



用户指南

AWS 最终用户消息社交



AWS 最终用户消息社交: 用户指南

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

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

什么是 AWS 最终用户消息社交？	1
您是否是首次使用 Master AWS nization？	1
AWS 最终用户消息社交的功能	1
相关服务	2
访问 AWS 最终用户消息社交网站	2
区域可用性	2
设置 AWS 最终用户消息社交	5
注册。AWS 账户	5
创建具有管理访问权限的用户	5
后续步骤	6
开始使用	7
注册 WhatsApp	7
先决条件	7
通过控制台注册	8
后续步骤	11
WhatsApp 企业账户 (WABA)	12
查看 WABA	12
添加一个 WABA	13
WhatsApp 企业账户类型	13
其他资源	14
电话号码	15
电话号码注意事项	15
添加电话号码	15
先决条件	16
将电话号码添加到 WABA	16
查看电话号码的状态	17
查看电话号码的 ID	17
提高消息对话限制	18
增加消息吞吐能力	19
了解电话号码质量评级	19
查看电话号码质量评级	19
消息模板	21
在 WhatsApp 管理器中使用消息模板	21
后续步骤	22

模板节奏	22
获取有关模板已降低状态的反馈	22
模板状态和质量评级	22
模板被拒绝的原因	24
消息和事件目标	25
添加事件目标	25
先决条件	25
添加消息和事件目的地	25
加密的 Amazon SNS 主题政策	26
后续步骤	27
消息和事件格式	27
AWS 最终用户消息社交事件标题	27
WhatsApp JSON短信示例	28
媒体消息示例 WhatsApp JSON	29
消息状态	30
消息状态	30
其他资源	31
上传媒体文件	32
支持的媒体文件类型	33
媒体文件类型	33
消息类型	35
其他资源	35
发送消息	36
发送模板消息	36
发送媒体消息	37
回复收到的消息	39
将消息的状态更改为已读	39
用反应回应	39
从以下地址将媒体文件下载到 Amazon S3 WhatsApp	40
回复消息的示例	41
先决条件	41
正在回应	41
其他资源	43
了解您的账单	44
示例 1：发送营销模板消息	47
示例 2：打开服务对话	47

账单ISO代码	48
监控	61
使用监控 CloudWatch	61
CloudTrail 日志	62
AWS 最终用户消息中的社交数据事件 CloudTrail	63
AWS 最终用户消息中的社交管理事件 CloudTrail	64
AWS 最终用户消息社交活动示例	64
最佳实践	67
Up-to-date 业务概况	67
获取权限	67
禁止的消息内容	68
审核客户列表	69
基于参与度调整您的发送	70
在适当时间发送	70
安全性	71
数据保护	71
数据加密	72
传输中加密	73
密钥管理	73
互连网络流量隐私	73
Identity and Access Management	74
受众	74
使用身份进行身份验证	75
使用策略管理访问	77
AWS 最终用户消息社交是如何与之配合使用的 IAM	79
基于身份的策略示例	85
AWS 托管策略	87
故障排除	88
合规性验证	90
弹性	91
基础架构安全性	91
防止跨服务混淆代理	91
安全最佳实操	93
使用服务相关角色	93
Application Servicati AWS on 的服务相关角色权限	93
为 Classic AWS 创建服务相关角色	94

为 Fleet Advisor AWS 编辑服务相关角色	94
为 Classic AWS 删除服务相关角色	94
Application A AWS pplication 服务相关角色的受支持区域	95
配额	96
文档历史记录	97
.....	xcviii

什么是 AWS 最终用户消息社交？

AWS 最终用户消息 Social，也称为社交消息，是一种消息服务，允许开发人员 WhatsApp 将其集成到他们的应用程序中。它提供了对丰富消息传递功能 WhatsApp 的访问权限，从而可以创建带有图像、视频和按钮的品牌化交互式内容。通过使用此服务，您可以将 WhatsApp 消息传递功能与现有渠道（例如 SMS 和推送通知）一起添加到应用程序中，从而允许您通过客户首选的沟通渠道与他们互动。

首先，您可以使用 AWS 最终用户消息社交控制台中的自助式入门流程创建新的 WhatsApp 企业账户 (WABA)，也可以 WABA 将现有账户关联到该服务。

主题

- [您是否是首次使用 Master AWS nization？](#)
- [AWS 最终用户消息社交的功能](#)
- [相关服务](#)
- [访问 AWS 最终用户消息社交网站](#)
- [区域可用性](#)

您是否是首次使用 Master AWS nization？

如果您是首次接触 Mess AWS ages Social 的用户，建议您先阅读以下部分：

- [设置 AWS 最终用户消息社交](#)
- [AWS 终端用户消息社交入门](#)
- [AWS 最终用户消息社交的最佳实践](#)

AWS 最终用户消息社交的功能

AWS 最终用户消息社交提供以下特征和功能：

- 通过 [创建并使用消息模板](#)，设计一致的消息并更有效地重用内容。消息模板包含要在发送的消息中重用的内容和设置。
- 使用全新的丰富消息传递功能，获得更具吸引力的体验。除了文字和媒体之外，您还可以发送位置和交互式消息。
- 接收来自客户的短信和媒体消息。
- 通过 Meta 验证您的企业身份，与客户建立信任。

相关服务

AWS 提供其他可在多渠道工作流程中一起使用的消息服务：

- 使用[AWS 最终用户消息SMS](#)发送SMS消息
- 使用[AWS 最终用户消息推送](#)发送推送通知
- 使用 [Amazon SES](#) 发送电子邮件

访问 AWS 最终用户消息社交网站

您可以使用以下方式访问 AWS 最终用户消息社交网站：

AWS 最终用户消息社交控制台

用于[创建](#)和管理资源的 Web 界面。

AWS Command Line Interface

在命令行 Shell 中使用命令与 AWS 服务进行交互。在 AWS Command Line Interface Windows、macOS 和 Linux 上受支持。有关更多信息 AWS CLI，请参阅《[AWS Command Line Interface 用户指南](#)》。您可以在《[AWS SMS 命令参考](#)》中找到这些AWS CLI 命令。

AWS SDKs

如果您是倾向于使用特定语言APIs而非提交请求来HTTP构建应用程序的软件开发人员HTTPS，AWS 提供库文件、示例代码、教程和其他资源。这些库文件提供可自动执行任务的基本功能，例如以加密方式对请求签名、重试请求和处理错误响应。这些功能有助于您更高效地入门。有关更多信息，请参阅[用于在 AWS上进行构建的工具](#)。

区域可用性

AWS 最终用户消息社交 AWS 区域 在北美、欧洲、亚洲和大洋洲的多个区域中均已推出。在每个区域中，AWS 维护多个可用区。这些可用区的物理位置是相互隔离的，但可通过私有、低延迟、高吞吐量和高度冗余的网络连接联合在一起。这些可用区用于提供极高水平的可用性和冗余，同时最大程度地减少延迟。

要了解更多信息 AWS 区域，请参阅中的[指定 AWS 区域 您的账户可以使用的](#)内容Amazon Web Services 一般参考。有关当前支持 AWS 最终用户消息社交的所有区域以及每个区域的终端节点的列

表，请参阅下表中的[终端 AWS 端用户消息社交API和AWS 服务终端节点的Amazon Web Services 一般参考终端节点和配额](#)。要详细了解每个区域中可用的可用区数量，请参阅[AWS 全球基础设施](#)。

区域可用性

区域名称	区域	终端节点	WhatsApp API版本
美国东部 (弗吉尼亚州北部)	us-east-1	social-messaging.us-east-1.amazonaws.com social-messaging-fips.us-east-1.api.aws social-messaging.us-east-1.api.aws	版本 20 及更高版本
美国东部 (俄亥俄州)	us-east-2	social-messaging.us-east-2.amazonaws.com social-messaging-fips.us-east-2.api.aws social-messaging.us-east-2.api.aws	版本 20 及更高版本
美国西部 (俄勒冈州)	us-west-2	social-messaging.us-west-2.amazonaws.com social-messaging-fips.us-west-2.api.aws social-messaging.us-west-2.api.aws	版本 20 及更高版本
亚太地区 (孟买)	ap-south-1	social-messaging.ap-south-1.amazonaws.com	版本 20 及更高版本

区域名称	区域	终端节点	WhatsApp API版本
		social-messaging.ap-south-1.api.aws	
亚太地区 (新加坡)	ap-southeast-1	social-messaging.ap-southeast-1.amazonaws.com social-messaging.ap-southeast-1.api.aws	版本 20 及更高版本
欧洲地区 (爱尔兰)	eu-west-1	social-messaging.eu-west-1.amazonaws.com social-messaging.eu-west-1.api.aws	版本 20 及更高版本
欧洲 (伦敦)	eu-west-2	social-messaging.eu-west-2.amazonaws.com social-messaging.eu-west-1.api.aws	版本 20 及更高版本

设置 AWS 最终用户消息社交

在首次使用 AWS 最终用户消息社交之前，您必须完成以下步骤。

主题

- [注册。AWS 账户](#)
- [创建具有管理访问权限的用户](#)
- [后续步骤](#)

注册。AWS 账户

如果您还没有 AWS 账户，请完成以下步骤创建一个账户。

如何注册。AWS 账户

1. 打开<https://portal.aws.amazon.com/billing/注册>。
2. 按照屏幕上的说明进行操作。

在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

当您注册时 AWS 账户，就会创建 AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务和资源。作为安全最佳实践，请为用户分配管理访问权限，并且只使用根用户来执行[需要根用户访问权限的任务](#)。

AWS 注册过程完成后，会向您发送一封确认电子邮件。在任何时候，您都可以通过转至 <https://aws.amazon.com/> 并选择 My Account (我的账户) 来查看当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

注册后 AWS 账户，请保护好您的 AWS 账户根用户 AWS IAM Identity Center，启用，并创建一个管理用户，以避免使用根用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。[AWS Management Console](#)在下一页上，输入您的密码。

要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的[以根用户身份登录](#)。

2. 对您的根用户启用多重身份验证 (MFA)。

有关说明，请参阅《用户指南》中的[“为 AWS 账户 root 用户（控制台）启用虚拟MFA设备” IAM](#)。

创建具有管理访问权限的用户

1. 启用IAM身份中心。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的[启用 AWS IAM Identity Center](#)。

2. 在 IAM Identity Center 中，为用户授予管理访问权限。

有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《[用户指南](#)》IAM Identity Center 目录中的[使用默认设置配置AWS IAM Identity Center 用户访问权限](#)。

以具有管理访问权限的用户身份登录

- 要使用您的 Identity Center 用户IAM身份登录URL，请使用您在创建 Ident IAM ity Center 用户时发送到您的电子邮件地址的登录信息。

要获取使用Ident IAM ity Center 用户[登录方面的帮助](#)，请参阅《AWS 登录 用户指南》中的[登录 AWS 访问门户](#)。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的[创建权限集](#)。

2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的[添加组](#)。

后续步骤

现在，您已经准备好使用 AWS 最终用户消息社交了，[AWS 终端用户消息社交入门](#)有关创建 WhatsApp 企业账户 (WABA) 或迁移现有 WhatsApp 企业账户的信息，请参阅。

AWS 终端用户消息社交入门

这些主题将指导您完成将 WhatsApp 企业账户 (WABA) 关联或迁移到 AWS 最终用户消息社交的步骤。

主题

- [注册 WhatsApp](#)

注册 WhatsApp

WhatsApp 企业账户 (WABA) 允许您的企业使用 WhatsApp 商业平台直接向客户发送消息。您的所有人 WABAs 都是您的 Meta 业务组合的一部分。A WABA 包含面向客户的资产，例如电话号码、模板和 WhatsApp 企业资料。WhatsApp 企业资料包含用户可以看到的贵公司的联系信息。有关 WhatsApp 企业账户的更多信息，请参阅[WhatsApp AWS 最终用户消息社交中的企业账户 \(WABA\)](#)。

按照本部分中的步骤来开始使用 AWS 最终用户消息 Social。使用嵌入式注册流程创建新的 WhatsApp 企业账户 (WABA) 或将现有账户迁移 WABA 到 AWS 最终用户消息社交网站。

先决条件

Important

使用 Meta/ WhatsApp

- 您对 WhatsApp 商业解决方案的使用需遵守商业[服务条款](#)、[WhatsApp 商业解决方案条款](#)、[WhatsApp WhatsApp 商业消息政策](#)、[消息传递指南](#)以及其中以引用方式纳入的所有其他条款、政策或指南（因为每项条款可能会不时更新）的条款和条件。WhatsApp
- Meta 或 WhatsApp 可能随时禁止您使用 WhatsApp 商业解决方案。
- 您必须使用 Meta 创建 WhatsApp 企业账户（“WABA”）和 WhatsApp。
- 您必须使用 Meta 创建商务经理账户并将其关联到您的 WABA。
- 您必须向我们提供 WABA 对您的控制权。根据您的要求，我们将使用 Meta WABA 向我们提供的方法，以合理和及时的方式将您的控制权移交给您。
- 在使用 WhatsApp 商业解决方案时，您不得提交任何受适用法律和/或法规保护和/或限制发布的内容、信息或数据。
- WhatsApp 有关使用 WhatsApp 业务解决方案的定价，请访问[基于对话](#)的定价。

- 要创建 WhatsApp 企业账户 (WABA)，您的企业需要一个[元企业账户](#)。检查您的公司是否已经拥有元企业账户。如果您没有 Meta Business 账户，则可以在注册过程中创建一个。
- 要使用已在 WhatsApp Messenger 应用程序或 WhatsApp 企业应用程序中使用的电话号码，必须先将其删除。
- 可以接收SMS或语音一次性密码 (OTP) 的电话号码。用于注册的电话号码将与您的 WhatsApp 帐户关联，并在您发送消息时使用该电话号码。该电话号码仍可用于SMSMMS、和语音消息。
- 如果要导入现有的电话号码WABA，则需要PINs为与导入的号码关联的所有电话号码WABA。要重置丢失或遗忘的PIN，请按照WhatsApp 商业平台云API参考PIN中的[更新](#)中的说明进行操作。

通过控制台注册

按照以下说明创建新 WhatsApp 帐户、迁移现有帐户或向现有帐户添加电话号码WABA。作为注册过程的一部分，您授予 AWS 最终用户消息社交访问您的 WhatsApp 企业账户的权限。您还允许 AWS 最终用户消息社交网站向您收取消息费用。有关 WhatsApp 企业账户的更多信息，请参阅[了解 WhatsApp 企业账户类型](#)。

1. 打开 AWS 最终用户消息社交控制台，网址为<https://console.aws.amazon.com/social-messaging/>。
2. 选择企业账户。
3. 在关联企业账户页面上，选择启动 Facebook 门户。将会出现一个来自 Meta 的新登录窗口。
4. 在元登录窗口中，输入你的 Facebook 账号凭证。

在WhatsApp 企业账户页面上，选择添加 WhatsApp 电话号码。在添加 WhatsApp 电话号码页面上，选择启动 Facebook 门户。将会出现一个来自 Meta 的新登录窗口。

5. 在元登录窗口中，输入你的 Facebook 账号凭证。
6. 作为注册过程的一部分，您授予 AWS 最终用户消息社交访问您的 WhatsApp 企业账户 (WABA) 的权限。您还允许 AWS 最终用户消息社交网站向您收取消息费用。选择继续。
7. 对于 Meta Business 账户，请选择现有的 Meta 企业账户或创建元企业账户。
 - a. (可选) 如果您需要创建一个 Meta Business 账户，请按照以下步骤操作：
 - b. 在企业名称中，输入您的公司名称。
 - c. 对于企业网站或个人资料页面，请输入您公司网站的，或者如果您的公司没有网站，请URL进入您的社交媒体页面。URL
 - d. 在“国家/地区”中，选择您的企业所在的国家。
 - e. (可选) 选择“添加地址”，然后输入您的公司地址。

8. 选择下一步。

9. 在“选择 WhatsApp 企业账户”中，选择现有的 WhatsApp 企业账户 (WABA)，或者如果您需要创建账户，请选择创建 WhatsApp 企业账户。

在“创建或选择 WhatsApp 企业档案”中，选择现有的 WhatsApp 企业资料或创建新的 WhatsApp 企业档案。

10. 选择下一步。

11. 在“创建企业简介”中，输入以下信息：

- 对于 WhatsApp 企业账户名称，输入您的账户名称。此字段不面向客户。
- 在“WhatsApp 企业资料显示名称”中，输入客户收到您的消息时向他们显示的名称。建议您使用公司名称作为显示名称。该名称由 Meta 审核，必须符合[WhatsApp 显示名称规则](#)。要使用与公司名称不同的品牌名称，您的公司与品牌之间必须存在对外公布的关联。此关联必须显示在您的网站和显示名称网站所代表的品牌上。

