



Guida per l'utente

# AWS Messaggistica sociale per utenti finali



# AWS Messaggistica sociale per utenti finali: Guida per l'utente

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

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

---

# Table of Contents

Cos'è il social di messaggistica per gli utenti AWS finali? .....	1
Sei un utente di AWS End User Messaging Social per la prima volta? .....	1
Funzionalità di AWS End User Messaging Social .....	1
Servizi correlati .....	2
Accesso ai social di messaggistica per gli utenti AWS finali .....	2
Disponibilità regionale .....	3
Configurazione dei social network di messaggistica per gli utenti AWS finali .....	6
Per registrarti e ottenere un account Account AWS .....	6
Crea un utente con accesso amministrativo .....	7
Passaggi successivi .....	8
Nozioni di base .....	9
Registrazione a WhatsApp .....	9
Prerequisiti .....	9
Registrati tramite la console .....	10
Passaggi successivi .....	14
WhatsApp Account aziendale (WABA) .....	15
Visualizza un WABA .....	16
Aggiungi un WABA .....	16
WhatsApp tipi di account aziendali .....	17
Risorse aggiuntive .....	17
Numeri di telefono .....	19
Considerazioni sul numero di telefono .....	19
Aggiungi un numero di telefono .....	20
Prerequisiti .....	20
Aggiungi un numero di telefono a WABA .....	20
Visualizzare lo stato di un numero di telefono .....	22
Visualizza l'ID di un numero di telefono .....	22
Aumentare i limiti delle conversazioni di messaggistica .....	22
Aumento della velocità .....	24
Comprendere la valutazione della qualità dei numeri di telefono .....	24
Visualizza una valutazione della qualità di un numero di telefono .....	25
Modelli dei messaggi .....	26
Utilizzo di modelli di messaggi con WhatsApp Manager .....	26
Passaggi successivi .....	27

Spacing del modello .....	27
Ottieni feedback sullo stato abbassato di un modello .....	27
Stato e valutazione della qualità del modello .....	28
Motivi per cui un modello viene rifiutato .....	30
Destinazioni di messaggio ed evento .....	32
Aggiungi una destinazione per l'evento .....	32
Prerequisiti .....	32
Aggiungi un messaggio e una destinazione per l'evento .....	33
Policy SNS tematiche crittografate di Amazon .....	33
Passaggi successivi .....	35
Formato di un messaggio e di un evento .....	35
AWS Intestazione dell'evento social di messaggistica per l'utente finale .....	35
Esempio WhatsApp JSON di messaggio di testo .....	36
Esempio WhatsApp JSON di messaggio multimediale .....	37
stato del messaggio .....	38
Stati del messaggio .....	38
Risorse aggiuntive .....	39
Caricamento di file multimediali .....	40
Tipi di file multimediali supportati .....	41
Tipi di file multimediali .....	41
tipi di messaggi .....	44
Risorse aggiuntive .....	44
Invio di messaggi .....	45
Invia un messaggio modello .....	46
Invio di un messaggio multimediale .....	47
Rispondere a un messaggio ricevuto .....	50
Modifica lo stato di lettura di un messaggio .....	50
Rispondi con una reazione .....	51
Scarica un file multimediale su Amazon S3 da WhatsApp .....	51
Esempio di risposta a un messaggio .....	52
Prerequisiti .....	52
Rispondere .....	52
Risorse aggiuntive .....	55
Comprendere la fattura .....	56
Esempio 1: invio di un messaggio modello di marketing .....	60
Esempio 2: apertura di una conversazione di assistenza .....	60

Codici di fatturazione ISO .....	61
Monitoraggio .....	75
Monitoraggio con CloudWatch .....	75
CloudTrail registri .....	76
AWS Messaggistica con l'utente finale Eventi relativi ai dati sociali in CloudTrail .....	78
AWS Messaggistica con l'utente finale Eventi di gestione sociale in CloudTrail .....	79
AWS Esempi di eventi End User Messaging Social .....	80
Best practice .....	82
Up-to-date profilo aziendale .....	82
Acquisizione dell'autorizzazione .....	82
Contenuto proibito dei messaggi .....	83
Controllo degli elenchi dei clienti .....	85
Adattamento dell'invio al coinvolgimento .....	85
Invio in orari appropriati .....	86
Sicurezza .....	87
Protezione dei dati .....	88
Crittografia dei dati .....	89
Crittografia in transito .....	89
Gestione delle chiavi .....	89
Riservatezza del traffico Internet .....	90
Gestione dell'identità e degli accessi .....	90
Destinatari .....	91
Autenticazione con identità .....	92
Gestione dell'accesso con policy .....	95
Come funziona AWS End User Messaging Social con IAM .....	98
Esempi di policy basate su identità .....	105
AWS politiche gestite .....	108
Risoluzione dei problemi .....	109
Convalida della conformità .....	111
Resilienza .....	113
Sicurezza dell'infrastruttura .....	113
Prevenzione del problema "confused deputy" tra servizi .....	113
Best practice di sicurezza .....	115
Uso di ruoli collegati ai servizi .....	115
Autorizzazioni di ruolo collegate al servizio per End User Messaging Social AWS .....	116
Creazione di un ruolo collegato al servizio per AWS End User Messaging Social .....	117

---

Modifica di un ruolo collegato al servizio per End User Messaging Social AWS .....	117
Eliminazione di un ruolo collegato al servizio per End User Messaging Social AWS .....	117
Regioni supportate per i ruoli collegati ai servizi social di messaggistica con l'utente AWS finale .....	118
AWS PrivateLink .....	119
Considerazioni .....	119
Creazione di un endpoint di interfaccia .....	119
Creazione di una policy dell'endpoint .....	120
Quote .....	122
Cronologia dei documenti .....	123
.....	cxxiv

# Cos'è il social di messaggistica per gli utenti AWS finali?

AWS End User Messaging Social, noto anche come social messaging, è un servizio di messaggistica che consente agli sviluppatori di WhatsApp integrarsi nelle proprie applicazioni. Fornisce l'accesso alle funzionalità WhatsApp di messaggistica, consentendo la creazione di contenuti interattivi di marca con immagini, video e pulsanti. Utilizzando questo servizio, puoi aggiungere funzionalità di WhatsApp messaggistica alle tue applicazioni insieme a canali esistenti come SMS e notifiche push. Ciò consente di interagire con i clienti attraverso il loro canale di comunicazione preferito.

Per iniziare, crea un nuovo account WhatsApp aziendale (WABA) utilizzando la procedura di onboarding autoguidata nella console AWS End User Messaging Social oppure collega un account esistente WABA al servizio.

## Argomenti

- [Sei un utente di AWS End User Messaging Social per la prima volta?](#)
- [Funzionalità di AWS End User Messaging Social](#)
- [Servizi correlati](#)
- [Accesso ai social di messaggistica per gli utenti AWS finali](#)
- [Disponibilità regionale](#)

## Sei un utente di AWS End User Messaging Social per la prima volta?

Se sei un utente per la prima volta di AWS End User Messaging Social, ti consigliamo di iniziare leggendo le seguenti sezioni:

- [Configurazione dei social network di messaggistica per gli utenti AWS finali](#)
- [Guida introduttiva a AWS End User Messaging Social](#)
- [Le migliori pratiche per la messaggistica sociale con gli utenti AWS finali](#)

## Funzionalità di AWS End User Messaging Social

AWS End User Messaging Social offre le seguenti caratteristiche e funzionalità:

- Progetta messaggi coerenti e riutilizza i contenuti in modo più efficace [creando e utilizzando modelli di messaggio](#). Un modello di messaggio contiene contenuti e impostazioni che desideri riutilizzare nei messaggi inviati.
- Accesso a funzionalità di messaggistica avanzate per un'esperienza più coinvolgente. Oltre a testo e contenuti multimediali, puoi inviare posizioni e messaggi interattivi.
- Ricevi messaggi di testo e multimediali in arrivo dai tuoi clienti.
- Crea fiducia con i tuoi clienti verificando la tua identità aziendale tramite Meta.

## Servizi correlati

AWS offre altri servizi di messaggistica che possono essere utilizzati insieme in un flusso di lavoro multicanale:

- Utilizza [AWS la messaggistica con l'utente finale SMS](#) per inviare SMS messaggi
- Utilizza [AWS End User Messaging Push](#) per inviare notifiche push
- Usa [Amazon SES](#) per inviare e-mail

## Accesso ai social di messaggistica per gli utenti AWS finali

È possibile accedere a AWS End User Messaging Social utilizzando quanto segue:

### AWS Console End User Messaging Social

L'interfaccia web in cui [creare](#) e gestire le risorse.

### AWS Command Line Interface

Interagisci Servizi AWS utilizzando i comandi nella shell della riga di comando. AWS Command Line Interface È supportato su Windows, macOS e Linux. Per ulteriori informazioni su AWS CLI, vedere la [Guida per AWS Command Line Interface l'utente](#). È possibile trovare i AWS SMS comandi nella Guida ai [AWS CLI comandi](#).

### AWS SDKs

Se preferisci creare applicazioni utilizzando specifiche lingue APIs anziché inviare una richiesta su HTTP oHTTPS, utilizza le librerie, il codice di esempio, i tutorial e le altre risorse fornite da AWS. Queste librerie forniscono funzioni di base che automatizzano le attività, come la firma crittografica delle richieste, il ritentativo delle richieste e la gestione delle risposte agli errori. Queste funzioni



consentono di iniziare in modo più efficiente. Per ulteriori informazioni, consulta [Strumenti su cui basarsi AWS](#).

## Disponibilità regionale

AWS End User Messaging Social è disponibile Regioni AWS in diversi paesi in Nord America, Europa, Asia e Oceania. In ogni regione, AWS gestisce più zone di disponibilità. Queste zone di disponibilità sono fisicamente isolate l'una dall'altra, ma sono unite da connessioni di rete private a bassa latenza, a velocità effettiva elevata e altamente ridondanti. Queste zone di disponibilità vengono utilizzate per fornire alti livelli di disponibilità e ridondanza, riducendo al minimo la latenza.

Per ulteriori informazioni Regioni AWS, consulta [Specificare quali contenuti Regioni AWS il tuo account può utilizzare](#) in. Riferimenti generali di Amazon Web Services Per un elenco di tutte le regioni in cui è attualmente disponibile AWS End User Messaging Social e l'endpoint per ciascuna regione, consulta [Endpoint e quote per gli endpoint](#) di [AWS servizio API](#) e di messaggistica con l'utente AWS finale nella tabella o nella seguente. Riferimenti generali di Amazon Web Services Per ulteriori informazioni sul numero di zone di disponibilità presenti in ciascuna regione, consulta [Infrastruttura globale AWS](#).

### Disponibilità nelle regioni

Nome Regione	Regione	Endpoint	WhatsApp API versione
US East (N. Virginia)	us-east-1	social-messaging.us-east-1.amazonaws.com  social-messaging-fips.us-east-1.api.aws  messaggistica sociale.us-east-1.api.aws	Versione 20 e successive
Stati Uniti orientali (Ohio)	us-east-2	social-messaging.us-east-2.amazonaws.com	Versione 20 e successive

Nome Regione	Regione	Endpoint	WhatsApp API versione
		social-messaging-fips.us-east-2.api.aws  messaggistica sociale.us-east-2.api.aws	
US West (Oregon)	us-west-2	social-messaging.us-west-2.amazonaws.com  social-messaging-fips.us-west-2.api.aws  messaggistica sociale.us-west-2.api.aws	Versione 20 e successive
Asia Pacific (Mumbai)	ap-south-1	social-messaging.ap-south-1.amazonaws.com  messaggistica sociale.ap-south-1.api.aws	Versione 20 e successive
Asia Pacific (Singapore)	ap-southeast-1	social-messaging.ap-southeast-1.amazonaws.com  messaggistica sociale.ap-southeast-1.api.aws	Versione 20 e successive

Nome Regione	Regione	Endpoint	WhatsApp API versione
Europa (Irlanda)	eu-west-1	social-messaging.eu-west-1.amazonaws.com social-messaging.eu-west-1.api.aws	Versione 20 e successive
Europe (London)	eu-west-2	social-messaging.eu-west-2.amazonaws.com social-messaging.eu-west-1.api.aws	Versione 20 e successive

# Configurazione dei social network di messaggistica per gli utenti AWS finali

Prima di utilizzare AWS End User Messaging Social per la prima volta, devi completare la procedura seguente.

Argomenti

- [Per registrarti e ottenere un account Account AWS](#)
- [Crea un utente con accesso amministrativo](#)
- [Passaggi successivi](#)

## Per registrarti e ottenere un account Account AWS

Se non si dispone di un Account AWS, completare la procedura seguente per crearne uno.

Per registrarti a un Account AWS

1. Apri la <https://portal.aws.amazon.com/billing/registrazione>.
2. Segui le istruzioni online.

Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

Quando ti iscrivi a un Account AWS, Utente root dell'account AWS viene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire [attività che richiedono l'accesso di un utente root](#).

AWS Al termine del processo di registrazione, riceverai un'e-mail di conferma da. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo <https://aws.amazon.com/e> scegliendo Il mio account.

## Crea un utente con accesso amministrativo

Dopo aver effettuato la registrazione di un Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministratore in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi [AWS Management Console](#) come proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

Per informazioni sull'accesso utilizzando un utente root, consulta la pagina [Signing in as the root user](#) della Guida per l'utente di Accedi ad AWS .

2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

Per istruzioni, consulta [Abilitare un MFA dispositivo virtuale per l'utente Account AWS root \(console\)](#) nella Guida per l'IAMutente.

Crea un utente con accesso amministrativo

1. Abilita Centro IAM identità.

Per istruzioni, consulta [Abilitazione di AWS IAM Identity Center](#) nella Guida per l'utente di AWS IAM Identity Center .

2. In IAM Identity Center, assegna l'accesso amministrativo a un utente.

Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta [Configurare l'accesso utente con i valori predefiniti IAM Identity Center directory](#) nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'accesso URL che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

Per assistenza nell'accesso mediante un utente IAM Identity Center, consulta [AWS Accedere al portale di accesso](#) nella Guida per l'Accedi ad AWS utente.

## Assegna l'accesso a ulteriori utenti

1. In IAM Identity Center, crea un set di autorizzazioni conforme alla best practice dell'applicazione di autorizzazioni con il privilegio minimo.

Segui le istruzioni riportate nella pagina [Creazione di un set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center .

2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

Per istruzioni, consulta [Aggiungere gruppi](#) nella Guida per l'utente di AWS IAM Identity Center .

## Passaggi successivi

Ora che sei pronto a lavorare con AWS End User Messaging Social, consulta la sezione [Guida introduttiva a AWS End User Messaging Social](#) relativa alla creazione del tuo account WhatsApp aziendale (WABA) o alla migrazione del tuo account aziendale esistente. WhatsApp

# Guida introduttiva a AWS End User Messaging Social

Questi argomenti ti guidano attraverso i passaggi per collegare o migrare il tuo account WhatsApp aziendale (WABA) a AWS End User Messaging Social.

Argomenti

- [Registrazione a WhatsApp](#)

## Registrazione a WhatsApp

Un account WhatsApp aziendale (WABA) consente alla tua azienda di utilizzare la WhatsApp Business Platform per inviare messaggi direttamente ai tuoi clienti. Tutti voi WABAs fate parte del vostro portafoglio aziendale Meta. A WABA contiene le risorse rivolte ai clienti, come il numero di telefono, i modelli e il profilo WhatsApp aziendale. Un profilo WhatsApp aziendale contiene le informazioni di contatto della tua attività che gli utenti possono visualizzare. Per ulteriori informazioni sugli account WhatsApp aziendali, consulta [WhatsApp Account aziendale \(WABA\) nei social di messaggistica per utenti AWS finali](#).

Segui la procedura riportata in questo tutorial per iniziare a utilizzare AWS End User Messaging Social. Utilizza la procedura di registrazione integrata per creare un nuovo account WhatsApp aziendale (WABA) o migrare un account esistente WABA su AWS End User Messaging Social.

## Prerequisiti

### Important

#### Lavorare con Meta/ WhatsApp

- L'utilizzo della WhatsApp Business Solution è soggetto ai termini e alle condizioni dei Termini di [servizio WhatsApp aziendali, dei Termini della WhatsApp Business Solution](#), della [Politica sulla messaggistica WhatsApp aziendale](#), delle [Linee guida sulla WhatsApp messaggistica](#) e a tutti gli altri termini, politiche o linee guida ivi inclusi come riferimento (poiché ciascuno può essere aggiornato di tanto in tanto).
- Meta or WhatsApp può vietare in qualsiasi momento l'uso della WhatsApp Business Solution.
- È necessario creare un account WhatsApp aziendale (« WABA ») con Meta e WhatsApp.

- Devi creare un account Business Manager con Meta e collegarlo al tuoWABA.
- Devi fornirci il controllo del tuoWABA. Su tua richiesta, ti trasferiremo il controllo delle tue WABA spalle in modo ragionevole e tempestivo utilizzando i metodi che Meta ci mette a disposizione.
- In relazione all'utilizzo della WhatsApp Business Solution, non invierai alcun contenuto, informazione o dato soggetto a protezione e/o limitazioni alla distribuzione ai sensi delle leggi e/o dei regolamenti applicabili.
- WhatsAppi prezzi per l'utilizzo della WhatsApp Business Solution sono disponibili alla pagina [Conversation-Based Pricing](#).

- Per creare un account WhatsApp aziendale (WABA), la tua azienda ha bisogno di un account [Meta Business](#). Verifica se la tua azienda ha già un account Meta Business. Se non si dispone di un account Meta Business, è possibile crearne uno durante la procedura di registrazione.
- Per utilizzare un numero di telefono già in uso con l'applicazione WhatsApp Messenger o l'applicazione WhatsApp Business, devi prima eliminarlo.
- Un numero di telefono che può ricevere un codice monouso SMS o vocale (OTP). Il numero di telefono utilizzato per la registrazione viene associato al tuo WhatsApp account e il numero di telefono viene utilizzato quando invii messaggi. Il numero di telefono può ancora essere utilizzato per SMSMMS, e per la messaggistica vocale.
- Se stai importando un numero esistenteWABA, ti servirà PINs per tutti i numeri di telefono associati a quello WABA importato. Per reimpostare un documento smarrito o dimenticatoPIN, segui le istruzioni riportate in [Aggiornamento PIN](#) in WhatsApp Business Platform Cloud API Reference.

## Registrati tramite la console

Segui queste istruzioni per creare un nuovo WhatsApp account, migrare il tuo account esistente o aggiungere un numero di telefono a uno esistenteWABA. Come parte della procedura di registrazione, concedi all'utente AWS finale di messaggistica sociale l'accesso al tuo account WhatsApp aziendale. Inoltre, consenti a AWS End User Messaging Social di fatturarti i messaggi. Per ulteriori informazioni sugli account WhatsApp aziendali, consulta [Comprendere i tipi di account WhatsApp aziendali](#).

1. Apri la console AWS End User Messaging Social all'indirizzo <https://console.aws.amazon.com/social-messaging/>.



2. Scegli Account aziendali.
3. Nella pagina Collega l'account aziendale, scegli Avvia il portale Facebook. Apparirà una nuova finestra di accesso da Meta.
4. Nella finestra di accesso di Meta, inserisci le credenziali del tuo account Facebook.

Nella pagina dell'account WhatsApp aziendale, scegli Aggiungi numero di WhatsApp telefono. Nella pagina Aggiungi numero di WhatsApp telefono, scegli Avvia il portale Facebook. Apparirà una nuova finestra di accesso da Meta.

