



사용자 가이드

AWS 최종 사용자 메시징 소셜



AWS 최종 사용자 메시징 소셜: 사용자 가이드

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 브랜드 디자인은 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

AWS 최종 사용자 메시징 소셜이란 무엇입니까?	1
AWS 최종 사용자 메시징 소셜을 처음 사용하는 사용자입니까?	1
AWS 최종 사용자 메시징 소셜의 기능	1
관련 서비스	2
AWS 최종 사용자 메시징 소셜 액세스	2
리전별 가용성	3
AWS 최종 사용자 메시징 소셜 설정	5
에 가입 AWS 계정	5
관리자 액세스 권한이 있는 사용자 생성	5
다음 단계	7
시작하기	8
에 가입 WhatsApp	8
사전 조건	8
콘솔을 통해 가입	9
다음 단계	13
WhatsApp 비즈니스 계정(WABA)	14
보기 WABA	15
추가 WABA	15
WhatsApp 비즈니스 계정 유형	15
추가 리소스	16
전화 번호	17
전화번호 고려 사항	17
전화번호 추가	17
사전 조건	18
에 전화번호 추가 WABA	18
전화번호 상태 보기	19
전화번호 ID 보기	20
메시징 대화 한도 증가	20
메시지 처리량 증가	21
전화번호 품질 등급 이해	21
전화번호 품질 등급 보기	22
메시지 템플릿	23
Manager에서 WhatsApp 메시지 템플릿 사용	23
다음 단계	24

템플릿 페이싱	24
템플릿 저하 상태에 대한 피드백 받기	24
템플릿 상태 및 품질 등급	25
템플릿이 거부되는 이유	26
메시지 및 이벤트 대상	28
이벤트 대상 추가	28
사전 조건	28
메시지 및 이벤트 대상 추가	28
암호화된 Amazon SNS 주제 정책	29
다음 단계	30
메시지 및 이벤트 형식	30
AWS 최종 사용자 메시징 소셜 이벤트 헤더	30
문자 메시지의 예 WhatsApp JSON	31
미디어 메시지의 예 WhatsApp JSON	32
상태 메시지	33
메시지 상태	33
추가 리소스	34
미디어 파일 업로드	35
지원되는 미디어 파일 유형	36
미디어 파일 유형	36
메시지 유형	39
추가 리소스	39
메시지 전송	40
템플릿 메시지 전송	41
미디어 메시지 전송	41
수신된 메시지에 응답	43
메시지 상태를 읽음으로 변경	43
반응으로 대응	43
에서 Amazon S3로 미디어 파일 다운로드 WhatsApp	44
메시지에 응답하는 예	45
사전 조건	45
응답	45
추가 리소스	47
청구서 이해	48
예제 1: 마케팅 템플릿 메시지 전송	51
예제 2: 서비스 대화 열기	51

결제 ISO 코드	52
모니터링	66
를 사용한 모니터링 CloudWatch	66
CloudTrail 로그	67
AWS 의 최종 사용자 메시징 소셜 데이터 이벤트 CloudTrail	69
AWS 의 최종 사용자 메시징 소셜 관리 이벤트 CloudTrail	70
AWS 최종 사용자 메시징 소셜 이벤트 예제	70
모범 사례	72
Up-to-date 비즈니스 프로파일	72
권한 획득	72
금지된 메시지 내용	73
고객 목록 감사	75
참여를 기반으로 전송 조정	75
적절한 시간에 전송	75
보안	76
데이터 보호	77
데이터 암호화	78
전송 중 암호화	78
키 관리	78
인터넷워크 트래픽 개인 정보 보호	79
자격 증명 및 액세스 관리	79
고객	80
ID를 통한 인증	80
정책을 사용한 액세스 관리	83
AWS 최종 사용자 메시징 소셜 작업 방식 IAM	85
자격 증명 기반 정책 예시	91
AWS 관리형 정책	94
문제 해결	95
규정 준수 확인	97
복원력	98
인프라 보안	99
교차 서비스 혼동된 대리인 방지	99
보안 모범 사례	100
서비스 링크 역할 사용	101
AWS 최종 사용자 메시징 소셜에 대한 서비스 연결 역할 권한	101
AWS 최종 사용자 메시징 소셜에 대한 서비스 연결 역할 생성	102

AWS 최종 사용자 메시징 소셜에 대한 서비스 연결 역할 편집	102
AWS 최종 사용자 메시징 소셜에 대한 서비스 연결 역할 삭제	102
AWS 최종 사용자 메시징 소셜 서비스 연결 역할에 지원되는 리전	103
할당량	104
문서 기록	106
.....	cvii

AWS 최종 사용자 메시징 소셜이란 무엇입니까?

AWS 소셜 메시징이라고도 하는 최종 사용자 메시징 소셜은 개발자가 애플리케이션에 통합할 WhatsApp 수 있는 메시징 서비스입니다. WhatsApp의 풍부한 메시징 기능에 대한 액세스를 제공하여 이미지, 비디오 및 버튼으로 브랜드화된 대화형 콘텐츠를 생성할 수 있습니다. 이 서비스를 사용하면 SMS 및 푸시 알림과 같은 기존 채널과 함께 애플리케이션에 WhatsApp 메시징 기능을 추가하여 선호하는 통신 채널을 통해 고객과 소통할 수 있습니다.

시작하려면 AWS 최종 사용자 메시징 소셜 콘솔에서 자체 안내 온보딩 프로세스를 사용하여 새 WhatsApp 비즈니스 계정(WABA)을 생성하거나 기존 를 서비스에 연결할 수 WABA 있습니다.

주제

- [AWS 최종 사용자 메시징 소셜을 처음 사용하는 사용자입니까?](#)
- [AWS 최종 사용자 메시징 소셜의 기능](#)
- [관련 서비스](#)
- [AWS 최종 사용자 메시징 소셜 액세스](#)
- [리전별 가용성](#)

AWS 최종 사용자 메시징 소셜을 처음 사용하는 사용자입니까?

AWS 최종 사용자 메시징 소셜을 처음 사용하는 경우 다음 섹션을 읽는 것으로 시작하는 것이 좋습니다.

- [AWS 최종 사용자 메시징 소셜 설정](#)
- [AWS 최종 사용자 메시징 소셜 시작하기](#)
- [AWS 최종 사용자 메시징 소셜 미디어 모범 사례](#)

AWS 최종 사용자 메시징 소셜의 기능

AWS 최종 사용자 메시징 소셜은 다음과 같은 기능을 제공합니다.

- [메시지 템플릿을 만들고 사용](#)하여 일관된 메시지를 디자인하고 콘텐츠를 보다 효과적으로 재사용할 수 있습니다. 메시지 템플릿에는 보내는 메시지에 재사용하려는 콘텐츠와 설정이 포함되어 있습니다.

- 더 매력적인 경험을 위해 새로운 리치 메시징 기능에 액세스합니다. 텍스트 및 미디어 외에도 위치와 대화형 메시지를 보낼 수 있습니다.
- 고객으로부터 수신되는 문자 및 미디어 메시지를 수신합니다.
- Meta를 통해 비즈니스 자격 증명을 확인하여 고객과 신뢰를 구축합니다.

관련 서비스

AWS 는 다중 채널 워크플로에서 함께 사용할 수 있는 다른 메시징 서비스를 제공합니다.

- [AWS 최종 사용자 메시징SMS](#)을 사용하여 SMS 메시지 전송
- [AWS 최종 사용자 메시징 푸시](#)를 사용하여 푸시 알림 전송
- [AmazonSES](#)을 사용하여 이메일 전송

AWS 최종 사용자 메시징 소셜 액세스

다음을 사용하여 AWS 최종 사용자 메시징 소셜에 액세스할 수 있습니다.

AWS 최종 사용자 메시징 소셜 콘솔

리소스를 [생성하고](#) 관리하는 웹 인터페이스입니다.

AWS Command Line Interface

명령줄 셸의 명령을 사용하여 AWS 서비스와 상호 작용합니다. AWS Command Line Interface 는 Windows, macOS 및 Linux에서 지원됩니다. 에 대한 자세한 내용은 [AWS Command Line Interface 사용 설명서 단원](#)을 AWS CLI참조하세요. AWS SMS 명령 [AWS CLI 참조](#) 에서 명령을 찾을 수 있습니다.

AWS SDKs

HTTP 또는 를 통해 요청을 제출하는 APIs 대신 언어별 애플리케이션을 구축하는 것을 선호하는 소프트웨어 개발자인 경우 HTTPS는 라이브러리, 샘플 코드, 자습서 및 기타 리소스를 AWS 제공합니다. 이러한 라이브러리는 요청에 암호화 방식으로 서명, 요청을 재시도, 오류 응답 처리 등 태스크를 자동화하는 기본 함수를 제공합니다. 이러한 함수를 사용하면 시작하는 것이 더 효율적입니다. 자세한 내용은 [AWS기반의 도구](#)를 참조하세요.

리전별 가용성

AWS 최종 사용자 메시징 소셜은 북미, 유럽, 아시아 및 오세아니아 AWS 리전 의 여러 에서 사용할 수 있습니다. 각 리전에서 여러 가용 영역을 AWS 유지합니다. 이러한 가용 영역은 물리적으로 서로 분리되어 있지만, 지연 시간이 짧고 처리량과 중복성이 우수한 프라이빗 네트워크 연결로 통합됩니다. 이러한 가용 영역은 매우 높은 수준의 가용성과 중복성을 제공하는 동시에 지연 시간을 최소화하는 데 사용됩니다.

에 대한 자세한 내용은 에서 계정에서 사용할 수 있는 항목 지정을 AWS 리전참조하세요Amazon Web Services 일반 참조. [AWS 리전](#) AWS 최종 사용자 메시징 소셜을 현재 사용할 수 있는 모든 리전과 각 리전의 엔드포인트 목록은 Amazon Web Services 일반 참조 또는 다음 표의 AWS 최종 사용자 메시징 소셜 및 [AWS 서비스 엔드포인트](#)의 [엔드포인트 및 할당량](#)을 참조하세요. API 각 리전에서 사용할 수 있는 가용 영역 수에 대한 자세한 내용은 [AWS 글로벌 인프라](#)를 참조하세요.

리전 가용성

지역명	지역	엔드포인트	WhatsApp API 버전
미국 동부(버지니아 북부)	us-east-1	social-messaging.us-east-1.amazonaws.com	버전 20 이상
		social-messaging-fips.us-east-1.api.aws	
		social-messaging.us-east-1.api.aws	
미국 동부(오하이오)	us-east-2	social-messaging.us-east-2.amazonaws.com	버전 20 이상
		social-messaging-fips.us-east-2.api.aws	
		social-messaging.us-east-2.api.aws	

지역명	지역	엔드포인트	WhatsApp API 버전
미국 서부(오레곤)	us-west-2	social-messaging.us-west-2.amazonaws.com social-messaging-fips.us-west-2.api.aws social-messaging.us-west-2.api.aws	버전 20 이상
아시아 태평양(뭄바이)	ap-south-1	social-messaging.ap-south-1.amazonaws.com social-messaging.ap-south-1.api.aws	버전 20 이상
아시아 태평양(싱가포르)	ap-southeast-1	social-messaging.ap-southeast-1.amazonaws.com social-messaging.ap-southeast-1.api.aws	버전 20 이상
유럽(아일랜드)	eu-west-1	social-messaging.eu-west-1.amazonaws.com social-messaging.eu-west-1.api.aws	버전 20 이상
유럽(런던)	eu-west-2	social-messaging.eu-west-2.amazonaws.com social-messaging.eu-west-1.api.aws	버전 20 이상

AWS 최종 사용자 메시징 소셜 설정

AWS 최종 사용자 메시징 소셜을 처음 사용하려면 먼저 다음 단계를 완료해야 합니다.

주제

- [에 가입 AWS 계정](#)
- [관리자 액세스 권한이 있는 사용자 생성](#)
- [다음 단계](#)

에 가입 AWS 계정

가 없는 경우 다음 단계를 AWS 계정완료하여 를 생성합니다.

에 가입하려면 AWS 계정

1. <https://portal.aws.amazon.com/billing/가입> 을 엽니다.
2. 온라인 지시 사항을 따릅니다.

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

에 가입하면 AWS 계정AWS 계정 루트 사용자가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 [루트 사용자 액세스 권한이 필요한 작업](#)을 수행하는 것입니다.

AWS 는 가입 프로세스가 완료된 후 확인 이메일을 보냅니다. 언제든지 <https://aws.amazon.com/>로 이동하여 내 계정을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

에 가입한 후 일상적인 작업에 루트 사용자를 사용하지 않도록 를 AWS 계정보호하고, 를 AWS 계정 루트 사용자활성화하고 AWS IAM Identity Center, 관리 사용자를 생성합니다.

보안 AWS 계정 루트 사용자

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자 [AWS Management Console](#)로 에 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

루트 사용자를 사용하여 로그인하는 데 도움이 필요하다면 AWS 로그인 User Guide의 [루트 사용자 로 로그인](#)을 참조하십시오.

2. 루트 사용자에게 다중 인증(MFA)을 켭니다.

지침은 IAM 사용 설명서의 [AWS 계정 루트 사용자\(콘솔\)에 대한 가상 MFA 디바이스 활성화](#)를 참조하십시오.

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

지침은 AWS IAM Identity Center 사용 설명서의 [AWS IAM Identity Center 설정](#)을 참조하십시오.

2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

를 자격 증명 소스 IAM Identity Center 디렉터리로 사용하는 방법에 대한 자습서는 AWS IAM Identity Center 사용 설명서의 [기본값으로 사용자 액세스 구성을 IAM Identity Center 디렉터리](#) 참조하십시오.

관리 액세스 권한이 있는 사용자로 로그인

- IAM Identity Center 사용자로 로그인하려면 IAM Identity Center 사용자를 생성할 때 이메일 주소로 전송URL된 로그인을 사용합니다.

IAM Identity Center 사용자를 사용하여 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 [AWS 액세스 포털에 로그인](#)을 참조하십시오.

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

지침은 AWS IAM Identity Center 사용 설명서의 [Create a permission set](#)를 참조하십시오.

2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

지침은 AWS IAM Identity Center 사용 설명서의 [Add groups](#)를 참조하십시오.

다음 단계

이제 AWS 최종 사용자 메시징 소셜을 사용할 준비가 되었으므로 WhatsApp 비즈니스 계정(WABA)을 생성하거나 기존 WhatsApp 비즈니스 계정을 마이그레이션하려면 [AWS 최종 사용자 메시징 소셜 시작하기](#) 섹션을 참조하세요.

AWS 최종 사용자 메시징 소셜 시작하기

이 주제에서는 WhatsApp 비즈니스 계정(WABA)을 AWS 최종 사용자 메시징 소셜에 연결하거나 마이그레이션하는 단계를 안내합니다.

주제

- [에 가입 WhatsApp](#)

에 가입 WhatsApp

WhatsApp 비즈니스 계정(WABA)을 사용하면 비즈니스 WhatsApp 플랫폼을 사용하여 고객에게 직접 메시지를 보낼 수 있습니다. 모든 WABAs는 메타 비즈니스 포트폴리오의 일부입니다. 에는 전화번호, 템플릿, WhatsApp 비즈니스 프로필과 같은 고객 응대 자산이 WABA 포함되어 있습니다. WhatsApp 비즈니스 프로필에는 사용자가 볼 수 있는 비즈니스의 연락처 정보가 포함되어 있습니다. WhatsApp 비즈니스 계정에 대한 자세한 내용은 섹션을 참조하세요 [WhatsApp AWS 최종 사용자 메시징 소셜의 비즈니스 계정\(WABA\)](#).

이 섹션의 단계에 따라 AWS 최종 사용자 메시징 소셜을 시작합니다. 임베디드 가입 프로세스를 사용하여 새 WhatsApp 비즈니스 계정(WABA)을 생성하거나 기존 를 AWS 최종 사용자 메시징 소셜로 마이그레이션WABA합니다.

사전 조건

Important

Meta/ 작업WhatsApp

- WhatsApp 비즈니스 솔루션 사용에는 [WhatsApp 비즈니스 서비스 약관](#), [WhatsApp 비즈니스 솔루션 약관](#), [WhatsApp 비즈니스 메시징 정책](#), [WhatsApp 메시징 지침](#), 참조로 통합된 기타 모든 약관, 정책 또는 지침(각각 수시로 업데이트될 수 있음)의 약관이 적용됩니다.
- Meta 또는 WhatsApp 는 언제든지 WhatsApp 비즈니스 솔루션 사용을 금지할 수 있습니다.
- 메타 및 를 사용하여 WhatsApp 비즈니스 계정("WABA")을 생성해야 합니다 WhatsApp.
- Meta로 Business Manager 계정을 생성하고 에 연결해야 합니다WABA.
- 사용자는 WABA 당사에 에 대한 제어를 제공해야 합니다. 귀하의 요청에 따라 당사는 Meta 가 제공하는 방법을 사용하여 합리적이고 시기 적절한 방식으로 귀하의 WABA 등에 대한 제어를 귀하에게 이전합니다.

- WhatsApp 비즈니스 솔루션 사용과 관련하여 귀하는 관련 법률 및/또는 규정에 따라 배포를 보호 및/또는 제한해야 하는 콘텐츠, 정보 또는 데이터를 제출하지 않습니다.
- WhatsApp 비즈니스 솔루션 사용에 대한 의 가격은 [대화 기반 요금](#) 에서 확인할 수 있습니다.

- WhatsApp 비즈니스 계정(WABA)을 생성하려면 비즈니스에 [메타 비즈니스 계정](#) 가 필요합니다. 회사에 이미 메타 비즈니스 계정이 있는지 확인합니다. Meta Business 계정이 없는 경우 가입 프로세스 중에 계정을 생성할 수 있습니다.
- WhatsApp Messenger 애플리케이션 또는 WhatsApp Business 애플리케이션에서 이미 사용 중인 전화번호를 사용하려면 먼저 삭제해야 합니다.
- SMS 또는 음성 일회용 암호()를 수신할 수 있는 전화번호입니다OTP. 가입에 사용되는 전화번호는 WhatsApp 계정과 연결되며 메시지를 보낼 때 전화번호가 사용됩니다. 전화번호는 SMS, MMS 및 음성 메시징에 계속 사용할 수 있습니다.
- 기존 를 가져오는 경우 가져온 와 연결된 모든 전화번호에 PINs 대해 가 WABA 필요합니다WABA. 분실 또는 잊어버린 를 재설정하려면 WhatsApp 비즈니스 플랫폼 클라우드 API 참조의 [업데이트에 PIN](#) 있는 지침을 PIN 따르세요.

콘솔을 통해 가입

다음 지침에 따라 새 WhatsApp 계정을 생성하거나, 기존 계정을 마이그레이션하거나, 기존 에 전화번호를 추가합니다WABA. 가입 프로세스의 일환으로 AWS 최종 사용자 메시징 소셜에 WhatsApp 비즈니스 계정에 대한 액세스 권한을 부여합니다. 또한 AWS 최종 사용자 메시징 소셜에서 메시지에 대한 요금을 청구하도록 허용합니다. WhatsApp 비즈니스 계정에 대한 자세한 내용은 섹션을 참조하세요 [WhatsApp 비즈니스 계정 유형 이해](#).

1. 에서 AWS 최종 사용자 메시징 소셜 콘솔을 엽니다<https://console.aws.amazon.com/social-messaging/>.
2. 비즈니스 계정을 선택합니다.
3. 비즈니스 계정 연결 페이지에서 Facebook 포털 시작을 선택합니다. Meta의 새 로그인 창이 나타납니다.
4. 메타 로그인 창에서 Facebook 계정 자격 증명을 입력합니다.

WhatsApp 비즈니스 계정 페이지에서 전화번호 추가 WhatsApp를 선택합니다. WhatsApp 전화번호 추가 페이지에서 Facebook 포털 시작을 선택합니다. Meta의 새 로그인 창이 나타납니다.

5. 메타 로그인 창에서 Facebook 계정 자격 증명을 입력합니다.
6. 가입 프로세스의 일환으로 AWS 최종 사용자 메시징 소셜에 WhatsApp 비즈니스 계정()에 대한 액세스 권한을 부여합니다WABA. 또한 AWS 최종 사용자 메시징 소셜에서 메시지에 대한 요금을 청구하도록 허용합니다. 계속을 선택합니다.
7. Meta Business 계정 에서 기존 Meta 비즈니스 계정 또는 Meta Business 계정 생성 을 선택합니다.
 - a. (선택 사항) Meta Business 계정을 생성해야 하는 경우 다음 단계를 따르세요.
 - b. 비즈니스 이름 에 비즈니스 이름을 입력합니다.
 - c. 비즈니스 웹 사이트 또는 프로필 페이지에 회사 웹 사이트의 URL를 입력하거나 회사에 웹 사이트가 없는 경우 소셜 미디어 페이지에 URL를 입력합니다.
 - d. 국가 에서 사업체가 위치한 국가를 선택합니다.
 - e. (선택 사항) 주소 추가를 선택하고 회사 주소를 입력합니다.
8. Next(다음)를 선택합니다.
9. WhatsApp 비즈니스 계정 선택 에서 기존 WhatsApp 비즈니스 계정(WABA)을 선택하거나 계정을 생성해야 하는 경우 WhatsApp 비즈니스 계정 생성을 선택합니다.

WhatsApp 비즈니스 프로필 생성 또는 선택 에서 기존 WhatsApp 비즈니스 프로필 또는 새 WhatsApp 비즈니스 프로필 생성 을 선택합니다.

10. Next(다음)를 선택합니다.
11. 비즈니스 프로필 생성 에 다음 정보를 입력합니다.
 - WhatsApp 비즈니스 계정 이름 에 계정 이름을 입력합니다. 이 필드는 고객 응대 필드가 아닙니다.
 - WhatsApp 비즈니스 프로필 표시 이름 에 고객이 메시지를 받을 때 표시할 이름을 입력합니다. 회사 이름을 표시 이름으로 사용하는 것이 좋습니다. 이름은 Meta에서 검토하며 [WhatsApp 표시 이름 규칙](#)을 준수해야 합니다. 회사 이름과 다른 브랜드 이름을 사용하려면 회사와 브랜드 간에 외부에 게시된 연결이 있어야 합니다. 이 연결은 웹 사이트와 표시 이름의 웹 사이트로 표시되는 브랜드에 표시되어야 합니다.