完成注册后，Meta 会对您的显示名称进行审核。Meta 会向您发送一封电子邮件，告知您显示名称是已被批准还是被拒绝。如果您的显示名称被拒绝，则您的每日消息限制会降低，并且您可能会与之断开连接 WhatsApp。


 Important

要更改显示名称，您必须创建一个支持 Meta 的票证。

- 在“时区”中，选择企业所在的时区。
 - 在“类别”中，选择最适合您的业务的类别。买家可以在您的联系信息中查看您的类别。
 - 对于业务描述，输入对公司的描述。客户可以将您的业务描述作为联系信息的一部分进行查看。
 - 对于网站，请输入贵公司的网站。客户可以将您的网站作为联系信息的一部分进行查看。
 - 选择下一步。
12. 在“添加电话号码”中 WhatsApp，输入要注册的电话号码。当您向客户发送消息时，该电话号码会显示给他们。
13. 在“选择您想要如何验证您的号码”中，选择短信或电话。
- 准备好接收验证码后，选择“下一步”。
 - 输入验证码，然后选择“下一步”。
14. 您的号码通过验证后，您可以选择“下一步”从 Meta 关闭窗口。
15. 对于 WhatsApp 企业账户，展开标签-可选择向您的 WhatsApp 企业账户添加标签。

标签是一对键和值，您可以选择将其应用于 AWS 资源，以控制对于资源的访问或使用。选择添加新标签，然后输入要添加键值对。

16. WhatsApp 企业账户可以有一个消息和一个事件目的地，用于记录 WhatsApp 企业账户的事件以及与 WhatsApp 企业账户关联的所有资源。要在 Amazon SNS 中启用事件记录（包括接收客户消息的记录），您必须开启消息和事件发布。有关更多信息，请参阅 [AWS 最终用户消息社交中的消息和事件目的地](#)。

 Important

为了能够回复客户消息，您必须启用消息和事件发布。

在消息和活动目标详细信息部分，打开活动发布。对于亚马逊 SNS，选择新的亚马逊 SNS 标准主题并在主题名称中输入名称，或者选择现有亚马逊 SNS 标准主题并从主题 arn 下拉列表选择一个主题。

17. 在“电话号码”下：

对于电话号码下的每个 WhatsApp 电话号码：

- a. 要进行电话号码验证，请输入现有验证码 PIN 或输入新验证 PIN 码。要重置丢失或遗忘的 PIN，请按照 WhatsApp 商业平台云 API 参考 PIN 中的 [更新](#) 中的说明进行操作。
- b. 有关其他设置：
 - i. 对于数据本地化区域-可选，选择一个 Meta 区域来存储静态数据。有关 Meta 数据隐私政策的更多信息，请参阅 WhatsApp 商业平台云 API 参考中的 [数据隐私和安全](#) 以及云 API [本地存储](#)。
 - ii. 标签是一对键和值，您可以选择将其应用于 AWS 资源，以控制对于资源的访问或使用。选择添加新标签，然后输入要添加键值对。

18. WhatsApp 企业账户可以有一个消息和一个事件目的地，用于记录 WhatsApp 企业账户的事件以及与 WhatsApp 企业账户关联的所有资源。要在 Amazon SNS 中启用事件记录（包括接收客户消息的记录），您需要开启消息和事件发布。有关更多信息，请参阅 [AWS 最终用户消息社交中的消息和事件目的地](#)。

 Important

您必须启用消息和事件发布才能回复客户消息。

在消息和活动目标详细信息部分，打开活动发布。对于亚马逊SNS，选择新的亚马逊SNS标准主题并在主题名称中输入名称，或者选择现有亚马逊SNS标准主题并从主题 arn 下拉列表选择一个主题。

19. 要完成设置，请选择添加电话号码。

后续步骤

注册，您可以开始发送消息。当您准备开始大规模发送消息，请完成[企业验证](#)。现在，您的 WhatsApp 企业账户和 AWS 最终用户消息社交账户已关联，请参阅以下主题：

- 了解用于记录[事件和接收传入消息的事件目的地](#)。
- 学习如何创建[消息模板](#)。
- 了解如何[发送短信或媒体消息](#)。
- 了解如何[接收消息](#)。
- 了解[官方企业账户](#)，在显示名称旁边加上绿色复选标记，提高消息吞吐量。

WhatsApp AWS 最终用户消息社交中的企业账户 (WABA)

WhatsApp 企业账户 (WABA) 允许您的企业使用 WhatsApp 商业平台直接向客户发送消息。您的所有人WABAs都是您的[元业务组合](#)的一部分。WhatsApp 企业账户包含面向客户的资产，例如电话号码、模板和业务联系信息。A WABA 只能存在于一个中 AWS 区域。有关 WhatsApp 企业账户的更多信息，请参阅[WhatsApp商业平台云API参考中的企业账户](#)。

Important

使用 Meta/ WhatsApp

- 您对 WhatsApp 商业解决方案的使用需遵守商业[服务条款](#)、[WhatsApp 商业解决方案条款](#)、[WhatsApp WhatsApp 商业消息政策](#)、[消息传递指南](#)以及其中以引用方式纳入的所有其他条款、政策或指南（因为每项条款可能会不时更新）的条款和条件。WhatsApp
- Meta 或 WhatsApp 可能随时禁止您使用 WhatsApp 商业解决方案。
- 您必须使用 Meta 创建 WhatsApp 企业账户（“WABA”）和 WhatsApp。
- 您必须使用 Meta 创建商务经理账户并将其关联到您的WABA。
- 您必须向我们提供WABA对您的控制权。根据您的要求，我们将使用 Meta WABA 向我们提供的方法，以合理和及时的方式将您的控制权移交给您。
- 在使用 WhatsApp 商业解决方案时，您不得提交任何受适用法律和/或法规保护和/或限制发布的内容、信息或数据。
- WhatsApp可以在[wh https://developers.facebook.com/docs/ats](https://developers.facebook.com/docs/ats) app/pricing中找到使用 WhatsApp 商业解决方案的定价。

主题

- [在“AWS 最终用户消息”社交中查看 WhatsApp 企业账户 \(WABA\)](#)
- [在 AWS 最终用户消息社交中添加 WhatsApp 企业账户 \(WABA\)](#)
- [了解 WhatsApp 企业账户类型](#)

在“AWS 最终用户消息”社交中查看 WhatsApp 企业账户 (WABA)

按照以下说明查看与您WABA关联的 AWS 账户。

1. 打开 AWS 最终用户消息社交控制台，网址为<https://console.aws.amazon.com/social-messaging/>。
2. 在企业账户中，选择一个WABA。
3. 在“电话号码”选项卡上，查看您的电话号码、显示名称、质量评级以及您当天剩下的企业发起的对话数量。

在“活动目的地”选项卡上，查看您的活动目的地。要编辑您的活动目的地，请按照中的说明进行操作[AWS 最终用户消息社交中的消息和事件目的地](#)。

在“模板”选项卡上，选择“管理消息模板”，通过 Meta 编辑您的 WhatsApp 模板。每个模板 WABA上限为 250 个。

在标签选项卡上，您可以管理您的WABA资源标签。

在 AWS 最终用户消息社交中添加 WhatsApp 企业账户 (WABA)

如果您已经有 WhatsApp 企业简介，请WABA向您的账户添加一个新账户。作为创建新号码的一部分，WABA您必须将[电话号码](#)添加到WABA。

- 要WABA向您的账户添加新账号，请按以下步骤操作[AWS 终端用户消息社交入门](#)：
 - 在步骤 8 中，选择您的 WhatsApp 企业资料并选择创建新的 WhatsApp 企业账户。

了解 WhatsApp 企业账户类型

您的 WhatsApp 企业账户决定了您向客户展示的方式。创建 WhatsApp 账户时，您的账户将成为企业账户。WhatsApp 业务有两种业务类型：

- 企业账户：WhatsApp 验证 WhatsApp 商业平台上每个账户的真实性。如果企业账户已完成企业验证流程，则即使用户尚未将企业添加到地址簿中，也能看到该企业的名称。此功能可帮助用户识别经过验证的企业账户 WhatsApp。
- 官方企业账户：除了企业账户的好处外，官方企业账户的个人资料和聊天话题标题中还有一个绿色的勾号徽章。

批准 WhatsApp 官方企业账户 (OBA) 需要提供证据，证明该企业广为人知并得到消费者的认可，例如通过文章、博客文章或独立评论。即使企业提供了所需的文件，也不能保证获得批准。WhatsApp OBA审批流程须经审查和批准 WhatsApp。WhatsApp 没有公开披露他们用来评估和批准官方商业

账户申请的具体标准。寻求信誉和认可的企业 WhatsApp OBA 必须证明自己的声誉和认可，但最终批准由以下各方自行决定 WhatsApp。

创建 WhatsApp 账户时，您的账户将成为企业账户。您可以向客户提供有关您的业务的信息，例如网站、地址和营业时间。对于尚未完成企业验证的 WhatsApp 企业，显示名称仅以小文本形式显示在联系人视图中的电话号码旁边，而不会显示在聊天列表或个人聊天中。Meta Business 验证完成后，WhatsApp 发件人的显示名称将显示在聊天列表和各个聊天话题中。

其他资源

- 有关企业账户和官方企业账户的更多信息，请参阅 [Business Platform Cloud API 参考中的 WhatsApp 企业账户](#)。
- 有关企业验证流程的更多信息，请参阅 [WhatsApp 商业平台云API参考中的企业验证](#)。

AWS 最终用户消息社交中的电话号码

所有 WhatsApp 企业账户都包含一个或多个用于验证您身份的电话号码，WhatsApp 并用作发送身份的一部分。您可以将多个电话号码与 WhatsApp 企业账户 (WABA) 相关联，并将每个电话号码用于不同的品牌。

主题

- [使用 WhatsApp 企业账户的电话号码注意事项](#)
- [向 WhatsApp 企业账户添加电话号码 \(WABA\)](#)
- [查看电话号码的状态](#)
- [在“AWS 最终用户消息”社交中查看电话号码的 ID](#)
- [提高消息对话限制 WhatsApp](#)
- [提高消息吞吐量 WhatsApp](#)
- [了解中的电话号码质量评级 WhatsApp](#)

使用 WhatsApp 企业账户的电话号码注意事项

将电话号码与 WhatsApp 企业账户 (WABA) 关联时，应考虑以下几点：

- 一次只能将电话号码关联 WABA 到一个号码。
- 该电话号码仍可用于 SMS/MMS、和语音通话。
- 每个电话号码都有来自 Meta 的质量评级。

您可以通过执行以下操作通过“AWS 最终用户消息”获取 SMS 支持该功能 SMS 的电话号码：

1. 确保电话号码的[国家或地区](#)支持双向 SMS。
2. 索取[电话号码](#)。根据国家或地区的不同，您可能需要注册电话号码。
3. 为电话号码@@ [启用双向 SMS 消息](#)。设置完成后，您的传入 SMS 消息将发送到活动目的地。

向 WhatsApp 企业账户添加电话号码 (WABA)

您可以将电话号码添加到现有的 WhatsApp 企业账户 (WABA) 中，也可以 WABA 为该电话号码创建一个新的电话号码。

先决条件

在您开始之前，必须满足以下先决条件：

- 电话号码必须能够接收SMS或语音一次性密码 (OTP)。这是添加到您的电话号码WABA。
- 电话号码不得与电话号码关联WABA。

将电话号码添加到 WABA

在现有电话号码中添加新电话号码 WABA

1. 打开 AWS 最终用户消息社交控制台，网址为<https://console.aws.amazon.com/social-messaging/>。
2. 选择企业账户，然后选择添加 WhatsApp 电话号码。
3. 在添加 WhatsApp 电话号码页面上，选择启动 Facebook 门户。将会出现一个来自 Meta 的新登录窗口。
4. 在 Meta 登录窗口中，输入您的 Meta 开发者账户凭证并选择您的业务组合。
5. 选择您要向其添加电话号码的WABA和 WhatsApp 公司简介。
6. 选择下一步。
7. 在“添加电话号码”中 WhatsApp，输入要注册的电话号码。当您向客户发送消息时，该电话号码会显示给他们。
8. 在“选择您想要如何验证您的号码”中，选择短信或电话。
9. 准备好接收验证码后，选择“下一步”
10. 输入验证码，然后选择“下一步”。您的号码通过验证后，您可以选择“下一步”从 Meta 关闭窗口。
11. 在“WhatsApp 电话号码”下：
 - a. 要进行电话号码验证，请输入现有验证码PIN或输入新验证PIN码。要重置丢失或遗忘的PIN，请按照WhatsApp 商业平台云API参考PIN中的[更新](#)中的说明进行操作。
 - b. 有关其他设置：
 - i. 对于数据本地化区域-可选，选择一个用于存储静态数据的Meta区域。有关 Meta 数据隐私政策的更多信息，请参阅WhatsApp商业平台云API参考中的[数据隐私和安全](#)以及云API[本地存储](#)。
 - ii. 标签是一对键和值，您可以选择将其应用于 AWS 资源，以控制对于资源的访问或使用。选择添加新标签，然后输入要附加键值对。

- WhatsApp 企业账户可以有一个消息和一个事件目的地，用于记录 WhatsApp 企业账户的事件以及与 WhatsApp 企业账户关联的所有资源。要在 Amazon 中启用事件记录 SNS，包括记录接收客户消息，请打开“消息和事件发布”。有关更多信息，请参阅 [AWS 最终用户消息社交中的消息和事件目的地](#)。

 Important

您必须启用消息和事件发布才能回复客户消息。


在消息和活动目标详细信息部分，打开活动发布。对于亚马逊 SNS，选择新的亚马逊 SNS 标准主题并在主题名称中输入名称，或者选择现有亚马逊 SNS 标准主题并从主题 arn 下拉列表选择一个主题。

- 要完成设置，请选择添加电话号码。

查看电话号码的状态

为了能够在 AWS 最终用户消息社交中发送消息，电话号码的状态必须为“有效”。

- 打开 AWS 最终用户消息社交控制台，网址为 <https://console.aws.amazon.com/social-messaging/>。
- 选择 Phone numbers (电话号码)。
- 在“电话号码”部分，“状态”列显示每个电话号码的状态。

 Note

如果电话号码的状态设置为“未完成”，则可以选择该电话号码，然后选择“完成设置”以完成电话号码的设置。

在“AWS 最终用户消息”社交中查看电话号码的 ID

为了能够使用发送消息 AWS CLI，您需要使用电话号码 ID 来识别发送时要使用的电话号码。

- 打开 AWS 最终用户消息社交控制台，网址为 <https://console.aws.amazon.com/social-messaging/>。
- 选择 Phone numbers (电话号码)。

3. 在电话号码部分，选择所需电话号码。
4. 电话号码详细信息部分包含电话号码的电话号码 ID。

提高消息对话限制 WhatsApp

消息限制是指企业电话号码可在 24 小时周期内打开的对话的最大数量。公司电话号码最初仅限于 24 小时移动期内的 250 次企业发起的对话。Meta 可以根据消息的质量评级和发送的消息数量来提高此限制。企业发起的对话只能使用模板消息。

当客户给您发消息时，这会打开 24 小时服务窗口。在此期间，您可以发送所有[类型的消息](#)。

您可以按照以下准则自行将消息限制提高到 1,000 封邮件：

- 您的公司电话号码必须处于“[激活](#)”状态。
- 如果您的公司电话号码的[质量评级较低](#)，则在[质量评级](#)提高之前，它可能会继续限制为每天 250 次企业发起的对话。
- 申请[企业验证](#)。如果您的企业获得批准，将对报文传送质量进行分析，以确定您的报文传送活动是否值得提高您的报文传送限制。根据分析，您提出的提高消息限制的请求将被 Meta 批准或拒绝。
- 申请[身份验证](#)。如果您完成了身份验证并确认了您的身份，Meta 将批准提高消息限制。
- 使用具有高质量评级的模板在 30 天内打开 1,000 个或更多由企业发起的对话。一旦达到 1,000 个对话的阈值，将对您的消息传递质量进行分析，以确定您的消息传递活动是否值得提高您的消息传递限制。目标是始终如一地发送高质量的消息，从而有可能提高您的消息限制。