5. Nella finestra di accesso di Meta, inserisci le credenziali del tuo account Facebook.
6. Come parte della procedura di registrazione, concedi all'utente AWS finale di Messaging Social l'accesso al tuo account WhatsApp aziendale (WABA). Inoltre, consenti a AWS End User Messaging Social di fatturarti i messaggi. Scegli Continua.
7. Per un account Meta Business, scegli un account Meta business esistente o Crea un account Meta Business.

a. (Facoltativo) Se devi creare un account Meta Business, segui questi passaggi:

- b. Per Nome dell'attività, inserisci il nome della tua attività.
- c. Per il sito Web o la URL pagina del profilo aziendale, inserisci il sito Web della tua azienda oppure, se la tua azienda non ha un sito Web, accedi URL alla pagina dei social media.
- d. Per Paese, scegli il paese in cui ha sede la tua attività.
- e. (Facoltativo) Scegli Aggiungi indirizzo e inserisci l'indirizzo della tua attività.


8. Scegli Next (Successivo).
9. Per Scegli un account WhatsApp aziendale, scegli un account WhatsApp aziendale esistente (WABA) oppure, se devi creare un account, scegli Crea un account WhatsApp aziendale.

Per Creare o selezionare un profilo WhatsApp aziendale, scegli un profilo WhatsApp aziendale esistente o Crea un nuovo profilo WhatsApp aziendale.

10. Scegli Next (Successivo).
11. Per Creare un profilo aziendale, inserisci le seguenti informazioni:
  - Per Nome account WhatsApp aziendale, inserisci un nome per il tuo account. Questo campo non è rivolto ai clienti.
  - Per il nome visualizzato del profilo WhatsApp aziendale, inserisci il nome da mostrare ai tuoi clienti quando ricevono un tuo messaggio. Consigliamo di utilizzare il nome della società come nome visualizzato. Il nome viene esaminato da Meta e deve essere conforme alle [regole del](#)

[nome WhatsApp visualizzato](#). Per utilizzare un marchio diverso dal nome della tua azienda, deve esserci un'associazione pubblicata esternamente tra la tua azienda e il marchio. Questa associazione deve essere visualizzata sul tuo sito Web e sul marchio rappresentato dal sito Web del nome visualizzato.

Una volta completata la registrazione, Meta esegue una revisione del nome visualizzato. Meta ti invia un'email per dirti se il nome visualizzato è stato approvato o rifiutato. Se il tuo nome visualizzato viene rifiutato, il limite giornaliero di messaggistica viene abbassato e potresti essere disconnesso. WhatsApp


 Important

Per modificare il nome visualizzato, devi creare un ticket con l'assistenza Meta.

- Per Timezone, scegli il fuso orario in cui ha sede l'attività.
  - Per Categoria, scegli la categoria più adatta alla tua attività. I clienti possono visualizzare la tua categoria come parte delle tue informazioni di contatto.
  - Nel campo Descrizione dell'attività, inserisci una descrizione della società. I clienti possono visualizzare la descrizione della tua attività come parte delle tue informazioni di contatto.
  - Per Sito Web, inserisci il sito Web della tua azienda. I clienti possono visualizzare il tuo sito Web come parte delle tue informazioni di contatto.
  - Scegli Next (Successivo).
12. In Aggiungi un numero di telefono per WhatsApp, inserisci un numero di telefono per la registrazione. Questo numero di telefono viene mostrato ai tuoi clienti quando invii loro un messaggio.
13. Per Scegli come verificare il tuo numero, scegli SMS o Telefonata.
- Quando sei pronto per ricevere il codice di verifica, scegli Avanti.
  - Inserisci il codice di verifica, quindi scegli Avanti.
14. Una volta verificato il tuo numero, puoi scegliere Avanti per chiudere la finestra di Meta.
15. Per l'account WhatsApp aziendale, espandi Tag: facoltativo per aggiungere tag al tuo account WhatsApp aziendale.

I tag sono coppie di chiavi e valori che puoi applicare facoltativamente alle AWS risorse per controllarne l'accesso o l'utilizzo. Scegli Aggiungi nuovo tag e inserisci una coppia chiave-valore da allegare.

16. Un account WhatsApp aziendale può avere un messaggio e una destinazione per l'evento per registrare gli eventi per l'account WhatsApp aziendale e tutte le risorse associate all'account WhatsApp aziendale. Per abilitare la registrazione degli eventi in AmazonSNS, inclusa la registrazione della ricezione di un messaggio da parte di un cliente, devi attivare la pubblicazione di messaggi ed eventi. Per ulteriori informazioni, consulta [Destinazioni di messaggi ed eventi in AWS End User Messaging Social](#).

 Important

Per poter rispondere ai messaggi dei clienti, devi abilitare la pubblicazione di messaggi ed eventi.

Nella sezione Dettagli sulla destinazione del messaggio e dell'evento, attiva la pubblicazione degli eventi. Per AmazonSNS, scegli Nuovo argomento SNS standard Amazon e inserisci un nome in Nome argomento oppure scegli Argomento SNSstandard Amazon esistente e scegli un argomento dall'elenco a discesa Arn degli argomenti.

17. In Numeri di telefono:

Per ogni numero di telefono in Numeri WhtsApp di telefono:

- a. Per la verifica del numero di telefono, inserisci il PIN codice esistente PIN o inserisci un nuovo. Per reimpostare un codice smarrito o dimenticatoPIN, segui le istruzioni riportate nella [sezione Aggiornamento PIN](#) in WhatsApp Business Platform Cloud API Reference.
- b. Per impostazioni aggiuntive:
  - i. Per la regione di localizzazione dei dati, facoltativo, scegli una delle regioni di Meta in cui archiviare i tuoi dati inattivi. Per ulteriori informazioni sulle politiche sulla privacy dei dati di Meta, consulta [Privacy e sicurezza dei dati](#) e [Cloud API Local Storage](#) in the WhatsApp Business Platform Cloud API Reference.
  - ii. I tag sono coppie di chiavi e valori che puoi applicare facoltativamente alle AWS risorse per controllarne l'accesso o l'utilizzo. Scegli Aggiungi nuovo tag e inserisci una coppia chiave-valore da allegare.

18. Un account WhatsApp aziendale può avere un messaggio e una destinazione per l'evento per registrare gli eventi per l'account WhatsApp aziendale e tutte le risorse associate all'account WhatsApp aziendale. Per abilitare la registrazione degli eventi in AmazonSNS, inclusa la registrazione della ricezione di un messaggio da parte di un cliente, devi attivare la pubblicazione

di messaggi ed eventi. Per ulteriori informazioni, consulta [Destinazioni di messaggi ed eventi in AWS End User Messaging Social](#).

 Important

Devi abilitare la pubblicazione di messaggi ed eventi per poter rispondere ai messaggi dei clienti.

Nella sezione Dettagli sulla destinazione dei messaggi e degli eventi, attiva la pubblicazione degli eventi. Per AmazonSNS, scegli Nuovo argomento SNS standard Amazon e inserisci un nome in Nome argomento oppure scegli Argomento SNSstandard Amazon esistente e scegli un argomento dall'elenco a discesa Arn degli argomenti.

19. Per completare la configurazione, scegli Aggiungi numero di telefono.

## Passaggi successivi

Una volta completata la registrazione, puoi iniziare a inviare messaggi. Quando sei pronto per iniziare a inviare messaggi su larga scala, completa [la verifica aziendale](#). Ora che il tuo account WhatsApp aziendale e gli account social di messaggistica per utenti AWS finali sono collegati, consulta i seguenti argomenti:

- Scopri la [destinazione degli eventi](#) per registrare gli eventi e ricevere messaggi in arrivo.
- Scopri come creare [modelli di messaggi](#).
- Scopri come [inviare un messaggio di testo o multimediale](#).
- Scopri come [ricevere un messaggio](#).
- Scopri come utilizzare [gli account aziendali ufficiali](#) per avere un segno di spunta verde accanto al nome visualizzato e aumentare la velocità di trasmissione dei messaggi.

# WhatsApp Account aziendale (WABA) nei social di messaggistica per utenti AWS finali

Con un account WhatsApp aziendale (WABA), puoi utilizzare la piattaforma WhatsApp aziendale per inviare messaggi direttamente ai tuoi clienti. Tutti voi WABAs fate parte del vostro [portafoglio Meta Business](#). Un account WhatsApp aziendale contiene risorse rivolte ai clienti come numero di telefono, modelli e informazioni di contatto aziendali. A WABA può esistere solo in una Regione AWS. Per ulteriori informazioni sugli account WhatsApp aziendali, consulta [Account WhatsApp aziendali](#) nel WhatsApp Business Platform Cloud API Reference.

## Important

### Lavorare con Meta/ WhatsApp

- L'utilizzo della WhatsApp Business Solution è soggetto ai termini e alle condizioni dei Termini di [servizio WhatsApp aziendali, dei Termini della WhatsApp Business Solution](#), della [Politica sulla messaggistica WhatsApp aziendale](#), delle [Linee guida sulla WhatsApp messaggistica](#) e a tutti gli altri termini, politiche o linee guida ivi inclusi come riferimento. Questi potrebbero essere aggiornati di tanto in tanto.
- Meta or WhatsApp può vietare in qualsiasi momento l'uso della WhatsApp Business Solution.
- È necessario creare un account WhatsApp aziendale (WABA) con Meta e WhatsApp.
- Devi creare un account Business Manager con Meta e collegarlo al tuoWABA.
- Devi concederci il controllo del tuoWABA. Su tua richiesta, ti trasferiremo il controllo delle tue WABA spalle in modo ragionevole e tempestivo utilizzando i metodi che Meta ci mette a disposizione.
- In relazione all'utilizzo della WhatsApp Business Solution, non invierai alcun contenuto, informazione o dato soggetto a protezione o limitazioni alla distribuzione ai sensi delle leggi o dei regolamenti applicabili.
- WhatsAppi prezzi per l'uso della WhatsApp Business Solution sono disponibili all'indirizzo <https://developers.facebook.com/docs/whatsapp/pricing>.

- [Visualizza un account WhatsApp aziendale \(WABA\) in AWS End User Messaging Social](#)
- [Aggiungi un account WhatsApp aziendale \(WABA\) in AWS End User Messaging Social](#)
- [Comprendere i tipi di account WhatsApp aziendali](#)

## Visualizza un account WhatsApp aziendale (WABA) in AWS End User Messaging Social

Puoi visualizzare quello WABA associato al tuo Account AWS.

Per visualizzare i WABA dati associati al tuo account

1. Apri la console AWS End User Messaging Social all'indirizzo <https://console.aws.amazon.com/social-messaging/>.
2. In Account aziendali, scegli unWABA.
3. Nella scheda Numeri di telefono, visualizza il numero di telefono, il nome visualizzato, la valutazione della qualità e il numero di conversazioni commerciali avviate che ti restano per la giornata.

Nella scheda Destinazioni dell'evento, visualizza la destinazione dell'evento. Per modificare la destinazione del tuo evento, segui le istruzioni riportate in [Destinazioni di messaggi ed eventi in AWS End User Messaging Social](#).

Nella scheda Modelli, scegli Gestisci modelli di messaggi per modificare i tuoi WhatsApp modelli tramite Meta. Ciascuno WABA ha un limite di 250 modelli.

Nella scheda Tag, puoi gestire i tag WABA delle risorse.

## Aggiungi un account WhatsApp aziendale (WABA) in AWS End User Messaging Social

Aggiungine uno nuovo WABA al tuo account se hai già un profilo WhatsApp aziendale. Come parte della creazione di un nuovoWABA, è necessario aggiungere un [numero di telefono](#) alWABA.

- Per aggiungerne uno nuovo WABA al tuo account, segui i passaggi in [Guida introduttiva a AWS End User Messaging Social](#):

- Nel passaggio 8, scegli il tuo profilo WhatsApp aziendale, quindi scegli Crea un nuovo account WhatsApp aziendale.

## Comprendere i tipi di account WhatsApp aziendali

Il tuo account WhatsApp aziendale determina il modo in cui appari ai tuoi clienti. Quando crei un WhatsApp account, il tuo account sarà un account aziendale. WhatsApp dispone di due tipi di account aziendali:

- Account aziendale: WhatsApp verifica l'autenticità di ogni account sulla piattaforma WhatsApp aziendale. Se un account aziendale ha completato la procedura di verifica aziendale, il nome dell'azienda sarà visibile a tutti gli utenti. Questa funzione aiuta gli utenti a identificare gli account aziendali verificati su WhatsApp.
- Account aziendale ufficiale: oltre ai vantaggi di un account aziendale, un account aziendale ufficiale presenta un segno di spunta verde nel profilo e nelle intestazioni dei thread di chat.

L'approvazione di un account aziendale WhatsApp ufficiale (OBA) richiede la dimostrazione che l'azienda è ben nota e riconosciuta dai consumatori, ad esempio articoli, post di blog o recensioni indipendenti. L'approvazione di un non WhatsApp OBA è garantita, anche se l'azienda fornisce la documentazione richiesta. Il processo di approvazione è soggetto alla revisione e all'approvazione di WhatsApp. WhatsApp non divulga pubblicamente i criteri specifici che utilizza per valutare e approvare le richieste di account aziendali ufficiali. Le aziende che cercano un WhatsApp OBA devono dimostrare la propria reputazione e il proprio riconoscimento, ma l'approvazione finale è a discrezione di WhatsApp.

Quando crei un WhatsApp account, il tuo account sarà un account aziendale. Puoi fornire ai tuoi clienti informazioni sulla tua attività, come sito web, indirizzo e orari. Per le aziende che non hanno completato la verifica WhatsApp aziendale, il nome visualizzato viene visualizzato in piccolo testo accanto al numero di telefono nella visualizzazione dei contatti, non nell'elenco delle chat o nella chat individuale. Una volta completata la verifica Meta Business, il nome visualizzato del WhatsApp mittente verrà visualizzato nell'elenco delle chat e nei singoli thread di chat.

## Risorse aggiuntive

- Per ulteriori informazioni sull'account aziendale e sull'account aziendale ufficiale, consulta Account aziendali nel [WhatsApp Business](#) Platform Cloud API Reference.

- Per ulteriori informazioni sul processo di verifica aziendale, consulta la sezione [Verifica aziendale](#) nel WhatsApp Business Platform Cloud API Reference.



# Numeri di telefono in AWS End User Messaging Social

Tutti gli account WhatsApp aziendali contengono uno o più numeri di telefono utilizzati per verificare la tua identità WhatsApp e vengono utilizzati come parte dell'identità di invio. Puoi avere più numeri di telefono associati a un account WhatsApp aziendale (WABA) e utilizzare ogni numero di telefono per un marchio diverso.

## Argomenti

- [Considerazioni sui numeri di telefono da utilizzare con un account WhatsApp aziendale](#)
- [Aggiungi un numero di telefono a un account WhatsApp aziendale \(WABA\)](#)
- [Visualizzare lo stato di un numero di telefono](#)
- [Visualizza l'ID di un numero di telefono in AWS End User Messaging Social](#)
- [Aumentare i limiti delle conversazioni di messaggistica in WhatsApp](#)
- [Aumenta la velocità di trasmissione dei messaggi in WhatsApp](#)
- [Comprensione della valutazione della qualità dei numeri di telefono in WhatsApp](#)

## Considerazioni sui numeri di telefono da utilizzare con un account WhatsApp aziendale

Quando colleghi un numero di telefono al tuo account WhatsApp aziendale (WABA), devi considerare quanto segue:

- I numeri di telefono possono essere collegati solo WABA a uno alla volta.
- Il numero di telefono può ancora essere utilizzato per SMS e chiamate vocali. MMS
- Ogni numero di telefono ha un punteggio di qualità assegnato da Meta.

È possibile ottenere un numero SMS di telefono compatibile tramite AWS End User Messaging SMS effettuando le seguenti operazioni:

1. Assicurati che il [Paese o l'area geografica](#) del numero di telefono supporti la modalità bidirezionaleSMS.
2. Richiedi il [numero di telefono](#). A seconda del Paese o della regione, potrebbe essere necessario registrare il numero di telefono.

3. [Abilita la SMS messaggistica bidirezionale](#) per il numero di telefono. Una volta completata la configurazione, i SMS messaggi in arrivo vengono inviati alla destinazione dell'evento.

## Aggiungi un numero di telefono a un account WhatsApp aziendale (WABA)

Puoi aggiungere numeri di telefono a un account WhatsApp aziendale esistente (WABA) o crearne uno nuovo WABA per il numero di telefono.

### Prerequisiti

Prima di iniziare, verifica che siano stati soddisfatti i seguenti prerequisiti:


- Il numero di telefono deve essere in grado di ricevere un codice monouso SMS o vocale (V). OTP. Questo è il numero di telefono che viene aggiunto al tuo WABA.
- Il numero di telefono non deve essere associato a nessun altro WABA.

## Aggiungi un numero di telefono a WABA

Per aggiungere un nuovo numero di telefono a quello esistente WABA

1. Apri la console AWS End User Messaging Social all'indirizzo <https://console.aws.amazon.com/social-messaging/>.
2. Scegli Account aziendali, quindi Aggiungi numero di WhatsApp telefono.
3. Nella pagina Aggiungi numero di WhatsApp telefono, scegli Avvia il portale Facebook. Apparirà una nuova finestra di accesso da Meta.
4. Nella finestra di accesso di Meta, inserisci le credenziali del tuo account di sviluppatore Meta e scegli il tuo portafoglio aziendale.
5. Scegli WABA il profilo dell' WhatsApp azienda a cui desideri aggiungere il numero di telefono.
6. Scegli Next (Successivo).
7. In Aggiungi un numero di telefono per WhatsApp, inserisci un numero di telefono per la registrazione. Questo numero di telefono viene mostrato ai tuoi clienti quando invii loro un messaggio.
8. Per Scegli come verificare il tuo numero, scegli SMS o Chiamata telefonica.

9. Quando sei pronto per ricevere il codice di verifica, scegli Avanti
10. Inserisci il codice di verifica, quindi scegli Avanti. Una volta verificato il tuo numero, puoi scegliere Avanti per chiudere la finestra di Meta.
11. In Numeri WhatsApp di telefono:
  - a. Per la verifica del numero di telefono, inserisci il PIN codice esistente PIN o inserisci un nuovo. Per reimpostare un codice smarrito o dimenticato PIN, segui le istruzioni riportate nella [sezione Aggiornamento PIN](#) in WhatsApp Business Platform Cloud API Reference.
  - b. Per impostazioni aggiuntive:
    - i. Per la regione di localizzazione dei dati, facoltativo, scegli una delle regioni di Meta in cui archiviare i dati inattivi. Per ulteriori informazioni sulle politiche sulla privacy dei dati di Meta, consulta [Privacy e sicurezza dei dati](#) e [Cloud API Local Storage](#) in the WhatsAppBusiness Platform Cloud API Reference.
    - ii. I tag sono coppie di chiavi e valori che puoi applicare facoltativamente alle AWS risorse per controllarne l'accesso o l'utilizzo. Scegli Aggiungi nuovo tag e inserisci una coppia chiave-valore da allegare.
12. Un account WhatsApp aziendale può avere un messaggio e una destinazione per l'evento per registrare gli eventi per l'account WhatsApp aziendale e tutte le risorse associate all'account WhatsApp aziendale. Per abilitare la registrazione degli eventi in AmazonSNS, inclusa la registrazione della ricezione di un messaggio da parte di un cliente, attiva la pubblicazione di messaggi ed eventi. Per ulteriori informazioni, consulta [Destinazioni di messaggi ed eventi in AWS End User Messaging Social](#).

 Important

Devi abilitare la pubblicazione di messaggi ed eventi per poter rispondere ai messaggi dei clienti.

Nella sezione Dettagli sulla destinazione dei messaggi e degli eventi, attiva la pubblicazione degli eventi. Per AmazonSNS, scegli Nuovo argomento SNS standard Amazon e inserisci un nome in Nome argomento oppure scegli Argomento SNSstandard Amazon esistente e scegli un argomento dall'elenco a discesa Arn degli argomenti.

13. Per completare la configurazione, scegli Aggiungi numero di telefono.

## Visualizzare lo stato di un numero di telefono

Per poter inviare messaggi in AWS End User Messaging Social, lo stato del numero di telefono deve essere Attivo.

