



User Guide

Amazon Pinpoint SMS



Amazon Pinpoint SMS: User Guide

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

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

What is Amazon Pinpoint SMS?	1
Are you a first-time Amazon Pinpoint SMS user?	4
Features of Amazon Pinpoint SMS	4
Accessing Amazon Pinpoint SMS	4
Regional availability	5
How does SMS messaging work	10
Amazon Pinpoint SMS concepts	11
Setting up Amazon Pinpoint SMS	14
Sign up for an AWS account	14
Create a user with administrative access	15
Working with AWS SDKs	16
Getting started	18
First time user tutorial	18
Step 1: Create a pool	20
Step 2: Create a configuration set	21
Step 3: Create a protect configuration	22
Step 4: Send a test message with the SMS simulator	23
Next steps: Move from sandbox to production	24
About the SMS/MMS and Voice sandbox	26
SMS/MMS sandbox	26
Moving from the SMS/MMS sandbox	27
Voice sandbox	29
Moving from the voice sandbox to production	30
Add a verified destination	32
Message part preview	34
Simulator phone numbers	34
Origination simulator phone numbers	35
Destination simulator phone numbers	35
Set a spending limit	38
Best Practices	41
SMS and MMS best practices	41
Comply with laws, regulations, and carrier requirements	42
Prohibited message content	43
Obtain permission	45

Don't send messages to old lists	49
Audit your customer lists	49
Keep records	50
Make your messages clear, honest, and concise	50
Respond appropriately	54
Adjust your sending based on engagement	54
Send at appropriate times	54
Avoid cross-channel fatigue	55
Use dedicated short codes	55
Verify your destination phone numbers	55
Design with redundancy in mind	56
Handling deactivated phone numbers	56
Voice best practices	59
Comply with laws and regulations	59
Send at appropriate times	60
Avoid cross-channel fatigue	60
Protect yourself against voice fraud	60
Configurations	62
SMS and MMS limits and restrictions	63
SMS character limits	63
MMS file types, size and character limits	66
Message Parts per Second (MPS) limits	68
Message routes	71
Opting out	71
Choosing a phone number or sender ID	72
Sender ID	73
Long codes	74
10 digit long code (10DLC)	75
Short codes	75
Toll-free number (TFN)	76
General considerations for choosing an origination identity	76
Choosing an origination identity for one-way messaging use cases	77
Choosing an origination identity for two-way messaging use cases	80
Phone pools	82
Managing phone pools	83
Add a phone number or sender ID	87

Two-way SMS messaging	90
Keywords	98
Opt-out list	103
How to turn on shared routes	106
Deletion protection	106
Tags	107
Phone numbers	108
SMS and MMS country capabilities and limitations	110
Supported countries and regions for voice	131
Request a phone number	134
Releasing a phone number	152
Two-way SMS messaging	153
Keywords	161
Opt-out list	167
Deletion protection	169
Tags	170
Sender IDs	172
Sender ID country capabilities and limitations	172
Registered and dynamic sender IDs	173
Considerations for a Sender ID	173
Manage sender IDs	173
Tags	178
Registrations	179
Create a new registration	181
Change your registration's name	202
Check your registration status	202
Edit your registration	203
India sender ID registration	205
Singapore registration process	210
China SMS template registration process	213
Toll-free number registration process	214
10DLC registration process	220
Configuration sets	234
Managing configuration set	235
Managing event destinations	238
Edit a configuration sets protect configuration association	273

Opt-Out lists	274
Opt-out list keywords	274
Managing opt-out lists	275
Managing opt-out list phone numbers	277
Tags	280
Example sending SMS or voice messages	281
Sending SMS Messages	281
Sending Voice Messages	284
Sending an MMS message	286
Setting up a bucket in S3 for MMS files	288
Understanding SMS billing and usage reports	289
Example 1: Sending messages to the United Kingdom	291
Example 2: Sending messages to the United States	292
Requesting support for SMS, MMS and voice messaging	292
Requesting a spending quota increase	293
Protect	297
Protect configuration	297
Create a protect configuration	299
Change protect configuration country rules	301
Change a protection configuration association	302
Delete a protect configuration	305
Manage deletion protection	306
Change a protect configuration's name	308
Tags	308
Security	311
Data protection	312
Data encryption	313
Encryption in transit	313
Key management	313
Inter-network traffic privacy	313
Creating an interface VPC endpoint for Amazon Pinpoint SMS	314
Identity and access management	315
Audience	316
Authenticating with identities	317
Managing access using policies	320
How Amazon Pinpoint SMS works with IAM	322

Identity-based policy examples	331
Troubleshooting	336
Amazon Pinpoint SMS policy actions	338
Compliance validation	351
Resilience	352
Infrastructure Security	352
Configuration and vulnerability analysis in Amazon Pinpoint SMS	353
Cross-service confused deputy prevention	353
Security best practices	355
Monitoring	356
Monitoring with CloudWatch	357
Monitoring spending	358
View your monthly spending	358
Create an SMS or voice spending alarm	359
CloudTrail logs	361
Amazon Pinpoint SMS information in CloudTrail	362
Amazon Pinpoint SMS and Voice v2 API actions that can be logged by CloudTrail	363
Understanding Amazon Pinpoint SMS log file entries	366
AWS PrivateLink	369
Considerations	369
Create an interface endpoint	369
Create an endpoint policy	370
Quotas	372
SMS and MMS quotas	376
10DLC quotas	378
Protect configuration quotas	379
Voice quotas	379
Requesting a quota increase	382
Document history	384

What is Amazon Pinpoint SMS?

Amazon Pinpoint SMS is an application-to-person (A2P) SMS, MMS, and voice messaging service which provides the global scale, resiliency, and flexibility required to deliver SMS messaging in any web, mobile, or business applications. SMS messages are used for their most important and urgent communications as SMS proves to be the most effective and ubiquitous communication channel available. Customers prioritize time critical and must-deliver use-cases such as one-time password (OTP) login and authentication, marketing messages, citizen outreach, delivery status updates, or appointment reminders to name a few.

Multimedia messaging service (MMS) is an extension of SMS that provides the ability to send media messages to a mobile phone which includes image, audio, text, or video files. You can use MMS to improve engagement through a variety of branding, workflow, and marketing use cases.

The information in this user guide is intended for all Amazon Pinpoint SMS users, including marketers, business users, and developers. This guide contains information that's especially helpful for users who mainly interact with Amazon Pinpoint SMS by using the AWS Management Console.

There are several other documents that are companions to this document. The following documents provide reference information related to the Amazon Pinpoint SMS APIs:

- [Amazon Pinpoint SMS and Voice v2 API](#)
- [Amazon Pinpoint SMS and Voice AWS CLI reference](#)

Amazon Pinpoint SMS includes an API (called the Amazon Pinpoint SMS and Voice v2 API) that was designed for sending SMS, MMS and voice messages. While the Amazon Pinpoint API is focused on sending messages through scheduled and event-driven campaigns and journeys, the Amazon Pinpoint SMS and Voice v2 API provides dedicated features and capabilities for sending SMS, MMS, and voice messages directly to individual recipients. You can use Amazon Pinpoint SMS and Voice API independently of the Amazon Pinpoint campaign and journey features, or you can use both at the same time to accommodate different use cases. If you already use Amazon Pinpoint to send SMS, MMS, or voice messages, your account is already configured to use this API. Here are some key feature differences between the two APIs.

APIs	Amazon Pinpoint API	Amazon Pinpoint SMS and voice v2 API
Features	<ol style="list-style-type: none"> 1. <i>Projects</i> – a project is a collection of recipient information, segments, campaigns, and journeys. 2. <i>Multichannel</i> – a channel represents the platform through which you engage your audience segment with messages. 3. <i>Segments</i> – a segment is a group of your customers that share certain attributes. 4. <i>Campaigns</i> – a campaign is a messaging initiative that engages a specific audience segment. 5. <i>Journeys</i> – a journey is a customized, multi-step engagement experience. 6. <i>Analytics</i> – using the analytics that Amazon Pinpoint provides, you can gain insight into your user base by viewing trends related to user engagement, campaign outreach, revenue, and more. 	<ol style="list-style-type: none"> 1. <i>Phone pool</i> – a phone pool is a collection of phone numbers and sender IDs that share the same settings that you can use to send messages and provide failover if a number in the pool fails. 2. <i>Phone number</i> – a phone number, also called originator number, is a numeric string of numbers that identifies the sender. 3. <i>Sender ID</i> – a sender ID is an alphanumeric name that identifies the sender of an SMS message. 4. <i>Configuration sets</i> – a configuration set is a set of rules that are applied when you send a message. 5. <i>Opt-out lists</i> – an opt-out list is list of destination identities that should not have messages sent to them. 6. <i>Registrations</i> – some countries require phone numbers and sender IDs to be registered for use

APIs	Amazon Pinpoint API	Amazon Pinpoint SMS and voice v2 API
		<p>in the country. In Amazon Pinpoint SMS you can manage your registrations.</p> <ol style="list-style-type: none"> <li data-bbox="1068 457 1455 730">7. <i>Multimedia messaging service (MMS)</i> – send media messages to a mobile phone which includes image, audio, text, or video files. <li data-bbox="1068 751 1484 1024">8. <i>Protect configurations</i> – to build a list of country rules that allow or block messages to each destination country in the world.
Number of AWS Regions	13 AWS Regions	30 AWS Regions

This API is a good solution for users who have a multi-tenant architecture, such as Independent Software Vendors (ISVs). This API can be used to establish that event data, origination phone numbers, and opt-out lists are separated for different tenants.

When you use the SMS and Voice v2 API, we recommend that you set up phone pools, configuration sets and event destinations. The SMS and Voice v2 API doesn't automatically emit event data for the messages that you send. Setting up event destinations to capture important event data, such as message delivery and failure events.

Version 2 of this API was preceded by Version 1. If you currently use Version 1 of this API, it will continue to be available, and you can continue to use it. However, if you migrate to Version 2, you will gain additional features, such as the ability to create pools of phone numbers, request new phone numbers programmatically, and enable or disable certain capabilities of phone numbers.

Topics

- [Are you a first-time Amazon Pinpoint SMS user?](#)
- [Features of Amazon Pinpoint SMS](#)
- [Accessing Amazon Pinpoint SMS](#)
- [Regional availability](#)
- [How Short Message Service \(SMS\) works](#)
- [Amazon Pinpoint SMS concepts](#)

Are you a first-time Amazon Pinpoint SMS user?

If you're using Amazon Pinpoint SMS for the first time, we recommend that you first read the following sections:

- [What is Amazon Pinpoint SMS?](#)
- [First time user tutorial](#)

Features of Amazon Pinpoint SMS

Amazon Pinpoint SMS provides the following features and capabilities:

Global application-to-person messaging

Application-to-person messaging provides SMS and MMS messaging to mobile phone numbers.

Registration of origination identities

Use Amazon Pinpoint SMS to register your phone numbers or sender IDs and track the registration status.

SMS simulator

Use the SMS simulator to test your messaging environment.

Accessing Amazon Pinpoint SMS

You can request and manage your Amazon Pinpoint SMS origination identities (phone number or sender ID) using the following interfaces:

Amazon Pinpoint SMS console

The web interface where you create and manage Amazon Pinpoint SMS resources. If you've signed up for an AWS account, you can access the Amazon Pinpoint SMS console from the AWS Management Console.

AWS Command Line Interface

Interact with AWS services using commands in your command line shell. The AWS Command Line Interface is supported on Windows, macOS, and Linux. For more information about the AWS CLI, see [AWS Command Line Interface User Guide](#). You can find the Amazon Pinpoint SMS commands in the [AWS CLI Command Reference](#).

AWS SDKs

If you're a software developer that prefers to build applications using language-specific APIs instead of submitting a request over HTTP or HTTPS, AWS provides libraries, sample code, tutorials, and other resources. These libraries provide basic functions that automate tasks, such as cryptographically signing your requests, retrying requests, and handling error responses. These functions help make it more efficient for you to get started. For more information, see [Tools to Build on AWS](#).

Regional availability

Amazon Pinpoint SMS is available in several AWS Regions in North America, Europe, Asia, and Oceania. In each Region, AWS maintains multiple Availability Zones. These Availability Zones are physically isolated from each other, but are united by private, low-latency, high-throughput, and highly redundant network connections. These Availability Zones are used to provide very high levels of availability and redundancy, while also minimizing latency.

To learn more about AWS Regions, see [Specify which AWS Regions your account can use](#) in the *Amazon Web Services General Reference*. For a list of all the Regions where Amazon Pinpoint SMS is currently available and the endpoint for each Region, see [Amazon Pinpoint SMS endpoints and quotas for Amazon Pinpoint SMS and Voice API v2](#) and [AWS service endpoints](#) in the *Amazon Web Services General Reference* or the following table. To learn more about the number of Availability Zones that are available in each Region, see [AWS global infrastructure](#).

Region availability

Region name	Region	Endpoint	Supports SMS/ MMS channel	Supports voice channel
US East (N. Virginia)	us-east-1	sms-voice.us-east-1.amazonaws.com sms-voice-fips.us-east-1.amazonaws.com	Yes	Yes
US East (Ohio)	us-east-2	sms-voice.us-east-2.amazonaws.com sms-voice-fips.us-east-2.amazonaws.com	Yes	Yes
US West (N. California)	us-west-1	sms-voice.us-west-1.amazonaws.com sms-voice-fips.us-west-1.amazonaws.com	Yes	Yes
US West (Oregon)	us-west-2	sms-voice.us-west-2.amazonaws.com sms-voice-fips.us-	Yes	Yes

Region name	Region	Endpoint	Supports SMS/ MMS channel	Supports voice channel
		west-2.am azonaws.com		
Africa (Cape Town)	af-south-1	sms-voice.af-south-1.amazonaws.com	Yes	Yes
Asia Pacific (Hyderabad)	ap-south-2	sms-voice.ap-south-2.amazonaws.com	Yes	No
Asia Pacific (Jakarta)	ap-southeast-3	sms-voice.ap-southeast-3.amazonaws.com	Yes	No
Asia Pacific (Melbourne)	ap-southeast-4	sms-voice.ap-southeast-4.amazonaws.com	Yes	No
Asia Pacific (Mumbai)	ap-south-1	sms-voice.ap-south-1.amazonaws.com	Yes	Yes
Asia Pacific (Osaka)	ap-northeast-3	sms-voice.ap-northeast-3.amazonaws.com	Yes	Yes
Asia Pacific (Seoul)	ap-northeast-2	sms-voice.ap-northeast-2.amazonaws.com	Yes	Yes
Asia Pacific (Singapore)	ap-southeast-1	sms-voice.ap-southeast-1.amazonaws.com	Yes	Yes

Region name	Region	Endpoint	Supports SMS/ MMS channel	Supports voice channel
Asia Pacific (Sydney)	ap-southeast-2	sms-voice.ap-southeast-2.amazonaws.com	Yes	Yes
Asia Pacific (Tokyo)	ap-northeast-1	sms-voice.ap-northeast-1.amazonaws.com	Yes	Yes
AWS GovCloud (US-East)	us-gov-east-1	sms-voice.us-gov-east-1.amazonaws.com sms-voice-fips.us-gov-east-1.amazonaws.com	Yes	No
AWS GovCloud (US-West)	us-gov-west-1	sms-voice.us-gov-west-1.amazonaws.com sms-voice-fips.us-gov-west-1.amazonaws.com	Yes	Yes
Canada (Central)	ca-central-1	sms-voice.ca-central-1.amazonaws.com sms-voice-fips.ca-central-1.amazonaws.com	Yes	Yes

Region name	Region	Endpoint	Supports SMS/ MMS channel	Supports voice channel
Canada West (Calgary)	ca-west-1	sms-voice.ca-west-1.amazonaws.com sms-voice-fips.ca-west-1.amazonaws.com	Yes	No
Europe (Frankfurt)	eu-central-1	sms-voice.eu-central-1.amazonaws.com	Yes	Yes
Europe (Ireland)	eu-west-1	sms-voice.eu-west-1.amazonaws.com	Yes	Yes
Europe (London)	eu-west-2	sms-voice.eu-west-2.amazonaws.com	Yes	Yes
Europe (Milan)	eu-south-1	sms-voice.eu-south-1.amazonaws.com	Yes	No
Europe (Paris)	eu-west-3	sms-voice.eu-west-3.amazonaws.com	Yes	Yes
Europe (Spain)	eu-south-2	sms-voice.eu-south-2.amazonaws.com	Yes	No
Europe (Stockholm)	eu-north-1	sms-voice.eu-north-1.amazonaws.com	Yes	Yes

Region name	Region	Endpoint	Supports SMS/ MMS channel	Supports voice channel
Europe (Zurich)	eu-central-2	sms-voice.eu-central-2.amazonaws.com	Yes	No
Israel (Tel Aviv)	il-central-1	sms-voice.il-central-1.amazonaws.com	Yes	No
Middle East (Bahrain)	me-south-1	sms-voice.me-south-1.amazonaws.com	Yes	Yes
Middle East (UAE)	me-central-1	sms-voice.me-central-1.amazonaws.com	Yes	No
South America (São Paulo)	sa-east-1	sms-voice.sa-east-1.amazonaws.com	Yes	Yes

How Short Message Service (SMS) works

Short Message Service, commonly known as SMS, is a service that allows the exchange of text messages between mobile devices. SMS messages are typically short, with a maximum length of 160 characters, supported by virtually all mobile devices, and can be sent and received on various mobile networks. SMS is widely used for personal and business communication, providing a quick and convenient way to send concise messages to individuals or groups of people.

How does application to person (A2P) SMS work?

SMS uses the infrastructure that's already in place for voice calls, operating on the signaling channels of mobile networks. Here's a simplified overview of how SMS works:

1. **Application initiates a message.** The application creates a text message and addresses the message to the recipient's phone number.

2. **Message is sent to the SMSC.** The sender's application sends the message to the Short Message Service Center (SMSC), which is a centralized server responsible for handling SMS messages.
3. **SMSC determines the message route.** By checking the recipient's phone number, the SMSC determines the appropriate network to deliver the message.
4. **SMSC delivers the message.** The SMSC uses a series of signaling messages to send the message to the recipient's mobile network.
5. **Message is stored.** The recipient's SMSC receives the message and temporarily stores it until the recipient's device is available to receive it.
6. **Recipient's device gets notified.** When the recipient's device is reachable, the recipient's SMSC sends a notification message indicating that a new SMS is available.
7. **Message is retrieved:** The recipient's mobile device connects to the recipient's SMSC to retrieve the message.
8. **Message displays:** The recipient's mobile device receives the message and displays it to the recipient.
9. **Possible delivery confirmation.** The recipient's mobile device might send a delivery receipt (DLR) confirmation back to the sender's SMSC, indicating that the message was successfully received.

Amazon Pinpoint SMS concepts

Configuration set

Configuration sets are sets of rules that are applied when you send a message. For example, a configuration set can specify a destination for events related to a message. When SMS events occur (such as delivery or failure events), they are routed to the destination associated with the configuration set that you specified when you sent the message.

Event destination

An event destination is a location (such as a Amazon CloudWatch Logs Group, a Amazon Data Firehose stream, or an Amazon Simple Notification Service topic) that SMS and voice events are sent to. To use event destinations, you first create the destination, and then associate it with a configuration set. When you send a message, your call to the API can include a reference to a configuration set.

Keywords

A keyword is a specific word or phrase that a customer can send to your number to elicit a response, such as an informational message, opting-in to receive more messages, a special offer and other promotional and transactional messages. When your number receives a message that begins with a keyword, Amazon Pinpoint responds with a customizable message.

Opt-out list

A list of destination identities that should not have messages sent to them. Destination identities are automatically added to the opt-out list if they reply to your origination number with the keyword STOP. If you attempt to send a message to a destination number that is on an opt-out list, and the opt-out list is associated with the pool used to send the message, Amazon Pinpoint doesn't attempt to send the message. If you enable the self-managed opt-out feature for a phone number, then your recipients aren't automatically opted out when they reply to your messages with the keyword STOP.

Originator

An originator refers to either a phone number or sender ID.

Origination phone number

See phone number.

Originator sender ID

See sender ID. Also called originator ID, an alphanumeric string that identifies the sender.

Phone number

Also called originator number, a numeric string of numbers that identifies the sender. This can be a long code, short code, toll-free number (TFN), or 10 digit long code (10DLC). For more information, see [Choosing a phone number or sender ID](#).

Phone pool

A collection of phone numbers and sender IDs that share the same settings that you can use to send messages. When you send messages through a phone pool, it chooses an appropriate origination identity to send the message as. If an origination identity in the phone pool fails, the phone pool will fail over to another origination identity if it is in the same phone pool.

Registered phone number

Some countries require you to register your company's identity before you can purchase phone numbers or sender IDs. They also require a review of the messages that you send to recipients in their country. Registrations are processed by external third parties, so the amount of time to process a registration varies by phone number type and country. After all required registrations are complete, the status of your phone numbers changes to **Active** and is available for use. For more information about which countries require registration, see [Supported countries and regions for SMS messaging](#).

Simulator phone number

A simulator phone number behaves as an origination phone number and verified destination phone number. Simulator phone numbers do not require registration.

Sender ID

Also called originator ID, an alphanumeric string that identifies the sender. For more information, see [Choosing a phone number or sender ID](#)

Verified phone number/Verified destination phone number

See phone number. When your account is in Sandbox you can only send SMS messages to phone numbers that have gone through the verification process. The phone number receives an SMS messaging with a verification code. The received code must be entered into the console to complete the process.

Setting up Amazon Pinpoint SMS

This topic provides tasks and information to help you start using Amazon Pinpoint SMS. After you complete this topic, you can move on to the [Getting started with Amazon Pinpoint SMS](#) tutorial. If you already have an AWS account, you can skip to the [Getting started with Amazon Pinpoint SMS](#) tutorial.

Topics

- [Sign up for an AWS account](#)
- [Create a user with administrative access](#)
- [Using this service with an AWS SDK](#)

Sign up for an AWS account

If you do not have an AWS account, complete the following steps to create one.

To sign up for an AWS account

1. Open <https://portal.aws.amazon.com/billing/signup>.
2. Follow the online instructions.

Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

When you sign up for an AWS account, an *AWS account root user* is created. The root user has access to all AWS services and resources in the account. As a security best practice, assign administrative access to a user, and use only the root user to perform [tasks that require root user access](#).

AWS sends you a confirmation email after the sign-up process is complete. At any time, you can view your current account activity and manage your account by going to <https://aws.amazon.com/> and choosing **My Account**.

Create a user with administrative access

After you sign up for an AWS account, secure your AWS account root user, enable AWS IAM Identity Center, and create an administrative user so that you don't use the root user for everyday tasks.

Secure your AWS account root user

1. Sign in to the [AWS Management Console](#) as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.

For help signing in by using root user, see [Signing in as the root user](#) in the *AWS Sign-In User Guide*.

2. Turn on multi-factor authentication (MFA) for your root user.

For instructions, see [Enable a virtual MFA device for your AWS account root user \(console\)](#) in the *IAM User Guide*.

Create a user with administrative access

1. Enable IAM Identity Center.

For instructions, see [Enabling AWS IAM Identity Center](#) in the *AWS IAM Identity Center User Guide*.

2. In IAM Identity Center, grant administrative access to a user.

For a tutorial about using the IAM Identity Center directory as your identity source, see [Configure user access with the default IAM Identity Center directory](#) in the *AWS IAM Identity Center User Guide*.

Sign in as the user with administrative access

- To sign in with your IAM Identity Center user, use the sign-in URL that was sent to your email address when you created the IAM Identity Center user.

For help signing in using an IAM Identity Center user, see [Signing in to the AWS access portal](#) in the *AWS Sign-In User Guide*.

Assign access to additional users

1. In IAM Identity Center, create a permission set that follows the best practice of applying least-privilege permissions.

For instructions, see [Create a permission set](#) in the *AWS IAM Identity Center User Guide*.

2. Assign users to a group, and then assign single sign-on access to the group.

For instructions, see [Add groups](#) in the *AWS IAM Identity Center User Guide*.

Using this service with an AWS SDK

AWS software development kits (SDKs) are available for many popular programming languages. Each SDK provides an API, code examples, and documentation that make it easier for developers to build applications in their preferred language.

SDK documentation	Code examples
AWS SDK for C++	AWS SDK for C++ code examples
AWS CLI	AWS CLI code examples
AWS SDK for Go	AWS SDK for Go code examples
AWS SDK for Java	AWS SDK for Java code examples
AWS SDK for JavaScript	AWS SDK for JavaScript code examples
AWS SDK for Kotlin	AWS SDK for Kotlin code examples
AWS SDK for .NET	AWS SDK for .NET code examples
AWS SDK for PHP	AWS SDK for PHP code examples
AWS Tools for PowerShell	Tools for PowerShell code examples
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) code examples
AWS SDK for Ruby	AWS SDK for Ruby code examples

SDK documentation	Code examples
AWS SDK for Rust	AWS SDK for Rust code examples
AWS SDK for SAP ABAP	AWS SDK for SAP ABAP code examples
AWS SDK for Swift	AWS SDK for Swift code examples

Example availability

Can't find what you need? Request a code example by using the **Provide feedback** link at the bottom of this page.

Getting started with Amazon Pinpoint SMS

This topic shows you how to use the Amazon Pinpoint SMS console to manage phone numbers, sender IDs, pools, and configuration sets, and then send test messages. The [Amazon Pinpoint SMS workshop](#) is targeted for developers and technical individuals who are comfortable using the AWS Command Line Interface (AWS CLI) to run API commands.

Note

When you set up a new Amazon Pinpoint SMS account, it is placed in a sandbox for SMS, MMS, and voice message channels until you request production access. In the sandbox, you can access all of features of Amazon Pinpoint SMS, with restrictions on your SMS, MMS, and voice messages.

- For information about the SMS/MMS sandbox restrictions, see [SMS/MMS sandbox](#).
- For information about the voice sandbox restrictions, see [Voice sandbox](#).

When you're ready to move from the sandbox to production, create an AWS Support case for a **Service limit increase** request for each channel that you want to move.

Topics

- [First time user tutorial](#)
- [About the SMS/MMS and Voice sandbox](#)
- [Message part preview](#)
- [Simulator phone numbers](#)
- [Set a spending limit](#)

First time user tutorial

This section provides an overview of the tutorial designed to help you start using Amazon Pinpoint SMS.

Intended Audience

This tutorial is designed for system administrators and developers responsible for setting up, testing, and deploying Amazon Pinpoint SMS.

Features Used

This tutorial shows you how to use the Amazon Pinpoint SMS console to:

- Create and configure a phone pool.
- Request an origination identity, which is either a phone number or sender ID.
- Create and configure a protect configuration.
- Send a test SMS message with the SMS simulator.

Time Required

It should take about 10–15 minutes to complete this tutorial.

Regional Restrictions

There are no country or regional restrictions associated with using this solution.

Resource Usage Costs

There's no charge for creating an AWS account. However, by implementing this solution, you might incur some or all of the costs that are listed in the following table.

Description	Cost (US dollars)
Message sending costs	You pay for each SMS message part that you send through Amazon Pinpoint SMS. For more information about pricing, see Amazon SMS Pricing .
Monthly phone number lease cost	You pay a recurring monthly fee to lease each phone number or sender ID. The monthly fee varies depending on the type of phone number and sender ID. For more information about pricing, see Amazon SMS Pricing .

AWS account permissions

The account that you use to sign in to the AWS Management Console has to be able to perform the following tasks:

- Create a pool
- Create a configuration set
- Create an event destination
- Send SMS messages

For more information about account permissions, see [Identity and access management for Amazon Pinpoint SMS](#).

Step 1: Create a pool

The procedures in this section show you how to create a pool and add either a phone number or sender ID to the pool.

To create a pool

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Overview**, in the **Quick start** section, choose **Create pool**.
3. Under the **Pool setup** section, enter a name for your pool in **Pool name**.
4. Choose one of the following options:
 - **Phone number** – If you choose this option, under **Phone numbers available for association**, choose either:
 - **Request simulator number**, and in the **Country** dropdown list, choose the destination country and then **Request number**.

Note

A simulated phone number doesn't require registration. It generates realistic events and is used for testing. Messages sent from a simulator number can only be sent to other simulator destination numbers and aren't sent over the carrier network.

- Choose a phone number that you've previously purchased.

- **Sender ID** – If you choose this option, choose a sender ID from **Sender IDs available for association**.
5. Choose **Create phone pool**.

Step 2: Create a configuration set

The procedures in this section show you how to create a configuration set, add a CloudWatch Events, Amazon Data Firehose, or Amazon SNS destination and choose the event types.

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Overview**, in the **Quick start** section, choose **Create set**.
3. Under the **Configuration set details** section, enter a name in **Configuration set name**.
4. For **Event destination setup**, choose either:
 - **Set up CloudFormation** (Recommended) to have AWS CloudFormation create and configure CloudWatch, Amazon Data Firehose and Amazon SNS to log all events.
 - For **Event destination name** enter a name for the event destination.
 - Choose **Launch stack**.
 - A new browser window will open. Review the **Quick create stack** form and check any acknowledgements. Choose **Create stack**.

Note

Creating the AWS CloudFormation stack can take up to five minutes.

- When the status indicator for the AWS CloudFormation stack on the **Create configuration set** page is **Stack created**, choose **Create**.
- **Setup event destination** to manually set up the configuration set and event destination.
 - For **Event destination name**, enter a name for the event destination.
 - For **Destination type**, choose either CloudWatch, Amazon Data Firehose or Amazon SNS. For more information on how to setup these event destinations see [Amazon CloudWatch event destinations](#), [Amazon Data Firehose event destinations](#) and [Amazon SNS event destinations](#)
 - Under **Event types**, choose the appropriate option:

- **All SMS events (Recommended)** – Send all SMS events listed in [Event types for SMS, MMS, and voice](#) to the event destination.
- **Custom SMS events** – Choose specific SMS events to send to the event destination. To edit the list of events choose **Edit SMS event selection**. In the **Edit SMS event selection** window choose only the events that you want to log. Choose **Save selection**.
- **All MMS events (Recommended)** – Send all MMS events listed in [Event types for SMS, MMS, and voice](#) to the event destination.
- **Custom MMS events** – Choose specific MMS events to send to the event destination. To edit the list of events choose **Edit MMS event selection**. In the **Edit MMS event selection** window choose only the events that you want to log. Choose **Save selection**.
- **All voice events (Recommended)** – Send all voice events listed in [Event types for SMS, MMS, and voice](#) to the event destination.
- **Custom voice events** – Choose specific voice events to send to the event destination. To edit the list of events, choose **Edit voice event selection**. In the **Edit voice event selection** window choose only the events the you want to log. Choose **Save selection**.
- Choose **Create**.

5. Choose **Create configuration set**

Step 3: Create a protect configuration

The procedures in this section show you how to create a protect configuration to specify which countries Amazon Pinpoint SMS can send messages to.

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Overview**, in the **Quick start** section, choose **Create configuration**.
3. Under **Protect configuration details** enter a friendly name for your protect configuration in **Protect configuration name**.
4. (Optional) We recommend you use protect configurations to control which destination countries Amazon Pinpoint SMS can send messages to.

Under **SMS country rules**, choose the countries to block sending messages to, by default all countries are allowed. After the countries are selected choose **Block**.

Note

Do not block the country that you are going to send a test message to in the next step.

5. In **Protect configuration associates** under **Association type**, choose **Configuration set association**. Under **Configuration sets available for association**, choose the configuration set you created in step 2.
6. Choose **Create configuration**.

Step 4: Send a test message with the SMS simulator

Note

To add a verified destination phone number you must have an originator that's status is *Active*, see [Phone number status and capabilities](#). If you don't have an *Active* originator then use a simulator phone number and a simulator destination phone number to send and receive the test SMS message.

The procedures in this section show you how to send a test SMS message to verify your environment is correctly configured.

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Overview**, in the **Quick start** section, choose **Test SMS sending**.
3. For **Originator**, choose either **Phone pool**, **Phone number** or **Sender ID** as the type of originator to send the test message. You then need to select the originator identity from the dropdown list.
 - (Optional) If you need a simulator phone number then choose **Request simulator number**. In the **Request simulator number** window choose a **Country** from the dropdown list and then choose **Request number**.

Note

Simulator phone numbers can only send to other simulator destination phone numbers however they behave like actual phone numbers without sending over

the carrier network. For example, US simulator phone numbers can only send to US destination simulator phone numbers.

4. In the **Destination number** section, choose either **Simulator number** or **Verified number** and then select the number from the dropdown list.

To view your current list of verified destination numbers choose **Verified number** then expand **Manage verified destination number**. If you don't have any verified destination phone numbers, or need to add a new verified destination phone number, do the following:

- a. To verify a new destination phone number, choose **Verify new number**.
 - b. In the **Add phone number** window for **Destination phone number**, enter the phone number of the device to receive the test message. The phone number must start with a '+' and can't contain any spaces, hyphens, or parentheses. For example, +1 (206) 555-0142 is not in the correct format, but +12065550142 is.
 - c. Choose **Send verification code**.
 - d. The destination device will receive a verification code that is valid for 15 minutes. Enter the code the device received into the **Verification code** field.
 - e. Choose **Verify number**.
5. For **Configuration set**, choose the event destination to receive the event data.
 6. For **Message body**, enter a custom SMS message.
 7. Choose **Send test message**.
 8. For **Event logs: CloudWatch**, choose the refresh button to display the event log of the test message.

Tip

Wait at least at 10 seconds after sending the test SMS message before refreshing.

Next steps: Move from sandbox to production

After fully testing your SMS environment in the SMS sandbox, you can request to move to production.

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.

2. In the navigation pane, under **Overview**, in the **Quick start** section, choose **Create request**.
3. On the **Support** menu, choose **Support Center**.
4. In the **Your support cases** pane, choose **Create case**.
5. Choose the **Looking for service limit increases?** link, then complete the following:
 - For **Service**, choose **Pinpoint SMS**.
 - (Optional) For **Provide a link to the site or app which will be sending SMS messages**, provide information about the website, application, or service that will send SMS messages.
 - (Optional) For **What type of messages do you plan to send**, choose the type of message that you plan to send by using your origination identity:
 - **One Time Password** – Messages that provide passwords that your customers use to authenticate with your website or application.
 - **Promotional** – Noncritical messages that promote your business or service, such as special offers or announcements.
 - **Transactional** – Important informational messages that support customer transactions, such as order confirmations or account alerts. Transactional messages must not contain promotional or marketing content.
 - (Optional) For **Which AWS Region will you be sending messages from**, choose the AWS Region that you will be sending messages from.
 - (Optional) For **Which countries do you plan to send messages to**, enter the country or region that you want to purchase short codes in.
 - (Optional) For **How do your customers opt to receive messages from you**, provide details about your opt-in process.
 - (Optional) For **Please provide the message template that you plan to use to send messages to your customers**, include the template that you will be using.
6. Under **Requests**, complete the following sections:
 - For the **Region**, choose the AWS Region from which you will be sending messages.

 **Note**

The Region is required in the **Requests** section. Even if you provided this information in the **Case details** section, you must also include it here.

- For **Resource Type**, choose **General Limits**.
 - For the **Quota**, choose **SMS Production Access**.
 - For **New quota value**, enter 1.
7. Under **Case description**, for **Use case description**, enter any relevant details about this request.
 8. (Optional) If you want to submit any further requests, choose **Add another request**.
 9. Under **Contact options**, for **Preferred contact language**, choose whether you want to receive communications for this case in **English** or **Japanese**.
 10. When you finish, choose **Submit**.

About the SMS/MMS and Voice sandbox

New Amazon Pinpoint SMS accounts are placed into an SMS/MMS or voice sandbox. The sandbox protects both AWS customers and recipients from fraud and abuse. It creates a safe environment for test and development.

Topics

- [SMS/MMS sandbox](#)
- [Moving from the SMS/MMS sandbox to production](#)
- [Voice sandbox](#)
- [Moving from the voice sandbox to production](#)
- [Verify a destination phone number while in the sandbox](#)

SMS/MMS sandbox

While your account is in the sandbox, you can use all of the SMS sending methods in the Amazon Pinpoint SMS console or the SendTextMessages API. To send an MMS message must use the SendMediaMessage API. However, the following restrictions are in place while your account is in the sandbox:

- You have a monthly SMS spending limit of \$1.00 (USD).
- You have a monthly MMS spending limit of \$1.00 (USD).

- You can send SMS and MMS messages only to verified destination phone numbers. You can add up to 10 verified numbers.
- The rules and restrictions for sending SMS and MMS messages to each destination country apply. For example, to send a message to a recipient in the United States, you must first request and register a US number.
- To verify that you own a phone number, we send a verification code to that number. While the standard fees for each SMS message typically apply, we waive the fee for the first verification code for each phone number. For more information about SMS pricing, see the [Amazon Pinpoint SMS Pricing](#) page.