如果您完成了企业验证或身份验证，或者打开了 1,000 次或更多业务对话，但您仍然只能进行 250 次企业发起的对话，请向 Meta 提交消息级别升级请求。

如果您的企业或身份验证被拒绝，您可以通过发送高质量的消息来提高获得批准的机会。通过发送高质量、合规且可选择加入的消息，可能会重新评估您的消息传递活动和质量，从而有可能提高您批准的消息传递能力。

您的消息质量得分 WhatsApp 是根据最近的用户反馈和互动计算得出的，而较新的数据则更受重视。这有助于评估平台上消息传递的整体质量和可靠性。

消息限制级别提高

- 1K 由企业发起的对话
- 1 万次企业发起的对话

- 10 万次企业发起的对话
- 不限数量的企业发起的对话

提高消息吞吐量 WhatsApp

消息吞吐量是电话号码每秒传入和传出的消息数量 (MPS)。默认情况下，每个电话号码 MPS 的值为 80。如果您满足以下要求，Meta 可以增加 MPS 到 1,000：

- 该电话号码必须能够发送无限数量的[企业发起](#)的对话
- 电话号码的[质量等级](#)必须为中等或更高。

了解中的电话号码质量评级 WhatsApp

您的电话号码和消息的质量由 Meta 决定。您的消息质量得分基于客户在过去 7 天内收到您的消息的情况，而较新的消息的权重更高。消息质量分数是根据您和 WhatsApp 用户之间对话的质量信号组合计算得出的。这些信号包括用户反馈，例如屏蔽、报告以及用户在屏蔽企业时提供的原因。Meta 会根据客户对消息的接受程度来评估消息的质量 WhatsApp，重点是最近的反馈和互动。

WhatsApp 电话号码质量评级

- 绿色：高品质
- 黄色：中等品质
- 红色：低质量

WhatsApp 电话号码状态

- 已连接：您可以在消息限制范围内发送消息。
- 已标记：您的电话号码质量不佳，需要改进。如果您的电话质量在 7 天内没有改善，则您的电话号码状态将更改为“已连接”，但您的企业发起的对话限制会降低一级。
- 受限：在当前 24 小时内，您已达到企业发起的对话上限，但您仍然可以回复收到的客户消息。24 小时期限结束后，您可以再次发送消息。

查看电话号码质量评级

按照以下说明查看电话号码的质量。

1. 打开 AWS 最终用户消息社交控制台，网址为 <https://console.aws.amazon.com/social-messaging/>。
2. 在企业账户中，选择一个WABA。
3. 在“电话号码”选项卡上，查看您的电话号码、显示名称、质量评级以及您当天剩下的企业发起的对话数量。

在 AWS 最终用户消息社交中使用消息模板

您可以将消息模板用于经常使用的消息类型，例如每周时事通讯或预约提醒。模板消息是唯一可以发送给尚未向您发送消息或在过去 24 小时内未向您发送消息的客户发送的消息类型。

Meta 会为每个模板分配一个质量评级和状态。质量评级会影响模板的状态并降低模板的节奏或发送速率。

模板与您的 WhatsApp 企业账户 (WABA) 关联，通过 WhatsApp 经理进行管理，并由其审核 WhatsApp。

您可以发送以下模板类型：

- 基于文本
- 基于媒体
- 交互式
- 基于位置
- 带有一次性密码按钮的身份验证模板
- 多产品信息模板

Meta 提供了预先批准的示例模板。要了解更多信息，请参阅[示例消息模板](#)。

有关消息模板类型的更多信息，请参阅 WhatsApp 业务平台云 API 参考中的[消息模板](#)。

在 WhatsApp 管理器中使用消息模板

使用[WhatsApp 管理器](#)创建、修改或检查模板状态。

1. 打开 AWS 最终用户消息社交控制台，网址为<https://console.aws.amazon.com/social-messaging/>。
2. 选择企业账户，然后选择一个 WABA。
3. 在“消息模板”选项卡上，选择“管理消息模板”。[WhatsApp 管理器](#)将在新窗口中打开，您可以在其中选择“消息模板”来管理您的模板。

后续步骤

创建或编辑模板后，必须将其提交以供审阅 WhatsApp。Meta 审核可能需要长达 24 小时才能完成。Meta 会向您的 Business Manager 管理员发送一封电子邮件，并在 WhatsApp 管理器中更新模板状态。使用 [WhatsApp 管理器](#) 来检查模板的状态。

了解模板节奏 WhatsApp

模板调整是 Meta 使用的一种方法，它允许客户有时间对新模板或修改后的模板进行早期反馈。它会识别并暂停参与度不佳或反馈不佳的模板，让您在向太多客户发送模板内容之前有时间调整模板内容。这样可以降低负面客户反馈影响业务的风险。例如，如果太多客户“屏蔽”您的消息，或者您的模板的阅读率较低，则您的模板质量评级可能会降低。

模板调整会影响新创建的模板、未暂停的模板以及没有高质量评级的模板。模板节奏通常是由以前的低质量模板或暂停模板的历史记录开始的。当模板设置节奏时，使用该模板的消息通常会发送到由 Meta 确定的特定阈值。之后，将保留后续消息，以便有时间听取客户反馈。如果反馈是正面的，则模板节奏会被放大。如果反馈为负面，则模板节奏会降低，允许您调整模板内容。有关更多信息，请参阅《[WhatsApp 商业平台云API参考](#)》中的 [模板节奏](#)。

使用 WhatsApp 管理器获取有关模板已降低状态的反馈

Meta 提供有关模板状态降低的原因的信息。使用来自 Meta 的反馈来编辑模板并提交以供重新批准、使用其他模板或更改应用程序的行为。如果您编辑消息模板并重新获得批准，则只要它不经常收到负面反馈或低阅读率，其质量评级就会逐渐提高。

1. 打开 AWS 最终用户消息社交控制台，网址为 <https://console.aws.amazon.com/social-messaging/>。
2. 选择企业账户，然后选择一个 WABA。
3. 在“消息模板”选项卡上，选择“管理消息模板”。[WhatsApp 管理员](#) 将在新窗口中打开。
4. 选择消息模板，然后将鼠标悬停在模板上。应显示一个工具提示，其中包含有关评分降低原因的反馈。

了解模板的状态和质量评级 WhatsApp

根据使用情况、客户反馈和客户参与度，为每个消息模板分配质量评级。只有当模板的状态为“活动”时，才能使用模板，但质量决定了模板的节奏。如果消息模板持续收到负面反馈或参与度低，则会导致模板状态发生变化。

Meta 会根据负面或正面反馈和参与度自动更改模板的状态或质量评级。如果您的模板状态发生变化，您将收到 WhatsApp 经理通知、电子邮件和活动通知。使用 [WhatsApp 管理器](#) 来检查模板的状态。

如果您的模板被拒绝 WhatsApp，您可以编辑模板并重新提交以获得批准或向提出申诉。WhatsApp 要了解更多信息，请参阅 WhatsApp 商业平台云 API 参考中的 [申诉](#)。

模板状态	质量评级	含义
审核中		消息模板正在审核中。这可能最多需要 24 小时才能完成。
已拒绝		消息模板已被拒绝，您可以提出申诉。
处于活动状态	待处理	消息模板尚未收到来自客户的质量反馈或阅读费率信息，但该模板仍可用于发送消息。
处于活动状态	高	消息模板几乎没有收到任何负面的买家反馈，可以用来发送消息。
处于活动状态	中	消息模板收到了来自客户的负面反馈或低阅读率，因此可能已暂停或关闭。
处于活动状态	低	<p>消息模板收到了来自客户的负面反馈或低阅读率。可以使用具有此状态的消息模板，但可能会被暂停或禁用。</p> <p>当模板变为 Active-Low 状态时，其发送将暂停。第一次暂停是三个小时，第二次暂停是六个小时，下一次暂停会禁用模板。</p>
Paused		由于客户反复出现负面反馈或阅读率低，消息模板已暂停。

模板状态	质量评级	含义
已禁用		由于买家反复出现负面反馈，消息模板已被禁用。
已请求上诉		已请求上诉。

模板被拒绝的原因 WhatsApp

如果您的消息模板被 Meta 审核并拒绝，您将收到一封电子邮件，说明该模板被拒绝的原因。您可以对拒绝提出申诉或修改您的消息模板。以下是 Meta 可能拒绝消息模板的一些常见原因：

- 变量参数包含特殊字符，例如 #、\$ 或%。
- 变量参数缺失、花括号不匹配或不连续。
- 消息模板包含违反[WhatsApp 商务政策](#)或[WhatsApps 商业政策](#)的内容。

有关更多信息，请参阅《WhatsApp 商业平台云API参考》中的[常见拒绝原因](#)。

AWS 最终用户消息社交中的消息和事件目的地

事件目的地是向其发送 WhatsApp 事件的 Amazon SNS 主题。当您开启针对亚马逊 SNS 主题的事件发布功能时，您的所有发送和接收事件都将发送到该亚马逊 SNS 主题。使用事件监控、跟踪和分析出站消息和传入客户通信的状态。

每个 WhatsApp 企业账户 (WABA) 可以有一个活动目的地。与 WhatsApp 企业账户关联的所有资源中的所有事件都将记录到该事件目的地。例如，您可以拥有一个 WhatsApp 企业账户，其中包含三个与之关联的电话号码，并且这些电话号码中的所有事件都将记录到同一个活动目的地。

主题

- [向 AWS 最终用户消息社交添加消息和事件目的地](#)
- [AWS 最终用户消息社交中的消息和事件格式](#)
- [WhatsApp 消息状态](#)

向 AWS 最终用户消息社交添加消息和事件目的地

当您开启消息和事件发布功能后，您的 WhatsApp 企业账户 (WABA) 生成的所有事件都将发送到 Amazon SNS 主题。这包括与 WhatsApp 企业账户关联的每个电话号码的事件。WABA 您可以将一个 Amazon SNS 主题与之关联。

先决条件

在您开始之前，您满足以下先决条件。

- (可选) 要使用使用 AWS KMS 密钥加密的 Amazon SNS 主题，您必须向 AWS 最终用户消息社交授予[现有密钥策略](#)的权限。

添加消息和事件目的地

1. 打开 AWS 最终用户消息社交控制台，网址为<https://console.aws.amazon.com/social-messaging/>。
2. 选择企业账户，然后选择一个 WABA。
3. 在“活动目的地”选项卡上，选择“编辑目的地”。
4. 要打开活动目的地，请选择“启用”。

5. 要将您的活动发送到新的亚马逊SNS目的地，请选择新SNS展位主题，然后在“主题名称”中输入名称。创建 Amazon SNS 主题的权限允许 AWS 最终用户社交消息访问该主题。

要将您的活动发送到现有的亚马逊SNS目的地，请选择现有SNS标准主题，然后从 Topic arn 中选择一个主题。您必须将以下权限应用于 Amazon SNS 主题：

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

6. 选择 Save changes (保存更改)。

加密的 Amazon SNS 主题政策

您可以使用通过 AWS KMS 密钥加密的 Amazon SNS 主题来提高安全级别。如果您的应用程序处理私有或敏感数据，这种增强的安全性会有所帮助。有关使用 AWS KMS 加密 Amazon SNS 主题的更多信息，请参阅《Amazon Simple Notification Service 开发人员指南》中的实现服务[中的事件源与加密主题之间的兼容性](#)。

该示例语句使用可选但建议，SourceAccount以及SourceArn条件（可选但建议）来避免混淆副手问题，只有 AWS 最终用户消息 Social 拥有者账户拥有访问权限。有关混淆副手问题的更多信息，请参阅[IAM用户指南中的混淆副手问题](#)。

您使用的密钥必须是对称的。加密的 Amazon SNS 主题不支持非对称 AWS KMS 密钥。

必须修改密钥政策以允许 AWS 最终用户消息 Social 使用该密钥。按照《AWS Key Management Service 开发人员指南》中[更改密钥策略](#)中的说明向现有密钥策略添加以下权限：

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

```

后续步骤

在您设置的 Amazon SNS 主题后，您必须为终端节点订阅该主题。终端节点将开始接收发布到关联主题的消息。有关订阅主题的更多信息，请参阅 [《亚马逊SNS开发者指南》中的订阅亚马逊SNS主题](#)。

AWS 最终用户消息社交中的消息和事件格式

事件的JSON对象包含 AWS 事件标头和 WhatsApp JSON有效负载。有关JSON WhatsApp 通知负载和值的列表，请参阅WhatsApp 业务平台云[参考中的 Webhooks 通知负载](#)API参考和[消息状态](#)。

AWS 最终用户消息社交事件标题

事件的JSON对象包含 AWS 事件标题和 WhatsApp JSON。标题包含您的 WhatsApp 企业账户 (WABA) 和ARNs电话号码的 AWS 标识符。

```

{
  "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
}
```

在上述示例事件中：

- *1234567890abcde* 是来自 Meta 的 WABA ID。
- *abcde1234567890* 是来自 Meta 的电话号码 ID。
- *fb2594b8a7974770b128a409e2example* 是 WhatsApp 企业账户 (WABA) 的 ID。
- *976c72a700aac43eaf573ae050example* 是电话号码的 ID。

接收短信 WhatsApp JSON的示例

以下显示了来自的传入短信的事件记录 WhatsApp。JSON由生成 WhatsApp。有关字段及其含义的列表，请参阅WhatsApp 商业平台云[参考中的 Webhooks 通知负载](#)API参考。

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

接收媒体消息 WhatsApp JSON的示例

以下显示了传入媒体消息的事件记录。要检索媒体文件，请使用 `GetWhatsAppMessageMedia` API 命令。有关字段及其含义的列表，请参阅 [Webhooks 通知负载](#) 参考

```
{
//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":
"wapid.HBgLMTQyNTY50DgzMDIVAgASGCBDNzBDRjM5MDU20DEwMDkwREY40DBDRDE0RjVGRkexample",
        "timestamp": "1723506230",
        "type": "image",
        "image": {
          "mime_type": "image/jpeg",
          "sha256": "BTD0xlqSZ7102o+/upusiNSt1EZhA/urkvKf143Uqjk=",
          "id": "530339869524171"
        }
      }
    ]
  },
  "field": "messages"
}
]
}

```

WhatsApp 消息状态

在发送消息时，您会收到有关消息状态更新。您必须启用事件记录才能接收这些通知，请参阅[AWS 最终用户消息社交中的消息和事件目的地](#)。

消息状态

下表包含可能的消息状态。

状态名称	描述
已删除	客户删除了邮件，如果邮件已下载到您的服务器，您也应该将其删除。
已交付	消息已成功发送给客户。
failed	消息发送失败。
read	客户阅读了消息。只有当客户开启已读回执时，才会发送此状态。

状态名称	描述
已发送	消息已发送，但仍在传输中。
warning	该消息包含不可用或不存在的项。

其他资源

有关更多信息，请参阅《WhatsApp 商业平台云API参考》中的[消息状态](#)。

上传要与之一起发送的媒体文件 WhatsApp

当您发送或接收媒体文件时，必须将其存储在 Amazon S3 存储桶中。Amazon S3 存储桶必须与您的 WhatsApp 企业账户 (WABA) 位于 AWS 区域相同 AWS 账户 和中。这些说明说明了如何创建 Amazon S3 存储桶、上传文件以及如何将其构建URL到文件中。有关 Amazon S3 命令的更多信息，请参阅[通过使用高级别 \(s3 \) 命令AWSCLI](#)。有关配置的更多信息 AWS CLI，请参阅[AWS Command Line Interface 用户指南AWSCLI中的配置](#)和 [Amazon S3 用户指南](#)中的[创建存储桶](#)和[上传对象](#)。

您也可以为媒体文件创建[URL预签名](#)。使用预签名URL，您可以授予对对象的限时访问权限并上传它们，而无需另一方拥有 AWS 安全证书或权限。

要创建 Amazon S3 存储桶，请使用 `create-bucket` AWS CLI 命令。在命令行输入以下命令：

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

在上述命令中：

- Replace (替换) `us-east-1` 随之而 AWS 区域 来WABA的是你所处的。
- Replace (替换) `BucketName` 将新存储桶的名称替换为新存储桶的名称。

要将文件复制到 Amazon S3 存储桶，请使用 `cp` AWS CLI 命令。在命令行输入以下命令：

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

在上述命令中：

- Replace (替换) `SourceFilePathAndName` 包含要复制的文件的文件路径和名称。
- Replace (替换) `BucketName` 将存储桶的名称替换为存储桶的名称。
- Replace (替换) `FileName` 并附上要用于该文件的名称。

发送时要使用的网址是：

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

要创建[预签名 URL](#)，请替换 `user input placeholders` 将您自己的信息。