등록을 완료하면 Meta는 표시 이름을 검토합니다. Meta는 표시 이름이 승인 또는 거부되었는지 여부를 알려주는 이메일을 보냅니다. 표시 이름이 거부되면 일별 메시징 한도가 낮아지고 에서 연결이 끊어질 수 있습니다 WhatsApp.

⚠ Important

표시 이름을 변경하려면 Meta 지원을 사용하여 티켓을 생성해야 합니다.

- 시간대 에서 비즈니스가 위치한 시간대를 선택합니다.
 - 범주 에서 비즈니스에 가장 적합한 범주를 선택합니다. 고객은 해당 범주를 연락처 정보의 일부로 볼 수 있습니다.
 - 비즈니스 설명 에 회사에 대한 설명을 입력합니다. 고객은 연락처 정보의 일부로 비즈니스 설명을 볼 수 있습니다.
 - 웹 사이트 에 회사 웹 사이트를 입력합니다. 고객은 웹 사이트를 연락처 정보의 일부로 볼 수 있습니다.
 - Next(다음)를 선택합니다.
12. 의 전화번호 추가 WhatsApp에 등록할 전화번호를 입력합니다. 이 전화번호는 메시지를 보낼 때 고객에게 표시됩니다.
13. 번호 확인 방법 선택에서 문자 메시지 또는 전화 통화를 선택합니다.
- 확인 코드를 받을 준비가 되면 다음을 선택합니다.
 - 확인 코드를 입력한 다음 다음을 선택합니다.
14. 번호가 확인되면 다음을 선택하여 Meta에서 창을 닫을 수 있습니다.
15. WhatsApp 비즈니스 계정의 경우 태그 확장 - 비즈니스 계정에 태그를 추가하는 선택 사항입니다.
- WhatsApp
- 태그는 액세스 또는 사용을 제어하기 위해 AWS 리소스에 선택적으로 적용할 수 있는 키와 값의 쌍입니다. 새 태그 추가를 선택하고 연결할 키-값 페어를 입력합니다.
16. WhatsApp 비즈니스 계정에는 비즈니스 계정 및 WhatsApp 비즈니스 계정에 연결된 모든 리소스에 대한 이벤트를 로깅할 수 있는 메시지와 이벤트 대상이 하나 있을 수 WhatsApp 있습니다. 고객 메시지 수신 로깅SNS을 포함하여 Amazon 에서 이벤트 로깅을 활성화하려면 메시지 및 이벤트 게시를 켜야 합니다. 자세한 내용은 [AWS 최종 사용자 메시징 소셜의 메시지 및 이벤트 대상](#) 단원을 참조하십시오.

⚠ Important

고객 메시지에 응답하려면 메시지 및 이벤트 게시를 활성화해야 합니다.

메시지 및 이벤트 대상 세부 정보 섹션에서 이벤트 게시를 엽니다. Amazon 의 경우 새 Amazon SNS 표준 주제를 SNS선택하고 주제 이름 에 이름을 입력하거나 기존 Amazon SNS 표준 주제를 선택하고 주제 삭제 드롭다운 목록에서 주제를 선택합니다.

17. 전화번호에서:

전화번호 아래의 각 WhtsApp 전화번호에 대해:

- a. 전화번호 확인 에 기존 코드를 입력PIN하거나 새 PIN 코드를 입력합니다. 분실 또는 잊어버린 를 재설정하려면 WhatsApp 비즈니스 플랫폼 클라우드 API 참조의 [업데이트PIN](#)에 있는 지침 을 PIN따르세요.
- b. 추가 설정의 경우:
 - i. 데이터 현지화 리전의 경우 - 선택 사항으로 저장 중인 데이터를 저장할 Meta의 리전 중 하나를 선택합니다. Meta의 데이터 개인 정보 보호 정책에 대한 자세한 내용은 비즈니스 플랫폼 클라우드 참조의 [데이터 개인 정보 보호 및 보안](#) 및 클라우드 로컬 스토리지를 참조하세요. [API](#) WhatsApp API
 - ii. 태그는 액세스 또는 사용을 제어하기 위해 AWS 리소스에 선택적으로 적용할 수 있는 키 와 값의 쌍입니다. 새 태그 추가를 선택하고 연결할 키-값 페어를 입력합니다.

18. WhatsApp 비즈니스 계정에는 비즈니스 계정 및 WhatsApp 비즈니스 계정에 연결된 모든 리소스 에 대한 이벤트를 로깅할 수 있는 메시지와 이벤트 대상이 하나 있을 수 WhatsApp 있습니다. 고객 메시지 수신 로깅SNS를 포함하여 Amazon 에서 이벤트 로깅을 활성화하려면 메시지 및 이벤트 게시를 켜야 합니다. 자세한 내용은 [AWS 최종 사용자 메시징 소셜의 메시지 및 이벤트 대상](#) 단원을 참조하십시오.

Important

고객 메시지에 응답하려면 메시지 및 이벤트 게시를 활성화해야 합니다.

메시지 및 이벤트 대상 세부 정보 섹션에서 이벤트 게시를 엽니다. Amazon 의 경우 새 Amazon SNS 표준 주제를 SNS선택하고 주제 이름 에 이름을 입력하거나 기존 Amazon SNS 표준 주제를 선택하고 주제 삭제 드롭다운 목록에서 주제를 선택합니다.

19. 설정을 완료하려면 전화번호 추가를 선택합니다.

다음 단계

가입을 완료하면 메시지 전송을 시작할 수 있습니다. 대규모로 메시지 전송을 시작할 준비가 되면 [비즈니스 검증](#)을 완료합니다. 이제 WhatsApp 비즈니스 계정과 AWS 최종 사용자 메시징 소셜 계정이 연결 되었으므로 다음 주제를 참조하세요.

- 이벤트를 로깅하고 수신 메시지를 수신할 이벤트 [대상](#)에 대해 알아봅니다.
- [메시지 템플릿](#)을 생성하는 방법을 알아봅니다.
- [텍스트 또는 미디어 메시지를 보내는](#) 방법을 알아봅니다.
- [메시지를 수신하는](#) 방법을 알아봅니다.
- 표시 이름 옆에 녹색 확인 표시가 있고 메시지 처리량을 늘리려면 [Official Business Accounts](#)에 대해 알아봅니다.

WhatsApp AWS 최종 사용자 메시징 소셜의 비즈니스 계정 (WABA)

WhatsApp 비즈니스 계정(WABA)을 사용하면 비즈니스 WhatsApp 플랫폼을 사용하여 고객에게 직접 메시지를 보낼 수 있습니다. 모든 WABAs는 [메타 비즈니스 포트폴리오](#)의 일부입니다. WhatsApp 비즈니스 계정에는 전화번호, 템플릿 및 비즈니스 연락처 정보와 같은 고객 응대 자산이 포함되어 있습니다. 는 하나의에만 존재할 WABA 수 있습니다 AWS 리전. WhatsApp 비즈니스 계정에 대한 자세한 내용은 [WhatsApp 비즈니스 플랫폼 클라우드 참조의 비즈니스 계정을 참조하세요](#). WhatsApp API

⚠ Important

Meta/ 작업WhatsApp

- WhatsApp 비즈니스 솔루션 사용에는 [WhatsApp 비즈니스 서비스 약관](#), [WhatsApp 비즈니스 솔루션 약관](#), [WhatsApp 비즈니스 메시징 정책](#), [WhatsApp 메시징 지침](#), 참조로 통합된 기타 모든 약관, 정책 또는 지침(각각 수시로 업데이트될 수 있음)의 약관이 적용됩니다.
- Meta 또는 WhatsApp 는 언제든지 WhatsApp 비즈니스 솔루션 사용을 금지할 수 있습니다.
- 메타 및 를 사용하여 WhatsApp 비즈니스 계정("WABA")을 생성해야 합니다 WhatsApp.
- Meta를 사용하여 Business Manager 계정을 생성하고 에 연결해야 합니다WABA.
- 사용자는 WABA 당사에 에 대한 제어를 제공해야 합니다. 귀하의 요청에 따라 당사는 Meta 가 제공하는 방법을 사용하여 합리적이고 시기 적절한 방식으로 귀하의 WABA 등에 대한 제어를 귀하에게 이전합니다.
- WhatsApp 비즈니스 솔루션 사용과 관련하여 귀하는 관련 법률 및/또는 규정에 따라 배포를 보호 및/또는 제한해야 하는 콘텐츠, 정보 또는 데이터를 제출하지 않습니다.
- WhatsApp WhatsApp 비즈니스 솔루션 사용에 대한 의 가격은 <https://developers.facebook.com/docs/whatsapp/pricing> 에서 확인할 수 있습니다.

주제

- [AWS 최종 사용자 메시징 소셜에서 WhatsApp 비즈니스 계정\(WABA\) 보기](#)
- [AWS 최종 사용자 메시징 소셜에 WhatsApp 비즈니스 계정\(WABA\) 추가](#)
- [WhatsApp 비즈니스 계정 유형 이해](#)

AWS 최종 사용자 메시징 소셜에서 WhatsApp 비즈니스 계정 (WABA) 보기

다음 지침에 따라 사용자와 WABA 연결된 를 확인합니다 AWS 계정.

1. 에서 AWS 최종 사용자 메시징 소셜 콘솔을 엽니다 <https://console.aws.amazon.com/social-messaging/>.
2. 비즈니스 계정에서 을 선택합니다 WABA.
3. 전화번호 탭에서 전화번호, 표시 이름, 품질 등급, 하루 동안 남긴 비즈니스 시작 대화 수를 확인합니다.

이벤트 대상 탭에서 이벤트 대상을 확인합니다. 이벤트 대상을 편집하려면 의 지침을 따르세요 [AWS 최종 사용자 메시징 소셜의 메시지 및 이벤트 대상](#).

템플릿 탭에서 메시지 템플릿 관리를 선택하여 메타를 통해 WhatsApp 템플릿을 편집합니다. 각 템플릿 WABA에는 250개의 템플릿 제한이 있습니다.

태그 탭에서 WABA 리소스 태그를 관리할 수 있습니다.

AWS 최종 사용자 메시징 소셜에 WhatsApp 비즈니스 계정(WABA) 추가

WhatsApp 비즈니스 프로필이 이미 있는 경우 WABA 계정에 새 을 추가합니다. 새 를 생성하려면 에 [전화번호](#)를 추가 WABA해야 합니다 WABA.

- WABA 계정에 새 를 추가하려면 의 단계를 따릅니다 [AWS 최종 사용자 메시징 소셜 시작하기](#).
 - 8단계에서 WhatsApp 비즈니스 프로필을 선택하고 새 WhatsApp 비즈니스 계정 생성 을 선택합니다.

WhatsApp 비즈니스 계정 유형 이해

WhatsApp 비즈니스 계정은 고객에게 어떻게 표시되는지 결정합니다. WhatsApp 계정을 생성하면 계정은 비즈니스 계정이 됩니다. WhatsApp 에는 두 가지 유형의 비즈니스 계정이 있습니다.

- 비즈니스 계정 : WhatsApp 비즈니스 플랫폼의 모든 계정의 신뢰성을 WhatsApp 확인합니다. 비즈니스 계정이 비즈니스 확인 프로세스를 완료한 경우 사용자가 주소록에 비즈니스를 추가하지 않았더

라도 비즈니스 이름이 사용자에게 표시됩니다. 이 기능은 사용자가 에서 확인된 비즈니스 계정을 식별하는 데 도움이 됩니다 WhatsApp.

- 공식 비즈니스 계정 : 공식 비즈니스 계정에는 비즈니스 계정의 이점과 함께 프로필 및 채팅 스레드 헤더에 녹색 체크마크 배지가 있습니다.

WhatsApp 공식 비즈니스 계정(OBA)에 대한 승인을 받으려면 기사, 블로그 게시물 또는 독립 검토를 통해 비즈니스가 잘 알려져 있고 소비자의 인정을 받는다는 증거를 제공해야 합니다. 비즈니스에서 필수 문서를 제공하더라도 WhatsApp OBA에 대한 승인은 보장되지 않습니다. 승인 프로세스는 의 검토 및 승인을 받아야 합니다 WhatsApp. 는 공식 비즈니스 계정의 애플리케이션을 평가하고 승인하는 데 사용하는 특정 기준을 공개적으로 공개하지 않습니다. 를 WhatsApp OBA 찾는 기업은 평판과 인정을 입증해야 하지만 최종 승인은 의 재량에 따릅니다 WhatsApp.

WhatsApp 계정을 생성하면 계정이 비즈니스 계정 가 됩니다. 웹 사이트, 주소 및 시간과 같은 비즈니스에 대한 정보를 고객에게 제공할 수 있습니다. WhatsApp 비즈니스 확인을 완료하지 않은 기업의 경우 표시 이름은 채팅 목록 또는 개별 채팅이 아닌 연락처 보기의 전화번호 옆에 작은 텍스트로만 표시됩니다. Meta Business Verification이 완료되면 WhatsApp 발신자의 표시 이름이 채팅 목록과 개별 채팅 스레드에 표시됩니다.

추가 리소스

- 비즈니스 계정 및 공식 비즈니스 계정 에 대한 자세한 내용은 [비즈니스 플랫폼 클라우드 참조의 비즈니스 계정을 참조하세요](#). WhatsApp API
- 비즈니스 확인 프로세스에 대한 자세한 내용은 비즈니스 WhatsApp 플랫폼 클라우드 API 참조의 [비즈니스 확인을](#) 참조하세요.

AWS 최종 사용자 메시징 소셜의 전화번호

모든 WhatsApp 비즈니스 계정에는 를 사용하여 WhatsApp 자격 증명을 확인하는 데 사용되는 전화번호가 하나 이상 포함되어 있으며 전송 자격 증명의 일부로 사용됩니다. WhatsApp 비즈니스 계정 (WABA)과 연결된 전화번호가 여러 개 있고 다른 브랜드에 각 전화번호를 사용할 수 있습니다.

주제

- [WhatsApp 비즈니스 계정과 함께 사용할 때 전화번호 고려 사항](#)
- [WhatsApp 비즈니스 계정에 전화번호 추가\(WABA\)](#)
- [전화번호 상태 보기](#)
- [AWS 최종 사용자 메시징 소셜에서 전화번호의 ID 보기](#)
- [에서 메시징 대화 제한 증가 WhatsApp](#)
- [에서 메시지 처리량 증가 WhatsApp](#)
- [의 전화번호 품질 등급 이해 WhatsApp](#)

WhatsApp 비즈니스 계정과 함께 사용할 때 전화번호 고려 사항

전화번호를 WhatsApp 비즈니스 계정(WABA)과 연결할 때는 다음 사항을 고려해야 합니다.

- 전화번호는 WABA 한 번에 하나씩만 연결할 수 있습니다.
- 전화번호는 SMS, MMS 및 음성 통화에 계속 사용할 수 있습니다.
- 각 전화번호는 Meta의 품질 등급을 갖습니다.

다음은 SMS 수행하여 AWS 최종 사용자 메시징을 통해 SMS 가능한 전화번호를 얻을 수 있습니다.

1. 전화번호의 [국가 또는 리전](#)이 양방향 를 지원하는지 확인합니다 SMS.
2. [전화번호를](#) 요청합니다. 국가 또는 지역에 따라 전화번호를 등록해야 할 수 있습니다.
3. 전화번호에 [양방향 SMS 메시징을 활성화합니다](#). 설정이 완료되면 수신 SMS 메시지가 이벤트 대상으로 전송됩니다.

WhatsApp 비즈니스 계정에 전화번호 추가(WABA)

기존 WhatsApp 비즈니스 계정(WABA)에 전화번호를 추가하거나 전화번호에 WABA 대한 새 를 생성할 수 있습니다.

사전 조건

시작하기 전에 다음 사전 조건을 충족해야 합니다.

- 전화번호는 SMS 또는 음성 일회용 암호()를 수신할 수 있어야 합니다OTP. 에 추가된 전화번호입니다WABA.
- 전화번호는 다른 와 연결되어서는 안 됩니다WABA.

에 전화번호 추가 WABA

기존 에 새 전화번호를 추가하려면 WABA

1. 에서 AWS 최종 사용자 메시징 소셜 콘솔을 엽니다<https://console.aws.amazon.com/social-messaging/>.
2. 비즈니스 계정을 선택한 다음 전화번호 추가 WhatsApp 를 선택합니다.
3. WhatsApp 전화번호 추가 페이지에서 Facebook 포털 시작을 선택합니다. Meta의 새 로그인 창이 나타납니다.
4. 메타 로그인 창에서 메타 개발자 계정 자격 증명을 입력하고 비즈니스 포트폴리오를 선택합니다.
5. 전화번호를 추가할 WABA 및 WhatsApp 비즈니스 프로필을 선택합니다.
6. Next(다음)를 선택합니다.
7. 의 전화번호 추가 WhatsApp에 등록할 전화번호를 입력합니다. 이 전화번호는 메시지를 보낼 때 고객에게 표시됩니다.
8. 번호 확인 방법 선택에서 문자 메시지 또는 전화 통화를 선택합니다.
9. 확인 코드를 받을 준비가 되면 다음을 선택합니다.
10. 확인 코드를 입력한 다음 다음 를 선택합니다. 번호가 확인되면 다음을 선택하여 Meta에서 창을 닫을 수 있습니다.
11. WhtsApp 전화번호에서:
 - a. 전화번호 확인 에 기존 코드를 입력PIN하거나 새 PIN 코드를 입력합니다. 분실 또는 잊어버린 를 재설정하려면 WhatsApp 비즈니스 플랫폼 클라우드 API 참조의 [업데이트에 PIN](#) 있는 지침을 PIN따르세요.
 - b. 추가 설정의 경우:
 - i. 데이터 현지화 리전 - 선택 사항인 의 경우 저장 데이터를 저장할 Meta의 리전 중 하나를 선택합니다. Meta의 데이터 프라이버시 정책에 대한 자세한 내용은 비즈니스 플랫폼

클라우드 참조의 [데이터 프라이버시 및 보안](#) 및 클라우드 로컬 스토리지를 참조하세요.

[API](#) WhatsApp API

- ii. 태그는 액세스 또는 사용을 제어하기 위해 AWS 리소스에 선택적으로 적용할 수 있는 키와 값의 쌍입니다. 새 태그 추가를 선택하고 연결할 키-값 페어를 입력합니다.
12. WhatsApp 비즈니스 계정에는 비즈니스 계정 및 WhatsApp 비즈니스 계정과 연결된 모든 리소스에 대한 이벤트를 로깅하는 메시지와 이벤트 대상이 하나 있을 수 있습니다. 고객 메시지 수신 로깅SNS를 포함하여 Amazon에서 이벤트를 로깅을 활성화하려면 메시지 및 이벤트 게시를 켭니다. 자세한 내용은 [AWS 최종 사용자 메시징 소셜의 메시지 및 이벤트 대상](#) 단원을 참조하십시오.

Important

고객 메시지에 응답하려면 메시지 및 이벤트 게시를 활성화해야 합니다.

메시지 및 이벤트 대상 세부 정보 섹션에서 이벤트를 게시를 켭니다. Amazon의 경우 새 Amazon SNS 표준 주제를 SNS선택하고 주제 이름에 이름을 입력하거나 기존 Amazon SNS 표준 주제를 선택하고 주제 삭제 드롭다운 목록에서 주제를 선택합니다.

13. 설정을 완료하려면 전화번호 추가를 선택합니다.

전화번호 상태 보기

AWS 최종 사용자 메시징 소셜에서 메시지를 보내려면 전화번호의 상태가 활성이어야 합니다.

1. 에서 AWS 최종 사용자 메시징 소셜 콘솔을 엽니다 <https://console.aws.amazon.com/social-messaging/>.
2. Phone numbers(전화 번호)를 선택합니다.
3. 전화번호 섹션에서 상태 열에는 각 전화번호의 상태가 있습니다.

Note

전화번호의 상태가 설정 미완료인 경우 전화번호를 선택한 다음 설정 완료를 선택하여 전화번호 설정을 완료할 수 있습니다.

AWS 최종 사용자 메시징 소셜에서 전화번호의 ID 보기

로 메시지를 보내려면 전송할 때 사용할 전화번호를 식별하는 전화번호 ID가 AWS CLI 필요합니다.

1. 에서 AWS 최종 사용자 메시징 소셜 콘솔을 엽니다 <https://console.aws.amazon.com/social-messaging/>.
2. Phone numbers(전화 번호)를 선택합니다.
3. 전화번호 섹션에서 전화번호를 선택합니다.
4. 전화번호 세부 정보 섹션에는 전화번호의 전화번호 ID가 포함되어 있습니다.

에서 메시징 대화 제한 증가 WhatsApp

메시징 제한은 24시간 동안 회사 전화번호가 열 수 있는 최대 업무 시작 대화 수를 나타냅니다. 회사 전화번호는 처음에 24시간 이동 기간 동안 250개의 업무 시작 대화로 제한됩니다. 이 제한은 메시지의 품질 등급과 보내는 메시지 수에 따라 Meta에서 늘릴 수 있습니다. 비즈니스 시작 대화는 템플릿 메시지만 사용할 수 있습니다.

고객이 메시지를 보내면 24시간 서비스 창이 열립니다. 이 시간 동안 모든 [메시지 유형](#)을 보낼 수 있습니다.

다음 지침에 따라 메시징 한도를 1,000개의 메시지로 늘릴 수 있습니다.