Note

Message and data rates apply for messages that you receive. We send one message per verification request.

- You can delete a destination phone number. However, you must wait 24 hours after adding a phone number before you can delete it.
- You can send SMS and MMS messages only to verified destination numbers. For more information about how to add a verified destination phone number, see [Add a verified destination](#).

You can remove these restrictions by requesting production access. For more information, see [Moving from the SMS/MMS sandbox to production](#).

Note

If your account is observed to be sending suspicious SMS/MMS traffic, your account's ability to send messages may be paused. If this occurs, please follow the steps in [Moving from the SMS/MMS sandbox to production](#) to gain production access.

Moving from the SMS/MMS sandbox to production

After fully testing your SMS/MMS environment in the SMS/MMS sandbox, you can request to move to production. Moving from the SMS sandbox to production also applies to MMS capability.


Note

If your account is in multiple AWS Regions, you must submit a support request for each Region.

To move to production from the SMS sandbox

1. Open the Support Center Console at <https://console.aws.amazon.com/support/home>.
2. In the left hand navigation choose **Your support cases**.
3. Choose **Create case**.
4. Choose the **Looking for service quota increases?** link.
5. In the **Looking for service quota increases?** window choose **Create a case instead**.
6. On the **Service Quota increase** page, complete the following:
 - For **Service**, choose **Pinpoint SMS**.
 - (Optional) For **Provide a link to the site or app which will be sending SMS messages**, provide information about the website, application, or service that will send SMS/MMS messages.
 - (Optional) For **What type of messages do you plan to send**, choose the type of message that you plan to send by using your long code:
 - **One Time Password** – Messages that provide passwords that your customers use to authenticate with your website or application.
 - **Promotional** – Noncritical messages that promote your business or service, such as special offers or announcements.
 - **Transactional** – Important informational messages that support customer transactions, such as order confirmations or account alerts. Transactional messages must not contain promotional or marketing content.
 - (Optional) For **Which AWS Region will you be sending messages from**, choose the AWS Region that you will be sending messages from.
 - (Optional) For **Which countries do you plan to send messages to**, enter the country or region that you want to purchase short codes in.
 - (Optional) In the **How do your customers opt to receive messages from you**, provide details about your opt-in process.

- (Optional) In the **Please provide the message template that you plan to use to send messages to your customers** field, include the template that you will be using.
7. Under **Requests**, complete the following sections:
 - For the **Region**, choose the AWS Regions from which you will be sending messages.

 **Note**

The AWS Regions is required in the **Requests** section. Even if you provided this information in the **Case details** section, you must also include it here.

- For **Resource Type**, choose **General Limits**.
 - For the **Quota**, choose **SMS Production Access**.
 - For **New quota value**, enter 1.
8. Under **Case description**, for **Use case description**, enter any relevant details about this request.
 9. (Optional) If you want to submit any further requests, choose **Add another request**.
 10. Under **Contact options**, for **Preferred contact language**, choose whether you want to receive communications for this case in **English** or **Japanese**.
 11. When you finish, choose **Submit**.

After we receive your request, we provide an initial response within 24 hours. We might contact you to request additional information.

Voice sandbox

To help protect our customers from fraud and abuse, we place your account in a sandbox environment when you first create it. The sandbox environment also helps you test the channel to help establish your reputation. While your account is in the sandbox, you have full access to Amazon Pinpoint SMS voice messaging, with the following restrictions:

- You have a daily limit of 20 messages.
- You can send a maximum of five voice messages to a single recipient during a 24-hour period.
- You can send a maximum of five calls per minute.
- The maximum voice message length is 30 seconds.

- You can send voice messages only to specific countries. For more information, see [Voice quotas](#).
- For more information on how to add a verified destination phone number, see [Add a verified destination](#).

When you're ready to move your account out of the voice sandbox, create an AWS Support case for a **Service limit increase** request. For more information, see [About the SMS/MMS and Voice sandbox](#).

Note

Before you request production access, you must send at least one voice message from your Amazon Pinpoint SMS account. You can send a voice message by using the [SendVoiceMessage](#) API.

Moving from the voice sandbox to production

When you first start using the voice channel, your account is in the *sandbox*.

To remove these quotas from your account, you can request to have your account removed from the sandbox. When your account is removed from the sandbox, it has *production access*.

Note

Before you request production access, you must send at least one voice message from your Amazon Pinpoint SMS account.

While in the sandbox, you are required to verify the destination numbers you're sending messages to. For more information on how to add a verified destination phone number, see [Add a verified destination](#).

To request production access

1. Open the Support Center Console at <https://console.aws.amazon.com/support/home>.
2. In the left hand navigation choose **Your support cases**.
3. Choose **Create case**.
4. Choose the **Looking for service quota increases?** link.

5. In the **Looking for service quota increases?** window choose **Create a case instead**.
6. For **Service**, choose **Pinpoint Voice**.
7. (Optional) Answer the following information:
 - **What's the maximum number of voice messages that you plan to send per day?**
 - **What will be the average length of each call that you send?**
 - **How do you obtain the phone numbers that you plan to send voice messages to?**
 - **How many dedicated phone numbers will you use to send your messages? Why did you choose this number?**
 - **How many calls do you expect to make from each phone number? (1 to X) messages per (day/week/month/other)**
 - **How do you obtain consent to send voice messages to your customers?**
 - **How can customers opt out of receiving messages from you? How will you process these requests?**
8. Under **Requests**, for **Region**, choose the AWS Region that you use to send voice messages.
9. For **Quota**, verify that **Production Access** is selected.
10. For **New quota value**, enter 1.
11. Under **Case description**, for **Use case description**, provide the following details:
 - The website or app of the company or service that will send voice messages.
 - The service that's provided by your website or app, and how your voice messages contribute to that service.
12. Under **Contact options**, for **Preferred contact language**, choose whether you want to receive communications for this case in **English** or **Japanese**.
13. When you finish, choose **Submit**.

The AWS Support team provides an initial response to your request within 24 hours.

To prevent our systems from being used to send unsolicited or malicious content, AWS Support must consider each request carefully. If we're able to do so, we'll grant your request within this 24-hour period. However, if we need to obtain additional information from you, it might take longer to resolve your request.

We might not be able to grant your request if your use case doesn't align with AWS Support policies.

Verify a destination phone number while in the sandbox

Note

Verified destination phone numbers are only required for testing while your account is in the sandbox. If your account is in production, you don't need to add verified destination phone numbers.

When your account is in the SMS/MMS or voice sandbox you can only send messages to verified destination phone numbers. You can add up to 10 verified destination phone numbers to your account. Adding a verified destination phone number requires you to send a text or voice message to the destination phone number and then entering the code the device received.

Before you begin you need an origination identity in your account that is active and has text or voice message capabilities. If you don't have an origination identity available you can use **Origination simulator phone numbers** and **Destination simulator phone numbers** to test sending and receiving messages. For more information about simulated phone numbers, see [Simulator phone numbers](#). The origination identity can only send messages within its country or region. For example, an origination identity for the United States can only send verification messages to destination phone numbers in the United States.

For more information about installing and configuring the AWS CLI, see the [AWS Command Line Interface User Guide](#).

1. Add the phone number to your account by using the [create-verified-destination-number](#) CLI command.

At the command line, enter the following command:

```
aws pinpoint-sms-voice-v2 create-verified-destination-number --destination-phone-number PhoneNumber
```

In the preceding command, make the following changes:

- Replace *PhoneNumber* with the E.164 formatted phone number to send the message to. For example, +1 (206) 555-0142 is not in the correct format, but +12065550142 is.

On completion the command will return the verified phone numbers `VerifiedDestinationNumberId` which is needed in the next steps.

2. Use the [send-destination-number-verification-code](#) CLI command to send a verification message to the device. Only the first verification code is free.

At the command line, enter the following command:

```
aws pinpoint-sms-voice-v2 send-destination-number-verification-code --verified-destination-number-id PhoneNumberID --verification-channel Channel
```

In the preceding command, make the following changes:

- Replace *PhoneNumberID* with the `VerifiedDestinationNumberId` you received in the previous step.
- Replace *Channel* with the channel to use to send the message. You need to have an origination identity that supports the channel you use. This can be TEXT or VOICE and is case sensitive.

The device should receive a message with a randomly generated code. You will need this code in the next step.

3. Use the [verify-destination-number](#) CLI command to send a verification message.

At the command line, enter the following command:

```
aws pinpoint-sms-voice-v2 verify-destination-number --verified-destination-number-id PhoneNumberID --verification-code Code
```

In the preceding command, make the following changes:

- Replace *PhoneNumberID* with the `VerifiedDestinationNumberId` you received in the previous step.
- Replace *Code* with the verification code the destination device received.

Upon successful completion the status of the verified destination phone number is `Active`. You can now send messages to the verified destination phone number while you are in the sandbox.

Message part preview

A single SMS message can contain up to 140 bytes of information. When a message contains more than the maximum number of characters, the message is split into multiple parts. Depending on the recipient's mobile carrier and device, multiple messages might be displayed as a single message, or as a sequence of separate messages.

If your message uses only characters in the GSM 03.38 character set, also known as the GSM 7-bit alphabet, it can contain up to 160 characters. If your message contains any characters that are outside the GSM 03.38 character set, it can have up to 70 characters. When you send an SMS message, Amazon Pinpoint SMS automatically determines the most efficient encoding to use.

You are billed for each message part that is sent. Phone numbers have a limit on the number of message parts they can send each second. If your message is split into two message parts, you are billed for each message part. Use the message part preview before you send your SMS message to see how many message parts it is. For more information about supported character sets, see [SMS character limits](#). For more information about message size and throughput, see [Message Parts per Second \(MPS\) limits](#).

Using the message part preview

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Shortcuts**, choose **Message part preview**.
3. In the **SMS message** section, enter your SMS message. As you enter the message, the **Part preview** displays the encoding, number of characters, and SMS message parts.

Simulator phone numbers

Amazon Pinpoint SMS includes an SMS simulator, which you can use to send text messages and receive realistic event records. The SMS simulator is a helpful way to view actual SMS event records. It's also useful for testing applications that use Amazon Pinpoint SMS to send SMS messages. Messages sent to these destination phone numbers are designed to stay within Amazon Pinpoint

SMS, so they are not sent over the carrier network. Origination and destination simulator phone numbers work with SMS and MMS.

Topics

- [Origination simulator phone numbers](#)
- [Destination simulator phone numbers](#)

Origination simulator phone numbers

You can request a simulator phone number to use as your origination identity to send test SMS and MMS messages. The simulator phone number will have a country code from the country that you choose. Amazon Pinpoint SMS currently supports origination simulator phone numbers in the United States. When you use a simulator phone number as the origination identity you can only send messages to the destination simulator phone number from the same country. If you try to send to a different county the message will fail. For example, if you use a simulator phone number from the United States and try to send a message to United Kingdoms success simulator phone number an error is returned.

Destination simulator phone numbers

Destination simulator phone numbers are available in several countries and regions. For each country and region, there are phone numbers that generate message success events, and numbers that generate message failure events. The following table contains SMS/MMS simulator phone numbers for all of the countries and regions in which the simulator is available.

Country	Event type	Phone number
Australia	Success	+61455944038
Australia	Failure	+61455944039
Austria	Success	+43676800442031
Austria	Failure	+43676800442032
Belgium	Success	+32460213922
Belgium	Failure	+32460213923

Country	Event type	Phone number
Chile	Success	+56229140630
Chile	Failure	+56229140631
Czech Republic	Success	+420790542286
Czech Republic	Failure	+420790542287
Denmark	Success	+4525919410
Denmark	Failure	+4525919215
Estonia	Success	+37282720792
Estonia	Failure	+37282720793
Finland	Success	+3584573979110
Finland	Failure	+3584573979111
France	Success	+33755512501
France	Failure	+33755512502
Hong Kong	Success	+85257048426
Hong Kong	Failure	+85257048854
Hungary	Success	+36707178770
Hungary	Failure	+36707178772
Italy	Success	+394390009172
Italy	Failure	+394390009174
Jersey	Success	+447937404990
Jersey	Failure	+447937404992

Country	Event type	Phone number
Luxembourg	Success	+352691385880
Luxembourg	Failure	+352691385882
Netherlands	Success	+3197008100148
Netherlands	Failure	+3197008100150
Norway	Success	+4759449384
Norway	Failure	+4759449387
Poland	Success	+48732141440
Poland	Failure	+48732141442
Portugal	Success	+351927946948
Portugal	Failure	+351927946950
Romania	Success	+40783900330
Romania	Failure	+40783900332
Spain	Success	+34683783440
Spain	Failure	+34683783442
Sweden	Success	+46790645100
Sweden	Failure	+46790645102
Switzerland	Success	+41798075872
Switzerland	Failure	+41798075874
Taiwan	Success	+886903444630
Taiwan	Failure	+886903444632

Country	Event type	Phone number
United Kingdom	Success	+447860019066
United Kingdom	Failure	+447860019067
United States	Success	+14254147755
United States	Failure	+14254147167

Set a spending limit

In Amazon Pinpoint SMS there are spending limits for each messaging channel.

The *account limit* is the maximum amount, in US dollars, that you can spend each month sending messages through a channel. When you reach your account limit, Amazon Pinpoint SMS stops sending your messages and, to send more messages, you need to request a spending limit increase. To learn more see [Requesting a spending quota increase](#).

The *remaining limit* is how much you have spent for the current month sending messages.

The *enforced limit* is an optional spending limit, in US dollars, between \$1 and the account limit. If you don't specify an enforced limit, you can spend up to your account limit. When you reach your enforced limit, Amazon Pinpoint SMS stops sending your messages. To resume sending messages, you can adjust your enforced limit through the console or AWS CLI. For example, if you set your SMS account limit to \$100 and your enforced limit to \$50, then once you've spent \$50, Amazon Pinpoint SMS stops sending your messages until you raise your enforced limit.

You can adjust your enforced limit to increase or decrease your spending without having to contact AWS Support.

MMS has a separate spend limit from SMS. For example you could set you MMS **Account limit** to \$10 and SMS **Account limit** to \$5.

To set up billing alarms for your spending, see [Monitoring spending](#). For more information about configuring the AWS CLI, see [Configure the AWS CLI](#) in the [AWS Command Line Interface User Guide](#).

View your spending limits (console)

View all of your spending limits

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. On the **Overview** page, navigate to **SMS Spending status**.
3. In the **SMS Spending status** pane, you can view your **Account limit**, **Enforced limit**, and **Remaining limit**.

If your **Enforced limit** displays a –, it means the limit is not set.

View your enforced spending limit (AWS CLI)

You can use the [describe-spend-limits](#) command to view all of your channel spending limits.

```
aws pinpoint-sms-voice-v2 describe-spend-limits
```

When the command completes, it returns the **Account limit** and **Enforced limit** for each channel.

Change your enforced spending limit (Console)

Change a spending limit

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. On the **Overview** page, navigate to **SMS Spending status**.
3. In the **SMS Spending status** pane, choose **Edit** for the channel for which you want to change the **Enforced limit**.
4. In the **Edit spending limits** window, choose:
 - **Update enforced spend limit** – Enter a new **Enforced limit** between one and your account limit.
 - **Default to the max send limit** – Choose this option to adjust your enforced limit to your account limit.
5. Choose **Save changes**.

Set enforced spending limit (AWS CLI)

You can use the [set-text-message-spend-limit-override](#) command to set the enforced limit for the SMS channel. For the voice channel, use the [set-voice-message-spend-limit-override](#) command.

The following command shows how to increase the enforced limit for the SMS channel.

```
aws pinpoint-sms-voice-v2 set-text-message-spend-limit-override --monthly-limit NewEnforcedLimit
```

Replace *NewEnforcedLimit* with a value between one and the account limit of the SMS channel.

When the command completes, it returns the value of your new set limit.

Remove an enforced spending limit (AWS CLI)

You can use the [delete-text-message-spend-limit-override](#) command to set your enforced limit to the account limit for the SMS channel. For the voice channel, use the [delete-voice-message-spend-limit-override](#) command.

The following command shows how to remove the enforced limit for the SMS channel.

```
aws pinpoint-sms-voice-v2 delete-text-message-spend-limit-override
```

When the command completes, it returns the value of your enforced limit.

Best Practices

For the best results for creating and sending messages, we recommend that you perform the following best practices.

Topics

- [SMS and MMS best practices](#)
- [Voice best practices](#)

SMS and MMS best practices

Additionally, mobile phone carriers continuously audit bulk SMS and MMS senders and throttle or block messages from originators that they determine to be sending unsolicited messages.

Sending unsolicited content is also a violation of the [AWS acceptable use policy](#). The Amazon Pinpoint SMS team routinely audits SMS and MMS message, and might throttle or block your ability to send messages if it appears that you're sending unsolicited messages.

Finally, in many countries, regions, and jurisdictions, there are severe penalties for sending unsolicited SMS or MMS messages. For example, in the United States, the Telephone Consumer Protection Act (TCPA) states that consumers are entitled to \$500–\$1,500 in damages (paid by the sender) for each unsolicited message that they receive.

Important

This section describes several best practices that might help you improve your customer engagement and avoid costly penalties. However, note that this section doesn't contain legal advice. Always consult an attorney to obtain legal advice.

Topics

- [Comply with laws, regulations, and carrier requirements](#)
- [Prohibited message content](#)
- [Obtain permission](#)
- [Don't send messages to old lists](#)

- [Audit your customer lists](#)
- [Keep records](#)
- [Make your messages clear, honest, and concise](#)
- [Respond appropriately](#)
- [Adjust your sending based on engagement](#)
- [Send at appropriate times](#)
- [Avoid cross-channel fatigue](#)
- [Use dedicated short codes](#)
- [Verify your destination phone numbers](#)
- [Design with redundancy in mind](#)
- [Handling deactivated phone numbers](#)

Comply with laws, regulations, and carrier requirements

You can face significant fines and penalties if you violate the laws and regulations of the places where your customers reside. For this reason, it's vital to understand the laws related to SMS and MMS messaging in each country or region where you do business.

Important

In many countries, the local carriers ultimately have the authority to determine what kind of traffic flows over their networks. This means that the carriers might impose restrictions on SMS and MMS content that exceed the minimum requirements of local laws.

The following list includes links to key laws that apply to SMS and MMS communications in some of the major markets around the world. This guide doesn't cover the laws for all locales, so it's important that you research them.

- **United States:** The Telephone Consumer Protection Act of 1991, also known as TCPA, applies to certain types of SMS messages. For more information, see the [rules and regulations](#) at the Federal Communications Commission website.
- **United Kingdom:** The Privacy and Electronic Communications (EC Directive) Regulations 2003, also known as PECR, applies to certain types of SMS messages. For more information, see [What are PECR?](#) at the website of the UK Information Commissioner's Office.

- **European Union:** The Privacy and Electronic Communications Directive 2002, sometimes known as the ePrivacy Directive, applies to some types of SMS messages. For more information, see the [full text of the law](#) at the Europa.eu website.
- **Canada:** The Fighting Internet and Wireless Spam Act, more commonly known as Canada's Anti-Spam Law or CASL, applies to certain types of SMS messages. For more information, see the [full text of the law](#) at the website of the Parliament of Canada.
- **Japan:** The Act on Regulation of Transmission of Specific Electronic Mail can apply to certain types of SMS messages.

As a sender, these laws can apply to you even if your company or organization isn't based in one of these countries. Some of the laws in this list were originally created to address unsolicited email or telephone calls, but have been interpreted or expanded to apply to SMS and MMS messages as well. Other countries and regions have their own laws related to the transmission of SMS and MMS messages. Consult an attorney in each country or region where your customers are located to obtain legal advice.

Prohibited message content

The following are general prohibited content categories for all message types globally. Some countries might allow content on the list in the following table, but no country actively allows unsolicited content. Some countries or mobile carriers require that you register your number or sender ID with them before live messaging will be enabled. When using or registering a number as an originator, follow these guidelines:

- Because regulators have a high bar for number registration, you must provide a valid opt-in workflow to register the number. For more information, see [SMS Best Practices: Obtain Permission](#).
- Don't use shortened URLs created from third-party URL shorteners, as these messages are more likely to be filtered as spam. If you want to use a shortened URL, use a 10LDC phone number or short code. Using either of these number types requires that you register your message template, which can then include a shortened URL in the message.
- For toll-free numbers, the keyword opt-out and opt-in responses are set at the carrier level, using STOP and UNSTOP. These are the only keywords that you can use, and you cannot modify them. Response messages when a user replies with STOP and UNSTOP are also managed by the carrier and you cannot modify them.

- Don't send the same or similar message contents using multiple numbers. This is considered *snowshoe spamming*, which is a practice used by spammers to avoid number rate and volume limitations.
- Any messages related to these industries could be considered restricted, and are subject to heavy filtering or being blocked outright. This can include one-time passwords and multi-factor authentication for services related to restricted categories.

If you had a registration denied for a noncompliant use case and you feel that this designation is incorrect, you can submit a request through AWS support.

The following table describes the types of restricted content.

Category	Examples
Gambling	<ul style="list-style-type: none"> • Casinos • Sweepstakes • App/Websites
High-risk financial services	<ul style="list-style-type: none"> • Payday loans • Short-term high-interest loans • Auto loans • Mortgage loans • Student loans • Debt collection • Stock alerts • Cryptocurrency
Debt forgiveness	<ul style="list-style-type: none"> • Debt consolidation • Debt reduction • Credit repair programs
Get-rich-quick schemes	<ul style="list-style-type: none"> • Work-from-home programs • Risk-investment opportunities • Pyramid or multi-level marketing schemes

Category	Examples
Illegal substances	<ul style="list-style-type: none">• Cannabis/CBD
Phishing/smishing	<ul style="list-style-type: none">• Attempts to get users to reveal personal information or website login information.
S.H.A.F.T.	<ul style="list-style-type: none">• Sex• Hate• Alcohol• Firearms• Tobacco/Vape
Third-Party Lead Generation	<ul style="list-style-type: none">• Companies that buy, sell, or share consumer information

Obtain permission

Never send messages to recipients who haven't explicitly asked to receive the specific types of messages that you plan to send. Don't share opt-in lists, even among organizations within the same company.

If recipients can sign up to receive your messages by using an online form, add systems that prevent automated scripts from subscribing people without their knowledge. You should also limit the number of times a user can submit a phone number in a single session.

When you receive an SMS or MMS opt-in request, send the recipient a message that asks them to confirm that they want to receive messages from you. Don't send that recipient any additional messages until they confirm their subscription. A subscription confirmation message might resemble the following example:

```
Text YES to join ExampleCorp alerts. 2 msgs/month. Msg & data rates may apply. Reply HELP for help, STOP to cancel.
```

Maintain records that include the date, time, and source of each opt-in request and confirmation. This might be useful if a carrier or regulatory agency requests it, and can also help you perform routine audits of your customer list.

Opt-in workflow

In some cases, such as US toll-free or short code registration, mobile carriers require you to provide mockups or screenshots of your entire opt-in workflow. The mockups or screenshots must closely resemble the opt-in workflow that your recipients will complete.

Your mockups or screenshots should include all of the following required disclosures to maintain the highest level of compliance.

Required disclosures for your opt-in

- A description of the messaging use case that you will send through your program.
- The phrase “Message and data rates may apply.”
- An indication of how often recipients will get messages from you. For example, a recurring messaging program might say “one message per week.” A one-time password or multi-factor authentication use case might say “message frequency varies” or “one message per login attempt.”
- Links to your Terms and Conditions and Privacy Policy documents.

Common rejection reasons for noncompliant opt-ins

- If the provided company name does not match what is provided in the mockup or screenshot. Any relationships that are not obvious should be explained in the opt-in workflow description.
- If it appears that a message will be sent to the recipient, but no consent is explicitly gathered before doing so. Explicit consent from the intended recipient is a requirement of all messaging.
- If it appears that receiving a text message is required to sign up for a service. This is not compliant if the workflow doesn't provide any alternative to receiving an opt-in message in another form, such as an email or a voice call.
- If the opt-in language is presented entirely in the Terms of Service. The disclosures should always be presented to the recipient at time of opt-in rather than housed inside of a linked policy document.
- If a customer provided consent to receive one type of text message from you and you send them other types of text messages. For example, they consent to receive one-time passwords, but are also sent polling and survey messages.
- If the previously listed required disclosures are not presented to the recipients.

The following example complies with the mobile carriers' requirements for a multi-factor authentication use case.

examplecorp

Ready to create your example.com account? We're glad to hear it! We just need a few pieces of information. Fields marked with * are required.

First name*

Last name*

Email address*

Next >

1. User provides basic account information.

examplecorp

You can enable Multi-Factor Authentication (MFA) to protect your account. If you do, we'll send you a unique password each time you sign in. Do you want to enable this feature?

Enable MFA

Disable MFA (less secure)

Next >

2. User decides whether to enable MFA.

examplecorp

How do you want to receive MFA messages? Choose one option.

Email

Phone call

Text message

Message and data rates may apply. If you choose to receive MFA passwords as text messages, we'll send you one text message per login attempt. To stop receiving messages, text "STOP" to 98765. For more information, text "HELP."

[Terms & Conditions](#) | [Privacy Policy](#)

Mobile number

When you press the **Next** button, we'll send you an MFA password to verify your phone number.

Next >

3. If MFA enabled, user chooses how to receive MFA token.

This section only appears when 'Text message' is selected

LTE 5:28 PM 75%

Messages 67876 Details

Your ExampleCorp Multi-factor Authentication code is 918273. Text HELP for more info or STOP to opt out.

Text Message Send

4. If user chooses to receive MFA token by text, send a token.

examplecorp

We sent a text message to you at (425) 555-0142. Enter the six digit code in that message to confirm your phone number.

[Resend code](#)

1	2 ABC	3 DEF
4 GHI	5 JKL	6 MNO
7 PQRS	8 TUV	9 WXYZ
+ * #	0	<X>

5. User enters MFA token to verify phone number.

It contains finalized text and images, and it shows the entire opt-in flow, complete with annotations. In the opt-in flow, the customer must take distinct, intentional actions to provide their consent to receive text messages and contains all of the required disclosures.

Other opt-in workflow types

Mobile carriers will also accept opt-in workflows outside of applications and websites, such as verbal or written opt-in if it complies with what has been described in the previous section. A compliant opt-in workflow and verbal or written script will gather explicit consent from the recipient to receive a specific message type. For example, a verbal script that a support agent uses to gather consent before recording into a service database, or a phone number listed on a promotional flyer. To provide a mockup of these opt-in workflow types, you can provide a screenshot of your opt-in script, marketing material, or database where numbers are collected. Mobile carriers might have additional questions around these use cases if an opt-in is not clear or the use case exceed certain volumes.

SMS and MMS specific Terms and Conditions page

Mobile carriers also require that you make a specific set of SMS and MMS Terms and Conditions available to your customers. The following terms and conditions comply with the mobile carriers' requirements. You can copy these terms and modify them to fit your use case.

Important

If you copy these terms, be sure to replace all of the items shown in {curly braces} with the appropriate values for your use case. Your legal department should also want to review these terms before you publish them, so plan accordingly.

- When you opt in to the service, we will send you {description of the messages that you plan to send}.
- You can cancel the SMS or MMS service at any time by texting "STOP" to {short code or phone number}. When you send the SMS message "STOP" to us, we reply with an SMS message that confirms that you have been unsubscribed. After this, you won't receive SMS any additional messages from us. If you want to join again, sign up as you did the first time and we will start sending SMS and MMS messages to you again.
- You can get more information at any time by texting "HELP" to {short code or phone number}. When you send the SMS message "HELP" to us, we respond with instructions on how to use our service and how to unsubscribe.
- We are able to deliver messages to the following mobile phone carriers: Major carriers: AT&T, Verizon Wireless, Sprint, T-Mobile, MetroPCS, US Cellular, Alltel, Boost Mobile, Nextel, and Virgin Mobile. Minor carriers: Alaska Communications Systems (ACS), Appalachian Wireless (EKN),

Bluegrass Cellular, Cellular One of East Central IL (ECIT), Cellular One of Northeast Pennsylvania, Cincinnati Bell Wireless, Cricket, Coral Wireless (Mobi PCS), COX, Cross, Element Mobile (Flat Wireless), Epic Touch (Elkhart Telephone), GCI, Golden State, Hawkeye (Chat Mobility), Hawkeye (NW Missouri), Illinois Valley Cellular, Inland Cellular, iWireless (Iowa Wireless), Keystone Wireless (Immix Wireless/PC Man), Mosaic (Consolidated or CTC Telecom), Nex-Tech Wireless, NTelos, Panhandle Communications, Pioneer, Plateau (Texas RSA 3 Ltd), Revol, RINA, Symmetry (TMP Corporation), Thumb Cellular, Union Wireless, United Wireless, Viaero Wireless, and West Central (WCC or 5 Star Wireless). Carriers are not liable for delayed or undelivered messages.

- Message and data rates may apply for any messages that we send to you or you send to us. You will receive {message frequency} messages per {time period}. Contact your wireless provider for more information about your text plan or data plan. If you have questions about the services provided by this short code, email us at {support email address}.
- If you have any questions regarding privacy, read our privacy policy at {link to privacy policy}

Important

If you don't provide your customers with a copy of these terms, the carriers won't approve your short code application. When these terms have been reviewed, plan to host them in a publicly accessible location. A URL that links to these terms is a required part of every short code application. If this URL isn't live when you submit your short code request, determine what the URL will be, and include a copy of the Terms and Conditions in a file that you include with your request.

Don't send messages to old lists

People change phone numbers often. A phone number that you gathered consent to contact two years ago might belong to somebody else today. Don't use an old list of phone numbers for a new messaging program. If you do, you're likely to have some messages fail because the number is no longer in service, or because some people opted out because they didn't remember giving you their consent in the first place.

Audit your customer lists

If you send recurring SMS or MMS messages, audit your customer lists on a regular basis. Auditing your customer lists helps to make sure that the only customers who receive your messages are those who are interested in receiving them.

When you audit your list, send each opted-in customer a message that reminds them that they're subscribed, and provides them with information about unsubscribing. A reminder message might resemble the following example:

```
You're subscribed to ExampleCorp alerts. Msg & data rates may apply. Reply
HELP for help, STOP to unsubscribe.
```

Keep records

Keep records that show when each customer requested to receive SMS and MMS messages from you, and which messages you sent to each customer. Many countries and regions around the world require SMS and MMS senders to maintain these records in a way that can be easily retrieved. Mobile carriers might also request this information from you at any time. The exact information that you must provide varies by country or region. For more information about record-keeping requirements, review the regulations about commercial SMS messaging in each country or region where your customers are located.

Occasionally, a carrier or regulatory agency asks us to provide proof that a customer opted to receive messages from you. In these situations, AWS Support contacts you with a list of the information that the carrier or agency requires. If you can't provide the necessary information, we may pause your ability to send additional SMS and MMS messages.

Make your messages clear, honest, and concise

SMS is a unique medium. The 160-character-per-message limit means that your messages must be concise. Techniques that you might use in other communication channels, such as email, might not apply to the SMS channel, and might even seem dishonest or deceptive when used with SMS messages. If the content in your messages doesn't align with best practices, recipients might ignore your messages. In the worst case scenario, the mobile carriers might identify your messages as spam and block future messages from your phone number.

MMS has a 1,600 character limit for the message body. Your message doesn't have to be concise, but it should still follow the best practices.

The following section provides some tips and ideas for creating an effective SMS message body.

Identify yourself as the sender

Your recipients should be able to immediately identify that a message is from you. Senders who follow this best practice include an identifying name ("program name") at the beginning of each message.

Don't do this:

Your account has been accessed from a new device. Reply Y to confirm.

Try this instead:

ExampleCorp Financial Alerts: You have logged in to your account from a new device. Reply Y to confirm, or STOP to opt-out.

Don't try to make your message look like a person-to-person message

Some marketers are tempted to add a personal touch to their messages by making their messages appear to come from an individual. However, this technique might make your message seem like a phishing attempt.

Don't do this:

Hi, this is Jane. Did you know that you can save up to 50% at Example.com? Click here for more info: <https://www.example.com>.

Try this instead:

ExampleCorp Offers: Save 25-50% on sale items at Example.com. Click here to browse the sale: <https://www.example.com>. Text STOP to opt-out.

Be careful when talking about money

Scammers often prey upon people's desire to save and receive money. Don't make offers seem too good to be true. Don't use the lure of money to deceive people. Don't use currency symbols to indicate money.

Don't do this:

Save big \$\$\$ on your next car repair by going to <https://www.example.com>.

Try this instead:

ExampleCorp Offers: Your ExampleCorp insurance policy gets you discounts at 2300+ repair shops nationwide. More info at <https://www.example.com>. Text STOP to opt-out.

Use only the necessary characters

Brands are often inclined to protect their trademarks by including trademark symbols such as ™ or ® in their messages. However, these symbols are not part of the standard set of characters that can be included in a 160-character SMS message. These characters are known as the GSM alphabet. When you send a message that contains one of these characters, your message is automatically sent using a different character encoding system, which supports only 70 characters for each message part. As a result, your message could be broken into several parts. Because you're billed for each message part that you send, it could cost you more than you expect to spend to send the entire message. Additionally, your recipients might receive several sequential messages from you, rather than one single message. For more information about SMS character encoding, see [SMS character limits](#).

Don't do this:

ExampleCorp Alerts: Save 20% when you buy a new ExampleCorp Widget® at example.com and use the promo code WIDGET.

Try this instead:

ExampleCorp Alerts: Save 20% when you buy a new ExampleCorp Widget(R) at example.com and use the promo code WIDGET.

Note

The two preceding examples are almost identical, but the first example contains a Registered Trademark symbol (®), which is not part of the GSM alphabet. As a result, the first example is sent as two message parts, while the second example is sent as one message part.

Use valid, safe links

If your message includes links, double-check the links to make sure that they work. Test your links on a device outside of your internal network to confirm that links resolve properly. Because of the 160-character limit of SMS messages, very long URLs could be split across multiple messages. You should use redirect domains to provide shortened URLs. However, you shouldn't use free link-shortening services such as tinyurl.com or bitly.com, because carriers tend to filter messages that include links on these domains. However, you can use paid link-shortening services as long as your links point to a domain that is dedicated to the exclusive use of your company or organization.

Don't do this:

Go to <https://tinyurl.com/4585y8mr> today for a special offer!

Try this instead:

ExampleCorp Offers: Today only, get an exclusive deal on an ExampleCorp Widget. See <https://a.co/cFKmaRG> for more info. Text STOP to opt-out.

Limit the number of abbreviations that you use

The 160-character limitation of the SMS channel leads some senders to believe that they need to use abbreviations extensively in their messages. However, the overuse of abbreviations can seem unprofessional to many readers, and could cause some users to report your message as spam. It's completely possible to write a coherent message without using an excessive number of abbreviations.

Don't do this:

Get a gr8 deal on ExampleCorp widgets when u buy a 4-pack 2day.

Try this instead:

ExampleCorp Alerts: Today only—an exclusive deal on ExampleCorp Widgets at example.com. Text STOP to opt-out.

Respond appropriately

When a recipient replies to your messages, make sure that you respond with useful information. For example, when a customer responds to one of your messages with the keyword "HELP", send them information about the program that they're subscribed to, the number of messages you will send each month, and the ways that they can contact you for more information. A HELP response might resemble the following example:

```
HELP: ExampleCorp alerts: email help@example.com or call 425-555-0199. 2
msgs/month. Msg & data rates may apply. Reply STOP to cancel.
```

When a customer replies with the keyword "STOP", let them know that they won't receive any further messages. A STOP response might resemble the following example:

```
You're unsubscribed from ExampleCorp alerts. No more messages will be sent.
Reply HELP, email help@example.com, or call 425-555-0199 for more info.
```

Adjust your sending based on engagement

Your customers' priorities can change over time. If customers no longer find your messages to be useful, they might opt out of your messages entirely, or even report your messages as unsolicited. For these reasons, it's important that you adjust your sending practices based on customer engagement.

For customers who rarely engage with your messages, you should adjust the frequency of your messages. For example, if you send weekly messages to engaged customers, you could create a separate monthly digest for customers who are less engaged.

Finally, remove customers who are completely unengaged from your customer lists. This step prevents customers from becoming frustrated with your messages. It also saves you money and helps protect your reputation as a sender.

Send at appropriate times

Send messages during normal daytime business hours. If you send messages at dinner time or in the middle of the night, there's a good chance that your customers will unsubscribe from your lists to avoid being disturbed. You might want to avoid sending SMS or MMS messages when your customers can't respond to them immediately.