```
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
```

返回的URL将是：`https://amzn-s3-demo-bucket1.s3.af-south-1.amazonaws.com/mydoc.txt?{Headers}`

支持的媒体文件类型和大小 WhatsApp

发送或接收媒体消息时，必须支持文件类型，且文件大小必须低于最大文件大小。有关更多信息，请参阅《WhatsApp 商业平台云API参考》中的[支持的媒体类型](#)。

媒体文件类型

音频格式

音频类型	扩展程序	MIME类型	最大大小
AAC	.aac	audio/aud	16 MB
AMR	.amr	audio/amr	16 MB
MP3	.mp3	audio/mpeg	16 MB
MP4音频	.m4a	audio/m	16 MB
OGG音频	.ogg	audio/ogg	16 MB

文档格式

文档类型	扩展程序	MIME类型	最大大小
文本	.text	text/plain	100 MB
Microsoft Excel	.xls、.xlsx	application/vnd.ms-excel , application/vnd.openxmlformats-officedocument.sread	100 MB
Microsoft Word	.doc、.docx	application/msword , application/vnd.o	100 MB

文档类型	扩展程序	MIME类型	最大大小
		penxmlformats-officedocument.w	
微软 PowerPoint	.ppt、.pptx	application/vnd.ms-PowerPoint , application/vnd.openxmlformats-officedocument.	100 MB
PDF	.pdf	application/pdf	100 MB

映像格式

映像类型	扩展程序	MIME类型	最大大小
JPEG	.jpeg	image/jpeg	5MB
PNG	.png	image/png	5MB

贴纸格式

贴纸类型	扩展程序	MIME类型	最大大小
动画	.webp	image/webp	500 KB
静态贴纸	.webp	image/webp	100KB

视频格式

VIDEO 类型	扩展程序	MIME类型	最大大小
3 GPP	.3gp	视频/3gp	16 MB
MP4视频	.mp4	视频/mp4	16 MB

WhatsApp 消息类型

本主题列出了支持的消息类型及其用法说明。有关消息类型的列表，请参阅WhatsApp 商业平台云API参考中的[消息](#)。

消息类型	描述
文本	向您的客户发送短信或URL发送短信
媒体	发送音频、文档、图像、贴纸或视频文件。您也可以发送媒体文件的链接。
Reaction	发送表情符号作为对消息的反应，比如竖起大拇指
模板	发送模板消息
位置	发送位置
联系人	发送联系人卡片
交互式	发送交互式消息

其他资源

有关 WhatsApp 消息对象的列表，请参阅WhatsApp 业务平台云API参考中的[消息](#)。

WhatsApp 使用 AWS 最终用户消息社交发送消息

在发送消息之前，您必须完成设置，WABA并且您的用户必须选择加入才能接收来自您的消息，请参阅。[获取权限](#)

当用户向您发送消息时，一个名为客户服务窗口的 24 小时计时器会启动或刷新。只有在您和用户之间打开客户服务窗口时，才能将所有类型的消息（模板消息除外）发送给用户。只要用户选择接收来自你的消息，就可以随时向用户发送模板消息。

对于您发送或接收的每条消息，都会生成消息状态并将其发送到事件目的地。如果您的客户尚未注册活动 WhatsApp，则会生成消息状态为 fail。您必须打开[消息和事件目标](#)才能接收[消息状态](#)。

Important

使用 Meta/ WhatsApp

- 您对 WhatsApp 商业解决方案的使用必须遵守商业[服务条款](#)、[WhatsApp 商业解决方案条款](#)、[WhatsApp WhatsApp 商业消息政策](#)、[消息传递指南](#)以及其中以引用方式纳入的所有其他条款、政策或指南（因为每项条款可能会不时更新）的条款和条件。WhatsApp
- Meta 或 WhatsApp 可能随时禁止您使用 WhatsApp 商业解决方案。
- 在使用 WhatsApp 商业解决方案时，您不得提交任何受适用法律和/或法规保护和/或限制发布的内容、信息或数据。

主题

- [在“AWS 最终用户消息 Social”中发送模板消息的示例](#)
- [在 AWS 最终用户消息 Social 中发送媒体消息的示例](#)

在“AWS 最终用户消息 Social”中发送模板消息的示例

以下示例介绍了如何使用模板将[消息发送](#)到，将消息发送到 AWS CLI 有关配置的更多信息 AWS CLI，请参阅 [《AWS Command Line Interface 用户指南》AWS CLI 中的配置](#)。

```
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

```

在上述命令中，执行以下操作：

- Replace（替换） `{PHONE_NUMBER}` 提供您客户的电话号码。
- Replace（替换） `{ORIGINATION_PHONE_NUMBER_ID}` 用你的电话号码的 ID。

在 AWS 最终用户消息 Social 中发送媒体消息的示例

以下示例介绍了如何使用向客户发送媒体消息 AWS CLI。有关配置的更多信息 AWS CLI，请参阅 [《AWS Command Line Interface 用户指南》AWS CLI 中的配置](#)。有关受支持媒体文件类型的列表，请参阅 [支持的媒体文件类型和大小 WhatsApp](#)。

1. 将媒体文件上传到 Amazon S3 存储桶，请参阅 [上传要与之一起发送的媒体文件 WhatsApp](#)。
2. WhatsApp 使用 [post-whatsapp-message-media](#) 命令将媒体文件上传到。成功完成后，该命令将返回 `{MEDIA_ID}` 这是发送媒体消息所必需的。

```

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

```

在上述命令中，执行以下操作：

- Replace（替换） `{ORIGINATION_PHONE_NUMBER_ID}` 用你的电话号码的 ID。
- Replace（替换） `{BUCKET}` 将替换为 Amazon S3 存储桶的名称。
- Replace（替换） `{MEDIA_FILE}` 将媒体文件的名称替换为媒体文件的名称。

您也可以使用 `--source-s3-presigned-url` 代替，使用 [预签名网址](#) 进行上传。`--source-s3-file` 您必须在标题字段 `Content-Type` 中添加。如果同时使用两者，`InvalidParameterException` 则返回一个。

```

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

```

3. 使用 [send-whatsapp-message](#) 命令发送媒体消息。

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

在上述命令中，执行以下操作：

- Replace (替换) `{PHONE_NUMBER}` 提供您客户的电话号码。
 - Replace (替换) `{ORINATION_PHONE_NUMBER_ID}` 用你的电话号码的 ID。
 - Replace (替换) `{MEDIA_ID}` 将替换上一步返回的媒体 ID。
4. 当您不再需要媒体文件时，可 WhatsApp 使用 [delete-whatsapp-message-media](#) 命令将其从中删除。这只会从 WhatsApp 您的 Amazon S3 桶中删除媒体文件。

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

在上述命令中，执行以下操作：

- Replace (替换) `{ORINATION_PHONE_NUMBER_ID}` 用你的电话号码的 ID。
- Replace (替换) `{MEDIA_ID}` 使用媒体 ID。

在 AWS 最终用户消息社交中回复收到的消息

您必须先完成设置WABA和设置活动目的地，然后才能收到短信或媒体消息。当您收到传入消息时，事件将保存在事件目的地 Amazon SNS 主题中。您必须订阅 Amazon SNS 主题终端节点才能收到通知。

有关收到的媒体消息的事件示例，请参阅[接收媒体消息 WhatsApp JSON的示例](#)。有关配置的更多信息 AWS CLI，请参阅《[AWS Command Line Interface 用户指南](#)》[AWS CLI中的配置](#)。有关受支持媒体文件类型的列表，请参阅[支持的媒体文件类型和大小 WhatsApp](#)。

Important

要接收传入的消息，必须为启用[事件目的地WABA](#)，请参阅[向 AWS 最终用户消息社交添加消息和事件目的地](#)。

使用 AWS 最终用户消息社交将邮件状态更改为阅读的示例

您可以将[消息的状态设置为](#)，以便在最终用户屏幕上read向其显示两个蓝色的复选标记。

```
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
```

在上述命令中，执行以下操作：

- Replace (替换) `{ORIGINATION_PHONE_NUMBER_ID}` 用你的电话号码的 ID。
- Replace (替换) `{MESSAGE_ID}` 将替换为邮件的唯一标识符。在 Amazon SNS 主题的消息对象中使用该id字段的值。

在“AWS 最终用户消息 Social”中用回复消息的示例

你可以对消息添加回应，比如竖起大拇指。

```
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
```

在上述命令中，执行以下操作：

- Replace (替换) `{PHONE_NUMBER}` 将替换为客户的电话号码。
- Replace (替换) `{MESSAGE_ID}` 将替换为邮件的唯一标识符。在 Amazon SNS 主题的消息对象中使用该id字段的值。
- Replace (替换) `{ORIGINATION_PHONE_NUMBER_ID}` 用你的电话号码的 ID。

将媒体文件从下载 WhatsApp 到 Amazon S3

要检索媒体文件并将其保存到 Amazon S3 存储桶中，请使用[get-whatsapp-message-media](#)命令。

```
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
}
```

在上述命令中，执行以下操作：

- Replace (替换) `{BUCKET}` 将替换为 Amazon S3 桶的名称。
- Replace (替换) `{MEDIA_ID}` 使用接收到的事件中的 id 字段的值。有关传入媒体事件的示例，请参阅[接收媒体消息 WhatsApp JSON的示例](#)。
- Replace (替换) `{ORIGINATION_PHONE_NUMBER_ID}` 用你的电话号码的 ID。

要从 Amazon S3 存储桶中检索媒体，请使用以下命令：

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

在上述命令中，执行以下操作：

- Replace (替换) `{BUCKET}` 将替换为 Amazon S3 桶的名称。
- Replace (替换) `{MEDIA_ID}` 将 MEDIA_ID。

通过阅读和回复来回复消息的示例

在此示例中，您的客户 Diego 向您发送了一条消息，上面写着“嗨”，您用已读回执和挥手表情符号回复他。

先决条件

您必须设置活动目的地 Amazon SNS 主题并订阅其中一个主题终端节点，才能收到 Diego 已发送消息的通知。

正在回应

1. 收到来自 Diego 的消息后，会向该主题的主题终端节点发布一个事件。以下是该主题发布的代码片段。

Note

由于 Diego 发起了对话，因此不计入您的企业发起的对话。

```
{
  "MetaWabaIds": [
    {
      "wabaId": "1234567890abcde",
      "arn": "arn:aws:social-messaging:us-east-1:123456789012:waba/fb2594b8a7974770b128a409e2example"
    }
  ],
  "MetaPhoneNumberIds": [
    {
      "metaPhoneNumberId": "abcde1234567890",
      "arn": "arn:aws:social-messaging:us-east-1:123456789012:phone-number-id/976c72a700aac43eaf573ae050example"
    }
  ]
}
{
  "id": "365731266123456",
  "changes": [
    {
      "value": {
```

```

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

```

2. 要显示 Diego 您已收到消息，请将状态设置为 read。迭戈将在设备上的消息旁边看到两个蓝色的复选标记。

```

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

```

在上述命令中，执行以下操作：

- Replace (替换) `{ORIGINATION_PHONE_NUMBER_ID}` 上面写着 Diego 向其发送消息的电话号码 ID `phone-number-id-976c72a700aac43eaf573ae050example`。

- Replace (替换) `{MESSAGE_ID}` 带有邮件的 ID。这与收到的消息中的 id 值相同wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRE0RjVGRke

3. 你可以给 Diego 发一个手挥手的反应。

```
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
```

在上述命令中，执行以下操作：

- Replace (替换) `{PHONE_NUMBER}` 用迭戈的电话14255550150号码
- Replace (替换) `{MESSAGE_ID}` 带有邮件的 ID。这与收到的消息中的 id 值相同wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRE0RjVGRke
- Replace (替换) `{ORIGINATION_PHONE_NUMBER_ID}` 上面写着 Diego 向其发送消息的电话号码 ID phone-number-id-976c72a700aac43eaf573ae050example。

其他资源

- 启用[事件目标](#)以记录事件和接收传入消息。
- 有关 WhatsApp 消息对象的列表，请参阅WhatsApp 业务平台云API参考中的[消息](#)。

了解“AWS 最终用户消息”社交的 WhatsApp 账单和使用情况报告

AWS 最终用户消息社交频道生成一种使用类型，其中包含以下格式的五个字段：*Region code-MessagingType-ISO-FeeDescription-FeeType*。每个 WhatsApp 对话有两个可能的计费项目，分别是 WhatsAppConversationFee、和 AWS per MessageFee。

当您通过发送模板消息发起对话时，AWS 每MessageFee人需要支付一封 WhatsApp ConversationFee和一封的费用。这将打开一个 24 小时窗口，您从同一客户那里发送或接收的每条消息都按 AWS 每MessageFee封计费。

WhatsApp 对话类型和定价详情可在WhatsApp 商业平台开发者[指南的基于对话的定价](#)中找到。

下表显示使用情况类型中的字段的可能值和描述。有关 AWS 最终用户消息社交定价的更多信息，请参阅[AWS 最终用户消息收发定价](#)。

字段	Options	描述
<i>Region code</i>	<ul style="list-style-type: none"> • USE1— 美国东部 (弗吉尼亚北部) 区域 • USE2— 美国东部 (俄亥俄州) 区域 • USW1— 美国西部 (俄勒冈) 区域 • APS1— 亚太地区 (孟买) 区域 • APSE1— 亚太地区 (新加坡) 区域 • EUW1— 欧洲 (爱尔兰) 区域 • EUW2— 欧洲 (伦敦) 区域 	指示 WhatsApp 消息发出地或接收地的 AWS 区域 前缀。
<i>MessagingType</i>	WhatsApp	此字段标识发送的消息类型。
<i>ISO</i>	查看 支持的国家/地区	消息发送到的两位数字ISO的国家/地区代码。

字段	Options	描述
<i>FeeDescription</i>	ConversationFee , MessageFee	此字段指定 the WhatsApp ConversationFee 或 p AWS er MessageFee 。

字段	Options	描述
<i>FeeType</i>	Authentication , Marketing , Service, Utility, Standard	<p>此字段显示所使用的对话类型的类型，或者指定每封邮件费用的标准</p> <p>企业发起的ConversationFee 类别</p> <ul style="list-style-type: none"> • Marketing — 用于实现各种目标，从提高知名度到推动销售和重新定位客户。示例包括新产品、服务或功能公告、定向促销/优惠以及购物车放弃提醒。 • Utility— 用于跟进用户操作或请求。示例包括选择加入确认、订单/配送管理（例如配送更新）、账户更新或提醒（例如付款提醒）或反馈调查。 • Authentication — 用于使用一次性密码对用户进行身份验证，可能是在登录过程的多个步骤（例如帐户验证、帐户恢复和完整性质疑）。 • Service— 用于解决客户查询。 <p>用户发起的ConversationFee 类别</p> <ul style="list-style-type: none"> • Service— 用于解决客户查询。

字段	Options	描述
		MessageFee 类别 <ul style="list-style-type: none"> • Standard— 发送或接收每封邮件的费用。

当您通过发送模板消息发起对话时，您需要支付—ConversationFee和—MessageFee的费用。这将打开一个 24 小时窗口，您发送给同一客户的每封模板消息均按个人MessageFee计费。在 24 小时窗口内，模板消息的类型必须相同，否则会开始新的对话。

例如，如果您向客户发送营销模板消息，则需要为ConversationFee和MessageFee付费。

```
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
```

如果客户向您发送消息并且您回复，则您需要支付开启新Service对话和消息的费用。