- 회사 전화번호는 [활성 상태](#)여야 합니다.
- 회사 전화번호의 [품질 등급이 낮은](#) 경우 품질 등급이 개선될 때까지 하루에 250개의 비즈니스 시작 대화로 제한될 수 있습니다.
- [Business Verification](#)을 신청합니다. 비즈니스가 승인되면 메시징 품질이 분석되어 메시징 활동이 메시징 한도를 늘려야 하는지 확인합니다. 분석에 따라 메시징 한도 증가 요청은 Meta에서 승인하거나 거부합니다.
- [Identity Verification](#)을 신청합니다. 자격 증명 확인을 완료하고 자격 증명이 확인되면 Meta는 메시징 한도 증가를 승인합니다.
- 품질 등급이 높은 템플릿을 사용하여 30일 이동 기간 동안 1,000개 이상의 비즈니스 시작 대화를 엽니다. 1,000회의 대화 임계값에 도달하면 메시징 품질이 분석되어 메시징 활동이 메시징 한도를 늘려야 하는지 확인합니다. 목표는 고품질 메시지를 일관되게 전송하여 잠재적으로 메시징 한도를 늘리는 것입니다.

비즈니스 확인 또는 자격 증명 확인을 완료했거나 1,000개 이상의 비즈니스 대화를 열었지만 여전히 250개의 비즈니스 시작 대화로 제한된 경우 메시지 계층 업그레이드를 위해 Meta에 요청을 제출합니다.

비즈니스 또는 자격 증명 확인이 거부되면 고품질 메시지를 보내 승인을 받을 가능성을 높일 수 있습니다. 고품질, 규정 준수 및 옵트인 메시지를 전송하면 메시징 활동 및 품질이 재평가되어 승인된 메시징 기능이 증가할 수 있습니다.

의 메시징 품질 점수는 최근 사용자 피드백 및 상호 작용을 기반으로 계산되며, 최신 데이터에 더 많은 가중치가 부여 WhatsApp 됩니다. 이를 통해 플랫폼에서 메시징의 전반적인 품질과 신뢰성을 평가할 수 있습니다.

메시지 제한 수준 증가

- 1K 비즈니스 주도 대화
- 10K000개의 비즈니스 시작 대화
- 100K 비즈니스 시작 대화
- 무제한의 비즈니스 시작 대화

에서 메시지 처리량 증가 WhatsApp

메시지 처리량은 전화번호의 초당 수신 및 발신 메시지 수(MPS)입니다. 기본적으로 각 전화번호는 80MPS입니다. 다음 요구 사항을 충족하는 경우 Meta는 를 1,000MPS으로 늘릴 수 있습니다.

- 전화번호는 [비즈니스에서 시작한 대화를](#) 무제한으로 보낼 수 있어야 합니다.
- 전화번호의 [품질 등급](#)은 중간 이상이어야 합니다.

의 전화번호 품질 등급 이해 WhatsApp

전화번호 및 메시지의 품질은 Meta에서 결정합니다. 메시징 품질 점수는 지난 7일 동안 고객이 메시지를 수신한 방식을 기반으로 하며, 최근 메시지는 가중치가 더 많이 적용됩니다. 메시징 품질 점수는 사용자와 WhatsApp 사용자 간의 대화에서 얻은 품질 신호의 조합을 기반으로 계산됩니다. 이러한 신호에는 블록, 보고서 및 사용자가 비즈니스를 차단할 때 제공하는 이유와 같은 사용자 피드백이 포함됩니다. Meta는 최근 피드백 및 상호 작용에 WhatsApp중점을 두고 고객이 에서 메시지를 얼마나 잘 수신하는지 기준으로 메시지의 품질을 평가합니다.

WhatsApp 전화번호 품질 등급

- 녹색: 고품질
- 노란색: 중간 품질
- 빨간색: 낮은 품질

WhatsApp 전화번호 상태

- 연결됨 : 메시지 제한 내에서 메시지를 보낼 수 있습니다.
- 플래그 지정 : 전화번호 품질이 낮으므로 개선해야 합니다. 7일 후에도 전화 품질이 개선되지 않으면 전화 번호 상태가 연결됨으로 변경되지만 비즈니스에서 시작한 대화 한도는 한 단계 낮아집니다.
- 제한됨 : 현재 24시간 동안 비즈니스 시작 대화 한도에 도달했지만 수신되는 고객 메시지에 계속 응답할 수 있습니다. 24시간이 지나면 메시지를 다시 보낼 수 있습니다.

전화번호 품질 등급 보기

전화번호 품질을 보려면 다음 지침을 따르세요.

1. 에서 AWS 최종 사용자 메시징 소셜 콘솔을 엽니다 <https://console.aws.amazon.com/social-messaging/>.
2. 비즈니스 계정에서 을 선택합니다 WABA.
3. 전화번호 탭에서 전화번호, 표시 이름, 품질 등급, 하루 동안 남긴 비즈니스 시작 대화 수를 확인합니다.

AWS 최종 사용자 메시징 소셜에서 메시지 템플릿 사용

주간 뉴스레터 또는 예약 알림과 같이 자주 사용하는 메시지 유형에 메시지 템플릿을 사용할 수 있습니다. 템플릿 메시지는 아직 메시지를 보내지 않았거나 지난 24시간 동안 메시지를 보내지 않은 고객에게 보낼 수 있는 유일한 유형의 메시지입니다.

Meta는 각 템플릿에 품질 등급과 상태를 할당합니다. 품질 등급은 템플릿의 상태에 영향을 미치고 템플릿의 페이싱 또는 전송 속도를 낮춥니다.

템플릿은 WhatsApp 비즈니스 계정(WABA)과 연결되고, WhatsApp 관리자를 통해 관리되며, 에서 검토합니다 WhatsApp.

다음 템플릿 유형을 보낼 수 있습니다.

- 텍스트 기반
- 미디어 기반
- 대화형 메시지
- 위치 기반
- 일회용 암호 버튼이 있는 인증 템플릿
- 다중 제품 메시지 템플릿

Meta는 사전 승인된 샘플 템플릿을 제공합니다. 자세한 내용은 [샘플 메시지 템플릿 섹션](#)을 참조하세요.

메시지 템플릿 유형에 대한 자세한 내용은 WhatsApp 비즈니스 플랫폼 클라우드 API 참조의 [메시지 템플릿](#)을 참조하세요.

Manager에서 WhatsApp 메시지 템플릿 사용

[WhatsApp Manager](#)를 사용하여 템플릿 상태를 생성, 수정 또는 확인합니다.

1. 에서 AWS 최종 사용자 메시징 소셜 콘솔을 엽니다 <https://console.aws.amazon.com/social-messaging/>.
2. 비즈니스 계정을 선택한 다음 WABA를 선택합니다.
3. 메시지 템플릿 탭에서 메시지 템플릿 관리를 선택합니다. [WhatsApp 관리자](#)는 새 창에서 열리며, 여기서 메시지 템플릿을 선택하여 템플릿을 관리할 수 있습니다.

다음 단계

템플릿을 생성하거나 편집한 후에는 에서 검토할 수 있도록 템플릿을 제출해야 합니다 WhatsApp. Meta의 검토에는 최대 24시간이 걸릴 수 있습니다. Meta는 비즈니스 관리자 관리자에게 이메일을 보내고 WhatsApp 관리자의 템플릿 상태를 업데이트합니다. [WhatsApp 관리자](#)를 사용하여 템플릿의 상태를 확인합니다.

의 템플릿 페이싱 이해 WhatsApp

템플릿 페이싱은 Meta에서 사용하는 메서드로, 새 템플릿 또는 수정된 템플릿에 대한 초기 고객 피드백을 위한 시간을 허용합니다. 참여도나 피드백이 좋지 않은 템플릿을 식별하여 일시 중지하므로 너무 많은 고객에게 보내기 전에 템플릿 콘텐츠를 조정할 수 있습니다. 이렇게 하면 부정적인 고객 피드백이 비즈니스에 영향을 미칠 위험이 줄어듭니다. 예를 들어 너무 많은 고객이 메시지를 “차단”하거나 템플릿의 읽기 속도가 낮은 경우 템플릿 품질 등급을 낮출 수 있습니다.

템플릿 페이싱은 새로 생성된 템플릿, 일시 중지되지 않은 템플릿 및 고품질 등급이 없는 템플릿에 영향을 미칩니다. 템플릿 페이싱은 품질이 낮거나 일시 중지된 템플릿의 이전 기록에서 시작되는 경우가 많습니다. 템플릿의 속도가 조정되면 해당 템플릿을 사용하는 메시지는 메타에서 결정한 특정 임계값까지 정상적으로 전송됩니다. 그런 다음 고객 피드백을 받을 시간을 허용하기 위해 후속 메시지가 보류됩니다. 피드백이 긍정적이면 템플릿 페이싱이 스케일 업됩니다. 피드백이 음수인 경우 템플릿 페이싱이 낮아져 템플릿 콘텐츠를 조정할 수 있습니다. 자세한 내용은 WhatsApp 비즈니스 플랫폼 클라우드 API 참조의 [템플릿 페이싱](#)을 참조하세요.

WhatsApp Manager를 사용하여 템플릿의 낮아진 상태에 대한 피드백 받기

Meta는 템플릿 상태가 낮아진 이유에 대한 정보를 제공합니다. Meta의 피드백을 사용하여 템플릿을 편집하고 재승인을 위해 제출하거나, 다른 템플릿을 사용하거나, 애플리케이션의 동작을 변경합니다. 메시지 템플릿을 편집하고 다시 승인하면 자주 부정적인 피드백이나 낮은 읽기 속도를 받지 않는 한 품질 등급이 점진적으로 개선됩니다.

1. 에서 AWS 최종 사용자 메시징 소셜 콘솔을 엽니다 <https://console.aws.amazon.com/social-messaging/>.
2. 비즈니스 계정을 선택한 다음 를 선택합니다 WABA.
3. 메시지 템플릿 탭에서 메시지 템플릿 관리를 선택합니다. [WhatsApp 관리자](#)가 새 창에서 열립니다.

4. 메시지 템플릿을 선택하고 템플릿 위에 마우스를 올려 놓습니다. 등급이 낮아진 이유에 대한 피드백과 함께 도구 설명이 나타나야 합니다.

에서 템플릿의 상태 및 품질 등급 이해 WhatsApp

각 메시지 템플릿에는 사용량, 고객 피드백 및 고객 참여를 기반으로 품질 등급이 할당됩니다. 템플릿은 상태가 활성화지만 품질에 따라 템플릿 페이싱이 결정되는 경우에만 사용할 수 있습니다. 메시지 템플릿이 지속적으로 부정적인 피드백을 받거나 참여도가 낮은 경우 템플릿 상태가 변경됩니다.

Meta는 부정적 또는 긍정적 피드백과 참여를 기반으로 템플릿의 상태 또는 품질 등급을 자동으로 변경합니다. 템플릿 상태가 변경되면 WhatsApp 관리자 알림, 이메일 및 이벤트 알림을 받게 됩니다.

[WhatsApp 관리자](#)를 사용하여 템플릿의 상태를 확인합니다.

에서 템플릿을 거부하는 경우 템플릿을 편집하고 승인을 위해 다시 제출하거나 에 항의를 제출할 수 있습니다 WhatsApp. 자세한 내용은 WhatsApp 비즈니스 플랫폼 클라우드 API 참조의 [항의](#)를 참조하세요.

템플릿 상태	품질 등급	의미
검토 중		메시지 템플릿을 검토 중입니다. 완료하는 데 최대 24시간이 걸릴 수 있습니다.
거부됨		메시지 템플릿이 거부되었으며 항의를 제출할 수 있습니다.
활성	보류중	메시지 템플릿은 고객으로부터 품질 피드백 또는 읽기 속도 정보를 받지 못했지만 여전히 템플릿을 사용하여 메시지를 보낼 수 있습니다.
활성	높음	메시지 템플릿은 부정적인 고객 피드백을 거의 또는 전혀 받지 못했으며 메시지를 보내는 데 사용할 수 있습니다.

템플릿 상태	품질 등급	의미
활성	중간	메시지 템플릿이 고객으로부터 부정적인 피드백 또는 낮은 읽기 속도를 받았으며 일시 중지되거나 꺼질 수 있습니다.
활성	낮음	메시지 템플릿이 고객으로부터 부정적인 피드백 또는 낮은 읽기 속도를 받았습니다. 이 상태의 메시지 템플릿을 사용할 수 있지만 일시 중지되거나 비활성화될 위험이 있습니다. 템플릿이 Active-Low 상태로 이동하면 전송이 일시 중지됩니다. 첫 번째 일시 중지는 3시간이고, 두 번째 일시 중지는 6시간이며, 다음 일시 중지는 템플릿을 비활성화합니다.
Paused		고객의 반복적인 부정적인 피드백 또는 낮은 읽기 속도로 인해 메시지 템플릿이 일시 중지되었습니다.
Disabled(비활성)		고객의 부정적인 피드백이 반복되어 메시지 템플릿이 비활성화되었습니다.
항의 요청됨		항의가 요청되었습니다.

에서 템플릿이 거부되는 이유 WhatsApp

Meta에서 메시지 템플릿을 검토하고 거부하는 경우 템플릿이 거부된 이유를 설명하는 이메일을 받게 됩니다. 거부에 이의를 제기하거나 메시지 템플릿을 수정할 수 있습니다. 다음은 Meta가 메시지 템플릿을 거부할 수 있는 몇 가지 일반적인 이유입니다.

- 변수 파라미터에는 #, \$ 또는 %와 같은 특수 문자가 포함되어 있습니다.
- 변수 파라미터가 누락되었거나, 쉼표 브레이스가 일치하지 않거나, 순차적이지 않습니다.
- 메시지 템플릿에는 [WhatsApp 상거래 정책](#) 또는 [WhatsApps 비즈니스 정책](#) 을 위반하는 콘텐츠가 포함되어 있습니다.

자세한 내용은 WhatsApp 비즈니스 플랫폼 클라우드 API 참조의 [일반적인 거부 이유](#) 를 참조하세요.

AWS 최종 사용자 메시징 소셜의 메시지 및 이벤트 대상

이벤트 대상은 WhatsApp 이벤트가 전송되는 Amazon SNS 주제입니다. Amazon SNS 주제에 이벤트 게시를 켜면 모든 송수신 이벤트가 Amazon SNS 주제로 전송됩니다. 이벤트를 사용하여 아웃바운드 메시지 및 수신 고객 커뮤니케이션의 상태를 모니터링, 추적 및 분석합니다.

각 WhatsApp 비즈니스 계정(WABA)에는 하나의 이벤트 대상이 있을 수 있습니다. WhatsApp 비즈니스 계정에 연결된 모든 리소스의 모든 이벤트는 해당 이벤트 대상으로 로깅됩니다. 예를 들어 3개의 전화번호가 연결된 WhatsApp 비즈니스 계정이 있을 수 있으며 해당 전화번호의 모든 이벤트는 하나의 이벤트 대상으로 기록됩니다.

주제

- [AWS 최종 사용자 메시징 소셜에 메시지 및 이벤트 대상 추가](#)
- [AWS 최종 사용자 메시징 소셜의 메시지 및 이벤트 형식](#)
- [WhatsApp 메시지 상태](#)

AWS 최종 사용자 메시징 소셜에 메시지 및 이벤트 대상 추가

메시지 및 이벤트 게시를 켜면 WhatsApp 비즈니스 계정(WABA)에서 생성된 모든 이벤트가 Amazon SNS 주제로 전송됩니다. 여기에는 WhatsApp 비즈니스 계정과 연결된 각 전화번호에 대한 이벤트가 포함됩니다. 하나의 Amazon SNS 주제가 연결될 WABA 수 있습니다.

사전 조건

시작하기 전에 다음 사전 조건을 충족해야 합니다.

- (선택 사항) AWS KMS 키를 사용하여 암호화된 Amazon SNS 주제를 사용하려면 [기존 키 정책](#)에 AWS 최종 사용자 메시징 소셜 권한을 부여해야 합니다.

메시지 및 이벤트 대상 추가

1. 에서 AWS 최종 사용자 메시징 소셜 콘솔을 엽니다 <https://console.aws.amazon.com/social-messaging/>.
2. 비즈니스 계정을 선택한 다음 WABA를 선택합니다.
3. 이벤트 대상 탭에서 대상 편집을 선택합니다.

4. 이벤트를 대상으로 켜려면 활성화를 선택합니다.
5. 이벤트를 새 Amazon SNS 대상으로 보내려면 새 SNS 스탠드 주제를 선택하고 주제 이름에 이름을 입력합니다. Amazon SNS 주제는 AWS 최종 사용자 메시징 소셜이 주제에 액세스할 수 있는 권한을 사용하여 생성됩니다.

이벤트를 기존 Amazon SNS 대상으로 보내려면 기존 SNS 표준 주제를 선택하고 주제 양식 주제 arn 을 선택합니다. Amazon SNS 주제에 다음 권한을 적용해야 합니다.

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": [
      "social-messaging.amazonaws.com"
    ]
  },
  "Action": "sns:Publish",
  "Resource": "arn:{PARTITION}:sns:{REGION}:{ACCOUNT}:{TOPIC_NAME}"
}
```

6. Save changes(변경 사항 저장)를 선택합니다.

암호화된 Amazon SNS 주제 정책

추가 보안 수준을 위해 AWS KMS 키를 사용하여 암호화된 Amazon SNS 주제를 사용할 수 있습니다. 애플리케이션에서 비공개 또는 민감한 데이터를 처리하는 경우 이 추가된 보안이 유용할 수 있습니다. AWS KMS 키를 사용하여 Amazon SNS 주제를 암호화하는 방법에 대한 자세한 내용은 Amazon Simple Notification Service 개발자 안내서의 [AWS 서비스에서 이벤트 소스와 암호화된 주제 간의 호환성 활성화](#)를 참조하세요.

예제 문은 선택 사항이지만 권장 사항 SourceAccount인 및 SourceArn 조건을 사용하여 혼동된 대리자 문제를 방지하고 AWS 최종 사용자 메시징 소셜 소유자 계정만 액세스할 수 있습니다. 혼동된 대리자 문제에 대한 자세한 내용은 [IAM 사용 설명서](#)의 [혼동된 대리자 문제를](#) 참조하세요.

사용하는 키는 대칭 이어야 합니다. 암호화된 Amazon SNS 주제는 비대칭 AWS KMS 키를 지원하지 않습니다.

AWS 최종 사용자 메시징 소셜에서 키를 사용하도록 허용하려면 키 정책을 수정해야 합니다. AWS Key Management Service 개발자 안내서의 [키 정책 변경](#)의 지침에 따라 기존 키 정책에 다음 권한을 추가합니다.

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": "social-messaging.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey*",
    "kms:Decrypt"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "{ACCOUNT_ID}"
    },
    "ArnLike": {
      "aws:SourceArn": "arn:{PARTITION}:social-messaging:{REGION}:{ACCOUNT_ID}:*"
    }
  }
}
```

다음 단계

Amazon SNS 주제를 설정한 후에는 해당 주제에 대한 엔드포인트를 구독해야 합니다. 엔드포인트는 연결된 주제에 게시된 메시지를 수신하기 시작합니다. 주제 구독에 대한 자세한 내용은 [Amazon 개발자 안내서의 Amazon SNS 주제 구독](#)을 참조하세요. SNS

AWS 최종 사용자 메시징 소셜의 메시지 및 이벤트 형식

이벤트의 JSON 객체에는 AWS 이벤트 헤더와 WhatsApp JSON 페이로드가 포함됩니다. JSON WhatsApp 알림 페이로드 및 값 목록은 비즈니스 플랫폼 클라우드 [참조의 Webhooks 알림 페이로드](#) 참조 및 [메시지 상태를](#) 참조하세요. WhatsApp API

AWS 최종 사용자 메시징 소셜 이벤트 헤더

이벤트의 JSON 객체에는 AWS 이벤트 헤더와 이 포함됩니다 WhatsApp JSON. 헤더에는 WhatsApp 비즈니스 계정(WABA)ARNs의 AWS 식별자 및 전화번호가 포함되어 있습니다.

```
{
  "MetaWabaIds": [
    {
```

```

    "wabaId": "1234567890abcde",
    "arn": "arn:aws:social-messaging:us-
east-1:123456789012:waba/fb2594b8a7974770b128a409e2example"
  }
],
"MetaPhoneNumberIds": [
  {
    "metaPhoneNumberId": "abcde1234567890",
    "arn": "arn:aws:social-messaging:us-east-1:123456789012:phone-number-
id/976c72a700aac43eaf573ae050example"
  }
]
}
{
//WhatsApp notification payload
}

```

앞의 예제 이벤트에서:

- *1234567890abcde* 는 Meta의 WABA ID입니다.
- *abcde1234567890* 는 Meta의 전화번호 ID입니다.
- *fb2594b8a7974770b128a409e2example* 는 WhatsApp 비즈니스 계정()의 ID입니다WABA.
- *976c72a700aac43eaf573ae050example* 는 전화번호의 ID입니다.

문자 메시지 WhatsApp JSON 수신 예제

다음은 에서 수신되는 텍스트 메시지의 이벤트 레코드를 보여줍니다 WhatsApp. JSON 는 에 의해 생성됩니다 WhatsApp. 필드 목록과 그 의미는 비즈니스 플랫폼 클라우드 참조 의 [Webhooks 알림 페이지](#) 참조를 참조하세요. WhatsApp API

```

{
//AWS End User Messaging Social header
}
{
  "id": "365731266123456",
  "changes": [
    {
      "value": {
        "messaging_product": "whatsapp",

```

```

    "metadata": {
      "display_phone_number": "12065550100",
      "phone_number_id": "321010217760100"
    },
    "contacts": [
      {
        "profile": {
          "name": "Diego"
        },
        "wa_id": "12065550102"
      }
    ],
    "messages": [
      {
        "from": "14255550150",
        "id":
"wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRE0RjVGRkexample",
        "timestamp": "1723506035",
        "text": {
          "body": "Hi"
        },
        "type": "text"
      }
    ]
  },
  "field": "messages"
}
]
}

```

미디어 메시지 수신 WhatsApp JSON 예제

다음은 수신 미디어 메시지의 이벤트 레코드를 보여줍니다. 미디어 파일을 검색하려면 명령을 `GetWhatsAppMessageMedia` API 사용합니다. 필드 목록과 그 의미는 [Webhooks Notification Payload Reference](#)를 참조하세요.

```

{
  //AWS End User Messaging Social header
}
{
  "id": "365731266123456",
  "changes": [
    {

```

```

"value": {
  "messaging_product": "whatsapp",
  "metadata": {
    "display_phone_number": "12065550100",
    "phone_number_id": "321010217760100"
  },
  "contacts": [
    {
      "profile": {
        "name": "Diego"
      },
      "wa_id": "12065550102"
    }
  ],
  "messages": [
    {
      "from": "14255550150",
      "id":
"wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRE0RjVGRkexample",
      "timestamp": "1723506230",
      "type": "image",
      "image": {
        "mime_type": "image/jpeg",
        "sha256": "BTD0xlqSZ7l02o+/upusiNStlEZhA/urkvKf143Uqjk=",
        "id": "530339869524171"
      }
    }
  ]
},
"field": "messages"
}
]
}

```

WhatsApp 메시지 상태

메시지를 보내면 메시지에 대한 상태 업데이트가 수신됩니다. 이러한 알림을 받으려면 이벤트 로깅을 활성화해야 합니다. 섹션을 참조하세요 [AWS 최종 사용자 메시징 소셜의 메시지 및 이벤트 대상](#).