If you send campaigns or journeys to very large audiences, double-check the throughput rates for your originator phone numbers. Divide the number of recipients by your throughput rate to determine how long it will take to send messages to all of your recipients.

Avoid cross-channel fatigue

In your campaigns, if you use multiple communication channels (such as email, SMS, MMS, and push messages), don't send the same message in every channel. When you send the same message at the same time in more than one channel, your customers will probably perceive your sending behavior to be annoying rather than helpful.

Use dedicated short codes

If you use short codes, maintain a separate short code for each brand and each type of message. For example, if your company has two brands, use a separate short code for each one. Similarly, if you send both transactional and promotional messages, use a separate short code for each type of message or register the short code once for transactional and create another registration for promotional. For more information about requesting short codes, see [Request a phone number](#).

Verify your destination phone numbers

When you send SMS and MMS messages through Amazon Pinpoint SMS, you're billed for each message part that you send. The price you pay per message part varies on the recipient's country or region. For more information about SMS and MMS pricing, see [Amazon Pinpoint SMS Pricing](#).

When Amazon Pinpoint SMS accepts a request to send an SMS or MMS message, you're charged for sending that message. This statement is true even if the intended recipient doesn't actually receive the message. For example, if the recipient's phone number is no longer in service, or if you sent the message to mobile phone number that wasn't valid, you're still billed for sending the message.

Amazon Pinpoint SMS accepts valid requests to send SMS messages and attempts to deliver them. For this reason, you should validate that the phone numbers that you send messages to are valid mobile numbers. You can use the Amazon Pinpoint SMS phone number validation service to determine if a phone number is valid and what type of number it is (such as mobile, landline, or VoIP). For more information, see [Validating phone numbers in Amazon Pinpoint SMS](#) in the *Amazon Pinpoint Developer Guide*.

Design with redundancy in mind

For mission-critical messaging programs, we recommend that you configure Amazon Pinpoint SMS in more than one AWS Region. Amazon Pinpoint SMS is available in several AWS Regions. For a complete list of Regions where Amazon Pinpoint SMS is available, see the [AWS General Reference](#).

The phone numbers that you use for SMS or MMS messages—including short codes, long codes, toll-free numbers, and 10DLC numbers—can't be replicated across AWS Regions. So to use Amazon Pinpoint SMS in multiple Regions, you must request separate phone numbers in each Region where you want to use Amazon Pinpoint SMS. For example, if you use a short code to send text messages to recipients in the United States, you must request separate short codes in each AWS Region that you plan to use.

In some countries, you can also use multiple types of phone numbers for added redundancy. For example, in the United States, you can request short codes, 10DLC numbers, and toll-free numbers. Each of these phone number types takes a different route to the recipient. Having multiple phone number types available—either in the same AWS Region or spread across multiple AWS Regions—provides an additional layer of redundancy, which can help improve resiliency.

Handling deactivated phone numbers

A deactivated phone number means that the mobile subscriber has terminated their service or transferred their phone number to a different mobile network provider. Eventually, deactivated numbers are recycled and reassigned to new subscribers. Therefore, it's possible to mistakenly send an SMS or MMS message to a phone number that now belongs to a different subscriber who has not opted in to your SMS or MMS message program.

Mobile network providers frequently publish deactivation reports that contain a current list of deactivated phone numbers in their networks. These reports are published to help keep your SMS and MMS sending list current and compliant.

Note

Many of the mobile phone numbers on deactivation reports are numbers that have been transferred to a different mobile network provider by the subscriber. Changing mobile network providers requires an opt-in from the new mobile network provider. There is a risk of removing a deactivated number that your end user believes should still receive

messages. You can engage with your end users through different channels, such as email or voice calls, if you find their phone number is deactivated.

Why is handling deactivated phone numbers important?

In the US, the Federal Communications Commission (FCC) considers sending messages to a phone number that belongs to a subscriber who has not opted in to your projects as spam. This stance can result in end-user and mobile network provider complaints, which can then lead to audits, and put your SMS and MMS message sending at risk of being entirely blocked by mobile network providers. In the worst-case scenarios, the FCC can impose fines, or you could be subject to a class-action lawsuit.

Additionally, when you send SMS or MMS messages through Amazon Pinpoint SMS, you're billed for each message that you send. By keeping your end-users lists up to date, you can prevent charges on unnecessary messages.

Amazon Pinpoint SMS provides a copy of the deactivation reports to allow you to keep all of your end-users lists up to date periodically. These reports originate from mobile network providers and are processed daily. Each report contains a list of phone numbers that have been deactivated on the mobile network provider networks. You should download and compare them to your existing end-users list. Delete all phone numbers from your end-users lists that have been deactivated.

Requesting deactivation reports

Before you can obtain a copy of a deactivation report, you must first request a deactivation report through an Amazon S3 GET OBJECT API request using the REQUESTER PAYS buckets option to download a file. For more information about Requester Pays buckets, see [Downloading objects in Requester Pays buckets](#) in the [Amazon S3 User Guide](#).

You pay for requests made against S3 buckets and objects requiring the Requester pays option. S3 request costs are based on the request type, and are charged on the quantity of requests. For more information about S3 request costs, see [Amazon S3 pricing](#).

Note

The deactivation reports retrieve only United States phone numbers.

Amazon Pinpoint SMS provides two types of deactivation reports. For ease of use, if you want the most recent deactivation report, you can submit a request using the latest object format. If you want a deactivation report for a specific date, you can submit a request using the date specific object format.

 **Note**

Amazon Pinpoint SMS stores only the last 90 days of date-specific objects.

You can use the following template example to request a deactivation report through the AWS CLI. For more information about configuring the AWS CLI, see [Configure the AWS CLI](#) in the [AWS Command Line Interface User Guide](#).

Bucket name format: `{region}-pinpoint-sms-voice/`

Latest object format: `/sms-deact-reports/{iso2}/latest-deact-report.csv`

Date specific object format: `/sms-deact-reports/{iso2}/{YYYY}-{MM}-{DD}-deact-report.csv`

In the preceding examples, make the following changes:

- Replace `{region}` with the AWS Region that host the report, for example `us-east-1`. For a list of supported AWS Regions for bucket name, see [Amazon Pinpoint API](#) in the *AWS General Reference*.
- Replace `{iso2}` with the two-letter ISO-3166 alpha-2 code for the country .
- Replace `{YYYY}` with the four digit year.
- Replace `{MM}` with the two digit month.
- Replace `{DD}` with the two digit day.

The following example shows you how to request the latest deactivation report using AWS CLI command.

```
aws s3api get-object --bucket us-east-1-pinpoint-sms-voice --key sms-deact-reports/us/latest-deact-report.csv OUTFILE.csv --request-payer requester
```

The following example shows you how to request a date-specific deactivation report using AWS CLI command.

```
aws s3api get-object --bucket us-east-1-pinpoint-sms-voice --key sms-deact-reports/US/2023-09-28-deact-report.csv OUTFILE.csv --request-payer requester
```

After the Amazon S3 GET OBJECT API request is submitted, the deactivation report is downloaded to the OUTFILE.csv specified in the command.

Using the Amazon S3 API, you can get a list of deactivation reports. You can list the deactivation reports only within the embedded sms-deact-reports/us/ folder.

The following example shows you how to get the list of deactivation reports available.

```
aws s3api list-objects-v2 --bucket us-east-1-pinpoint-sms-voice --prefix "sms-deact-reports/us/" --request-payer requester
```

Voice best practices

This section contains several best practices related to sending voice messages using Amazon Pinpoint SMS. These practices can help with the satisfaction of your recipients, and can protect you from unexpected charges.

Topics in this section:

- [Comply with laws and regulations](#)
- [Send at appropriate times](#)
- [Avoid cross-channel fatigue](#)
- [Protect yourself against voice fraud](#)

Comply with laws and regulations

You can face significant fines and penalties if you violate the laws and regulations of the places where your customers reside. For this reason, it's vital to understand the laws related to automated voice calls in each country where you do business. As a sender, these laws might apply to you even if you don't reside in one of these countries. You are responsible for complying with all applicable laws. Note that some national subdivisions have stricter rules than their parent countries. For example, several US states have rules that are more strict than the US Federal laws concerning

voice calls. This information is not intended to be legal advice. Consult an attorney in each country or region where your customers are located to obtain legal advice.

Send at appropriate times

Only send messages during normal daytime business hours in each recipient's time zone. If you send messages at dinner time or in the middle of the night, there's a good chance that your customers will unsubscribe from your lists in order to avoid being disturbed again in the future. Additionally, many countries and regions restrict the days and times at which people can receive automated messages. Although regulations vary by country, it's a good idea to not send messages before 9 AM or after 8 PM. Many countries also prohibit sending messages on Sundays and national holidays. This information is not intended to be legal advice. Consult an attorney in each country or region where your customers are located to obtain legal advice.

Avoid cross-channel fatigue

If you use multiple communication channels (such as voice, email, SMS, and push messages), don't send the same message across multiple channels unless there's a good reason for doing so. If you send the same message at the same time in more than one channel, your customers are likely to perceive this behavior as annoying rather than helpful.

Protect yourself against voice fraud

Because voice calls can be expensive, it's important to secure your AWS account against unauthorized access, and to monitor the destinations of the messages that you send.

Carefully manage IAM roles, policies, and users

In general, the IAM policies of your users should grant *least privilege*—that is, only the permissions that are required to do a task, and nothing more. You can restrict these permissions so that only a small number of users have them. For more information, see [Security best practices in IAM](#) in the *IAM User Guide*.

Additionally, you should change the passwords and access keys for your users regularly. The process of changing passwords and access keys is known as *credential rotation*. For more information, see [Security best practices in IAM](#)

Know which country you're sending to

The per-minute price that you pay for sending voice messages depends on the recipient's country. The country code of the recipient's phone number isn't always the best way to tell

which country they're in. For example, many senders realize that the United States and Canada both use the same country code (+1). However, they might not realize that 23 other countries and territories (mainly in the Pacific and Caribbean) also use this country code. Sending voice messages to some of these countries can be significantly more expensive than for others. For example, sending messages to recipients in the US and Canada costs \$0.013 per minute, but sending to Jamaica costs \$0.564 per minute¹. Phone numbers in all three of these countries begin with +1 followed by 10 digits, so to the untrained eye they can be difficult to distinguish.

You can use the [Amazon Pinpoint phone number validation service](#) to verify the country of each phone number that you send messages to.

Limit your sending to specific countries

If you plan to send messages only to recipients in specific countries, configure your message-sending applications to send messages only to those countries.

Limit the number of messages that you send to a single number

Configure your applications so that they can only send a certain number of voice messages to the same recipient each day.

¹ Prices quoted are accurate as of December 2021. Per-minute rates are subject to change. For current pricing, see [Amazon Pinpoint SMS Pricing](#).

Configurations

You can use the configurations in Amazon Pinpoint SMS to provision phone numbers or sender IDs to send SMS messages, MMS messages, or voice messages to your customers' mobile devices. Amazon Pinpoint SMS can send messages to recipients in [over 200 countries and regions](#). In some countries and regions, you can also receive messages from your customers by using the two-way SMS feature. When you create a new Amazon Pinpoint SMS account, your account is placed in an SMS sandbox. This initially limits your monthly spending and who you can send messages to. For more information, see [Amazon Pinpoint SMS sandbox](#).

To receive text messages using Amazon Pinpoint SMS, you should first obtain a dedicated number, you can then enable two-way SMS for it. Finally, you can specify the messages that Amazon Pinpoint SMS sends to customers when it receives incoming messages.

Note

When you configure SMS channel settings in Amazon Pinpoint SMS, your changes apply to other AWS services that send SMS messages, such as Amazon SNS.

Topics

- [SMS and MMS limits and restrictions](#)
- [Choosing a phone number or sender ID](#)
- [Phone pools](#)
- [Phone numbers](#)
- [Sender IDs](#)
- [Registrations](#)
- [Configuration sets](#)
- [Opt-Out lists](#)
- [Example sending SMS or voice messages](#)
- [Sending an MMS message](#)
- [Understanding SMS billing and usage reports](#)
- [Requesting support for SMS, MMS, and voice messaging](#)

SMS and MMS limits and restrictions

The SMS protocol is subject to several limitations and restrictions. For example, there are technical limitations that limit the length of each SMS message and MMS has limitations on the size of the media file and length of the message body. There are also restrictions on the type of content that you can send using SMS and MMS. This topic discusses several of these limitations and restrictions.

When you're setting up SMS and MMS messaging in Amazon Pinpoint SMS, you must consider these limitations and restrictions. As a best practice, you should also implement the techniques discussed in [SMS and MMS best practices](#).

Topics

- [SMS character limits](#)
- [MMS file types, size and character limits](#)
- [Message Parts per Second \(MPS\) limits](#)
- [Differences between message type and message routes](#)
- [Opting out](#)

SMS character limits

A single SMS message can contain up to 140 bytes of information. The number of characters you can include in a single SMS message depends on the type of characters the message contains.

If your message uses only characters in the GSM 03.38 character set, also known as the GSM 7-bit alphabet, it can contain up to 160 characters. If your message contains any characters that are outside of the GSM 03.38 character set, it can have up to 70 characters. When you send an SMS message, Amazon Pinpoint SMS automatically determines the most efficient encoding to use.

When a message contains more than the maximum number of characters, the message is split into multiple parts. When messages are split into multiple parts, each part contains additional information about the message part that precedes it. When the recipient's device receives message parts that are separated in this way, it uses this additional information to confirm that all of the message parts are displayed in the correct order. Depending on the recipient's mobile carrier and device, multiple messages might be displayed as a single message, or as a sequence of separate messages. As a result, the number of characters in each message part is reduced to 153 for messages that only contain GSM 03.38 characters, or 67 for messages that contain other characters. You can estimate how many message parts your message contains before you send it by

using SMS length calculator tools, several of which are available online. The maximum supported size of any message is 1530 GSM characters or 630 non-GSM characters. If the message size is greater than the supported size, the message will fail and Amazon Pinpoint SMS will return an **Invalid Message Exception**. For more information about throughput and message size, see [Message Parts per Second \(MPS\) limits](#).

Important

When you send a message that contains more than one message parts, you're charged for the number of message parts contained in the message. For more information about throughput and message size, see [Message Parts per Second \(MPS\) limits](#).

GSM 03.38 character set

The following table lists all of the characters that are present in the GSM 03.38 character set. If you send a message that includes only the characters shown in the following table, then the message can contain up to 160 characters.

GSM 03.38 standard characters												
A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	b	c	d	e	f	g	h	i	j	k	l	m
n	o	p	q	r	s	t	u	v	w	x	y	z
à	Å	å	Ä	ä	Ç	É	é	è	ì	Ñ	ñ	ò
Ø	ø	Ö	ö	ù	Ü	ü	Æ	æ	ß	0	1	2
3	4	5	6	7	8	9	&	*	@	:	,	¤
\$	=	!	>	#	-	ı	¿	(<	%	.	+
£	?	")	§	;	'	/	_	¥	Δ	Φ	Γ
Λ	Ω	Π	Ψ	Σ	Θ	Ξ						

The GSM 03.38 character set includes several symbols in addition to those shown in the preceding table. However, each of these characters is counted as two characters because it also includes an invisible escape character:

- ^
- {
- }
- \
- [
-]
- ~
- |
- €

Finally, the GSM 03.38 character set also includes the following nonprinted characters:

- A space character.
- A line feed control, which signifies the end of one line of text and the beginning of another.
- A carriage return control, which moves to the beginning of a line of text (usually following a line feed character).
- An escape control, which is automatically added to the characters in the preceding list.

Example messages

This section contains several example SMS messages. For each example, this section shows the total number of characters, and the number of message parts for the message.

Example 1: A long message that only contains characters in the GSM 03.38 alphabet

The following message contains only characters that are in the GSM 03.38 alphabet.

Hello Carlos. Your Example Corp. bill of \$100 is now available. Autopay is scheduled for next Thursday, April 9. To view the details of your bill, go to <https://example.com/bill1>.

The preceding message contains 180 characters, so it has to be split into multiple message parts. When a message is split into multiple message parts, each part can contain 153 GSM 03.38 characters. As a result, this message is sent as two message parts.

Example 2: A message that contains multi-byte characters

The following message contains several Chinese characters, all of which are outside of the GSM 03.38 alphabet.

```
#####.#####1994#7#####
```

The preceding message contains 71 characters. However, because almost all of the characters in the message are outside of the GSM 03.38 alphabet, it's sent as two message parts. Each of these message parts can contain a maximum of 67 characters.

Example 3: A message that contains a single non-GSM character

The following message contains a single character that isn't part of the GSM 03.38 alphabet. In this example, the character is a closing single quote ('), which is a different character from a regular apostrophe ('). Word processing applications, such as Microsoft Word, often automatically replace apostrophes with closing single quotes. If you draft your SMS messages in Microsoft Word and paste them into Amazon Pinpoint SMS, remove these special characters and replace them with apostrophes.

John: Your appointment with Dr. Salazar's office is scheduled for next Thursday at 4:30pm. Reply YES to confirm, NO to reschedule.

The preceding message contains 130 characters. However, because it contains the closing single quote character, which isn't part of the GSM 03.38 alphabet, it's sent as two message parts.

If you replace the closing single quote character in this message with an apostrophe, which is part of the GSM 03.38 alphabet, then the message is sent as a single message part.

MMS file types, size and character limits

A single MMS media file can be up to 2 MB for all image types (gif, jpeg, png) and 600 KB in size for all audio and video media file types. The text message body can contain 1600 from any character set. Unlike SMS, MMS message are not broken into multiple parts when they are sent.

File type	MIME types	Maximum file size
Graphics Interchange Format	image/gif	2 MB
Joint Photographic Experts Group	image/jpeg	2 MB
Portable Network Graphics	image/png	2 MB
Tag image file format	image/tiff	600 KB
Third generation partnership project	audio/3gpp , video/3gp p	600 KB
Third generation partnership project 2	audio/3gpp2 , video/3gp p2	600 KB
Adaptive Multi-Rate	audio/amr	600 KB
MPEG-4	audio/mp4 , video/mp4	600 KB
Moving picture experts group	audio/mpeg Only MP3 files are supported for audio/mpeg	600 KB
Ogg	audio/ogg	600 KB
QuickTime	video/quicktime	600 KB
WebM	video/webm	600 KB
iCalendar	text/calendar	600 KB
vCard	text/vcard , text/x-vc ard	600 KB
Portable Document Format	application/pdf	600 KB

Message Parts per Second (MPS) limits

SMS messages are delivered in 140-byte sections known as *message parts*. Messages that are very long, or that contain many multi-byte characters, are split into several message parts. These messages are usually re-assembled on the recipient's device, appearing as a single long message rather than several small ones. For more information about SMS character limits, see [SMS character limits](#).

For this reason, SMS throughput limits, also referred to as throttling, are measured in *Message Parts per Second* (MPS)—that is, the maximum number of message parts that you can send in a second. Your MPS limit depends on the destination country of your messages, and the type of phone number, known as the *origination number*, that you use to send the message. For example, if you use a United States short code to send messages to recipients in the US, you can send 100 MPS. However, if you use a US toll-free number to send to US recipients, you are throttled to only send 3 MPS.

MMS message are delivered as a single *message part* and are not broken into multiple *message parts*. The maximum media file size can be up to 2MB for gif, jpeg, png, and 600KB in size for all other media file types and can contain up to 1600 characters, from any character set, in the message body, see [MMS file types, size and character limits](#). If you are sending SMS messages that have more than 3 *message parts* you should consider sending an MMS message instead. For example if you send an SMS message with 481 GSM 03.38 characters then the SMS message will be split into 4 *message parts*. You are billed for each of those *message parts*. If you send the 481 GSM 03.38 characters in the MMS message body you are only billed for one *message parts*. Also only sending 1 MMS *message part* instead of 4 SMS *message parts* will increase your message throughput. For more information on pricing, see [Amazon Pinpoint pricing](#).

The following sections describe the MPS for various types of origination numbers and for various countries.

Short codes

The following table shows general MPS limits for dedicated short codes.

Geographic area	SMS MPS	MMS MPS
United States (US)	100 MPS	40 MPS

Geographic area	SMS MPS	MMS MPS
Canada (CA)	100 MPS	40 MPS
All other countries and regions	Varies by country or region.	N/A

Long codes

The following table shows general MPS limits for dedicated long codes.

Geographic area	SMS MPS	MMS MPS
United States (US) (10DLC)	Default 1 MPS. Limit increase varies. Carrier-dependent, based on the type or brand level, see 10DLC registration process . To submit a limit increase see Quotas for Amazon Pinpoint SMS .	1 MPS
Canada (CA)	1 MPS	1 MPS
All other countries and regions	10 MPS	N/A

Toll-free numbers

Toll-free numbers are currently only available in the United States. US toll-free numbers support 3 MPS and require that you register the toll-free number. For more information about registering a toll-free number, see [US toll-free number registration form](#).

Geographic area	SMS MPS	MMS MPS
United States (US)	3 MPS	3 MPS

⚠ Important

If your throughput requirements exceed 3 MPS, you should use a 10DLC number or a short code. If you purchase multiple toll-free numbers and attempt to distribute your throughput across them, the mobile carriers are likely to identify this as "snowshoeing" and filter all of your messages from their networks. For more information about "snowshoeing", see [Prohibited message content](#)

Sender IDs

The following table shows general MPS limits for sender IDs.

Sender ID type	SMS MPS	MMS MPS
Customer-defined using the Amazon Pinpoint SMS API or from the Amazon Pinpoint SMS console	10 MPS	N/A

Shared routes

The following table shows general MPS limits for shared routes.

Sender ID type	SMS MPS	MMS MPS
Shared routes/ customer-owned number	20 MPS	N/A

Differences between message type and message routes

Messages sent through Amazon Pinpoint SMS can either be promotional or transactional. A promotional message type is typically comprised of marketing or sales-related messages. Some countries or regions have quiet time hours when you're not permitted to send promotional messages. A transactional message type is for more time-sensitive messages, such as password resets or one-time passwords.

You pass the message type as an optional parameter using the [SendTextMessage](#) operation of the Amazon Pinpoint SMS and voice v2 API. In some cases you might use a sender ID as the originator, or you might have a shared pool of numbers. If you have both transactional and promotional numbers associated with your account for the destination country, Amazon Pinpoint SMS chooses a transactional number by default. Delivery receipts and the Delivery dashboard show the route as either promotional or transactional, based on the chosen number.

Opting out

By default, opt-outs are managed by AWS automatically. You can choose to disable this automatic opt-out handling by enabling self-managed opt-outs. Your account can contain both numbers for which opt-outs are managed by AWS, and numbers for which you manage opt-outs yourself. For more information about enabling self-managed opt-outs, see [Self managed opt-outs](#).

Supported opt-out keywords

Where required by local laws and regulations (such as in the US and Canada), SMS and MMS recipients can use their devices to opt out by replying to the message with any of the following:

Note

You can add custom keywords to phone numbers and phone pools to opt-out.

- ARRET
- CANCEL
- END
- OPT-OUT
- OPTOUT
- QUIT

- REMOVE
- STOP
- TD
- UNSUBSCRIBE

To opt out, the recipient must reply to the same phone number that Amazon Pinpoint SMS used to deliver the message. After opting out, the recipient no longer receives SMS or MMS messages from your AWS account.

 **Note**

For US toll-free numbers, opt-outs are managed at the carrier level. The only supported opt-out keyword for a US toll-free number is `STOP`. You can't add additional opt-out keywords, or change the response message that your recipients get when they opt-out. A user can resubscribe by sending a new message to the toll-free using either `UNSTOP` or `START` as the keyword.

To configure allowing a user to resubscribe add the keywords `UNSTOP`, `START` or both to your toll-free number and set the keyword action to `Opt-in`. For more information on adding keywords, see [Manage keywords](#).

Choosing a phone number or sender ID

Dedicated phone numbers are country-specific. You can't request a dedicated phone number for one country but then use it as an identity for another country.

When you send SMS or MMS messages using Amazon Pinpoint SMS, you can identify yourself to your recipients by using a sender ID, long code, 10 digit long code(10DLC), short code or toll-free number. Each of these types of identities has its own advantages and disadvantages, which are discussed in the following sections. Origination identities are resources that are unique to each AWS Region, so they can't be shared across AWS Regions. You can grant cross AWS account and AWS Region access to your origination identities.

For example if your use case requires you to send message to the United States and Canada you have to provision origination identities for both of those countries. You do not need to provision the origination identities in AWS Regions that are local to that country. You could provision both origination identities in US West (Oregon). As another example if your use case requires you to

send message to the United States and India you might want to provision the origination identities in AWS Regions that are geographically close to their message destinations to reduce latency. For more information see the [Amazon Pinpoint Resilient Architecture Guide](#).

Using the Amazon Pinpoint SMS console, we'll recommend one of the below origination identities depending on your use-case. Recommendations are based on your input criteria including if you require SMS and/or voice capabilities, a two-way number, and estimate monthly messages.

Topics

- [Sender ID](#)
- [Long codes](#)
- [10 digit long code \(10DLC\)](#)
- [Short codes](#)
- [Toll-free number \(TFN\)](#)
- [General considerations for choosing an origination identity](#)
- [Choosing an origination identity for one-way messaging use cases](#)
- [Choosing an origination identity for two-way messaging use cases](#)

Sender ID

A sender ID is an alphanumeric name that identifies the sender of an SMS message. When you send an SMS message using a sender ID, and the recipient is in an area where sender ID authentication is supported, your sender ID appears on the recipient's device instead of a phone number. A sender ID provides SMS recipients with more information about the sender than a phone number or short code provides.

Sender IDs are supported in several countries and regions around the world. In some places, if you're a business that sends SMS messages to individual customers, you must use a sender ID that's pre-registered with a regulatory agency or industry group. For a complete list of countries and regions that support or require sender IDs, see [SMS and MMS country capabilities and limitations](#).

Advantages

Sender IDs provide the recipient with more information about the message sender. It's easier to establish your brand identity by using a sender ID than by using a short or long code. There's no additional charge for using a sender ID.

Disadvantages

Support and requirements for sender ID authentication aren't consistent across all countries or regions. Several major markets (including Canada, China, and the United States) don't support sender ID. In some areas, you must have your sender IDs pre-approved by a regulatory agency before you can use them. Sender IDs do not support two-way SMS messaging.

Long codes

Long codes are phone numbers that use the number format of the country or region where your recipients are located. Long codes are also referred to as long numbers or virtual mobile numbers. For example, in the United States and Canada, long codes contain 11 digits: the number 1 (the country code), a three-digit area code, and a seven-digit phone number. Long codes support MMS in the United States and Canada.

Advantages

Dedicated long codes are reserved for use by your Amazon Pinpoint SMS account only—they aren't shared with other users. When you use dedicated long codes, you can specify which long code you want to use when you send each message. If you send multiple messages to the same customer, each message appears to be sent from the same phone number. For this reason, dedicated long codes can be helpful in establishing your brand or identity. Dedicated long codes support two-way SMS messages and you can receive incoming messages from your customers.

Disadvantages

If you send several hundred messages per day from a dedicated long code, mobile carriers might identify your number as one that sends unsolicited messages. If your long code is flagged, your messages might not be delivered to your recipients.

Long codes also have limited throughput. In the United States and Canada, where long codes are most commonly used, you can send a maximum of one message per second. The maximum sending rates for other countries vary. Contact AWS Support for more information. If you plan to send large volumes of SMS messages, or you plan to send at a rate greater than one message per second, you should purchase a dedicated short code.

In the United States, local long codes cannot be used for A2P SMS messages. For more information see [10 digit long code \(10DLC\)](#).

10 digit long code (10DLC)

If you want to use local long codes in the United States to send SMS or MMS messages you need to request a 10DLC, which is a ten-digit long code dedicated only for use in the United States.

Many jurisdictions have restrictions related to using long codes to send Application-to-Person (A2P) SMS messages. An A2P SMS or MMS is a message that's sent to a customer's mobile device when that customer submits his or her mobile number to an application. A2P messages are one-way conversations, such as marketing messages, one-time passwords, and appointment reminders. If you plan to send A2P messages, you should purchase a dedicated short code (if your customers are in the United States or Canada), request a 10DLC (only if your customers are in the United States), or use a sender ID (if your recipients are in a country or region where sender IDs are supported).

A 10DLC number is used only for sending messages within the US. Using a 10DLC number requires that you register your company brand and the campaign that you want to associate the number with. After approval you can request a 10DLC phone number. Once requested, the time to receive approval is 7-10 days. The number can't be used with any other campaigns.

Short codes

Short codes are numeric sequences that are shorter than a regular phone number. For example, in the United States and Canada, standard phone numbers (long codes) contain 11 digits, while short codes contain five or six digits. If you send a large volume of SMS or MMS messages to recipients in the United States or Canada, you can purchase a short code. This short code is reserved for your exclusive use. Short codes support MMS in the United States and Canada.

Advantages

Using a memorable short code can help build trust. If you need to send sensitive information, such as one-time passwords, it's a good idea to send it using a short code so that your customer can quickly determine whether a message is actually from you.

If you're running a new customer acquisition campaign, you can invite potential customers to send a keyword to your short code (for example, "Text FOOTBALL to 10987 for football news and information"). Short codes are easier to remember than long codes, and it's easier for customers to enter short codes into their devices. By reducing the amount of difficulty that customers encounter when they sign up for your marketing programs, you can increase the effectiveness of your campaigns.

Because mobile carriers must approve new short codes before making them active, they are less likely to flag messages sent from short codes as unsolicited.

When you use short codes to send SMS or MMS messages, you can send a higher volume of messages per 24-hour period than you can when you use other types of originating identities. In other words, you have a much higher *sending quota*. You can also send a much higher volume of messages per second. That is, you have a much higher *sending rate*.

Disadvantages

There are additional costs to acquire short codes, and they can take a long time to implement. For example, in the United States, there's a one-time setup fee for each short code, plus an additional recurring charge per month for each short code. It can take 8–12 weeks for short codes to become active on all carrier networks. For more information on pricing, see [Amazon Pinpoint pricing](#).

Toll-free number (TFN)

Toll-free numbers are typically used for transactional messaging, such as registration confirmation or for sending one-time passwords and only used within the US. They can be used for voice, SMS and MMS messaging. Average throughput is three message parts per second (MPS); however, this throughput is affected by character encoding. For more information about how character encoding affects message parts, see [SMS and MMS limits and restrictions](#).

US mobile carriers require that you register your toll-free number before live messaging will be enabled, see [Registrations](#). When using or registering a toll-free number, it's best to follow the guidelines in the Best Practices section for [Prohibited message content](#)

General considerations for choosing an origination identity

There are several guidelines to consider when you're deciding what type of origination identity to use:

- Sender IDs are a great option for one-way use cases. However, they're not available in all countries.
- Short codes are a great option for two-way use cases. If you have to choose between using a short code or a long code, you should choose the short code.
- In some countries (such as India and Saudi Arabia), long codes can be used to receive incoming messages, but can't be used to send outgoing messages. You can use these inbound-only long

codes to provide your recipients with a way to opt out of messages that you send using a Sender ID.

- In some countries, we maintain a pool of shared origination identities. If you send messages to recipients in a particular country, but you don't have a dedicated origination identity in that country, we make an effort to deliver your message using one of these shared identities. Shared identities are unavailable in some countries, including the United States and China.
- The mobile industry changes rapidly. In many countries, there is a trend toward increased regulation of commercial SMS messages. Carriers can, with little or no warning, decide to disallow messages sent from shared origination identities. If this happens, we will attempt to tell you about these changes with as much advance warning as possible. However, carriers generally provide us with little advance notice of these changes. For these reasons, dedicated origination identities are always preferred to shared ones.

Choosing an origination identity for one-way messaging use cases

A *one-way messaging* use case is a use case that only involves sending outgoing SMS messages to your recipients. This section provides information about choosing the right type of origination identity for your one-way messaging use case. If your use case requires two-way messaging—that is, the ability to both send outgoing messages and receive incoming messages—answer the questions in [Choosing an origination identity for two-way messaging use cases](#) instead.

One-way messaging use cases can use short codes, long codes, toll-free numbers, or alphanumeric Sender IDs as their origination identity. The right kind of origination identity to use depends on your specific needs, and on the countries that your recipients are located in.

Answer the following questions to determine the right type of origination identity for your needs. If you have recipients in multiple countries, answer these questions for each country that your recipients are located in.

1. Are you planning to send messages to recipients in the United States?
 - If you answered **Yes**, proceed to [question 2](#).
 - If you answered **No**, proceed to [question 3](#).
2. Which of the following throughput rates best fits your use case? Your throughput rate is the number of message parts that you can send each second.

- **1–3 message parts per second:** Use a toll-free number. You can also use 10DLC numbers or short codes. These number types provide plenty of room for growth, but also cost more and take longer to obtain than a toll-free number.

For more information about requesting a toll-free number, see [Request a phone number](#).

If you want to determine what kind of origination number to use for another country, return to [question 1](#). Otherwise, **stop here**.

- **10–75 message parts per second:** Use a 10DLC number. You can also use a short code, which would provide additional room for growth, but would also cost more.

For more information about setting up 10DLC, see [10DLC registration process](#).

If you want to determine what kind of origination number to use for another country, return to [question 1](#). Otherwise, **stop here**.

- **100 message parts per second or more:** Use a short code. When you create your request in the AWS Support Center Console, specify the throughput rate that you want your short code to support. US short codes support 100 message parts per second by default, but the throughput rate can be increased beyond that rate for an additional monthly fee.

For more information about requesting a short code, see [How to request short codes for messaging](#).

If you want to determine what kind of origination number to use for another country, return to [question 1](#). Otherwise, **stop here**.

3. Is it important for all of your messages to come from the same origination identity?

- If you answered **Yes**, proceed to [question 4](#).
- If you answered **No**, proceed to [question 6](#).

4. Are Sender IDs supported in the country that you plan to send messages to? For a list of countries that support Sender IDs, see [Supported countries and regions for SMS messaging](#).

- If you answered **Yes**, proceed to [question 5](#).
- If you answered **No**, proceed to [question 7](#).

5. Does the country that you plan to send messages to require pre-registration of Sender IDs? For a list of countries that require Sender ID registration, see [Supported countries and regions for SMS messaging](#).

- If you answered **Yes**, complete the Sender ID process for the destination country. When the registration process is complete, you can use your Sender ID to send messages.

If you want to determine what kind of origination identity to use for another country, return to [question 1](#). Otherwise, **stop here**.

- If you answered **No**, you can specify your Sender ID when you send your messages.

If you want to determine what kind of origination identity to use for another country, return to [question 1](#). Otherwise, **stop here**.

6. Are you planning to send messages to recipients in India?

- If you answered **Yes**, you can start sending immediately. However, the messages that you send are charged at the International Long-Distance Operator (ILDO) rate, which costs several times more than messages sent using a registered Sender ID. If costs are an important factor, you should consider registering your company and use case in India. When you complete this registration process, you can send messages at the less-expensive local rate.

If you want to determine what kind of origination identity to use for another country, return to [question 1](#). Otherwise, **stop here**.

- If you answered **No**, you can start sending without obtaining an origination identity. Your messages are sent using an origination identity that is shared with other Amazon Pinpoint users. The capabilities of the mobile networks in the destination country determine what identity is shown to recipients when they receive a message from you. In countries that support unregistered Sender IDs, your messages are sent using a generic Sender ID (such as "NOTICE"). In countries that don't support Sender IDs, your messages are sent from a random long code or short code.

If you want to determine what kind of origination identity to use for another country, return to [question 1](#). Otherwise, **stop here**.

7. Are dedicated short codes available in the country that you plan to send messages to? For a list of countries that support dedicated short codes, see [Supported countries and regions for SMS messaging](#).

- If you answered **Yes**, you should use a **short code**.
- If you answered **No**, proceed to [question 8](#).

8. Are dedicated long codes available in the country that you plan to send messages to? For a list of countries that support dedicated long codes, see [Supported countries and regions for SMS messaging](#).

- If you answered **Yes**, you can use a dedicated long code. However, if any other type of dedicated identity is available in that country (such as Sender IDs or short codes), you should use the other identity type instead. Carriers are more likely to block messages that are sent using long codes if other origination identity types are also available.

For more information about requesting dedicated SMS long codes, see [Requesting dedicated long codes for messaging](#).

If you want to determine what kind of origination identity to use for another country, return to [question 1](#). Otherwise, **stop here**.

- If you answered **No**, you can start sending without obtaining an origination ID. Your messages are sent using an origination identity that is shared with other Amazon Pinpoint users. The capabilities of the mobile networks in the destination country determine what identity is shown to recipients when they receive a message from you. In countries that support unregistered Sender IDs, your messages are sent using a generic Sender ID (such as "NOTICE"). In countries that don't support Sender IDs, your messages are sent from a random long code or short code.

