 있습니다. WickrGov	AWS Wickr는 이제 와 통합되었습니다. AWS CloudTrail자세한 내용은 AWS CloudTrail을 사용하여 AWS Wickr API 호출 로깅을 참조하십시오. 또한 Wickr는 이제 AWS GovCloud (미국 서부) 에서도 사용할 수 있습니다. WickrGov 자세한 내용은 사용 설명서를 참조하십시오 AWS WickrGov.AWS GovCloud (US)	2023년 3월 30일
태깅 및 다중 네트워크 생성	이제 AWS Wickr에서 태깅이 지원됩니다. 자세한 내용은 네트워크 태그 관리를 참조하세요. 여러 네트워크를 이제 Wickr에서 만들 수 있습니다. 자세한 내용은 네트워크 생성을 참조하세요.	2023년 3월 7일
최초 릴리스	Wickr 관리 설명서의 최초 릴리스	2022년 11월 28일

릴리스 정보

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

2024년 3월

- 글로벌 페더레이션은 이제 제한된 페더레이션을 지원합니다. 제한된 페더레이션으로 추가된 선택된 네트워크에 대해서만 글로벌 페더레이션을 활성화할 수 있습니다. 이는 다른 지역의 Wickr 네트워크에서도 작동합니다. AWS 리전자세한 내용은 보안 그룹을 참조하십시오.
- 이제 관리자는 관리 콘솔의 애널리틱스 대시보드에서 사용량 분석을 볼 수 있습니다. 자세한 내용은 애널리틱스 대시보드를 참조하십시오.

2024년 2월

- AWS Wickr는 현재 최대 30명의 사용자에게 프리미엄 요금제의 3개월 무료 평가판을 제공하고 있습니다. 변경 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 평가판 기간에는 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 요금제를 프리미엄 무료 평가판으로 업그레이드할 수 있습니다. 자세한 내용은 플랜 관리를 참조하십시오.

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 정보는 게스트 사용자을 참조하세요.

2023년 3월

- 이제 Wickr가 통합되었습니다. AWS CloudTrail자세한 정보는 AWS CloudTrail를 사용하여 AWS Wickr API 호출 로깅 을 참조하세요.
- Wickr는 이제 AWS GovCloud (미국 서부) 광고에서도 사용할 수 있습니다. WickrGov 자세한 내용은 사용 설명서를 참조하십시오 AWS WickrGov.AWS GovCloud (US)
- 이제 Wickr에서 태그 지정을 지원합니다. 자세한 정보는 네트워크 태그 관리을 참조하세요. 여러 네트워크를 이제 Wickr에서 만들 수 있습니다. 자세한 정보는 1단계: 네트워크 생성을 참조하세요.

2023년 2월

- Wickr는 이제 Android Tactical Assault Kit(ATAK)를 지원합니다. 자세한 정보는 Wickr 네트워크 대시보드에서 ATAK 활성화을 참조하세요.

2023년 1월

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

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