메시지 상태

다음 표에는 가능한 메시지 상태가 포함되어 있습니다.

상태 이름	설명
삭제됨	고객이 메시지를 삭제했으며, 메시지가 서버에 다운로드된 경우에도 삭제해야 합니다.
전송됨	메시지가 고객에게 성공적으로 전달되었습니다.
failed	메시지가 전송되지 않았습니다.
읽기	고객이 메시지를 읽었습니다. 이 상태는 고객이 읽은 영수증을 켜 경우에만 전송됩니다.
전송됨	메시지가 전송되었지만 아직 전송 중입니다.
warning	메시지에 사용할 수 없거나 존재하지 않는 항목이 포함되어 있습니다.

추가 리소스

자세한 내용은 WhatsApp 비즈니스 플랫폼 클라우드 API 참조의 [메시지 상태를](#) 참조하세요.

로 전송할 미디어 파일 업로드 WhatsApp

미디어 파일을 보내거나 받을 때는 Amazon S3 버킷에 저장해야 합니다. Amazon S3 버킷은 WhatsApp 비즈니스 계정() AWS 계정 과 같고 AWS 리전 같아야 합니다WABA. 다음 지침은 Amazon S3 버킷을 생성하고, 파일을 업로드하고, 를 파일에 빌드URL하는 방법을 보여줍니다. Amazon S3 명령에 대한 자세한 내용은 [AWS 에서 상위 수준\(s3\) 명령 사용을 CLI](#) 참조하세요. 구성에 대한 자세한 내용은 [AWS Command Line Interface 사용 설명서AWS의 구성CLI](#), [Amazon S3 사용 설명서의 버킷 생성 및 객체 업로드](#)를 AWS CLI참조하세요.

미디어 파일에 [미리 서명된 URL](#) 를 생성할 수도 있습니다. 미리 서명된 를 사용하면 다른 당사자에게 AWS 보안 자격 증명 또는 권한을 요구하지 않고 객체에 대한 시간 제한 액세스 권한을 부여하고 업로드할 URL 수 있습니다.

Amazon S3 버킷을 생성하려면 [create-bucket](#) AWS CLI 명령을 사용합니다. 명령줄에 다음 명령을 입력합니다.

```
aws s3api create-bucket --region 'us-east-1' --bucket BucketName
```

앞의 명령에서:

- Replace *us-east-1* 에 AWS 리전 있는 를 사용합니다WABA.
- Replace *BucketName* 새 버킷의 이름을 사용합니다.

Amazon S3 버킷에 파일을 복사하려면 [cp](#) AWS CLI 명령을 사용합니다. 명령줄에 다음 명령을 입력합니다.

```
aws s3 cp SourceFilePathAndName s3://BucketName/FileName
```

앞의 명령에서:

- Replace *SourceFilePathAndName* 복사할 파일의 파일 경로와 이름이 표시됩니다.
- Replace *BucketName* 버킷의 이름을 사용합니다.
- Replace *FileName* 파일에 사용할 이름을 포함합니다.

전송할 때 사용할 URL은 다음과 같습니다.

```
s3://BucketName/FileName
```

[미리 서명된 URL](#)을 생성하려면 *user input placeholders* 자신의 정보를 사용합니다.

```
aws s3 presign s3://amzn-s3-demo-bucket1/mydoc.txt --expires-in 604800 --region af-south-1 --endpoint-url https://s3.af-south-1.amazonaws.com
```

반환URL되는 는 다음과 같습니다. `https://amzn-s3-demo-bucket1.s3.af-south-1.amazonaws.com/mydoc.txt?{Headers}`

에서 지원되는 미디어 파일 유형 및 크기 WhatsApp

미디어 메시지를 보내거나 받을 때는 파일 유형을 최대 파일 크기로 지원해야 합니다. 자세한 내용은 WhatsApp 비즈니스 플랫폼 클라우드 API 참조의 [지원되는 미디어 유형을 참조하세요](#).

미디어 파일 유형

오디오 형식

오디오 유형	확장	MIME 유형	최대 크기
AAC	.aac	오디오/aac	16MB
AMR	.amr	오디오/amr	16MB
MP3	.mp3	오디오/mpeg	16MB
MP4 오디오	.m4a	오디오/mp4	16MB
OGG 오디오	.ogg	오디오/ogg	16MB

문서 형식

문서 유형	확장	MIME 유형	최대 크기
텍스트	.text	text/plain	100MB
Microsoft Excel	.xls, .xlsx	application/vnd.ms-excel, application/	100MB

문서 유형	확장	MIME 유형	최대 크기
		vnd.openxmlformats-officedocument.spreadsheetml.sheet	
Microsoft Word	.doc, .docx	application/msword, application/vnd.openxmlformats-officedocument.wordprocessingml.document	100MB
Microsoft PowerPoint	.ppt, .pptx	application/vnd.ms-powerpoint, application/vnd.openxmlformats-officedocument.presentationml.presentation	100MB
PDF	.pdf	application/pdf	100MB

이미지 형식

이미지 유형	확장	MIME 유형	최대 크기
JPEG	.jpeg	image/jpeg	5MB
PNG	.png	image/png	5MB

스티커 형식

스티커 유형	확장	MIME 유형	최대 크기
애니메이션 스티커	.webp	이미지/웹	500KB
정적 스티커	.webp	이미지/웹	100KB

비디오 형식

비디오 유형	확장	MIME 유형	최대 크기
3GPP	.3gp	비디오/3gp	16MB
MP4 비디오	.mp4	비디오/mp4	16MB

WhatsApp 메시지 유형

이 주제에서는 지원되는 메시지 유형과 사용 설명을 나열합니다. 메시지 유형 목록은 WhatsApp 비즈니스 플랫폼 클라우드 API 참조의 [메시지를](#) 참조하세요.

메시지 유형	설명
텍스트	URL 고객에게 문자 메시지 또는 전송
미디어	오디오, 문서, 이미지, 스티커 또는 비디오 파일을 전송합니다. 미디어 파일의 링크를 보낼 수도 있습니다.
반응	엄지손가락 올리기와 같은 메시지에 대한 반응으로 이모티콘 전송
템플릿	템플릿 메시지 전송
위치	위치 전송
연락처	연락처 카드 전송
대화형	대화형 메시지 전송

추가 리소스

WhatsApp 메시지 객체 목록은 WhatsApp 비즈니스 플랫폼 클라우드 API 참조의 [메시지를](#) 참조하세요.

AWS 최종 사용자 메시징 소셜 WhatsApp 을 사용하여 를 통 해 메시지 전송

메시지를 전송하기 전에 의 설정을 완료했어야 하며 WABA 사용자가 메시지를 수신하도록 옵트인했어야 합니다. 섹션을 참조하세요 [권한 획득](#).

사용자가 메시지를 보내면 고객 서비스 창이라는 24시간 타이머가 시작되거나 새로 고쳐집니다. 템플릿 메시지를 제외한 모든 메시지 유형은 사용자와 사용자 간에 고객 서비스 창이 열려 있는 경우에만 사용자에게 전송할 수 있습니다. 템플릿 메시지는 사용자가 사용자로부터 메시지를 수신하도록 옵트인한 경우 언제든지 사용자에게 전송할 수 있습니다.

보내거나 받는 각 메시지에 대해 메시지 상태가 생성되어 이벤트 대상으로 전송됩니다. 고객이 WhatsApp 이벤트에 가입하지 않은 경우 메시지 상태가 로 생성됩니다 fail. [메시지 상태를 수신하려면 메시지 및 이벤트 대상](#)을 켜야 합니다. ???

Important

Meta/ 작업WhatsApp

- WhatsApp 비즈니스 솔루션 사용에는 [WhatsApp 비즈니스 서비스 약관](#) , [WhatsApp 비즈니스 솔루션 약관](#) , [WhatsApp 비즈니스 메시징 정책](#) , [WhatsApp 메시징 지침](#) , 참조로 통합된 기타 모든 약관, 정책 또는 지침(각각 수시로 업데이트될 수 있음)의 약관이 적용됩니다.
- Meta 또는 WhatsApp 는 언제든지 WhatsApp 비즈니스 솔루션 사용을 금지할 수 있습니다.
- WhatsApp 비즈니스 솔루션 사용과 관련하여 귀하는 관련 법률 및/또는 규정에 따라 배포를 보호 및/또는 제한해야 하는 콘텐츠, 정보 또는 데이터를 제출하지 않습니다.

주제

- [AWS 최종 사용자 메시징 소셜에서 템플릿 메시지를 보내는 예제](#)
- [AWS 최종 사용자 메시징 소셜에서 미디어 메시지를 보내는 예제](#)

AWS 최종 사용자 메시징 소셜에서 템플릿 메시지를 보내는 예제

다음 예제에서는 템플릿을 사용하여 를 사용하여 고객에게 [메시지를 보내는](#) 방법을 보여줍니다 AWS CLI. 구성에 대한 자세한 내용은 [AWS Command Line Interface 사용 설명서의 구성을 AWS CLI](#) AWS CLI참조하세요.

```
aws socialmessaging send-whatsapp-message --message
'{"messaging_product":"whatsapp","to":"' {PHONE_NUMBER} ','type":"template","template":
{"name":"statement","language":{"code":"en_US"},"components":
[{"type":"body","parameters":[{"type":"text","text":"1000"}]}]}' --origination-phone-
number-id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version v20.0
```

위의 명령에서 다음을 수행합니다.

- Replace `{PHONE_NUMBER}` 고객 전화번호를 사용합니다.
- Replace `{ORIGINATION_PHONE_NUMBER_ID}` 전화번호의 ID를 사용합니다.

AWS 최종 사용자 메시징 소셜에서 미디어 메시지를 보내는 예제

다음 예제에서는 를 사용하여 고객에게 미디어 메시지를 보내는 방법을 보여줍니다 AWS CLI. 구성에 대한 자세한 내용은 [AWS Command Line Interface 사용 설명서의 구성을 AWS CLI](#) AWS CLI참조하세요. 지원되는 미디어 파일 유형의 목록은 [섹션을 참조하세요에서 지원되는 미디어 파일 유형 및 크기](#) [WhatsApp](#).

1. Amazon S3 버킷에 미디어 파일을 업로드합니다. [섹션을 참조하세요로 전송할 미디어 파일 업로드](#) [WhatsApp](#).
2. [post-whatsapp-message-media](#) 명령을 WhatsApp 사용하여 에 미디어 파일을 업로드합니다. 성공적으로 완료되면 명령은 `{MEDIA_ID}` 미디어 메시지를 보내는 데 필요합니다.

```
aws socialmessaging post-whatsapp-message-media --origination-
phone-number-id {ORIGINATION_PHONE_NUMBER_ID} --source-s3-file
bucketName={BUCKET},key={MEDIA_FILE}
```

위의 명령에서 다음을 수행합니다.

- Replace `{ORIGINATION_PHONE_NUMBER_ID}` 전화번호의 ID를 사용합니다.
- Replace `{BUCKET}` Amazon S3 버킷의 이름을 사용합니다.

- Replace `{MEDIA_FILE}` 미디어 파일의 이름을 사용합니다.

--source-s3-presigned-url 대신 [사용하여 사전 서명 URL](#)을 사용하여 업로드할 수도 있습니다--source-s3-file. 헤더 필드에 Content-Type 를 추가해야 합니다. 둘 다 사용하면 InvalidParameterException가 반환됩니다.

```
--source-s3-presigned-url headers={"Name":"Value"},url=https://BUCKET.s3.REGION/MEDIA_FILE
```

3. [send-whatsapp-message](#) 명령을 사용하여 미디어 메시지를 전송합니다.

```
aws socialmessaging send-whatsapp-message --message
'{"messaging_product":"whatsapp","to":"' {PHONE_NUMBER} "',"type":"image","image":
{"id":"' {MEDIA_ID} '"}' --origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID}
--meta-api-version v20.0
```

위의 명령에서 다음을 수행합니다.

- Replace `{PHONE_NUMBER}` 고객 전화번호를 사용합니다.
 - Replace `{ORIGINATION_PHONE_NUMBER_ID}` 전화번호의 ID를 사용합니다.
 - Replace `{MEDIA_ID}` 이전 단계에서 반환된 미디어 ID를 사용합니다.
4. 미디어 파일이 더 이상 필요하지 않으면 [delete-whatsapp-message-media](#) 명령을 WhatsApp 사용하여 에서 삭제할 수 있습니다. 이렇게 하면 Amazon S3 버킷이 WhatsApp 아닌 에서 미디어 파일만 제거됩니다.

```
aws socialmessaging delete-whatsapp-message-media --media-id {MEDIA_ID} --
origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID}
```

위의 명령에서 다음을 수행합니다.

- Replace `{ORIGINATION_PHONE_NUMBER_ID}` 전화번호의 ID를 사용합니다.
- Replace `{MEDIA_ID}` 미디어 ID를 사용합니다.

AWS 최종 사용자 메시징 소셜에서 수신된 메시지에 응답

텍스트 또는 미디어 메시지를 받으려면 먼저 [이 설정을 완료](#)하고 이벤트를 대상으로 WABA 설정해야 합니다. 수신 메시지를 받으면 이벤트가 이벤트 대상 Amazon SNS 주제에 저장됩니다. 알림을 받으려면 Amazon SNS 주제 엔드포인트를 구독해야 합니다.

수신된 미디어 메시지의 예제 이벤트는 [섹션을 참조하세요](#) [미디어 메시지 수신 WhatsApp JSON 예제](#). 구성에 대한 자세한 내용은 [AWS Command Line Interface 사용 설명서](#)의 [구성을 AWS CLI](#) AWS CLI 참조하세요. 지원되는 미디어 파일 유형의 목록은 [섹션을 참조하세요](#) [에서 지원되는 미디어 파일 유형 및 크기](#) [WhatsApp](#).

Important

수신 메시지를 수신하려면 [이벤트 대상](#)이 활성화되어 있어야 합니다. WABA 섹션을 참조하세요 [AWS 최종 사용자 메시징 소셜에 메시지 및 이벤트 대상 추가](#).

AWS 최종 사용자 메시징 소셜을 사용하여 읽도록 메시지 상태를 변경하는 예

[메시지 상태를](#) `read`로 설정하여 최종 사용자에게 화면에 파란색 확인 표시 두 개를 표시할 수 있습니다.

```
aws socialmessaging send-whatsapp-message --message
 '{"messaging_product":"whatsapp","message_id":"' {MESSAGE_ID} ','status":"read"}' --
 origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version v20.0
```

위의 명령에서 다음을 수행합니다.

- Replace `{ORIGINATION_PHONE_NUMBER_ID}` 전화번호의 ID를 사용합니다.
- Replace `{MESSAGE_ID}` 메시지의 고유 식별자를 사용합니다. Amazon SNS 주제의 메시지 객체에서 `id` 필드 값을 사용합니다.

AWS 최종 사용자 메시징 소셜에서 반응으로 메시지에 응답하는 예

엄지손가락을 올리는 것처럼 메시지에 반응을 추가할 수 있습니다.

```
aws socialmessaging send-whatsapp-message --message
 '{"messaging_product":"whatsapp","recipient_type":"individual","to":"' {PHONE_NUMBER} ','type":
 "reaction","reaction": {"message_id": "' {MESSAGE_ID} ','emoji":"\uD83D\uDC4D"}' --
 origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version v20.0
```

위의 명령에서 다음을 수행합니다.

- Replace `{PHONE_NUMBER}` 고객 전화번호를 사용합니다.
- Replace `{MESSAGE_ID}` 메시지의 고유 식별자를 사용합니다. Amazon SNS 주제의 메시지 객체에서 id 필드 값을 사용합니다.
- Replace `{ORIGINATION_PHONE_NUMBER_ID}` 전화번호의 ID를 사용합니다.

에서 Amazon S3 WhatsApp 로 미디어 파일 다운로드

미디어 파일을 검색하여 Amazon S3 버킷에 저장하려면 [get-whatsapp-message-media](#) 명령을 사용합니다.

```
aws socialmessaging get-whatsapp-message-media --media-id {MEDIA_ID} --
 origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID} --destination-s3-file
 bucketName={BUCKET},key=inbound_
 {
   "mimeType": "image/jpeg",
   "fileSize": 78144
 }
```

위의 명령에서 다음을 수행합니다.

- Replace `{BUCKET}` Amazon S3 버킷의 이름을 사용합니다.
- Replace `{MEDIA_ID}` 수신된 이벤트의 ID 필드 값입니다. 수신 미디어 이벤트의 예는 섹션을 참조하세요 [미디어 메시지 수신 WhatsApp JSON 예제](#).
- Replace `{ORIGINATION_PHONE_NUMBER_ID}` 전화번호의 ID를 사용합니다.

Amazon S3 버킷에서 미디어를 검색하려면 다음 명령을 사용합니다.

```
aws s3 cp s3://{BUCKET}/inbound_{MEDIA_ID}.jpeg
```

위의 명령에서 다음을 수행합니다.

- Replace `{BUCKET}` Amazon S3 버킷의 이름을 사용합니다.
- Replace `{MEDIA_ID}` 이전 단계에서 반환된 MEDIA_ID.

읽기 및 응답을 사용하여 메시지에 응답하는 예

이 예에서는 고객인 Diego가 '안녕하세요'라는 메시지를 보냈고 귀하는 읽기 수신증과 핸드 웨이브 이모티콘으로 응답했습니다.

사전 조건

Diego가 메시지를 보냈다는 알림을 받으려면 이벤트 대상 Amazon SNS 주제를 설정하고 주제 엔드포인트 중 하나를 구독해야 합니다.

응답

1. Diego의 메시지가 수신되면 이벤트가 주제의 엔드포인트에 게시됩니다. 다음은 주제가 게시하는 내용을 요약한 것입니다.

Note

디에고는 대화를 시작했으므로 비즈니스 시작 대화에는 포함되지 않습니다.

```
{
  "MetaWabaIds": [
    {
      "wabaId": "1234567890abcde",
      "arn": "arn:aws:social-messaging:us-east-1:123456789012:waba/fb2594b8a7974770b128a409e2example"
    }
  ],
  "MetaPhoneNumberIds": [
    {
      "metaPhoneNumberId": "abcde1234567890",
      "arn": "arn:aws:social-messaging:us-east-1:123456789012:phone-number-id/976c72a700aac43eaf573ae050example"
    }
  ]
}
```

```
{
  "id": "365731266123456",
  "changes": [
    {
      "value": {
        "messaging_product": "whatsapp",
        "metadata": {
          "display_phone_number": "12065550100",
          "phone_number_id": "321010217712345"
        },
        "contacts": [
          {
            "profile": {
              "name": "Diego"
            },
            "wa_id": "12065550102"
          }
        ],
        "messages": [
          {
            "from": "14255550150",
            "id":
"wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRE0RjVGRkexample",
            "timestamp": "1723506035",
            "text": {
              "body": "Hi"
            },
            "type": "text"
          }
        ]
      },
      "field": "messages"
    }
  ]
}
```

2. 디에고를 표시하려면 상태를 `read`로 설정하는 메시지를 받았습니까. 디에고는 디바이스의 메시지 옆에 두 개의 파란색 확인 표시를 보게 됩니다.

```
aws socialmessaging send-whatsapp-message --message
'{"messaging_product":"whatsapp","message_id":"' {MESSAGE_ID} "',"status":"read"}'
--origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version
v20.0
```

위의 명령에서 다음을 수행합니다.

- Replace `{ORIGINATION_PHONE_NUMBER_ID}` Diego가 에 메시지를 보낸 전화번호 ID가 인 경우 `phone-number-id-976c72a700aac43eaf573ae050example`.
- Replace `{MESSAGE_ID}` 메시지의 고유 식별자를 사용합니다. 수신된 메시지 의 ID와 동일한 값입니
다 `wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRE0RjVGRke`

3. 디에고에 핸드 웨이브 응답을 보낼 수 있습니다.

```
aws socialmessaging send-whatsapp-message --message
'{"messaging_product":"whatsapp","recipient_type":"individual","to":"' {PHONE_NUMBER} ','ty
"reaction","reaction": {"message_id": "' {MESSAGE_ID} ','emoji": "\uD83D\uDC4B"}'
--origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version
v20.0
```

위의 명령에서 다음을 수행합니다.

- Replace `{PHONE_NUMBER}` 디에고의 전화번호 를 사용합니다 `14255550150`.
- Replace `{MESSAGE_ID}` 메시지의 고유 식별자를 사용합니다. 수신된 메시지 의 ID와 동일한 값입니
다 `wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRE0RjVGRke`
- Replace `{ORIGINATION_PHONE_NUMBER_ID}` Diego가 에 메시지를 보낸 전화번호 ID가 인 경우 `phone-number-id-976c72a700aac43eaf573ae050example`.

추가 리소스

- [이벤트 대상이](#) 이벤트를 로깅하고 수신 메시지를 수신하도록 활성화합니다.
- 메시지 객체 목록은 WhatsApp 비즈니스 플랫폼 클라우드 API 참조의 WhatsApp [메시지](#)를 참조하세요.