If you want to determine what kind of origination identity to use for another country, return to [question 1](#). Otherwise, **stop here**.

Choosing an origination identity for two-way messaging use cases

A *two-way messaging* use case is a use case that involves both sending outgoing SMS messages to your customers and receiving incoming SMS messages from them. This section provides information about choosing the right type of origination identity for your two-way messaging use case. If your use case requires one-way messaging—that is, only the ability to send outgoing messages—answer the questions in [Choosing an origination identity for one-way messaging use cases](#) instead.

If you plan to receive incoming SMS messages, you must have a dedicated phone number. There are different types of dedicated phone numbers depending on the country where your customers are located.

Answer the following questions to determine the right type of origination identity for your needs. If you have recipients in multiple countries, answer these questions for each country that your recipients are located in.

1. Is two-way messaging supported in the country that you plan to send messages to? For a full list of countries that support two-way messaging, see [Supported countries and regions for SMS messaging](#).
 - If you answered **Yes**, proceed to [question 2](#).
 - If you answered **No**, your two-way messaging use case isn't supported, but you can still send one-way messages. To find an origination ID for sending one-way messages, see [Choosing an origination identity for one-way messaging use cases](#).
2. Are you planning to send messages to recipients in the United States?
 - If you answered **Yes**, proceed to [question 3](#).
 - If you answered **No**, proceed to [question 4](#).
3. Which of the following throughput rates best fits your requirements? Your throughput rate is the number of message parts that you can send each second.
 - **1–3 message parts per second:** Use a toll-free number. You can also use 10DLC numbers or short codes. These number types will provide plenty of room for growth, but will also cost more and take longer to obtain.

For more information about requesting a toll-free number, see [Request a phone number](#).

If you want to determine what kind of origination number to use for another country, return to [question 1](#). Otherwise, **stop here**.

- **10–75 message parts per second:** Use a 10DLC number. A short code will also work for your use case, and will provide additional room for growth, but it will also cost more.

For more information about setting up 10DLC, see [10DLC registration process](#).

If you want to determine what kind of origination number to use for another country, return to [question 1](#). Otherwise, **stop here**.

- **100 message parts per second or more:** Use a short code. When you create your request in the AWS Support Center Console, specify the throughput rate that you want your short code to support. US short codes support 100 message parts per second by default, but the throughput rate can be increased beyond that rate for an additional monthly fee.

For more information about requesting a short code, see [How to request short codes for messaging](#).

If you want to determine what kind of origination number to use for another country, return to [question 1](#). Otherwise, **stop here**.

4. Are dedicated short codes available in the country that you plan to send messages to? For a list of countries where short codes are available, see [Supported countries and regions for SMS messaging](#).

- If you answered **Yes**, use a dedicated short code. For more information about requesting a short code, see [How to request short codes for messaging](#).

If you want to determine what kind of origination number to use for another country, return to [question 1](#). Otherwise, **stop here**.

- If you answered **No**, use a dedicated long code. For more information about requesting dedicated SMS long codes, see [Requesting dedicated long codes for messaging](#).

Note

If both dedicated short codes and dedicated long codes are available in the destination country, you should use a dedicated short code. Mobile carriers are more likely to block or limit the messages that are sent from long codes if short codes are also available.

If you want to determine what kind of origination number to use for another country, return to [question 1](#). Otherwise, **stop here**.

Phone pools

A pool is a collection of phone numbers or sender IDs that share the same settings that you can use to send messages. When you send messages through a phone pool, it chooses an appropriate origination identity to send the message as. If an origination identity in the phone pool fails, the phone pool will fail over to another origination identity if it is in the same phone pool.

When you create a pool, you can configure a specified origination identity. This identity includes keywords, message type, opt-out list, two-way configuration, and self-managed opt-out configuration. For example, by using pools, you can associate a list of opted-out destination phone numbers with your phone number for a particular country. By doing so, you can prevent messages from being sent to users who have already opted out of receiving messages from you.

The configuration of every phone number that you add to a pool has to match the configuration of the first phone number that you specified when you created the pool. For example, if you create a

pool that contains a phone number that has two-way messaging enabled, the other numbers that you add to the pool must also have two-way messaging enabled.

Topics

- [Managing phone pools](#)
- [Adding a phone number or sender ID to a phone pool](#)
- [Two-way SMS messaging](#)
- [Keywords](#)
- [Opt-out list](#)
- [How to turn on shared routes](#)
- [Deletion protection](#)
- [Tags](#)

Managing phone pools

When you create a new phone pool it will inherit all of the settings from the first phone number or sender ID that is added. For example, if you create a pool that contains a phone number that has two-way messaging enabled, the other numbers that you add to the pool must also have two-way messaging enabled.

Before you can delete a pool you need to turn off **Deletion protection** and remove all but one of originators from the phone pool. For more information on how to disable deletion protection, see [Deletion protection](#). The phone numbers and sender IDs that were associated with the pool remain in your Amazon Pinpoint SMS account.

Note

When you add a phone number or sender ID to a phone pool and you need make an update then you make the change in the phone pool. For example, if you want to add a new Keyword to a phone number then you would add the Keyword to the phone pool and not the phone number.

Create a phone pool (Console)

To create a pool using the Amazon Pinpoint SMS console, follow these steps:

To create a pool (Console)

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone pools**.
3. On the **Phone pools** page, choose **Create phone pool**.
4. Under the **Pool setup** section, for **Pool name** enter a name for your pool.
5. Choose one of the following options:
 - **Phone number** – In the **Phone numbers available for association** section, choose a phone number to associate with the pool.
 - **Simulator number** (Optional)– If you don't have any phone numbers and want to request a simulator phone number then choose **Phone number** and in the **Phone numbers available for association** section, do the following:
 - Choose **Request simulator number**.
 - In **Request simulator number**, choose your country from the dropdown list.
 - Choose **Request number**.
 - In **Phone numbers available for association**, choose the new simulator phone number.
 - **Sender ID** – In the **Sender IDs available for association** section, choose a sender ID to associate with the pool.
6. (Optional) Expand the **Tags** and choose **Add new tag**.
 - a. Enter a new blank key/value pair.
 - b. (Optional) Choose **Add new tag** to add another tag.
7. Choose **Create phone pool**.

Create a phone pool (AWS CLI)

You can use the [create-pool](#) command to create new pools.

You can also add a phone number to a pool when you use the `RequestPhoneNumber` API to purchase a phone number. For more information, see [Request a phone number](#).

To create a pool using the AWS CLI

- At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 create-pool \  
> --origination-identity originationIdentity \  
> --iso-country-code XX \  
> --message-type TRANSACTIONAL
```

In the preceding command, make the following changes:

- Replace *originationIdentity* with the unique ID or Amazon Resource Name (ARN) of the phone number or sender ID that you want to add to the pool.

Tip

You can find both the ID and ARN of a phone number by using the [describe-phone-numbers](#) operation. You can find the ID and ARN of a sender ID by using the [describe-sender-ids](#) operation.

- Replace *XX* with the ISO-3166 alpha-2 identifier of the country for the *originationIdentity*.
- If you plan to use the pool to send marketing or promotional messages, replace *TRANSACTIONAL* with PROMOTIONAL. Otherwise, use TRANSACTIONAL.

List phone pools (AWS CLI)

You can use the [describe-pools](#) CLI to view information about existing pools.

This operation can provide a complete list of all of the pools in your Amazon Pinpoint account, information about a specific pool, or a list of pools that is filtered based on criteria that you define.

To retrieve a list of all of your pools using the AWS CLI

- At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 describe-pools
```

To find information about specific pools, use the `PoolId` parameter.

To get information about specific pools using the AWS CLI

- At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 describe-pools \  
> --pool-id poolId
```

In the preceding command, replace *poolId* with the ID or Amazon Resource Name (ARN) of the pool.

To see a filtered list of pools, use the `Filters` parameter. You can use the following filter values:

- `status` – The current status of the pool, such as `ACTIVE`.
- `message-type` – The type of messages that the pool is used to send. Possible values are `TRANSACTIONAL` or `PROMOTIONAL`.
- `two-way-enabled` – A boolean that indicates whether two-way SMS messaging is enabled for numbers in the pool.
- `self-managed-opt-outs-enabled` – A boolean that indicates whether self-managed SMS opt-outs are enabled for numbers in the pool.
- `opt-out-list-name` – The name of the opt-out list associated with the pool.
- `shared-routes-enabled` – A boolean that indicates whether shared routes are enabled for the pool.
- `deletion-protection-enabled` – A boolean that indicates whether or not the phone number can be deleted using the `DeletePhoneNumber` operation.

For example, if you want to view a list of pools for transactional messages that support two-way messaging, enter the following command at the command line:

```
$ aws pinpoint-sms-voice-v2 describe-pools \  
> --filters Name=message-type,Values=TRANSACTIONAL \  
> --filters Name=two-way-enabled,Values=true
```

Delete a phone pool (Console)

Before you can delete a pool you need to turn off Deletion protection and remove all originators from the phone pool. To delete a pool using the Amazon Pinpoint SMS console, follow these steps:

To delete a pool (Console)

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone pool**.
3. On the **Phone Pools** page, choose the pool to delete.
4. Choose **Delete**.
5. Enter **release** and then **Confirm** to delete the pool.

Delete a phone pool (AWS CLI)

Before you can delete a pool you need to turn off Deletion protection and remove all originators from the phone pool. You can use the [delete-pool](#) API to delete pools.

To delete a pool using the AWS CLI

- To delete a pool, enter the following command at the command line:

```
$ aws pinpoint-sms-voice-v2 delete-pool \  
> --pool-id pool-78ec067f62f94d57bd3bab991example
```

In the preceding command, replace *pool-78ec067f62f94d57bd3bab991example* with the unique ID or the Amazon Resource Name (ARN) of the pool. You can find both of these values by using the [describe-pools](#) operation.

Adding a phone number or sender ID to a phone pool

Important

The configuration of every phone number or sender ID that you add to a pool has to match the configuration of the phone pool. For example, if you create a pool that contains a

phone number that has two-way messaging enabled, the other numbers that you add to the pool must also have two-way messaging enabled.

Add a phone number or sender ID to a pool (Console)

To add a phone number or sender ID to a pool using the Amazon Pinpoint SMS console, follow these steps:

Add a phone number or sender ID (Console)

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone pools**.
3. On the **Phone Pools** page, choose the phone pool to add the origination identity to.
4. On the **Associated pool originators** tab, choose **Add originator**.
5. Choose one of the following options:
 - **Phone number** – If you choose this option, under the **Phone numbers available for association** section, do the following:
 - Choose a phone number to add to the phone pool.
 - **Sender ID** – If you choose this option, under the **Sender IDs available for association** section, do the following:
 - Choose a sender ID to add the phone pool.
6. Choose **Add originator to pool**.

Add a phone number or sender ID to a pool (AWS CLI)

You can use the [associate-origination-identity](#) CLI to add phone numbers or sender IDs to an existing pool.

The configuration of every phone number or sender ID that you add to a pool has to match the configuration of the first phone number or sender ID that you specified when you created the pool. For example, if you create a pool that contains a phone number that has two-way messaging enabled, the other numbers that you add to the pool must also have two-way messaging enabled.

To add a phone number or sender ID to a pool using the AWS CLI

- At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 associate-origination-identity \  
> --pool-id poolId \  
> --origination-identity originationIdentity \  
> --iso-country-code US
```

In the preceding command, make the following changes:

- Replace *poolId* with the ID or Amazon Resource Name (ARN) of the pool that you want to add the origination identity to.
- Replace *originationIdentity* with the unique ID or Amazon Resource Name (ARN) of the phone number or sender ID that you want to add to the pool.
- Replace *+12065550142* with the origination identity that you want to add to the pool. This value can be a short code, a phone number, or a sender ID.
- Replace *US* with the two-letter ISO-3166 alpha-2 code for the country of the origination identity.

List origination identities (AWS CLI)

You can use the [list-pool-origination-identities](#) CLI to view information about all of the origination identities that have been added to a specific pool.

To view a list of origination IDs in a pool using the AWS CLI

- At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 list-pool-origination-identities \  
> --pool-id pool-78ec067f62f94d57bd3bab991example
```

In the preceding command, replace *poolId* with the ID or Amazon Resource Name (ARN) of the pool.

Two-way SMS messaging

Amazon Pinpoint SMS includes support for two-way SMS. When you set up two-way SMS, you can receive incoming messages from your customers. You can also use two-way messaging together with other AWS services, such as Lambda and Amazon Lex, to create interactive text messaging experiences.

When one of your customers sends a message to your phone number, the message body is sent to an Amazon SNS topic or Amazon Connect for processing.

Two-way SMS is only available in certain countries and regions. For more information about two-way SMS support by country or region, see [SMS and MMS country capabilities and limitations](#).

Sender IDs do not support two-way SMS messaging.

Note

Two-way SMS is only available in certain countries and regions. For more information about two-way SMS support by country or region, see [SMS and MMS country capabilities and limitations](#).

Two-way MMS is not available.

Amazon Connect for two-way SMS is available in the AWS Regions listed in [Chat messaging: SMS subtype](#) in the *Amazon Connect administrator guide*.

Two-way SMS messaging (Console)

To enable two-way SMS using the Amazon Pinpoint SMS console, follow these steps:

Enable two-way SMS

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone pools**.
3. On the **Phone pools** page, choose a phone pool.
4. On the **Two-way SMS** tab, choose **Edit settings**.
5. On the **Edit settings** page turn on **Enable two-way message**.
6. For **Destination type**, choose either **Amazon SNS** or **Amazon Connect**.

- For Amazon SNS choose either **New Amazon SNS topic** or **Existing Amazon SNS topic** and then for **Two-way channel role**, choose either **Choose existing IAM role** or **Use Amazon SNS topic policies**.
- **New Amazon SNS topic** – If you choose this option, Amazon Pinpoint SMS creates a topic in your account. The topic is automatically created with all of the required permissions. For more information on Amazon SNS topics see [Configuring Amazon SNS](#) in the *Amazon SNS developer guide*.
- **Existing Amazon SNS topic** – If you choose this option, you must choose an existing Amazon SNS topic from the **Incoming messages destination** dropdown.
- For **Two-way channel role**, choose either:
 - **Choose existing IAM role** – Choose an existing IAM policy to apply to the Amazon SNS topic. For example Amazon SNS policies see [IAM policies for Amazon SNS topics](#).
 - **Use Amazon SNS topic policies** – The Amazon SNS topic requires the appropriate Amazon SNS topic policy to grant access to Amazon Pinpoint SMS. For example Amazon SNS policies, see [Amazon SNS topic policies for Amazon SNS topics](#).
- For Amazon Connect in **Two-way channel role**, choose **Choose existing IAM roles**.
 - In the **Existing IAM roles** drop down choose an existing IAM role as the message destination. For example IAM policies, see [IAM policies for Amazon Connect](#) .

7. Choose **Save changes**.

Two-way SMS messaging (AWS CLI)

You can use the [update-pool](#) command to enable two-way SMS.

At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 update-pool \  
> --pool-id poolid \  
> --two-way-channel-arn TwoWayARN \  
> --two-way-channel-role TwoChannelWayRole
```

In the preceding command, make the following changes:

- Replace *poolid* with the PhonePoolID or Amazon Resource Name (ARN) of the phone number.

- Replace *TwoWayARN* with the Amazon Resource Name (ARN) to receive the incoming SMS messages. For example Amazon SNS policies, see [Amazon SNS topic policies for Amazon SNS topics](#). To set Amazon Connect as the inbound destination set *TwoWayARN* to `connect.region.amazonaws.com`. Replace *region* with the AWS Region the Amazon Connect instance is hosted in.
- Replace *TwoChannelWayRole* with the Amazon Resource Name (ARN) of the IAM role to use. For example SNS permission policies, see [IAM policies for Amazon SNS topics](#) and for example Amazon Connect policies, see [IAM policies for Amazon Connect](#). This parameter is only required if you choose to use IAM permission policies.

IAM policies for Amazon SNS topics

If you want Amazon Pinpoint SMS to use an existing IAM role or if you create a new role, attach the following policies to that role so that Amazon Pinpoint SMS can assume it. For information about how to modify the trust relationship of a role, see [Modifying a Role](#) in the [IAM user guide](#).

The following is the **trust policy** for the IAM role, make the following changes:

- Replace *accountId* with the unique ID for your AWS account.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SMSVoice",
      "Effect": "Allow",
      "Principal": {
        "Service": "sms-voice.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "accountId"
        }
      }
    }
  ]
}
```

The following is the **permission policy** for the IAM role. The `SMSVoiceAllowSNSPublish` Sid is a permission policy to allow for publishing to Amazon SNS topics and the `SMSVoiceAllowEncryptedSNSTopics` Sid is an option for encrypted Amazon SNS topics.

In the following IAM permission policy, make the following changes:

- Replace *partition* with the AWS partition that you use Amazon Pinpoint SMS in.
- Replace *region* with the AWS Region that you use Amazon Pinpoint SMS in.
- Replace *accountId* with the unique ID for your AWS account.
- Replace *snsTopicArn* with the Amazon SNS topics that will receive messages.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SMSVoiceAllowSNSPublish",
      "Effect": "Allow",
      "Action": "sns:Publish",
      "Resource": "arn:partition:sns:region:accountId:snsTopicArn",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "accountId"
        }
      }
    },
    {
      "Sid": "SMSVoiceAllowEncryptedSNSTopics",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:EncryptionContext:aws:sns:topicArn":
            "arn:partition:sns:region:accountId:snsTopicArn",
          "aws:CalledViaLast": "sns.amazonaws.com"
        }
      }
    }
  ]
}
```

```
]
}
```

Amazon SNS topic policies for Amazon SNS topics

The Amazon SNS topic requires the appropriate topic policy to grant access to Amazon Pinpoint SMS if they are not provided in the *TwoChannelWayRole* parameter.

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": "sms-voice.amazonaws.com"
  },
  "Action": "sns:Publish",
  "Resource": "snsTopicArn"
}
```

In the preceding example, make the following changes:

- Replace *snsTopicArn* with the Amazon SNS topic that will send and receive messages.

Note

Amazon SNS FIFO topics are not supported.

Although Amazon Pinpoint SMS data is encrypted, you can use Amazon SNS topics that are encrypted using AWS KMS keys for an additional level of security. This added security can be helpful if your application handles private or sensitive data.

You need to perform some additional setup steps to use encrypted Amazon SNS topics with two-way messaging.

The following example statement uses the, optional but recommended, `SourceAccount` and `SourceArn` conditions to avoid the confused deputy problem and only the Amazon Pinpoint SMS owner account has access. For more information on the confused deputy problem, see [The confused deputy problem](#) in the [IAM user guide](#).

First, the key that you use must be *symmetric*. Encrypted Amazon SNS topics don't support asymmetric AWS KMS keys.

Second, the key policy must be modified to allow Amazon Pinpoint SMS to use the key. Add the following permissions to the existing key policy:

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": "sms-voice.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey*",
    "kms:Decrypt"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "accountId"
    },
    "ArnLike": {
      "aws:SourceArn": "arn:aws:sms-voice:region:accountId:*"
    }
  }
}
```

For more information about editing key policies, see [Changing a key policy](#) in the *AWS Key Management Service Developer Guide*.

For more information about encrypting Amazon SNS topics using AWS KMS keys, see [Enable compatibility between event sources from AWS services and encrypted topics](#) in the *Amazon Simple Notification Service Developer Guide*.

Example of a two-way SMS message payload

When your number receives an SMS message, Amazon Pinpoint SMS sends a JSON payload to an Amazon SNS topic that you designate. The JSON payload contains the message and related data, as in the following example:

```
{
  "originationNumber":"+14255550182",
  "destinationNumber":"+12125550101",
  "messageKeyword":"JOIN",
  "messageBody":"EXAMPLE",
  "inboundMessageId":"cae173d2-66b9-564c-8309-21f858e9fb84",
```

```
"previousPublishedMessageId": "wJa1rXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
}
```

The incoming message payload contains the following information:

Property	Description
originationNumber	The phone number that sent the incoming message to you (in other words, your customer's phone number).
destinationNumber	The phone number that the customer sent the message to (your dedicated phone number).
messageKeyword	The registered keyword that's associated with your dedicated phone number.
messageBody	The message that the customer sent to you.
inboundMessageId	The unique identifier for the incoming message.
previousPublishedMessageId	The unique identifier of the message that the customer is responding to.

IAM policies for Amazon Connect

If you want Amazon Pinpoint SMS to use an existing IAM role or if you create a new role, attach the following policies to that role so that Amazon Pinpoint SMS can assume it. For information about how to modify an existing trust relationship of a role, see [Modifying a Role](#) in the *IAM user guide*.

To create new IAM policies, do the following:

1. Create a new **permission policy** by following the directions in [Creating policies using the JSON editor](#) in the IAM User Guide.
 - In step 4 use the **permission policy** defined below.
2. Create a new **trust policy** by following the directions in [Creating a role using custom trust policies](#) in the IAM User Guide.

- a. In step 4 use the **trust policy** defined below.
- b. In step 11 add the **permission policy** that you created in the previous step.

The following is the **permission policy** for the IAM role. to allow for publishing to Amazon Connect.

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

The following is the **trust policy** for the IAM role, make the following changes:

- Replace *accountId* with the unique ID for your AWS account.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SMSVoice",
      "Effect": "Allow",
      "Principal": {
        "Service": "sms-voice.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "accountId"
        }
      }
    }
  ]
}
```



```
}  
]  
}
```

Keywords

A *keyword* is a specific word or phrase that a customer can send to your phone number to elicit a response, such as an informational message, opting-in to receive more messages, a special offer and other promotional and transactional messages. When your number receives a message that begins with a keyword, Amazon Pinpoint SMS responds with a customizable message.

For short codes, the console shows the keywords and responses that you initially define when you request a short code from AWS Support. AWS Support registers your keywords and responses with wireless carriers when it provisions your short code.

For long codes, the console shows the default keywords and responses.

Important

Your keywords and response messages must comply with the guidelines that are set by wireless carriers and wireless industry groups. Otherwise, following an audit, such groups might take action against your short code or long code. This action can include deny listing your number and blocking your messages.

A keyword can be between 1 and 30 characters in length and can't start or end with a space. Keywords are case insensitive.

Wireless carriers in the US require short codes to support the following keywords. In addition, AWS expects all long codes and short codes to support these keywords:

HELP

Used to obtain customer support. The response message must include customer-support contact information, as in the following example:

"For assistance with your account, call (206) 555-0199."

STOP

Used to opt out of receiving messages from your number. In addition to *STOP*, your audience can use any supported opt-out keyword, such as *CANCEL* or *OPTOUT*. For a list of supported

opt-out keywords, see [Required opt-out keywords](#). After your number receives an SMS message that contains an opt-out keyword, Amazon Pinpoint SMS stops sending SMS messages from your account to the individual who opted out.

The response message must confirm that messages will stop being sent to the individual who opted out, as in the following example:

"You are now opted out and will no longer receive messages."

Note

If a recipient responds with one of these keywords as the first word of their message, Amazon Pinpoint SMS responds with the response for that keyword. For example, if a recipient responds to one of your messages with "Help me understand what this means," then Amazon Pinpoint SMS responds with the response that you specified for the HELP keyword.

Topics

- [Required opt-out keywords](#)
- [Keyword actions](#)
- [Manage keywords](#)

Required opt-out keywords

Where required by local laws and regulations (such as in the US and Canada), SMS and MMS recipients can use their devices to opt out by replying to the message with any of the following:

Note

You can add custom keywords to phone numbers and phone pools to opt-out.

- ARRET
- CANCEL
- END
- OPT-OUT

- OPTOUT
- QUIT
- REMOVE
- STOP
- TD
- UNSUBSCRIBE

To opt out, the recipient must reply to the same phone number that Amazon Pinpoint SMS used to deliver the message. After opting out, the recipient no longer receives SMS or MMS messages from your AWS account.

Note

For US toll-free numbers, opt-outs are managed at the carrier level. The only supported opt-out keyword for a US toll-free number is `STOP`. You can't add additional opt-out keywords, or change the response message that your recipients get when they opt-out. A user can resubscribe by sending a new message to the toll-free using either `UNSTOP` or `START` as the keyword.

To configure allowing a user to resubscribe add the keywords `UNSTOP`, `START` or both to your toll-free number and set the keyword action to `Opt-in`. For more information on adding keywords, see [Manage keywords](#).

Keyword actions

A keyword can have one of three actions associated with it. When a customer responds with the keyword the action will be performed.

- `Opt-out` – The recipient is added to the opt-out list and will not receive future messages.
- `Opt-in` – The recipient wants to receive future messages.
- `Automatic response` – A message is sent to the recipient.

Manage keywords

Use the Amazon Pinpoint SMS console or AWS CLI to customize the keyword responses for your phone number.

Add a keyword (Console)

Use the Amazon Pinpoint SMS console to add keywords to your pool.

Add a keyword

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone pools**.
3. On the **Phone Pools** page, choose the pool to add a keyword to.
4. On the **Keywords** tab, choose **Add keyword**.
5. In the **Custom Keyword** pane do the following:
 - **Keyword** – The new keyword to add.
 - **Response message** – The message to send back to the recipient.
 - **Keyword action** – The action to perform when the keyword is received.
6. Choose **Add keyword**.

Edit a keyword (Console)

Use the Amazon Pinpoint SMS console to edit keywords in your pool.

To edit a keyword

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone pools**.
3. On the **Phone Pools** page, choose the pool that contains the keyword.
4. On the **Keywords** tab, choose the keyword to edit and then **Edit keyword**.
5. In the **Custom Keyword** pane modify any of the following:
 - **Keyword** – The keyword to edit.
 - **Response message** – The message to send back to the recipient.
 - **Keyword action** – The action to perform when the keyword is received.
6. Choose **Save keyword**.

Delete a keyword (Console)

Use the Amazon Pinpoint SMS console to delete keywords in your pool.

Note

Required opt-out keywords can't be deleted.

To delete a keyword

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone pools**.
3. On the **Phone Pools** page, choose the pool that contains the keyword.
4. On the **Keywords** tab, choose the keyword and then **Remove keyword**.

Add or edit a keyword (AWS CLI)

You can use the [put-keyword](#) command to create a new keyword or edit. If the keyword already exists then it will be over written.

To create a keyword, run the following command in the AWS CLI:

```
$ aws pinpoint-sms-voice-v2 put-keyword \  
> --origination-identity OriginationIdentity \  
> --keyword Keyword \  
> --keyword-message KeywordMessage \  
> --keyword-action KeywordAction
```

In the preceding command, make the following changes:

- Replace *OriginationIdentity* with the unique ID or Amazon Resource Name (ARN) of the pool that you want to add the keyword to.
- Replace *Keyword* with the new keyword.
- Replace *KeywordMessage* with the message to use when responding to the keyword.
- Replace *KeywordAction* the action (AUTOMATIC_RESPONSE, OPT_OUT, OPT_IN) to perform when the keyword is received.

List keywords (AWS CLI)

You can use the [describe-keywords.html](#) command to view information about the keywords associated with an origination identity.

To view a list of keywords using the AWS CLI at the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 describe-keywords \  
> --origination-identity OriginationIdentity
```

In the preceding command, make the following changes:

Replace *OriginationIdentity* with the unique ID or Amazon Resource Name (ARN) of the phone number or sender ID that you want a list of keywords from.

Delete a keyword (AWS CLI)

You can use the [delete-keyword](#) CLI to delete a keyword.

At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 delete-keyword \  
> --origination-identity OriginationIdentity \  
> --keyword Keyword
```

In the preceding command, make the following changes:

- Replace *OriginationIdentity* with the unique ID or Amazon Resource Name (ARN) of the phone number or sender ID that you want to remove the keyword from.
- Replace *Keyword* with the keyword to delete.

Opt-out list

An *opt-out list* is list of destination phone numbers that should not have messages sent to them. When you send SMS messages, destination identities are automatically added to the opt-out list if they reply to your origination number with the keyword STOP (unless you enable the self-managed opt-out option). If you attempt to send a message to a destination number that is on an opt-out list, and the opt-out list is associated with the pool used to send the message, Amazon Pinpoint SMS doesn't attempt to send the message.

Topics

- [Manage opt-out lists](#)
- [Self managed opt-outs](#)

Manage opt-out lists

By default, when a pool is created it is assigned to the *Default* opt-out list. Pools can share the same opt-out list. When you change a pool's opt-out list any recipients who previously opt-out might not be in the new list and start to receive messages. For more information on adding or removing destination phone numbers from an opt-out list, see [Managing opt-out list phone numbers](#).

Change opt-out list (Console)

To change the opt-out list using the Amazon Pinpoint SMS console, follow these steps:

Change opt-out list

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone pools**.
3. On the **Phone Pools** page, choose the pool.
4. On the **Opt-out list** tab, choose **Edit settings**.
 - **Create a new opt-out list** – Create a new empty opt-out list and enter a friendly name.
 - **Choose an existing opt-out list** – Choose a previously created opt-out list from the dropdown.
5. (Optional) To enable self-managed opt-outs choose **Enable self-managed opt-out**.
6. Choose **Save changes**.

Change opt-out list (AWS CLI)

You can use the [update-pool](#) command to change the opt-out list used by the pool.

At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 update-pool --pool-id poolId --opt-out-list-name OptOutListName
```

In the preceding command, make the following changes:

- Replace *poolId* with the poolID or Amazon Resource Name (ARN) of the pool.
- Replace *OptOutListName* with the Amazon Resource Name (ARN) or opt-out list name.

Self managed opt-outs

By default, when a customer sends a message that begins with *HELP* or *STOP* to one of your dedicated numbers, Amazon Pinpoint SMS automatically replies with a customizable message. In the case of incoming *STOP* messages, Amazon Pinpoint SMS also opts the customer out of receiving future SMS messages. If you prefer to manage *HELP* and *STOP* responses by using a service other than Amazon Pinpoint SMS, you can enable self-managed opt-outs.

When you enable this feature, there are three changes to the way that Amazon Pinpoint SMS handles incoming messages that your customers sends. First, it stops sending automatic responses to incoming *HELP* and *STOP* messages. Second, Amazon Pinpoint SMS stops automatically opting your customers out of receiving future SMS and MMS messages when they send a *STOP* message. And finally, it routes incoming *HELP* and *STOP* messages to the Amazon SNS topic that you use to receive two-way SMS messages, rather than responding to the sender automatically.

If you enable this feature, you're responsible for responding to *HELP* and *STOP* requests. You're also responsible for tracking and honoring opt-out requests.

Important

Many countries, regions, and jurisdictions impose severe penalties for sending unwanted SMS messages. If you enable this feature, make sure you have systems and processes in place for capturing and managing opt-out requests.

Note

To enable self-managed opt-outs for a pool, you must first enable two-way SMS messaging. Self-managed opt-outs are not supported when using Amazon Connect for two-way SMS. For more information on using Amazon Connect with two-way SMS messaging, see [Set up SMS messaging](#) in the *Amazon Connect administrator guide*.

Turn on self managed opt-outs (Console)

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone pools**.
3. On the **Phone Pools** page, choose the pool.
4. On the **Opt-out list** tab, choose **Edit settings**.
5. On the **Opt-out management** page, choose **Enable self-managed opt-out** and then **Save changes**.

How to turn on shared routes

In some countries, Amazon Pinpoint SMS maintains a pool of shared origination identities. When you activate shared routes, Amazon Pinpoint SMS makes an effort to deliver your message using one of the shared identities. The origination identity could be a sender ID, long code or short code and could vary within each country. When shared routes uses a sender ID as the origination identity, the sender ID will be a generic sender ID, such as NOTICE. Shared identities are unavailable in some countries, including the United States.

Note

Shared routes can be subject to increased downstream filtering and dedicated routes, where available, are preferred.

Turn on shared routes (AWS Management Console)

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone pools**.
3. On the **Phone Pools** page, choose the pool that will have shared routes enabled.
4. On the **Shared routes** tab, choose the **Edit settings** button.
5. Choose **Enable shared routes** and then **Save changes**.

Deletion protection

When you turn on deletion protection you will not be able to delete the pool until deletion protection is disabled. By default deletion protection is disabled.

Enable deletion protection (Console)

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone pools**.
3. On the **Phone Pools** page, choose the phone pool that will have deletion enabled.
4. On the **Deletion protection** tab, choose **Edit settings**.
5. Choose **Enable deletion protection** and then **Save changes**.

Tags

Tags are pairs of keys and values that you can optionally apply to your AWS resources to control access or usage. To change the name of a Pool by editing the value of the Name key/value pair.

Manage tags (Console)

Use the Amazon Pinpoint SMS console to add or edit a Tag in your pool.

Manage tags (Console)

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone pools**.
3. On the **Phone Pools** page, choose the phone pool to add a tag to.
4. On the **Tags** tab, choose **Manage tags**.
 - **Add a tag** – In **Manage tags**, choose **Add new tag** to create a new blank key/value pair.
 - **Delete a tag** – In **Manage tags**, choose **Remove** next to the key/value pair.
 - **Edit a tag** – In **Manage tags**, choose the **Key** or **Value** and edit the text.
5. Choose **Save changes**.

Manage tags (AWS CLI)

Use the AWS CLI to add or edit a Tag.

```
$ aws pinpoint-sms-voice-v2 tag-resource \  
  --resource-arn resource-arn \  
  --tags tags={key1=value1,key2=value2}
```

In the preceding example, do the following:

- Replace *resource-arn* with the Amazon Resource Name (ARN) that you want to add the tags to.
- Replace *key1* and *key2* with the keys of the tags that you want to add to the resource.
- Replace *value1* and *value2* with the values of the tags that you want to add for the respective keys.

Use the AWS CLI to delete a Tag.

```
$ aws pinpoint-sms-voice-v2 untag-resource \  
  --resource-arn resource-arn \  
  --tag-keys tags={key1=value1,key2=value2}
```

In the preceding example, do the following:

- Replace *resource-arn* with the Amazon Resource Name (ARN) that you want to remove the tag from.
- Replace *key1* and *key2* with the keys of the tags that you want to remove.
- Replace *value1* and *value2* with the values of the tags that you want to remove.

Phone numbers

A phone number is an identity that your recipients see on their devices when you send them an SMS or MMS message. There are several types of identities, including long codes (standard phone numbers that typically have 10 or more digits), 10 digit long codes (10DLC), toll free numbers (TFN) and short codes (phone numbers that contain between four and seven digits).

Phone numbers are resources that are unique to each AWS Region, so they can't be shared across AWS Regions. You can grant cross AWS account and AWS Region access to phone numbers. Dedicated phone numbers are country-specific. You can't request a dedicated phone number for one country but then use it as an identity for another country.

For example if your use case requires you to send message to the United States and Canada you should provision origination identities for both of those countries. You do not need to provision the origination identities in AWS Regions that are local to that country. You could provision both origination identities in US West (Oregon). As another example if your use case requires you to

send message to the United States and India you might want to provision the origination identities in AWS Regions that are geographically close to their message destinations to reduce latency. For more information see the [Amazon Pinpoint Resilient Architecture Guide](#).

There are several guidelines to consider when you're deciding what type of origination identity to use:

- Sender IDs are a great option for one-way use cases. However, they're not available in all countries.
- Short codes are a great option for two-way use cases. If you have to choose between using a short code or a long code, you should choose the short code.
- In some countries (such as India and Saudi Arabia), long codes can be used to receive incoming messages, but can't be used to send outgoing messages. You can use these inbound-only long codes to provide your recipients with a way to opt out of messages that you send using a Sender ID.
- In some countries, we maintain a pool of shared routes. If you send messages to recipients in a particular country, but you don't have a dedicated origination identity in that country, we make an effort to deliver your message using one of these shared identities. Shared identities are unavailable in some countries, including the United States and China.
- The mobile industry changes rapidly. In many countries, there is a trend toward increased regulation of commercial SMS messages. Carriers can, with little or no warning, decide to disallow messages sent from shared origination identities. If this happens, we will attempt to tell you about these changes with as much advance warning as possible. However, carriers generally provide us with little advance notice of these changes. For these reasons, dedicated origination identities are always preferred to shared ones.

Topics

- [SMS and MMS country capabilities and limitations](#)
- [Supported countries and regions for voice](#)
- [Request a phone number](#)
- [Releasing a phone number from your Amazon Pinpoint SMS account.](#)
- [Two-way SMS messaging](#)
- [Keywords](#)
- [Opt-out list](#)

- [Deletion protection](#)
- [Tags](#)

SMS and MMS country capabilities and limitations

Amazon Pinpoint SMS is currently unable to send SMS or MMS messages to a small number of countries, including Cuba, Iran, North Korea, Syria, and Sudan. For a complete list of countries and regions that you can send SMS messages to, see [Supported countries and regions for SMS messaging](#) and [Supported countries and regions for MMS messaging](#).