1. Apri la console AWS End User Messaging Social all'indirizzo <https://console.aws.amazon.com/social-messaging/>.
2. Scegliere Phone numbers (Numeri di telefono).
3. Nella sezione Numeri di telefono, la colonna Stato riporta lo stato di ogni numero di telefono.

### Note

Se lo stato di un numero di telefono è Configurazione incompleta, puoi scegliere il numero di telefono e quindi scegliere Configurazione completa per completare la configurazione del numero di telefono.

## Visualizza l'ID di un numero di telefono in AWS End User Messaging Social

Per poter inviare messaggi con AWS CLI, è necessario l'ID del numero di telefono per identificare il numero di telefono da utilizzare per l'invio.

1. Apri la console AWS End User Messaging Social all'indirizzo <https://console.aws.amazon.com/social-messaging/>.
2. Scegliere Phone numbers (Numeri di telefono).
3. Nella sezione Numeri di telefono scegli un numero di telefono.
4. La sezione Dettagli del numero di telefono contiene l'ID del numero di telefono.

## Aumentare i limiti delle conversazioni di messaggistica in WhatsApp

I limiti di messaggistica si riferiscono al numero massimo di conversazioni avviate da un'azienda in un periodo di 24 ore. I numeri di telefono aziendali sono inizialmente limitati a 250 conversazioni avviate dall'azienda in un periodo di trasloco di 24 ore. Questo limite può essere aumentato da Meta in base

alla valutazione della qualità dei tuoi messaggi e al numero di messaggi che invii. Le conversazioni avviate dall'azienda possono utilizzare solo messaggi modello.

Quando un cliente ti invia un messaggio, si apre una finestra di assistenza di 24 ore su 24. Durante questo periodo, puoi inviare tutti i [tipi di messaggi](#).

Puoi aumentare il limite di messaggistica a 1.000 messaggi da solo seguendo queste linee guida:

- Il numero di telefono aziendale deve avere [lo stato Attivo](#).
- Se il numero di telefono aziendale ha una [classificazione di bassa qualità](#), potrebbe continuare a essere limitato a 250 conversazioni avviate dall'azienda al giorno fino a quando il livello di qualità non migliorerà.
- [Richiedi la verifica aziendale](#). Se la tua attività viene approvata, la qualità della messaggistica verrà analizzata per determinare se la tua attività di messaggistica giustifica un aumento del limite di messaggistica. In base all'analisi, la tua richiesta di aumento del limite di messaggistica verrà approvata o respinta da Meta.
- Richiedi la [verifica dell'identità](#). Se completi la verifica dell'identità e la tua identità viene confermata, Meta approverà un aumento del limite di messaggistica.
- Apri 1.000 o più conversazioni avviate dall'azienda in un periodo di trasloco di 30 giorni utilizzando un modello con un punteggio di alta qualità. Una volta raggiunta la soglia delle 1.000 conversazioni, la qualità della messaggistica verrà analizzata per determinare se l'attività di messaggistica giustifica un aumento del limite di messaggistica. L'obiettivo è inviare messaggi di alta qualità in modo coerente per aumentare potenzialmente il limite di messaggistica.

Se hai completato la verifica aziendale o la verifica dell'identità o hai aperto 1.000 o più conversazioni commerciali e hai ancora un limite di 250 conversazioni avviate dall'azienda, invia una richiesta a Meta per un upgrade al livello di messaggi.

Se la verifica della tua attività o dell'identità viene rifiutata, puoi aumentare le tue possibilità di ottenere l'approvazione inviando messaggi di alta qualità. Inviando messaggi di alta qualità, conformi e con consenso esplicito, l'attività e la qualità della messaggistica potrebbero essere rivalutate, con un potenziale aumento delle funzionalità di messaggistica approvate.

Il punteggio di qualità della messaggistica su WhatsApp viene calcolato in base ai feedback e alle interazioni recenti degli utenti, dando maggiore importanza ai dati più recenti. Questo aiuta a valutare la qualità e l'affidabilità complessive della messaggistica sulla piattaforma.

## Il livello dei limiti dei messaggi aumenta

- 1.000 conversazioni avviate dall'azienda
- 10.000 conversazioni avviate dall'azienda
- 100.000 conversazioni avviate dall'azienda
- Un numero illimitato di conversazioni avviate dall'azienda

## Aumenta la velocità di trasmissione dei messaggi in WhatsApp

La velocità effettiva dei messaggi è il numero di messaggi in entrata e in uscita al secondo (MPS) per un numero di telefono. Per impostazione predefinita, ogni numero di telefono ha un MPS valore di 80. Meta può aumentare il tuo MPS valore fino a 1.000 se soddisfi i seguenti requisiti:

- Il numero di telefono deve essere in grado di inviare un numero illimitato di conversazioni [avviate dall'azienda](#)
- Il numero di telefono deve avere una [valutazione di qualità](#) media o superiore.

## Comprensione della valutazione della qualità dei numeri di telefono in WhatsApp

La qualità del numero di telefono e dei messaggi è determinata da Meta. Il tuo punteggio di qualità dei messaggi si basa sul modo in cui i tuoi messaggi sono stati ricevuti dai clienti negli ultimi sette giorni, con un peso maggiore per i messaggi più recenti. Il punteggio di qualità della messaggistica viene calcolato in base a una combinazione di segnali di qualità provenienti dalle conversazioni tra te e i tuoi WhatsApp utenti. Questi segnali includono il feedback degli utenti, ad esempio blocchi, report e i motivi adottati dagli utenti quando bloccano un'attività. Meta valuta la qualità dei tuoi messaggi in base al modo in cui vengono ricevuti dai tuoi clienti WhatsApp, concentrandosi sui feedback e sulle interazioni recenti.

### WhatsApp valutazioni della qualità dei numeri di telefono

- Verde: alta qualità
- Giallo: qualità media
- Rosso: bassa qualità

## WhatsApp stato del numero di telefono

- **Connesso:** puoi inviare messaggi entro la tua quota di messaggi.
- **Contrassegnato:** la qualità del tuo numero di telefono è bassa e deve essere migliorata. Se la qualità non migliora entro sette giorni, lo stato del numero di telefono viene impostato su Connesso, ma il limite delle conversazioni avviate dall'azienda viene abbassato di un livello.
- **Limitato:** hai raggiunto il limite di conversazioni avviate dall'azienda per l'attuale periodo di 24 ore. Puoi comunque rispondere ai messaggi in arrivo. Una volta trascorso il periodo di 24 ore, puoi inviare nuovamente i messaggi.

## Visualizza una valutazione della qualità di un numero di telefono

Segui queste istruzioni per visualizzare la qualità dei numeri di telefono.

1. Apri la console AWS End User Messaging Social all'indirizzo <https://console.aws.amazon.com/social-messaging/>.
2. In Account aziendali, scegli un account WhatsApp aziendale (WABA).
3. Nella scheda Numeri di telefono, visualizza il numero di telefono, il nome visualizzato, la valutazione della qualità e il numero di conversazioni avviate dall'azienda che ti restano per la giornata.

# Utilizzo di modelli di messaggi in AWS End User Messaging Social

È possibile utilizzare modelli di messaggio per i tipi di messaggio che si utilizzano di frequente, ad esempio newsletter settimanali o promemoria di appuntamenti. I messaggi modello sono l'unico tipo di messaggio che può essere inviato ai clienti che non ti hanno ancora inviato un messaggio o che non te lo hanno inviato nelle ultime 24 ore.

Meta assegna a ciascun modello una valutazione e uno status di qualità. La valutazione di qualità influisce sullo stato del modello e ne riduce il ritmo o la velocità di invio.

I modelli sono associati al tuo account WhatsApp aziendale (WABA), gestiti tramite il WhatsApp Manager e esaminati da WhatsApp.

Puoi inviare i seguenti tipi di modelli:

- Basato su testo
- Basato su media
- Messaggio interattivo
- Basato sulla posizione
- Modelli di autenticazione con pulsanti monouso
- Modelli di messaggi multiprodotto

Meta fornisce modelli di esempio preapprovati. Per saperne di più, consulta [Modelli di messaggi di esempio](#).

Per ulteriori informazioni sui tipi di modelli di messaggio, consulta [Modello di messaggio](#) nel WhatsApp Business Platform Cloud API Reference.

## Utilizzo di modelli di messaggi con WhatsApp Manager

Usa il [WhatsAppManager](#) per creare, modificare o controllare lo stato di un modello.

1. Apri la console AWS End User Messaging Social all'indirizzo <https://console.aws.amazon.com/social-messaging/>.



2. Scegli Account aziendale, quindi scegli unWABA.
3. Nella scheda Modelli di messaggi, scegli Gestisci modelli di messaggi. Il [WhatsApp gestore](#) si apre in una nuova finestra in cui puoi gestire i tuoi modelli scegliendo Modelli di messaggi.

## Passaggi successivi

Dopo aver creato o modificato un modello, devi inviarlo per la revisione con WhatsApp. La visualizzazione della visualizzazione di Meta può richiedere fino a 24 ore. Meta invia un'email all'amministratore di Business Manager e aggiorna lo stato del modello in WhatsApp Manager. Usa il [WhatsApp gestore](#) per controllare lo stato del tuo modello.

## Comprendere la tempistica dei modelli WhatsApp

Il template pacing è un metodo, utilizzato da Meta, che concede tempo per dare un feedback tempestivo ai clienti sui modelli nuovi o modificati. Identifica e mette in pausa i modelli che ricevono scarso coinvolgimento o feedback, dandoti il tempo di modificare il contenuto del modello prima di inviarlo a troppi clienti. Ciò riduce il rischio che il feedback negativo dei clienti influisca sull'attività. Ad esempio, se troppi clienti «bloccano» il tuo messaggio o se il tuo modello ha percentuali di lettura basse, la valutazione della qualità del modello può essere ridotta.

Il ritmo dei modelli influisce sui modelli appena creati, sui modelli che non sono stati messi in pausa e sui modelli senza un punteggio di qualità elevato. Il ritmo dei modelli viene spesso avviato da una cronologia precedente di modelli di bassa qualità o in pausa. Quando un modello è impostato, i messaggi che utilizzano quel modello vengono inviati normalmente fino a una certa soglia determinata da Meta. Dopodiché, vengono conservati i messaggi successivi per lasciare il tempo necessario per il feedback dei clienti. Se il feedback è positivo, il ritmo del modello viene quindi aumentato. Se il feedback è negativo, il ritmo del modello viene abbassato, consentendoti di modificare il contenuto del modello. Per ulteriori informazioni, consulta [Template pacing](#) nel WhatsApp Business Platform Cloud Reference. API

## Ottieni feedback sullo stato ridotto di un modello con Manager WhatsApp

Meta fornisce informazioni sul motivo per cui lo stato di un modello è stato abbassato. Usa il feedback di Meta per modificare il modello e inviarlo per la nuova approvazione, usa un modello diverso o

cambia il comportamento della tua applicazione. Se modifichi il modello di messaggio e questo viene nuovamente approvato, la sua valutazione di qualità migliorerà gradualmente, purché non riceva feedback negativi frequenti o percentuali di lettura basse.

1. Apri la console AWS End User Messaging Social all'indirizzo <https://console.aws.amazon.com/social-messaging/>.
2. Scegli Account aziendale, quindi scegli unWABA.
3. Nella scheda Modelli di messaggi, scegli Gestisci modelli di messaggi. Il [WhatsApp gestore](#) si apre in una nuova finestra.
4. Scegli Modelli di messaggi e passa il mouse sul modello. Dovrebbe apparire un tooltip con un feedback sul motivo per cui la valutazione è stata abbassata.

## Comprendere lo stato e la valutazione di qualità di un modello in WhatsApp

A ogni modello di messaggio viene assegnata una valutazione di qualità basata sull'utilizzo, sul feedback dei clienti e sul coinvolgimento dei clienti. Un modello può essere utilizzato solo se lo stato è Attivo, ma la qualità determina il ritmo del modello. Se un modello di messaggio riceve costantemente feedback negativi o registra uno scarso coinvolgimento, ciò provocherà un cambiamento nello stato del modello.

Meta modifica automaticamente lo stato o la valutazione di qualità di un modello in base al feedback e al coinvolgimento negativi o positivi. Se lo stato del modello cambia, riceverai una notifica al WhatsApp Manager, un'e-mail e una notifica di eventi. Usa il [WhatsApp gestore](#) per controllare lo stato del tuo modello.

Se il modello viene rifiutato da WhatsApp, puoi modificarlo e inviarlo nuovamente per l'approvazione o presentare un ricorso con WhatsApp. Per ulteriori informazioni, consulta [Appeals](#) in WhatsApp Business Platform Cloud API Reference.

Status del template	Valutazione della qualità	Significato
In fase di revisione		Il modello di messaggio è in fase di revisione. L'esecuzione di questa operazione può richiedere fino a 24 ore.

Status del template	Valutazione della qualità	Significato
Rifiutato		Il modello di messaggio è stato rifiutato e puoi presentarne un ricorso.
Attivo	In attesa	Il modello di messaggio non ha ricevuto feedback sulla qualità o informazioni sulla percentuale di lettura dai clienti, ma può ancora essere utilizzato per inviare messaggi.
Attivo	Elevata	Il modello di messaggio ha ricevuto pochi o nessun feedback negativo da parte dei clienti e può essere utilizzato per inviare messaggi.
Attivo	Media	Il modello di messaggio ha ricevuto feedback negativi dai clienti o ha ricevuto percentuali di lettura basse e potrebbe essere messo in pausa o disattivato.

Status del template	Valutazione della qualità	Significato
Attivo	Bassa	<p>Il modello di messaggio ha ricevuto feedback negativi dai clienti o tassi di lettura bassi. I modelli di messaggio con questo stato possono essere utilizzati, ma rischiano di essere sospesi o disabilitati.</p> <p>Quando un modello passa allo stato Active-Low, l'invio viene sospeso. La prima pausa dura tre ore, la seconda pausa è di sei ore e la pausa successiva disabilita il modello.</p>
In pausa		<p>Il modello di messaggio è stato messo in pausa a causa di feedback negativi ricorrenti da parte dei clienti o di bassi tassi di lettura.</p>
Disabilitato		<p>Il modello di messaggio è stato disabilitato a causa di feedback negativi ricorrenti da parte dei clienti.</p>
Appello richiesto		<p>Un ricorso è stato richiesto.</p>

## Motivi per cui un modello viene rifiutato in WhatsApp

Se il tuo modello di messaggio viene esaminato e rifiutato da Meta, riceverai un'email che spiega perché il modello è stato rifiutato. Puoi presentare ricorso contro il rifiuto o modificare il modello del tuo messaggio. Questi sono alcuni dei motivi più comuni per cui Meta potrebbe rifiutare un modello di messaggio:

- I parametri variabili contengono caratteri speciali, come #, \$ o%.
- I parametri variabili sono mancanti, presentano parentesi graffe non corrispondenti o non sono sequenziali.
- [Il modello di messaggio contiene contenuti che violano la politica commerciale o WhatsApp la politica aziendale. WhatsApps](#)

Per ulteriori informazioni, consulta [Common Rejection Reasons](#) nel WhatsApp Business Platform Cloud API Reference.

# Destinazioni di messaggi ed eventi in AWS End User Messaging Social

La destinazione di un evento è un SNS argomento di Amazon a cui vengono inviati WhatsApp gli eventi. Quando attivi la pubblicazione di eventi su un SNS argomento Amazon, tutti gli eventi di invio e ricezione vengono inviati all'SNSargomento Amazon. Utilizza gli eventi per monitorare, tracciare e analizzare lo stato dei messaggi in uscita e delle comunicazioni in arrivo con i clienti.

Ogni account WhatsApp aziendale (WABA) può avere una destinazione per l'evento. Tutti gli eventi di tutte le risorse associate all'account WhatsApp aziendale vengono registrati nella destinazione dell'evento. Ad esempio, potresti avere un account WhatsApp aziendale a cui sono associati tre numeri di telefono e tutti gli eventi di quei numeri di telefono vengono registrati nell'unica destinazione dell'evento.

## Argomenti

- [Aggiungi un messaggio e una destinazione di eventi a AWS End User Messaging Social](#)
- [Formato di messaggi ed eventi in AWS End User Messaging Social](#)
- [WhatsApp stato del messaggio](#)

## Aggiungi un messaggio e una destinazione di eventi a AWS End User Messaging Social

Quando attivi la pubblicazione di messaggi ed eventi, tutti gli eventi generati dal tuo account WhatsApp aziendale (WABA) vengono inviati all'SNSargomento Amazon. Ciò include gli eventi per ogni numero di telefono associato a un account WhatsApp aziendale. WABAPuoi avere un SNS argomento Amazon associato ad esso.

## Prerequisiti

Prima di iniziare, è necessario soddisfare i seguenti prerequisiti.

- (Facoltativo) Per utilizzare un SNS argomento Amazon crittografato tramite AWS KMS chiavi, devi concedere le autorizzazioni AWS End User Messaging Social per la [politica delle chiavi esistente](#).

## Aggiungi un messaggio e una destinazione per l'evento

1. Apri la console AWS End User Messaging Social all'indirizzo <https://console.aws.amazon.com/social-messaging/>.
2. Scegli Account aziendale, quindi scegli unWABA.
3. Nella scheda Destinazione dell'evento, scegli Modifica destinazione.
4. Per attivare la destinazione di un evento, scegli Abilita.
5. Per inviare i tuoi eventi a una nuova SNS destinazione Amazon, scegli Nuovo argomento SNS dello stand e inserisci un nome in Nome argomento. L'SNSargomento Amazon viene creato con le autorizzazioni per consentire all'utente AWS finale di messaggistica sociale di accedere all'argomento.

### Note

SNSFIFO Gli argomenti di Amazon non sono supportati.

Per inviare i tuoi eventi a una SNS destinazione Amazon esistente, scegli Argomento SNS standard esistente e scegli un argomento da Topic arn. Devi applicare le seguenti autorizzazioni all'SNSargomento Amazon:

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

6. Scegli Save changes (Salva modifiche).

## Policy SNS tematiche crittografate di Amazon

Puoi utilizzare SNS argomenti Amazon crittografati tramite AWS KMS chiavi per un ulteriore livello di sicurezza. Questo livello aggiuntivo di sicurezza può essere utile se l'applicazione gestisce dati privati

o sensibili. Per ulteriori informazioni sulla crittografia SNS degli argomenti di Amazon utilizzando AWS KMS le chiavi, consulta [Abilitare la compatibilità tra le fonti di eventi AWS dei servizi e gli argomenti crittografati](#) nella Amazon Simple Notification Service Developer Guide.

### Note

SNSFIFO Gli argomenti di Amazon non sono supportati.

L'istruzione di esempio utilizza le SourceArn condizioni, facoltative ma consigliate, SourceAccount per evitare il confuso problema dell'assistente e solo l'account proprietario di AWS End User Messaging Social può accedervi. Per ulteriori informazioni sul problema del deputato confuso, vedere [Il problema del deputato confuso](#) nella [guida per l'IAMutente](#).

La chiave da usare deve essere simmetrica. SNS Gli argomenti crittografati di Amazon non supportano le chiavi asimmetriche AWS KMS .

La policy chiave deve essere modificata per consentire all'utente AWS finale di Messaging Social di utilizzare la chiave. Segui le istruzioni riportate in [Modifica di una politica chiave](#), nella Guida per gli AWS Key Management Service sviluppatori, per aggiungere le seguenti autorizzazioni alla politica chiave esistente:

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



## Passaggi successivi

Dopo aver impostato l'SNSargomento Amazon, devi sottoscrivere un endpoint all'argomento. L'endpoint inizierà a ricevere messaggi pubblicati sull'argomento associato. Per ulteriori informazioni sulla sottoscrizione a un argomento, consulta [Abbonamento a un SNS argomento Amazon nella Amazon SNS Developer Guide](#).