AWS 최종 사용자 메시징 소셜에 대한 WhatsApp 결제 및 사용 보고서 이해

AWS 최종 사용자 메시징 소셜 채널은 다음 형식의 5개 필드가 포함된 사용 유형을 생성합니다. `Region code-MessagingType-ISO-FeeDescription-FeeType`. 각 WhatsApp 대화에 대해 ConversationFee와 AWS 당에 WhatsApp 대해 두 가지 가능한 결제 항목이 있습니다. MessageFee.

템플릿 메시지를 전송하여 대화를 시작하면 1 AWS 개당 1개 WhatsApp ConversationFee 및 1개에 대한 요금이 청구됩니다. MessageFee. 이렇게 하면 동일한 고객으로부터 보내거나 받는 각 메시지가 AWS 당 로 청구되는 24시간 창이 열립니다. MessageFee.

WhatsApp 대화 유형 및 요금 세부 정보는 WhatsApp 비즈니스 플랫폼 개발자 안내서의 [대화 기반 요금](#)에서 확인할 수 있습니다.

다음 표에는 사용 유형의 필드에 표시될 수 있는 값과 설명이 나와 있습니다. AWS 최종 사용자 메시징 소셜 요금에 대한 자세한 내용은 [AWS 최종 사용자 메시징 요금 섹션](#)을 참조하세요.

필드	옵션	설명
<i>Region code</i>	<ul style="list-style-type: none"> USE1 – 미국 동부(버지니아 북부) 리전 USE2 – 미국 동부(오하이오) 리전 USW1 – 미국 서부(오레곤) 리전 APS1 – 아시아 태평양(뭄바이) 리전 APSE1 – 아시아 태평양(싱가포르) 리전 EUW1 – 유럽(아일랜드) 리전 EUW2 – 유럽(런던) 리전 	WhatsApp 메시지를 보내거나 받은 위치를 나타내는 AWS 리전 접두사입니다.

필드	옵션	설명
<i>MessagingType</i>	WhatsApp	이 필드는 전송 중인 메시지 유형을 식별합니다.
<i>ISO</i>	지원되는 국가 보기	메시지가 전송된 두 자리 ISO 국가 코드입니다.
<i>FeeDescription</i>	ConversationFee , MessageFee	이 필드는 또는 를 WhatsApp ConversationFee 에 AWS 따라 지정합니다MessageFee .

필드	옵션	설명
<i>FeeType</i>	Authentication , Marketing , Service, Utility, Standard	<p>이 필드는 사용된 대화 유형의 유형을 표시하거나 메시지당 요금에 대한 표준을 지정합니다.</p> <p>비즈니스 시작 ConversationFee 범주</p> <ul style="list-style-type: none"> • Marketing - 인식 제고에서 판매 촉진 및 고객 재대상 지정에 이르기까지 광범위한 목표를 달성하는 데 사용됩니다. 예를 들어 신제품, 서비스 또는 기능 공지, 대상 프로모션/제안, 장바구니 포기 알림 등이 있습니다. • Utility - 사용자 작업 또는 요청을 후속 조치하는 데 사용됩니다. 예를 들어 옵트인 확인, 주문/배송 관리(예: 배송 업데이트), 계정 업데이트 또는 알림(예: 결제 알림), 피드백 설문조사 등이 있습니다. • Authentication - 로그인 프로세스의 여러 단계(예: 계정 확인, 계정 복구 및 무결성 문제)에서 일회용 암호로 사용자를 인증하는 데 사용됩니다. • Service - 고객 문의를 해결하는 데 사용됩니다.

필드	옵션	설명
		<p>사용자 시작 ConversationFee 범주</p> <ul style="list-style-type: none"> • Service - 고객 문의를 해결하는 데 사용됩니다. <p>MessageFee 범주</p> <ul style="list-style-type: none"> • Standard - 전송되거나 수신된 메시지당 요금입니다.

템플릿 메시지를 보내 대화를 시작하면 하나 ConversationFee와 하나의 에 대한 요금이 청구됩니다 MessageFee. 이렇게 하면 동일한 고객에게 보내는 각 템플릿 메시지가 개별 로 청구되는 24시간 창이 열립니다 MessageFee. 24시간 기간 동안 템플릿 메시지는 동일한 유형이거나 새 대화 시작되어야 합니다.

예를 들어 고객에게 마케팅 템플릿 메시지를 보내는 경우 ConversationFee 및 에 대한 요금이 청구됩니다 MessageFee.

```
Marketing Template Message 1: APS1-WhatsApp-CA-ConversationFee-Marketing
Marketing Template Message 1: APS1-WhatsApp-CA-MessageFee-Standard
Marketing Template Message 2: APS1-WhatsApp-CA-MessageFee-Standard
```

고객이 메시지를 보내고 응답하면 새 Service 대화 및 메시지를 열 때 요금이 청구됩니다.

```
Service Message 1: APS1-WhatsApp-CA-ConversationFee-Service
Service Message 1: APS1-WhatsApp-CA-MessageFee-Standard
Service Message 2: APS1-WhatsApp-CA-MessageFee-Standard
Service Message 3: APS1-WhatsApp-CA-MessageFee-Standard
```

예제 1: 마케팅 템플릿 메시지 전송

예를 들어 고객에게 마케팅 템플릿 메시지를 보내는 경우 1 AWS 개당 1 WhatsApp ConversationFee개 및 1개에 대한 요금이 청구됩니다 MessageFee.

```
Marketing Template Message 1: APS1-WhatsApp-CA-ConversationFee-Marketing
```

Marketing Template Message 1: APS1-WhatsApp-CA-MessageFee-Standard

예제 2: 서비스 대화 열기

서비스 대화 요금은 비즈니스에서 시작한 활성 24시간 대화 기간을 벗어나는 사용자의 인바운드 메시지에 기업이 응답할 때 적용됩니다. 이 시나리오에서는 각 인바운드 및 아웃바운드 메시지에 대해 하나 WhatsApp ConversationFee와 가 AWS MessageFee 청구됩니다.

```
Service Message 1: APS1-WhatsApp-CA-ConversationFee-Service
Service Message 1: APS1-WhatsApp-CA-MessageFee-Standard
Service Message 2: APS1-WhatsApp-CA-MessageFee-Standard
Service Message 3: APS1-WhatsApp-CA-MessageFee-Standard
```

AWS 최종 사용자 메시징 소셜 결제 ISO 코드 및 WhatsApp 대화 요금 매핑

지원되는 국가

두 자리 ISO 국가 코드	국가 이름	WhatsApp 대화 결제 리전
AF	아프가니스탄	아시아 태평양 나머지 지역
AX	엘랜드 제도	기타
AL	알바니아	중부 및 동부 유럽의 나머지 지역
DZ	알제리	아프리카 나머지 지역
AS	미국령 사모아	기타
AD	안도라	기타
AO	앙골라	아프리카 나머지 지역
AI	양귀라	기타
AQ	남극	기타

두 자리 ISO 국가 코드	국가 이름	WhatsApp 대화 결제 리전
AG	앤티가 바부다	기타
AR	아르헨티나	아르헨티나
AM	아르메니아	중부 및 동부 유럽의 나머지 지역
AW	아루바 섬	기타
AC	어센션 아일랜드	기타
AU	호주	아시아 태평양 나머지 지역
AT	오스트리아	기타 서유럽
AZ	아제르바이잔	중부 및 동부 유럽의 나머지 지역
BS	바하마	기타
BH	바레인	중동 나머지 지역
BD	방글라데시	아시아 태평양 나머지 지역
BB	바베이도스	기타
BY	벨로루시	중부 및 동부 유럽의 나머지 지역
BE	벨기에	기타 서유럽
BZ	벨리즈	기타
BJ	베냉	아프리카 나머지 지역
BM	버뮤다	기타
BT	부탄	기타
BO	볼리비아	라틴 아메리카 나머지 지역

두 자리 ISO 국가 코드	국가 이름	WhatsApp 대화 결제 리전
BQ	보네르	기타
BA	보스니아 헤르체코비나	기타
BW	보츠와나	아프리카 나머지 지역
BV	부베 섬	기타
BR	브라질	브라질
IO	영국령 인도양 지역	기타
VG	영국령 버진 제도	기타
BN	브루나이 다루살람	기타
BG	불가리아	중부 및 동부 유럽의 나머지 지역
BF	BurkinaFaso	아프리카 나머지 지역
BI	부룬디	아프리카 나머지 지역
KH	캄보디아	아시아 태평양 나머지 지역
CM	카메룬	아프리카 나머지 지역
CA	캐나다	북미
CV	카보베르데	기타
KY	케이맨 제도	기타
CF	중앙아프리카 공화국	기타
TD	차드	아프리카 나머지 지역
CL	칠레	칠레
CN	중국	아시아 태평양 나머지 지역

두 자리 ISO 국가 코드	국가 이름	WhatsApp 대화 결제 리전
CX	크리스마스 섬	기타
CC	코코스(킬링) 제도	기타
CO	콜롬비아	콜롬비아
KM	코모로	기타
CG	콩고	기타
CD	콩고	아프리카 나머지 지역
CK	쿡 제도	기타
CR	코스타리카	라틴 아메리카 나머지 지역
CI	Cote d'Ivoire	아프리카 나머지 지역
HR	크로아티아	중부 및 동부 유럽의 나머지 지역
CW	큐라소	기타
CY	사이프러스	기타
CZ	체코 공화국	중부 및 동부 유럽의 나머지 지역
DK	덴마크	기타 서유럽
DJ	지부티	기타
DM	도미니카	기타
DO	도미니카 공화국	라틴 아메리카 나머지 지역
EC	에콰도르	라틴 아메리카 나머지 지역
EG	이집트	이집트

두 자리 ISO 국가 코드	국가 이름	WhatsApp 대화 결제 리전
SV	엘살바도르	라틴 아메리카 나머지 지역
GQ	적도 기니	기타
ER	에리트레아	아프리카 나머지 지역
EE	에스토니아	기타
ET	에티오피아	아프리카 나머지 지역
FK	포클랜드 제도	기타
FO	페로 제도	기타
FJ	피지	기타
FI	핀란드	기타 서유럽
FR	프랑스	프랑스
GF	프랑스령 기아나	기타
PF	프랑스령 폴리네시아	기타
TF	프랑스령 남방 지역	기타
GA	가봉	아프리카 나머지 지역
GM	감비아	아프리카 나머지 지역
GE	그루지야	중부 및 동부 유럽의 나머지 지역
DE	독일	독일
GH	가나	아프리카 나머지 지역
GI	지브롤터	기타

두 자리 ISO 국가 코드	국가 이름	WhatsApp 대화 결제 리전
GR	그리스	중부 및 동부 유럽의 나머지 지역
GL	그린란드	기타
GD	그레나다	기타
GP	과들루프	기타
GU	괌	기타
GT	과테말라	라틴 아메리카 나머지 지역
GG	건지	기타
GN	기니	기타
GW	기니비사우	아프리카 나머지 지역
GY	가이아나	기타
HT	아이티	라틴 아메리카 나머지 지역
HM	들음 및 McDonald 섬	기타
HN	온두라스	라틴 아메리카 나머지 지역
HK	홍콩	아시아 태평양 나머지 지역
HU	헝가리	중부 및 동부 유럽의 나머지 지역
IS	아이슬란드	기타
IN	인도	인도
IN	인도 국제	인도 국제
ID	인도네시아	인도네시아

두 자리 ISO 국가 코드	국가 이름	WhatsApp 대화 결제 리전
ID	인도네시아 국제	인도네시아 국제
IQ	이라크	중동 나머지 지역
IE	아일랜드	기타 서유럽
IM	맨 섬	기타
IL	이스라엘	이스라엘
IT	이탈리아	이탈리아
JM	자메이카	라틴 아메리카 나머지 지역
JP	일본	아시아 태평양 나머지 지역
JE	저지	기타
JO	요르단	중동 나머지 지역
KZ	카자흐스탄	기타
KE	케냐	아프리카 나머지 지역
KI	키리바시	기타
XK	코소보	기타
KW	쿠웨이트	중동 나머지 지역
KG	키르기스스탄	기타
LA	라오 PDR	아시아 태평양 나머지 지역
LV	라트비아	중부 및 동부 유럽의 나머지 지역
LB	레바논	중동 나머지 지역
LS	레소토	아프리카 나머지 지역

두 자리 ISO 국가 코드	국가 이름	WhatsApp 대화 결제 리전
LR	라이베리아	아프리카 나머지 지역
LY	리비아	아프리카 나머지 지역
LI	리히텐슈타인	기타
LT	리투아니아	중부 및 동부 유럽의 나머지 지역
LU	룩셈부르크	기타
MO	마카오	기타
MK	마케도니아	중부 및 동부 유럽의 나머지 지역
MG	마다가스카르	아프리카 나머지 지역
MW	말라위	아프리카 나머지 지역
MY	말레이시아	말레이시아
MV	몰디브	기타
ML	말리	아프리카 나머지 지역
MT	몰타	기타
MH	마셜 제도	기타
MQ	마르티니크	기타
MR	모리타니아	아프리카 나머지 지역
MU	모리셔스	기타
YT	마요트	기타
MX	멕시코	멕시코

두 자리 ISO 국가 코드	국가 이름	WhatsApp 대화 결제 리전
FM	미크로네시아	기타
MD	몰도바	중부 및 동부 유럽의 나머지 지역
MC	모나코	기타
MN	몽골	아시아 태평양 나머지 지역
ME	몬테네그로	기타
MS	몬트세라트 섬	기타
MA	모로코	아프리카 나머지 지역
MZ	모잠비크	아프리카 나머지 지역
MM	미얀마	기타
NA	나미비아	아프리카 나머지 지역
NR	나우루	기타
NP	네팔	아시아 태평양 나머지 지역
NL	네덜란드	네덜란드
NC	뉴칼레도니아	기타
NZ	뉴질랜드	아시아 태평양 나머지 지역
NI	니카라과	라틴 아메리카 나머지 지역
NE	니제르	아프리카 나머지 지역
NG	나이지리아	나이지리아
NU	니우에	기타
NF	노퍽 섬	기타

두 자리 ISO 국가 코드	국가 이름	WhatsApp 대화 결제 리전
MP	북마리아나 제도	기타
NO	노르웨이	기타 서유럽
OM	오만	중동 나머지 지역
PK	파키스탄	파키스탄
PW	팔라우	기타
PS	팔레스타인 영토	기타
PA	파나마	라틴 아메리카 나머지 지역
PG	파푸아뉴기니	아시아 태평양 나머지 지역
PY	파라과이	라틴 아메리카 나머지 지역
PE	페루	페루
PH	필리핀	아시아 태평양 나머지 지역
PN	피트케언	기타
PL	폴란드	중부 및 동부 유럽의 나머지 지역
PT	포르투갈	기타 서유럽
PR	푸에르토리코	라틴 아메리카 나머지 지역
QA	카타르	중동 나머지 지역
RE	레위니옹	기타
RO	루마니아	중부 및 동부 유럽의 나머지 지역
RU	러시아 연방	러시아

두 자리 ISO 국가 코드	국가 이름	WhatsApp 대화 결제 리전
RW	르완다	아프리카 나머지 지역
SH	세인트 헬레나	기타
KN	세인트 크리스토퍼 네비스	기타
LC	세인트루시아	기타
PM	세인트 피에르 미켈론	기타
VC	세인트 빈센트 그레나딘	기타
BL	Saint-Barthelemy	기타
MF	세인트마틴	기타
WS	사모아	기타
SM	산마리노	기타
ST	상투메 프린시페	기타
SA	사우디아라비아	사우디아라비아
SN	세네갈	아프리카 나머지 지역
RS	세르비아	중부 및 동부 유럽의 나머지 지역
SC	세이셸	기타
SL	시에라리온	아프리카 나머지 지역
SG	싱가포르	아시아 태평양 나머지 지역
SX	신트마르턴	기타
SK	슬로바키아	중부 및 동부 유럽의 나머지 지역

두 자리 ISO 국가 코드	국가 이름	WhatsApp 대화 결제 리전
SI	슬로베니아	중부 및 동부 유럽의 나머지 지역
SB	솔로몬 제도	기타
SO	소말리아	아프리카 나머지 지역
ZA	남아프리카공화국	남아프리카공화국
GS	사우스조지아 사우스샌드위치 제도	기타
KR	대한민국	기타
SS	남수단	아프리카 나머지 지역
ES	스페인	스페인
LK	스리랑카	아시아 태평양 나머지 지역
SR	수리남	기타
SJ	스발바드 및 얀 메이엔 제도	기타
SZ	스와질란드	아프리카 나머지 지역
SE	스웨덴	기타 서유럽
CH	스위스	기타 서유럽
TW	대만	아시아 태평양 나머지 지역
TJ	타지키스탄	아시아 태평양 나머지 지역
TZ	탄자니아	아프리카 나머지 지역
TH	태국	아시아 태평양 나머지 지역
TL	동티모르	기타

두 자리 ISO 국가 코드	국가 이름	WhatsApp 대화 결제 리전
TG	토고	아프리카 나머지 지역
TK	토켈라우	기타
TO	통가	기타
TT	트리니다드 토바고	기타
TA	Trist와 Cunha	기타
TN	튀니지	아프리카 나머지 지역
TR	터키	터키
TM	투르크메니스탄	아시아 태평양 나머지 지역
TC	터크스 카이코스 군도	기타
TV	투발루	기타
UG	우간다	아프리카 나머지 지역
UA	우크라이나	중부 및 동부 유럽의 나머지 지역
AE	아랍 에미리트 연합국	아랍 에미리트 연합국
GB	영국	영국
미국	미국	북미
UY	우루과이	라틴 아메리카 나머지 지역
UM	미국 마이너 아웃라이딩 제도	기타
UZ	우즈베키스탄	아시아 태평양 나머지 지역
VU	바누아투	기타
VA	바티칸 시국	기타

두 자리 ISO 국가 코드	국가 이름	WhatsApp 대화 결제 리전
VE	베네수엘라	라틴 아메리카 나머지 지역
VN	베트남	아시아 태평양 나머지 지역
VI	버진 아일랜드	기타
WF	월리스 푸투나 제도	기타
EH	서사하라	기타
YE	예멘	중동 나머지 지역
ZM	잠비아	아프리카 나머지 지역
ZW	짐바브웨	기타

AWS 최종 사용자 메시징 소셜 모니터링

모니터링은 AWS 최종 사용자 메시징 소셜 및 기타 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는데 중요한 부분입니다. AWS는 AWS 최종 사용자 메시징 소셜을 감시하고, 문제가 있을 때 보고하고, 적절한 경우 자동 조치를 취할 수 있는 다음과 같은 모니터링 도구를 제공합니다.

- Amazon CloudWatch은 AWS 리소스와 실행 중인 애플리케이션을 AWS 실시간으로 모니터링합니다. 지표를 수집 및 추적하고, 사용자 지정 대시보드를 생성할 수 있으며, 지정된 지표가 지정된 임계값에 도달하면 사용자에게 알리거나 조치를 취하도록 경보를 설정할 수 있습니다. 예를 들어 Amazon EC2 인스턴스의 CPU 사용량 또는 기타 지표를 CloudWatch 추적하고 필요한 경우 새 인스턴스를 자동으로 시작할 수 있습니다. 자세한 내용은 [Amazon CloudWatch 사용 설명서 섹션](#)을 참조하세요.
- Amazon CloudWatch Logs를 사용하면 Amazon EC2 인스턴스 및 기타 소스에서 로그 파일을 모니터링 CloudTrail, 저장 및 액세스할 수 있습니다. CloudWatch Logs는 로그 파일의 정보를 모니터링하고 특정 임계값이 충족되면 사용자에게 알릴 수 있습니다. 또한 매우 내구력 있는 스토리지에 로그 데이터를 저장할 수 있습니다. 자세한 내용은 [Amazon CloudWatch Logs 사용 설명서](#)를 참조하세요.
- AWS CloudTrail는 AWS 계정에서 직접 또는 계정을 대신하여 수행된 API 통화 및 관련 이벤트를 캡처하고 사용자가 지정한 Amazon S3 버킷에 로그 파일을 전달합니다. 이는 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시점을 식별할 수 있습니다. 자세한 내용은 [AWS CloudTrail 사용 설명서](#)를 참조하십시오.

Amazon을 사용한 AWS 최종 사용자 메시징 소셜 모니터링 CloudWatch

원시 데이터를 CloudWatch수집하고 읽기 가능한 실시간에 가까운 지표로 처리하는 를 사용하여 AWS 최종 사용자 메시징 소셜을 모니터링할 수 있습니다. 이러한 통계는 15개월간 보관되므로 기록 정보에 액세스하고 웹 애플리케이션 또는 서비스가 어떻게 실행되고 있는지 전체적으로 더 잘 파악할 수 있습니다. 특정 임계값을 주시하다가 해당 임계값이 충족될 때 알림을 전송하거나 조치를 취하도록 경보를 설정할 수도 있습니다. 자세한 내용은 [Amazon CloudWatch 사용 설명서 섹션](#)을 참조하세요.

AWS 최종 사용자 메시징 소셜의 경우 를 감시WhatsAppMessageFeeCount하고 지출 임계값에 도달하면 경보를 감시WhatsAppConversationFeeCount하고 트리거할 수 있습니다.

다음 표에는 AWS 최종 사용자 메시징 소셜이 AWS/SocialMessaging 네임스페이스로 내보내는 지표와 차원이 나열되어 있습니다.