Most countries and regions place restrictions on the type of content that you can send using SMS. These restrictions vary, but the following types of content are restricted in most countries or regions:

- Pornographic content
- Content that is profane or hateful
- Content that depicts or endorses violence
- Content that endorses illegal drugs

In many countries and regions, if a customer receives restricted content and complains to a mobile carrier or regulatory agency, the sender might be subject to fines and penalties. Governments of a few countries and regions actively filter all incoming messages to remove content that they deem offensive or inappropriate. Always familiarize yourself with the laws and regulations about sending commercial SMS or MMS messages for the countries and regions where your customers are located.

Each country might also have additional capabilities and limitations when using SMS or MMS with Amazon Pinpoint SMS. These capabilities and limitations are described in the following topics.

Note

Two-way SMS is only available in certain countries and regions. For more information about two-way SMS support by country or region, see [Supported countries and regions for SMS messaging](#).

Topics

- [Supported countries and regions for SMS messaging](#)

Supported countries and regions for SMS messaging

You can use Amazon Pinpoint SMS to send SMS messages to the countries, regions, and territories listed in the following table. This table also lists the countries and regions that support Sender IDs and two-way SMS messaging.

If you are unsure of which origination identity will work best for you then see [Choosing a phone number or sender ID](#) for each origination types advantages and disadvantages. Depending on your use case you can also use [General considerations for choosing an origination identity](#), [Choosing an origination identity for one-way messaging use cases](#) and [Choosing an origination identity for two-way messaging use cases](#) to help choose the correct origination identity for your use case.

Before you can use two-way SMS messaging to receive messages, you have to obtain either a dedicated short code or a dedicated long code for the SMS channel.

Note

You can purchase long codes for some countries directly through the Amazon Pinpoint SMS console. The long codes that you purchase through the console are intended for use with the voice channel. However, if you purchase a long code that is based in the United States (including Puerto Rico) or Canada, you can also use it to send SMS messages.

Country or region	ISO code	Dialing code	Supports short codes	Supports long codes	Supports Sender IDs	Supports two-way SMS
A						
Afghanistan	AF	93	No	No	Yes	No
Albania	AL	355	No	No	Yes	No
Algeria	DZ	213	No	No	Yes	No
Andorra	AD	376	No	No	Yes	No
Angola	AO	244	No	No	Yes	No

Country or region	ISO code	Dialing code	Supports short codes	Supports long codes	Supports Sender IDs	Supports two-way SMS
Anguilla	AI	1-264	No	No	Yes	No
Antigua and Barbuda	AG	1-268	No	No	Yes	No
Argentina	AR	54	Yes	No	No	No
Armenia	AM	374	No	No	Yes	No
Aruba	AW	297	No	No	Yes	No
Australia	AU	61	No	Yes	Registration required ¹	Yes
Austria	AT	43	Yes	Yes	Yes	Yes
Azerbaijan	AZ	994	No	No	Yes	No
B						
Bahamas	BS	1-242	No	No	No	No
Bahrain	BH	973	No	No	Yes	No
Bangladesh	BD	880	No	No	Yes	No
Barbados	BB	1-246	No	No	Yes	No
Belarus	BY	375	No	No	Registration required ¹	No
Belgium	BE	32	Yes	Yes	No	Yes

Country or region	ISO code	Dialing code	Supports short codes	Supports long codes	Supports Sender IDs	Supports two-way SMS
Belize	BZ	501	No	No	Yes	No
Bermuda	BM	1-441	No	No	Yes	No
Bhutan	BT	975	No	No	Yes	No
Bolivia	BO	591	No	No	Yes	No
Bosnia and Herzegovina	BA	387	No	No	Yes	No
Botswana	BW	267	No	No	Yes	No
Brazil	BR	55	Yes	No	No	Yes
Brunei	BN	673	No	No	Yes	No
Bulgaria	BG	359	Yes	No	Yes	Yes
Burkina Faso	BF	226	No	No	Yes	No
Burundi	BI	257	No	No	Yes	No
C						
Cambodia	KH	855	No	No	Yes	No
Cameroon	CM	237	Yes	No	Yes	Yes
Canada	CA	1	Yes	Yes	No	Yes
Cape Verde	CV	238	No	No	Yes	No
Cayman Islands	KY	1-345	No	No	No	No

Country or region	ISO code	Dialing code	Supports short codes	Supports long codes	Supports Sender IDs	Supports two-way SMS
Central African Republic	CF	236	No	No	Yes	No
Chad	TD	235	No	No	Yes	No
Chile	CL	56	Yes	Yes	No	Yes
China	CN	86	Yes	No	No 2	Yes
Colombia	CO	57	No	Yes	No	Yes
Comoros	KM	269	No	No	Yes	No
Cook Islands	CK	682	No	No	Yes	Yes
Costa Rica	CR	506	Yes	Yes	No	Yes
Croatia	HR	385	Yes	No	Yes	Yes
Cyprus	CY	357	No	No	Yes	No
Czechia (Czech Republic)	CZ	420	No	Yes	Yes	Yes
D						
Democratic Republic of the Congo	CD	243	No	No	Yes	No
Denmark	DK	45	Yes	Yes	Yes	Yes

Country or region	ISO code	Dialing code	Supports short codes	Supports long codes	Supports Sender IDs	Supports two-way SMS
Djibouti	DJ	253	No	No	Yes	No
Dominica	DM	1-767	No	No	Yes	No
Dominican Republic	DO	1-809, 1-829, 1-849	Yes	No	No	Yes
E						
Ecuador	EC	593	Yes	No	No	Yes
Egypt	EG	20	Yes	No	Registration required ¹	Yes
El Salvador	SV	503	No	No	No	No
Equatorial Guinea	GQ	240	No	No	Yes	No
Eritrea	ER	291	No	No	Yes	No
Estonia	EE	372	No	Yes	Yes	Yes
Eswatini	SZ	268	Yes	No	Yes	Yes
Ethiopia	ET	251	No	No	Yes	No
F						
Faroe Islands	FO	298	No	No	Yes	No
Fiji	FJ	679	No	No	Yes	No

Country or region	ISO code	Dialing code	Supports short codes	Supports long codes	Supports Sender IDs	Supports two-way SMS
Finland	FI	358	Yes	Yes	Yes	Yes
France	FR	33	Yes	No	Yes	Yes
French Guiana	GF	594	No	No	Yes	No
French Polynesia	PF	689	No	No	Yes	No
G						
Gabon	GA	241	No	No	Yes	No
Gambia	GM	220	No	No	Yes	No
Georgia	GE	995	No	No	Yes	No
Germany	DE	49	Yes	Yes	Yes	Yes
Ghana	GH	233	No	Yes	Yes	Yes
Gibraltar	GI	350	No	No	Yes	No
Greece	GR	30	No	Yes	Yes	Yes
Greenland	GL	299	No	No	Yes	No
Grenada	GD	1-473	No	No	Yes	No
Guadeloupe	GP	590	No	No	Yes	No
Guam	GU	1-671	No	Yes	No	Yes
Guatemala	GT	502	No	Yes	No	Yes

Country or region	ISO code	Dialing code	Supports short codes	Supports long codes	Supports Sender IDs	Supports two-way SMS
Guernsey	GG	44-1481	No	No	Yes	No
Guinea	GN	224	No	No	Yes	No
Guinea-Bissau	GW	245	No	No	Yes	N/A
Guyana	GY	592	No	No	Yes	No
H						
Haiti	HT	509	No	No	Yes	No
Honduras	HN	504	No	Yes	Yes	Yes
Hong Kong	HK	852	No	Yes	Yes	Yes
Hungary	HU	36	No	Yes	No	Yes
I						
Iceland	IS	354	No	No	Yes	No
India	IN	91	Yes	No	Registration required ³	Yes
Indonesia	ID	62	No	No	Yes	No
Iraq	IQ	964	No	No	Yes	No
Ireland	IE	353	No	Yes	Yes	Yes
Isle of Man	IM	44-1624	No	No	Yes	No
Israel	IL	972	No	Yes	Yes	Yes

Country or region	ISO code	Dialing code	Supports short codes	Supports long codes	Supports Sender IDs	Supports two-way SMS
Italy	IT	39	Yes	Yes	Yes	Yes
Ivory Coast	CI	225	No	No	Yes	No
J						
Jamaica	JM	1-876	No	No	Yes	No
Japan	JP	81	Yes	Yes	Yes	Yes
Jersey	JE	44-1434	No	Yes	Yes	Yes
Jordan	JO	962	No	No	Registration required ¹	No
K						
Kazakhstan	KZ	7	No	No	Yes	No
Kenya	KE	254	Yes	Yes	Yes	Yes
Kosovo	XV	383	No	No	Yes	No
Kuwait	KW	965	No	Yes	Registration required ¹	Yes
Kyrgyzstan	KG	996	No	No	Yes	No
L						
Laos	LA	856	No	No	Yes	No
Latvia	LV	371	No	Yes	Yes	Yes

Country or region	ISO code	Dialing code	Supports short codes	Supports long codes	Supports Sender IDs	Supports two-way SMS
Lebanon	LB	961	No	No	Yes	No
Lesotho	LS	266	Yes	No	Yes	Yes
Liberia	LR	231	No	Yes	No	No
Libya	LY	218	No	No	Yes	No
Liechtenstein	LI	423	No	No	Yes	No
Lithuania	LT	370	No	Yes	Yes	Yes
Luxembourg	LU	352	No	Yes	Yes	Yes
M						
Macau	MO	853	No	No	Yes	No
Macedonia	MK	389	No	No	Yes	Yes
Madagascar	MG	261	No	No	Yes	No
Malawi	MW	265	Yes	No	Yes	Yes
Malaysia	MY	60	Yes	No	No	Yes
Maldives	MV	960	No	No	Yes	No
Mali	ML	223	No	No	Yes	No
Malta	MT	356	No	Yes	Yes	Yes

Country or region	ISO code	Dialing code	Supports short codes	Supports long codes	Supports Sender IDs	Supports two-way SMS
Marshall Islands, The	MH	692	No	No	No	No
Martinique	MQ	596	No	No	Yes	No
Mauritania	MR	222	No	No	Yes	No
Mauritius	MU	230	No	Yes	Yes	Yes
Mayotte	YT	262	No	No	Yes	No
Mexico	MX	52	Yes	No	No	Yes
Micronesia (Federated States of)	FM	691	No	No	No	No
Moldova	MD	373	No	No	Yes	No
Monaco	MC	377	No	No	No	No
Mongolia	MN	976	No	No	Yes	No
Montenegro	ME	382	No	No	Yes	No
Montserrat	MS	1-664	No	No	Yes	No
Morocco	MA	212	Yes	No	Yes	Yes
Mozambique	MZ	258	No	No	No	No
Myanmar	MM	95	No	Yes	Yes	Yes

N

Country or region	ISO code	Dialing code	Supports short codes	Supports long codes	Supports Sender IDs	Supports two-way SMS
Namibia	NA	264	Yes	No	Yes	Yes
Nepal	NP	977	No	No	Yes	No
Netherlands	NL	31	Yes	Yes	Yes	Yes
Netherlands Antilles	AN	599	No	No	Yes	No
New Caledonia	NC	687	No	No	Yes	No
New Zealand ⁶	NZ	64	Yes	No	No	Yes
Nicaragua	NI	505	No	No	No	No
Niger	NE	227	No	No	Yes	No
Nigeria	NG	234	Yes	No	Yes	Yes
Niue	NU	683	No	No	Yes	No
Norway	NO	47	No	Yes	Yes	Yes
O						
Oman	OM	968	No	No	Yes	No
P						
Pakistan	PK	92	No	Yes ⁴	Yes	No
Palestine	PS	970	No	No	Yes	No
Panama	PA	507	Yes	No	Yes	Yes

Country or region	ISO code	Dialing code	Supports short codes	Supports long codes	Supports Sender IDs	Supports two-way SMS
Papua New Guinea	PG	675	No	No	Yes	No
Paraguay	PY	595	No	No	No	No
Peru	PE	51	Yes	No	No	Yes
Philippines	PH	63	No	Yes ⁴	Registration required ¹	No
Poland	PL	48	No	Yes	Yes	Yes
Portugal	PT	351	No	Yes	Yes	Yes
Puerto Rico	PR	1-787, 1-939	Yes	Yes	No	Yes
Q						
Qatar	QA	974	Yes	No	Registration required ¹	Yes
R						
Republic of the Congo	CG	242	No	No	No	No
Réunion (France)	RE	262	No	No	Yes	No
Romania	RO	40	No	Yes	Yes	Yes

Country or region	ISO code	Dialing code	Supports short codes	Supports long codes	Supports Sender IDs	Supports two-way SMS
Russia	RU	7	Yes	No	Registration required ¹	Yes
Rwanda	RW	250	No	No	Yes	No
S						
Saint Kitts and Nevis	KN	1-869	No	No	No	No
Saint Lucia	LC	1-758	No	No	No	No
Samoa	WS	685	No	Yes	No	No
San Marino	SM	378	No	No	Yes	No
São Tomé and Príncipe	ST	239	No	No	Yes	No
Saudi Arabia	SA	966	No	Yes ⁴	Registration required ¹	No
Senegal	SN	221	No	No	Yes	No
Serbia	RS	381	Yes	No	Yes	Yes
Seychelles	SC	248	No	No	Yes	No
Sierra Leone	SL	232	No	No	Yes	No
Singapore	SG	65	Yes	Yes	Yes ⁵	Yes

Country or region	ISO code	Dialing code	Supports short codes	Supports long codes	Supports Sender IDs	Supports two-way SMS
Slovakia	SK	421	No	Yes	Yes	Yes
Slovenia	SI	386	No	No	Yes	No
Solomon Islands	SB	677	No	No	Yes	No
Somalia	SO	252	No	No	Yes	No
South Africa	ZA	27	Yes	Yes	No	Yes
South Korea	KR	82	No	No	No	No
South Sudan	SS	211	No	No	Yes	No
Spain	ES	34	Yes	Yes	Yes	Yes
Sri Lanka	LK	94	Yes	Yes	Registration required ¹	Yes
Suriname	SR	597	No	No	Yes	No
Sweden	SE	46	Yes	Yes	Yes	Yes
Switzerland	CH	41	No	No	Yes	No
T						
Taiwan	TW	886	No	Yes	No	Yes
Tajikistan	TJ	992	No	No	Yes	No

Country or region	ISO code	Dialing code	Supports short codes	Supports long codes	Supports Sender IDs	Supports two-way SMS
Tanzania	TZ	255	No	Yes	Yes	Yes
Thailand	TH	66	No	Yes	Registration required ¹	Yes
Timor-Leste	TL	670	No	No	Yes	No
Togo	TG	228	No	No	Yes	No
Tonga	TO	676	No	No	Yes	No
Trinidad and Tobago	TT	1-868	No	No	Yes	No
Tunisia	TN	216	No	No	Yes	No
Turkey	TR	90	No	No	Registration required ¹	No
Turkmenistan	TM	993	No	No	No	No
Turks and Caicos Islands	TC	1-649	No	No	Yes	No
Tuvalu	TC	688	No	No	Yes	No
U						
Uganda	UG	256	No	No	Yes	No

Country or region	ISO code	Dialing code	Supports short codes	Supports long codes	Supports Sender IDs	Supports two-way SMS
Ukraine	UA	380	No	Yes	Yes	Yes
United Arab Emirates (UAE)	AE	971	Yes	Yes ⁴	Registration required ¹	Yes
United Kingdom	GB	44	Yes	Yes	Yes	Yes
United States	US	1	Yes	Yes	No	Yes
Uruguay	UY	598	Yes	No	No	Yes
Uzbekistan	UZ	998	No	No	Yes	No
V						
Vanuatu	VU	678	No	No	Yes	No
Venezuela	VE	58	No	No	No	No
Vietnam	VN	84	No	No	Registration required ¹	No
Virgin Islands, British	VG	1-284	No	No	Yes	No
Virgin Islands, US	VI	1-340	No	Yes	No	Yes
W						

Country or region	ISO code	Dialing code	Supports short codes	Supports long codes	Supports Sender IDs	Supports two-way SMS
X						
Y						
Yemen	YE	967	No	No	Yes	No
Z						
Zambia	ZM	260	No	No	Yes	No
Zimbabwe	ZW	263	No	No	Yes	No

Notes

- Senders are required to use a pre-registered alphabetic Sender ID. To request a Sender ID from AWS Support, [Open an Amazon Pinpoint SMS support case to request a sender ID](#). Some countries require senders to meet specific requirements or abide by certain restrictions in order to obtain approval. In these cases, AWS Support might contact you for additional information after you submit your Sender ID request.
 - Senders are required to use a pre-registered template for each type of message that they plan to send. If a sender doesn't meet this requirement, their messages will be blocked. To register a template, [China SMS template registration process](#). Some countries require senders to meet additional, specific requirements or abide by certain restrictions in order to obtain approval. In these cases, AWS Support might ask you for additional information.
- Note**

In order to send messages to China, you must first register your templates through AWS Support for approval.
- Senders are required to use a pre-registered alphabetic Sender ID. Additional registration steps are required. For more information, see [India sender ID registration process](#).

4. Long codes in these countries only support inbound messaging. In other words, you can't use these long codes to send messages *to* your recipients, but you can use them to receive messages *from* your recipients. These long codes are useful way to allow your recipients to opt-out if you send messages using an alphabetic Sender ID, because Sender IDs only support outbound messages.
5. Amazon Pinpoint SMS can send SMS traffic to Singapore using a sender ID that has been registered on the Singapore SMS Sender ID Registry (SSIR), a registry created by the [Info-communications Media Development Authority \(IMDA\)](#) of Singapore. For more information on requirements to use a Singapore Sender ID, see [Singapore registration process](#). You can also send SMS traffic in Singapore using an alternative origination identity types such as Short Codes or Long Codes.

If you do not register your sender ID any message sent using a sender ID will have its ID changed to **LIKELY-SCAM** per regulatory agency rules. Regulators will filter or block unregistered traffic at their discretion.
6. Without a dedicated short code, Amazon Pinpoint SMS still attempts to send messages to New Zealand recipients using a shared pool of short codes. Due to local carrier restrictions around shared numbers, deliverability over these shared numbers are made on a best-effort basis. Therefore, Amazon Pinpoint SMS highly recommends procuring a dedicated short code for all traffic being sent to New Zealand. Messages containing URLs must be allow-listed through the dedicated short code process. For more information on purchasing a short code, see [How to request short codes for messaging](#).

Sender ID support

The following table explains which ID is displayed when you send SMS messages to countries where Sender IDs are supported, compared to those where Sender IDs aren't supported.

If the recipient is located...	And your SMS message...	The message is sent from...
In a country or region where Sender ID registration is required	Specifies a Sender ID that has been registered	The Sender ID.

If the recipient is located...	And your SMS message...	The message is sent from...
	Doesn't specify a Sender ID, or specifies an unregistered sender ID	Amazon Pinpoint SMS attempts to deliver the message with the Sender ID <i>NOTICE</i> . The message might not be received by the recipient based on the carrier requirements in the destination country or region.
In a country or region where Sender IDs are supported but Sender ID registration isn't required	Specifies a Sender ID	The Sender ID.
	Doesn't specify a Sender ID, but the account includes a dedicated phone number for the SMS channel in the destination country	The dedicated phone number.
	Doesn't specify a Sender ID, and the account doesn't include a dedicated phone number for the SMS channel in the destination country	<ul style="list-style-type: none"> • A random long or short code in countries and regions where Sender IDs aren't supported. • The word <i>NOTICE</i> in countries and regions where Sender IDs are supported.

If the recipient is located...	And your SMS message...	The message is sent from...
In a country or region where Sender IDs aren't supported	Specifies a Sender ID	Varies depending on the destination country. In some countries, your message is sent using a random long code. In other countries, your message is sent using a shared short code. In the United States, you can only send messages using dedicated phone numbers. If you don't have a dedicated US phone number, your message isn't delivered.
	Doesn't specify a Sender ID	Varies—see above.

Supported countries and regions for MMS messaging

You can use Amazon Pinpoint SMS to send MMS messages to the countries, regions, and territories listed in the following table.

Country or Region	ISO code	Dialing Code	Short codes support MMS	Long codes support MMS	Toll-free supports MMS	Sender ID support MMS
Canada	CA	1	Yes	Yes	No	No
United States	US	1	Yes	Yes	Yes	No

Supported countries and regions for voice

You can use the voice channel to send voice messages to recipients all around the world. However, in some countries and regions, you have to use a local phone number in order to make automated calls, such as the calls that you make by using the Amazon Pinpoint SMS voice channel. You can obtain local phone numbers, also referred to as *long codes*, directly from AWS for several countries and regions.

The following table lists the countries that you can obtain local phone numbers in to use the voice channel. If a country or region isn't listed in this table, you might still be able to send voice messages to recipients in that country or region.

If the value in the **Local address required** column is *Yes*, then you must request the long code by creating a case in the AWS Support Center Console. For more information, see . If the value in the **Local address required** column is *No*, you can lease local phone numbers directly through the Amazon Pinpoint SMS console.

Country or Region	Local address required?
Argentina	Yes
Australia	Yes
Austria	No
Bahrain	Yes
Barbados	No
Brazil	No
Bulgaria	Yes
Burkina Faso	No
Canada	No
Cayman Islands	No
Chile	No

Country or Region	Local address required?
Colombia	No
Cambodia	Yes
Croatia	Yes
Cyprus	No
Dominican Republic	No
Ecuador	No
El Salvador	No
Finland	Yes
Germany	Yes
Greece	Yes
Grenada	No
Guatemala	No
Hungary	Yes
Iceland	Yes
Indonesia	No
Ireland	Yes
Israel	No
Italy	Yes
Jamaica	No
Kazakhstan	Yes

Country or Region	Local address required?
Kenya	No
Latvia	Yes
Lithuania	No
Luxembourg	Yes
Mali	Yes
Mexico	Yes
Moldova	Yes
New Zealand	No
Nicaragua	Yes
Norway	Yes
Peru	No
Philippines	No
Poland	Yes
Puerto Rico	No
Romania	Yes
Slovakia	Yes
Slovenia	Yes
South Africa	Yes
Switzerland	Yes
Taiwan	Yes

Country or Region	Local address required?
Tajikistan	Yes
Thailand	Yes
Trinidad and Tobago	No
United Kingdom	No
United States	No
Uruguay	Yes
Venezuela	Yes
Vietnam	No

Request a phone number

Using the Amazon Pinpoint SMS console, we'll recommend one of the below origination identities depending on your use-case. Recommendations are based on your input criteria including if you require SMS, MMS, and/or voice capabilities, a two-way number, and estimate monthly messages.

Note

The following phone number types have to be requested in the Support Center Console.

- **Short codes** – [How to request short codes for messaging.](#)
- **Long codes** – [Requesting dedicated long codes for messaging.](#)

You can use either the Amazon Pinpoint SMS console or AWS CLI to request a new phone number.

Request a phone number (Console)

Important

To request a new phone number for the United States through the Pinpoint SMS console follow the directions in the [Request a phone number for the United States \(Console\)](#) tab.

To request a phone number using the Amazon Pinpoint SMS console, follow these steps:

Request a phone number (Console)

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone numbers** and then **Request originator**.
3. On the **Select country** page you must choose the **Message destination country** from the dropdown that messages will be sent to. Choose **Next**.
4. On the **Messaging use case** section, enter the following:
 - Under **Number capabilities**, choose any combination of available capabilities:

Important

Capabilities for SMS, MMS, and Voice can't be changed after the phone number has been purchased.

- **Text messages (SMS)** Choose this if you need SMS capabilities.
- **Text and media messages (SMS, MMS)** – Choose this if you need SMS and/or MMS capabilities.

Note

MMS capabilities are only available in certain countries and are only supported on certain origination types. **Text and media messages (SMS, MMS)** is only present if MMS is supported in the **Message destination country**. For more

information, see [Supported countries and regions for MMS messaging](#) and [Choosing a phone number or sender ID](#).

- **Text to audio messages (Voice)** – Choose this if you need voice capabilities.
 - Under **Estimated monthly message volume – optional**, choose the estimated number of SMS messages you will send each month.
 - For **Company headquarters - optional**, choose either of the following:
 - **Local** – Choose this if your company's headquarters is in the same country as your customers who will receive SMS messages. For example, you would choose this option if your headquarters is in the United States and your users who will receive messages are also in the United States.
 - **International** – Choose this if your company's headquarters is not in the same country as your customers who will receive SMS messages.
 - For **Two-way messaging**, choose **Yes** if you require two-way messaging.
5. Choose **Next**.
 6. Under **Select originator type**, choose either the recommend phone number type or one of the available number types. The available options are based on the use case information you filled out in the previous steps.
 - If you choose 10DLC and already have a registered campaign you can choose the campaign from the **Associate to registered campaign** to add the 10DLC phone number to the 10DLC campaign.
 - If the number type you want isn't available you can choose **Previous** to go back and modify your use case. Also check the [Supported countries and regions for SMS messaging](#) to make sure the originator type you want is supported in the destination country.
 - If you want to request a short code or long code you need to open a case with AWS Support. For more information, see [How to request short codes for messaging](#) and [Requesting dedicated long codes for messaging](#).
 7. Choose **Next**.
 8. On **Review and request** you can verify and edit your request before submitting it. Choose **Request**.
 9. A **Registration Required** window might appear depending on the type of phone number you requested. Your phone number or sender ID is associated with this registration and

can't send messages until your registration has been approved. For more information about registrations requirements see [Registrations](#).

- a. For **Registration form name** enter a friendly name.
- b. Choose **Begin registration** to finish registering the phone number or **Register later**.

 **Important**

Your phone number or sender ID can't send messages until your registration has been approved.

You are still billed the recurring monthly lease fee for the phone number regardless of registration status. For more information about registrations requirements see [Registrations](#).

Request a phone number for the United States (Console)

 **Important**

Follow these directions to request a new phone number for the United States through the Pinpoint SMS console.

Before requesting a 10DLC phone number you must have an approved 10DLC registered brand and 10DLC registered campaign to associate with the 10DLC phone number.

For more information on registering a 10DLC registered brand and 10DLC registered campaign, see [10DLC brand registration form](#) and [10DLC campaign registration form](#).

The **Messaging capabilities** (SMS, MMS, or VOICE) are specified in the 10DLC registered campaign and applied to your 10DLC phone number request.

Request a phone number for the United States (Console)

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone numbers** and then **Request originator**.
3. On the **Select country** page you must choose the **United States (US)** from the **Message destination country** dropdown. Choose **Next**.
4. On the **Messaging use case** section, enter the following:

- Under **Estimated monthly message volume – optional**, choose the estimated number of SMS messages you will send each month.
 - For **Company headquarters – optional**, choose either of the following:
 - **Local** – Choose this if your company's headquarters is in the same country as your customers who will receive SMS messages. For example, you would choose this option if your headquarters is in the United States and your users who will receive messages are also in the United States.
 - **International** – Choose this if your company's headquarters is not in the same country as your customers who will receive SMS messages.
 - For **Two-way messaging**, choose **Yes** if you require two-way messaging.
5. Choose **Next**.
 6. Under **Originator type**, choose either the recommended phone number type or one of the available number types. The available options are based on the use case information you filled out in the previous steps.
 - For a 10DLC phone number you have to choose the registered brand and registered campaign to associate with the 10DLC phone number request.
 - Use **Associate to registered brand** to choose a brand.
 - Use **Associate to registered campaign** to choose a campaign.
 - If you want to request a short code or long code you need to open a case with AWS Support. For more information, see [How to request short codes for messaging](#) and [Requesting dedicated long codes for messaging](#).
 7. Choose **Next**.
 8. On **Review and request** you can verify and edit your request before submitting it. Choose **Request**.
 9. A **Registration Required** window might appear depending on the type of phone number you requested. Your phone number or sender ID is associated with this registration and can't send messages until your registration has been approved. For more information about registrations requirements see [Registrations](#).
 - a. For **Registration form name** enter a friendly name.
 - b. Choose **Begin registration** to finish registering the phone number or **Register later**.

⚠ Important

Your phone number or sender ID can't send messages until your registration has been approved.

You are still billed the recurring monthly lease fee for the phone number regardless of registration status. For more information about registrations requirements see [Registrations](#).

Request a phone number (AWS CLI)

You can use the [request-phone-number](#) command to add new phone numbers to your account. Phone number availability and supported features vary by country.

⚠ Important

You might need to register the phone number or sender ID after you complete the request. You are still billed the recurring monthly lease fee for the phone number regardless of registration status. For more information about registrations requirements see [Registrations](#).

MMS capabilities are only available in some countries. For more information on supported countries for SMS and MMS, see [Supported countries and regions for SMS messaging](#) and [Supported countries and regions for MMS messaging](#).

To request a phone number

- At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 request-phone-number \  
> --iso-country-code XX \  
> --message-type TRANSACTIONAL \  
> --number-capabilities VOICE \  
> --number-type LONG_CODE \  
> --pool-id poolId \  
> --deletion-protection-enabled \  
> --opt-out-list-name optOutListName \  
> --registration-id C0123EX
```

In the preceding command, make the following changes:

- Replace *XX* with the two-letter ISO-3166 alpha-2 code for the country of the phone number (such as CA for Canada).
- If you want to use the phone number to send promotional or marketing-related content, replace *TRANSACTIONAL* with PROMOTIONAL. Otherwise, use TRANSACTIONAL.
- If you want to request a phone number for sending SMS messages, replace *VOICE* with SMS. You can request a phone number with SMS, MMS, and voice message capabilities by specifying SMS MMS VOICE.
- Replace *LONG_CODE* with the type of phone number you want to request. Acceptable values are LONG_CODE, TOLL_FREE, and TEN_DLC.
- Replace *poolId* with the ID or Amazon Resource Name (ARN) of the pool that you want to add the phone number to. This parameter is optional. If you don't want to add the phone number to a pool, omit this parameter.
- If you want to enable deletion protection for this phone number, add the `--deletion-protection-enabled` parameter. Deletion protection is disabled by default. If deletion protection is enabled, you can't delete the phone number using the [ReleasePhoneNumber](#) API, unless you update the configuration of the phone number to disable this feature.
- Replace *optOutListName* with the name or ARN of the opt-out list that you want to associate with the phone number. This parameter is optional. If you don't want to associate the phone number with an opt-out list, omit this parameter.
- If you're requesting a phone number to use with a 10DLC campaign, replace *C0123EX* with the ID of the 10DLC campaign that you want to use.

 **Note**

If you plan to use a 10DLC phone number, you must first register your company and campaign. Currently, the only way to complete these registration processes is to use the Amazon Pinpoint SMS console. For more information about 10DLC registration, see [10DLC registration process](#).

If the number is successfully added to your account, you see output similar to the following:

```
{
  "PhoneNumberArn": "arn:aws:sms-voice:us-east-1:111122223333:phone-number/
phone-615790209ea34aea8da9b729fexample",
  "PhoneNumberId": "phone-615790209ea34aea8da9b729fexample",
  "PhoneNumber": "+12045550123",
  "Status": "PENDING",
  "IsoCountryCode": "CA",
  "MessageType": "TRANSACTIONAL",
  "NumberCapabilities": [
    "SMS"
  ],
  "NumberType": "LONG_CODE",
  "MonthlyLeasingPrice": "1.00",
  "TwoWayEnabled": false,
  "SelfManagedOptOutsEnabled": false,
  "OptOutListName": "Default",
  "DeletionProtectionEnabled": false,
  "CreatedTimestamp": 1645568542.0
}
```

Note

When you first purchase a phone number, the value of the Status attribute is PENDING. When the phone number is ready to use, the value of Status changes to ACTIVE.

If a phone number that meets the parameters you specified isn't available, the request fails with an error.

Modify phone number capabilities (AWS CLI)

After you request a phone number, you can use the [update-phone-number](#) CLI to change the settings of that phone number, or to enable additional features. You can change several phone number settings, including the pool and opt-out list that are associated with the phone number, as well as the deletion protection setting.

An example of an additional feature that you can enable by updating a phone number is two-way messaging. Support for two-way messaging varies depending on which country you plan to send messages to. For a list of supported countries, see [Supported countries and regions for SMS messaging](#).

```
$ aws pinpoint-sms-voice-v2 update-phone-number \  
> --phone-number-id phone-d2b0f5dd4fd14ebdb2a3b9128example \  
> --deletion-protection-enabled true \  
> --opt-out-list-name optOutListName \  
> --self-managed-opt-outs-enabled true \  
> --two-way-enabled true \  
> --two-way-channel-arn arn:aws:sns:us-east-1:111122223333:MyTopic
```

In the preceding command, do the following:

- Replace *phone-d2b0f5dd4fd14ebdb2a3b9128example* with the PhoneNumberID or the Amazon Resource Name (ARN) of the phone number that you want to update. You can find both of these values by using the DescribePhoneNumbers operation.
- Replace *optOutListName* with the name of the opt-out list that you want to associate with this phone number.
- If you want to disable the deletion protection feature, change the value of the DeletionProtectionEnabled parameter to false.
- If you want to self-managed SMS opt-outs feature, change the value of the SelfManagedOptOutsEnabled parameter to false.
- If you want to disable two-way SMS messaging for this phone number, change the value of the TwoWayEnabled parameter to false.
- If you enable the two-way messaging feature for the phone number, you must specify the ARN of an Amazon SNS topic. Replace *arn:aws:sns:us-east-1:111122223333:MyTopic* with the ARN of the Amazon SNS topic that you want to use. When you receive incoming messages, they are sent to the topic that you specify.

The PhoneNumberId parameter is the only required parameter for this command. You can omit any of the other parameters if you don't want to change the corresponding settings.

List phone numbers (AWS CLI)

You can use the [describe-phone-numbers](#) to get more information about the origination phone numbers in your Amazon Pinpoint account.

To list all of the phone numbers in your account using the AWS CLI

- At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 describe-phone-numbers
```

The output of this command includes details about all of the phone numbers in your account. You can also view information about specific phone numbers by including the `PhoneNumberId` parameter.

To view information about a specific phone number using the AWS CLI

- At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 describe-phone-numbers \  
> --phone-number-id phone-d2b0f5dd4fd14ebdb2a3b9128example
```

In the preceding example, replace *phone-d2b0f5dd4fd14ebdb2a3b9128example* with the `PhoneNumberID` or the Amazon Resource Name (ARN) of the phone number that you want to view more information about.

You can also use the `filter` parameter to filter the list of phone numbers based on criteria that you define. For example, you can filter by the country of the phone number, or by its capabilities (that is, whether it supports SMS, MMS, voice messages, or all).

To view a filtered list of phone numbers using the AWS CLI

- At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 describe-phone-numbers \  
> --filters Name=number-capability,Values=SMS \  
> --filters Name=iso-country-code,Values=CA
```

The filter `Name` can be any of the following values:

- `status` – The current status of the phone number, such as `ACTIVE`.
- `iso-country-code` – The two-character ISO-3166 alpha-2 code of the phone number's country.
- `message-type` – The type of messages that the phone number is used to send. Possible values are `TRANSACTIONAL` or `PROMOTIONAL`.

- `number-capability` – The messaging channels that the phone number supports. Possible values are SMS, MMS, and VOICE.
- `number-type` – The type of phone number, such as LONG_CODE, SHORT_CODE, or TOLL_FREE.
- `two-way-enabled` – A boolean that indicates whether or not two-way SMS messaging is enabled.
- `self-managed-opt-outs-enabled` – A boolean that indicates whether or not self-managed SMS opt-outs are enabled.
- `opt-out-list-name` – The name of the opt-out list associated with the phone number.
- `deletion-protection-enabled` – A boolean that indicates whether or not the phone number can be deleted using the `DeletePhoneNumber` operation.

Topics

- [Phone number status and capabilities](#)
- [How to request short codes for messaging](#)
- [Requesting dedicated long codes for messaging](#)

Phone number status and capabilities

This section explains how to check that status and capabilities of your phone number.

Phone number status

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone numbers**.
3. The following image shows the parts of the phone number status.

	Origination number ▾	Originator type ▾	Country ▾	Number st... ▾	Capabilities ▾	Pool ▾	Creation d... ▾
	+18007468122	Toll free	US	⌚ Pending	SMS, MMS, Voice	-	May 26, 2022 2:...
	+12024867888	Long code	US	⚠ Action required	SMS, MMS	View pool details	May 26, 2022 2:...
	+18773361234	Toll free	US	✅ Active	SMS	Add to phone p...	May 26, 2022 2:...
	+14157547877	Long code	CA	⌚ Pending	SMS, MMS, Voice	-	May 26, 2022 2:...
	+18007868888	Short code	US	✅ Active	SMS, Voice	View pool details	May 26, 2022 2:...