```
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
```

示例 1：发送营销模板消息

例如，如果您向客户发送营销模板消息，则 AWS 每MessageFee人需要支付一封 WhatsApp ConversationFee和一封的费用。

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

示例 2：打开服务对话

当企业回复用户在企业发起的任何 24 小时活跃对话窗口之外的入站消息时，将收取服务对话费。在这种情况下，您需要为每封入站 WhatsApp ConversationFee和 AWS MessageFee出站邮件分别收费。

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 最终用户消息社交账单ISO代码和 WhatsApp 对话费用映射

国家/地区

两位数字ISO的国家/地区代码	国家/地区名称	WhatsApp 对话计费区域
AF	阿富汗	亚太区域
AX	福克兰群岛	其他
AL	阿尔巴尼亚	中欧和东欧其他地区
DZ	阿尔及利亚	非洲和中东
AS	美属萨摩亚	其他
AD	安道尔	其他
AO	安哥拉	非洲和中东
AI	安圭拉岛	其他
AQ	南极洲	其他
AG	安提瓜和巴布达	其他
AR	阿根廷	阿根廷
AM	亚美尼亚	中欧和东欧其他地区
AW	阿鲁巴岛	其他
AC	阿留申群岛	其他
AU	澳大利亚	亚太区域

两位数字ISO的国家/地区代码	国家/地区名称	WhatsApp 对话计费区域
AT	奥地利	西欧其他地区
AZ	阿塞拜疆	中欧和东欧其他地区
BS	巴哈马	其他
BH	巴林	中东标准时间
BD	孟加拉国	亚太区域
BB	巴巴多斯	其他
BY	白俄罗斯	中欧和东欧其他地区
BE	比利时	西欧其他地区
BZ	伯利兹	其他
BJ	贝宁	非洲和中东
BM	百慕大	其他
BT	不丹	其他
BO	玻利维亚	拉丁美洲其他地区
BQ	博内尔岛	其他
BA	波斯尼亚和黑塞哥维那	其他
BW	博茨瓦纳	非洲和中东
BV	布韦岛	其他
BR	巴西	巴西
IO	英属印度洋领地	其他
VG	英属维尔京群岛	其他

两位数字ISO的国家/地区代码	国家/地区名称	WhatsApp 对话计费区域
BN	文莱达鲁萨兰国	其他
BG	保加利亚	中欧和东欧其他地区
BF	BurkinaFaso	非洲和中东
BI	布隆迪	非洲和中东
KH	柬埔寨	亚太区域
CM	喀麦隆	非洲和中东
CA	加拿大	北美洲
CV	佛得角	其他
KY	开曼群岛	其他
CF	中非共和国	其他
TD	乍得	非洲和中东
CL	智利	智利
CN	中国	亚太区域
CX	圣诞岛	其他
CC	科科斯（基林）群岛	其他
CO	哥伦比亚	哥伦比亚
KM	科摩罗	其他
CG	刚果	其他
CD	刚果	非洲和中东
CK	库克群岛	其他

两位数字ISO的国家/地区代码	国家/地区名称	WhatsApp 对话计费区域
CR	哥斯达黎加	拉丁美洲其他地区
CI	科特迪瓦	非洲和中东
HR	克罗地亚	中欧和东欧其他地区
CW	库拉索	其他
CY	塞浦路斯	其他
CZ	捷克共和国	中欧和东欧其他地区
DK	丹麦	西欧其他地区
DJ	吉布提	其他
DM	多米尼加	其他
DO	多米尼加共和国	拉丁美洲其他地区
EC	厄瓜多尔	拉丁美洲其他地区
EG	埃及	埃及
SV	萨尔瓦多	拉丁美洲其他地区
GQ	赤道几内亚	其他
ER	厄立特里亚	非洲和中东
EE	爱沙尼亚	其他
ET	埃塞俄比亚	非洲和中东
FK	福克兰群岛	其他
FO	法罗群岛	其他
FJ	斐济	其他

两位数字ISO的国家/地区代码	国家/地区名称	WhatsApp 对话计费区域
FI	芬兰	西欧其他地区
FR	法国	法国
GF	法属圭亚那	其他
PF	法属玻里尼西亚	其他
TF	法属南部领地	其他
GA	加蓬	非洲和中东
GM	冈比亚	非洲和中东
GE	格鲁吉亚	中欧和东欧其他地区
DE	德国	德国
GH	加纳	非洲和中东
GI	直布罗陀	其他
GR	希腊	中欧和东欧其他地区
GL	格陵兰	其他
GD	格林纳达	其他
GP	瓜德罗普	其他
GU	关岛	其他
GT	危地马拉	拉丁美洲其他地区
GG	根西岛	其他
GN	几内亚	其他
GW	几内亚比绍	非洲和中东

两位数字ISO的国家/地区代码	国家/地区名称	WhatsApp 对话计费区域
GY	圭亚那	其他
HT	海地	拉丁美洲其他地区
HM	赫德和 McDonald 岛屿	其他
HN	洪都拉斯	拉丁美洲其他地区
HK	中国香港	亚太区域
HU	匈牙利	中欧和东欧其他地区
IS	冰岛	其他
IN	印度	印度
IN	东部标准时间	东部标准时间
ID	印度尼西亚	印度尼西亚
ID	印度尼西亚国际	印度尼西亚国际
IQ	伊拉克	中东标准时间
IE	爱尔兰	西欧其他地区
IM	马恩岛	其他
IL	以色列	以色列
IT	意大利	意大利
JM	牙买加	拉丁美洲其他地区
JP	日本	亚太区域
JE	泽西岛	其他
JO	约旦	中东标准时间

两位数字ISO的国家/地区代码	国家/地区名称	WhatsApp 对话计费区域
KZ	哈萨克	其他
KE	肯尼亚	非洲和中东
KI	基里巴斯	其他
XK	科索沃	其他
KW	科威特	中东标准时间
KG	吉尔吉斯斯坦	其他
LA	老挝语 PDR	亚太区域
LV	拉脱维亚	中欧和东欧其他地区
LB	黎巴嫩	中东标准时间
LS	莱索托	非洲和中东
LR	利比里亚	非洲和中东
LY	利比亚	非洲和中东
LI	列支敦士登	其他
LT	立陶宛	中欧和东欧其他地区
LU	卢森堡	其他
MO	澳门	其他
MK	马其顿	中欧和东欧其他地区
MG	马达加斯加	非洲和中东
MW	马拉维	非洲和中东
MY	马来西亚	马来西亚

两位数字ISO的国家/地区代码	国家/地区名称	WhatsApp 对话计费区域
MV	马尔代夫	其他
ML	Mali	非洲和中东
MT	马耳他	其他
MH	马绍尔群岛	其他
MQ	马提尼克	其他
MR	毛里塔尼亚	非洲和中东
MU	毛里求斯	其他
YT	马约特岛	其他
MX	墨西哥	墨西哥
FM	密克罗尼西亚	其他
MD	摩尔多瓦	中欧和东欧其他地区
MC	摩纳哥	其他
MN	蒙古	亚太区域
ME	黑山共和国	其他
MS	蒙特塞拉特岛	其他
MA	摩洛哥	非洲和中东
MZ	莫桑比克	非洲和中东
MM	缅甸	其他
NA	纳米比亚	非洲和中东
NR	瑙鲁	其他

两位数字ISO的国家/地区代码	国家/地区名称	WhatsApp 对话计费区域
NP	尼泊尔	亚太区域
NL	荷兰	荷兰
NC	新喀里多尼亚	其他
NZ	新西兰	亚太区域
NI	尼加拉瓜	拉丁美洲其他地区
NE	尼日尔	非洲和中东
NG	尼日利亚	尼日利亚
NU	纽埃岛	其他
NF	诺福克岛	其他
MP	北马里亚纳群岛	其他
NO	挪威	西欧其他地区
OM	阿曼	中东标准时间
PK	巴基斯坦	巴基斯坦
PW	帕劳群岛	其他
PS	巴基斯坦领土	其他
PA	巴拿马	拉丁美洲其他地区
PG	巴布亚新几内亚	亚太区域
PY	巴拉圭	拉丁美洲其他地区
PE	秘鲁	秘鲁
PH	菲律宾	亚太区域

两位数字ISO的国家/地区代码	国家/地区名称	WhatsApp 对话计费区域
PN	皮特凯恩	其他
PL	波兰	中欧和东欧其他地区
PT	葡萄牙	西欧其他地区
PR	波多黎各	拉丁美洲其他地区
QA	卡塔尔	中东标准时间
RE	留尼汪	其他
RO	罗马尼亚	中欧和东欧其他地区
RU	俄罗斯联邦	俄罗斯
RW	卢旺达	非洲和中东
SH	圣马丁	其他
KN	圣基茨和尼维斯	其他
LC	圣卢西亚岛	其他
PM	圣皮埃尔和密克隆群岛	其他
VC	圣文森特和格林纳丁斯	其他
BL	圣巴泰勒米	其他
MF	圣马丁	其他
WS	萨摩亚群岛	其他
SM	圣马力诺	其他
ST	圣多美与普林希比共和国	其他
SA	沙特阿拉伯	沙特阿拉伯

两位数字ISO的国家/地区代码	国家/地区名称	WhatsApp 对话计费区域
SN	塞内加尔	非洲和中东
RS	塞尔维亚	中欧和东欧其他地区
SC	塞舌尔	其他
SL	塞拉利昂	非洲和中东
SG	新加坡	亚太区域
SX	荷属圣马丁	其他
SK	斯洛伐克	中欧和东欧其他地区
SI	斯洛文尼亚	中欧和东欧其他地区
SB	所罗门群岛	其他
SO	索马里	非洲和中东
ZA	南非	南非
GS	南乔治亚岛和南桑威奇群岛	其他
KR	韩国	其他
SS	南苏丹	非洲和中东
ES	西班牙	西班牙
LK	斯里兰卡	亚太区域
SR	苏里南	其他
SJ	斯瓦尔巴群岛和扬马延岛	其他
SZ	斯威士兰	非洲和中东
SE	瑞典	西欧其他地区

两位数字ISO的国家/地区代码	国家/地区名称	WhatsApp 对话计费区域
CH	瑞士	西欧其他地区
TW	中国台湾	亚太区域
TJ	塔吉克斯坦	亚太区域
TZ	坦桑尼亚	非洲和中东
TH	泰国	亚太区域
TL	东帝汶	其他
TG	多哥	非洲和中东
TK	托克劳	其他
TO	汤加	其他
TT	特立尼达和多巴哥	其他
TA	Trist and a Cunha	其他
TN	突尼斯	非洲和中东
TR	土耳其	土耳其
TM	土库曼斯坦	亚太区域
TC	特克斯和凯科斯群岛	其他
TV	图瓦卢	其他
UG	乌干达	非洲和中东
UA	乌克兰	中欧和东欧其他地区
AE	阿拉伯联合酋长国	阿拉伯联合酋长国
GB	英国	英国

两位数字ISO的国家/地区代码	国家/地区名称	WhatsApp 对话计费区域
美国	美国	北美洲
UY	乌拉圭	拉丁美洲其他地区
UM	美国本土外小岛屿	其他
UZ	乌兹别克斯坦	亚太区域
VU	瓦努阿图	其他
VA	圣巴泰勒米	其他
VE	委内瑞拉	拉丁美洲其他地区
VN	越南	亚太区域
VI	福克兰群岛	其他
WF	瓦利斯和富图纳群岛	其他
EH	西撒哈拉	其他
YE	也门	中东标准时间
ZM	赞比亚	非洲和中东
ZW	津巴布韦	其他

监控 AWS 最终用户消息社交

监控是保持 Amazon Social 和您的其他 AWS 解决方案的可靠性、可用性和性能的重要环节。AWS 提供了以下监控工具来监控 Amazon Social、在出现错误时进行报告并在适当的时候自动执行操作：

- Amazon CloudWatch 实时监控您的 AWS 资源以及 AWS 上运行的应用程序。您可以收集和跟踪指标，创建自定义的控制平面，以及设置警报以在指定的指标达到您指定的阈值时通知您或采取措施。例如，您可以具有 Amazon EC2 实例的 CloudWatch 跟踪 CPU 使用率或其他指标并且在需要时自动启动新实例。有关更多信息，请参阅 [Amazon CloudWatch 用户指南](#)。
- Amazon CloudWatch Logs 使您能够监控、存储和访问来自 Amazon EC2 实例 CloudTrail、和其他来源的日志文件。CloudWatch 日志可以监控日志文件中的信息，并在达到特定阈值时通知您。您还可以在高持久性存储中检索您的日志数据。有关更多信息，请参阅 [Amazon CloudWatch Logs 用户指南](#)。
- AWS CloudTrail 捕获由您的账户或代表该 AWS 账户发出的 API 调用和相关事件，并将日志文件传输到您指定的 Amazon S3 存储桶。您可以标识哪些用户和账户调用了 AWS、从中发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅 [用户指南。AWS CloudTrail](#)

监控 AWS 最终用户消息通过 Amazon 进行社交 CloudWatch

您可以使用监控 Amazon Social 的 CloudWatch。Amazon Social 会收集原始数据并将其处理为易读且近乎实时的指标。这些统计数据会保存 15 个月，从而使您能够访问历史信息，并能够更好地了解您的 Web 应用程序或服务的执行情况。此外，可以设置用于监测特定阈值的警报，并在达到相应阈值时发送通知或执行操作。有关更多信息，请参阅 [Amazon CloudWatch 用户指南](#)。

对于 AWS 最终用户消息社交平台，您可能需要留意 WhatsAppMessageFeeCount，并在达到支出阈值时观看 WhatsAppConversationFeeCount 并触发警报。

以下各表列出了 Amazon Social 用户 Messaging Social 导出到 AWS/SocialMessaging 命名空间的指标和维度。

指标	单位	描述
WhatsAppConversationFeeCount	计数	会 WhatsApp 话费的计数

指标	单位	描述
WhatsAppMessageFeeCount	计数	WhatsApp 消息费用计数

维度	描述
MessageFeeType	有效的费用类型包括服务、营销、公用事业和身份验证
DestinationCountryCode	该国家/地区的两个字母的ISO代码
WhatsAppPhoneNumberArn	电话号码的边框

使用记录 AWS 最终用户消息社交API通话 AWS CloudTrail

AWS 已与集成，后者作为一项服务 [AWS CloudTrail](#)，提供 Sype Manager 中由用户、角色或服务所执行的操作的记录 AWS 服务。CloudTrail 将所有对 AWS 最终用户消息社交的API呼叫捕获为事件。捕获的调用包含来自 Ma AWS inframe Modernizati AWS on 控制台的调API用。借助通过 CloudTrail 收集的信息 CloudTrail，您可以确定向 CloudFrong 发出的请求、发出请求的 IP 地址、请求的发出时间以及其他详细信息。AWS

每个事件或日记账条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根用户凭证还是用户凭证发出的。
- 请求是否代表 IAM Ident IAM ity Center 用户发出。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

CloudTrail 查看 CloudTra AWS 账户 il CloudTrail 事件历史记录提供对中过去 90 天的已记录管理事件。CloudTrail 事件历史记录提供对中过去 90 天的已记录管理事件的可查看、可下载和不可变记录。AWS 区域有关更多信息，请参阅《AWS CloudTrail 用户指南》中的“[使用 CloudTrail 事件历史记录](#)”。查看事件历史记录不会 CloudTrail收取 CloudTra il 费用。

要持续记录您的 AWS 账户 过去 90 天的事件，请创建跟踪或 CloudTrail [CloudTrailLake](#) 事件数据存储。

CloudTrail 步道

通过跟踪，CloudTrail 可将日志文件传送 CloudTrail 至 Amazon S3 存储桶。使用创建的所有跟踪均 AWS Management Console 具有多区域属性。您可以通过使用 AWS CLI 创建单区域或多区域跟踪。建议创建多区域跟踪，因为您可记录您账户 AWS 区域中的所有的活动。如果您创建单区域跟踪，则只能查看跟踪的 AWS 区域中记录的事件。有关跟踪的更多信息，请参阅《AWS CloudTrail 用户指南》中的[为您的 AWS 账户创建跟踪](#)和[为组织创建跟踪](#)。

通过创建跟踪，您可以从 CloudTrail CloudTrail 免费向您的 Amazon S3 存储桶传送一份正在进行的管理事件的副本，但会收取 Amazon S3 存储费用。有关 CloudTrail 定价的更多信息，请参阅[AWS CloudTrail 定价](#)。有关 Amazon S3 定价的信息，请参阅[Amazon S3 定价](#)。

CloudTrail Lake 事件数据存储

CloudTrail Lake 允许您对事件运行 SQL 基于 SQL 的查询。CloudTrail CloudTrail 将基于行的 JSON 格式的现有事件转换为 [Apache ORC](#) ORC 是一种针对快速检索数据进行优化的列式存储格式。事件将被聚合到事件数据存储中，它是基于您通过应用[高级事件选择器](#)选择的条件的不可变的事件集合。应用于事件数据存储的选择器用于控制哪些事件持续存在并可供您查询。有关 CloudTrail Lake 的更多信息，请参阅《AWS CloudTrail 用户指南》中的“[使用 AWS CloudTrail Lake](#)”。

CloudTrail Lake 事件数据存储和查询会产生费用。创建事件数据存储时，您可以选择要用于事件数据存储的[定价选项](#)。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。有关 CloudTrail 定价的更多信息，请参阅[AWS CloudTrail 定价](#)。

AWS 最终用户消息中的社交数据事件 CloudTrail

[数据事件](#)可提供对资源或在资源中所执行资源操作（例如，读取或写入 Amazon S3 对象）的相关信息。这些也称为数据层面操作。数据事件通常是高容量活动。默认情况下，CloudTrail CloudTrail 不记录数据事件。CloudTrail 事件历史记录不记录数据事件。

记录数据事件将收取额外费用。有关 CloudTrail 定价的更多信息，请参阅[AWS CloudTrail 定价](#)。

您可以使用 CloudTrail 控制台、AWS CLI 或 CloudTrail API 操作记录 AWS 最终用户消息社交资源类型的数据事件。有关如何记录数据事件的更多信息，请参阅《AWS CloudTrail 用户指南》中的[使用 AWS Management Console 记录数据事件](#)和[使用 AWS Command Line Interface 记录数据事件](#)。

下表列出了您可以为其 AWS 记录数据事件的 Amazon Systems Manager 资源类型。数据事件类型（控制台）列显示可从 CloudTrail CloudTrail 控制台上的数据事件类型列表中选择。resources.type 值列显示了您在使用或 CloudTrail API 配置高级事件选择器时需要指定

的 `resources.type` 值。AWS CLI CloudTrail APIs“APIs已记录到的数据 CloudTrail”列显示该资源类型的已记录到 CloudTrail 的API呼叫。

数据事件类型 (控制台)	resources.type 值	数据APIs已记录到 CloudTrail
社交消息电话号码 ID	AWS::SocialMessaging::PhoneNumberId	<ul style="list-style-type: none"> • DeleteWhatsAppMessageMedia • GetWhatsAppMessageMedia • PostWhatsAppMessageMedia • SendWhatsAppMessage

您可以将高级事件选择器配置为在 `eventName`、`readOnly` 和 `resources.ARN` 字段上进行筛选，从而仅记录那些对您很重要的事件。有关这些准则的更多信息，请参阅 [AdvancedFieldSelector](#) 在 AWS CloudTrail API 参考资料中。

AWS 最终用户消息中的社交管理事件 CloudTrail

[管理事件](#) 提供对您账户内的资源所执行管理操作的相关信息 AWS 账户。这些也称为控制层面操作。默认情况下，跟踪 CloudTrail 记录会记录管理事件。

AWS Amazon S3 AWS 将所有控制面板操作记录为管理事件。有关最终用户消息社交记录 AWS 的最终用户消息社交控制平面操作的列表 CloudTrail，请参阅 [《AWS 最终用户消息社交API参考》](#)。AWS

AWS 最终用户消息社交活动示例

一个事件表示一个来自任何源的请求，包括有关所请求API的 API 操作、请求参数等方面的信息。CloudTrail CloudTrail 日志文件不是公API用 API 调用的有序堆栈跟踪，因此条目不会按任何特定顺序显示。

下面的示例显示了一个 CloudTrail 日志条目，该条目说明了操作。