지표	단위	설명
WhatsAppConversationFeeCount	개수	WhatsApp 대화 요금 수
WhatsAppMessageFeeCount	개수	WhatsApp 메시지 요금 수

측정기준	설명
MessageFeeType	유효한 요금 유형은 서비스, 마케팅, 유틸리티 및 인증입니다.
DestinationCountryCode	국가의 두 글자 ISO 코드
WhatsAppPhoneNumberArn	전화번호의 탄생

를 사용하여 AWS 최종 사용자 메시징 소셜 API 통화 로깅 AWS CloudTrail

AWS 최종 사용자 메시징 소셜은 사용자 [AWS CloudTrail](#), 역할 또는 AWS 서비스가 수행한 작업의 레코드를 제공하는 서비스인 와 통합됩니다. 는 AWS 최종 사용자 메시징 소셜에 대한 모든 API 호출을 이벤트로 CloudTrail 캡처합니다. 캡처된 호출에는 AWS 최종 사용자 메시징 소셜 콘솔의 호출과 AWS 최종 사용자 메시징 소셜 API 작업에 대한 코드 호출이 포함됩니다. 에서 수집한 정보를 사용하여 AWS 최종 사용자 메시징 소셜에 수행된 요청 CloudTrail, 요청이 수행된 IP 주소, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

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

- 요청을 루트 사용자로 했는지 사용자 보안 인증으로 했는지 여부.
- IAM Identity Center 사용자를 대신하여 요청이 이루어졌는지 여부입니다.
- 역할 또는 페더레이션 사용자에게 대한 임시 보안 인증을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

CloudTrail 는 계정을 생성할 AWS 계정 때 에서 활성화되며 CloudTrail 이벤트 기록 에 자동으로 액세스할 수 있습니다. CloudTrail 이벤트 기록은 에서 기록된 관리 이벤트의 지난 90일에 대한 보기 가능하고, 검색 가능하고, 다운로드 가능하고, 변경할 수 없는 레코드를 제공합니다 AWS 리전. 자세한 내용은 AWS CloudTrail 사용 설명서의 [CloudTrail 이벤트 기록 작업을](#) 참조하세요. 이벤트 기록 보기에는 요금이 부과되지 않습니다 CloudTrail.

AWS 계정 지난 90일 동안 진행 중인 이벤트 레코드의 경우 추적 또는 [CloudTrail Lake](#) 이벤트 데이터 스토어를 생성합니다.

CloudTrail 추적

추적을 사용하면 CloudTrail 가 Amazon S3 버킷에 로그 파일을 전달할 수 있습니다. 를 사용하여 생성된 모든 추적 AWS Management Console 은 다중 리전입니다. AWS CLI를 사용하여 단일 리전 또는 다중 리전 추적을 생성할 수 있습니다. 계정 AWS 리전 의 모든 에서 활동을 캡처하기 때문에 다중 리전 추적을 생성하는 것이 좋습니다. 단일 리전 추적을 생성하는 경우 추적의 AWS 리전에 로깅된 이벤트만 볼 수 있습니다. 추적에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 [Creating a trail for your AWS 계정](#) 및 [Creating a trail for an organization](#)을 참조하세요.

추적을 생성하여 에서 Amazon S3 버킷 CloudTrail 에 진행 중인 관리 이벤트의 사본 하나를 무료로 전달할 수 있지만 Amazon S3 스토리지 요금이 있습니다. CloudTrail 요금에 대한 자세한 내용은 [AWS CloudTrail 요금 섹션을](#) 참조하세요. Amazon S3 요금에 대한 자세한 내용은 [Amazon S3 요금](#)을 참조하세요.

CloudTrail Lake 이벤트 데이터 스토어

CloudTrail Lake를 사용하면 이벤트에 대해 SQL기반 쿼리를 실행할 수 있습니다. CloudTrail Lake 는 기존 이벤트를 행 기반 JSON 형식으로 [Apache ORC](#) 형식으로 변환합니다. ORC 는 빠른 데이터 검색에 최적화된 열 스토리지 형식입니다. 이벤트는 이벤트 데이터 스토어로 집계되며, 이벤트 데이터 스토어는 [고급 이벤트 선택기](#)를 적용하여 선택한 기준을 기반으로 하는 변경 불가능한 이벤트 컬렉션입니다. 이벤트 데이터 스토어에 적용하는 선택기는 어떤 이벤트가 지속되고 쿼리할 수 있는지 제어합니다. CloudTrail Lake에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 [AWS CloudTrail Lake 작업을](#) 참조하세요.

CloudTrail Lake 이벤트 데이터 스토어 및 쿼리에는 비용이 발생합니다. 이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 사용할 [요금 옵션](#)을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. CloudTrail 요금에 대한 자세한 내용은 [AWS CloudTrail 요금 섹션을](#) 참조하세요.

AWS 의 최종 사용자 메시징 소셜 데이터 이벤트 CloudTrail

데이터 이벤트는 리소스 기반 또는 리소스에서 수행된 리소스 작업에 대한 정보를 제공합니다(예: Amazon S3 객체 읽기 또는 쓰기). 이를 데이터 영역 작업이라고도 합니다. 데이터 이벤트가 대량 활동인 경우도 있습니다. 기본적으로 CloudTrail 는 데이터 이벤트를 로깅하지 않습니다. CloudTrail 이벤트 기록은 데이터 이벤트를 기록하지 않습니다.

데이터 이벤트에는 추가 요금이 적용됩니다. CloudTrail 요금에 대한 자세한 내용은 [AWS CloudTrail 요금 섹션을](#) 참조하세요.

CloudTrail 콘솔 AWS CLI 또는 CloudTrail API 작업을 사용하여 AWS 최종 사용자 메시징 소셜 리소스 유형에 대한 데이터 이벤트를 로깅할 수 있습니다. 데이터 이벤트를 로깅하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 [Logging data events with the AWS Management Console](#) 및 [Logging data events with the AWS Command Line Interface](#)를 참조하세요.

다음 표에는 데이터 이벤트를 로깅할 수 있는 AWS 최종 사용자 메시징 소셜 리소스 유형이 나열되어 있습니다. 데이터 이벤트 유형(콘솔) 열에는 CloudTrail 콘솔의 데이터 이벤트 유형 목록에서 선택할 값이 표시됩니다. resources.type 값 열에는 AWS CLI 또는 를 사용하여 고급 이벤트 선택기를 구성할 때 지정하는 resources.type 값이 표시됩니다 CloudTrail APIs. 에 APIs 기록된 데이터 CloudTrail 열에는 리소스 유형에 CloudTrail 대해 에 기록된 API 통화가 표시됩니다.

데이터 이벤트 유형(콘솔)	resources.type 값	에 APIs 기록된 데이터 CloudTrail
소셜 메시지 전화번호 ID	AWS::SocialMessaging::PhoneNumberId	<ul style="list-style-type: none"> • DeleteWhatsAppMessageMedia • GetWhatsAppMessageMedia • PostWhatsAppMessageMedia • SendWhatsAppMessage

eventName, readOnly 및 resources.ARN 필드를 필터링하여 중요한 이벤트만 로깅하도록 고급 이벤트 선택기를 구성할 수 있습니다. 이러한 필드에 대한 자세한 내용은 섹션을 참조하세요.

[AdvancedFieldSelector](#) AWS CloudTrail API 참조 의 .

AWS 의 최종 사용자 메시징 소셜 관리 이벤트 CloudTrail

[관리 이벤트](#)는 의 리소스에서 수행되는 관리 작업에 대한 정보를 제공합니다 AWS 계정. 이를 제어 영역 작업이라고도 합니다. 기본적으로 는 관리 이벤트를 CloudTrail 기록합니다.

AWS 최종 사용자 메시징 소셜은 모든 AWS 최종 사용자 메시징 소셜 제어 영역 작업을 관리 이벤트로 기록합니다. AWS 최종 사용자 메시징 소셜이 에 로그인하는 AWS 최종 사용자 메시징 소셜 제어 영역 작업 목록은 [AWS 최종 사용자 메시징 소셜 API 참조](#)를 CloudTrail참조하세요.

AWS 최종 사용자 메시징 소셜 이벤트 예제

이벤트는 모든 소스의 단일 요청을 나타내며 요청된 API 작업, 작업 날짜 및 시간, 요청 파라미터 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 퍼블릭 API 호출의 주문된 스택 추적이 아니므로 이벤트는 특정 순서로 표시되지 않습니다.

다음 예제에서는 작업을 보여주는 CloudTrail 이벤트를 보여줍니다.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "GR632462JDSBDSHHGS39:session",
    "arn": "arn:aws:sts::123456789101:assumed-role/Role_name/Session_name",
    "accountId": "123456789101",
    "accessKeyId": "12345678901234567890",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "GR632462JDSBDEXAMPLE",
        "arn": "arn:aws:sts::123456789101:assumed-role/Role_name/Session_name",
        "accountId": "123456789101",
        "userName": "user"
      },
      "attributes": {
        "creationDate": "2024-10-03T17:25:08Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2024-10-03T17:25:23Z",
  "eventSource": "social-messaging.amazonaws.com",
```