- **Origination number** – The numeric number that customers see on their handsets.

- **Origination type** – The type of origination number. This can be a long code, short code or toll-free.
- **Country** – The country or region the **Origination number** is provisioned from.
- **Number status** – The status of the **Origination number**. This can be Pending, Active or Action required.
- **Capabilities** – The capabilities of the **Origination number**. This can be a combination of SMS, MMS, or Voice.
- **Pool** – The pool, if any, that the **Origination number** is associated with.
- **Creation date** – The time the **Origination number** was requested.

When you first purchase a phone number, the phone number's **Number status** is PENDING. When the phone number is ready to use, the phone number's **status** is ACTIVE. If the phone number requires registration then that must be completed before the phone number's **Number status** is changed to ACTIVE.

How to request short codes for messaging

A short code is a number that you can use for high-volume SMS and MMS message sending. Short codes are often used for application-to-person (A2P) messaging, two-factor authentication (2FA), and marketing. A short code typically contains between three and seven digits, depending on the country that it's based in.

You can only use short codes to send messages to recipients in the same country where the short code is based. If your use case requires you to use short codes in more than one country, you must request a separate short code for each country that your recipients are located in.

For information about short code pricing, see [Amazon Pinpoint SMS pricing](#).

Important considerations

Before you request a short code, consider the following information:

- If you plan to use the short code to send messages that contain Protected Health Information (PHI), you should identify this purpose in the **Case description** field of your support case.
- Amazon Pinpoint SMS currently only supports standard short codes. Free-to-End-User (FTEU) short codes aren't supported.

- If you're new to SMS and MMS messaging with Amazon Pinpoint SMS, you should request a monthly SMS and MMS spending threshold that meets the expected demands of your SMS and MMS use case. By default, your monthly spending threshold is \$1.00 (USD). You can request to increase your spending threshold in the same support case that includes your request for a short code.

Step 1: Open a support case

The first step in requesting a short code is to open a Service Limit Increase case in the Support Center Console.

To request a short code

1. Open the Support Center Console at <https://console.aws.amazon.com/support/home>.
2. In the left hand navigation choose **Your support cases**.
3. Choose **Create case**.
4. In the **Looking for service quota increases?** window choose **Create a case instead**.


5.

Important

Some of the fields on this form are labelled "optional." However, you must provide *all* of the information listed above to begin the short code setup process.


- For **Service**, choose **Pinpoint SMS**.
- For **Provide a link to the site or app which will be sending SMS messages - optional**, provide information about the website, application, or service that will send SMS messages.
- For **What type of messages do you plan to send - optional**, choose the type of messages that you plan to send using your short code:
 - **One Time Password** – Messages that provide passwords that your customers use to authenticate with your website or application.
 - **Promotional** – Noncritical messages that promote your business or service, such as special offers or announcements.
 - **Transactional** – Important informational messages that support customer transactions, such as order confirmations or account alerts. Transactional messages must not contain promotional or marketing content.

- For **Which AWS Region will you be sending messages from - optional**, choose the AWS Region that you will be sending messages from.

 **Note**


A short code can only exist in one AWS Region. If you want to be able to use short codes in more than one AWS Region, you must request separate short codes for each Region.

- For **Which countries do you plan to send messages to - optional**, enter the country that you want to purchase short codes in.

 **Note**

Each short code is specific to a single country. For example, you can't use a United States–based short code to send messages to recipients with Canadian phone numbers.

- In the **How do your customers opt to receive messages from you - optional**, provide details about your opt-in process.
 - In the **Please provide the message template that you plan to use to send messages to your customers - optional** field, include the template that you will be using.
6. In the **Requests** section, do the following:
- For the **Region**, choose the AWS Region that you plan to send messages from.

 **Note**

The Region is required in the **Requests** section. Even if you provided this information in the **Case details** section you must also include it here.

- For **Resource Type**, choose **Dedicated SMS Short Codes**.
- For **Quota**, choose the message type that you plan to send using your short code.
 - **One Time Password/Two-Factor Authentication** – Messages that provide passwords that your customers use to authenticate with your website or application.
 - **Promotional/Marketing** – Noncritical messages that promote your business or service, such as special offers or announcements.

- **Transactional** – Important informational messages that support customer transactions, such as order confirmations or account alerts. Transactional messages must not contain promotional or marketing content.
- **Transactional/Notifications/OTP/2FA** – All message types.
- For **New quota value**, enter the number of short codes that you want to purchase for the target country and use case.

 **Note**

If you want to request a short code for a different country, or for a separate use case in the same country, open a separate case in the Support Center Console. By creating separate cases, all communications for a particular country or use case are restricted to a single AWS Support case, which reduces the potential for miscommunications.

7. Under **Case description**, for **Use case description**, provide details about your use case.
8. Under **Contact options**, for **Preferred contact language**, choose whether you want to receive communications for this case in **English** or **Japanese**.
9. When you finish, choose **Submit**.

AWS Support acknowledges your request within 24 hours of receipt. If we're able to provide you with a short code, we provide you with a short code registration form as an attachment to your AWS Support case. Complete the registration form in its entirety. The information in this form is required in order to set up a short code with the mobile carriers. For more information about completing this form, see [Obtaining a short code for sending text messages to US recipients](#) on the AWS Messaging and Targeting Blog. This blog post covers the process of applying for US short codes, but the information it provides is also useful when applying for short codes in other countries.

There is no Service Level Agreement for the time required to obtain a short code. The amount of time required depends on whether or not your use case is compliant with the requirements of the carriers. If the carriers do not think that your use case is compliant, they will reject your application and provide information about the reasons for the rejection. If this happens, you will find this information in your AWS Support case. You can address the issues with your application in your AWS Support case. When you do, we send this updated information back to the carriers so that they can reconsider your application.

The fees associated with using short codes begin immediately after we initiate your short code request with carriers. You're responsible for paying these charges, even if the short code hasn't been completely provisioned yet. In order to prevent our systems from being used to send unsolicited or malicious content, we must consider each request carefully. We might not be able to grant your request if your use case doesn't align with our policies.

Step 2: Update your SMS settings in the Amazon Pinpoint SMS console

After we notify you that your short code has been provisioned, complete the following steps.

Note

You can't complete this step until the short code request has been approved and the short code has been added to your AWS account.

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone number**.
3. On the **Phone number** page, choose the short code.
4. On the **Keywords** tab, verify that the responses for the *HELP* and *STOP* keywords match the values that you specified in your request.

Requesting dedicated long codes for messaging

A long code (also referred to as a long virtual number, or LVN) is a standard phone number that contains up to 12 digits, depending on the country that it's based in. Long codes are typically meant for low-volume, person-to-person communication. In some countries, you can use long codes for sending test messages, or for sending low volumes of messages to your customers. In other countries, including the United States, senders are prohibited from using long codes to send Application-to-Person (A2P) messages, which includes the messages that you send from Amazon Pinpoint SMS.

Note

If you're new to SMS messaging with Amazon Pinpoint SMS, you should also request a monthly SMS and MMS spending threshold that meets the expected demands of your SMS

and MMS use case. By default, your monthly spending threshold is \$1.00 (USD). For more information, see [Requesting increases to your monthly SMS, MMS, or Voice spending quota](#).

Requesting a long code

You can request a long code by opening a case in the AWS Support Center.


Important

To send messages to recipients in the United States or the US territories of Puerto Rico, US Virgin Islands, Guam and American Samoa, you must use either a short code, a 10DLC phone number, or a toll-free number. If you complete the following steps and request a long code for the United States or US territories of Puerto Rico, US Virgin Islands, Guam and American Samoa, your request will be rejected.

To request a dedicated long code by opening a case in the AWS Support Center

1. Open the Support Center Console at <https://console.aws.amazon.com/support/home>.
2. In the left hand navigation choose **Your support cases**.
3. Choose **Create case**.
4. In the **Looking for service quota increases?** window choose **Create a case instead**.
5.
 - For **Service**, choose **Pinpoint SMS**.
 - For **Provide a link to the site or app which will be sending SMS messages - optional**, provide information about the website, application, or service that will send SMS messages.
 - For **What type of messages do you plan to send - optional**, choose the type of message that you plan to send using your long code:
 - **One Time Password** – Messages that provide passwords that your customers use to authenticate with your website or application.
 - **Promotional** – Noncritical messages that promote your business or service, such as special offers or announcements.
 - **Transactional** – Important informational messages that support customer transactions, such as order confirmations or account alerts. Transactional messages must not contain promotional or marketing content.

- For **Which AWS Region will you be sending messages from - optional**, choose the region that you will be sending messages from.
 - For **Which countries do you plan to send messages to - optional**, enter the country or region that you want to purchase short codes in.
 - In the **How do your customers opt to receive messages from you - optional**, provide details about your opt-in process.
 - In the **Please provide the message template that you plan to use to send messages to your customers - optional** field, include the template that you will be using.
6. Under **Requests**, complete the following sections:
- For the **Region**, choose the AWS Region from which you will be sending messages.

 **Note**

The Region is required in the **Requests** section. Even if you provided this information in the **Case details** section you must also include it here.

- For **Resource Type**, choose **Dedicated SMS Long Codes**.
 - For **Quota**, choose the type of messages that you plan to send using your long code.
 - For **New quota value**, enter the number of long codes that you want to purchase.
7. Under **Case description**, for **Use case description**, provide details about your use case.
8. (Optional) If you want to submit any further requests, choose **Add another request**.
9. Under **Contact options**, for **Preferred contact language**, choose whether you want to receive communications for this case in **English** or **Japanese**.
10. When you finish, choose **Submit**.

After we receive your request, we provide an initial response within 24 hours. We might contact you to request additional information. Once approved, you can add keywords and response messages to your long code.

If we're able to provide you with a long code, we send you information about the costs associated with obtaining it. We also provide an estimate of the amount of time that's required to provision the long code. In many countries, we can provide you with a dedicated long code within 24 hours.

However, in some countries and regions, it can take several weeks to obtain a dedicated long code for the SMS channel.

In order to prevent our systems from being used to send unsolicited or malicious content, we must consider each request carefully. We might not be able to grant your request if your use case doesn't align with our policies.

Releasing a phone number from your Amazon Pinpoint SMS account.

If you don't need a phone number that you had previously requested through Amazon Pinpoint SMS anymore, you can release it from your Amazon Pinpoint SMS account. When you release a number, AWS stops charging you for it in your bill for the next calendar month.

Important

Releasing a phone number from your Amazon Pinpoint SMS account is permanent and can't be undone. If you release a phone number, you won't be able to obtain the same number again in the future.

Deletion protection has to be disabled before you can release a phone number. For more information on deletion protection, see [Deletion protection](#).

Release a phone number from your Amazon Pinpoint SMS account (Console)

To release a phone number from your Amazon Pinpoint SMS account using the Amazon Pinpoint SMS console, follow these steps:

Release a phone number (Console)

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone numbers**.
3. Choose the phone number that you want to release and then choose **Release phone number**.
4. On the **Release phone number** window enter **release** and choose **Release phone number**.

Release a phone number from your Amazon Pinpoint SMS account (AWS CLI)

You can use the [release-phone-number](#) CLI to *release* phone numbers from your account.

```
$ aws pinpoint-sms-voice-v2 release-phone-number \  
> --phone-number-id phoneNumberId
```

In the preceding command, replace *phoneNumberId* with the unique ID or Amazon Resource Name (ARN) of the phone number.

Two-way SMS messaging

Amazon Pinpoint SMS includes support for two-way SMS. When you set up two-way SMS, you can receive incoming messages from your customers. You can also use two-way messaging together with other AWS services, such as Lambda and Amazon Lex, to create interactive text messaging experiences.

When one of your customers sends a message to your phone number, the message body is sent to an Amazon SNS topic or Amazon Connect instance for processing.

Note

- Two-way SMS is only available in certain countries and regions. For more information about two-way SMS support by country or region, see [SMS and MMS country capabilities and limitations](#).
- Amazon Connect for two-way SMS is available in the AWS Regions listed in [Chat messaging: SMS subtype](#) in the *Amazon Connect Administrator Guide*.
- Two-way MMS is not supported but your phone number can still receive incoming SMS messages in response to an outbound MMS message.

Two-way SMS messaging (Console)

To enable two-way SMS using the Amazon Pinpoint SMS console, follow these steps:

Enable two-way SMS

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone numbers**.
3. On the **Phone numbers** page, choose a phone number.

4. On the **Two-way SMS** tab, choose the **Edit settings** button.
5. On the **Edit settings** page, choose **Enable two-way message**.
6. For **Destination type**, choose either **Amazon SNS** or **Amazon Connect**.
 - For Amazon SNS choose either **New Amazon SNS topic** or **Existing Amazon SNS topic** and then for **Two-way channel role**, choose either **Choose existing IAM role** or **Use Amazon SNS topic policies**.
 - **New Amazon SNS topic** – If you choose this option, Amazon Pinpoint SMS creates a topic in your account. The topic is automatically created with all of the required permissions. For more information on Amazon SNS topics see [Configuring Amazon SNS](#) in the [Amazon Simple Notification Service Developer Guide](#).
 - **Existing Amazon SNS topic** – If you choose this option, you must choose an existing Amazon SNS topic from the **Incoming messages destination** dropdown.
 - For **Two-way channel role**, choose either:
 - **Choose existing IAM role** – Choose an existing IAM policy to apply to the Amazon SNS topic. For example Amazon SNS policies see [IAM policies for Amazon SNS topics](#).
 - **Use Amazon SNS topic policies** – The Amazon SNS topic requires the appropriate Amazon SNS topic policy to grant access to Amazon Pinpoint SMS. For example Amazon SNS policies, see [Amazon SNS topic policies for Amazon SNS topics](#).
 - For Amazon Connect, in **Two-way channel role**, choose **Choose existing IAM roles**.
 - In the **Existing IAM roles** drop down choose an existing IAM role as the message destination. For example IAM policies, see [IAM policies for Amazon Connect](#) .
7. Choose **Save changes**.
8. *(Optional)* If you've chosen Amazon Connect as the **Destination type** then in the **Import Phone Number to Amazon Connect** window:
 - a. For the **Incoming messages destination** dropdown choose the Amazon Connect instance that will receive incoming messages.
 - b. Choose **Import Phone Number**.

Two-way SMS messaging (AWS CLI)

You can use the [update-phone-number](#) command to enable two-way SMS.

At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 update-phone-number \
> --phone-number-id PhoneNumber \
> --two-way-enabled True \
> --two-way-channel-arn TwoWayARN \
> --two-way-channel-role TwoChannelWayRole
```

In the preceding command, make the following changes:

- Replace *PhoneNumber* with the PhoneNumberID or Amazon Resource Name (ARN) of the of the phone number.
- Replace *TwoWayARN* with the Amazon Resource Name (ARN) to receive the incoming SMS messages. For example Amazon SNS policies, see [Amazon SNS topic policies for Amazon SNS topics](#). To set Amazon Connect as the inbound destination set *TwoWayARN* to `connect.region.amazonaws.com`. Replace *region* with the AWS Region the Amazon Connect instance is hosted in.
- Replace *TwoChannelWayRole* with the Amazon Resource Name (ARN) of the IAM role to use. For example SNS permission policies, see [IAM policies for Amazon SNS topics](#) and for example Amazon Connect policies, see [IAM policies for Amazon Connect](#). This parameter is only required if you choose to use IAM permission policies.

IAM policies for Amazon SNS topics

If you want Amazon Pinpoint SMS to use an existing IAM role or if you create a new role, attach the following policies to that role so that Amazon Pinpoint SMS can assume it. For information about how to modify the trust relationship of a role, see [Modifying a Role](#) in the [IAM user guide](#).

The following is the **trust policy** for the IAM role. In the following IAM policy, make the following changes:

- Replace *accountId* with the unique ID for your AWS account.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SMSVoice",
      "Effect": "Allow",
      "Principal": {
```

```

    "Service": "sms-voice.amazonaws.com"
  },
  "Action": "sts:AssumeRole",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "accountId"
    }
  }
}
]
}

```

The following is the **permission policy** for the IAM role. The `SMSVoiceAllowSNSPublish` Sid is a permission policy to allow for publishing to Amazon SNS topics and the `SMSVoiceAllowEncryptedSNSTopics` Sid is an option for encrypted Amazon SNS topics.

In the following IAM permission policy, make the following changes:

- Replace *partition* with the AWS partition that you use Amazon Pinpoint SMS in.
- Replace *region* with the AWS Region that you use Amazon Pinpoint SMS in.
- Replace *accountId* with the unique ID for your AWS account.
- Replace *snsTopicArn* with the Amazon SNS topics that will receive messages.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SMSVoiceAllowSNSPublish",
      "Effect": "Allow",
      "Action": "sns:Publish",
      "Resource": "arn:partition:sns:region:accountId:snsTopicArn",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "accountId"
        }
      }
    },
    {
      "Sid": "SMSVoiceAllowEncryptedSNSTopics",
      "Effect": "Allow",
      "Action": [

```

```

        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:aws:sns:topicArn":
"arn:partition:sns:region:accountId:snsTopicArn",
            "aws:CalledViaLast": "sns.amazonaws.com"
        }
    }
}
]
}

```

Amazon SNS topic policies for Amazon SNS topics

The Amazon SNS topic requires the appropriate topic policy to grant access to Amazon Pinpoint SMS if they are not provided in the *TwoChannelWayRole* parameter.

```

{
  "Effect": "Allow",
  "Principal": {
    "Service": "sms-voice.amazonaws.com"
  },
  "Action": "sns:Publish",
  "Resource": "snsTopicArn"
}

```

In the preceding example, make the following changes:

- Replace *snsTopicArn* with the Amazon SNS topic that will send and receive messages.

Note

Amazon SNS FIFO topics are not supported.

Although Amazon Pinpoint SMS data is encrypted, you can use Amazon SNS topics that are encrypted using AWS KMS keys for an additional level of security. This added security can be helpful if your application handles private or sensitive data.

You need to perform some additional setup steps to use encrypted Amazon SNS topics with two-way messaging.

The following example statement uses the, optional but recommended, `SourceAccount` and `SourceArn` conditions to avoid the confused deputy problem and only the Amazon Pinpoint SMS owner account has access. For more information on the confused deputy problem, see [The confused deputy problem](#) in the *IAM user guide*.

First, the key that you use must be *symmetric*. Encrypted Amazon SNS topics don't support asymmetric AWS KMS keys.

Second, the key policy must be modified to allow Amazon Pinpoint SMS to use the key. Add the following permissions to the existing key policy:

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": "sms-voice.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey*",
    "kms:Decrypt"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "accountId"
    },
    "ArnLike": {
      "aws:SourceArn": "arn:aws:sms-voice:region:accountId:*"
    }
  }
}
```

For more information about editing key policies, see [Changing a key policy](#) in the *AWS Key Management Service Developer Guide*.

For more information about encrypting Amazon SNS topics using AWS KMS keys, see [Enable compatibility between event sources from AWS services and encrypted topics](#) in the *Amazon Simple Notification Service Developer Guide*.

Example of a two-way SMS message payload for Amazon SNS topics

When your number receives an SMS message, Amazon Pinpoint SMS sends a JSON payload to an Amazon SNS topic that you designate. The JSON payload contains the message and related data, as in the following example:

```
{
  "originationNumber":"+14255550182",
  "destinationNumber":"+12125550101",
  "messageKeyword":"JOIN",
  "messageBody":"EXAMPLE",
  "inboundMessageId":"cae173d2-66b9-564c-8309-21f858e9fb84",
  "previousPublishedMessageId":"wJa1rXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
}
```

The incoming message payload contains the following information:

Property	Description
originationNumber	The phone number that sent the incoming message to you (in other words, your customer's phone number).
destinationNumber	The phone number that the customer sent the message to (your dedicated phone number).
messageKeyword	The registered keyword that's associated with your dedicated phone number.
messageBody	The message that the customer sent to you.
inboundMessageId	The unique identifier for the incoming message.
previousPublishedMessageId	The unique identifier of the message that the customer is responding to.

IAM policies for Amazon Connect

If you want Amazon Pinpoint SMS to use an existing IAM role or if you create a new role, attach the following policies to that role so that Amazon Pinpoint SMS can assume it. For information about how to modify an existing trust relationship of a role, see [Modifying a Role](#) in the *IAM user guide*.

To create new IAM polices, do the following:

1. Create a new **permission policy** by following the directions in [Creating policies using the JSON editor](#) in the IAM User Guide.
 - In step 4 use the **permission policy** defined below.
2. Create a new **trust policy** by following the directions in [Creating a role using custom trust policies](#) in the IAM User Guide.
 - a. In step 4 use the **trust policy** defined below.
 - b. In step 11 add the **permission policy** that you created in the previous step.

The following is the **permission policy** for the IAM role to allow for publishing to Amazon Connect.

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

The following is the **trust policy** for the IAM role, make the following changes:

- Replace *accountId* with the unique ID for your AWS account.

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "SMSVoice",
    "Effect": "Allow",
    "Principal": {
      "Service": "sms-voice.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "accountId"
      }
    }
  }
]
```

Keywords

A *keyword* is a specific word or phrase that a customer can send to your phone number to elicit a response, such as an informational message, opting-in to receive more messages, a special offer and other promotional and transactional messages. When your number receives a message that begins with a keyword, Amazon Pinpoint SMS responds with a customizable message.

For short codes, the console shows the keywords and responses that you initially define when you request a short code from AWS Support. AWS Support registers your keywords and responses with wireless carriers when it provisions your short code.

For long codes, the console shows the default keywords and responses.

Important

Your keywords and response messages must comply with the guidelines that are set by wireless carriers and wireless industry groups. Otherwise, following an audit, such groups might take action against your short code or long code. This action can include deny listing your number and blocking your messages.

A keyword can be between 1 and 30 characters in length and can't start or end with a space. Keywords are case insensitive.

Wireless carriers in the US require short codes to support the following keywords. In addition, AWS expects all long codes and short codes to support these keywords:

HELP

Used to obtain customer support. The response message must include customer-support contact information, as in the following example:

"For assistance with your account, call (206) 555-0199."

STOP

Used to opt out of receiving messages from your number. In addition to *STOP*, your audience can use any supported opt-out keyword, such as *CANCEL* or *OPTOUT*. For a list of supported opt-out keywords, see [Required opt-out keywords](#). After your number receives an SMS message that contains an opt-out keyword, Amazon Pinpoint SMS stops sending SMS messages from your account to the individual who opted out.

The response message must confirm that messages will stop being sent to the individual who opted out, as in the following example:

"You are now opted out and will no longer receive messages."

Note

If a recipient responds with one of these keywords as the first word of their message, Amazon Pinpoint SMS responds with the response for that keyword. For example, if a recipient responds to one of your messages with "Help me understand what this means," then Amazon Pinpoint SMS responds with the response that you specified for the HELP keyword.

Topics

- [Required opt-out keywords](#)
- [Keyword actions](#)
- [Manage keywords](#)

Required opt-out keywords

Where required by local laws and regulations (such as in the US and Canada), SMS and MMS recipients can use their devices to opt out by replying to the message with any of the following:

Note

You can add custom keywords to phone numbers and phone pools to opt-out.

- ARRET
- CANCEL
- END
- OPT-OUT
- OPTOUT
- QUIT
- REMOVE
- STOP
- TD
- UNSUBSCRIBE

To opt out, the recipient must reply to the same phone number that Amazon Pinpoint SMS used to deliver the message. After opting out, the recipient no longer receives SMS or MMS messages from your AWS account.

Note

For US toll-free numbers, opt-outs are managed at the carrier level. The only supported opt-out keyword for a US toll-free number is STOP. You can't add additional opt-out keywords, or change the response message that your recipients get when they opt-out. A user can resubscribe by sending a new message to the toll-free using either UNSTOP or START as the keyword.

To configure allowing a user to resubscribe add the keywords UNSTOP, START or both to your toll-free number and set the keyword action to Opt -in. For more information on adding keywords, see [Manage keywords](#).

Keyword actions

A keyword can have one of three actions associated with it. When a customer responds with the keyword the action will be performed.

- **Opt-out** – The recipient is added to the opt-out list and will not receive future messages.
- **Opt-in** – The recipient wants to receive future messages.
- **Automatic response** A message is sent to the recipient.

Manage keywords

Use the Amazon Pinpoint SMS console or AWS CLI to customize the keyword responses for your phone number.

Add a keyword (Console)

Use the Amazon Pinpoint SMS console to add keywords to your phone number.

Add a keyword

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone number**.
3. On the **Phone number** page, choose the phone number to add a keyword to.
4. On the **Keywords** tab, choose the **Add keyword** button.
5. In the **Custom Keyword** pane add the following:
 - **Keyword** – The new keyword to add.
 - **Response message** – The message to send back to the recipient.
 - **Keyword action** – The action to perform when the keyword is received.
6. Choose **Add keyword**.

Edit a keyword (Console)

Use the Amazon Pinpoint SMS console to edit keywords.

To edit a keyword

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.

2. In the navigation pane, under **Configurations**, choose **Phone number**.
3. On the **Phone number** page, choose the phone number that contains the keyword.
4. On the **Keywords** tab, choose the keyword to edit and then the **Edit keyword** button.
5. In the **Custom Keyword** pane modify any of the following:
 - **Keyword** – The keyword to change.
 - **Response message** – The message to send back to the recipient.
 - **Keyword action** – The action to perform when the keyword is received.
6. Choose **Save keyword**.

Delete a keyword (Console)

Use the Amazon Pinpoint SMS console to delete keywords.

Note

Required opt-out keywords can't be deleted.

To delete a keyword

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone numbers**.
3. On the **Phone numbers** page, choose the phone number that contains the keyword.
4. On the **Keywords** tab, choose the keyword to delete and then **Remove keyword**.

Add or edit a keyword (AWS CLI)

You can use the [put-keyword](#) command to create a new keyword or edit. If the keyword already exists then it will be over written.

To create a keyword, run the following command in the AWS CLI:

```
$ aws pinpoint-sms-voice-v2 put-keyword \  
> --origination-identity OriginationIdentity \  
> --keyword Keyword \  
>
```

```
> --keyword-message KeywordMessage \  
> --keyword-action KeywordAction
```

In the preceding command, make the following changes:

- Replace *OriginationIdentity* with the unique ID or Amazon Resource Name (ARN) of the phone number that you want to add the keyword to.
- Replace *Keyword* with the new keyword.
- Replace *KeywordMessage* with the message to use when responding to the keyword.
- Replace *KeywordAction* the action (AUTOMATIC_RESPONSE, OPT_OUT, OPT_IN) to perform when the keyword is received.

List keywords (AWS CLI)

You can use the [describe-keywords.html](#) command to view information about the keywords associated with an origination identity.

To view a list of keywords using the AWS CLI at the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 describe-keywords \  
> --origination-identity OriginationIdentity
```

In the preceding command, make the following changes:

Replace *OriginationIdentity* with the unique ID or Amazon Resource Name (ARN) of the phone number or sender ID that you want a list of keywords from.

Delete a keyword (AWS CLI)

You can use the [delete-keyword](#) command to delete a keyword.

At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 delete-keyword \  
> --origination-identity OriginationIdentity \  
> --keyword Keyword
```

In the preceding command, make the following changes:

- Replace *OriginationIdentity* with the unique ID or Amazon Resource Name (ARN) of the phone number or sender ID that you want to remove the keyword from.
- Replace *Keyword* with the keyword to delete.

Opt-out list

An *opt-out list* is a list of destination phone numbers that should not have messages sent to them. When you send SMS or MMS messages, destination identities are automatically added to the opt-out list if they reply to your origination number with the keyword STOP (unless you enable the self-managed opt-out option). If you attempt to send a message to a destination number that is on an opt-out list, and the opt-out list is associated with the phone number used to send the message, Amazon Pinpoint SMS doesn't attempt to send the message.

Manage opt-out lists

By default, when a phone number is created it is assigned to the *Default* opt-out list. For more information on adding or removing destination phone numbers from an opt-out list, see [Managing opt-out list phone numbers](#).

Create or change opt-out list (Console)

To change the opt-out list using the Amazon Pinpoint SMS console, follow these steps:

Create or change an opt-out list

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone numbers**.
3. On the **Phone numbers** page, choose the phone number.
4. On the **Opt-out list** tab, choose the **Edit settings** button.
5. For **Opt-out list**, choose either:
 - **Create a new opt-out list** – Create a new empty opt-out list. In **List name** enter a name for the opt-out list.
 - **Choose an existing opt-out list** – Choose a previously created opt-out list from the dropdown.
6. Choose **Save changes**.

Create an opt-out list (AWS CLI)

You can use the [create-opt-out-list](#) command to create an opt-out list.

At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 create-opt-out-list --opt-out-list-name OptOutListName
```

In the preceding command replace *OptOutListName* with the opt-out list name.

Change an opt-out list (AWS CLI)

You can use the [update-phone-number](#) command to change the opt-out list used by the phone number.

At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 update-phone-number --phone-number-id PhoneNumberid --opt-out-list-name OptOutListName
```

In the preceding command, make the following changes:

- Replace *PhoneNumberid* with the PhoneNumberId or Amazon Resource Name (ARN) of the phone number.
- Replace *OptOutListName* with the Amazon Resource Name (ARN) or opt-out list name.

Self managed opt-outs

By default, when a customer sends a message that begins with *HELP* or *STOP* to one of your dedicated numbers, Amazon Pinpoint SMS automatically replies with a customizable message. In the case of incoming *STOP* messages, Amazon Pinpoint SMS also opts the customer out of receiving future SMS messages. If you prefer to manage *HELP* and *STOP* responses by using a service other than Amazon Pinpoint SMS, you can enable self-managed opt-outs.

When you enable this feature, there are three changes to the way that Amazon Pinpoint SMS handles incoming messages that your customers sends. First, it stops sending automatic responses to incoming *HELP* and *STOP* messages. Second, Amazon Pinpoint SMS stops automatically opting your customers out of receiving future SMS messages when they send a *STOP* message. And finally, it routes incoming *HELP* and *STOP* messages to the Amazon SNS topic that you use to receive two-way SMS messages, rather than responding to the sender automatically.

If you enable this feature, you're responsible for responding to HELP and STOP requests. You're also responsible for tracking and honoring opt-out requests.

Important

Many countries, regions, and jurisdictions impose severe penalties for sending unwanted SMS messages. If you enable this feature, make sure you have systems and processes in place for capturing and managing opt-out requests.

Note

To enable self-managed opt-outs for a phone number, you must first enable two-way SMS messaging. Self-managed opt-outs are not supported when using Amazon Connect for two-way SMS. For more information on using Amazon Connect with two-way SMS messaging, see [Set up SMS messaging](#) in the *Amazon Connect administrator guide*.

Turn on self managed opt-outs (Console)

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone numbers**.
3. On the **Numbers** page, choose the phone number.
4. On the **Opt-out list** tab, choose the **Edit settings** button.
5. On the **Opt-out management** page, choose **Enable self-managed opt-out** and then **Save changes**.

Deletion protection

When you turn on deletion protection you will not be able to release the phone number until deletion protection is disabled. By default deletion protection is turned off.

Enable deletion protection (Console)

To change deletion protection using the Amazon Pinpoint SMS console, follow these steps:

Enable deletion protection (Console)

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Phone numbers**.
3. On the **Phone numbers** page, choose the phone number that will have deletion protection enabled.
4. On the **Deletion protection** tab, choose the **Edit settings** button.
5. Choose **Enable deletion protection** and then **Save changes**.

Enable deletion protection (AWS CLI)

You can use the [update-phone-number](#) command to enable deletion protection the phone number.

At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 update-phone-number --phonenumber-id PhoneNumberid --deletion-protection-enabled
```

In the preceding command, make the following changes:

- Replace *PhoneNumberid* with the PhoneNumberID or Amazon Resource Name (ARN) of the phone number.

Tags

Tags are pairs of keys and values that you can optionally apply to your AWS resources to control access or usage. Adding a tag to a resource can help you categorize and manage resources in different ways, such as by purpose, owner, environment, or other criteria. You can use tags to easily find existing resources, or to control which users can access specific resources.

Manage tags (Console)

Use the Amazon Pinpoint SMS console to add, edit or delete a Tag.

Manage tags (Console)

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.

2. In the navigation pane, under **Configurations**, choose **Phone numbers**.
3. On the **Phone numbers** page, choose the phone number to add a tag to.
4. On the **Tags** tab, choose **Manage tags**.
 - **Add a tag** – In **Manage tags**, choose **Add new tag** to create a new blank key/value pair.
 - **Delete a tag** – In **Manage tags**, choose **Remove** next to the key/value pair.
 - **Edit a tag** – In **Manage tags**, choose the **Key** or **Value** and edit the text.
5. Choose **Save changes**.

Manage tags (AWS CLI)

Use the AWS CLI to add or edit a Tag.

```
$ aws pinpoint-sms-voice-v2 tag-resource \  
  --resource-arn resource-arn \  
  --tags tags={key1=value1,key2=value2}
```

In the preceding example, do the following:

- Replace *resource-arn* with the Amazon Resource Name (ARN) that you want to add the tags to.
- Replace *key1* and *key2* with the keys of the tags that you want to add to the resource.
- Replace *value1* and *value2* with the values of the tags that you want to add for the respective keys.

Use the AWS CLI to delete a Tag.

```
$ aws pinpoint-sms-voice-v2 untag-resource \  
  --resource-arn resource-arn \  
  --tag-keys tags={key1=value1,key2=value2}
```

In the preceding example, do the following:

- Replace *resource-arn* with the Amazon Resource Name (ARN) that you want to remove the tag from.
- Replace *key1* and *key2* with the keys of the tags that you want to remove.
- Replace *value1* and *value2* with the values of the tags that you want to remove.

Sender IDs

A sender ID is an alphanumeric name that identifies the sender of an SMS message. When you send an SMS message using a sender ID, and the recipient is in an area where sender ID authentication is supported, your sender ID appears on the recipient's device instead of a phone number. A sender ID provides SMS recipients with more information about the sender than a phone number or short code provides. For example, a fictitious company Example Corp could use the sender ID EXAMPLECO

Sender IDs are supported in many countries and regions around the world. In some places, if you're a business that sends SMS messages to individual customers, you must use a sender ID that's pre-registered with a regulatory agency or industry group. For a complete list of countries and regions that support or require sender IDs, see [SMS and MMS country capabilities and limitations](#).

Advantages

Sender IDs provide the recipient with more information about the message sender. It's easier to establish your brand identity by using a sender ID than by using a short or long code. There's no additional charge for using a sender ID.

Disadvantages

Support and requirements for sender ID authentication aren't consistent across all countries or regions. Several major markets (including Canada, China, and the United States) don't support sender ID. In some areas, you must have your sender IDs pre-approved by a regulatory agency before you can use them.

Topics

- [Sender ID country capabilities and limitations](#)
- [Registered and dynamic sender IDs](#)
- [Considerations for a Sender ID](#)
- [Manage sender IDs](#)
- [Tags](#)

Sender ID country capabilities and limitations

For more information on which countries support sender IDs see the **Supports Sender IDs** column in [Supported countries and regions for SMS messaging](#).

Registered and dynamic sender IDs

Registered sender ID – A registered sender ID is registered with a regulatory agency or industry group. For a complete list of countries and regions that support or require sender IDs, see [Supported countries and regions for SMS messaging](#).

Dynamic sender ID – A dynamic sender ID does not have to be registered with a regulatory agency or industry group. Registration requirements can change quickly and it is recommended that you complete any optional registration for dynamic sender IDs. For a complete list of countries and regions that support or optionally have sender ID registration, see [Supported countries and regions for SMS messaging](#).

Considerations for a Sender ID

When you are creating a Sender ID you should consider the following:

- Choose a Sender ID that matches your company branding and SMS service or use case
- Numeric-only Sender IDs are not supported
- Amazon Pinpoint SMS sender ID supported characters (some countries might override these):
 - No special characters except for dashes (-)
 - No spaces
 - Valid characters: a-z, A-Z, 0-9
 - Minimum of 3 characters
 - Maximum of 11 characters
- If the country you're sending to requires registration you must submit a registration for each AWS Region you plan on sending from

Manage sender IDs

Before you request a sender ID verify that they are available, see [Supported countries and regions for SMS messaging](#).

Note

Some countries require you to register your sender ID or open a support case to request the sender ID.