## Formato di messaggi ed eventi in AWS End User Messaging Social

L'JSONoggetto di un evento contiene l'intestazione e il WhatsApp JSON payload AWS dell'evento. Per un elenco del payload e dei valori della JSON WhatsApp notifica, consulta [Webhooks Notification Payload Reference e Message Status in Business Platform Cloud Reference](#). WhatsApp API

## AWS Intestazione dell'evento social di messaggistica per l'utente finale

L'JSONoggetto di un evento contiene l'intestazione dell' AWS evento e. WhatsApp JSON L'intestazione contiene gli AWS identificatori e il tuo account WhatsApp aziendale (WABA) e il numero ARNs di telefono.

```
{
  "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
}
```

Nel caso dell'esempio precedente:

- *1234567890abcde* è l'WABAid di Meta.
- *abcde1234567890* è l'id del numero di telefono di Meta.
- *fb2594b8a7974770b128a409e2example* è l'ID dell'account WhatsApp aziendale (WABA).
- *976c72a700aac43eaf573ae050example* è l'ID del numero di telefono.

## Esempio WhatsApp JSON di ricezione di un messaggio di testo

Di seguito viene mostrato il record dell'evento per un messaggio di testo in arrivo da WhatsApp.

JSONViene generato da WhatsApp. Per un elenco dei campi e il loro significato, consulta [Webhooks Notification Payload Reference nel WhatsApp Business Platform Cloud Reference](#). 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"
}
]
}

```

## Esempio di ricezione WhatsApp JSON di un messaggio multimediale

Quanto segue mostra il record dell'evento per un messaggio multimediale in arrivo. Per recuperare il file multimediale, utilizzate il `GetWhatsAppMessageMedia` API comando. Per un elenco dei campi e il loro significato, consulta [Webhooks Notification Payload Reference](#)

```

{
//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": "BTD0xlqSZ7102o+/upusiNSt1EZhA/urkvKf143Uqjk=",
          "id": "530339869524171"
        }
      }
    ],
    "field": "messages"
  }
]
}

```

## WhatsApp stato del messaggio

Quando invii un messaggio, ricevi aggiornamenti sullo stato del messaggio. Devi abilitare la registrazione degli eventi per ricevere queste notifiche, vedi [Destinazioni di messaggi ed eventi in AWS End User Messaging Social](#).

### Stati del messaggio

La tabella seguente contiene i possibili stati del messaggio.

Nome dello stato	Descrizione
deleted (eliminato)	Il cliente ha eliminato il messaggio e dovresti eliminare anche il messaggio se è stato scaricato sul tuo server.
consegnato	Il messaggio è stato correttamente recapitato al cliente.
Non riuscito	Il messaggio non è stato inviato.
read	Il cliente ha letto il messaggio. Questo stato viene inviato solo se il cliente ha attivato le ricevute di lettura.
inviato	Il messaggio è stato inviato ma è ancora in transito.

Nome dello stato	Descrizione
attenzione	Il messaggio contiene un elemento che non è disponibile o non esiste.

## Risorse aggiuntive

Per ulteriori informazioni, consulta [Message Status](#) in WhatsApp Business Platform Cloud API Reference.

# Caricamento di file multimediali da inviare con WhatsApp

Quando invii o ricevi un file multimediale, questo deve essere archiviato in un bucket Amazon S3. Il bucket Amazon S3 deve trovarsi nella Regione AWS stesso Account AWS account WhatsApp aziendale (). WABA Queste istruzioni mostrano come creare un bucket Amazon S3, caricare un file e URL crearlo nel file. Per ulteriori informazioni sui comandi di Amazon S3, consulta [Usare i comandi di alto livello \(s3\)](#) con. AWS CLI Per ulteriori informazioni sulla configurazione AWS CLI, consulta [Configure the AWS CLI](#) nella [AWS Command Line Interface User Guide](#), [Creating a bucket](#) e [Uploading objects](#) in the [Amazon S3 User Guide](#).

Puoi anche creare un file multimediale [predefinito. URL](#). Con un prefissoURL, puoi concedere un accesso limitato nel tempo agli oggetti e caricarli senza richiedere a terzi di disporre di credenziali o autorizzazioni AWS di sicurezza.

[Per creare un bucket Amazon S3, usa il comando create-bucket.](#) AWS CLI Nella riga di comando, inserisci il comando seguente:

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

Nel precedente comando:

- Replace (Sostituisci) *us-east-1* con quello in cui si trova il tuo. Regione AWS WABA
- Replace (Sostituisci) *BucketName* con il nome del nuovo secchio.

[Per copiare un file nel bucket Amazon S3, usa il comando cp.](#) AWS CLI Nella riga di comando, inserisci il comando seguente:

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

Nel precedente comando:

- Replace (Sostituisci) *SourceFilePathAndName* con il percorso e il nome del file da copiare.
- Replace (Sostituisci) *BucketName* con il nome del bucket.
- Replace (Sostituisci) *FileName* con il nome da usare per il file.

L'URL da usare per l'invio è:

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

Per creare un [predefinitoURL](#), sostituisci il *user input placeholders* con le tue informazioni.

```
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
```

Il reso URL sarà: `https://amzn-s3-demo-bucket1.s3.af-south-1.amazonaws.com/mydoc.txt?{Headers}`

## Tipi e dimensioni di file multimediali supportati in WhatsApp

Quando si invia o si riceve un messaggio multimediale, il tipo di file deve essere supportato e non deve superare la dimensione massima del file. Per ulteriori informazioni, consulta la sezione [Tipi di file multimediali supportati](#) nel WhatsApp Business Platform Cloud API Reference.

### Tipi di file multimediali

#### Formati audio

Tipo di audio	Estensione	MIMETipo	Dimensione massima
AAC	.aac	audio/aac	16 MB
AMR	.amr	audio/amr	16 MB
MP3	.mp3	audio/mpeg	16 MB
MP4Audio	.m4a	audio/mp4	16 MB
OGGaudio	.ogg	audio/ogg	16 MB

#### Formati di documenti

Tipo di documento	Estensione	MIMETipo	Dimensione massima
Testo	.testo	text/plain	100 MB
Microsoft Excel	.xls, .xlsx	application/vnd.ms-excel, application/	100 MB

Tipo di documento	Estensione	MIMETipo	Dimensione massima
		vnd.openxmlformats-officedocument.spreadsheetml.sheet	
Microsoft Word	.doc, .docx	application/msword, application/vnd.openxmlformats-officedocument.wordprocessingml.document	100 MB
Microsoft PowerPoint	.ppt, .pptx	application/vnd.ms-powerpoint, application/vnd.openxmlformats-officedocument.presentationml.presentation	100 MB
PDF	.pdf	application/pdf	100 MB

### Formati di immagine

Tipo di immagine	Estensione	MIMETipo	Dimensione massima
JPEG	.jpeg	immagine/jpeg	5 MB
PNG	.png	immagine/png	5 MB

### Formati di adesivi

Tipo di adesivo	Estensione	MIMETipo	Dimensione massima
Adesivo animato	.webp	immagine/webp	500 KB
Adesivo statico	.webp	immagine/webp	100 KB



## Formati video

Tipo di video	Estensione	MIMETipo	Dimensione massima
3 GPP	.3 gp	video/3gp	16 MB
MP4video	.mp4	video/mp4	16 MB

## WhatsApp tipi di messaggi

Questo argomento elenca i tipi di messaggi supportati e una descrizione del loro utilizzo. Per un elenco dei tipi di [messaggi, vedere Messages](#) in the WhatsApp Business Platform Cloud API Reference.

Tipo di messaggio	Descrizione
Testo	Invia un messaggio di testo o URL al tuo cliente.
Media	Invia un file audio, documento, immagine, adesivo o video. Puoi anche inviare link al file multimediale.
Reaction	Invia un'emoji come reazione a un messaggio, ad esempio con il pollice alzato.
Modello	Invia un messaggio modello.
Ubicazione	Invia una località.
Contatti	Invia una scheda di contatto.
Interactive	Invia un messaggio interattivo.

## Risorse aggiuntive

Per un elenco degli oggetti dei WhatsApp [messaggi, vedere Messages](#) in the WhatsApp Business Platform Cloud API Reference.

# Invio di messaggi WhatsApp tramite AWS End User Messaging Social

Prima di inviare un messaggio, devi configurare il tuo account WhatsApp aziendale (WABA) e l'utente deve attivare la ricezione di messaggi da te. Per ulteriori informazioni, consulta [Acquisizione dell'autorizzazione](#).

Quando un utente ti invia un messaggio, si avvia o si aggiorna un timer di 24 ore chiamato finestra del servizio clienti. Tutti i tipi di messaggi, ad eccezione dei messaggi modello, possono essere inviati solo quando è aperta una finestra del servizio clienti tra te e l'utente. I messaggi modello possono essere inviati in qualsiasi momento, purché l'utente abbia scelto di ricevere messaggi da te.

Per ogni messaggio inviato o ricevuto, viene generato uno stato del messaggio che viene inviato alla destinazione dell'evento. Se il cliente non si è registrato WhatsApp, viene generato un evento con lo stato del messaggio pari a `fail`. È necessario attivare un [messaggio e la destinazione dell'evento](#) per ricevere lo [stato del messaggio](#).

Per un elenco dei tipi di messaggi, consulta [Messaggi](#) nella WhatsApp Business Platform Cloud API Reference.

## Important

### Lavorare con Meta/ WhatsApp

- L'utilizzo della WhatsApp Business Solution è soggetto ai termini e alle condizioni dei Termini di [servizio WhatsApp aziendali, dei Termini della WhatsApp Business Solution](#), della [Politica sulla messaggistica WhatsApp aziendale](#), delle [Linee guida sulla WhatsApp messaggistica](#) e a tutti gli altri termini, politiche o linee guida ivi inclusi come riferimento. Questi potrebbero essere aggiornati di tanto in tanto.
- Meta or WhatsApp può vietare in qualsiasi momento l'uso della WhatsApp Business Solution.
- In relazione all'utilizzo della WhatsApp Business Solution, l'utente non invierà alcun contenuto, informazione o dato soggetto a salvaguardia o limitazioni alla distribuzione ai sensi delle leggi o dei regolamenti applicabili.

## Argomenti

- [Esempio di invio di un messaggio modello in AWS End User Messaging Social](#)
- [Esempio di invio di un messaggio multimediale in AWS End User Messaging Social](#)

## Esempio di invio di un messaggio modello in AWS End User Messaging Social

Per ulteriori informazioni sui tipi di modelli di messaggio che possono essere inviati, consulta [Modello di messaggio](#) nel WhatsApp Business Platform Cloud API Reference. Per un elenco dei tipi di messaggi che possono essere inviati, consulta [Messaggi](#) nella WhatsApp Business Platform Cloud API Reference.

L'esempio seguente mostra come utilizzare un modello per [inviare un messaggio](#) al cliente utilizzando il AWS CLI. Per ulteriori informazioni sulla configurazione di AWS CLI, vedere [Configurare the AWS CLI](#) nella [Guida per l'AWS Command Line Interface utente](#).

### Note

È necessario specificare la codifica base64 quando si utilizza la versione 2. AWS CLI. Questo può essere fatto aggiungendo il AWS CLI parametro `--cli-binary-format raw-in-base64-out` o modificando il file di configurazione globale. AWS CLI Per ulteriori informazioni, consultate la Guida per l'utente dell'interfaccia [cli\\_binary\\_formata](#) riga di AWS comando per la versione 2.

```
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
```

Nel comando precedente, procedi come segue.

- Replace (Sostituisci) `{PHONE_NUMBER}` con il numero di telefono del cliente.
- Replace (Sostituisci) `{ORIGINATION_PHONE_NUMBER_ID}` con l'ID del tuo numero di telefono.

L'esempio seguente mostra come inviare un messaggio modello che non contiene alcun componente.

```
aws socialmessaging send-whatsapp-message --message '{"messaging_product":
"whatsapp","to": "'{PHONE_NUMBER}'","type": "template","template":
{"name":"simple_template","language": {"code": "en_US"}}}' --origination-phone-number-
id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version v20.0
```

- Replace (Sostituisci) `{PHONE_NUMBER}` con il numero di telefono del cliente.
- Replace (Sostituisci) `{ORIGINATION_PHONE_NUMBER_ID}` con l'ID del tuo numero di telefono.

## Esempio di invio di un messaggio multimediale in AWS End User Messaging Social

L'esempio seguente mostra come inviare un messaggio multimediale al cliente utilizzando il AWS CLI. Per ulteriori informazioni sulla configurazione di AWS CLI, vedere [Configure the AWS CLI](#) nella [Guida per l'AWS Command Line Interface utente](#). Per un elenco dei tipi di file multimediali supportati, vedere [Tipi e dimensioni di file multimediali supportati in WhatsApp](#).

1. Carica il file multimediale in un bucket Amazon S3. Per ulteriori informazioni, consulta [Caricamento di file multimediali da inviare con WhatsApp](#).
2. Carica il file multimediale WhatsApp utilizzando il [post-whatsapp-message-media](#) comando. Una volta completato con successo, il comando restituirà il `{MEDIA_ID}`, necessario per l'invio del messaggio multimediale.

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

Nel comando precedente, procedi come segue.

- Replace (Sostituisci) `{ORIGINATION_PHONE_NUMBER_ID}` con l'ID del tuo numero di telefono.
- Replace (Sostituisci) `{BUCKET}` con il nome del bucket Amazon S3.
- Replace (Sostituisci) `{MEDIA_FILE}` con il nome del file multimediale.

Puoi anche caricare utilizzando un [URL predefinito utilizzando](#) `--source-s3-presigned-url` instead of `--source-s3-file`. Devi aggiungere Content-Type nel headers campo. Se si utilizzano entrambi, `InvalidParameterException` viene restituito un.

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

3. Usa il [send-whatsapp-message](#) comando per inviare il messaggio multimediale.

```
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
```

### Note

È necessario specificare la codifica base64 quando si utilizza la AWS CLI versione 2. Questo può essere fatto aggiungendo il AWS CLI parametro `--cli-binary-format raw-in-base64-out` o modificando il file di configurazione globale. AWS CLI Per ulteriori informazioni, consultate la Guida per l'utente dell'interfaccia [cli\\_binary\\_formata](#) riga di AWS comando per la versione 2.

```
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 --cli-binary-
 format raw-in-base64-out
```

Nel comando precedente, procedi come segue.

- Replace (Sostituisci) `{PHONE_NUMBER}` con il numero di telefono del cliente.
  - Replace (Sostituisci) `{ORIGINATION_PHONE_NUMBER_ID}` con l'ID del tuo numero di telefono.
  - Replace (Sostituisci) `{MEDIA_ID}` con l'ID multimediale restituito dal passaggio precedente.
4. Quando il file multimediale non è più necessario, è possibile eliminarlo WhatsApp utilizzando il [delete-whatsapp-message-media](#) comando. Questa operazione rimuove solo il file multimediale WhatsApp e non il bucket Amazon S3.

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

Nel comando precedente, procedi come segue.

- Replace (Sostituisci) `{ORIGINATION_PHONE_NUMBER_ID}` con l'ID del tuo numero di telefono.
- Replace (Sostituisci) `{MEDIA_ID}` con l'ID multimediale.

# Risposta a un messaggio in AWS End User Messaging Social

Prima di poter ricevere un messaggio di testo o multimediale, devi aver configurato il tuo account WhatsApp aziendale (WABA) e una destinazione per l'evento. Quando ricevi un messaggio in arrivo, un evento viene salvato nell'SNSargomento Amazon sulla destinazione dell'evento. Per ricevere una notifica, devi abbonarti all'endpoint Amazon SNS Topics.

Per un esempio di evento relativo a un messaggio multimediale ricevuto, consulta [Esempio di ricezione WhatsApp JSON di un messaggio multimediale](#). Per ulteriori informazioni sulla configurazione di AWS CLI, vedere [Configurare the AWS CLI](#) nella [Guida per l'AWS Command Line Interface utente](#). Per un elenco dei tipi di file multimediali supportati, vedere [Tipi e dimensioni di file multimediali supportati in WhatsApp](#).

## Important

Per ricevere messaggi in arrivo, è necessario che le [destinazioni degli eventi](#) siano abilitate per WABA. Per ulteriori informazioni, consulta [Aggiungi un messaggio e una destinazione di eventi a AWS End User Messaging Social](#).

## Esempio di modifica dello stato di un messaggio da leggere in AWS End User Messaging Social

È possibile impostare lo [stato del messaggio](#) in modo da mostrare read all'utente finale due segni di spunta blu sullo schermo.

```
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
```

Nel comando precedente, procedi come segue.

- Replace (Sostituisci) `{ORIGINATION_PHONE_NUMBER_ID}` con l'ID del tuo numero di telefono.
- Replace (Sostituisci) `{MESSAGE_ID}` con l'identificatore univoco del messaggio. Usa il valore del `id` campo nell'oggetto messaggio dell'SNSargomento Amazon.



# Esempio di risposta a un messaggio con una reazione in AWS End User Messaging Social

Puoi aggiungere una reazione al messaggio, ad esempio un pollice in alto.

```
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
```

Nel comando precedente, procedi come segue.

- Replace (Sostituisci) `{PHONE_NUMBER}` con il numero di telefono del cliente.
- Replace (Sostituisci) `{MESSAGE_ID}` con l'identificatore univoco del messaggio. Usa il valore del id campo nell'oggetto messaggio dell'SNSargomento Amazon.
- Replace (Sostituisci) `{ORIGINATION_PHONE_NUMBER_ID}` con l'ID del tuo numero di telefono.

## Scarica un file multimediale WhatsApp da Amazon S3

Per recuperare un file multimediale e salvarlo in un bucket Amazon S3, usa il comando. [get-whatsapp-message-media](#)

```
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
 }
```

Nel comando precedente, procedi come segue.

- Replace (Sostituisci) `{BUCKET}` con il nome del bucket Amazon S3.
- Replace (Sostituisci) `{MEDIA_ID}` con il valore del id campo dell'evento ricevuto. Per un esempio di evento multimediale in arrivo, vedi [Esempio di ricezione WhatsApp JSON di un messaggio multimediale](#).
- Replace (Sostituisci) `{ORIGINATION_PHONE_NUMBER_ID}` con l'ID del tuo numero di telefono.

Per recuperare i file multimediali dal bucket Amazon S3, usa il seguente comando:

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

Nel comando precedente, procedi come segue.

- Replace (Sostituisci) `{BUCKET}` con il nome del bucket Amazon S3.
- Replace (Sostituisci) `{MEDIA_ID}` con il `MEDIA_ID` restituito dal passaggio precedente.

## Esempio di risposta a un messaggio con una conferma di lettura e una reazione

In questo esempio, il tuo cliente Diego ti ha inviato un messaggio dicendo «Ciao» e tu gli rispondi con una ricevuta di lettura e un'emoji agitata con la mano.

### Prerequisiti

Per ricevere una notifica relativa all'invio di un messaggio da parte di Diego, devi aver impostato un SNS argomento Amazon sulla destinazione dell'evento e aver sottoscritto un endpoint di argomento.

### Rispondere

1. Quando viene ricevuto il messaggio di Diego, viene pubblicato un evento nelle estremità dell'argomento. Quello che segue è un frammento di ciò che l'argomento pubblica.

#### Note

Poiché Diego ha avviato la conversazione, questa non viene conteggiata nella quota delle conversazioni avviate dalla tua azienda.

```
{
  "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"
    }
  ]
}
```

}

- Per mostrare a Diego che hai ricevuto il messaggio, imposta lo stato su. read Diego vedrà due segni di spunta blu accanto al messaggio sul suo dispositivo.

### Note

È necessario specificare la codifica base64 quando si utilizza la AWS CLI versione 2. Questo può essere fatto aggiungendo il AWS CLI parametro `--cli-binary-format raw-in-base64-out` o modificando il file di configurazione globale. AWS CLI Per ulteriori informazioni, consultate la Guida per l'utente dell'interfaccia [cli\\_binary\\_formata](#) riga di AWS comando per la versione 2.