```
    "eventName": "SendWhatsAppMessage",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "1.x.x.x",
    "userAgent": "agent",
    "requestParameters": {
      "originationPhoneNumberId": "phone-number-id-aa012345678901234567890123456789",
      "metaApiVersion": "v20.0",
      "message": "Hi"
    },
    "responseElements": {
      "messageId": "message_id"
    },
    "requestID": "request_id",
    "eventID": "event_id",
    "readOnly": false,
    "resources": [{
      "accountId": "123456789101",
      "type": "AWS::SocialMessaging::PhoneNumberId",
      "ARN": "arn:aws:social-messaging:us-east-1:123456789101:phone-number-id/phone-number-id-aa012345678901234567890123456789"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789101",
    "eventCategory": "Data",
    "tlsDetails": {
      "clientProvidedHostHeader": "social-messaging.us-east-1.amazonaws.com"
    }
  }
}
```

CloudTrail 레코드 내용에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 [CloudTrail 레코드 내용](#)을 참조하세요.

AWS 최종 사용자 메시징 소셜 미디어 모범 사례

이 섹션에서는 고객 참여를 개선하고 계정 일시 중지를 방지하는 데 도움이 될 수 있는 몇 가지 모범 사례를 설명합니다. 그러나 이 단원에서는 법률적인 조언은 다루지 않습니다. 항상 변호사에게 문의하여 법률 자문을 받으세요.

최신 WhatsApp 모범 사례 목록은 [WhatsApp 비즈니스 메시징 정책 섹션](#)을 참조하세요.

주제

- [Up-to-date 비즈니스 프로필](#)
- [권한 획득](#)
- [금지된 메시지 내용](#)
- [고객 목록 감사](#)
- [참여를 기반으로 전송 조정](#)
- [적절한 시간에 전송](#)

Up-to-date 비즈니스 프로필

이메일 주소, 웹 사이트 주소 또는 전화번호와 같은 고객 지원 연락처 정보가 포함된 정확한 up-to-date WhatsApp 비즈니스 프로필을 유지합니다. 제공된 정보가 진실되고 다른 비즈니스를 허위 진술하거나 가장하지 않도록 하세요.

권한 획득

보내려는 특정 유형의 메시지를 받도록 명시적으로 요청하지 않은 수신자에게는 메시지를 보내지 마세요. 다음 옵트인 정보를 유지합니다.

- 옵트인 프로세스는 를 통해 비즈니스에서 메시지 또는 전화를 수신하는 데 동의함을 해당 사람에게 명확하게 알려야 합니다 WhatsApp. 비즈니스 이름을 명시적으로 명시해야 합니다.
- 옵트인 동의를 얻는 방법을 결정하는 것은 전적으로 사용자의 책임입니다. 옵트인 프로세스가 통신에 적용되는 모든 관련 법률을 준수하는지 확인합니다. 필요한 모든 공지를 제공하고 관련 법률에 따라 필요한 모든 권한을 얻습니다.

WhatsApp 옵트인 요구 사항에 대한 자세한 내용은 [WhatsApp](#)

수신자가 온라인 양식을 사용하여 메시지를 수신하도록 가입할 수 있는 경우 자동 스크립트가 모르는 사람이 구독하는 것을 방지하세요. 또한 사용자가 단일 세션에서 전화번호를 제출할 수 있는 횟수를 제한합니다.

연락처 목록에서 해당 사용자를 제거하는 것을 포함하여 통신을 차단, 중단 또는 거부 WhatsApp하기 위해 켜거나 끄는 사람의 모든 요청을 존중합니다.

각 옵트인 요청 및 확인에 대한 날짜, 시간 및 원본을 포함하는 기록을 유지합니다. 또한 고객 목록에 대한 정기 감사를 수행하는 데 도움이 될 수 있습니다.

금지된 메시지 내용

Important

Meta/ 작업WhatsApp

- WhatsApp 비즈니스 솔루션 사용에는 [WhatsApp 비즈니스 서비스 약관](#), [WhatsApp 비즈니스 솔루션 약관](#), [WhatsApp 비즈니스 메시징 정책](#), [WhatsApp 메시징 지침](#), 참조로 통합된 기타 모든 약관, 정책 또는 지침(각각 수시로 업데이트될 수 있음)의 약관이 적용됩니다.
- Meta 또는 WhatsApp 는 언제든지 WhatsApp 비즈니스 솔루션 사용을 금지할 수 있습니다.
- WhatsApp 비즈니스 솔루션 사용과 관련하여 관련 법률 또는 규정에 따라 배포를 보호하거나 제한해야 하는 콘텐츠, 정보 또는 데이터는 제출하지 않습니다.

WhatsApp 정책을 위반하면 일정 기간 동안 메시지 전송이 차단되거나, 항의를 제출할 때까지 잠기거나, 영구적으로 차단될 수 있습니다. Meta는 이메일과 WhatsApp 비즈니스 관리자를 통해 계정 또는 자산이 정책을 위반했는지 여부를 알려줍니다. 모든 항의는 Meta에 해야 합니다. 정책 위반을 보거나 Meta에 항의를 제출하려면 Meta Business 도움말 센터의 [WhatsApp 비즈니스 계정에 대한 정책 위반 세부 정보 보기를 참조하세요](#). 금지된 메시지 콘텐츠의 최신 목록은 [WhatsApp 비즈니스 메시징 정책 섹션](#)을 참조하세요.

다음은 전 세계 모든 메시지 유형에 대해 금지된 콘텐츠 범주입니다. 로 메시지를 보낼 때는 다음 지침을 WhatsApp따르세요.

범주	예시
도박	• 카지노

범주	예시
	<ul style="list-style-type: none"> • 경품행사 • 앱/웹 사이트
고위험 금융 서비스	<ul style="list-style-type: none"> • 월급 대출 • 단기 고이자 대출 • 자동차 대출 • 모기지론 • 학생 대출 • 채권 추심 • 주식 알림 • 암호화폐
부채 탕감	<ul style="list-style-type: none"> • 부채 통합 • 부채 감면 • 신용 회복 프로그램
Get-rich-quick 체계	<ul style="list-style-type: none"> • Work-from-home 프로그램 • 위험-투자 기회 • 피라미드 또는 다단계 마케팅 방식
불법 약물	<ul style="list-style-type: none"> • 대마초/CBD
피싱/스미싱	<ul style="list-style-type: none"> • 사용자가 개인 정보 또는 웹 사이트 로그인 정보를 공개하도록 시도합니다.
S.H.A.F.T.	<ul style="list-style-type: none"> • Sex • 증오 • 알코올 • 총기 • 담배/베이프
타사 리드 생성	<ul style="list-style-type: none"> • 소비자 정보를 구매, 판매 또는 공유하는 회사

고객 목록 감사

반복 WhatsApp 메시지를 보내는 경우 정기적으로 고객 목록을 감사하세요. 고객 목록을 감사하면 메시지를 받는 유일한 고객이 메시지를 수신하려는 고객인지 확인하는 데 도움이 됩니다.

목록을 감사할 때 각 옵트인 고객에게 구독 사실을 알리고 구독 해지 관련 정보를 제공하는 메시지를 전송합니다.

참여를 기반으로 전송 조정

시간에 따라 고객의 우선 순위가 변경될 수 있습니다. 고객이 메시지가 더 이상 유용하지 않다고 판단할 경우 메시지를 완전히 옵트아웃하거나 원치 않는 메시지로 보고할 수 있습니다. 따라서 고객의 참여에 따라 전송 방법을 조정하는 것이 중요합니다.

메시지에 거의 반응하지 않는 고객에 대해서는 메시지 빈도를 조정해야 합니다. 예를 들어, 참여하는 고객에게 주간 메시지를 발송하는 경우 참여도가 낮은 고객을 위해 월간 дай제스트를 별도로 만들 수 있습니다.

마지막으로 전혀 참여하지 않는 고객을 고객 목록에서 제거합니다. 이 단계는 고객이 메시지에 대해 불만을 갖는 것을 방지할 수 있습니다. 또한 비용을 절감하고 발신자로서 평판을 보호할 수 있습니다.

적절한 시간에 전송

정상 주간 업무 시간 동안 메시지를 전송합니다. 저녁 시간이나 밤중에 메시지를 보내면 고객이 방해받지 않도록 목록에서 구독을 취소할 가능성이 높습니다. 고객이 메시지에 즉시 응답할 수 없는 경우 WhatsApp 메시지 전송을 피하고 싶을 수 있습니다.

AWS 최종 사용자 메시징 소셜의 보안

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

보안은 AWS 와 사용자 간의 공동 책임입니다. [공동 책임 모델](#)은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - 에서 AWS 서비스를 실행하는 인프라를 보호할 AWS 책임이 있습니다 AWS 클라우드. AWS 또한 는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 [AWS 규정 준수 프로그램](#) 프로그램의 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. AWS 최종 사용자 메시징 소셜에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 [AWS 범위 내 서비스 규정 준수 프로그램](#) .
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 AWS 최종 사용자 메시징 소셜을 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표에 맞게 AWS 최종 사용자 메시징 소셜을 구성하는 방법을 보여줍니다. 또한 AWS 최종 사용자 메시징 소셜 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

- [AWS 최종 사용자 메시징 소셜의 데이터 보호](#)
- [AWS 최종 사용자 메시징 소셜을 위한 자격 증명 및 액세스 관리](#)
- [AWS 최종 사용자 메시징 소셜에 대한 규정 준수 검증](#)
- [AWS 최종 사용자 메시징 소셜의 복원력](#)
- [AWS 최종 사용자 메시징 소셜의 인프라 보안](#)
- [교차 서비스 혼동된 대리인 방지](#)
- [보안 모범 사례](#)
- [AWS 최종 사용자 메시징 소셜에 서비스 연결 역할 사용](#)

AWS 최종 사용자 메시징 소셜의 데이터 보호

AWS [공동 책임 모델](#) AWS 최종 사용자 메시징 소셜의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든 를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 [데이터 프라이버시 섹션을 FAQ](#) 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 [AWS 책임 공유 모델 및 GDPR](#) 블로그 게시물을 참조하세요.

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

- 각 계정에 다단계 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2가 필요하며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 [CloudTrail 추적 작업을](#) 참조하세요.
- 의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 FIPS 를 AWS 통해 에 액세스할 때 140-3개의 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 API사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 [연방 정보 처리 표준\(FIPS\) 140-3](#)을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, 또는 를 사용하여 AWS 최종 사용자 메시징 소셜 또는 기타 AWS 서비스 로 작업하는 경우가 포함됩니다API AWS CLI AWS SDKs. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL를 제공하는 경우 해당 서버에 대한 요청을 검증URL하기 위해 에 보안 인증 정보를 포함하지 않는 것이 좋습니다.

Important

WhatsApp 는 보안 통신을 위해 신호 프로토콜을 사용합니다. 그러나 AWS 최종 사용자 메시징 소셜은 타사이므로 는 이러한 메시지를 end-to-end 암호화된 것으로 간주하지 않습니다. WhatsApp 않습니다. WhatsApp 데이터 보호에 대한 자세한 내용은 [데이터 프라이버시 및 보안](#) 및 [WhatsApp 암호화 개요](#) 백서를 참조하세요.

데이터 암호화

AWS 최종 사용자 메시징 소셜 데이터는 전송 중 및 AWS 경계 내에서 유휴 상태로 암호화됩니다. AWS 최종 사용자 메시징 소셜에 데이터를 제출하면 데이터를 수신한 대로 암호화하고 저장합니다. AWS 최종 사용자 메시징 소셜에서 데이터를 검색하면 현재 보안 프로토콜을 사용하여 데이터를 전송합니다.

저장 중 암호화

AWS 최종 사용자 메시징 소셜은 AWS 경계 내에 저장된 모든 데이터를 암호화합니다. 여기에는 구성 데이터, 등록 데이터 및 AWS 최종 사용자 메시징 소셜에 추가하는 모든 데이터가 포함됩니다. 데이터를 암호화하기 위해 AWS End User Messaging Social은 서비스가 사용자를 대신하여 소유하고 유지하는 내부 AWS Key Management Service (AWS KMS) 키를 사용합니다. AWS KMS에 대한 자세한 내용은 [AWS Key Management Service 개발자 가이드](#)를 참조하십시오.

전송 중 암호화

AWS 최종 사용자 메시징 소셜은 HTTPS 및 전송 계층 보안(TLS) 1.2를 사용하여 클라이언트, 애플리케이션 및 메타와 통신합니다. 다른 AWS 서비스와 통신하려면 AWS End User Messaging Social에서 HTTPS 및 TLS 1.2를 사용합니다. 또한 콘솔, AWS SDK또는 를 사용하여 AWS SMS 리소스를 생성하고 관리하면 HTTPS 및 TLS 1.2를 사용하여 AWS Command Line Interface모든 통신이 보호됩니다.

키 관리

데이터를 암호화하기 위해 AWS End User Messaging Social은 서비스가 사용자를 대신하여 소유하고 유지하는 내부 AWS KMS 키를 사용합니다. 이들 키는 정기적으로 교체됩니다. AWS 최종 사용자 메시징 소셜에 저장하는 데이터를 암호화하기 위해 자체 키 AWS KMS 또는 기타 키를 프로비저닝하고 사용할 수 없습니다.

인터넷워크 트래픽 개인 정보 보호

Internetwork 트래픽 프라이버시는 AWS 최종 사용자 메시징 소셜과 온프레미스 클라이언트 및 애플리케이션 간의 연결 및 트래픽과 AWS 최종 사용자 메시징 소셜과 동일한 의 기타 AWS 리소스 간의 연결을 보호하는 것을 말합니다 AWS 리전. 다음 기능과 관행은 AWS 최종 사용자 메시징 소셜을 위한 Internetwork 트래픽 프라이버시를 보호하는 데 도움이 될 수 있습니다.

AWS SMS 과 온프레미스 클라이언트 및 애플리케이션 간의 트래픽

AWS 최종 사용자 메시징 소셜과 온프레미스 네트워크의 클라이언트 및 애플리케이션 간에 프라이빗 연결을 설정하려면 를 사용할 수 있습니다 AWS Direct Connect. 이렇게 하면 표준 광섬유 이더넷 케이블을 사용하여 네트워크를 AWS Direct Connect 위치에 연결할 수 있습니다. 케이블의 한쪽 끝이 라우터에 연결되어 있습니다. 다른 쪽 끝은 AWS Direct Connect 라우터에 연결됩니다. 자세한 내용은 AWS Direct Connect사용 설명서의 [AWS Direct Connect 이란 무엇입니까?](#) 섹션을 참조하십시오.

게시된 를 통해 AWS 최종 사용자 메시징 소셜에 안전하게 액세스하려면 API 호출에 대한 AWS 최종 사용자 메시징 소셜 요구 사항을 준수하는 것이 APIs 좋습니다. AWS 최종 사용자 메시징 소셜을 사용하려면 클라이언트가 전송 계층 보안(TLS) 1.2 이상을 사용해야 합니다. 또한 클라이언트는 Ephemeral Diffie-Hellman(PFS) 또는 Elliptic Curve Diffie-Hellman Ephemeral()과 같이 완벽한 순방향 보안(DHE)을 갖춘 암호 제품군을 지원해야 합니다ECDHE. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 액세스 키 ID와 AWS 계정의 AWS Identity and Access Management (IAM) 보안 주체와 연결된 보안 액세스 키를 사용하여 요청에 서명해야 합니다. 또는 [AWS Security Token Service](#)(AWS STS)를 사용해 임시 보안 자격 증명을 생성하여 요청에 서명할 수 있습니다.

AWS 최종 사용자 메시징 소셜을 위한 자격 증명 및 액세스 관리

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 되는 서비스입니다. IAM 관리자는 AWS 최종 사용자 메시징 소셜 리소스를 사용할 수 있는 인증(로그인) 및 권한 부여(권한 보유) 대상을 제어합니다. IAM 는 추가 비용 없이 사용할 수 있는 서비스입니다.

주제

- [고객](#)
- [ID를 통한 인증](#)
- [정책을 사용한 액세스 관리](#)

- [AWS 최종 사용자 메시징 소셜 작업 방식 IAM](#)
- [AWS 최종 사용자 메시징 소셜에 대한 자격 증명 기반 정책 예제](#)
- [AWS 최종 사용자 메시징 소셜에 대한 관리형 정책](#)
- [AWS 최종 사용자 메시징 소셜 ID 및 액세스 문제 해결](#)

고객

AWS Identity and Access Management (IAM) 사용 방법은 AWS 최종 사용자 메시징 소셜에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - AWS 최종 사용자 메시징 소셜 서비스를 사용하여 작업을 수행하는 경우 관리자는 필요한 자격 증명과 권한을 제공합니다. 작업을 수행하는 데 더 많은 AWS 최종 사용자 메시징 소셜 기능을 사용하므로 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. AWS 최종 사용자 메시징 소셜에서 기능에 액세스할 수 없는 경우 섹션을 참조하세요 [AWS 최종 사용자 메시징 소셜 ID 및 액세스 문제 해결](#).

서비스 관리자 - 회사에서 AWS 최종 사용자 메시징 소셜 리소스를 담당하는 경우 AWS 최종 사용자 메시징 소셜에 대한 전체 액세스 권한이 있을 수 있습니다. 서비스 사용자가 액세스해야 하는 AWS 최종 사용자 메시징 소셜 기능 및 리소스를 결정하는 것은 사용자의 작업입니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 이 개념을 이해합니다 IAM. 회사에서 AWS 최종 사용자 메시징 소셜 IAM에서 사용하는 방법에 대한 자세한 내용은 섹션을 참조하세요 [AWS 최종 사용자 메시징 소셜 작업 방식 IAM](#).

IAM 관리자 - IAM 관리자인 경우 AWS 최종 사용자 메시징 소셜에 대한 액세스를 관리하기 위한 정책을 작성하는 방법에 대한 세부 정보를 알고 싶을 수 있습니다. 에서 사용할 수 있는 AWS 최종 사용자 메시징 소셜 자격 증명 기반 정책의 예를 보려면 섹션을 IAM참조하세요 [AWS 최종 사용자 메시징 소셜에 대한 자격 증명 기반 정책 예제](#).

ID를 통한 인증

인증은 자격 증명 AWS 으로 에 로그인하는 방법입니다. 로 AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할을 수입하여 인증(에 로그인 AWS)되어야 합니다.

자격 증명 소스를 통해 제공된 자격 증명을 사용하여 에 페더레이션 자격 증명 AWS 으로 로그인할 수 있습니다. AWS IAM Identity Center (IAM Identity Center) 사용자, 회사의 Single Sign-On 인증 및 Google 또는 Facebook 자격 증명은 페더레이션 자격 증명의 예입니다. 페더레이션 자격 증명으로 로그인하면 관리자가 이전에 IAM 역할을 사용하여 자격 증명 페더레이션을 설정했습니다. 페더레이션을 사용하여 AWS 에 액세스하면 간접적으로 역할을 수입하게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 에 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 [에 로그인하는 방법을 AWS 계정 AWS참조하세요.](#)

AWS 프로그래밍 방식으로 에 액세스하는 경우는 소프트웨어 개발 키트(SDK)와 명령줄 인터페이스(CLI)를 AWS 제공하여 자격 증명을 사용하여 요청에 암호화 방식으로 서명합니다. AWS 도구를 사용하지 않는 경우 직접 요청에 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 [요청 서명을 참조하세요 AWS API.](#)

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, 다중 인증(MFA)을 사용하여 계정의 보안을 강화하는 것이 AWS 좋습니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 [다중 인증 및 사용 설명서의 다중 인증 사용\(MFA\) AWS](#)을 참조하세요IAM.

AWS 계정 루트 사용자

를 생성하면 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 AWS 계정 루트 사용자라고 하며 계정을 생성하는데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 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 작업의 전체 목록은 IAM 사용 설명서의 [루트 사용자 보안 인증이 필요한 작업을](#) 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 포함한 인간 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 AWS 서비스에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, , AWS Directory Service Identity Center 디렉터리 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스에 액세스하는 모든 사용자의 사용자입니다. 페더레이션 자격 증명에 액세스하면 역할을 AWS 계정수입하고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center(을)를 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 및 애플리케이션에서 사용할 수 있도록 자체 자격 증명 소스의 사용자 AWS 계정 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 [IAM Identity Center란 무엇입니까?](#)를 참조하세요.

IAM 사용자 및 그룹

[IAM 사용자](#)는 한 사람 또는 애플리케이션에 대한 특정 권한이 AWS 계정 있는 내 자격 증명입니다. 가능한 경우 암호 및 액세스 키와 같은 장기 보안 인증 정보가 있는 IAM 사용자를 생성하는 대신 임시 보

안 인증 정보를 사용하는 것이 좋습니다. 그러나 IAM 사용자와 장기 보안 인증이 필요한 특정 사용 사례가 있는 경우 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 [장기 보안 인증이 필요한 사용 사례에 대한 액세스 키 정기적으로 교체](#)를 참조하세요.

[IAM 그룹](#)은 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 라는 이름의 그룹을 지정IAMAdmins하고 해당 그룹에 IAM 리소스를 관리할 수 있는 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 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서의 [\(역할 대신\) IAM 사용자를 생성할 시기](#)를 참조하세요.

IAM 역할

[IAM 역할](#)은 특정 권한이 AWS 계정 있는 내 자격 증명입니다. IAM 사용자와 유사하지만 특정 사람과는 관련이 없습니다. IAM 역할을 전환 AWS Management Console 하여 에서 역할을 일시적으로 수임할 수 있습니다. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html 또는 AWS API 작업을 호출 AWS CLI 하거나 사용자 지정 를 사용하여 역할을 수임할 수 있습니다URL. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 [역할 수임 방법](#)을 참조하세요.

IAM 임시 자격 증명이 있는 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 [타사 자격 증명 공급자에 대한 역할 생성](#)을 참조하세요. IAM Identity Center를 사용하는 경우 권한 세트를 구성합니다. 인증 후 자격 증명이 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 의 역할과 상호 연관시킵니다IAM. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 [권한 세트](#)를 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 작업에 대해 다른 권한을 일시적으로 수임할 수 있습니다.
- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 누군가(신뢰할 수 있는 보안 주체)가 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 에서는 정책을 리소스에 직접 연결할 AWS 서비스수 있습니다(역할을 프록시로 사용하는 대신). 크로스 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 [에서 크로스 계정 리소스 액세스를 IAM](#) 참조하세요.

- 교차 서비스 액세스 - 일부는 다른에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어 서비스에서 호출할 때 해당 서비스가 Amazon에서 애플리케이션을 실행EC2하거나 Amazon S3에 객체를 저장하는 것이 일반적입니다. 서비스는 직접적으로 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
- 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여에서 작업을 수행하면 보안 주체로 AWS간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS 는 를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 다른 AWS 서비스 또는 리소스와 의 상호 작용을 완료해야 하는 요청을 수신할 때만 수행됩니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 [액세스 세션 전달](#)을 참조하세요.
- 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수입하는 [IAM 역할](#)입니다. IAM 관리자는 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다IAM. 자세한 내용은 IAM 사용 설명서의 [에 권한을 위임할 역할 생성을 AWS 서비스](#) 참조하세요.
- 서비스 연결 역할 - 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수입할 수 있습니다. 서비스 연결 역할은 에 표시 AWS 계정되며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.
- Amazon에서 실행되는 애플리케이션 EC2 - IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 보안 인증을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장하는 것보다 좋습니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로필에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행 중인 프로그램이 임시 보안 인증을 가져올 수 있습니다. 자세한 내용은 IAM 사용 설명서[EC2의 IAM 역할 사용을 참조하세요](#).

IAM 역할 또는 IAM 사용자를 사용할지 여부를 알아보려면 IAM 사용 설명서의 [IAM 역할 생성 시기\(사용자 대신\)](#)를 참조하세요.

정책을 사용한 액세스 관리

정책을 AWS 생성하고 AWS 자격 증명 또는 리소스에 연결하여 의 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결된 AWS 경우 권한을 정의하는 의 객체입니다. 는 보안 주체(사용자, 루트 사용자 또는 역할 세션)가 요청할 때 이러한 정책을 AWS 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서의 구조 및 내용에 대한 자세한 내용은 IAM 사용 설명서[의 JSON 정책 개요](#)를 참조하세요.

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 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 필요한 리소스에 대한 작업을 수행할 수 있는 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성할 수 있습니다. 그런 다음 관리자는 IAM 정책을 역할에 추가하고 사용자는 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하는 데 사용하는 방법에 관계없이 작업에 대한 권한을 정의합니다. 예를 들어, iam:GetRole 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI 또는 어서 역할 정보를 가져올 수 있습니다 AWS API.

보안 인증 기반 정책

자격 증명 기반 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 생성](#)을 참조하세요.

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 의 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립 실행형 정책입니다 AWS 계정. 관리형 정책에는 AWS 관리형 정책 및 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책 중에서 선택하는 방법을 알아보려면 IAM 사용 설명서의 [관리형 정책 및 인라인 정책 선택](#)을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예로는 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 [보안 주체를 지정](#)해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는 이 포함될 수 있습니다 AWS 서비스.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책IAM에서는 의 AWS 관리형 정책을 사용할 수 없습니다.

액세스 제어 목록(ACLs)

액세스 제어 목록(ACLs)은 리소스에 액세스할 수 있는 권한이 있는 보안 주체(계정 멤버, 사용자 또는 역할)를 제어합니다. ACLs 는 리소스 기반 정책과 유사하지만 JSON 정책 문서 형식을 사용하지는 않습니다.

Amazon S3 AWS WAF 및 Amazon VPC은 를 지원하는 서비스의 예입니다. ACLs. 에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 안내서의 [액세스 제어 목록\(ACL\) 개요](#)를 ACLs 참조하세요.

기타 정책 타입

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

- 권한 경계 - 권한 경계는 자격 증명 기반 정책이 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. Principal 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 [IAM 엔터티에 대한 권한 경계](#)를 참조하세요.
- 서비스 제어 정책(SCPs) - 의 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations. SCPs AWS Organizations 는 비즈니스가 소유 AWS 계정 한 여러 을 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직의 모든 기능을 활성화하면 서비스 제어 정책(SCPs)을 계정의 일부 또는 전체에 적용할 수 있습니다. 는 각 를 포함하여 멤버 계정의 엔터티에 대한 권한을 SCP 제한합니다. AWS 계정 루트 사용자. 조직 및 에 대한 자세한 내용은 AWS Organizations 사용 설명서의 [서비스 제어 정책을](#) SCPs 참조하세요.
- 세션 정책 - 세션 정책은 역할 또는 페더레이션 사용자에게 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 보안 인증 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM 사용 설명서의 [세션 정책을](#) 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. AWS 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 결정하는 방법을 알아보려면 IAM 사용 설명서의 [정책 평가 로직](#)을 참조하세요.

AWS 최종 사용자 메시징 소셜 작업 방식 IAM

IAM 를 사용하여 AWS 최종 사용자 메시징 소셜에 대한 액세스를 관리하기 전에 AWS 최종 사용자 메시징 소셜에서 사용할 수 있는 IAM 기능에 대해 알아보십시오.

IAM AWS 최종 사용자 메시징 소셜에서 사용할 수 있는 기능

IAM 기능	AWS 최종 사용자 메시징 소셜 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예
ACLs	아니요
ABAC (정책의 태그)	부분
임시 보안 인증	예
보안 주체 권한	예
서비스 역할	예
서비스 연결 역할	예

AWS 최종 사용자 메시징 소셜 및 기타 AWS 서비스가 대부분의 IAM 기능을 어떻게 사용하는지 자세히 알아보려면 IAM 사용 설명서의 에서 [AWS 를 사용하는 서비스를 IAM](#) 참조하세요.

AWS 최종 사용자 메시징 소셜에 대한 자격 증명 기반 정책

ID 기반 정책 지원: 예

자격 증명 기반 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 생성](#)을 참조하세요.

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부된 작업 및 리소스와 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 보안 인증 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적

용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 [IAM JSON 정책 요소 참조](#)를 참조하세요.

AWS 최종 사용자 메시징 소셜에 대한 자격 증명 기반 정책 예제

AWS 최종 사용자 메시징 소셜 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요 [AWS 최종 사용자 메시징 소셜에 대한 자격 증명 기반 정책 예제](#).

AWS 최종 사용자 메시징 소셜 내 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예로는 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 [보안 주체를 지정](#)해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는 이 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려면 리소스 기반 정책의 보안 주체로 전체 계정 또는 다른 계정의 IAM 엔터티를 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 보안 주체와 리소스가 다른 계정에 있는 경우 신뢰할 수 있는 AWS 계정 있는 계정의 IAM 관리자는 보안 주체 엔터티(사용자 또는 역할)에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 [에서 크로스 계정 리소스 액세스를 IAM](#) 참조하세요.

AWS 최종 사용자 메시징 소셜에 대한 정책 작업

정책 작업 지원: 예

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 Action 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 연결된 AWS API 작업과 이름이 동일합니다. 일치하는 API 작업이 없는 권한 전용 작업과 같은 몇 가지 예외가 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

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

AWS 최종 사용자 메시징 소셜 작업 목록을 보려면 서비스 승인 참조의 [AWS 최종 사용자 메시징 소셜에서 정의한 작업을](#) 참조하세요.

AWS 최종 사용자 메시징 소셜의 정책 작업은 작업 전에 다음 접두사를 사용합니다.

```
social-messaging
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
  "social-messaging:action1",
  "social-messaging:action2"
]
```

AWS 최종 사용자 메시징 소셜 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요 [AWS 최종 사용자 메시징 소셜에 대한 자격 증명 기반 정책 예제](#).

AWS 최종 사용자 메시징 소셜에 대한 정책 리소스

정책 리소스 지원: 예

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Resource JSON 정책 요소는 작업이 적용되는 객체를 지정합니다. 문장에는 Resource 또는 NotResource 요소가 반드시 추가되어야 합니다. 가장 좋은 방법은 [Amazon 리소스 이름\(ARN\)을 사용하여 리소스를](#) 지정하는 것입니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 태스크를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

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

AWS 최종 사용자 메시징 소셜 리소스 유형 및 해당의 목록을 보려면 서비스 승인 참조의 [AWS 최종 사용자 메시징 소셜에서 정의한 리소스를](#) ARNs 참조하세요. 각 리소스 ARN의 를 지정할 수 있는 작업을 알아보려면 [AWS 최종 사용자 메시징 소셜에서 정의한 작업을](#) 참조하세요.

AWS 최종 사용자 메시징 소셜 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요 [AWS 최종 사용자 메시징 소셜에 대한 자격 증명 기반 정책 예제](#).

AWS 최종 사용자 메시징 소셜의 정책 조건 키

서비스별 정책 조건 키 지원: 예

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 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 작음과 같은 [조건 연산자](#)를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 Condition 요소를 지정하거나 단일 Condition 요소에서 여러 키를 지정하는 경우, AWS는 논리적 AND 태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우는 논리적 OR 작업을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어 리소스에 IAM 사용자 IAM 이름으로 태그가 지정된 경우에만 사용자에게 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [IAM 정책 요소: 변수 및 태그](#)를 참조하세요.

AWS는 전역 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 [AWS 전역 조건 컨텍스트 키](#)를 참조하세요.

AWS 최종 사용자 메시징 소셜 조건 키 목록을 보려면 서비스 승인 참조의 [AWS 최종 사용자 메시징 소셜 조건 키](#)를 참조하세요. 조건 키를 사용할 수 있는 작업 및 리소스를 알아보려면 [AWS 최종 사용자 메시징 소셜에서 정의한 작업을](#) 참조하세요.

AWS 최종 사용자 메시징 소셜 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요 [AWS 최종 사용자 메시징 소셜에 대한 자격 증명 기반 정책 예제](#).

ACLs AWS 최종 사용자 메시징 소셜에서

지원 ACLs: 아니요

액세스 제어 목록(ACLs)은 리소스에 액세스할 수 있는 권한이 있는 보안 주체(계정 멤버, 사용자 또는 역할)를 제어합니다. ACLs는 리소스 기반 정책과 유사하지만 JSON 정책 문서 형식을 사용하지는 않습니다.

ABAC AWS 최종 사용자 메시징 소셜 사용

지원ABAC(정책의 태그): 부분

속성 기반 액세스 제어(ABAC)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. 여기서는 AWS이러한 속성을 태그라고 합니다. IAM 엔터티(사용자 또는 역할) 및 여러 AWS 리소스에 태그를 연결할 수 있습니다. 엔터티 및 리소스에 태그를 지정하는 것은 의 첫 번째 단계입니다ABAC. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하는 ABAC 정책을 설계합니다.

ABAC 는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로워지는 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 [조건 요소](#)에 태그 정보를 제공합니다.

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

에 대한 자세한 내용은 IAM 사용 설명서의 [란 무엇입니까ABAC?](#)를 ABAC참조하세요. 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 [속성 기반 액세스 제어 사용\(ABAC\)](#)을 ABAC참조하세요.

AWS 최종 사용자 메시징 소셜에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

임시 자격 증명을 사용하여 로그인할 때 작동하지 AWS 서비스 않는 경우도 있습니다. 임시 자격 증명으로 AWS 서비스 작업하는 경우를 비롯한 자세한 내용은 IAM 사용 설명서의 [AWS 서비스 에서 작업하는 IAM](#) 섹션을 참조하세요.

사용자 이름 및 암호를 제외한 방법을 AWS Management Console 사용하여 에 로그인하는 경우 임시 자격 증명을 사용합니다. 예를 들어 회사의 Single Sign-On(SSO) 링크를 AWS 사용하여 에 액세스하면 해당 프로세스가 임시 자격 증명을 자동으로 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 [역할\(콘솔\)로 전환](#)을 참조하세요.

AWS CLI 또는 를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS API. 그런 다음 이러한 임시 자격 증명을 사용하여 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 AWS. AWS recommends에 액세스할 수 있습니다. 자세한 내용은 [의 임시 보안 자격 증명을 IAM](#)참조하세요.

AWS 최종 사용자 메시징 소셜에 대한 서비스 간 보안 주체 권한

전달 액세스 세션 지원(FAS): 예

IAM 사용자 또는 역할을 사용하여 에서 작업을 수행하는 경우 보안 주체로 AWS간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS 는 를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 다른 AWS 서비스 또는 리소스와의 상호 작용을 완료해야 하는 요청을 수신할 때만 수행됩니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 [액세스 세션 전달](#)을 참조하세요.

AWS 최종 사용자 메시징 소셜의 서비스 역할

서비스 역할 지원: 예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수입하는 [IAM 역할](#)입니다. IAM 관리자는 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다IAM. 자세한 내용은 IAM 사용 설명서의 [에 권한을 위임할 역할 생성을 AWS 서비스](#) 참조하세요.

Warning

서비스 역할에 대한 권한을 변경하면 AWS 최종 사용자 메시징 소셜 기능이 중단될 수 있습니다. AWS 최종 사용자 메시징 소셜에서 지침을 제공하는 경우에만 서비스 역할을 편집합니다.

AWS 최종 사용자 메시징 소셜의 서비스 연결 역할

서비스 링크 역할 지원: 예

서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수입할 수 있습니다. 서비스 연결 역할은 에 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 [AWS 에서 작동하는 서비스를 참조하세요IAM](#). 서비스 연결 역할 열에서 Yes(이)가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 Yes(네) 링크를 선택합니다.

AWS 최종 사용자 메시징 소셜에 대한 자격 증명 기반 정책 예제

기본적으로 사용자 및 역할에는 AWS 최종 사용자 메시징 소셜 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는

를 사용하여 작업을 수행할 수 없습니다 AWS API. 사용자에게 필요한 리소스에 대한 작업을 수행할 수 있는 권한을 부여하기 위해 IAM 관리자는 IAM 정책을 생성할 수 있습니다. 그런 다음 관리자는 IAM 정책을 역할에 추가하고 사용자는 역할을 수입할 수 있습니다.

이러한 예제 정책 문서를 사용하여 IAM 자격 증명 기반 JSON 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 [IAM 정책 생성](#)을 참조하세요.

각 리소스 유형에 ARNs 대한 형식을 포함하여 AWS 최종 사용자 메시징 소셜에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 승인 참조의 [AWS 최종 사용자 메시징 소셜에 대한 작업, 리소스 및 조건 키](#)를 참조하세요.

주제

- [정책 모범 사례](#)
- [AWS 최종 사용자 메시징 소셜 콘솔 사용](#)
- [사용자가 자신의 고유한 권한을 볼 수 있도록 허용](#)

정책 모범 사례

자격 증명 기반 정책은 계정에서 AWS 최종 사용자 메시징 소셜 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 [관리형 정책](#) 또는 [AWS 작업 함수에 대한 관리형 정책](#)을 참조하세요.
- 최소 권한 적용 - IAM 정책으로 권한을 설정할 때 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. 를 사용하여 권한을 적용하는 IAM 방법에 대한 자세한 내용은 IAM 사용 설명서의 [의 정책 및 권한을 IAM](#) 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 - 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 정책 조건을 작성하여 를 사용하여 모든 요청을 전송하도록 지정할 수 있습니다 SSL. AWS 서비스와 같은 특정 를 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 AWS CloudFormation. 자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: 조건](#)을 참조하세요.

- IAM Access Analyzer를 사용하여 IAM 정책을 검증하여 안전하고 기능적인 권한을 보장합니다. IAM Access Analyzer는 정책이 정책 언어(JSON) 및 IAM 모범 사례를 준수하도록 새 정책 및 기존 IAM 정책을 검증합니다. IAM Access Analyzer는 안전하고 기능적인 정책을 작성하는 데 도움이 되는 100개 이상의 정책 확인 및 실행 가능한 권장 사항을 제공합니다. 자세한 내용은 IAM 사용 설명서의 [IAM Access Analyzer 정책 검증](#)을 참조하세요.
- 다중 인증 필요(MFA) - 에 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 MFA 위해 를 AWS 계정입니다. API 작업을 호출할 MFA 때 를 요구하려면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 [MFA-보호된 API 액세스 구성](#)을 참조하세요.

의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 [의 보안 모범 사례를 IAM](#) 참조하세요.

AWS 최종 사용자 메시징 소셜 콘솔 사용

AWS 최종 사용자 메시징 소셜 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한을 사용하면 에서 AWS 최종 사용자 메시징 소셜 리소스에 대한 세부 정보를 나열하고 볼 수 있어야 합니다. AWS 계정. 최소 필수 권한보다 더 제한적인 자격 증명 기반 정책을 만들면 콘솔이 해당 정책에 연결된 엔터티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 에만 전화를 거는 사용자에게 대해서는 최소 콘솔 권한을 허용할 필요가 없습니다. AWS API. 대신 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 허용합니다.

사용자와 역할이 AWS 최종 사용자 메시징 소셜 콘솔을 계속 사용할 수 있도록 하려면 AWS 최종 사용자 메시징 소셜 *ConsoleAccess* 또는 *ReadOnly* AWS 관리형 정책도 엔터티에 연결합니다. 자세한 내용은 IAM 사용 설명서의 [사용자에게 권한 추가](#)를 참조하세요.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제에서는 IAM 사용자가 사용자 자격 증명에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함되어 있습니다. AWS API.

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