- **India sender ID registration** – Register a sender ID for use in India. For more information on completing the registration for see [India sender ID registration process](#).
- **Singapore sender ID registration** – Register a sender ID in Singapore. For more information on completing the registration for see [Singapore registration form](#).
- **Request a Sender ID from AWS Support** Senders are required to use a pre-registered alphabetic sender ID. To request a Sender ID from AWS Support, [Open an Amazon Pinpoint SMS support case to request a sender ID](#). Some countries require senders to meet specific requirements or abide by certain restrictions in order to obtain approval. In these cases, AWS Support might contact you for additional information after you submit your sender ID request. For a list of countries that require a support ticket to request a sender ID, see the Supports Sender IDs column in [Supported countries and regions for SMS messaging](#).

Request a sender ID (Console)

To request a sender ID using the Amazon Pinpoint SMS console, follow these steps:

Request a sender ID

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Sender ID** and then **Request originator**.
3. On the **Select country** page you must choose the country from the dropdown that messages will be sent to.

Choose **Next** to continue defining the use case and for a suggested phone number or sender ID type.

4. On the **Messaging use case** section, enter the following:
 - Under **Number capabilities**, choose either **SMS**, **Voice** or both depending on your requirements.
 - **SMS** – Choose if you need SMS capabilities.
 - **Voice (text to audio)** – Choose if you need voice capabilities.
5. Under **Estimated monthly SMS message volume per month – optional**, choose the estimated number of SMS messages you will send each month.

6. For **Company headquarters - optional**, choose either of the following:
 - **Local** – Choose this if your companies headquarters is in the same country as your customers who will receive SMS messages. For example, you would choose this option if your headquarters is in the United States and your users who will receive messages are also in the United States.
 - **International** – Choose this if your companies headquarters is not in the same country as your customers who will receive SMS messages.
7. Choose **Next**.
8. Under **Originator type**, choose Sender ID.

If sender ID isn't available then choose **Previous** to go back and modify your use case. Also check the [Supported countries and regions for SMS messaging](#) to sender IDs are supported in the destination country.

In the **Sender ID** field enter a sender ID. The sender ID must be 1-11 alphanumeric characters including letters (A-Z), numbers (0-9), or hyphens (-). The sender ID must begin with a letter.

9. Choose **Next**.
10. On **Review and request** you can verify and edit your request before submitting it. Choose **Request**.
11. A **Registration Required** window might appear depending on the type of number you requested. For more information about registrations requirements see [Registrations](#).
 - a. For **Registration form name** enter a name.
 - b. Choose **Complete registration** to finish registering the sender ID or **Register later**.

 **Important**

You are still billed the recurring monthly lease fee regardless of registration status.

Release a sender ID (Console)

If you don't need a sender ID anymore, you can remove it from your account. When you remove a sender ID, we stop charging you for it in your bill for the next calendar month.

Release a sender ID

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Sender Ids**.
3. Choose the sender ID that you want to release and then choose **delete**.
4. On the **Release Sender ID** dialog enter **re1ease** and choose **Release sender ID**.

Open an Amazon Pinpoint SMS support case to request a sender ID

If you plan to send messages to recipients a country where sender IDs are required, you can request a sender ID by creating a new case in the AWS Support Center.


Important

- If you need to register a sender ID in India, complete the procedures in [India sender ID registration process](#) *before* you open a case in Support Center.
- If you need to register a sender ID in Singapore, complete the procedures in [Singapore registration process](#).

To request a sender ID

1. Open the Support Center Console at <https://console.aws.amazon.com/support/home>.
2. On the **Your support cases** pane, choose **Create case**.
3. Choose the **Looking for service limit increases?** link, then complete the following:
 - For **Service**, choose **Pinpoint SMS**.
 - (Optional) For **Provide a link to the site or app which will be sending SMS messages**, provide information about the website, application, or service that will send SMS messages.
 - (Optional) For **What type of messages do you plan to send**, choose the type of message that you plan to send using your long code:
 - **One Time Password** – Messages that provide passwords that your customers use to authenticate with your website or application.
 - **Promotional** – Noncritical messages that promote your business or service, such as special offers or announcements.

- **Transactional** – Important informational messages that support customer transactions, such as order confirmations or account alerts. Transactional messages must not contain promotional or marketing content.
 - (Optional) For **Which AWS Region will you be sending messages from**, choose the AWS Region that you will be sending messages from.
 - (Optional) For **Which countries do you plan to send messages to**, enter the country or region that you want to purchase short codes in.
 - (Optional) In the **How do your customers opt to receive messages from you**, provide details about your opt-in process.
 - (Optional) In the **Please provide the message template that you plan to use to send messages to your customers** field, include the template that you will be using.
4. Under **Requests**, complete the following sections:
- For the **Region**, choose the AWS Region from which you will be sending messages.

 **Note**

The Region is required in the **Requests** section. Even if you provided this information in the **Case details** section you must also include it here.

- For **Resource Type**, choose **Sender ID Registration**.
 - For **Quota**, choose the type of messages that you plan to send.
 - For **New quota value**, enter the number of sender IDs that you're requesting. Typically, this value is **1**.
5. Under **Case description**, for **Use case description**, provide the following information:
- The sender ID that you want to register.
 - The template that you plan to use for your SMS messages.
 - The number of messages that you plan to send to each recipient per month.
 - Information about how your customers opt in to receiving messages from you.
 - The name of your company or organization.
 - The address that's associated with your company or organization.
 - The country where your company or organization is based.

- A phone number for your company or organization.
 - The URL of the website for your company or organization.
6. (Optional) If you want to submit any further requests, choose **Add another request**.
 7. Under **Contact options**, for **Preferred contact language**, choose the language that you prefer to use when communicating with the AWS Support team..
 8. When you finish, choose **Submit**.

After we receive your request, we provide an initial response within 24 hours. We might contact you to request additional information.

If we're able to provide you with a Sender ID, we send you an estimate of the amount of time that's required to provision it. In many countries, we can provide you with a Sender ID within 2–4 weeks. However, in some countries, it can take several weeks to obtain a Sender ID.

In order to prevent our systems from being used to send unsolicited or malicious content, we have to consider each request carefully. We might not be able to grant your request if your use case doesn't align with our policies.

Tags

Tags are pairs of keys and values that you can optionally apply to your AWS resources to control access or usage. Adding a tag to a resource can help you categorize and manage resources in different ways, such as by purpose, owner, environment, or other criteria. You can use tags to easily find existing resources, or to control which users can access specific resources.

Manage tags (Console)

Use the Amazon Pinpoint SMS console to add, edit or delete a Tag.

Manage tags (Console)

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Sender IDs**.
3. On the **Sender IDs** page, choose the sender ID to add a tag to.
4. On the **Tags** tab, choose **Manage tags**.
5.
 - **Add a tag** – In **Manage tags**, choose **Add new tag** to create a new blank key/value pair.
 - **Delete a tag** – In **Manage tags**, choose **Remove** next to the key/value pair.

- **Edit a tag** – In **Manage tags**, choose the **Key** or **Value** and edit the text.
6. Choose **Save changes**.

Manage tags (AWS CLI)

Use the AWS CLI to add or edit a Tag.

```
$ aws pinpoint-sms-voice-v2 tag-resource \  
  --resource-arn resource-arn \  
  --tags tags={key1=value1,key2=value2}
```

In the preceding example, do the following:

- Replace *resource-arn* with the Amazon Resource Name (ARN) that you want to add the tags to.
- Replace *key1* and *key2* with the keys of the tags that you want to add to the resource.
- Replace *value1* and *value2* with the values of the tags that you want to add for the respective keys.

Use the AWS CLI to delete a Tag.

```
$ aws pinpoint-sms-voice-v2 untag-resource \  
  --resource-arn resource-arn \  
  --tag-keys tags={key1=value1,key2=value2}
```

In the preceding example, do the following:

- Replace *resource-arn* with the Amazon Resource Name (ARN) that you want to remove the tag from.
- Replace *key1* and *key2* with the keys of the tags that you want to remove.
- Replace *value1* and *value2* with the values of the tags that you want to remove.

Registrations

Some countries require you to register your company's identity to be able to purchase phone numbers or sender IDs and review the messages you send to recipients in their country. For more

information on which countries require registration, see [Supported countries and regions for SMS messaging](#).

Note

With our updated console experience you are now seeing a registration **Name** field for your registration. This field is set to "-" as we do not manually backfill any of your service values to prevent interruption to your service and let you maintain your security posture. A registration **Name** is an optional friendly name field that can be updated using the tags on the registration details page. For more information on how to add a **Name** tag, see [Change your registration's name](#).

Tip

We recommend that you complete all registrations, even if it is *optional*, as registration could be required in the future.

The following registration forms can be filled out and submitted through the Amazon Pinpoint SMS console.

- **US Toll free numbers** – (Only the United States and the US territories of Puerto Rico, US Virgin Islands, Guam, and American Samoa) A toll-free number (TFN) that begins with 888, 877, 866, 855, 844, or 833. Throughput for toll-free numbers is limited to 3 message parts per second. Toll-free numbers support both SMS, MMS, and voice messages. They can't be used to send messages to recipients outside of the United States or the US territories of Puerto Rico, US Virgin Islands, Guam, and American Samoa. For more information on completing the registration, see [US toll-free number registration form](#).
- **US 10DLC Brand registration** – Register your company or brand to be able to use 10DLC phone numbers and campaigns. For more information on completing the registration, see [10DLC brand registration form](#).
- **US 10DLC Brand vetting** – Before you can request a 10DLC phone number or 10DLC campaign, you must register your company or brand. You only need to register your company once. Company registrations are managed by an industry organization called the Campaign Registry. For more information on completing the registration, see [10DLC brand vetting](#)

- **US 10DLC Campaign registration** – A 10DLC campaign is required to be registered before it can be used. For more information on completing the registration, see [10DLC campaign registration form](#).
- **Singapore sender ID registration** – Register a sender ID in Singapore. For more information on completing the registration, see [Singapore registration form](#).
- **United Kingdom sender ID registration** – Register a sender ID in the United Kingdom. For more information on completing the registration, see [United Kingdom registration form](#).

The following registrations require you to open a support case in the Support Center Console.

- **India sender ID registration** – Register a sender ID for use in India. For more information on completing the registration for see [India sender ID registration process](#).
- **China SMS template registration** – Register an SMS template for use in China. For more information on completing the registration for see [China SMS template registration process](#).

Topics

- [Create a new registration](#)
- [Change your registration's name](#)
- [Check your registration status](#)
- [Edit your registration](#)
- [India sender ID registration process](#)
- [Singapore registration process](#)
- [China SMS template registration process](#)
- [Toll-free number registration process](#)
- [10DLC registration process](#)

Create a new registration

You can use the Amazon Pinpoint SMS console to manage registrations for your Amazon Pinpoint SMS account. If your registration was already created as part of requesting a phone number or sender ID then you do not need to create a new registration. You can view the resources associated with a registration in the **Associated resources** tab, for more information see [View your registration resources](#).

Important

Some registrations have multiple steps that need to be completed in exact order.

- To register a US 10DLC number, you must first register and complete a **US 10DLC Brand registration**, then apply for optional **US 10DLC Brand vetting** to increase your Messages per second (MPS), and then register a **US 10DLC Campaign registration**. If you require sending 10DLC SMS messages from more than one AWS Region and from a single account, you must re-registering all 10DLC resources for each AWS Region required. For more information about the process, see [10DLC registration process](#).
- To register a **Singapore sender ID registration** you must first obtain a Singapore Unique Entity Number (UEN), create and submit a Singapore sender ID registration, once the registration is approved then register the sender ID with Singapore Network Information Centre (SGNIC). For more information about the process, see [Singapore registration process](#).
- To register a **India sender ID registration** you must first register your company and use case with TRAI, create and submit a case with AWS Support and then to send messages you must specify **Entity ID** and **Template ID** values that you received. For more information about the process, see [India sender ID registration process](#).

Create a new registration

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Registrations**, choose **Create registration**.

Note

If you already created a registration when requesting the origination identity then you should use that registration form.

3. For **Registration form name** enter a friendly name.
4. For **Registration type**, choose the registration form from the dropdown list. Each **Registration type** has different forms depending on the regulator body the registration form is sent to.
 - **US toll-free number registration** – In **Available toll-free numbers**, choose a toll-free number to register.

If you don't have a toll-free number to register you can request one by choosing **Request number** and follow the steps in [Request a phone number](#).

- **US 10DLC Brand registration** – Choose to register your 10DLC brand. You only need to register your brand once.
 - **US 10DLC Brand vetting** – Choose a 10DLC brand for vetting from the **Available 10DLC brands** list.
 - **US-10DLC campaign registration** – Choose a 10DLC brand in **Available brands**.
 - **Singapore sender ID registration** – Choose to register a sender ID in Singapore.
 - **United Kingdom sender ID registration** – Choose to register a sender ID in the United Kingdom.
5. (optional) Expand **Tags** to:
- **Add a tag** – In **Manage tags** choose **Add new tag** to create a new blank key/value pair.
 - **Delete a tag** – In **Manage tags**, choose **Remove** next to the key/value pair.
 - **Edit a tag** – In **Manage tags** choose the **Key** or **Value** and edit the text.
6. Choose **Create**.
7. Your registration has now been created and you need to enter in all required information then submit.
- **US toll-free number registration** – [US toll-free number registration form](#).
 - **US 10DLC Brand vetting** – The 10DLC brand has been submitting for vetting and you don't need to fill out any additional forms, see [10DLC brand vetting](#).
 - **US 10DLC Brand registration** – [10DLC brand registration form](#).
 - **US-10DLC campaign registration** – [10DLC campaign registration form](#).
 - **Singapore sender ID registration** – [Singapore registration form](#).

US toll-free number registration form

Note

With our updated console experience you are now seeing a registration **Name** field for your registration. This field is set to "-" as we do not manually backfill any of your service values to prevent interruption to your service and let you maintain your security posture. A registration **Name** is an optional friendly name field that can be updated using the tags on

the registration details page. For more information on how to add a **Name** tag, see [Change your registration's name](#).

After you've created your toll-free number registration you need to complete the form and submit it for approval.

Complete a toll-free number registration

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Registrations**, choose the toll-free number registration to complete.

Note

If you already created a registration when requesting the toll-free number then you can use that registration form.

3. In the **Company info** section, enter the following:
 - For **Company Name**, enter the name of your company.
 - For **Company website**, enter the URL for your company's website.
 - For **Address 1**, enter the street address of your corporate headquarters.
 - For **Address 2 - optional**, if needed enter suite number of your corporate headquarters.
 - For **City**, enter the city of your corporate headquarters.
 - For **State/Province**, enter the state of your corporate headquarters.
 - For **Zip Code/Postal code**, enter the zip code of your corporate headquarters.
 - For **Country**, enter the two digit ISO country code.
 - Choose **Next**.
4. In the **Contact info** section, enter the following:
 - For **First Name**, enter the first name of the person who will be your business's point of contact.
 - For **Last Name**, enter the last name of the person who will be your business's point of contact.

- For **Support Email**, enter the email address of the person who will be your business's point of contact.
- For **Support Phone Number**, enter the phone number of the person who will be your business's point of contact. The phone number must start with a '+' and can't contain any spaces, hyphens, or parentheses. For example, +1 (206) 555-0142 is not in the correct format, but +12065550142 is.

Choose **Next**.

5. In **Messaging Use Case**, do the following:

- For **Monthly SMS Volume**, choose the number of SMS messages that will be each month.
- For **Use Case Category**, choose one of the following use case types:
 - **Two-factor authentication** – Use this for sending two factor authentication codes.
 - **One-time passwords** – Use this for sending a user a one time password.
 - **Notifications** – Use this if you only intend to send your users important notifications.
 - **Polling and surveys** – Use this to poll users on their preferences.
 - **Info on demand** – This is for sending users messages after they have sent a request.
 - **Promotions and Marketing** – Use this if you only intend to send marketing messages to your users.
 - **Other** – Use this if your use case doesn't fall into any other category. Be sure that you fill out the **Use Case Details** for this option.
- Complete **Use Case Details** to provide additional context to the selected **Use Case Category**.
- For **Opt-in Workflow Description** enter a description of how users consent to receive SMS messages. For example, by filling out an online form on your website.
- For **Opt-in workflow image**, upload an image showing how users consent to receiving messages. The supported file type is PNG and the maximum file size is 400KB. Additional information and examples of a compliant opt-in workflow can be found at [Obtain permission](#).

⚠ Important**Examples of opt-in mockups or screenshots:**

- **Website opt-in:** Mockup or screenshots of a web-form where the client adds their number and agrees to receive messages.
- **Website Posting (Support):** Where is the number advertised and where does the customer find the number to text in.
- **Keyword or QR Code Opt-in:** Where does the customer find the keyword or QR code in order to opt-in to these messages.
- **2FA/OTP:** Mockup or screenshot of opt-in if applicable, if verbal, provide a mockup or screenshot of the verbal opt-in script.
- **Informational:** Provide a mockup or screenshot of a verbal consent workflow and provide the messaging content.

6. Choose **Next**.
7. In **Message samples**, do the following:
 - For **Message Sample 1**, enter an example message of an SMS message body that will be sent to your end users.
 - For **Message Sample 2 – optional** and **Message Sample 3 – optional**, enter additional example messages, if needed, of the SMS message body that will be sent.
8. Choose **Next**.
9. On the **Review and submit** page verify the information you are about to submit is correct. To make updates choose **Edit** next to the section.
10. Choose **Submit registration**.

10DLC brand registration form

ⓘ Note


With our updated console experience you are now seeing a registration **Name** field for your registration. This field is set to "-" as we do not manually backfill any of your service values to prevent interruption to your service and let you maintain your security posture. A registration **Name** is an optional friendly name field that can be updated using the tags on

the registration details page. For more information on how to add a **Name** tag, see [Change your registration's name](#).

Before you can request a 10DLC phone number, you must register your company or brand. Brand registrations are managed by an industry organization called the Campaign Registry. You need to register your company per each AWS account and AWS Region that will use the company.

After you've created your 10DLC brand registration you need to complete the form and submit it for approval.

If your 10DLC brand registration is successful and you want to register for higher throughput capabilities, then you must vet your 10DLC brand registration. For more information on 10 DLC brand vetting, see [10DLC brand vetting](#).

 **Note**

For more information on expected registration times, see [10DLC registration process](#).

Complete a 10DLC brand registration


1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Registrations**, choose the 10DLC brand registration to complete.
3. In the **Brand Registration Information** section, enter the following:
 - For **Legal company name**, enter the name that the company is registered under. The name that you enter must be an exact match for the company name that's associated with the tax ID that you provide.

 **Important**

Make sure to use your company's exact legal name. Incorrect or incomplete information might result in your registration being delayed or denied.

- For **Country of tax registration**, enter the two letter ISO country code for the country where your company is registered. For a list of ISO country codes, see [Supported countries and regions for SMS messaging](#).

- For **Tax ID or Business Registration Number**, enter your company's tax ID. The ID that you enter depends on the country that your company is registered in.
- If you're registering a US or non-US entity that has an IRS Employer Identification Number (EIN), enter your nine-digit EIN. The legal company name, EIN, and physical address that you enter must all match the company information that is registered with the IRS.
- If you're registering a Canadian entity, enter your federal or provincial Corporation number. Don't enter the Business Number (BN) provided by the CRA. The legal company name, Corporation number, and physical address that you enter must all match the company information that is registered with Corporations Canada.
- If you're registering an entity that is based in another country, enter the primary tax ID for your country. In many countries, this is the numeric portion of your VAT ID number.
- For **Legal form of organization**, choose the option that best describes your company.

 **Note**

The **US government** and **Not-for-profit** options can only be used to register United States-based organizations. If your organization is based in a country other than the US, you must register as **Private for-profit**, regardless of the actual legal form of your organization.

- For **Stock symbol - optional** enter your companies stock symbol.

For **Stock exchange - optional**, choose the stock exchange your company is listed on

 **Note**

If you chose **Public for profit** in the previous step, the company's stock symbol and the stock exchange fields are required.

- For **Physical business address – Address/Street**, enter the physical street address associated with your company.
- For **Physical business address – City**, enter the city where the physical address is located.
- For **Physical business address – State or region**, enter the state or region where the address is located.
- For **Physical business address – Zip Code/Postal Code**, enter the ZIP or postal code for the address.

- For **Physical business address – Country**, enter the two digit ISO country code.
4. Choose **Next**.
 5. In the **Additional company and contact info** section, enter the following:
 - For **Doing Business As (DBA) or brand name**, enter any other names that your company does business as.
 - For **Vertical**, choose the category that best describes the company you're registering.
 - For **Company website**, enter the full URL of your company's website. Include "http://" or "https://" at the beginning of the address.
 - For **Support Email**, enter the email address of the person who will be your business's point of contact.
 - For **Support Phone Number**, enter the phone number of the person who will be your business's point of contact. The phone number must start with a '+' and can't contain any spaces, hyphens, or parentheses. For example, +1 (206) 555-0142 is not in the correct format, but +12065550142 is.

Choose **Next**.

6. On the **Review and submit** page verify the information you are about to submit is correct. To make updates choose **Edit** next to the section.
7. Choose **Submit registration**.

Note

After your registration has been approved you need to either register for the optional **US 10DLC Brand vetting** or [10DLC campaign registration form](#). For more information on registering for 10DLC, see [10DLC registration process](#).

10DLC brand vetting

If your company's registration is successful and you want to register a 10DLC campaign with higher throughput capabilities, then you must vet your company registration.


When you vet your registration, a third-party organization analyzes the company details that you provided and returns a vetting score. A high vetting score can lead to higher throughput rates for

your 10DLC company and the campaigns associated with it. However, vetting isn't guaranteed to increase your throughput.

Vetting scores aren't applied retroactively. In other words, if you've already created a 10DLC campaign, and you later vet your company registration, your vetting score isn't automatically applied to your existing campaign. For this reason, you should vet your company or brand *before* you create any of your 10DLC campaigns.

 **Note**

There is a \$40 non-refundable fee for vetting your company or brand.


 **Note**

For more information on expected registration times, see [10DLC registration process](#).

To vet your company registration

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Registrations**, choose **Create registration**.
3. For **Registration form name** enter a friendly name.
4. For **Registration type**, choose **US 10DLC brand vetting**.
5. For **Available 10DLC brands**, choose the 10DLC brand to vet.
6. Choose **Create**.

10DLC campaign registration form

 **Note**

With our updated console experience you are now seeing a registration **Name** field for your registration. This field is set to "-" as we do not manually backfill any of your service values to prevent interruption to your service and let you maintain your security posture. A registration **Name** is an optional friendly name field that can be updated using the tags on

the registration details page. For more information on how to add a **Name** tag, see [Change your registration's name](#).

Amazon Pinpoint SMS's vendors perform a manual review processes on 10DLC (10 Digit Long Code) campaigns to address SMS spam concerns raised by US carriers. Reviews are triggered when a number is associated to a 10DLC campaign. Reviews take at least 4 to 6 weeks to process.

When you register a 10DLC campaign, you provide a description of your use case, as well as the message templates that you plan to use. Before you can create and register a 10DLC campaign, you must first register your company. For information on registering your company, see [10DLC brand registration form](#).

Note

For more information on expected registration times, see [10DLC registration process](#). For more information on 10DLC campaign registration issues, see [10DLC campaign registration rejection reasons](#).

In this section, you provide additional details about your 10DLC campaign.

To register a 10DLC campaign

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Registrations**, choose the 10DLC campaign registration to complete.
3. On the **10DLC campaign registration information** page, do the following:
 - a. For **Campaign description**, enter a name for the 10DLC campaign and description of the campaigns purpose.
 - b. For **Vertical**, choose the option that represents your company.
 - c. For **Campaign opt-in workflow**, enter a description of how users consent to receive SMS and MMS messages. The description has to be a minimum of 40 characters. For example, by filling out an online form on your website. If you have multiple opt-in methods, they have to be listed as well.

Your **Opt-in workflow** should include the following:

- Program or product description
 - Identify your organization and service being represented in the initial message sent to your end users
 - Clear and thorough information about how your end-users opt-in to your SMS service and any associated fees or charges
 - Include a link to the Terms & Conditions (which must be publicly accessible).
 - Include a link to the Privacy Policy (which must be publicly accessible).
 - Explain if the Opt-in/Call to Action requires service log-in, is not yet published publicly, is a verbal opt-in, or if it occurs on printed sources such as fliers and paper forms.
 - The Call to Action/Opt-in location must include the following:
 - Comprehensive terms and conditions might be presented in full beneath the call-to-action, or they might be accessible from a link in proximity to the call-to-action.
 - Program (brand) name.
 - Message frequency disclosure.
 - Product description.
 - Customer care contact information.
 - Opt-out information.
 - "Message and data rates may apply" disclosure.
- d. For **Opt-in keyword – optional** enter the keyword that your customers will send to consent to opt-ing in.
- e. For **Opt-in confirmation message – optional** enter the message that your customers receive if they send the Opt-in keyword to your 10DLC phone number.
- f. For **Help Message**, enter the message that your customers receive if they send the keyword "HELP" to your 10DLC phone number. The message has to be a minimum of 20 characters.
- g. For **Stop Message**, enter the message that your customers receive if they send the keyword "STOP" to your 10DLC phone number. The message has to be a minimum of 20 characters.

 **Tip**

Your customers can reply to your messages with the word "HELP" to learn more about the messages that they're receiving from you. They can also reply "STOP"

to opt-out of receiving messages from you. The US mobile carriers require you to provide responses to both of these keywords.

The following is an example of a HELP response that complies with the requirements of the US mobile carriers:

ExampleCorp Account Alerts: For help call 1-888-555-0142 or go to example.com. Msg&data rates may apply. Text STOP to cancel.

The following is an example of a compliant STOP response:


You are unsubscribed from ExampleCorp Account Alerts. No more messages will be sent. Reply HELP for help or call 1-888-555-0142.

Your responses to these keywords must contain 160 characters or fewer.

4. Choose **Next**.
5. For the **Messaging capabilities** section, do the following:
 - a. The capabilities you select are applied to your 10DLC phone number when you create the phone number request.

For **Number capabilities**, choose:

- Choose **SMS** to enable text messages for the 10DLC campaign.
- Choose **SMS and MMS** to enable text and multimedia messages for the 10DLC campaign.
- Choose **SMS and Voice** to enable text and voice messages for the 10DLC campaign.

 **Note**

When you choose to enable voice messages, it lengthens the amount of time to review your registration.

- Choose **SMS and MMS and VOICE** to enable text and multimedia messages for the 10DLC campaign.
- b. For **Message type – optional**, choose either **Transactional** or **Promotional** message type.
 - **Transactional** – Choose this option if your use case is for time-sensitive content, such as alerts and one-time passwords.
 - **Promotional** – Choose this option if your use case is for marketing-related content.

6. Choose **Next**.
7. For the **Campaign use case** section, do the following:
 - a. For **Use case**, choose a use case that most closely resembles your campaign from the preset list of use cases.
 - **Account Notifications** – Standard notifications for account holders, relating to and being about an account.
 - **Charity** – Communications from a non-religious registered [501\(c\)\(3\) charity](#) aimed at providing help and raising money for those in need.
 - **Customer care** – All customer interaction, including account management and customer support.
 - **Delivery notifications** – Information about the status of the delivery of a product or service.
 - **Fraud alert messaging** – Messaging regarding potential fraudulent activity on an account.
 - **Higher education** – Campaigns created on behalf of Colleges or Universities. It also includes School Districts and education institutions that fall outside of any "free to the consumer" messaging model.
 - **Low Volume** – Small throughput, any combination of use-cases. Examples include: test, demo accounts.
 - **Marketing** – Any communication with marketing and/or promotional content.
 - **Mixed** – Mixed messaging reserved for specific consumer service industry.
 - **Public service announcement** – An informational message that is meant to raise the audience's awareness about an important issue.
 - **Polling and voting** – Requests for surveys and voting for non political arenas.
 - **Security alert** – A notification that the security of a system, either software or hardware, has been compromised in some way and there is an action the end users need to take.
 - **Two factor authentication** – Any authentication, verification, or one-time passcode.
 - b. For **Sub use case – optional**, choose up to five sub use cases.
 - c. **Subscriber opt-in** – Subscribers can opt in to receive messages about this campaign.
 - d. **Subscriber opt-out** – Subscribers can opt out of receiving messages about this campaign.

- e. **Subscriber help** – Subscribers can contact the message sender after sending the HELP keyword.
 - f. **Direct lending or loan arrangement** – The campaign includes information about direct lending or other loan arrangements.
 - g. **Embedded link** – The 10DLC campaign includes an embedded link. Links from common URL shorteners, such as TinyUrl or Bit.ly, are not allowed. However, you can use URL shorteners that offer custom domains.
 - h. **Embedded phone number** – The campaign includes a phone number that isn't a customer support number.
 - i. **Age-gated content** – The 10DLC campaign includes age-gated content as defined by carrier and Cellular Telecommunications and Internet Association (CTIA) guidelines.
8. Choose **Next**.
 9. In the **Message samples** section, do the following:
 - Enter at least one **Message sample**. This is the sample text message that you plan to send to your customers. Each sample message has to be a minimum of 20 characters. If you plan to use multiple message templates for this 10DLC campaign, include them as well.

 **Important**

Don't use placeholder text for your sample messages. The example messages that you provide should reflect the actual messages that you plan to send as accurately as possible and should not contain any [Prohibited message content](#).

10. Choose **Next**.
11. In the **MMS file samples** section, do the following:
 - (Optional) MMS sample files are only required if you plan to send MMS messages. In **MMS file samples** upload at least one sample image. A single MMS media file can be up to 2 MB for gif, jpeg, png, and 600 KB in size for all other media file types, see [MMS file types, size and character limits](#).

⚠ Important

Don't use placeholder text in your sample MMS images. The example MMS images that you provide should reflect the actual MMS image that you plan to send as accurately as possible and should not contain any [Prohibited message content](#).

12. Choose **Next**.
13. On the **Review and submit** page, verify the information you're about to submit is correct. To make updates choose **Edit** next to the section.
14. Choose **Submit registration**.

ℹ Note

After your 10DLC campaign registration has been approved you can request a new 10DLC phone number or use an existing 10DLC phone number and associate it with the 10DLC campaign. For more information on registering for 10DLC, see [Requesting dedicated long codes for messaging](#).

United Kingdom registration form

ℹ Note

With our updated console experience you are now seeing a registration **Name** field for your registration. This field is set to "-" as we do not manually backfill any of your service values to prevent interruption to your service and let you maintain your security posture. A registration **Name** is an optional friendly name field that can be updated using the tags on the registration details page. For more information on how to add a **Name** tag, see [Change your registration's name](#).

The United Kingdom's (UK) Mobile Ecosystem Forum (MEF) SMS Sender ID Protection Registry was established to facilitate the identification and blocking of fraudulent SMS messages, protecting consumers as well as legitimate businesses and organizations. The registry enables organizations to register the Sender IDs used when sending SMS to customers in the UK, limiting the ability of fraudsters to impersonate a brand.

If you have protected your Sender ID with MEF you are required to register your Sender ID through Amazon Pinpoint SMS. If you have not protected your Sender ID with MEF you can optionally register your Sender ID information through Amazon Pinpoint SMS to make future mandated registrations of Sender IDs easier.

Complete a United Kingdom sender ID registration

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Registrations**, choose the United Kingdom sender ID registration to complete.
3. In the **Company info** section, enter the following:
 - For **Company Name**, enter the name of your company.
 - For **Tax ID or Business Registration Number**, enter you tax ID.
 - For **Company website**, enter the URL for your company's website.
 - For **Address 1**, enter the street address of your corporate headquarters.
 - For **Address 2 - optional**, if needed enter suite number of your corporate headquarters.
 - For **City**, enter the city of your corporate headquarters.
 - For **State/Province**, enter the state of your corporate headquarters.
 - For **Zip Code/Postal code**, enter the zip code of your corporate headquarters.
 - For **Country**, enter the two digit ISO country code.
 - Choose **Next**.
4. In the **Contact info** section, enter the following:
 - For **First Name**, enter the first name of the person who will be your business's point of contact.
 - For **Last Name**, enter the last name of the person who will be your business's point of contact.
 - For **Contact Email**, enter the email address of the person who will be your business's point of contact.
 - For **Contact Phone Number**, enter the phone number of the person who will be your business's point of contact.

Choose **Next**.

5. In the **Sender ID info** section, enter the following:

- For **Sender ID**, enter the sender ID to request. For more information on sender ID formatting rules, see [Considerations for a Sender ID](#)
- For **Letter of authorization image – optional**, if your Sender ID is protected by MEF then a Letter of Authorization (LOA) is required and the sender ID must be in the exact format as registered with MEF. A template for the LOA can be [downloaded](#) for your convenience. The supported file type is PNG and the maximum file size is 400KB.
- For **Sender ID connection – optional** you can add more details about the connection between the requested sender ID and company name.

Choose **Next**.

6. In **Messaging Use Case**, do the following:

- For **Monthly SMS Volume**, choose the number of SMS messages that will be each month.
- For **Use case category**, choose one of the following use case types:
 - **Two-factor authentication** – Use this for sending two factor authentication codes.
 - **One-time passwords** – Use this for sending a user a one time password.
 - **Notifications** – Use this if you only intend to send your users important notifications.
 - **Polling and surveys** – Use this to poll users on their preferences.
 - **Info on demand** – This is for sending users messages after they have sent a request.
 - **Promotions and Marketing** – Use this if you only intend to send marketing messages to your users.
 - **Other** – Use this if your use case doesn't fall into any other category. Be sure that you fill out the **Use case details** for this option.
- Complete **Use case details** to provide additional context to the selected **Use case category**.

7. Choose **Next**.

8. In **Message samples**, do the following:

- For **Message Sample 1**, enter an example message of an SMS message body that will be sent to your end users.
- For **Message Sample 2 – optional** and **Message Sample 3 – optional**, enter additional example messages, if needed, of the SMS message body that will be sent.

9. Choose **Next**.

10. On the **Review and submit** page verify the information you are about to submit is correct. To make updates choose **Edit** next to the section.
11. Choose **Submit registration**.

Singapore registration form

Note

With our updated console experience you are now seeing a registration **Name** field for your registration. This field is set to "-" as we do not manually backfill any of your service values to prevent interruption to your service and let you maintain your security posture. A registration **Name** is an optional friendly name field that can be updated using the tags on the registration details page. For more information on how to add a **Name** tag, see [Change your registration's name](#).

Amazon Pinpoint SMS customers are able to send SMS traffic in Singapore using a Sender ID that has been registered through the Singapore SMS Sender ID Registry (SSIR). SSIR was launched in March of 2022 through the Singapore Network Information Centre (SGNIC) which is owned by Info-communications Media Development Authority (IMDA) of Singapore, and enables organizations to register their Sender ID when sending SMS to mobile phones in Singapore. In order to use a registered Singapore Sender ID you must obtain a Unique Entity Number (UEN), then submit a request to Amazon Pinpoint SMS to allow-list your account for usage of your Sender ID and finally complete the registration process through SSIR.

Note

Before you request and register your sender ID you must obtain a Singapore Unique Entity Number (UEN). For more information, see [Registering for a Singapore Unique Entity Number \(UEN\)](#).

Complete a Singapore sender ID registration

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Registrations**, choose the Singapore sender ID registration to complete.

3. In the **Company info** section, enter the following:

- For **Company Name**, enter the name of your company.
- For **Tax ID**, enter your Singapore Unique Entity Number.
- For **Company website**, enter the URL for your company's website.
- For **Address 1**, enter the street address of your corporate headquarters.
- For **Address 2 - optional**, if needed enter suite number of your corporate headquarters.
- For **City**, enter the city of your corporate headquarters.
- For **State/Province**, enter the state of your corporate headquarters.
- For **Zip Code/Postal code**, enter the zip code of your corporate headquarters.
- For **Country**, enter the two digit ISO country code.
- Choose **Next**.

4. In the **Contact info** section, enter the following:

- For **First Name**, enter the first name of the person who will be your business's point of contact.
- For **Last Name**, enter the last name of the person who will be your business's point of contact.
- For **Support Email**, enter the email address of the person who will be your business's point of contact.
- For **Support Phone Number**, enter the phone number of the person who will be your business's point of contact.

Choose **Next**.

5. In the **Sender ID info** section, enter the following:

- For **Sender ID**, enter the sender ID to request. For more information on sender ID formatting rules, see [Considerations for a Sender ID](#)
- For **Are you registering on behalf of another brand/entity?** if yes then choose True. If you are not the end user sending the messages you are considered a "Representative" of the other brand/entity.
- For **Letter of authorization image – optional**, if you checked the box as **Registering on behalf of another brand/entity?** , upload an image of the complete Letter of Authorization

(LOA). The supported file type is PNG and the maximum file size is 400KB. A template for the LOA can be [downloaded](#) for your convenience.

- For **Sender ID connection – optional** you can add more details about the connection between the requested sender ID and company name.

Choose **Next**.