```
{
  "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": "GR632462JDSBEXAMPLE",
        "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"
}
}
```

有关 CloudTrail 录音内容的信息，请参阅《AWS CloudTrail 用户指南》中的[CloudTrail 录制内容](#)。

AWS 最终用户消息社交的最佳实践

本部分介绍可帮助您提升客户参与度并避免账户被冻结的几种最佳实践。但请注意，本节不包含法律建议。务必咨询律师来获取法律建议。

有关 WhatsApp 最佳实践的最新列表，请参阅[WhatsApp 企业消息政策](#)。

主题

- [Up-to-date 业务概况](#)
- [获取权限](#)
- [禁止的消息内容](#)
- [审核客户列表](#)
- [基于参与度调整您的发送](#)
- [在适当时间发送](#)

Up-to-date 业务概况

维护准确的 up-to-date WhatsApp 企业档案，包括客户支持联系信息，例如电子邮件地址、网站地址或电话号码。确保所提供的信息是真实的，不会歪曲或冒充其他企业。

获取权限

在您计划发送特定类型的消息时，切勿向未明确要求接收此类消息的收件人发送消息。使用以下资源来帮助实现合规性：

- 选择加入流程必须明确告知该人他们同意接收来自贵公司的消息或电话。WhatsApp 您必须明确说明您的公司名称。
- 您全权负责确定获得选择性同意的的方法。确保选择加入流程符合所有适用于您的通信的适用法律。提供所有必需的通知，并根据相关法律获得所有必要的许可。

有关 WhatsApp 选择加入要求的更多信息，请参阅“[获取选择加入](#)” WhatsApp

如果收件人可以使用在线表格进行注册以接收您的消息，请防范自动化脚本在人员不知道的情况下进行订阅。此外，还限制用户在单个会话中可以提交某个电话号码的次数。

尊重某人提出的封锁、停止或以其他方式退出通信的所有请求，包括将该人从您的联系人列表中删除，无论是开启还是关闭 WhatsApp。

维护包含每个选择加入请求和确认的日期、时间和来源的记录。这也可以帮助您对客户名单进行例行审计。

禁止的消息内容

Important

使用 Meta/ WhatsApp

- 您对 WhatsApp 商业解决方案的使用必须遵守商业[服务条款](#)、[WhatsApp 商业解决方案条款](#)、[WhatsApp 商业消息政策](#)、[消息传递指南](#)以及其中以引用方式纳入的所有其他条款、政策或指南（因为每项条款可能会不时更新）的条款和条件。WhatsApp
- Meta 或 WhatsApp 可能随时禁止您使用 WhatsApp 商业解决方案。
- 在使用 WhatsApp 商业解决方案时，您不得提交任何受适用法律或法规保护或限制发布的内容、信息或数据。

如果您违反该 WhatsApp 政策，您的帐户可能会在一段时间内被禁止发送消息，在您提出申诉之前被锁定，或者被永久封锁。如果您的任何账户或资产违反了政策，Meta 将通过电子邮件和 WhatsApp 业务经理通知您。所有上诉都必须向 Meta 提出。要查看违反政策的行为或向 Meta 提出申诉，请参阅在 Meta Business 帮助中心查看您的 WhatsApp 企业[账户的政策违规详情](#)。有关最新的禁止邮件内容列表，请参阅[WhatsApp 企业消息政策](#)。

以下是全球所有消息类型的禁止内容类别。将 TFN 用作源时 WhatsApp，请遵循以下指南：

类别	示例
赌博	<ul style="list-style-type: none"> • 赌场 • 抽奖活动 • 应用程序/网站
高风险金融服务	<ul style="list-style-type: none"> • 发薪日贷款 • 短期高息贷款

类别	示例
	<ul style="list-style-type: none"> • 汽车贷款 • 按揭贷款 • 学生贷款 • 收债 • 股市提醒 • 加密货币
债务豁免	<ul style="list-style-type: none"> • 债务重整 • 债务减免 • 信用修复计划
Get-rich-quick 计划	<ul style="list-style-type: none"> • Work-from-home 节目 • 风险投资机会 • 金字塔或多层次营销计划
非法物质	<ul style="list-style-type: none"> • 大麻/大麻素 CBD
网络钓鱼/SMishing	<ul style="list-style-type: none"> • 试图让用户透露个人信息或网站登录信息。
S.H.A.F.T。	<ul style="list-style-type: none"> • 性 • 仇恨 • 酒精 • 枪支 • 烟草/电子烟
第三方潜在客户开发	<ul style="list-style-type: none"> • 购买、出售或共享消费者信息的公司

审核客户列表

如果您要发送周期性 WhatsApp 消息，请定期审核您的客户列表。审核您的客户列表有助于确保只有想要接收消息的客户才是想要接收消息的客户。

审核您的列表时，向每个选择加入的客户发送提醒他们已订阅的消息，并为他们提供有关取消订阅的信息。

基于参与度调整您的发送

您客户的优先级可能随着时间推移而发生变化。如果客户发现您的消息不再有用，则他们可能会选择完全不再使用您的消息，或者甚至将您的消息报告为未经请求的消息。出于这些原因，您必须基于客户参与度调整您的发送活动。

对于与您的消息互动很少的客户，您应调整相应的消息发送频率。例如，如果向参与的客户每周发送消息，您可以为参与度较低的客户创建单独的每月摘要文件。

最后，从您的客户列表中删除完全未参与的客户。此步骤可防止客户对您的消息感到沮丧。这还可为您节省资金并且帮助保护您作为发件人的声誉。

在适当时间发送

仅在每个收件人所在时区的正常白天工作时间发送消息。如果您在晚餐时间或午夜发送消息，则很可能导致您的客户退订您的消息以免被打扰。您可能需要避免在您的客户无法立即响应 WhatsApp 消息时进行发送操作。

AWS 最终用户消息社交中的安全性

的云安全 AWS 性的优先级最高。为了满足对 AWS 安全性最敏感的组织的需求，我们打造了具有超高安全性的数据中心和网络架构。

安全性是 AWS 和您的共同责任。[责任共担模式](#)将其描述为云的安全性和云中的安全性：

- 云的安全性 — AWS 负责保护在中运行 AWS 服务的基础设施 AWS Cloud。AWS Amazon Services 还为您提供可以安心使用的服务。第三方审计人员定期测试和验证我们的安全性的有效性，作为 Compliance Programs Comp [AWS li](#) ance P r pli 要了解适用于 AWS 最终用户消息社交的合规性计划，请参阅合规性计划范围内的[AWS 服务合规性计划范围内的服务](#)范围内的服务。
- 云中的安全性 — 您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

此文档帮助您了解如何在使用 AWS 最终用户消息社交时应用责任共担模式。以下主题说明如何配置 AWS 最终用户消息社交以实现您的安全性和合规性目标。您还会了解如何使用其他 AWS 服务来帮助您监控和保护您的 AWS 最终用户消息社交资源。

主题

- [AWS 最终用户消息社交中的数据保护](#)
- [适用于 AppFabri AWS c 的身份和访问管理](#)
- [AWS 最终用户消息社交的合规性验证](#)
- [AWS 最终用户消息社交中的弹性](#)
- [AWS 最终用户消息社交中的基础设施安全](#)
- [防止跨服务混淆代理](#)
- [安全最佳实操](#)
- [为 Classic AWS 创建服务相关角色](#)

AWS 最终用户消息社交中的数据保护

分 AWS [担责任模型](#)适用于 AWS 最终用户消息社交中的数据保护。如该模式中所述 AWS ，负责保护运行所有的全球基础设施 AWS Cloud。您负责维护对托管在此基础架构上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅[数据隐私FAQ](#)。有关欧洲数据保护的信息，请参阅[责任AWS 共担模型和AWS安全GDPR](#)博客上的博客文章。

出于数据保护目的，我们建议您保护 AWS 账户凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置单个用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用 Multi MFA c。
- 使用SSL/TLS与 AWS 资源通信。我们要求TLS使用 TLS TLS 1.3。
- 使用设置 AP API I 和用户活动日志记录 AWS CloudTrail。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的[使用跟 CloudTrail 踪](#)。
- 使用 AWS 加密解决方案以及中的所有默认安全控制 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果在 AWS 通过命令行界面或访问时需要经过 FIPS 140-3 验证的加密模块API，请使用终端节点。FIPS有关可用FIPS终端节点的更多信息，请参阅[美国联邦信息处理标准 \(FIPS\) 第 140-3 版](#)。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您 AWS 服务使用控制台、、或处理 AWS 最终用户消息API AWS CLI、社交或其他内容时 AWS SDKs。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。当您URL向外部服务器提供 a 时，强烈建议您不要在中包含凭证信息URL来验证您对该服务器的请求。

Important

WhatsApp 使用信号协议进行安全通信。但是，由于 AWS 最终用户消息社交是第三方，因此 WhatsApp 不认为这些消息 end-to-end 已加密。有关 WhatsApp 数据保护的更多信息，请参阅[数据隐私和安全](#)以及[WhatsApp 加密概述](#)白皮书。

数据加密

AWS 最终用户消息社交数据在传输中和 AWS 边界内静态时均加密。当您向 AWS 最终用户消息社交提交数据时，它会在接收和存储时加密数据。当您从 AWS 最终用户消息社交中检索数据时，它会使用当前的安全协议将数据传输给您。

静态加密

AWS 最终用户消息社交会加密其在 AWS 边界内为您存储的所有数据。这包括配置数据、注册数据以及您添加到 AWS 最终用户消息社交中的任何数据。为加密数据，AWS 最终用户消息社交使用内部

AWS Key Management Service (AWS KMS) 密钥，这是一种由该服务代表您拥有和维护的密钥。有关 AWS KMS 的更多信息，请参阅 [AWS Key Management Service 开发人员指南](#)。

传输中加密

AWS 最终用户消息社交使用 HTTPS 和传输层安全性协议 (TLS) 1.2 与您的客户端、应用程序和元数据进行通信。为了与其他 AWS 服务进行通信，AWS 最终用户消息社交使用 HTTPS 和 TLS 1.2。此外，当您使用控制台创建和管理 AWS SMS 资源时 AWS SDK AWS Command Line Interface，所有通信都使用 HTTPS 和 TLS 1.2 进行保护。

密钥管理

为加密数据，AWS 最终用户消息社交使用内部 AWS KMS 密钥，这是一种由该服务代表您拥有和维护的密钥。我们会定期轮换这些密钥。您不能配置和使用自己的 AWS KMS 或其他密钥来加密存储在 AWS 最终用户消息社交中的数据。

互连网络流量隐私

互连网络流量隐私保护是指保护《AWS 最终用户消息传递 Social》与您的本地客户端和应用程序之间，以及 AWS 最终用户消息社交网络与同一 AWS 区域中的其他 AWS 资源之间的连接和流量。以下功能和实践可以帮助您保护 AWS 最终用户消息社交的互连网络流量隐私保护。

AWS SMS 与本地客户端和应用程序之间的流量

要在 AWS 最终用户消息社交与您的本地网络上的客户端和应用程序之间建立私有连接，您可以使用 AWS Direct Connect。这使您能够使用标准的光纤以太网电缆将您的网络链接到一个 AWS Direct Connect 位置。电缆的一端连接您的路由器，另一端连接 AWS Direct Connect 路由器。有关更多信息，请参阅 AWS Direct Connect 《用户指南》中的 [什么是 AWS Direct Connect?](#)。

为了有助于通过已发布的安全地访问 AWS 最终用户消息社交 APIs 网站，我们建议您遵守有关 API 呼叫 AWS 的最终用户消息社交的要求。AWS 最终用户消息社交要求客户端使用传输层安全性 (TLS) 1.2 或更高版本。客户端还必须支持具有完全向前保密 () 的密码套件，例如 Ephemeral Diffie-Hellman (PFS) 或 Elliptic Curve Diffie-Hellman ()。DHE ECDHE 大多数现代系统 (如 Java 7 及更高版本) 都支持这些模式。

此外，必须使用访问密钥 ID 和与您的 AWS 账户的 AWS Identity and Access Management (IAM) 主体关联的秘密访问密钥来对请求进行签名。或者，您可以使用 [AWS Security Token Service \(AWS STS\)](#) 生成临时安全凭证来签名请求。

适用于 AppFabri AWS c 的身份和访问管理

AWS Identity and Access Management (IAM) AWS 服务 可以帮助管理员安全地控制对 AWS 资源的访问权限。IAM管理员控制谁可以通过身份认证 (登录) 并获得使用 AWS 最终用户消息社交资源的授权 (具有权限)。IAMIA AWS 服务 M 是一项无需额外费用即可使用的。

主题

- [受众](#)
- [使用身份进行身份验证](#)
- [使用策略管理访问](#)
- [AWS 最终用户消息社交是如何与之配合使用的 IAM](#)
- [适用于 Gli AWS ent VPN 的基于身份的策略示例](#)
- [AWSAWS 最终用户消息社交的托管策略](#)
- [AWS 最终用户消息疑难解答社交身份和访问权限](#)

受众

使用 AWS Identity and Access Management (IAM) 的方式因您可以在 AWS 最终用户消息社交中执行的操作而异。

服务用户 — 如果使用 AWS 最终用户消息社交服务完成任务，则您的管理员会为您提供所需的凭证和权限。当您使用更多 AWS 最终用户消息社交功能来完成工作时，则可能需要额外权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 AWS 最终用户消息社交中的特征，请参阅[AWS 最终用户消息疑难解答社交身份和访问权限](#)。

服务管理员 — 如果您在公司负责管理 AWS 最终用户消息社交资源，则您可能具有 AWS 最终用户消息社交的完全访问权限。您有责任确定您的服务用户应访问哪些 AWS 最终用户消息社交功能和资源。然后，您必须向IAM管理员提交请求，这样才能更改您的服务用户的权限。检查此页上的信息，了解的基本概念IAM。要了解有关您的公司如何IAM与 AWS 最终用户消息社交搭配使用的更多信息，请参阅[AWS 最终用户消息社交是如何与之配合使用的 IAM](#)。

IAM管理员-如果您是IAM管理员，您可能希望了解有关如何编写策略以管理对 AWS 最终用户消息社交网站的访问权限的详细信息。要查看您可在中使用 AWS 的最终用户消息社交身份策略示例IAM，请参阅。[适用于 Gli AWS ent VPN 的基于身份的策略示例](#)

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方法。您必须以 AWS 账户根用户、IAM 用户身份或通过担任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭证以 AWS 联合身份登录到。AWS IAM Identity Center（IAM Identity Center）用户、您的单点登录身份验证以及您的 Google 或 Facebook 凭证都是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当您使用联合身份 AWS 验证访问时，您就是在间接代入角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》[中的如何登录到您 AWS 账户的](#)。

如果您 AWS 以编程方式访问，则将 AWS 提供软件开发工具包（SDK）和命令行界面（CLI），以便使用您的凭证对您的请求进行加密签名。如果您不使用 AWS 工具，则必须自行对请求签名。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》[中的签署 AWS API 请求](#)。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如，AWS 建议您使用多重验证（MFA）来提高账户的安全性。要了解更多信息，请参阅用户指南中的[多重身份验证](#)和 AWS IAM Identity Center 用户指南 AWS [中的使用多因素身份验证 \(MFA\)](#)。IAM

AWS 账户 root 用户

在创建时 AWS 账户，最初使用的是一个对账户中所有 AWS 服务和资源拥有完全访问权限的登录身份。此身份称为 AWS 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《用户指南》中的[需要根用户凭证的 IAM 任务](#)。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）结合使用联合身份验证和身份提供程序，以使用临时凭证 AWS 服务来访问。

联合身份是来自企业用户目录、Web 身份提供程序、Identity Center 目录的用户，或任何使用 AWS 服务通过身份源提供的凭证来访问的用户。AWS Directory Service 当联合身份访问时 AWS 账户，他们代入角色，而角色提供临时凭证。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 Identity Center 中创建用户和组，也可以连接并同步到您自己的身份源中的一组用户和组，以跨所有 AWS 账户和应用程序

使用。有关IAM身份中心的信息，请参阅[什么是IAM身份中心？](#)在《AWS IAM Identity Center 用户指南》中。

IAM 用户和组

[IAM用户](#)是您内部 AWS 账户对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的IAM用户。但是，如果您有一些特定的使用案例需要长期凭证以及IAM，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM用户指南》中的[对于需要长期凭证的使用场景定期轮换访问密钥](#)。

[IAM群组](#)是指定IAM用户集合的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您有一个名为的组IAMAdmins并为该组授予管理IAM资源的权限。

用户与角色不同。用户唯一地与某个人或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《[IAM用户指南](#)》中的[何时创建IAM用户（而不是角色）](#)。

IAM角色

[IAM角色](#)是您内部具有特定权限 AWS 账户的身份。它类似于IAM用户，但未与特定人员关联。您可以通过[切换IAM角色，在中暂 AWS Management Console 时代入角色](#)。您可以通过调用 AWS CLI 或 AWS API操作或使用自定义操作来代入角色URL。有关使用角色的方法的更多信息，请参阅《IAM用户指南》中的[代入角色的方法](#)。

IAM具有临时凭证的角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《IAM用户指南》中的[为第三方身份提供商创建角色](#)。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 会将权限集与中的IAM角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的[权限集](#)。
- 临时IAM用户权限 — IAM 用户或角色可代入IAM角色，以暂时获得针对特定任务的不同权限。
- 跨账户访问 — 您可以使用IAM角色允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅《IAM用户指南》[IAM中的跨账户资源访问](#)。

- 跨服务访问 — 某些 AWS 服务 使用其它 AWS 服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon 中运行应用程序 EC2 或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
- 转发访问会话：当您使用 IAM 用户或角色在中执行操作时 AWS，您将被视为主体。FAS 使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用主体调用的权限 AWS 服务，结合请求的，AWS 服务 向下游服务发出请求。FAS 只有在服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详细信息，请参阅 [转发访问会话](#)。
- 服务角色 — 服务 [IAM 角色](#) 是服务代表您在您的账户中执行操作而担任的角色。IAM 管理员可以从创建、修改和删除服务角色 IAM。有关更多信息，请参阅《IAM 用户指南》AWS 服务中的 [创建角色以向委派权限](#)。
- 服务相关角色 — 服务相关角色是与关联的一种服务角色。AWS 服务服务可以代入代表您执行操作的角色。服务相关角色显示在您的中 AWS 账户，并归该服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon 上运行的应用程序 EC2 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这优先于在 EC2 EC2 实例中存储访问密钥。要将 AWS 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅 IAM 用户指南中的 [使用 IAM 角色向在 Amazon EC2 实例上运行的应用程序授予权限](#)。

要了解是使用 IAM 角色还是使用 IAM 用户，请参阅 [《用户指南》中的何时创建 IAM 角色（而不是 IAM 用户）](#)。

使用策略管理访问

您将创建策略并将其附加到 AWS 身份或资源，以便控制中的 AWS 访问。策略是中的对象；AWS 在与标识或资源相关联时，策略定义它们的权限。AWS 在主体（用户、根用户或角色会话）发出请求时，将评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略在中存储 AWS 为 JSON 文档。有关 JSON 策略文档结构和内容的更多信息，请参阅 [《IAM 用户指南》中的 JSON 策略概述](#)。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入这些角色。

IAM策略定义操作的权限，无论您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或中获取角色信息 AWS API。

基于身份的策略

基于身份的策略是可附加到身份（如IAM用户、用户组或角色）的JSON权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅IAM用户指南中的[创建IAM策略](#)。

基于身份的策略可以进一步归类为内联策略或托管策略。内联策略直接嵌入单个用户、组或角色中。托管策略是可以附加到中的多个用户、组和角色的独立策略 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM用户指南》中的在[托管策略与内联策略之间进行选择](#)。

基于资源的策略

基于资源的JSON策略是附加到资源的策略文档。基于资源的策略的示例包括IAM角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中[指定主体](#)。主体可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略IAM中使用来自的 AWS 托管策略。

访问控制列表 (ACLs)

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。ACLs与基于资源的策略类似，尽管它们不使用JSON策略文档格式。

Amazon S3 AWS WAF、和亚马逊VPC就是支持的服务示例ACLs。要了解更多信息ACLs，请参阅 Amazon Simple Storage Service 开发人员指南中的[访问控制列表 \(ACL\) 概述](#)。

其他策略类型

AWS 支持额外的、不太常用的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- **权限边界**：权限边界是一个高级特征，用于设置基于身份的策略可以授予IAM实体（IAM用户或角色）的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交

集。在 Principal 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅《IAM用户指南》中的[IAM实体的权限边界](#)。

- 服务控制策略 (SCPs) — SCPs 是指定中的组织或组织单位 (OU) 的最大权限的JSON策略 AWS Organizations。AWS Organizations 是用于对您的企业拥有的多个进行分组和集中管理 AWS 账户的服务。如果您在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCPs)。SCP 限制成员账户中实体 (包括每个) 的权限 AWS 账户根用户。有关 Organization SCPs 的更多信息，请参阅《AWS Organizations 用户指南》中的[服务控制策略](#)。
- 会话策略 – 会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅《IAM用户指南》中的[会话策略](#)。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解如何 AWS 确定在涉及多种策略类型时是否允许请求，请参阅《IAM用户指南》中的[策略评估逻辑](#)。

AWS 最终用户消息社交是如何与之配合使用的 IAM

在使用管理IAM对 AWS 最终用户消息社交的访问权限之前，请先了解哪些IAM功能可用于 AWS 最终用户消息社交网站。

IAM可在 AWS 最终用户消息社交中使用的功能

IAM功能	AWS 最终用户消息社交支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	是
策略条件键	是
ACLs	否

IAM功能	AWS 最终用户消息社交支持
ABAC (策略中的标签)	部分
临时凭证	是
主体权限	是
服务角色	是
服务相关角色	是

要全面了解 AWS 最终用户消息 Social 和其他 AWS 服务如何与大多数IAM功能配合使用，请参阅《IAM用户指南》IAM中[与之配合使用的AWS 服务](#)。

适用于 Glue Managem AWS ent 的基于身份的策略

支持基于身份的策略：是

基于身份的策略是可附加到身份（如IAM用户、用户组或角色）的JSON权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅IAM用户指南中的[创建IAM策略](#)。

通过使用IAM基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可以在JSON策略中使用的所有元素，请参阅IAM用户指南中的[IAMJSON策略元素参考](#)。

适用于 Gli AWS ent VPN 的基于身份的策略示例

要查看 Eniz AWS ation 基于社交身份的策略的示例，请参阅。[适用于 Gli AWS ent VPN 的基于身份的策略示例](#)

Application AWS 中基于资源的策略

支持基于资源的策略：否

基于资源的JSON策略是附加到资源的策略文档。基于资源的策略的示例包括IAM角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件

下执行。您必须在基于资源的策略中[指定主体](#)。主体可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当主体和资源处于不同的 AWS 账户，则信任账户中的 IAM 管理员还必须授予主体实体（用户或角色）对该资源的访问权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM 用户指南》IAM [中的跨账户资源访问权限](#)。

AWS 最终用户消息 Social 的策略操作

支持策略操作：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 Action 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 AWS 最终用户消息社交操作列表，请参阅《[服务授权参考](#)》中的“[AWS 最终用户消息 Social 定义的操作](#)”。

E AWS nization Messaging Social 中的策略操作在操作前使用以下前缀：