```

```

        "iam:ListGroupsWithUser",
        "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": "*"
}
]
}

```

AWSAWS 최종 사용자 메시징 소셜에 대한 관리형 정책

사용자, 그룹 및 역할에 권한을 추가하려면 직접 정책을 작성하는 것보다 AWS 관리형 정책을 사용하는 것이 더 쉽습니다. 필요한 권한만 팀에 제공하는 [IAM 고객 관리형 정책을 생성하는](#) 데는 시간과 전문성이 필요합니다. 빠르게 시작하려면 AWS 관리형 정책을 사용할 수 있습니다. 이 정책은 일반적인 사용 사례를 다루며 사용자의 AWS 계정에서 사용할 수 있습니다. AWS 관리형 정책에 대한 자세한 내용은 IAM 사용 설명서의 [AWS 관리형 정책을](#) 참조하세요.

AWS 서비스는 AWS 관리형 정책을 유지 관리하고 업데이트합니다. AWS 관리형 정책의 권한은 변경할 수 없습니다. 서비스에서 때때로 추가 권한을 AWS 관리형 정책에 추가하여 새로운 기능을 지원합니다. 이 유형의 업데이트는 정책이 연결된 모든 ID(사용자, 그룹 및 역할)에 적용됩니다. 서비스는 새

로운 기능이 시작되거나 새 작업을 사용할 수 있을 때 AWS 관리형 정책에 업데이트됩니다. 서비스는 AWS 관리형 정책에서 권한을 제거하지 않으므로 정책 업데이트가 기존 권한을 손상시키지 않습니다.

또한 여러 서비스에 걸쳐 있는 작업 기능에 대한 관리형 정책을 AWS 지원합니다. 예를 들어 ReadOnlyAccess AWS 관리형 정책은 모든 AWS 서비스 및 리소스에 대한 읽기 전용 액세스를 제공합니다. 서비스가 새 기능을 시작하면 는 새 작업 및 리소스에 대한 읽기 전용 권한을 AWS 추가합니다. 작업 함수 정책의 목록 및 설명은 IAM 사용 설명서의 [AWS 작업 함수에 대한 관리형 정책을](#) 참조하세요.

AWSAWS 관리형 정책에 대한 최종 사용자 메시징 소셜 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 AWS 최종 사용자 메시징 소셜의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 AWS 최종 사용자 메시징 소셜 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
AWS 최종 사용자 메시징 소셜에서 변경 사항 추적 시작	AWS 최종 사용자 메시징 소셜은 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2024년 9월 26일

AWS 최종 사용자 메시징 소셜 ID 및 액세스 문제 해결

다음 정보를 사용하여 AWS 최종 사용자 메시징 소셜 및 로 작업할 때 발생할 수 있는 일반적인 문제를 진단하고 해결할 수 있습니다IAM.

주제

- [AWS 최종 사용자 메시징 소셜에서 작업을 수행할 권한이 없습니다.](#)
- [iam을 수행할 권한이 없습니다.PassRole](#)
- [내 외부의 사람이 내 AWS 최종 사용자 메시징 소셜 리소스 AWS 계정에 액세스하도록 허용하고 싶습니다.](#)

AWS 최종 사용자 메시징 소셜에서 작업을 수행할 권한이 없습니다.

작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 가상 *my-example-widget* 리소스에 대한 세부 정보를 보려고 하지만 가상 social-messaging:*GetWidget* 권한이 없는 경우에 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: social-messaging:GetWidget on resource: my-example-widget
```

이 경우 social-messaging:*GetWidget* 작업을 사용하여 *my-example-widget* 리소스에 액세스할 수 있도록 mateojackson 사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

iam을 수행할 권한이 없습니다.PassRole

iam:PassRole 작업을 수행할 권한이 없다는 오류가 수신되면 AWS 최종 사용자 메시징 소셜에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있도록 AWS 서비스 허용합니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 라는 IAM 사용자가 콘솔을 사용하여 AWS 최종 사용자 메시징 소셜에서 작업을 수행하려고 marymajor 할 때 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

이 경우, Mary가 iam:PassRole 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 외부의 사람이 내 AWS 최종 사용자 메시징 소셜 리소스 AWS 계정에 액세스하도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACLs)을 지원하는 서비스의 경우 이러한 정책을 사용하여 사용자에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- AWS 최종 사용자 메시징 소셜에서 이러한 기능을 지원하는지 알아보려면 섹션을 참조하세요 [AWS 최종 사용자 메시징 소셜 작업 방식 IAM](#).
- 소유 AWS 계정 한 의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 [소유 AWS 계정 한 다른 의 IAM 사용자에게 액세스 권한 제공을 참조하세요](#).
- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 [타사 AWS 계정 소유 에 대한 액세스 권한 제공을](#) AWS 계정참조하세요.
- 자격 증명 페더레이션을 통해 액세스를 제공하는 방법을 알아보려면 IAM 사용 설명서의 [외부 인증 사용자\(자격 증명 페더레이션\)에 대한 액세스 제공을](#) 참조하세요.
- 교차 계정 액세스를 위한 역할 및 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 [에서 교차 계정 리소스 액세스를 IAM](#) 참조하세요.

AWS 최종 사용자 메시징 소셜에 대한 규정 준수 검증

AWS 서비스가 특정 규정 준수 프로그램의 범위 내에 있는지 알아보려면 [AWS 서비스 규정 준수 프로그램 범위](#) 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반 정보는 [AWS 규정 준수 프로그램](#) 참조하세요.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 [의 보고서 다운로드 AWS Artifact](#).

사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률 및 규정에 따라 AWS 서비스 결정됩니다. 는 규정을 지원하는 다음 리소스를 AWS 제공합니다.

- [보안 및 규정 준수 빠른 시작 안내서](#) - 이 배포 안내서에서는 아키텍처 고려 사항에 대해 설명하고 보안 및 규정 준수에 중점을 둔 에 기존 환경을 배포 AWS 하기 위한 단계를 제공합니다.
- [Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 아키텍처](#) HIPAA- 이 백서에서는 기업이 AWS 를 사용하여 적격 애플리케이션을 생성하는 방법을 설명합니다.

Note

모두 HIPAA 적합한 AWS 서비스 것은 아닙니다. 자세한 내용은 [HIPAA 적격 서비스 참조를](#) 참조하세요.

- [AWS 규정 준수 리소스](#) - 이 워크북 및 가이드 모음은 해당 산업 및 위치에 적용될 수 있습니다.
- [AWS 고객 규정 준수 가이드](#) - 규정 준수의 관점에서 공동 책임 모델을 이해합니다. 이 가이드에는 여러 프레임워크(미국 국립표준기술연구소(), 결제카드 산업보안표준위원회(NIST), 국제표준화기구(ISO) 포함)의 보안 제어PCI에 대한 지침을 보호하고 AWS 서비스 매핑하는 모범 사례가 요약되어 있습니다.
- AWS Config 개발자 안내서의 [규칙을 사용하여 리소스 평가](#) - 이 AWS Config 서비스는 리소스 구성 이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- [AWS Security Hub](#) - 이를 AWS 서비스 통해 내 보안 상태를 포괄적으로 볼 수 있습니다 AWS. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 [Security Hub 제어 참조](#)를 참조하세요.
- [Amazon GuardDuty](#) - 의심스러운 활동 및 악의적인 활동이 있는지 환경을 모니터링하여 AWS 계정, 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. 는 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족DSS하여 PCI 와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 GuardDuty 수 있습니다.
- [AWS Audit Manager](#) - 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 규정 및 업계 표준 준수 및 위험을 관리하는 방법을 간소화할 수 있습니다.

AWS 최종 사용자 메시징 소셜의 복원력

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 기반으로 구축됩니다. 는 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워크와 연결된 물리적으로 분리되고 격리된 여러 가용 영역을 AWS 리전 제공합니다. 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.

AWS 리전 및 가용 영역에 대한 자세한 내용은 [AWS 글로벌 인프라 섹션](#)을 참조하세요.

AWS 글로벌 인프라 외에도 AWS 최종 사용자 메시징 소셜은 데이터 복원력 및 백업 요구 사항을 지원하는 데 도움이 되는 몇 가지 기능을 제공합니다.

AWS 최종 사용자 메시징 소셜의 인프라 보안

관리형 서비스인 AWS 최종 사용자 메시징 소셜은 Amazon Web Services: 보안 프로세스 개요 백서에 설명된 AWS 글로벌 네트워크 보안 절차에 의해 보호됩니다. https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

AWS 게시된 API 호출을 사용하여 네트워크를 통해 AWS 최종 사용자 메시징 소셜에 액세스합니다. 클라이언트는 전송 계층 보안(TLS) 1.0 이상을 지원해야 합니다. TLS 1.2 이상을 사용하는 것이 좋습니다. 또한 클라이언트는 (Ephemeral Diffie-HellmanPFS) 또는 DHE (Elliptic Curve Ephemeral Diffie-Hellman)과 같은 완벽한 순방향 보안ECDHE()을 갖춘 암호 제품군을 지원해야 합니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 액세스 키 ID와 IAM 보안 주체와 연결된 보안 액세스 키를 사용하여 요청에 서명해야 합니다. 또는 [AWS Security Token Service](#)(AWS STS)를 사용하여 임시 보안 인증을 생성하여 요청에 서명할 수 있습니다.

교차 서비스 혼동된 대리인 방지

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. 에서 서비스 AWS간 사칭은 혼동된 대리자 문제를 초래할 수 있습니다. 교차 서비스 가장은 한 서비스(호출하는 서비스)가 다른 서비스(호출되는 서비스)를 직접적으로 호출할 때 발생할 수 있습니다. 직접적으로 호출하는 서비스는 다른 고객의 리소스에 대해 액세스 권한이 없는 방식으로 작동하게 권한을 사용하도록 조작될 수 있습니다. 이를 방지하기 위해 AWS 에서는 계정의 리소스에 대한 액세스 권한이 부여된 서비스 보안 주체를 사용하여 모든 서비스에 대한 데이터를 보호하는 데 도움이 되는 도구를 제공합니다.

리소스 정책에서 [aws:SourceArn](#) 및 [aws:SourceAccount](#) 전역 조건 컨텍스트 키를 사용하여 Social Messaging이 리소스에 다른 서비스를 제공하는 권한을 제한하는 것이 좋습니다. 하나의 리소스만 교차 서비스 액세스와 연결되도록 허용하려는 경우 [aws:SourceArn](#)를 사용하십시오. 해당 계정의 모든 리소스가 교차 서비스 사용과 연결되도록 허용하려는 경우 [aws:SourceAccount](#)을(를) 사용합니다.

혼동된 대리자 문제로부터 보호하는 가장 효과적인 방법은 [aws:SourceArn](#) 글로벌 조건 컨텍스트 키를 전체 리소스와 함께 사용하는 ARN 것입니다. 리소스 ARN 전체를 모르는 경우 또는 여러 리소스를 지정하는 경우 의 알 수 없는 부분에 와일드카드 문자(*)와 함께 [aws:SourceArn](#) 전역 컨텍스트 조건 키를 사용합니다. 예: `arn:aws:social-messaging:*:123456789012:*`.

[aws:SourceArn](#) 값에 Amazon S3 버킷과 같은 계정 ID가 포함되어 있지 않은 경우 두 전역 조건 컨텍스트 키를 모두 사용하여 권한을 제한ARN해야 합니다.

aws:SourceArn 값은 ResourceDescription이어야 합니다.

다음 예제에서는 소셜 메시징에서 aws:SourceArn 및 aws:SourceAccount 전역 조건 컨텍스트 키를 사용하여 혼동된 대리자 문제를 방지하는 방법을 보여줍니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "social-messaging.amazonaws.com"
    },
    "Action": "social-messaging:ActionName",
    "Resource": [
      "arn:aws:social-messaging::ResourceName/*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:social-messaging:*:123456789012:*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

보안 모범 사례

AWS 최종 사용자 메시징 소셜은 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.

- 자신을 포함하여 AWS SMS 리소스를 관리하는 각 사람에 대해 개별 사용자를 생성합니다. AWS 루트 자격 증명을 사용하여 AWS SMS 리소스를 관리하지 마세요.
- 각 사용자에게 각자의 임무를 수행하는 데 필요한 최소 권한 집합을 부여합니다.
- IAM 그룹을 사용하여 여러 사용자의 권한을 효과적으로 관리합니다.
- IAM 자격 증명을 정기적으로 교체합니다.

AWS 최종 사용자 메시징 소셜에 서비스 연결 역할 사용

AWS 최종 사용자 메시징 소셜은 AWS Identity and Access Management (IAM) [서비스 연결 역할](#) 을 사용합니다. 서비스 연결 역할은 AWS 최종 사용자 메시징 소셜에 직접 연결되는 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 AWS 최종 사용자 메시징 소셜에서 사전 정의하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 AWS 최종 사용자 메시징 소셜을 더 쉽게 설정할 수 있습니다. AWS 최종 사용자 메시징 소셜은 서비스 연결 역할의 권한을 정의하며, 달리 정의되지 않는 한 AWS 최종 사용자 메시징 소셜만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책 및 권한 정책이 포함되며 해당 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 실수로 제거할 수 없으므로 AWS 최종 사용자 메시징 소셜 리소스를 보호할 수 있습니다.

서비스 연결 역할을 지원하는 다른 서비스에 대한 자세한 내용은 [AWS 를 사용하여 작업하는 서비스를 IAM](#) 참조하고 서비스 연결 역할 열에서 Yes인 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

AWS 최종 사용자 메시징 소셜에 대한 서비스 연결 역할 권한

AWS 최종 사용자 메시징 소셜은 AWSServiceRoleForSocialMessaging 라는 서비스 연결 역할을 사용하여 지표를 게시하고 소셜 메시지 전송에 대한 인사이트를 제공합니다.

AWSServiceRoleForSocialMessaging 서비스 연결 역할은 다음 서비스를 신뢰하여 역할을 수임합니다.

- `social-messaging.amazonaws.com`

라는 역할 권한 정책은 AWS 최종 사용자 메시징 소셜이 지정된 리소스에 대해 다음 작업을 완료할 수 있도록 AWSSocialMessagingServiceRolePolicy 허용합니다.

- 작업: `all AWS resources in the AWS/SocialMessaging namespace.`에 대한 `"cloudwatch:PutMetricData"`

사용자, 그룹 또는 역할이 서비스 연결 역할을 생성, 편집 또는 삭제할 수 있도록 사용 권한을 구성해야 합니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 권한](#)을 참조하세요.

정책에 대한 업데이트는 섹션을 참조하세요 [AWS 관리형 정책에 대한 최종 사용자 메시징 소셜 업데이트](#).

AWS 최종 사용자 메시징 소셜에 대한 서비스 연결 역할 생성

IAM 콘솔을 사용하여 `AWSEndUserMessagingSocial` - 지표 사용 사례로 서비스 연결 역할을 생성할 수 있습니다. AWS CLI 또는 에서 서비스 이름으로 `social-messaging.amazonaws.com` 서비스 연결 역할을 AWS API 생성합니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 생성](#)을 참조하세요. 이 서비스 연결 역할을 삭제하면 동일한 프로세스를 사용하여 역할을 다시 생성할 수 있습니다.

AWS 최종 사용자 메시징 소셜에 대한 서비스 연결 역할 편집

AWS 최종 사용자 메시징 소셜에서는 `AWSServiceRoleForSocialMessaging` 서비스 연결 역할을 편집할 수 없습니다. 서비스 링크 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 그러나 를 사용하여 역할에 대한 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 편집](#)을 참조하세요.

AWS 최종 사용자 메시징 소셜에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 단, 서비스 링크 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

Note

리소스를 삭제하려고 할 때 AWS 최종 사용자 메시징 소셜 서비스가 역할을 사용하는 경우 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

에서 사용하는 AWS 최종 사용자 메시징 소셜 리소스를 제거하려면 `AWSServiceRoleForSocialMessaging`

1. 를 호출 `list-linked-whatsapp-business-accounts` API 하여 보유한 리소스를 확인합니다.
2. 연결된 각 Whats 앱 비즈니스 계정에 대해 를 호출 `disassociate-whatsapp-business-account` API 하여 `SocialMessaging` 서비스에서 리소스를 제거합니다.
3. 를 `list-linked-whatsapp-business-accounts` API 다시 호출하여 리소스가 반환되지 않는지 확인합니다.

를 사용하여 서비스 연결 역할을 수동으로 삭제하려면 IAM

IAM 콘솔, AWS CLI 또는 AWS API 를 사용하여 `AWSServiceRoleForSocialMessaging` 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 삭제](#)를 참조하세요.

AWS 최종 사용자 메시징 소셜 서비스 연결 역할에 지원되는 리전

AWS 최종 사용자 메시징 소셜은 서비스를 사용할 수 있는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 [AWS 리전 및 엔드포인트](#) 섹션을 참조하십시오.

AWS 최종 사용자 메시징 소셜의 할당량

AWS 계정에는 각 AWS 서비스에 대해 이전에 제한이라고 하는 기본 할당량이 있습니다. 다르게 표시되지 않는 한 리전별로 각 할당량이 적용됩니다. 일부 할당량에 대한 증가를 요청할 수 있으며 다른 할당량은 늘릴 수 없습니다.

AWS 최종 사용자 메시징 소셜의 할당량을 보려면 [Service Quotas 콘솔](#)을 엽니다. 탐색 창에서 AWS 서비스를 선택하고 AWS 최종 사용자 메시징 소셜을 선택합니다.

할당량 증가를 요청하려면 Service Quotas 사용 설명서의 [할당량 증가 요청](#)을 참조하십시오. Service Quotas에서 아직 할당량을 사용할 수 없는 경우 [한도 증가 양식](#)을 사용합니다.

AWS 계정에는 AWS 최종 사용자 메시징 소셜과 관련된 다음과 같은 할당량이 있습니다.

Resource	기본값
WhatsApp 비즈니스 계정(WABA)	리전당 25개

AWS 최종 사용자 메시징 소셜은 API에서 AWS 최종 사용자 메시징 소셜에 수행할 수 있는 요청 수를 제한하는 할당량을 구현합니다 AWS 계정.

Operation	Rate
SendWhatsAppMessage	1,000
PostWhatsAppMessageMedia	100
GetWhatsAppMessageMedia	100
DeleteWhatsAppMessageMedia	100
DisassociateWhatsAppBusinessAccount	10
ListWhatsAppBusinessAccount	10
TagResource	10
UntagResourceRate	10

Operation	Rate
ListTagsForResourceRate	10

AWS 최종 사용자 메시징 소셜 사용 설명서의 문서 기록

다음 표에서는 AWS 최종 사용자 메시징 소셜에 대한 설명서 릴리스를 설명합니다.

변경 사항	설명	날짜
최초 릴리스	AWS 최종 사용자 메시징 소셜 사용 설명서의 최초 릴리스	2024년 10월 10일

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