```
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
```

Nel comando precedente, procedi come segue.

- Replace (Sostituisci) `{ORIGINATION_PHONE_NUMBER_ID}` con il numero di telefono ID a cui Diego ha inviato il messaggio `phone-number-id-976c72a700aac43eaf573ae050example`.
  - Replace (Sostituisci) `{MESSAGE_ID}` con l'identificatore univoco del messaggio. È lo stesso valore del id campo nel messaggio `wamid.HBG LMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRE0RjVGRkexa` ricevuto.
- Puoi inviare a Diego una reazione con la mano.

```
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
```

Nel comando precedente, procedi come segue.

- Replace (Sostituisci) `{PHONE_NUMBER}` con il numero di telefono di Diego,14255550150.
- Replace (Sostituisci) `{MESSAGE_ID}` con l'identificatore univoco del messaggio. È lo stesso valore del id campo nel messaggio `wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU20DEwMDkwREY40DBDRDE0RjVGRkexa` ricevuto.
- Replace (Sostituisci) `{ORIGINATION_PHONE_NUMBER_ID}` con il numero di telefono ID a cui Diego ha inviato il suo messaggio:`phone-number-id-976c72a700aac43eaf573ae050example`.

## Risorse aggiuntive

- Abilita [le destinazioni degli eventi](#) per registrare gli eventi e ricevere messaggi in arrivo.
- Per un elenco degli oggetti dei WhatsApp messaggi, consulta [Messages](#) in the WhatsApp Business Platform Cloud API Reference.

# Comprensione dei report WhatsApp di fatturazione e utilizzo per AWS End User Messaging Social

Il canale AWS End User Messaging Social genera un tipo di utilizzo che contiene cinque campi nel seguente formato: *Region code-MessagingType-ISO-FeeDescription-FeeType*. Esistono due possibili elementi di fatturazione per ogni WhatsApp conversazione: il WhatsAppConversationFee, e il AWS per. MessageFee

Quando inizi una conversazione inviando un messaggio modello, ti verrà addebitato uno per volta WhatsApp ConversationFee. AWS MessageFee Si apre una finestra di 24 ore in cui ogni messaggio inviato o ricevuto dallo stesso cliente viene fatturato in base alla tariffa. AWS MessageFee

Il tipo di WhatsApp conversazione e i dettagli sui prezzi sono disponibili nella sezione [Prezzi basati sulla conversazione](#) nella WhatsApp Business Platform Developer Guide.

La tabella seguente mostra i valori e le descrizioni possibili per i campi del tipo di utilizzo. Per ulteriori informazioni sui prezzi di AWS End User Messaging Social, consulta [AWS End User Messaging Pricing](#).

Campo	Opzioni	Descrizione
<i>Region code</i>	<ul style="list-style-type: none"> <li>• USE1— Regione Stati Uniti orientali (Virginia settentrionale)</li> <li>• USE2— Regione Stati Uniti orientali (Ohio)</li> <li>• USW1— Regione Stati Uniti occidentali (Oregon)</li> <li>• APS1— Regione Asia Pacifico (Mumbai)</li> <li>• APSE1— Regione Asia Pacifico (Singapore)</li> <li>• EUW1— Regione Europa (Irlanda)</li> </ul>	Il Regione AWS prefisso che indica da dove è stato inviato o ricevuto il WhatsApp messaggio.

Campo	Opzioni	Descrizione
	<ul style="list-style-type: none"><li>EUW2— Regione Europa (Londra)</li></ul>	
<i>MessagingType</i>	WhatsApp	Questo campo identifica il tipo di messaggio inviato.
<i>ISO</i>	Vedi i paesi <a href="#">supportati</a>	Il ISO prefisso internazionale a due cifre a cui è stato inviato il messaggio.
<i>FeeDescription</i>	ConversationFee , MessageFee	Questo campo specifica il o il per. WhatsApp ConversationFee AWS MessageFee

Campo	Opzioni	Descrizione
<i>FeeType</i>	Authentication , Marketing , Service, Utility, Standard	<p>Questo campo mostra il tipo di conversazione utilizzato o specifica lo standard per la tariffa per messaggio</p> <p>Categorie avviate dall'<b>ConversationFee</b> attività</p> <ul style="list-style-type: none"> <li>• <b>Marketing</b> — Utilizzato per raggiungere un'ampia gamma di obiettivi, dalla generazione di consapevolezza all'incremento delle vendite e al retargeting dei clienti. Gli esempi includono annunci di nuovi prodotti, servizi o funzionalità, promozioni/offerte mirate e promemoria di abbandono del carrello.</li> <li>• <b>Utility</b>— Utilizzato per dare seguito alle azioni o alle richieste degli utenti. Gli esempi includono la conferma dell'attivazione, la gestione degli ordini/della consegna (ad esempio un aggiornamento sulla consegna), gli aggiornamenti o gli avvisi dell'account (ad esempio un promemoria di pagamento) o i sondaggi di feedback.</li> </ul>



Campo	Opzioni	Descrizione
		<ul style="list-style-type: none"> <li>• <b>Authentication</b> — Utilizzato per autenticare gli utenti con codici di accesso monouso, potenzialmente in più fasi del processo di accesso (ad esempio verifica dell'account, ripristino dell'account e problemi di integrità).</li> <li>• <b>Service</b>— Utilizzato per risolvere le richieste dei clienti.</li> </ul> <p>Categorie avviate dall'utente</p> <p><b>ConversationFee</b></p> <ul style="list-style-type: none"> <li>• <b>Service</b>— Utilizzato per risolvere le richieste dei clienti.</li> </ul> <p>Categorie <b>MessageFee</b></p> <ul style="list-style-type: none"> <li>• <b>Standard</b>— Tariffa per messaggio inviato o ricevuto.</li> </ul>

Quando inizi una conversazione inviando un messaggio modello, ti verrà addebitato l'importo uno alla volta `ConversationFee`. `MessageFee` Si apre una finestra di 24 ore in cui ogni messaggio modello inviato allo stesso cliente viene fatturato individualmente. `MessageFee` Durante la finestra di 24 ore, i messaggi modello devono essere dello stesso tipo o viene avviata una nuova conversazione.

Ad esempio, se invii un messaggio modello di marketing a un cliente, ti verrà addebitato il costo del `ConversationFee` e `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
```

Se il cliente ti invia un messaggio e tu rispondi, ti verrà addebitato il costo dell'apertura di una nuova Service conversazione e di un nuovo messaggio.

```
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
```

## Esempio 1: invio di un messaggio modello di marketing

Ad esempio, se invii un messaggio modello di marketing a un cliente, ti verrà addebitato uno WhatsApp ConversationFee per volta AWS . MessageFee

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

## Esempio 2: apertura di una conversazione di assistenza

Una tariffa per una conversazione di servizio si applica quando un'azienda risponde al messaggio in entrata di un utente che non rientra in una finestra di conversazione attiva di 24 ore avviata dall'azienda. In questo scenario, ti viene addebitata una fattura alla volta AWS MessageFee per ogni messaggio in entrata WhatsApp ConversationFee e in uscita.

```
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 Messaggistica per l'utente finale, ISO codici di fatturazione social e mappatura delle tariffe di conversazione. WhatsApp

### Paesi supportati

Prefisso internazionale a due cifre ISO	Nome paese	WhatsApp regione di fatturazione delle conversazioni
AF	Afghanistan	Rest of Asia Pacific
AX	Aland Islands	Other
AL	Albania	Rest of Central & Eastern Europe
DZ	Algeria	Rest of Africa
AS	American Samoa	Other
AD	Andorra	Other
AO	Angola	Rest of Africa
AI	Anguilla	Other
AQ	Antarctica	Other
AG	Antigua and Barbuda	Other
AR	Argentina	Argentina
AM	Armenia	Rest of Central & Eastern Europe
AW	Aruba	Other
AC	Ascension Island	Other
AU	Australia	Rest of Asia Pacific
AT	Austria	Rest of Western Europe

Prefisso internazionale a due cifre ISO	Nome paese	WhatsApp regione di fatturazione delle conversazioni
AZ	Azerbaijan	Rest of Central & Eastern Europe
BS	Bahamas	Other
BH	Bahrain	Rest of Middle East
BD	Bangladesh	Rest of Asia Pacific
BB	Barbados	Other
BY	Belarus	Rest of Central & Eastern Europe
BE	Belgium	Rest of Western Europe
BZ	Belize	Other
BJ	Benin	Rest of Africa
BM	Bermuda	Other
BT	Bhutan	Other
BO	Bolivia	Rest of Latin America
BQ	Bonaire	Other
BA	Bosnia and Herzegovina	Other
BW	Botswana	Rest of Africa
BV	Bouvet Island	Other
BR	Brazil	Brazil
IO	British Indian Ocean Territory	Other
VG	British Virgin Islands	Other

Prefisso internazionale a due cifre ISO	Nome paese	WhatsApp regione di fatturazione delle conversazioni
BN	Brunei Darussalam	Other
BG	Bulgaria	Rest of Central & Eastern Europe
BF	BurkinaFaso	Rest of Africa
BI	Burundi	Rest of Africa
KH	Cambodia	Rest of Asia Pacific
CM	Cameroon	Rest of Africa
CA	Canada	North America
CV	Cape Verde	Other
KY	Cayman Islands	Other
CF	Central African Republic	Other
TD	Chad	Rest of Africa
CL	Chile	Chile
CN	China	Rest of Asia Pacific
CX	Christmas Island	Other
CC	Cocos(Keeling) Islands	Other
CO	Colombia	Colombia
KM	Comoros	Other
CK	Cook Islands	Other
CR	Costa Rica	Rest of Latin America

Prefisso internazionale a due cifre ISO	Nome paese	WhatsApp regione di fatturazione delle conversazioni
CI	Cote d'Ivoire	Rest of Africa
HR	Croatia	Rest of Central & Eastern Europe
CW	Curacao	Other
CY	Cyprus	Other
CZ	Czech Republic	Rest of Central & Eastern Europe
CD	Democratic Republic of the Congo	Rest of Africa
DK	Denmark	Rest of Western Europe
DJ	Djibouti	Other
DM	Dominica	Other
DO	Dominican Republic	Rest of Latin America
EC	Ecuador	Rest of Latin America
EG	Egypt	Egypt
SV	El Salvador	Rest of Latin America
GQ	Equatorial Guinea	Other
ER	Eritrea	Rest of Africa
EE	Estonia	Other
ET	Ethiopia	Rest of Africa
SZ	Eswatini	Rest of Africa

Prefisso internazionale a due cifre ISO	Nome paese	WhatsApp regione di fatturazione delle conversazioni
FK	Falkland Islands	Other
FO	Faroe Islands	Other
FJ	Fiji	Other
FI	Finland	Rest of Western Europe
FR	France	France
GF	French Guiana	Other
PF	French Polynesia	Other
TF	French Southern Territories	Other
GA	Gabon	Rest of Africa
GM	Gambia	Rest of Africa
GE	Georgia	Rest of Central & Eastern Europe
DE	Germany	Germany
GH	Ghana	Rest of Africa
GI	Gibraltar	Other
GR	Greece	Rest of Central & Eastern Europe
GL	Greenland	Other
GD	Grenada	Other
GP	Guadeloupe	Other
GU	Guam	Other

Prefisso internazionale a due cifre ISO	Nome paese	WhatsApp regione di fatturazione delle conversazioni
GT	Guatemala	Rest of Latin America
GG	Guernsey	Other
GN	Guinea	Other
GW	Guinea-Bissau	Rest of Africa
GY	Guyana	Other
HT	Haiti	Rest of Latin America
HM	Heard and McDonald Islands	Other
HN	Honduras	Rest of Latin America
HK	Hong Kong	Rest of Asia Pacific
HU	Hungary	Rest of Central & Eastern Europe
IS	Iceland	Other
IN	India	India
ID	Indonesia	Indonesia
IQ	Iraq	Rest of Middle East
IE	Ireland	Rest of Western Europe
IM	Isle of Man	Other
IL	Israel	Israel
IT	Italy	Italy
JM	Jamaica	Rest of Latin America



Prefisso internazionale a due cifre ISO	Nome paese	WhatsApp regione di fatturazione delle conversazioni
JP	Japan	Rest of Asia Pacific
JE	Jersey	Other
JO	Jordan	Rest of Middle East
KZ	Kazakhstan	Other
KE	Kenya	Rest of Africa
KI	Kiribati	Other
XK	Kosovo	Other
KW	Kuwait	Rest of Middle East
KG	Kyrgyzstan	Other
LA	Lao PDR	Rest of Asia Pacific
LV	Latvia	Rest of Central & Eastern Europe
LB	Lebanon	Rest of Middle East
LS	Lesotho	Rest of Africa
LR	Liberia	Rest of Africa
LY	Libya	Rest of Africa
LI	Liechtenstein	Other
LT	Lithuania	Rest of Central & Eastern Europe
LU	Luxembourg	Other
MO	Macao	Other

Prefisso internazionale a due cifre ISO	Nome paese	WhatsApp regione di fatturazione delle conversazioni
MK	Macedonia	Rest of Central & Eastern Europe
MG	Madagascar	Rest of Africa
MW	Malawi	Rest of Africa
MY	Malaysia	Malaysia
MV	Maldives	Other
ML	Mali	Rest of Africa
MT	Malta	Other
MH	Marshall Islands	Other
MQ	Martinique	Other
MR	Mauritania	Rest of Africa
MU	Mauritius	Other
YT	Mayotte	Other
MX	Mexico	Mexico
FM	Micronesia	Other
MD	Moldova	Rest of Central & Eastern Europe
MC	Monaco	Other
MN	Mongolia	Rest of Asia Pacific
ME	Montenegro	Other
MS	Montserrat	Other

Prefisso internazionale a due cifre ISO	Nome paese	WhatsApp regione di fatturazione delle conversazioni
MA	Morocco	Rest of Africa
MZ	Mozambique	Rest of Africa
MM	Myanmar	Other
NA	Namibia	Rest of Africa
NR	Nauru	Other
NP	Nepal	Rest of Asia Pacific
NL	Netherlands	Netherlands
NC	New Caledonia	Other
NZ	New Zealand	Rest of Asia Pacific
NI	Nicaragua	Rest of Latin America
NE	Niger	Rest of Africa
NG	Nigeria	Nigeria
NU	Niue	Other
NF	Norfolk Island	Other
MP	Northern Mariana Islands	Other
NO	Norway	Rest of Western Europe
OM	Oman	Rest of Middle East
PK	Pakistan	Pakistan
PW	Palau	Other
PS	Palestinian Territory	Other

Prefisso internazionale a due cifre ISO	Nome paese	WhatsApp regione di fatturazione delle conversazioni
PA	Panama	Rest of Latin America
PG	Papua New Guinea	Rest of Asia Pacific
PY	Paraguay	Rest of Latin America
PE	Peru	Peru
PH	Philippines	Rest of Asia Pacific
PN	Pitcairn	Other
PL	Poland	Rest of Central & Eastern Europe
PT	Portugal	Rest of Western Europe
PR	Puerto Rico	Rest of Latin America
QA	Qatar	Rest of Middle East
CG	Republic of Congo	Other
RE	Reunion	Other
RO	Romania	Rest of Central & Eastern Europe
RU	Russian Federation	Russia
RW	Rwanda	Rest of Africa
SH	Saint Helena	Other
KN	Saint Kitts and Nevis	Other
LC	Saint Lucia	Other
PM	Saint Pierre and Miquelon	Other

Prefisso internazionale a due cifre ISO	Nome paese	WhatsApp regione di fatturazione delle conversazioni
VC	Saint Vincent and Grenadines	Other
BL	Saint-Barthelemy	Other
MF	Saint-Martin	Other
WS	Samoa	Other
SM	San Marino	Other
ST	Sao Tome and Principe	Other
SA	Saudi Arabia	Saudi Arabia
SN	Senegal	Rest of Africa
RS	Serbia	Rest of Central & Eastern Europe
SC	Seychelles	Other
SL	Sierra Leone	Rest of Africa
SG	Singapore	Rest of Asia Pacific
SX	Sint Maarten	Other
SK	Slovakia	Rest of Central & Eastern Europe
SI	Slovenia	Rest of Central & Eastern Europe
SB	Solomon Islands	Other
SO	Somalia	Rest of Africa
ZA	South Africa	South Africa

Prefisso internazionale a due cifre ISO	Nome paese	WhatsApp regione di fatturazione delle conversazioni
GS	South Georgia and the South Sandwich Islands	Other
KR	South Korea	Other
SS	South Sudan	Rest of Africa
ES	Spain	Spain
LK	Sri Lanka	Rest of Asia Pacific
SR	Suriname	Other
SJ	Svalbard and Jan Mayen Islands	Other
SE	Sweden	Rest of Western Europe
CH	Switzerland	Rest of Western Europe
TW	Taiwan	Rest of Asia Pacific
TJ	Tajikistan	Rest of Asia Pacific
TZ	Tanzania	Rest of Africa
TH	Thailand	Rest of Asia Pacific
TL	Timor-Leste	Other
TG	Togo	Rest of Africa
TK	Tokelau	Other
TO	Tonga	Other
TT	Trinidad and Tobago	Other
TA	Tristan da Cunha	Other

Prefisso internazionale a due cifre ISO	Nome paese	WhatsApp regione di fatturazione delle conversazioni
TN	Tunisia	Rest of Africa
TR	Turkey	Turkey
TM	Turkmenistan	Rest of Asia Pacific
TC	Turks and Caicos Islands	Other
TV	Tuvalu	Other
UG	Uganda	Rest of Africa
UA	Ukraine	Rest of Central & Eastern Europe
AE	United Arab Emirates	United Arab Emirates
GB	United Kingdom	United Kingdom
US	United States	North America
UY	Uruguay	Rest of Latin America
UM	US Minor Outlying Islands	Other
UZ	Uzbekistan	Rest of Asia Pacific
VU	Vanuatu	Other
VA	Vatican City State	Other
VE	Venezuela	Rest of Latin America
VN	Vietnam	Rest of Asia Pacific
VI	Virgin Islands	Other
WF	Wallis and Futuna Islands	Other

Prefisso internazionale a due cifre ISO	Nome paese	WhatsApp regione di fatturazione delle conversazioni
EH	Western Sahara	Other
YE	Yemen	Rest of Middle East
ZM	Zambia	Rest of Africa
ZW	Zimbabwe	Other



# Monitoraggio AWS della messaggistica social per gli utenti finali

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di AWS End User Messaging Social e delle altre AWS soluzioni. AWS fornisce i seguenti strumenti di monitoraggio per monitorare i social network degli utenti AWS finali, segnalare quando qualcosa non va e intraprendere azioni automatiche quando necessario:

- Amazon CloudWatch monitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale. Puoi raccogliere i parametri e tenerne traccia, creare pannelli di controllo personalizzati e impostare allarmi per inviare una notifica o intraprendere azioni quando un parametro specificato raggiunge una determinata soglia. Ad esempio, puoi tenere CloudWatch traccia CPU dell'utilizzo o di altri parametri delle tue EC2 istanze Amazon e avviare automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consulta la [Amazon CloudWatch User Guide](#).
- Amazon CloudWatch Logs ti consente di monitorare, archiviare e accedere ai tuoi file di registro da EC2 istanze Amazon e altre fonti. CloudTrail CloudWatch I log possono monitorare le informazioni contenute nei file di registro e avvisarti quando vengono raggiunte determinate soglie. Puoi inoltre archiviare i dati del log in storage estremamente durevole. Per ulteriori informazioni, consulta la [Amazon CloudWatch Logs User Guide](#).
- AWS CloudTrail acquisisce le API chiamate e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di registro a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la [Guida per l'utente AWS CloudTrail](#).

## Monitoraggio AWS della messaggistica sociale degli utenti finali con Amazon CloudWatch

Puoi monitorare l'utilizzo dei social network per gli utenti AWS finali CloudWatch, che raccoglie dati grezzi e li elabora in metriche leggibili quasi in tempo reale. Queste statistiche vengono conservate per un periodo di 15 mesi, per permettere l'accesso alle informazioni storiche e offrire una prospettiva migliore sulle prestazioni del servizio o dell'applicazione web. È anche possibile impostare allarmi che controllano determinate soglie e inviare notifiche o intraprendere azioni quando queste soglie vengono raggiunte. Per ulteriori informazioni, consulta la [Amazon CloudWatch User Guide](#).

Per quanto riguarda `AWS End User Messaging SocialWhatsAppMessageFeeCount`, potresti voler controllare `WhatsAppConversationFeeCount` e attivare un allarme quando viene raggiunta una soglia di spesa.

### Note

Prima di poter utilizzare le CloudWatch metriche, devi [creare un ruolo service-link](#).

Le tabelle seguenti elencano le metriche e le dimensioni che `AWS End User Messaging Social` esporta nel namespace. `AWS/SocialMessaging`

Parametro	Unità	Descrizione
<code>WhatsAppConversationFeeCount</code>	Conteggio	Il conteggio dei costi di conversazione WhatsApp
<code>WhatsAppMessageFeeCount</code>	Conteggio	Il conteggio delle tariffe per i WhatsApp messaggi

Dimensione	Descrizione
<code>MessageFeeType</code>	I tipi di tariffa validi sono Service, Marketing, Utility e Authentication
<code>DestinationCountryCode</code>	Il ISO codice a due lettere del paese
<code>WhatsAppPhoneNumberArn</code>	L'avviso del numero di telefono

## Registrazione della messaggistica con l'utente AWS finale API Le chiamate social utilizzando AWS CloudTrail

AWS La cronologia di gestione di un utente è integrata con [AWS CloudTrail](#), un ruolo o un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o un servizio che offre un registro delle operazioni eseguite da un utente, un ruolo o un servizio in Servizio AWS Neputy CloudTrail

acquisisce tutte le API chiamate per AWS End User Messaging Social come eventi. Le chiamate acquisite includono le chiamate dalla console della AWS console in AppStream 2.0 e le chiamate di codice alle API operazioni API AWS di Amazon EMR su EKS. Le informazioni raccolte da CloudTrail, consentono di determinare la richiesta effettuata a, l'indirizzo IP AWS di origine da cui è partita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente root o utente.
- Un percorso basato su una singola richiesta è stata eseguita per il momento in cui è stata eseguita la richiesta IAM effettuata a, l'indirizzo IP della
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro Servizio AWS.

CloudTrail Per impostazione predefinita Account AWS , consulta la cronologia degli CloudTrail eventi nel tuo account. La cronologia CloudTrail degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli eventi di gestione verificatisi negli ultimi 90 giorni in una. Regione AWS Per ulteriori informazioni, consulta [Lavorare con la cronologia degli CloudTrail eventi](#) nella Guida per l'utente.AWS CloudTrail Non sono CloudTrail previsti costi CloudTrail per la visualizzazione della cronologia degli eventi.

Per una registrazione continua degli eventi nel Account AWS tuo, crea un datastore di [CloudTraileventi](#) oppure un percorso.

## CloudTrail sentieri

Un trail consente CloudTrail a CloudTrail di distribuire i file di log in un bucket Amazon S3. Tutti i percorsi che vengono creati utilizzando la AWS Management Console console sono multi-regionali. Puoi creare un percorso basato su una singola Regione solo utilizzando la. AWS CLI La creazione di un percorso multi-regionale è una singola Regione solo Regioni AWS utilizzando la. Puoi creare un percorso basato su una singola Regione solo utilizzando la. Regione AWS Per ulteriori informazioni sui sentieri, consulta [Creazione di un percorso per te Account AWS](#) e [Creazione di un percorso per un'organizzazione nella Guida](#) per l'AWS CloudTrail utente.

Puoi fornire gratuitamente una copia dei tuoi eventi di gestione in corso al tuo bucket Amazon S3 da CloudTrail CloudTrail creando un percorso, tuttavia devono essere considerati i costi di

archiviazione di Amazon S3. [Per ulteriori informazioni sui CloudTrail prezzi, consulta la pagina Prezzi.AWS CloudTrail](#) Per informazioni sui prezzi di Amazon S3, consulta [Prezzi di Amazon S3](#).

CloudTrail I datastore di eventi di eventi.

CloudTrail Lake consente di eseguire query SQL basate su SQL sugli eventi dell'utente. CloudTrail CloudTrail registrano un record di dati basato su una singola regione in formato JSON basato su una JSON singola regione in formato [JSON ORC](#) ORC è un formato di archiviazione a colonne ottimizzato per il recupero rapido dei dati Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili basate sui criteri selezionati applicando i [selettori di eventi avanzati](#). I selettori applicati a un archivio di dati degli eventi controllano quali eventi persistono e sono disponibili per l'esecuzione della query. Per ulteriori informazioni su CloudTrail Lake, consulta [Working with AWS CloudTrail Lake](#) nella Guida per l'utente.AWS CloudTrail

CloudTrail I datastore di eventi e le query di Data Lake comportano addebiti. Quando crei un datastore di eventi, scegli l'[opzione di prezzo](#) da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. [Per ulteriori informazioni sui CloudTrail prezzi, consulta la sezione Prezzi.AWS CloudTrail](#)

## AWS Messaggistica con l'utente finale Eventi relativi ai dati sociali in CloudTrail

Gli [eventi di dati](#) forniscono informazioni sulle operazioni delle risorse eseguite su o in una risorsa (ad esempio, lettura o scrittura su un oggetto Amazon S3). Queste operazioni sono definite anche operazioni del piano dei dati. Gli eventi di dati sono spesso attività che interessano volumi elevati di dati. Per impostazione predefinita, i CloudTrail trail non registrano gli eventi di dati La cronologia CloudTrail degli eventi non registra gli eventi relativi ai dati.

Per gli eventi di dati sono previsti costi aggiuntivi. Per ulteriori informazioni sui CloudTrail prezzi, consulta la sezione [AWS CloudTrail Prezzi](#).

Puoi registrare gli eventi relativi ai dati per i tipi di risorse AWS End User Messaging Social utilizzando la CloudTrail AWS CLI console o CloudTrail API le operazioni. Per ulteriori informazioni su come registrare gli eventi relativi ai dati, vedere [Registrazione degli eventi relativi ai dati con AWS Management Console e Registrazione degli eventi relativi ai dati con the AWS Command Line Interface nella Guida](#) per l'AWS CloudTrail utente.

La tabella seguente elenca i tipi di risorse social di messaggistica per l'utente AWS finale per i quali è possibile registrare gli eventi relativi ai dati. La colonna Tipo di evento Data (console) mostra il valore da scegliere dall'elenco dei tipi di evento Data sulla CloudTrail console. La colonna del valore `resources.type` mostra il `resources.type` valore, da specificare durante la configurazione dei selettori di eventi avanzati utilizzando o. AWS CLI CloudTrail APIs La CloudTrail colonna Dati APIs registrati mostra le API chiamate registrate per il tipo di risorsa. CloudTrail

Tipo di evento di dati (console)	valore <code>resources.type</code>	Dati registrati APIs su CloudTrail
ID del numero di telefono di messaggistica sociale	<code>AWS::SocialMessaging::PhoneNumberId</code>	<ul style="list-style-type: none"> <li>• <a href="#">DeleteWhatsAppMessageMedia</a></li> <li>• <a href="#">GetWhatsAppMessageMedia</a></li> <li>• <a href="#">PostWhatsAppMessageMedia</a></li> <li>• <a href="#">SendWhatsAppMessage</a></li> </ul>

Puoi configurare selettori di eventi avanzati per filtrare `resources.ARN` i campi `eventNameReadOnly`, e per registrare solo gli eventi che ritieni importanti. Per ulteriori informazioni sui campi, consulta [AdvancedFieldSelector](#) nel AWS CloudTrail API Reference.

## AWS Messaggistica con l'utente finale Eventi di gestione sociale in CloudTrail

[Gli eventi di gestione](#) forniscono informazioni sulle operazioni di gestione eseguite sulle operazioni di gestione eseguite sulle risorse nel tuo account Account AWS. Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Per impostazione predefinita, CloudTrail registra gli eventi di gestione.

AWS End User Messaging Social registra tutte le operazioni del piano di controllo AWS End User Messaging Social come eventi di gestione. Per un elenco delle operazioni del piano di controllo AWS End User Messaging Social a cui accede AWS End User Messaging Social CloudTrail, vedere [AWS End User Messaging Social API Reference](#).

## AWS Esempi di eventi End User Messaging Social

Un evento rappresenta una singola richiesta da un'origine e include informazioni sull'API/operazione richiesta, data e ora dell'operazione, parametri della richiesta e così via. CloudTrail I file di log CloudTrail non sono una traccia stack ordinata delle API chiamate API pubbliche e di conseguenza non devono apparire in base a un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail log di log di che illustra l'operazione:

```
{
  "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"
    }
  }
}
```

Per informazioni sul contenuto dei CloudTrail record, consultate il [contenuto dei CloudTrail record](#) nella Guida per l'AWS CloudTrail utente.

# Le migliori pratiche per la messaggistica sociale con gli utenti AWS finali

Questa sezione descrive diverse best practice che potrebbero aiutarti a migliorare il coinvolgimento dei clienti ed evitare la sospensione dell'account. Non contiene tuttavia consulenza legale. Consulta sempre un avvocato per ottenere adeguati pareri legali.

Per l'elenco più recente delle WhatsApp best practice, consulta la [Politica sulla messaggistica WhatsApp aziendale](#).

## Argomenti

- [Up-to-date profilo aziendale](#)
- [Acquisizione dell'autorizzazione](#)
- [Contenuto proibito dei messaggi](#)
- [Controllo degli elenchi dei clienti](#)
- [Adattamento dell'invio al coinvolgimento](#)
- [Invio in orari appropriati](#)

## Up-to-date profilo aziendale

Mantieni un profilo up-to-date WhatsApp aziendale accurato che includa le informazioni di contatto dell'assistenza clienti, come indirizzo e-mail, indirizzo del sito Web o numero di telefono. Assicurati che le informazioni fornite siano veritiere e non rappresentino in modo errato o si spaccino per un'altra azienda.

## Acquisizione dell'autorizzazione

Non inviare mai messaggi a destinatari che non hanno richiesto esplicitamente di ricevere i tipi specifici di messaggi che intendi inviare. Conserva le seguenti informazioni di attivazione:

- La procedura di opt-in deve informare chiaramente la persona che acconsente a ricevere messaggi o chiamate dalla vostra azienda. WhatsApp Devi indicare esplicitamente il nome della tua attività.
- L'utente è l'unico responsabile della determinazione del metodo per ottenere il consenso esplicito. Assicurati che la procedura di opt-in sia conforme a tutte le leggi applicabili che regolano le tue



comunicazioni. Fornisci tutte le notifiche richieste e ottieni tutte le autorizzazioni necessarie ai sensi delle leggi pertinenti.

[Per ulteriori informazioni sui requisiti di WhatsApp opt-in, consulta Get Opt-in per WhatsApp](#)

Se i destinatari possono iscriversi per ricevere i tuoi messaggi utilizzando un modulo online, impedisce agli utenti di iscriversi a loro insaputa tramite script automatici. Limita anche il numero di volte in cui un utente può inviare un numero di telefono in una singola sessione.

Rispetta tutte le richieste fatte da una persona, attiva o disattivata WhatsApp, per bloccare, interrompere o altrimenti disattivare le comunicazioni, inclusa la rimozione di quella persona dall'elenco dei contatti.

Mantieni una documentazione della data, dell'ora e dell'origine di ogni richiesta con consenso esplicito e di ogni conferma. Questo può anche aiutarti a eseguire controlli di routine del tuo elenco di clienti.

## Contenuto proibito dei messaggi

### Important

#### Lavorare con Meta/ WhatsApp

- L'utilizzo della WhatsApp Business Solution è soggetto ai termini e alle condizioni dei Termini di [servizio WhatsApp aziendali](#), dei [Termini della WhatsApp Business Solution](#), della [Politica sulla messaggistica WhatsApp aziendale](#), delle [Linee guida sulla WhatsApp messaggistica](#) e a tutti gli altri termini, politiche o linee guida ivi inclusi per riferimento (poiché ciascuno può essere aggiornato di tanto in tanto).
- Meta or WhatsApp può vietare in qualsiasi momento l'uso della WhatsApp Business Solution.
- In relazione all'utilizzo della WhatsApp Business Solution, l'utente non invierà alcun contenuto, informazione o dato soggetto a salvaguardia o limitazioni alla distribuzione in base alle leggi o ai regolamenti applicabili.

In caso di violazione delle WhatsApp norme, il tuo account potrebbe essere bloccato dall'invio di messaggi per un periodo di tempo, bloccato fino alla presentazione di un ricorso o bloccato

definitivamente. Meta ti informerà se uno dei tuoi account o risorse ha violato la politica, tramite e-mail e il WhatsApp Business Manager. Tutti i ricorsi devono essere presentati a Meta. Per visualizzare una violazione delle norme o presentare un ricorso a Meta, consulta [Visualizza i dettagli della violazione delle norme per il tuo account WhatsApp Business](#) nel Centro assistenza Meta Business. Per l'elenco più recente dei contenuti proibiti dei messaggi, consulta la [Politica sulla messaggistica WhatsApp aziendale](#).

Le seguenti sono categorie di contenuti proibiti per tutti i tipi di messaggi a livello globale. Quando invii un messaggio con WhatsApp, segui queste linee guida:

Categoria	Esempi
Gioco d'azzardo	<ul style="list-style-type: none"> <li>• Casinò</li> <li>• Lotterie</li> <li>• App/siti Web</li> </ul>
Servizi finanziari ad alto rischio	<ul style="list-style-type: none"> <li>• Prestiti Payday</li> <li>• Prestiti a breve termine</li> <li>• Auto prestiti</li> <li>• Mutui ipotecari</li> <li>• Prestiti per studenti</li> <li>• Recupero crediti</li> <li>• Avvisi di azioni</li> <li>• Criptovalute</li> </ul>
Remissione debito	<ul style="list-style-type: none"> <li>• Consolidamento debito</li> <li>• Riduzione debito</li> <li>• Programmi di riparazione crediti</li> </ul>
Get-rich-quick schemi	<ul style="list-style-type: none"> <li>• Work-from-home programmi</li> <li>• Opportunità di investimento in rischio</li> <li>• Sistemi di marketing piramidali o multilivello</li> </ul>
Sostanze illegali	<ul style="list-style-type: none"> <li>• Cannabis/ CBD</li> </ul>

Categoria	Esempi
Phishing/smishing	<ul style="list-style-type: none"><li>• Tenta di convincere gli utenti a rivelare informazioni personali o informazioni di accesso al sito web.</li></ul>
S.H.A.F.T.	<ul style="list-style-type: none"><li>• Sex</li><li>• Odio</li><li>• Alcol</li><li>• Armi da fuoco</li><li>• Tabacco/Vape</li></ul>
Lead generation di terze parti	<ul style="list-style-type: none"><li>• Aziende che acquistano, vendono o condividono informazioni sui consumatori</li></ul>

## Controllo degli elenchi dei clienti

Se invii WhatsApp messaggi ricorrenti, controlla regolarmente gli elenchi dei tuoi clienti. Il controllo degli elenchi dei clienti aiuta a garantire che gli unici clienti che ricevono i tuoi messaggi siano quelli che desiderano riceverli.

Quando controlli l'elenco, invia a ogni cliente che ha acconsentito esplicitamente un messaggio di promemoria della sottoscrizione con le informazioni per annullarla.

## Adattamento dell'invio al coinvolgimento

Le priorità dei clienti possono cambiare nel tempo. Se i clienti non ritengono più utili i tuoi messaggi, potrebbero cancellarsi completamente dalla ricezione o addirittura segnalare i tuoi messaggi come non sollecitati. Per questi motivi, è importante adattare le tue procedure di invio al coinvolgimento dei clienti.

Per i clienti che raramente interagiscono con i tuoi messaggi, dovresti adattare la frequenza dei messaggi. Se ai clienti coinvolti invii messaggi settimanali, ad esempio, potresti creare un riepilogo mensile separato per i clienti meno coinvolti.

Rimuovi infine dai tuoi elenchi i clienti che non sono affatto coinvolti. Questo evita che i tuoi messaggi generino frustrazione nei clienti e ti consente inoltre di risparmiare denaro e proteggere la tua reputazione come mittente.

## Invio in orari appropriati

Invia messaggi durante il normale orario lavorativo diurno. Se invii messaggi all'ora di cena o nel cuore della notte, ci sono buone probabilità che i tuoi clienti annullino l'iscrizione alle tue liste per evitare di essere disturbati. Potresti voler evitare di inviare WhatsApp messaggi quando i tuoi clienti non possono rispondere immediatamente.

# Sicurezza nella messaggistica sociale per utenti AWS finali

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il [modello di responsabilità condivisa](#) descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei [AWS Programmi di AWS conformità dei Programmi di conformità](#) dei di . Per maggiori informazioni sui programmi di conformità che si applicano ai social network per utenti AWS finali, consulta la sezione [AWS Servizi rientranti nell'ambito del programma di conformitàAWS](#) .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa quando si utilizza AWS End User Messaging Social. I seguenti argomenti mostrano come configurare AWS End User Messaging Social per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse social di messaggistica per gli utenti AWS finali.

## Argomenti

- [Protezione dei dati in AWS End User Messaging Social](#)
- [Gestione delle identità e degli accessi per AWS End User Messaging Social](#)
- [Convalida della conformità per End User Messaging Social AWS](#)
- [Resilienza nella messaggistica sociale per gli utenti AWS finali](#)
- [Sicurezza dell'infrastruttura nella messaggistica AWS sociale degli utenti finali](#)
- [Prevenzione del problema "confused deputy" tra servizi](#)
- [Best practice di sicurezza](#)
- [Utilizzo di ruoli collegati ai servizi per AWS End User Messaging Social](#)

## Protezione dei dati in AWS End User Messaging Social

Il modello di [responsabilità AWS condivisa modello](#) si applica alla protezione dei dati in AWS End User Messaging Social. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, consulta la sezione [Privacy dei dati FAQ](#). Per informazioni sulla protezione dei dati in Europa, consulta il [Modello di responsabilitàAWS condivisa e GDPR](#) il post sul blog sulla AWS sicurezza.

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e di configurare i singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con AWS le risorse. Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Configurazione API e registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'uso dei CloudTrail percorsi per registrare AWS le attività, consulta [Lavorare con i CloudTrail percorsi](#) nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di FIPS 140-3 moduli crittografici convalidati per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint. FIPS Per ulteriori informazioni sugli FIPS endpoint disponibili, vedere [Federal Information Processing Standard \(\) 140-3. FIPS](#)

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con AWS End User Messaging Social o altro Servizi AWS utilizzando la console, API AWS CLI, o. AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per la fatturazione o i log di diagnostica. Se fornisci un URL a un server esterno, ti consigliamo vivamente di non includere le informazioni sulle credenziali URL per convalidare la tua richiesta a quel server.

### Important

WhatsApp utilizza il protocollo Signal per comunicazioni sicure. Tuttavia, poiché AWS End User Messaging Social è una terza parte, WhatsApp non considera questi messaggi end-to-end crittografati. Per ulteriori informazioni sulla protezione WhatsApp dei dati, consulta il white paper sulla [panoramica sulla privacy e la sicurezza dei dati e sulla WhatsApp crittografia](#).

## Crittografia dei dati

AWS Messaggistica con l'utente finale I dati social sono crittografati in transito e quando sono inattivi entro i confini. AWS Quando invii dati a AWS End User Messaging Social, i dati vengono crittografati non appena vengono ricevuti e li archivia. Quando recuperi i dati da AWS End User Messaging Social, questi ti trasmette i dati utilizzando i protocolli di sicurezza correnti.

### Crittografia a riposo

AWS End User Messaging Social crittografa tutti i dati che archivia per te all'interno del limite. AWS Ciò include i dati di configurazione, i dati di registrazione e tutti i dati aggiunti a AWS End User Messaging Social. Per crittografare i dati, AWS End User Messaging Social utilizza chiavi interne AWS Key Management Service (AWS KMS) che il servizio possiede e gestisce per conto dell'utente. Per ulteriori informazioni su AWS KMS, consulta la [Guida per sviluppatori di AWS Key Management Service](#).

### Crittografia in transito

AWS End User Messaging Social utilizza HTTPS Transport Layer Security (TLS) 1.2 per comunicare con i clienti, le applicazioni e Meta. Per comunicare con altri AWS servizi, AWS End User Messaging Social utilizza HTTPS e TLS 1.2. Inoltre, quando si creano e gestiscono AWS SMS risorse utilizzando la console, un o il AWS SDK AWS Command Line Interface, tutte le comunicazioni vengono protette utilizzando HTTPS e TLS 1.2.

### Gestione delle chiavi

Per crittografare i dati, AWS End User Messaging Social utilizza AWS KMS chiavi interne che il servizio possiede e gestisce per conto dell'utente. Queste chiavi vengono ruotate su base regolare. Non puoi fornire e utilizzare le tue AWS KMS o altre chiavi per crittografare i dati archiviati in AWS End User Messaging Social.

## Riservatezza del traffico Internet

La privacy del traffico internetwork si riferisce alla protezione delle connessioni e del traffico tra AWS End User Messaging Social e i client e le applicazioni locali e tra AWS End User Messaging Social e altre AWS risorse degli stessi. Regione AWS Le seguenti funzionalità e pratiche possono aiutarti a proteggere la privacy del traffico di rete per AWS End User Messaging Social.

### Traffico tra AWS SMS e applicazioni e client locali

Per stabilire una connessione privata tra AWS End User Messaging Social e i client e le applicazioni sulla rete locale, puoi usare AWS Direct Connect. Consente di collegare la rete a una posizione AWS Direct Connect utilizzando un cavo Ethernet standard in fibra ottica. Un'estremità del cavo è collegata al router. L'altra estremità è connessa a un AWS Direct Connect router. Per ulteriori informazioni, consulta [Che cos'è AWS Direct Connect?](#) nella Guida per l'utente di AWS Direct Connect.

Per garantire l'accesso sicuro a AWS End User Messaging Social tramite Published APIs, ti consigliamo di rispettare i requisiti social di messaggistica per gli utenti AWS finali per API le chiamate. AWS End User Messaging Social richiede ai client di utilizzare Transport Layer Security (TLS) 1.2 o versione successiva. I client devono inoltre supportare suite di crittografia con Perfect Forward Secrecy (PFS), come Ephemeral Diffie-Hellman () o Elliptic Curve Diffie-Hellman Ephemeral (). DHE ECDHE La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata al principale () dell'account. AWS Identity and Access Management IAM In alternativa, è possibile utilizzare [AWS Security Token Service](#) (AWS STS) per generare le credenziali di sicurezza temporanee per firmare le richieste.

## Gestione delle identità e degli accessi per AWS End User Messaging Social

AWS Identity and Access Management (IAM) è un servizio Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. IAM gli amministratori controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse social di messaggistica con l'utente AWS finale. IAM è un servizio Servizio AWS che puoi utilizzare senza costi aggiuntivi.

### Argomenti



- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso con policy](#)
- [Come funziona AWS End User Messaging Social con IAM](#)
- [Esempi di policy basate sull'identità per End User Messaging Social AWS](#)
- [AWS politiche gestite per AWS End User Messaging Social](#)
- [Risoluzione dei problemi relativi all'identità e all'accesso social di AWS End User Messaging](#)

## Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in AWS End User Messaging Social.

Utente del servizio: se utilizzi il servizio AWS End User Messaging Social per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità social di messaggistica con l'utente AWS finale per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di AWS End User Messaging Social, consulta [Risoluzione dei problemi relativi all'identità e all'accesso social di AWS End User Messaging](#).

Amministratore del servizio: se sei responsabile delle risorse AWS End User Messaging Social della tua azienda, probabilmente hai pieno accesso a AWS End User Messaging Social. Spetta a te determinare a quali funzionalità e risorse AWS End User Messaging Social devono accedere gli utenti del servizio. È quindi necessario inviare richieste all'IAM amministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base di IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM AWS End User Messaging Social, consulta [Come funziona AWS End User Messaging Social con IAM](#).

IAM amministratore: se sei un IAM amministratore, potresti voler saperne di più su come scrivere politiche per gestire l'accesso a AWS End User Messaging Social. Per visualizzare esempi di policy basate sull'identità sociale di AWS End User Messaging che puoi utilizzare in IAM, consulta. [Esempi di policy basate sull'identità per End User Messaging Social AWS](#)

## Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. È necessario autenticarsi (accedere a AWS) come Utente root dell'account AWS, come IAM utente o assumendo un ruolo. IAM

È possibile accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Quando accedi come identità federata, l'amministratore aveva precedentemente configurato la federazione delle identità utilizzando i ruoli. IAM Quando si accede AWS utilizzando la federazione, si assume indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi [Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente](#).

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando () per firmare crittograficamente le tue richieste utilizzando le tue credenziali. CLI Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta [AWS Signature Version 4 per API le richieste](#) nella Guida per l'IAMutente.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta [Autenticazione a più fattori](#) nella Guida per l'AWS IAM Identity Center utente e [Autenticazione a AWS più fattori IAM nella Guida per l'IAMutente](#).

### Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per l'elenco completo delle attività che richiedono l'accesso come utente root, consulta [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'IAMutente.

## Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per informazioni su IAM Identity Center, vedi [Cos'è IAM Identity Center?](#) nella Guida AWS IAM Identity Center per l'utente.

## IAM users and groups

Un [IAMutente](#) è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare IAM utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine con IAM gli utenti, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta [Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine](#) nella Guida per l'utente. IAM

Un [IAMgruppo](#) è un'identità che specifica un insieme di utenti. IAM Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per IAM amministrare le risorse.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta [Casi d'uso per IAM gli utenti nella Guida per l'IAMutente](#).

## IAMruoli

Un [IAMruolo](#) è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un IAM utente, ma non è associato a una persona specifica. Per assumere temporaneamente un IAM ruolo in AWS Management Console, puoi [passare da un utente a un IAM ruolo \(console\)](#). È possibile assumere un ruolo chiamando un' AWS API o operazione AWS CLI o utilizzando un'operazione personalizzata URL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere [Metodi per assumere un ruolo](#) nella Guida per l'IAM utente.

IAM i ruoli con credenziali temporanee sono utili nelle seguenti situazioni:

- **Accesso utente federato:** per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per informazioni sui ruoli per la federazione, consulta [Creare un ruolo per un provider di identità di terze parti \(federazione\)](#) nella Guida per l'IAM utente. Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla il set di autorizzazioni a un ruolo in IAM. Per informazioni sui set di autorizzazioni, consulta [Set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center.
- **Autorizzazioni IAM utente temporanee:** un IAM utente o un ruolo può assumere il IAM ruolo di assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- **Accesso su più account:** puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la [sezione Accesso alle risorse su più account IAM nella Guida per l'utente](#). IAM
- **Accesso tra servizi:** alcuni Servizi AWS utilizzano funzionalità in altri. Servizi AWS Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
- **Sessioni di accesso diretto (FAS):** quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un Servizio AWS, in combinazione con la richiesta di effettuare richieste Servizio AWS ai servizi downstream. FAS le richieste vengono effettuate solo quando

un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta [Forward access sessions](#).

- Ruolo di servizio: un ruolo di servizio è un [IAMruolo](#) che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, consulta [Creare un ruolo per delegare le autorizzazioni a un utente Servizio AWS nella Guida per l'IAMutente](#).
- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2istanza e che effettuano AWS CLI o effettuano AWS API richieste. È preferibile archiviare le chiavi di accesso all'interno dell'EC2istanza. Per assegnare un AWS ruolo a un'EC2istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'EC2istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta [Utilizzare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida per l'IAMutente](#).

## Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come JSON documenti. Per ulteriori informazioni sulla struttura e il contenuto dei documenti relativi alle JSON politiche, vedere [Panoramica delle JSON politiche](#) nella Guida per l'IAMutente.

Gli amministratori possono utilizzare AWS JSON le politiche per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore

può creare IAM politiche. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

IAMLe politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale criterio può ottenere informazioni sul ruolo da AWS Management Console, da o da. AWS CLI AWS API

## Policy basate su identità

I criteri basati sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta [Definire le IAM autorizzazioni personalizzate con](#) le politiche gestite dal cliente nella Guida per l'utente. IAM

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli all'interno del tuo Account AWS Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una politica gestita o una politica in linea, consulta [Scegliere tra politiche gestite e politiche in linea nella Guida](#) per l'IAMutente.

## Policy basate su risorse

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di policy basate sulle risorse sono le policy di IAM role trust e le policy di Amazon S3 bucket. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite contenute IAM in una policy basata sulle risorse.

## Elenchi di controllo degli accessi (ACLs)

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la [panoramica di Access control list \(ACL\)](#) nella Amazon Simple Storage Service Developer Guide.

## Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- **Limiti delle autorizzazioni:** un limite di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità (utente o ruolo). IAM È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. [Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità nella Guida per l'utente. IAM IAM](#)
- **Politiche di controllo del servizio (SCPs):** SCPs sono JSON politiche che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. SCP Limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna Utente root dell'account AWS. Per ulteriori informazioni su Organizations and SCPs, consulta [le politiche di controllo dei servizi](#) nella Guida AWS Organizations per l'utente.
- **Criteri di controllo delle risorse (RCPs):** RCPs sono JSON criteri che puoi utilizzare per impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare le IAM politiche allegate a ciascuna risorsa di tua proprietà. RCP Limita le autorizzazioni per le risorse negli account dei membri e può influire sulle autorizzazioni effettive per le identità, incluse le Utente root dell'account AWS, indipendentemente dal fatto che appartengano o meno all'organizzazione. Per ulteriori informazioni su Organizations e RCPs, incluso un elenco di Servizi AWS tale



supportoRCPs, vedere [Resource control policies \(RCPs\)](#) nella Guida per l'AWS Organizations utente.

- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta [le politiche di sessione](#) nella Guida IAM per l'utente.

## Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determinare se consentire una richiesta quando sono coinvolti più tipi di policy, consulta [Logica di valutazione delle politiche](#) nella Guida per l'IAMutente.

## Come funziona AWS End User Messaging Social con IAM

Prima di utilizzare IAM per gestire l'accesso a AWS End User Messaging Social, scopri quali IAM funzionalità sono disponibili per l'uso con AWS End User Messaging Social.

IAMfunzionalità che puoi utilizzare con AWS End User Messaging Social

IAMfunzionalità	AWS Messaggistica con l'utente finale Supporto sociale
<a href="#">Policy basate su identità</a>	Sì
<a href="#">Policy basate su risorse</a>	No
<a href="#">Azioni di policy</a>	Sì
<a href="#">Risorse relative alle policy</a>	Sì
<a href="#">Chiavi di condizione delle policy</a>	Sì
<a href="#">ACLs</a>	No



IAMfunzionalità	AWS Messaggistica con l'utente finale Supporto sociale
<a href="#">ABAC(tag nelle politiche)</a>	Parziale
<a href="#">Credenziali temporanee</a>	Sì
<a href="#">Autorizzazioni del principale</a>	Sì
<a href="#">Ruoli di servizio</a>	Sì
<a href="#">Ruoli collegati al servizio</a>	Sì

Per una panoramica generale del funzionamento dei AWS servizi di messaggistica con l'utente AWS finale, social e di altro tipo, con la maggior parte delle IAM funzionalità, consulta [AWS i servizi compatibili IAM](#) nella Guida per l'IAMutente.

## Politiche basate sull'identità per AWS End User Messaging Social

Supporta le policy basate su identità: sì

Le politiche basate sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta [Definire le IAM autorizzazioni personalizzate con](#) le politiche gestite dal cliente nella Guida per l'utente. IAM

Con le politiche IAM basate sull'identità, puoi specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per ulteriori informazioni su tutti gli elementi che è possibile utilizzare in una JSON politica, vedere il [riferimento agli elementi IAM JSON della politica](#) nella Guida per l'IAMutente.

## Esempi di policy basate sull'identità per AWS End User Messaging Social

Per visualizzare esempi di politiche basate sull'identità sociale di messaggistica con l'utente AWS finale, vedere. [Esempi di policy basate sull'identità per End User Messaging Social AWS](#)

## Politiche basate sulle risorse all'interno di End User Messaging Social AWS

Supporta le policy basate su risorse: no

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di policy basate sulle risorse sono le policy di IAM role trust e le policy di Amazon S3 bucket. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per abilitare l'accesso tra più account, puoi specificare un intero account o IAM entità in un altro account come principale in una politica basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un IAM amministratore dell'account fidato deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta la sezione [Cross Account Resource Access IAM nella Guida IAM per l'utente](#).

## Azioni politiche per AWS End User Messaging Social

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'Actionelemento di una JSON policy descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome dell' AWS APIoperazione associata. Esistono alcune eccezioni, come le azioni basate solo sulle autorizzazioni che non hanno un'operazione corrispondente. API Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni social di messaggistica dell'utente AWS finale, consulta [Azioni definite da AWS End User Messaging Social](#) nel Service Authorization Reference.

Le azioni politiche in AWS End User Messaging Social utilizzano il seguente prefisso prima dell'azione:

```
social-messaging
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

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

Per visualizzare esempi di politiche basate sull'identità sociale di AWS End User Messaging, vedere.

[Esempi di policy basate sull'identità per End User Messaging Social AWS](#)

## Risorse politiche per AWS End User Messaging Social

Supporta le risorse di policy: sì

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento Resource JSON policy specifica l'oggetto o gli oggetti a cui si applica l'azione. Le istruzioni devono includere un elemento Resource o un elemento NotResource. Come best practice, specifica una risorsa utilizzando il relativo [Amazon Resource Name \(ARN\)](#). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (\*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di risorse social per l'utente AWS finale e relativi ARNs, consulta [Resources Defined by AWS End User Messaging Social](#) nel Service Authorization Reference.

Per sapere con quali azioni è possibile specificare le diverse ARN risorse, consulta [Azioni definite dall'utente AWS finale di messaggistica sociale](#).

Per visualizzare esempi di politiche basate sull'identità dei social network di messaggistica per gli utenti AWS finali, vedere. [Esempi di policy basate sull'identità per End User Messaging Social AWS](#)

## Chiavi delle condizioni delle policy per AWS End User Messaging Social

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano [operatori di condizione](#), ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione AND logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica OR. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile concedere a un IAM utente l'autorizzazione ad accedere a una risorsa solo se è contrassegnata con il suo nome IAM utente. Per ulteriori informazioni, consulta [gli elementi IAM della politica: variabili e tag](#) nella Guida IAM per l'utente.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di [contesto delle condizioni AWS globali nella Guida](#) per l'IAM utente.

Per visualizzare un elenco delle chiavi di condizione di AWS End User Messaging Social, consulta [Condition Keys for AWS End User Messaging Social](#) nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave condizionale, vedi [Azioni definite da AWS End User Messaging Social](#).

Per visualizzare esempi di politiche basate sull'identità sociale di AWS End User Messaging, consulta. [Esempi di policy basate sull'identità per End User Messaging Social AWS](#)

## ACLsin AWS End User Messaging Social

SupportiACLs: no

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

## ABACcon AWS End User Messaging Social

Supporti ABAC (tag nelle politiche): Parziale

Il controllo degli accessi basato sugli attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. È possibile allegare tag a IAM entità (utenti o ruoli) e a molte AWS risorse. L'etichettatura di entità e risorse è il primo passo di ABAC. Quindi si progettano ABAC politiche per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa a cui sta tentando di accedere.

ABAC è utile in ambienti in rapida crescita e aiuta in situazioni in cui la gestione delle politiche diventa complicata.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'[elemento condizione](#) di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni in merito ABAC, vedere [Definizione delle autorizzazioni con ABAC autorizzazione](#) nella Guida per l'IAM utente. Per visualizzare un tutorial con i passaggi per la configurazione ABAC, consulta [Use Attribute-based access control \(ABAC\)](#) nella Guida per l'utente. IAM

## Utilizzo di credenziali temporanee con AWS End User Messaging Social

Supporta le credenziali temporanee: sì

Alcune Servizi AWS non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione [Servizi AWS relativa alla funzionalità IAM nella Guida](#) per l'IAM utente.

Si utilizzano credenziali temporanee se si accede AWS Management Console utilizzando qualsiasi metodo tranne il nome utente e la password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-on (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sul cambio di ruolo, consulta [Passare da un utente a un IAM ruolo \(console\)](#) nella Guida per l'IAMutente.

È possibile creare manualmente credenziali temporanee utilizzando AWS CLI o AWS API. È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, vedere [Credenziali di sicurezza temporanee](#) in IAM.

## Autorizzazioni principali multiservizio per AWS End User Messaging Social

Supporta sessioni di accesso diretto (FAS): Sì

Quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. FAS le richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta [Forward access sessions](#).

## Ruoli di servizio per AWS End User Messaging Social

Supporta i ruoli di servizio: sì

Un ruolo di servizio è un [IAM ruolo](#) che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'interno IAM. Per ulteriori informazioni, consulta [Creare un ruolo per delegare le autorizzazioni a un utente Servizio AWS nella Guida per l'IAMutente](#).

### Warning

La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità social di messaggistica con l'utente AWS finale. Modifica i ruoli di servizio solo quando AWS End User Messaging Social fornisce indicazioni in tal senso.

## Ruoli collegati ai servizi per AWS End User Messaging Social

Supporta ruoli collegati ai servizi: Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un servizio AWS. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

[Per informazioni dettagliate sulla creazione o la gestione di ruoli collegati ai servizi, consulta AWS Servizi compatibili con IAM](#) Trova un servizio nella tabella che include un Yes nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

## Esempi di policy basate sull'identità per End User Messaging Social AWS

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare le risorse AWS End User Messaging Social. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS API. Per concedere agli utenti il permesso di eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM policy. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

Per informazioni su come creare una politica IAM basata sull'identità utilizzando questi documenti di esempio, consulta [Create JSON IAM policy \(console\)](#) nella Guida per l'IAMutente.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da AWS End User Messaging Social, incluso il formato di ARNs per ogni tipo di risorsa, consulta [Azioni, risorse e chiavi di condizione per AWS End User Messaging Social](#) nel Service Authorization Reference.

### Argomenti

- [Best practice per le policy](#)
- [Utilizzo della console AWS End User Messaging Social](#)
- [Consentire agli utenti di visualizzare le loro autorizzazioni](#)

## Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse social di messaggistica con l'utente AWS finale nel tuo account. Queste azioni possono comportare

costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni. AWS Sono disponibili nel tuo Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta [le politiche AWS gestite o le politiche AWS gestite per le funzioni lavorative](#) nella Guida per l'IAM utente.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le IAM politiche, concedi solo le autorizzazioni necessarie per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo per applicare le autorizzazioni, consulta [Politiche](#) e autorizzazioni nella Guida IAM per l'utente. IAM IAM
- Utilizza le condizioni nelle IAM politiche per limitare ulteriormente l'accesso: puoi aggiungere una condizione alle tue politiche per limitare l'accesso ad azioni e risorse. Ad esempio, puoi scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. È inoltre possibile utilizzare condizioni per concedere l'accesso alle azioni di servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta [Elementi IAM JSON della politica: Condizione](#) nella Guida IAM per l'utente.
- Usa IAM Access Analyzer per convalidare IAM le tue policy e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio delle IAM policy ( ) e alle best practice. JSON IAM IAM Access Analyzer fornisce più di 100 controlli delle politiche e consigli pratici per aiutarti a creare policy sicure e funzionali. Per ulteriori informazioni, consulta [Convalida delle politiche con IAM Access Analyzer](#) nella Guida per l'utente. IAM
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede l'utilizzo di IAM utenti o di un utente root Account AWS, attiva questa opzione MFA per una maggiore sicurezza. Per richiedere MFA quando vengono richiamate API le operazioni, aggiungi MFA delle condizioni alle tue politiche. Per ulteriori informazioni, consulta [Secure API access with MFA](#) nella Guida IAM per l'utente.