```
social-messaging
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

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

要查看 Eniz AWS ation 基于社交身份的策略的示例，请参阅。[适用于 Gli AWS ent VPN 的基于身份的策略示例](#)

AWS 最终用户消息 Social 的政策资源

支持策略资源：是

管理员可以使用 AWS JSON策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

ResourceJSON策略元素指定要向其应用操作的对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 [Amazon 资源名称 \(ARN\)](#) 指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

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

要查看 AWS 最终用户消息社交资源类型及其列表ARNs，请参阅《[服务授权参考](#)》中的“[AWS 最终用户消息 Social 定义的资源](#)”。要了解您可以在哪些操作中指定每个资源，请参阅ARN《[AWS 最终用户消息社交定义的操作](#)》。

要查看 Eniz AWS ation 基于社交身份的策略的示例，请参阅。[适用于 Gli AWS ent VPN 的基于身份的策略示例](#)

Application Sy AWS nc 中存储的策略条件键

支持特定于服务的策略条件键：是

管理员可以使用 AWS JSON策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用[条件运算符](#)（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，仅当用户使用其IAMIAM用户名进行标记时，您才可为其授予访问资源的权限。有关更多信息，请参阅《IAM用户指南》中的[IAM策略元素：变量和标签](#)。

AWS 支持全局条件键和特定于服务的条件键。要查看所有 AWS 全局条件键，请参阅《IAM用户指南》中的[AWS 全局条件上下文键](#)。

要查看 AWS 最终用户消息社交条件键列表，请参阅《服务授权参考》中的“[AWS 最终用户消息 Social 条件密钥](#)”。要了解您可以对哪些操作和资源使用条件键，请参阅[由 AWS 最终用户消息社交定义的操作](#)。

要查看 Eniz AWS ation 基于社交身份的策略的示例，请参阅。[适用于 Gli AWS ent VPN 的基于身份的策略示例](#)

ACLs在 AWS 最终用户消息社交中

支持ACLs：否

访问控制列表 (ACLs) 控制哪些委托人 (账户成员、用户或角色) 有权访问资源。ACLs与基于资源的策略类似，尽管它们不使用JSON策略文档格式。

ABAC使用 AWS 最终用户消息社交功能

支持ABAC (策略中的标签)：部分

基于属性的访问控制 (ABAC) 是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以将标签附加到IAM实体 (用户或角色) 以及众多 AWS 资源。标记实体和资源是 ABS 的第一步。ABAC然后设计ABAC策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的[条件元素](#)中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关的更多信息ABAC，请参阅[什么是ABAC？](#)在《IAM用户指南》中。要查看包含设置步骤的教程 ABAC，请参阅IAM用户指南中的[使用基于属性的访问控制 \(ABAC\)](#)。

将临时凭证用 AWS 于 Glue

支持临时凭证：是

某 AWS 服务 些服务在您使用临时凭证登录时无法正常工作。有关其他信息，包括哪些 AWS 服务 适用于临时证书 [AWS 服务](#)，请参阅《IAM用户指南》IAM中的“[适用于临时证书](#)”。

如果您不使用用户名和密码而 AWS Management Console 用其它方法登录到，则使用临时凭证。例如，当您 AWS 使用贵公司的单点登录 (SSO) 链接访问时，该过程将自动创建临时凭证。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM用户指南》中的[切换到角色 \(控制台\)](#)。

您可以使用 AWS CLI 或手动创建临时证书 AWS API。然后，您可以使用这些临时证书进行访问 AWS。AWS 建议您动态生成临时凭证，而不是使用长期访问密钥。有关更多信息，请参阅[中的临时安全凭证IAM](#)。

Application 的 AWS 跨服务主体权限

支持转发访问会话 (FAS) : 是

当您使用IAM用户或角色在中执行操作时 AWS，您将被视为主体。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS使用主体调用的权限 AWS 服务，结合请求的，AWS 服务 向下游服务发出请求。FAS只有在服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出FAS请求时的策略详细信息，请参阅[转发访问会话](#)。

AWS 最终用户消息 Social 的服务角色

支持服务角色 : 是

服务角色是由一项服务代入、代表您执行操作的[IAM角色](#)。IAM管理员可以从中创建、修改和删除服务角色IAM。有关更多信息，请参阅《IAM用户指南》AWS 服务中的[创建角色以向委派权限](#)。

Warning

更改服务角色的权限可能会中断 AWS 最终用户消息社交的功能。仅当 AWS 最终用户消息社交提供相关指导时才编辑服务角色。

AWS 最终用户消息社交的服务相关角色

支持服务相关角色 : 是

服务相关角色是一种与服务相关的服务角色。AWS 服务服务可以代入代表您执行操作的角色。服务相关角色显示在您的中 AWS 账户，并归该服务所有。IAM管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理服务相关角色的详细信息，请参阅[使用IAM的AWS 服务](#)。在表中查找服务相关角色列表中包含 Yes 的表。选择是链接以查看该服务的服务相关角色文档。

适用于 Gli AWS ent VPN 的基于身份的策略示例

默认情况下，用户和角色没有创建或修改 AWS 最终用户消息社交资源的权限。他们也无法使用 AWS Management Console、AWS Command Line Interface (AWS CLI) 或来执行任务 AWS API。要授予用户对所需资源执行操作的权限，IAM管理员可以创建IAM策略。管理员随后可以向角色添加IAM策略，用户可以代入这些角色。

要了解如何使用这些示例策略文档创建IAM基于身份的JSON策略，请参阅IAM用户指南中的[创建IAM策略](#)。

有关 Eni AWS d 用户Messaging Social 定义的操作和资源类型的详细信息，包括每种资源类型的格式，请参阅《服务授权参考》中的[AWS 最终用户消息 Social 的操作、资源和条件键](#)。ARNs

主题

- [策略最佳实践](#)
- [使用 AWS 最终用户消息社交控制台](#)
- [允许用户查看他们自己的权限](#)

策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的 AWS 终端用户消息社交资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- AWS 托管策略及转向最低权限许可入门 — 要开始向用户和工作负载授予权限，请使用AWS 托管策略来为许多常见使用场景授予权限。它们在你的版本中可用 AWS 账户。我们建议通过定义特定于您的使用场景的 AWS 客户托管式策略来进一步减少权限。有关更多信息，请参阅《IAM用户指南》中的[AWS 托管策略或工作职能托管策略](#)。
- 应用最低权限许可 — 在使用IAM策略设置权限时，请仅授予执行任务所需的许可。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用应用权限IAM的更多信息，请参阅《IAM用户指南》IAM[中的策略和权限](#)。
- 使用IAM策略中的条件进一步限制访问权限 — 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用发送所有请求SSL。如果通过特定 AWS 服务（例如）使用服务操作，您还可以使用条件来授予对服务操作的访问权限 AWS CloudFormation。有关更多信息，请参阅《IAM用户指南》中的[IAMJSON策略元素：条件](#)。