Per ulteriori informazioni sulle best practice in IAM, consulta la sezione [Procedure consigliate in materia di sicurezza IAM](#) nella Guida IAM per l'utente.



## Utilizzo della console AWS End User Messaging Social

Per accedere alla console AWS End User Messaging Social, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse social di AWS End User Messaging presenti nel tuo Account AWS. Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso il AWS CLI o il AWS API. Consenti invece l'accesso solo alle azioni che corrispondono all'API operazione che stanno cercando di eseguire.

Per garantire che gli utenti e i ruoli possano ancora utilizzare la console AWS End User Messaging Social, allega anche la policy AWS End User Messaging Social *ConsoleAccess* o *ReadOnly* AWS gestita alle entità. Per ulteriori informazioni, consulta [Aggiungere autorizzazioni a un utente](#) nella Guida per l'IAM utente.

## Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra come è possibile creare una politica che consenta IAM agli utenti di visualizzare le politiche in linea e gestite allegate alla loro identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando o a livello di codice. AWS CLI  
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": "*"
}
]
```

## AWS politiche gestite per AWS End User Messaging Social

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare le policy AWS gestite che scrivere le politiche da soli. Ci vogliono tempo ed esperienza per [creare politiche gestite dai IAM clienti](#) che forniscano al team solo le autorizzazioni di cui ha bisogno. Per iniziare rapidamente, puoi utilizzare le nostre politiche AWS gestite. Queste policy coprono i casi d'uso comuni e sono disponibili nel tuo Account AWS. Per ulteriori informazioni sulle politiche AWS gestite, consulta [le politiche AWS gestite](#) nella Guida IAM per l'utente.

AWS i servizi mantengono e aggiornano le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi occasionalmente aggiungono altre autorizzazioni a una policy gestita da AWS per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una policy gestita da AWS quando viene avviata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy AWS gestita, quindi gli aggiornamenti delle policy non comprometteranno le autorizzazioni esistenti.

Inoltre, AWS supporta politiche gestite per le funzioni lavorative che si estendono su più servizi. Ad esempio, la policy ReadOnlyAccess AWS gestita fornisce l'accesso in sola lettura a tutti i AWS

servizi e le risorse. Quando un servizio lancia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per un elenco e le descrizioni delle politiche relative alle funzioni lavorative, consulta le [politiche AWS gestite per le funzioni lavorative nella Guida per l'utente](#).  
IAM

## AWS Messaggistica con l'utente finale Aggiornamenti social alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti alle politiche AWS gestite per AWS End User Messaging Social da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al RSS feed nella pagina di cronologia dei documenti social di messaggistica per l'utente AWS finale.

Modifica	Descrizione	Data
AWS End User Messaging Social ha iniziato a tenere traccia delle modifiche	AWS End User Messaging Social ha iniziato a tenere traccia delle modifiche alle politiche AWS gestite.	10 ottobre 2024

## Risoluzione dei problemi relativi all'identità e all'accesso social di AWS End User Messaging

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con AWS End User Messaging Social and IAM.

### Argomenti

- [Non sono autorizzato a eseguire alcuna azione in AWS End User Messaging Social](#)
- [Non sono autorizzato a eseguire iam: PassRole](#)
- [Desidero consentire a persone esterne a me di accedere Account AWS alle mie risorse social di messaggistica per gli utenti AWS finali](#)

## Non sono autorizzato a eseguire alcuna azione in AWS End User Messaging Social

Se ricevi un errore che indica che non disponi dell'autorizzazione per eseguire un'operazione, le tue policy devono essere aggiornate in modo che ti sei consentito eseguire tale operazione.

L'errore di esempio seguente si verifica quando l'utente `mateojackson` tenta di utilizzare la console per visualizzare i dettagli su una `my-example-widget` risorsa fittizia ma non dispone delle autorizzazioni fittizie `social-messaging:GetWidget`.

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

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa `my-example-widget` utilizzando l'azione `social-messaging:GetWidget`.

Se hai bisogno di assistenza, contatta l'amministratore. AWS L'amministratore è la persona che ti ha fornito le credenziali di accesso.

## Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'azione `iam:PassRole`, le tue politiche devono essere aggiornate per consentirti di assegnare un ruolo a AWS End User Messaging Social.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio anziché creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un IAM utente denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in AWS End User Messaging Social. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

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

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta AWS l'amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Desidero consentire a persone esterne a me di accedere Account AWS alle mie risorse social di messaggistica per gli utenti AWS finali

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS End User Messaging Social supporta queste funzionalità, consulta [Come funziona AWS End User Messaging Social con IAM](#)
- Per sapere come fornire l'accesso alle risorse di tua proprietà, consulta [Fornire l'accesso a un IAM utente di un altro Account AWS utente di tua proprietà](#) nella Guida per l'IAMutente. Account AWS
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta [Fornire l'accesso a persone Account AWS di proprietà di terzi](#) nella Guida per l'IAMutente.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso agli utenti autenticati esternamente \(federazione delle identità\)](#) nella Guida per l'IAMutente.
- Per conoscere la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle [risorse tra account nella Guida per l'utente](#). IAM IAM


## Convalida della conformità per End User Messaging Social AWS

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione [Scope by Compliance Program Servizi AWS](#) e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di [AWS conformità Programmi](#) di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta [Scaricamento dei report in AWS Artifact](#) .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- [Sicurezza, conformità e governance](#): queste guide all'implementazione della soluzione illustrano le considerazioni relative all'architettura e forniscono i passaggi per l'implementazione delle funzionalità di sicurezza e conformità.
- [Architettura per la HIPAA sicurezza e la conformità su Amazon Web Services](#): questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee. HIPAA

 Note

Non tutte sono idonee. Servizi AWS HIPAA Per ulteriori informazioni, consulta la [Guida ai servizi HIPAA idonei](#).

- [AWS Risorse per AWS](#) per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe riguardare il tuo settore e la tua località.
- [AWS Guide alla conformità dei clienti](#): comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization ()). ISO
- [Evaluating Resources with Rules](#) nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- [AWS Security Hub](#)— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina [Documentazione di riferimento sui controlli della Centrale di sicurezza](#).
- [Amazon GuardDuty](#): Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, ad esempio PCI DSS soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- [AWS Audit Manager](#)— Ciò Servizio AWS consente di verificare continuamente AWS l'utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

## Resilienza nella messaggistica sociale per gli utenti AWS finali

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

[Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS](#)

Oltre all'infrastruttura AWS globale, AWS End User Messaging Social offre diverse funzionalità per supportare le esigenze di resilienza e backup dei dati.

## Sicurezza dell'infrastruttura nella messaggistica AWS sociale degli utenti finali

In quanto servizio gestito, AWS End User Messaging Social è protetto dalle procedure di sicurezza di rete AWS globali descritte nel white paper [Amazon Web Services: Overview of Security Processes](#).

Utilizzi API le chiamate AWS pubblicate per accedere a AWS End User Messaging Social attraverso la rete. I client devono supportare Transport Layer Security (TLS) 1.0 o versione successiva. Consigliamo TLS 1.2 o versioni successive. I client devono inoltre supportare suite di crittografia con Perfect Forward Secrecy (PFS) come (Ephemeral Diffie-Hellman) o DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale. IAM O puoi utilizzare [AWS Security Token Service](#) (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

## Prevenzione del problema "confused deputy" tra servizi

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. Nel frattempo AWS, l'impersonificazione tra servizi può portare al confuso

problema del vice. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare ciò, AWS fornisce strumenti per poterti a proteggere i tuoi dati per tutti i servizi con entità di servizio a cui è stato concesso l'accesso alle risorse del tuo account.

Ti consigliamo di utilizzare le chiavi di contesto [aws:SourceArn](#) la condizione [aws:SourceAccount](#) globale nelle politiche delle risorse per limitare le autorizzazioni che Social Messaging concede a un altro servizio alla risorsa. Utilizza `aws:SourceArn` se desideri consentire l'associazione di una sola risorsa all'accesso tra servizi. Utilizza `aws:SourceAccount` se desideri consentire l'associazione di qualsiasi risorsa in tale account all'uso tra servizi.

Il modo più efficace per proteggersi dal confuso problema del vice è utilizzare la chiave di contesto ARN della condizione `aws:SourceArn` globale con l'intera risorsa. Se non conosci la dimensione completa ARN della risorsa o se stai specificando più risorse, usa la chiave `aws:SourceArn` global context condition con caratteri jolly (\*) per le parti sconosciute di. ARN Ad esempio `arn:aws:social-messaging:*:123456789012:*`.

Se il `aws:SourceArn` valore non contiene l'ID dell'account, ad esempio un bucket Amazon S3 ARN, devi utilizzare entrambe le chiavi di contesto della condizione globale per limitare le autorizzazioni.

Il valore di `aws:SourceArn` deve essere `ResourceDescription`.

L'esempio seguente mostra come utilizzare le chiavi contestuali `aws:SourceArn` e `aws:SourceAccount` global condition in Social Messaging per evitare il confuso problema del vice.

```
{
  "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"
}
}
}
```

## Best practice di sicurezza

AWS End User Messaging Social offre una serie di funzionalità di sicurezza da prendere in considerazione durante lo sviluppo e l'implementazione delle proprie politiche di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per l'ambiente, gestiscile come considerazioni utili anziché prescrizioni.

- Crea un utente individuale per ogni persona che gestisce AWS SMS le risorse, incluso te stesso. Non utilizzare le credenziali AWS root per gestire AWS SMS le risorse.
- Assegna a ciascun utente un set minimo di autorizzazioni richieste per eseguire le proprie mansioni.
- Usa IAM i gruppi per gestire efficacemente le autorizzazioni per più utenti.
- Ruota periodicamente le credenziali IAM.

## Utilizzo di ruoli collegati ai servizi per AWS End User Messaging Social

AWS End User Messaging Social utilizza AWS Identity and Access Management (IAM) ruoli collegati [ai servizi](#). Un ruolo collegato al servizio è un tipo unico di IAM ruolo collegato direttamente a AWS End User Messaging Social. I ruoli collegati ai servizi sono predefiniti da AWS End User Messaging Social e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per conto dell'utente. AWS

Un ruolo collegato ai servizi semplifica la configurazione di AWS End User Messaging Social perché non è necessario aggiungere manualmente le autorizzazioni necessarie. AWS End User Messaging

Social definisce le autorizzazioni dei suoi ruoli collegati al servizio e, se non diversamente definito, solo AWS End User Messaging Social può assumerne i ruoli. Le autorizzazioni definite includono la politica di fiducia e la politica di autorizzazione e tale politica di autorizzazione non può essere associata a nessun'altra entità. IAM

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. In questo modo si proteggono le risorse social di messaggistica per gli utenti AWS finali, in quanto non è possibile rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta [AWS i servizi che funzionano con IAM](#) e cerca i servizi con Sì nella colonna Ruoli collegati ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

## Autorizzazioni di ruolo collegate al servizio per End User Messaging Social AWS

AWS End User Messaging Social utilizza il ruolo collegato al servizio denominato `AWSServiceRoleForSocialMessaging`— Per pubblicare metriche e fornire informazioni dettagliate per l'invio di messaggi sui social.

Il ruolo `AWSServiceRoleForSocialMessaging` collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `social-messaging.amazonaws.com`

La politica di autorizzazione dei ruoli denominata `AWSSocialMessagingServiceRolePolicy` consente a AWS End User Messaging Social di completare le seguenti azioni sulle risorse specificate:

- Operazione: `"cloudwatch:PutMetricData"` su all AWS resources in the AWS/SocialMessaging namespace.

Per consentire a utenti, gruppi o ruoli di creare, modificare o eliminare un ruolo orientato ai servizi, devi configurare le autorizzazioni. Per ulteriori informazioni, consulta le [autorizzazioni dei ruoli collegati ai servizi](#) nella Guida per l'utente. IAM

Per gli aggiornamenti alla politica, vedere. [AWS Messaggistica con l'utente finale Aggiornamenti social alle politiche AWS gestite](#)

## Creazione di un ruolo collegato al servizio per AWS End User Messaging Social

Puoi utilizzare la IAM console per creare un ruolo collegato al servizio con lo use case `AWSEndUserMessagingSocial-Metrics`. In AWS CLI o il AWS API, crea un ruolo collegato al servizio con il nome del servizio. `social-messaging.amazonaws.com` Per ulteriori informazioni, consulta [Creazione di un ruolo collegato al servizio](#) nella Guida per l'utente. IAM Se elimini il ruolo collegato ai servizi, puoi utilizzare lo stesso processo per crearlo nuovamente.

È possibile creare il ruolo collegato al servizio per AWS End User Messaging Social con il seguente comando: AWS CLI

```
aws iam create-service-linked-role --aws-service-name social-messaging.amazonaws.com
```

## Modifica di un ruolo collegato al servizio per End User Messaging Social AWS

AWS End User Messaging Social non consente di modificare il ruolo collegato al `AWSServiceRoleForSocialMessaging` servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. Tuttavia, è possibile modificare la descrizione del ruolo utilizzando. IAM Per ulteriori informazioni, consulta [Modifica di un ruolo collegato al servizio nella Guida](#) per l'IAMutente.

## Eliminazione di un ruolo collegato al servizio per End User Messaging Social AWS

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

### Note

Se il servizio AWS End User Messaging Social utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per rimuovere le risorse social di messaggistica per l'utente AWS finale utilizzate dal `AWSServiceRoleForSocialMessaging`

1. Chiama `list-linked-whatsapp-business-accounts` API per vedere le risorse che hai.
2. Per ogni account Whats App Business collegato, chiama `disassociate-whatsapp-business-account` API per rimuovere la risorsa dal SocialMessaging servizio.
3. Verifica che non vengano restituite risorse chiamando `list-linked-whatsapp-business-accounts` API nuovamente il.

Per eliminare manualmente il ruolo collegato al servizio utilizzando IAM

Usa la IAM console AWS CLI, o il AWS API per eliminare il ruolo collegato al `AWSServiceRoleForSocialMessaging` servizio. Per ulteriori informazioni, vedere [Eliminazione di un ruolo collegato al servizio nella Guida per l'utente](#). IAM

## Regioni supportate per i ruoli collegati ai servizi social di messaggistica con l'utente AWS finale

AWS End User Messaging Social supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta [AWS Regioni ed endpoint](#).

# Accedi a AWS End User Messaging Social utilizzando un'interfaccia endpoint ( )AWS PrivateLink

Puoi utilizzarlo AWS PrivateLink per creare una connessione privata tra il tuo account VPC e AWS End User Messaging Social. Puoi accedere a AWS End User Messaging Social come se fosse sul tuo computerVPC, senza l'uso di un gateway, NAT dispositivo, VPN connessione o AWS Direct Connect connessione Internet. Le istanze del tuo VPC non hanno bisogno di indirizzi IP pubblici per accedere a AWS End User Messaging Social.

Stabilisci questa connessione privata creando un endpoint di interfaccia attivato da AWS PrivateLink. In ciascuna sottorete viene creata un'interfaccia di rete endpoint da abilitare per l'endpoint di interfaccia. Si tratta di interfacce di rete gestite dai richiedenti che fungono da punto di ingresso per il traffico destinato all'End User Messaging Social. AWS

Per ulteriori informazioni, consulta la sezione [Accesso Servizi AWS tramite AWS PrivateLink](#) nella Guida.AWS PrivateLink

## Considerazioni sulla messaggistica social per gli utenti AWS finali

Prima di configurare un endpoint di interfaccia per AWS End User Messaging Social, consulta [le considerazioni nella Guida](#).AWS PrivateLink

AWS End User Messaging Social supporta l'esecuzione di chiamate a tutte le sue API azioni tramite l'interfaccia endpoint.

VPCle politiche degli endpoint non sono supportate per AWS End User Messaging Social. Per impostazione predefinita, l'accesso completo a AWS End User Messaging Social è consentito tramite l'interfaccia endpoint. In alternativa, è possibile associare un gruppo di sicurezza alle interfacce di rete dell'endpoint per controllare il traffico verso AWS End User Messaging Social tramite l'endpoint dell'interfaccia.

## Crea un endpoint di interfaccia per AWS End User Messaging Social

Puoi creare un endpoint di interfaccia per AWS End User Messaging Social utilizzando la VPC console Amazon o AWS Command Line Interface (AWS CLI). Per ulteriori informazioni, consulta la sezione [Creazione di un endpoint di interfaccia](#) nella Guida per l'utente di AWS PrivateLink .

Crea un endpoint di interfaccia per AWS End User Messaging Social utilizzando il seguente nome di servizio:

- `com.amazonaws.region.social-messaging`

Se abiliti private DNS per l'endpoint dell'interfaccia, puoi effettuare API richieste a AWS End User Messaging Social utilizzando il nome regionale DNS predefinito. Ad esempio `service-name.us-east-1.amazonaws.com`.

## Creazione di una policy dell' endpoint per l'endpoint dell'interfaccia

Una policy per gli endpoint è una IAM risorsa che è possibile allegare a un endpoint di interfaccia. La policy predefinita per gli endpoint consente l'accesso completo a AWS End User Messaging Social tramite l'interfaccia endpoint. Per controllare l'accesso consentito a AWS End User Messaging Social dal tuoVPC, allega una policy personalizzata per l'endpoint all'endpoint di interfaccia.

Una policy di endpoint specifica le informazioni riportate di seguito:

- I principali che possono eseguire azioni (IAMutenti Account AWS e IAM ruoli).
- Le azioni che possono essere eseguite.
- Le risorse in cui è possibile eseguire le operazioni.

Per ulteriori informazioni, consulta la sezione [Controllo dell'accesso ai servizi con policy di endpoint](#) nella Guida di AWS PrivateLink .

Esempio: policy VPC sugli endpoint per le azioni social di messaggistica con l'utente AWS finale

Di seguito è riportato l'esempio di una policy dell'endpoint personalizzata. Quando alleghi questa policy all'endpoint dell'interfaccia, concede l'accesso alle azioni social elencate di AWS End User Messaging a tutti i responsabili su tutte le risorse.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "social-messaging:DeleteWhatsAppMessageMedia",

```

```
        "social-messaging:PostWhatsAppMessageMedia",
        "social-messaging:SendWhatsAppMessage"
    ],
    "Resource": "*"
}
]
```

## Quote per la messaggistica AWS sociale degli utenti finali

Il tuo AWS account ha delle quote predefinite, precedentemente denominate limiti, per ogni servizio. AWS Salvo diversa indicazione, ogni quota si applica a una regione specifica. Se per alcune quote è possibile richiedere aumenti, altre quote non possono essere modificate.

Il tuo AWS account ha le seguenti quote relative a AWS End User Messaging Social.

Risorsa	Di default
WhatsApp Account aziendale ( ) WABA	25 per regione

AWS End User Messaging Social implementa quote che limitano il numero di richieste che puoi inviare all' AWS End User Messaging Social API dal tuo. Account AWS

Operazione	Quota di velocità predefinita (richieste al secondo)
SendWhatsAppMessage	1.000
PostWhatsAppMessageMedia	100
GetWhatsAppMessageMedia	100
DeleteWhatsAppMessageMedia	100
DisassociateWhatsAppBusinessAccount	10
ListWhatsAppBusinessAccount	10
TagResource	10
UntagResourceRate	10
ListTagsForResourceRate	10



# Cronologia dei documenti per l' AWS End User Messaging Social User Guide

La tabella seguente descrive le versioni della documentazione per AWS End User Messaging Social.

Modifica	Descrizione	Data
<a href="#">AWS PrivateLink</a>	È stato aggiunto il supporto per AWS PrivateLink. Per ulteriori informazioni, consulta <a href="#">AWS PrivateLink</a> .	22 ottobre 2024
<a href="#">Versione iniziale</a>	Versione iniziale della AWS End User Messaging Social User Guide	10 ottobre 2024

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.