- 使用 A IAM cccccc Analyzer 验证您的IAM策略，以确保权限的安全性和功能性 — A IAM cccccc Analyzer 会验证新策略和现有策略，以确保IAM策略符合策略语言 (JSON) 和IAM最佳实践。IAMAccess Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM用户指南》中的 [IAMAccess Analyzer 策略验证](#)。
- 需要多重身份验证 (MFA) — 如果您所处的场景要求您的中有IAM用户或根用户 AWS 账户，请启 MFA用以提高安全性。要在调用API操作MFA时进行要求，请向您的策略添加MFA条件。有关更多信息，请参阅《IAM用户指南》中的[配置MFA受保护的API访问权限](#)。

有关最佳实践的更多信息IAM，请参阅《IAM用户指南》中的[IAM中的安全最佳实践](#)。

使用 AWS 最终用户消息社交控制台

要访问 AWS 最终用户消息社交控制台，您必须拥有一组最低的权限。这些权限必须允许您列出和查看有关您的中的 AWS 最终用户消息社交资源的详细信息 AWS 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于只需要调用 AWS CLI 或的用户，无需为其提供最低控制台权限 AWS API。相反，只允许访问与其尝试执行的API操作相匹配的操作。

为确保用户和角色仍可使用 AWS 最终用户消息社交控制台，请同时将 AWS 最终用户消息社交策略 *ConsoleAccess* 或 *ReadOnly* AWS 托管策略添加到实体。有关更多信息，请参阅 [《用户指南》中的向IAM用户添加权限](#)。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以便允许IAM用户查看附加到其用户身份的内联和托管策略。此策略包括在控制台上完成此操作或者以编程方式使用或以编程方式使用 AWS CLI 或 AWS API所需的权限。

```
{
  "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 最终用户消息社交的托管策略

要向用户、组和角色添加权限，与您自己编写策略相比，使用 AWS 托管策略更简单。[创建 IAM 仅为团队提供所需权限的托管式策略](#)需要时间和专业知识。要快速入门，您可以使用我们的 AWS 托管策略。这些策略涵盖常见使用案例，可在您的 AWS 账户中使用。有关 AWS 托管策略的更多信息，请参阅《IAM 用户指南》中的[AWS 托管策略](#)。

AWS 服务负责维护和更新 AWS 管理型策略。您无法更改 AWS 管理型策略中的权限。服务偶尔会向 AWS 管理型策略添加额外权限以支持新特征。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新特征或新操作可用时，服务最有可能更新 AWS 管理型策略。服务不会从 AWS 托管策略中删除权限，因此策略更新不会破坏您的现有权限。

此外，AWS 还支持跨多种服务的工作职能的托管策略。例如，ReadOnlyAccess AWS 托管策略提供对所有 AWS 服务和资源的只读访问权限。当服务启动新特征时，AWS 会为新操作和资源添加只读

权限。有关工作职能策略的列表和说明，请参阅《IAM用户指南》中的[适用于工作职能的AWS 托管策略](#)。

AWS 最终用户消息 AWS 托管策略的社交更新

查看自《AWS 最终用户消息社交网站》开始跟踪更改以来，适用于该服务的 AWS 托管策略的更新详细信息。有关此页面更改的自动提醒，请订阅《AWS 最终用户消息社交文档历史记录》（文档历史记录）页面上的 RSS Feed（文档历史记录）页面上的 Feed。

更改	描述	日期
AWS 最终用户消息 Social 已开始跟踪更改	AWS Enization Messaging Social 开始跟踪其 AWS 托管策略的更改	2024 年 9 月 26 日

AWS 最终用户消息疑难解答社交身份和访问权限

使用以下信息可帮助您诊断和修复在使用 AWS 最终用户消息社交时可能遇到的常见问题IAM。

主题

- [我无权在 Application Sc AWS aling 中执行操作](#)
- [我无权执行：PassRole](#)
- [我想要允许我的 E AWS nization Mess AWS 账户 aging Socization 社交资源](#)

我无权在 Application Sc AWS aling 中执行操作

如果您收到错误提示，表明您无权执行某个操作，则您必须更新策略以允许执行该操作。

当mateojacksonIAM用户尝试使用控制台查看有关虚构`my-example-widget`资源的详细信息，但不具有虚构权限时，会发生以下示例错误。social-messaging:`GetWidget`

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

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 social-messaging: *GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行：PassRole

如果您收到一个错误，表明您无权执行 iam:PassRole 操作，则必须更新策略以允许您将角色传递给 AWS 最终用户消息社交网站。

有些 AWS 服务 允许您将现有角色传递到该服务，而不是创建新服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

在名为的 IAM 用户 marymajor 尝试使用控制台在 AWS 最终用户消息社交中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

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

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系 AWS 管理员。您的管理员是提供登录凭证的人。

我想要允许我的 E AWS nization Mess AWS 账户 aging Socization 社交资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表 (ACLs) 的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Eni AWS zation Social 是否支持这些功能，请参阅 [AWS 最终用户消息社交是如何与之配合使用的 IAM](#)。
- 要了解如何提供对您拥有的中的 AWS 账户 资源的访问权限，请参阅 [《IAM 用户指南》中的为您拥有 AWS 账户 的另一个中的 IAM 用户提供访问权限](#)。

- 要了解如何为[第三方提供您的资源的访问权限 AWS 账户](#)，请参阅《IAM用户指南》中的[为第三方 AWS 账户 拥有的提供访问](#)权限。
- 要了解如何通过身份联合验证提供访问权限，请参阅《用户指南》中的[为经过外部身份验证的用户 \(身份联合验证 \) 提供访问](#)权限。IAM
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM用户指南》[IAM中的跨账户资源访问](#)。

AWS 最终用户消息社交的合规性验证

要了解是否在特定合规性计划范围内，请参阅AWS 服务 合规性计划范围内的[合规性计划AWS 服务](#)范围内的，然后选择您感兴趣的合规性计划。AWS 服务 有关一般信息，请参阅[AWS 合规计划AWS](#)。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅在中[下载报告在中 AWS Artifact](#)。

您在使用时的合规性责任 AWS 服务 由您的数据的敏感性、您公司的合规性目标以及适用的法律法规决定。AWS 提供以下资源来帮助实现合规性：

- [安全性与合规性快速入门指南](#)-这些部署指南讨论了架构注意事项，并提供了在上部署以安全性和合规性为重点 AWS 的基准环境的步骤。
- [Amazon Web Services 上的HIPAA安全性和合规性架构设计](#) — 该白皮书介绍了公司 AWS 如何使用创建HIPAA符合条件的应用程序。

Note

并非所有 AWS 服务 人都有HIPAA资格。有关更多信息，请参阅[HIPAA符合条件的服务参考](#)。

- [AWS 合规AWS 性资源](#) — 此业务手册和指南集合可能适用于您的行业和位置。
- [AWS 客户合规指南](#)：从合规角度了解责任共担模式。这些指南总结了保护的最佳实践，AWS 服务 并将指南映射到跨多个框架的安全控制，包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)。
- AWS Config 开发人员指南中的@@ [使用规则评估资源](#) — AWS Config 服务评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- [AWS Security Hub](#)— 这 AWS 服务 提供了您内部安全状态的全面视图 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 [Security Hub 控件参考](#)。

- [Amazon GuardDuty](#) — 该通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的、工作负载、容器和数据面临的潜在威胁。GuardDuty 可以帮助您满足各种合规性要求 PCIDSS，例如满足某些合规性框架规定的入侵检测要求。
- [AWS Audit Manager](#)— 此 AWS 服务 可帮助您持续审计您的 AWS 使用情况，以简化管理风险以及与相关法规和行业标准的合规性的方式。

AWS 最终用户消息社交中的弹性

AWS 全球基础设施围绕 AWS 区域 和可用区而构建。AWS 区域 提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域 和可用区的更多信息，请参阅[AWS 全球基础设施](#)。

除了 AWS 全球基础设施之外，AWS 最终用户消息社交还提供多种功能来帮助支持您的数据弹性和备份需求。

AWS 最终用户消息社交中的基础设施安全

作为一项托管服务，AWS 最终用户消息社交服务由 [Amazon Web Services : 安全流程概览白皮书中所述的 AWS 全球网络安全](#) 程序提供保护。

您可以使用 AWS 已发布的API呼叫通过网络访问 AWS 最终用户消息社交网站。客户端必须支持 TLS 1.0 或更高版本。建议使用 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密 () 的密码套件，例如 (Ephemeral Diffie-HellmanPFS) 或 (Elliptic Curve DHE vs Ephemeral Diffie-Hellman)。ECDHE 大多数现代系统 (如 Java 7 及更高版本) 都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 主体关联的秘密访问密钥来对请求进行签名。或者，您可以使用 [AWS Security Token Service](#) (AWS STS) 生成临时安全凭证来对请求进行签名。

防止跨服务混淆代理

混淆代理问题是一个安全性问题，即不具有操作执行权限的实体可能会迫使具有更高权限的实体执行该操作。在中 AWS，跨服务模拟可能会导致混淆代理问题。一个服务 (呼叫服务) 调用另一项服务 (所谓的被调服务) 时，可能会发生跨服务模拟。可以操纵调用服务，使用其权限以在其他情况下该服务不应有

访问权限的方式对另一个客户的资源进行操作。为防止这种情况，AWS 提供可帮助您保护所有服务的数据的工具，而这些服务中的服务主体有权限访问账户中的资源。

我们建议在资源策略中使用[aws:SourceArn](#)和[aws:SourceAccount](#)全局条件上下文密钥来限制社交消息为该资源提供的其他服务的权限。如果您只希望将一个资源与跨服务访问相关联，请使用 `aws:SourceArn`。如果您想允许该账户中的任何资源与跨服务使用操作相关联，请使用 `aws:SourceAccount`。

防范混淆代理问题最有效的方法是使用全 `aws:SourceArn` 全局条件上下文键 ARN 和资源充足。如果不知道资源的完整 ARN 性，或者正在指定多个资源，请针对未知部分使用带有通配符 (*) 的 `aws:SourceArn` 全局上下文条件键。ARN 例如，`arn:aws:social-messaging:*:123456789012:*`。

如果 `aws:SourceArn` 值不包含账户 ID，例如 Amazon S3 存储桶 ARN，您必须使用两个全局条件上下文键来限制权限。

`aws:SourceArn` 的值必须为 `ResourceDescription`。

以下示例演示如何使用社交消息中的 `aws:SourceArn` 和 `aws:SourceAccount` 全局条件上下文键来防范混淆代理问题。

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

}

安全最佳实操

AWS 最终用户消息社交提供了在您开发和实施自己的安全策略时需要考虑的大量安全功能。以下最佳实践是一般指导原则，并不代表完整安全解决方案。这些最佳实践可能不适合环境或不满足环境要求，请将其视为有用的考虑因素而不是惯例。

- 为管理 AWS SMS 资源的每个人（包括您自己）创建一个单独的用户。请勿使用 AWS 根凭证管理 AWS SMS 资源。
- 授予每位用户执行其职责所需的最低权限集。
- 使用 IAM IAM 组有效地管理适用于多个用户的权限。
- 定期轮换 IAM 凭证。

为 Classic AWS 创建服务相关角色

AWS 最终用户消息社交使用 AWS Identity and Access Management (IAM) [与服务相关的角色](#)。服务相关角色是一种独特类型的 IAM 角色，它与 AWS 最终用户消息社交直接相关。服务相关角色由 AWS 最终用户消息社交网站预定义，并包含该服务代表您调用其它 AWS 服务所需的一切权限。

服务相关角色可让您更轻松设置 AWS 最终用户消息社交网站，因为您不必手动添加必要的权限。AWS 最终用户消息 Social 定义其服务相关角色的权限，除非另外定义，否则只有 AWS 最终用户消息社交网站可以代入该角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

只有在首先删除相关资源后，您才能删除服务相关角色。这将保护您的 AWS 最终用户消息社交资源，因为您不会无意中删除对资源的访问权限。

有关支持服务相关角色的其他服务的信息，请参阅 [AWS 与服务相关角色配合 IAM 使用的服务](#) 并查找服务相关角色列为是的服务。选择是和链接，查看该服务的服务相关角色文档。

Application Servicati AWS on 的服务相关角色权限

AWS 最终用户消息 Social 使用名为 “AWSServiceRoleForSocialMessaging-” 的服务相关角色来发布指标并为您的社交消息发送提供见解。

AWSServiceRoleForSocialMessaging 服务相关角色信任以下服务代入该角色：

- `social-messaging.amazonaws.com`

角色权限策略 `AWSSocialMessagingServiceRolePolicy` 允许 `En AWS d user Messaging Social` 对指定资源完成以下操作：

- 操作：`all AWS resources in the AWS/SocialMessaging namespace.` 上的 `"cloudwatch:PutMetricData"`

您必须配置允许用户、组或角色创建、编辑或删除服务相关角色的权限。有关更多信息，请参阅《IAM 用户指南》中的[服务相关角色权限](#)。

有关该政策的更新，请参阅[AWS 最终用户消息 AWS 托管策略的社交更新](#)。

为 Classic AWS 创建服务相关角色

您可以使用 IAM 控制台为 `AWSEndUserMessagingSocial-Metrics` 用例创建服务相关角色。在 AWS CLI 或中 AWS API，使用服务名称创建服务相关角色。`social-messaging.amazonaws.com` 有关更多信息，请参阅《IAM 用户指南》中的[创建服务相关角色](#)。如果您删除了此服务相关角色，可以使用同样的过程再次创建角色。

为 Fleet Advisor AWS 编辑服务相关角色

AWS Enization Messaging Social 不允许您编辑 `AWSServiceRoleForSocialMessaging` 服务相关角色。创建服务相关角色后，将无法更改角色名称，因为可能有多个实体引用该角色。但是，您可以使用编辑角色的说明 IAM。有关更多信息，请参阅《IAM 用户指南》中的[编辑服务相关角色](#)。

为 Classic AWS 删除服务相关角色

如果不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，必须先清除服务相关角色的资源，然后才能手动删除它。

Note

如果在您试图删除资源时，AWS 最终用户消息社交服务正在使用该角色，则删除操作可能会失败。如果发生这种情况，请等待几分钟后重试。

移除用户使用 AWS 的最终用户消息社交资源 `AWSServiceRoleForSocialMessaging`

1. `list-linked-whatsapp-business-accounts` API 致电查看您拥有的资源。

2. 对于每个关联的 whats 应用程序企业账户，请致电disassociate-whatsapp-business-accountAPI以从 SocialMessaging 服务中移除该资源。
3. list-linked-whatsapp-business-accountsAPI再次调用，验证未返回任何资源。

使用手动删除服务相关角色 IAM

使用IAM控制台 AWS CLI、或删除 AWSServiceRoleForSocialMessaging 服务相关角色。AWS API有关更多信息，请参阅《IAM用户指南》中的[删除服务相关角色](#)。

Application A AWS pplication 服务相关角色的受支持区域

AWS 最终用户消息社交支持在服务可用的所有区域中使用服务相关角色。有关更多信息，请参阅[AWS 区域和端点](#)。

AWS 最终用户消息社交配额

您的AWS账户对于每项AWS服务都具有默认配额（以前称为限制）。除非另有说明，否则，每个限额是区域特定的。您可以请求增加某些配额，但其他一些配额无法增加。

要查看 Service Quot AWS as 配额，请打开 [Service Quotas 控制台](#)。在导航窗格中，选择AWS服务，然后选择AWS 最终用户消息 Social。

要请求提高配额，请参阅《Service Quotas 用户指南》中的[请求提高配额](#)。如果配额在服务限额中尚不可用，请使用[提高限制表格](#)。

您的AWS账户具有以下与 AWS 最终用户消息 Social 相关的限额。

资源	默认
WhatsApp 企业账户 (WABA)	每个

AWS 最终用户消息社交实施配额，限制您可以向 AWS 最终用户消息社交网站发API出的请求数量 AWS 账户。

操作	费率
SendWhatsAppMessage	1000
PostWhatsAppMessageMedia	100
GetWhatsAppMessageMedia	100
DeleteWhatsAppMessageMedia	100
DisassociateWhatsAppBusinessAccount	10
ListWhatsAppBusinessAccount	10
TagResource	10
UntagResourceRate	10
ListTagsForResourceRate	10

《AWS 最终用户消息社交用户指南》的文档历史记录

下表介绍了 Mainframe Modernization 的文档版本。

变更	说明	日期
初始版本	《AWS 最终用户消息社交用户指南》的初始版本	2024 年 7 月 10 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。