6. In **Messaging Use Case**, do the following:

- For **Monthly SMS Volume**, choose the number of SMS messages that will be each month.
- For **Use case category**, choose one of the following use case types:
 - **Two-factor authentication** – Use this for sending two factor authentication codes.
 - **One-time passwords** – Use this for sending a user a one time password.
 - **Notifications** – Use this if you only intend to send your users important notifications.
 - **Polling and surveys** – Use this to poll users on their preferences.
 - **Info on demand** – This is for sending users messages after they have sent a request.
 - **Promotions and Marketing** – Use this if you only intend to send marketing messages to your users.
 - **Other** – Use this if your use case doesn't fall into any other category. Be sure that you fill out the **Use case details** for this option.
- Complete **Use case details** to provide additional context to the selected **Use case category**.

7. Choose **Next**.

8. In **Message samples**, do the following:

- For **Message Sample 1**, enter an example message of an SMS message body that will be sent to your end users.
- For **Message Sample 2 – optional** and **Message Sample 3 – optional**, enter additional example messages, if needed, of the SMS message body that will be sent.

9. Choose **Next**.

10. On the **Review and submit** page verify the information you are about to submit is correct. To make updates choose **Edit** next to the section.

11. Choose **Submit registration**.

Note

After your registration has been approved you need to register the send ID with Singapore Network Information Centre (SGNIC). For more information on how to register, see [Registering a Sender ID with Singapore Network Information Centre \(SGNIC\)](#).

Change your registration's name

To help manage your registrations you should give them a descriptive name. You can add or edit the name of your registration at any time without having to resubmit it. You need to add a tag with the **Key** set to **Name** and the **Value** set to the name to use.

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Registrations**.
3. On the **Registrations** page, choose the registration to add a tag to.
4. On the **Tags** tab, choose **Manage tags**. In **Manage tags** choose **Add new tag**.
5. For **Key** enter **Name** and for **Value** enter a friendly name for the registration.
6. Choose **Save changes**.

Check your registration status

Your registration will be in one of these different statuses:

- **Closed** – You deleted the resources and must also delete the registration for the number.
- **Complete** – Your registration has been approved and you can start using the resource.
- **Created** – Your registration is created but not submitted.
- **Deleted** – Your registration has been deleted.
- **Reviewing** – Your registration has been accepted and is being reviewed.
- **Requires Updates** – You must fix your registration and resubmit it. See [Edit your registration](#) for more information. Fields that require updates display a warning icon and a brief description of the issue.
- **Submitted** – Your registration has been submitted and is awaiting review.

Check your registration status

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Registrations**.
3. On the **Registrations** table, you can then view the registration **Status** of each registration.

Edit your registration

After you submit your registration, the **registration status** will display as **Requires Updates** if there is an issue with the registration. In this state, the registration form is editable. Fields that require updates have a warning icon and a brief description of the issue.

The following registration forms can be edited through the Amazon Pinpoint SMS console.

- **US Toll free numbers** – For more information on completing the registration, see [US toll-free number registration form](#).
- **US 10DLC Brand registration** – For more information on completing the registration, see [10DLC brand registration form](#).
- **US 10DLC Brand vetting** – For more information on completing the registration, see [10DLC brand vetting](#)
- **US 10DLC Campaign registration** – For more information on completing the registration, see [10DLC campaign registration form](#).
- **Singapore sender ID registration** – For more information on completing the registration, see [Singapore registration form](#).

To edit a registration

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Registrations**.
3. On the **Registrations** table, select the **Registration ID** that you want to edit.
4. Choose **Update registration** to edit the form and correct fields that have a warning icon.

Note

If your registration was rejected and requires updates the banner lists the reason the registration was rejected and which fields need to be updated. For more information

about registration rejections, see [Toll-free number registration rejection reasons](#) and [10DLC campaign registration rejection reasons](#).

5. Choose **Submit registration** to resubmit when you're done.

⚠ Important

Recheck all fields to confirm that they're correct.

Discard your registration

You can discard the current version of your registration and make any needed updates. If you find an error in the registration that you have submitted you can use this feature to correct the error and resubmit instead of waiting to have your registration denied and then correct the error. You can only discard the registration if its status is `Submitted`. This will permanently delete the current version of the registration.

To discard a registration

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Registrations**.
3. On the **Registrations** table, select the **Registration ID** that you want.
4. Choose **Discard version** and in the window enter **discard**.
5. Choose **Discard version**.

Delete your registration

You can delete your registration if it is no longer needed. This will permanently delete the registration.

To delete a registration

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Registrations**.
3. On the **Registrations** table, select the **Registration ID** that you want.
4. Choose **Delete registration** and in the window enter **delete**.

5. Choose **Delete registration**.

View your registration resources

Registrations can have one to many resources associated with them depending on the registration type. You can view any resources associated with a registration on the **Associated resources tab of the registration**.

Associate registration resources

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Registrations**, choose a registration from the table.
3. Choose the **Associated resources** tab. Choose a resource to view more information about the resources.

India sender ID registration process

By default, when you send messages to recipients in India, Amazon Pinpoint SMS uses International Long-Distance Operator (ILDO) routes to transmit those messages. When recipients see a message sent over an ILDO connection, it appears to be sent from a random numeric ID (unless you purchase a dedicated short code).

Companies that are registered in India can also use dedicated sender IDs to send their messages. If you prefer to use a sender ID, you have to send those messages over *local routes* rather than ILDO routes.

Note

The price for sending messages using ILDO routes is much higher than the price for sending messages through local routes. The prices for sending messages using both ILDO and local routes are shown on the [Amazon Pinpoint SMS Pricing](#) page.

To send messages using local routes, you must first register your use case and message templates with the Telecom Regulatory Authority of India (TRAI) through a Distributed Ledger Technology (DLT) portal. When you register your use case through a DLT portal, you receive an Entity ID and a Template ID, which you must specify when you send your messages through Amazon Pinpoint SMS.

These registration requirements are designed to reduce the number of unsolicited messages that Indian consumers receive and to protect consumers from potentially harmful messages.

To complete the registration process, you must provide the following information:

- Your organization's Permanent Account Number (PAN).
- Your organization's Tax Deduction Account Number (TAN).
- Your organization's Goods and Services Tax Identification Number (GSTIN).
- Your organization's Corporate Identity Number (CIN).
- A letter of authorization that gives you the authority to register your organization with Vilpower. The Vilpower website includes a template that you can download and modify to fit your needs.

To send SMS messages to India, follow these steps:

- [Step 1: Register your company and use case with the TRAI](#)
- [Step 2: Create a case with AWS Support](#)
- [Step 3: Specify the Entity ID and Template ID values when you send messages](#)
- [Understanding template matching issues](#)

Step 1: Register your company and use case with the TRAI

The first step is to register your company and use case with TRAI. This section includes information about registering your sender ID using Vodafone Idea's Vilpower portal. However, there are several other registration portals. All DLT registration portals require you to provide the same registration details. The Entity ID and Template ID values that you receive from these portals are interchangeable. That is, if you register your use case using a portal other than the Vilpower portal, you can still use your Entity ID and Template ID to send messages using Amazon Pinpoint SMS.

Note

Vilpower charges a fee for registering your company. The current fee is shown on the [Vilpower website](#).

To register your organization with the TRAI

1. In a web browser, go to the Vilpower website at <https://www.vilpower.in>.

2. Choose **Signup** to create another account. During the registration process, do the following:
 - When you're asked to specify the type of entity that you want to register as, choose **As Enterprise**.
 - For **Telemarketer Name**, choose **Infobip Private Limited - ALL**. When prompted, start typing **Infobip** and then choose **Infobip Private Limited – ALL** from the dropdown list.
 - For **Enter Telemarketer ID**, enter **110200001152**.
 - When prompted to provide your Header IDs, enter the sender IDs that you want to register.
 - When prompted to provide your Content Templates, enter the message content that you plan to send to your recipients. Include a template for every message that you plan to send.

Note

The Vilpower website is not maintained by Amazon Web Services. Steps on the Vilpower website are subject to change.

Step 2: Create a case with AWS Support

After you register your company and use case with TRAI, you must create a case with AWS Support. The AWS Support team uses the information that you provide in your case to associate your Entity ID and Template ID with your AWS account.

Note

India allows transactional sender IDs to be 3–6 characters in length. Promotional sender IDs are required to be 6 characters. All sender ID approval is owned by TRAI.

To open an AWS Support case

- Complete the steps at [Open an Amazon Pinpoint SMS support case to request a sender ID](#). In your request, provide the following required information:
 - The AWS Region that you use with Amazon Pinpoint SMS.
 - The company name. The name that you provide must exactly match the name that you provided during the registration process.

- The Principal Entity ID (PEID) that you received after completing the registration process.
- An estimate of the number of messages that you plan to send each month.
- A description of your use case.
- Information about the steps that your recipients must complete to opt in to receiving your messages.
- Confirmation that you collect and manage opt-ins and opt-outs.

Step 3: Specify the Entity ID and Template ID values when you send messages

To successfully deliver your messages using local routes, you must specify Entity ID and Template ID values that you received after completing the sender ID registration process. You must also choose the correct entity type, and confirm that your messages match the example templates that you registered.

The steps that you complete depend on how you send your SMS messages. If you use the [SendTextMessage](#) API to send your messages, you can include these attributes in your call to the API. If you use campaigns or journeys to send your messages, you can specify the correct values when you set up the campaign or journey. This section includes information for both scenarios.

To send messages over Indian local routes using the SendTextMessages API


1. In your call to the SendTextMessages API, provide values for the following parameters:
 - EntityId – The entity ID or Principal Entity (PE) ID that you received after completing the sender ID registration process.
 - TemplateId – The template ID that you received after completing the sender ID registration process.

Important

Make sure that the Template ID that you specify matches your message template exactly. If your message doesn't match the template that you provided during the registration process, the mobile carriers might reject your message.

2. For the MessageType parameter, specify the appropriate route type for your message. You can specify one of the following values:

- **Promotional** – Specify this message type for promotional messages. Promotional sender IDs only contain numbers.
- **Transactional** – Specify this message type for transactional messages. Transactional sender IDs only contain letters, and are case-sensitive.

 **Note**

You can register both promotional (numeric) sender IDs and transactional (alphabetic) sender IDs in the same AWS account.

For additional content guidelines, see the Vilpower website at <https://www.vilpower.in>.

3. When you add content to your message, review your content thoroughly to verify that it matches the content in the DLT registered template exactly. If you include additional character returns, spaces, punctuation, or mismatched sentence case, carriers will block your SMS messages. For more information about issues related to template matching, see [Understanding template matching issues](#).

Understanding template matching issues

Indian carriers will reject your messages if they don't align exactly with the templates that you submitted during the registration process. If you experience message delivery issues, check your messages for the following common issues:

- **Message content doesn't match registered template** – All of the messages that you send must correspond to a registered template. If you send a message that doesn't exactly match the template associated with the Template ID that you provided, the mobile carriers will reject your message.
- **The value of a variable is too long** – If the value of a variable contains more than 30 characters, the mobile carriers will reject your message.
- **Case mismatch** – The mobile carriers compare your messages to the templates that you registered. This comparison process is case-sensitive.
- **Slightly different characters** – Your message can be rejected if it contains characters that look similar to the characters in your registered template, but are actually different. For example, if you copy text from Microsoft Word, the text might include curly-quote characters (" and "),

as opposed to the straight quote character ("). Make sure that your message matches your registered templates exactly.

Singapore registration process

Amazon Pinpoint SMS customers are able to send SMS traffic in Singapore using a Sender ID that has been registered through the Singapore SMS Sender ID Registry (SSIR). SSIR was launched in March of 2022 through the Singapore Network Information Centre (SGNIC) which is owned by Info-communications Media Development Authority (IMDA) of Singapore, and enables organizations to register their Sender ID when sending SMS to mobile phones in Singapore. In order to use a registered Singapore Sender ID you must obtain a Unique Entity Number (UEN), then submit a request to Amazon Pinpoint SMS to allow-list your account for usage of your Sender ID and finally complete the registration process through SSIR.

If you do not register your sender ID any message sent using a sender ID will have its ID changed to **LIKELY-SCAM** per regulatory agency rules. Regulators will filter or block unregistered traffic at their discretion.

Important

Your Singapore registration must be completed in this order:

1. [Registering for a Singapore Unique Entity Number \(UEN\)](#)
2. [Create a new registration](#) with **Registration type** set to Singapore sender ID registration.
3. [Registering a Sender ID with Singapore Network Information Centre \(SGNIC\)](#)

Registering for a Singapore Unique Entity Number (UEN)

In order to start a registration with the SSIR you must first obtain a Singapore Unique Entity Number (UEN). A UEN is a unique entity number you receive when you register your business with the Account and Corporate Registry Authority (ACRA), for more information see [Who Must Register with ACRA?](#). The amount of time to process can vary depending on how easily the ACRA can validate your request.

Registering a Sender ID with Singapore Network Information Centre (SGNIC)

To register a sender ID with Singapore Network Information Centre (SGNIC) there are two steps that must be completed in the following order:

Register a sender ID with Singapore Network Information Centre (SGNIC)

1. You must first work with Amazon Pinpoint SMS to register your Singapore (SG) Sender ID for your account. After this step is complete you can proceed to the next step.
2. Work with SGNIC to register your sender ID using the process at [SGNIC SMS Sender ID Registry](#).
 - When completing the process list AMCS SG Private Limited (Amazon Media Communications Services) as your participating aggregator.

Warning

Doing these steps out of order might result in your sender ID being blocked by the service or will prevent your Sender ID from being preserved on the mobile device.

Note

Please note that you are required to submit a sender ID registration from each individual AWS account you require to use the sender ID.

Singapore sender ID registration frequently asked questions

Frequently asked questions about the Singapore sender ID number registration process with Amazon Pinpoint SMS.

Do I currently have a Singapore sender ID

To check if you own a Singapore sender ID

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Sender ID**.
3. On the **Sender IDs** page, you can search by two letter country code **SG** to find if you have any Singapore sender IDs.

How long will registration take?

While a typical review takes 1 – 3 weeks, it can take up to 5 weeks or longer in some cases to verify your information with government agencies.

What is a Unique Entity Number (UEN) and how do i get one?

A UEN is a Singapore business ID issued by Accounting and Corporate Regulatory Agency (ACRA). Local companies and businesses in Singapore can get a UEN by applying through ACRA. Once you pass through the registration and standard incorporation procedure, it will be issued. You can apply for a UEN with ACRA via [Bizfile](#).

Do I have to register for a Singapore Sender ID?

Yes. If you haven't registered your Singapore Sender ID any message sent using a Sender ID will likely have its ID changed to **LIKELY-SCAM**

How do I register my Singapore Sender ID with Amazon Pinpoint SMS?

Follow the directions at [Create a new registration](#) to register a Sender ID.

What is the registration status of my Singapore Sender ID and what does it mean?

Follow the directions at [Check your registration status](#) to check your registration and status.

What information do I need to provide?

You will need to provide your companies address, a business contact, and a use case. You can find the required information at [Create a new registration](#).

What if my Singapore Sender ID registration is rejected?

If your registration is rejected, its status will be changed to **Requires Updates** and you can make updates by following the directions in [Edit your registration](#).

What permissions do I need?

The IAM user/role that you use to visit the Amazon Pinpoint SMS console must be enabled with the `"sms-voice:*"` permission.

Are there any restrictions to the formatting or allowed special characters for Singapore Sender IDs?

Yes. For more information on sender ID formatting rules, see [Considerations for a Sender ID](#).

China SMS template registration process

To register your SMS template you must open a support case in the Support Center Console.

Note

Only China requires SMS template registration for your account to be allowed sending there.

Register an SMS template

1. Open the Support Center Console at <https://console.aws.amazon.com/support/home>.
2. In the **Your support cases** section, choose **Create case**.
3. On the **Create case** page, choose **Looking for service limit increases?** link.
4. In the **Create Case** section, do the following:
 - For **Limit type**, choose **Pinpoint SMS**.
 - For **Provide a link to the site or app which will be sending SMS messages**, identify the website or application where your audience members opt in to receive your SMS messages.
 - For **What type of messages do you plan to send**, choose the type of message that you plan to send using your Sender ID:
 - **One Time Password** – Messages that provide passwords that your customers use to authenticate with your website or application.
 - **Promotional** – Noncritical messages that promote your business or service, such as special offers or announcements.
 - **Transactional** – Important informational messages that support customer transactions, such as order confirmations or account alerts. Transactional messages must not contain promotional or marketing content.
 - For **Which countries do you plan to send messages to**, choose the AWS Region that you will be sending messages from.

Note

Only China requires template registration for your account to be allowed sending there.

5. In the **Requests** section, do the following:
 - For the **Region**, choose the AWS Region that you plan to make API requests from.
 - For **Resource Type**, choose **Template Registration**.
 - For **Limit**, choose one of the following:
 - **One Time Password** – Messages that provide passwords that your customers use to authenticate with your website or application.
 - **Promotional** – Noncritical messages that promote your business or service, such as special offers or announcements.
 - **Transactional** – Important informational messages that support customer transactions, such as order confirmations or account alerts. Transactional messages must not contain promotional or marketing content.
6. Under **Case description**, for **Use case description**, explain your use case and opt-in workflow.
7. Under **Contact options**, for **Preferred contact language**, choose whether you want to receive communications for this case in **English** or **Japanese**.
8. When you finish, choose **Submit**.

After we receive your request, we provide an initial response within 24 hours. We will send you a country-specific registration form for you to complete and provide back to us for downstream processing.

Important

In order to prevent our systems from being used to send unsolicited or malicious content, we consider each request carefully. We might not be able to grant your request if your use case doesn't align with our policies.

Toll-free number registration process

Important

It can take up to 15 business days for your registration to be processed after it is submitted.

If you use Amazon Pinpoint SMS to send messages to recipients in the United States or the US territories of Puerto Rico, US Virgin Islands, Guam and American Samoa, you can use toll-free phone numbers (TFN) to deliver those messages. After you request a TFN you can register your company using the TFN. Each TFN requires a specific use case. For example, if you register a TFN to use for one-time passwords, it can only be used for sending one-time passwords. If a TFN is used for anything other than the specified use case, it can be revoked.

Register a toll-free number

1. You first need to request the toll-free number. When you request the toll-free number in the **Registration Required** window enter a friendly name for the registration.
2. You can begin the registration process by choosing **Begin registration** or choose **Register later** to come back and complete the form.

Toll-free number forbidden use cases

Please be aware that AWS is limited in our ability to send any messages or register TFNs for some use cases. Certain use cases are blocked entirely (for example, use cases related to controlled substance, or phishing) and other might be subject to high levels of filtering (for example, high risk financial messages). You might be unable to register TFNs associated with restricted content use cases defined in [Prohibited message content](#).

Toll-free number registration rejection reasons

If your Toll-free number registration was rejected, use the following table to determine why it was rejected and what you can do to fix your Toll-free number registration. After you determine why the registration was rejected, you can modify the existing registration to address that issue and resubmit. For more information, see [Edit your registration](#).

Reason for rejection

Amazon Pinpoint SMS rejection short description	Amazon Pinpoint SMS rejection long description
Compliant Opt In Missing	The opt-in process or screenshot is missing. A compliant opt-in process or screenshot will clearly specify how your recipient is able to provide their explicit consent to receive SMS messages. Some common rejection reasons:

Amazon Pinpoint SMS rejection short description	Amazon Pinpoint SMS rejection long description
	<p>missing explicit language around SMS opt-in consent, mismatch between provided company name and opt-in screenshots, receiving a text message cannot be required to sign up for service, or SMS opt-in consent cannot be included in the Terms of Service. For more information, see Obtain permission.</p>
Invalid Business Connection	<p>The contact information and company/application information does not have a clear connection. SMS Messages can't be sent on behalf of a 3rd party. In order to be verified please resubmit explaining the connection between your contact and company/application information.</p>
Invalid Company Info	<p>The company information you provided is unable to be verified. In order to be verified please confirm your company website is valid and aligns with your company name and address.</p>
Invalid Multi Numbers	<p>A single Toll Free number can only be associated with a single business. Please either resubmit a new registration request for each company with its own phone number or explain the connections between the multiple businesses called out.</p>
Invalid Overall	<p>The information provided has been considered invalid. Please confirm your company website, use case, opt-in, and message samples are all valid inputs and align with other inputs in your registration.</p>

Amazon Pinpoint SMS rejection short description	Amazon Pinpoint SMS rejection long description
Invalid URL	The company URL you provided is unable to be accessed. In order to be verified please confirm your provided company website is valid and active.
Non Compliant Opt In	The opt-in process or screenshot you have provided is either insufficient or non compliant . A compliant opt-in process or screenshot will clearly specify how your recipient is able to provide their explicit consent to receive SMS messages. Some common rejection reasons: missing explicit language around SMS opt-in consent, mismatch between provided company name and opt-in screenshots, receiving a text message cannot be required to sign up for service, or SMS opt-in consent cannot be included in the Terms of Service. For more information, see Obtain permission .

Amazon Pinpoint SMS rejection short description	Amazon Pinpoint SMS rejection long description
Non Compliant Opt In Consent	<p>The opt-in process or screenshot you have provided does not show explicit consent. Explicit consent is the deliberate action of a user having the option to request a specific message. A compliant opt-in process or screenshot will clearly specify how your recipient is able to provide their explicit consent to receive SMS messages. Some common rejection reasons: missing explicit language around SMS opt-in consent, mismatch between provided company name and opt-in screenshots, receiving a text message cannot be required to sign up for service, or SMS opt-in consent cannot be included in the Terms of Service. For more information, see Obtain permission.</p>
Non Compliant Opt In Third Party	<p>The opt-in process or screenshot you have provided is either insufficient or non compliant due to opt-in information being shared with 3rd parties. A compliant opt-in process or screenshot will clearly specify how your recipient is able to provide their explicit consent to receive SMS messages and is not shared with 3rd parties. Please resubmit after you remove any language around opt-in information sharing or include language specifically stating opt-in information is not shared with 3rd parties. For more information, see Obtain permission.</p>

Amazon Pinpoint SMS rejection short description	Amazon Pinpoint SMS rejection long description
Non Compliant Use Case	The use case and/or message samples provided are considered restricted content under US Telecom regulations. Please refer to the documentation below for a full list of items considered restricted content. If you believe your content is falsely considered restricted you can attempt to update your sample messages and use case and re-submit the registration. For more information, see Obtain permission .

Toll-free number frequently asked questions

Frequently asked questions about the toll-free number registration process.

Do I currently own a toll-free number?

To check if you own a toll-free number

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **SMS and voice**, choose **Phone numbers**.
3. Toll-free numbers have their **type** listed as **toll free**.

Do I have to register my toll-free number?

Yes. If you currently own a toll-free number, you must register to use it.

How do I purchase a toll-free number?

Follow the directions at [Request a phone number](#) to purchase a toll-free number.

How do I register my toll-free number?

If you already procured your TFN and created a registration form then follow the directions at [US toll-free number registration form](#) to complete the form. If you need to create a registration then follow the directions at [Create a new registration](#) to register a toll-free number.

What is the registration status of my toll-free number and what does it mean?

Follow the directions at [Check your registration status](#) to check your registration and status.

What information do I need to provide?

You will need to provide your companies address, a business contact, and a use case. You can find the required information at [US toll-free number registration form](#).

What if my registration is rejected?

If your registration is rejected, its status will be changed to **Requires Updates** and you can make updates by following the directions in [Edit your registration](#).

What permissions do I need?

The IAM permissions that you use to visit the Amazon Pinpoint SMS console must be enabled with the `"sms-voice:*"` permission.

10DLC registration process

Important


The following table has the expected times for each 10DLC registration step based on if your business is located in the United States or internationally.

10DLC registration step	US based companies	International based companies
Register your brand/company	1-2 business days	Up to 3 weeks
Apply for vetting	1-2 business days	Up to 3 weeks
Register your campaign	Up to 4 weeks	Up to 4 weeks
Request your 10DLC number	Up to 10 days	Up to 10 days

If you use Amazon Pinpoint SMS to send messages to recipients in the United States or the US territories of Puerto Rico, US Virgin Islands, Guam and American Samoa, you can use 10DLC phone numbers to deliver those messages. The abbreviation *10DLC* stands for "10-digit long code." A 10DLC phone number is registered for use by a single sender and for a single use case. This registration process gives the mobile carriers insight into the approved use cases for each phone number that is used to send messages. As a result, 10DLC phone numbers can offer high throughput and deliverability rates.

A message that you send from a 10DLC phone number appears on the devices of your recipients as a 10-digit phone number. You can use 10DLC phone numbers to send both transactional and promotional messages. If you already use short codes or toll-free numbers to send your messages, then you don't need to set up 10DLC.

To set up 10DLC, you first register your company or brand. Next, you create a *10DLC campaign*, which is a description of your use case. This information is then shared with the Campaign Registry, an industry organization that collects 10DLC registration information.

 **Note**

For more information about how the Campaign Registry uses your information, see the FAQ on the [Campaign Registry website](#).

After your company and 10DLC campaign are approved, you can purchase a phone number and associate it with your 10DLC campaign. Associating a phone number with a 10DLC campaign can take approximately 14 days to complete. Although you can associate multiple phone numbers with a single campaign, you can't use the same phone number across multiple 10DLC campaigns. For each 10DLC campaign that you create, you must have at least one unique phone number. Throughput for 10DLC phone numbers is based on the company and campaign registration information that you provide. Associating multiple phone numbers with a 10DLC campaign doesn't provide any additional throughput.

If you have an existing unregistered long code in your Amazon Pinpoint SMS account, you can request that it be converted to a 10DLC number. To convert an existing long code, complete the registration process, and then create a case in the AWS Support Center. In some situations, it isn't possible to convert an unregistered long code to a 10DLC phone number. In this case, you must request a new number through the Amazon Pinpoint SMS console and associate it with your 10DLC

campaign. For more information about using 10DLC with existing long codes, see [Associating a long code with a 10DLC campaign](#).

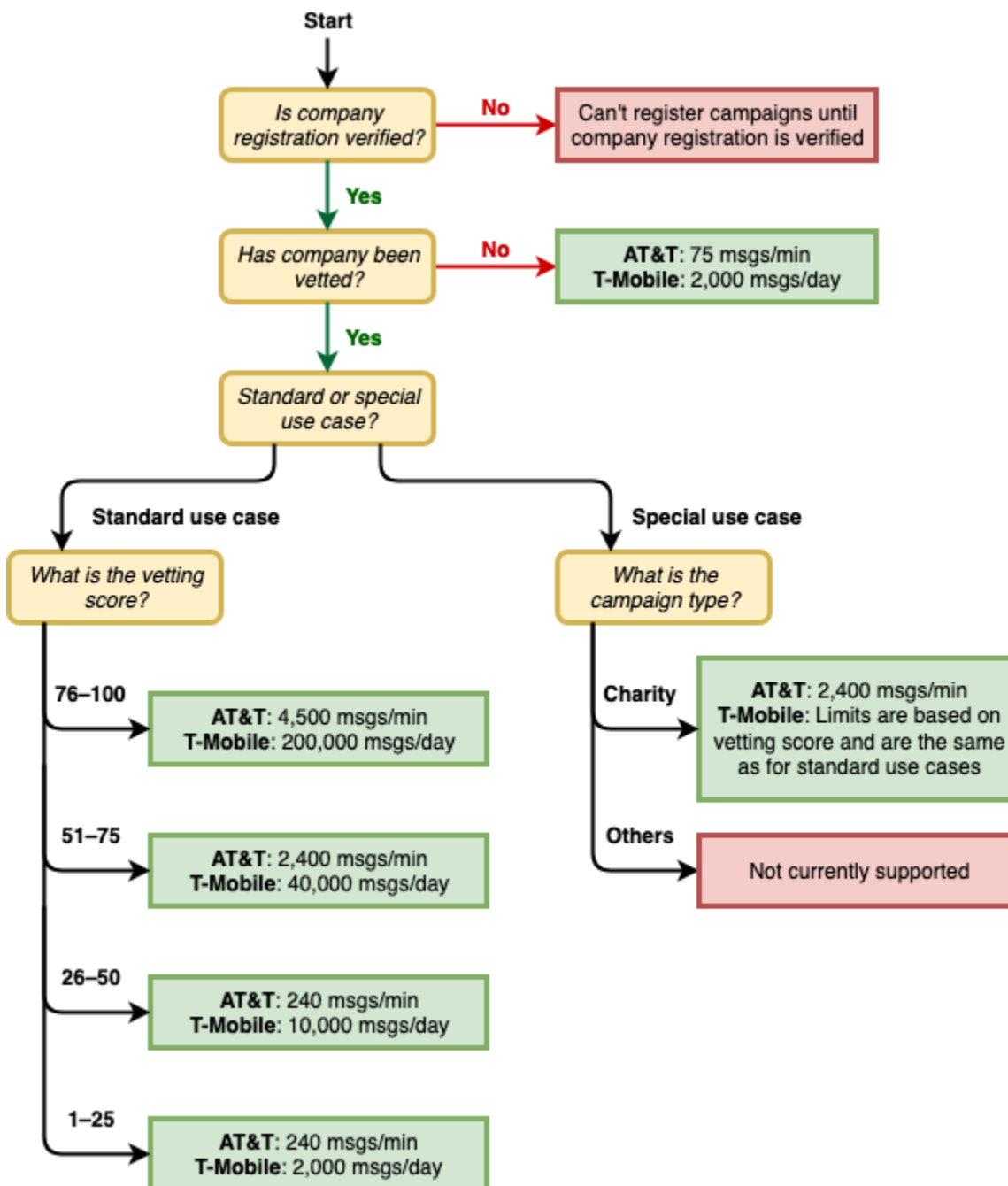
10DLC capabilities

The capabilities of 10DLC phone numbers depend on which mobile carriers your recipients use. AT&T provides a limit on the number of message parts that can be sent each minute for each campaign. T-Mobile provides a daily limit of messages that can be sent for each company, with no limit on the number of message parts that can be sent per minute. Verizon hasn't published throughput limits, but uses a filtering system for 10DLC that is designed to remove spam, unsolicited messages, and abusive content, with less emphasis on the actual message throughput.

New 10DLC campaigns that are associated with *unvetted* companies can send 75 message parts per minute to recipients who use AT&T, and 2,000 messages per day to recipients who use T-Mobile. The company limit is shared across all of your 10DLC campaigns. For example, if you have registered one company and two campaigns, the daily allotment of 2,000 messages to T-Mobile customers is shared across those campaigns. Similarly, if you register the same company in more than one AWS account, the daily allotment is shared across those accounts.

If your throughput needs exceed these limits, you can request that your company registration be vetted. When you vet your company registration, a third-party verification provider analyzes your company details. The verification provider then provides a vetting score, which determines the capabilities of your 10DLC campaigns. There is a one-time charge for the vetting service. For more information, see [10DLC brand vetting](#).

Your actual throughput rate will vary depending on various factors, such as whether or not your company has been vetted, your campaign types, and your vetting score. The following flowchart shows the throughput rates for various situations.



Throughput rates for 10DLC are determined by the US mobile carriers in cooperation with the Campaign Registry. Neither Amazon Pinpoint SMS nor any other SMS sending service can increase 10DLC throughput beyond these rates. If you need high throughput rates and high deliverability rates across all US carriers, we recommend that you use a short code.

10DLC registration process

You can set up 10DLC directly in the Amazon Pinpoint SMS console. To set up 10DLC, you must complete all of the following steps.

1. Register your brand/company

The first step in setting up 10DLC is to register your company or brand. For information about company registration, see [10DLC brand registration form](#). There is a one-time registration fee to register your company. This fee is shown on the registration page.

2. (Optional, but recommended) Apply for vetting

If your company registration is successful, you can begin creating low-volume, mixed-use 10DLC campaigns. These campaigns can send 75 messages per minute to recipients who use AT&T, and your registered company can send 2,000 messages per day to recipients who use T-Mobile. If your use case requires a throughput rate that exceeds these values, you can apply for vetting of your company registration. Vetting your company registration can increase the throughput rates for your companies and campaigns, but it isn't guaranteed to do so. For more information about vetting, see [10DLC brand vetting](#).

3. Register your campaign

If the Campaign Registry is able to verify the company information that you provided, you can create a 10DLC campaign. A 10DLC campaign contains information about your use case. Each 10DLC campaign can be associated with one company. Amazon Pinpoint SMS sends this campaign information to the Campaign Registry for approval. In most cases, 10DLC campaign approval is instantaneous. In some cases, the Campaign Registry can require additional information. It can take up to 4 weeks to receive a response on if your 10DLC campaign was approved or needs to be revised.

You're charged a recurring monthly fee for each 10DLC campaign that you register. The monthly fee varies depending on your use case. The recurring fee for your campaign is shown on the registration page.

4. Request your 10DLC number

After your 10DLC campaign is approved, you can request a phone number and associate that number with the approved 10DLC campaign. Each phone number can only be associated with a single 10DLC campaign. For more information on requesting a 10DLC phone number,

see [Request a phone number](#) and [Associating a long code with a 10DLC campaign](#). There is a monthly recurring fee for leasing the phone number. This fee is shown on the purchase page.

Note

You are charged the monthly 10DLC number lease price regardless of status. For example, 10DLC numbers in a **Pending** state still generate a month fee. For more information about pricing, see [Amazon Pinpoint SMS Pricing](#).

Associating a long code with a 10DLC campaign

After your 10DLC campaign is approved, you have provisioned a new long code or have an existing long code you can then associate that long code with the approved 10DLC campaign. The long code that you associate with the 10DLC campaign can only be used with that campaign, and you can't use it for any other 10DLC campaign.

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Registrations**, choose the 10DLC campaign(US_TEN_DLC_CAMPAIGN_REGISTRATION) to associate the long code with.
3. Choose the **Associated resourced** tab and **Add resource**.
4. For **Supported association**, choose **TEN_DLC** from the dropdown list.
5. For **Available resources**, choose the 10DLC phone number to add.
6. Choose **Associate resource**.

You can associate more than one long code with the 10DLC campaign.

10DLC registration and monthly fees


There are registration and monthly fees associated with using 10DLC, such as registering your company and 10DLC campaign. These are separate from any other monthly or AWS fees. For more information about 10DLC fees, see the [Amazon Pinpoint SMS Pricing](#) page.

10DLC campaign registration rejection reasons

If your 10DLC campaign was rejected, use the following table to determine why it was rejected and what you can do to fix your 10DLC campaign registration. After you determine why the campaign

was rejected, you can modify the existing campaign to address that issue and resubmit. For more information, see [Edit your registration](#).


Reason for rejection


Amazon Pinpoint SMS rejection short description	Amazon Pinpoint SMS rejection long description
<p>Campaign Attributes don't match the website, sample message content, or both.</p>	<p>The campaign attributes do not align or match with the company website, sample message content, or both. Update the registration to align the campaign attributes with the company website, sample message content, or both. Campaign attributes can include company vertical, subscriber opt-in/-out, help responses, and age-gated content.</p> <div data-bbox="829 884 1507 1388" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Important</p> <p>Campaigns are not automatically resubmitted when you resubmit your company registration. If you make any changes to your company information, then you must resubmit the company information. If you make any campaign changes, you must resubmit the campaign registration.</p> </div>
<p>Use case and message samples are inconsistent.</p>	<p>There are inconsistencies between the use case and messages samples provided in the campaign. Update the registration to align the use case and message samples.</p>
<p>Company and message samples are inconsistent or missing message samples.</p>	<p>There are inconsistencies between the company website and message samples provided in the campaign, or the campaign was missing message samples. Update your company and campaign registration informati</p>

Amazon Pinpoint SMS rejection short description	Amazon Pinpoint SMS rejection long description
	<p>on so that the website and message samples align.</p> <div data-bbox="829 384 1507 888" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"> <p>⚠ Important</p> <p>Campaigns are not automatically resubmitted when you resubmit your company registration. If you make any changes to your company information, then you must resubmit the company information. If you make any campaign changes, you must resubmit the campaign registration.</p> </div>
<p>Use case, message samples, or both are considered restricted or disallowed by mobile operators; prohibited content: cannabis.</p>	<p>The use case, message samples provided, or both are considered restricted content under US Telecom regulations. If you believe that your content is falsely considered restricted, you can attempt to update your sample messages and use case, and resubmit the registration. Prohibited content: cannabis.</p>
<p>Use case, message samples, or both are considered restricted or disallowed by mobile operators; prohibited content: guns/ammo.</p>	<p>The use case, message samples provided, or both are considered restricted content under US Telecom regulations. If you believe that your content is falsely considered restricted, you can attempt to update your sample messages and use case, and resubmit the registration. Prohibited content: guns/ammo.</p>

Amazon Pinpoint SMS rejection short description	Amazon Pinpoint SMS rejection long description
Use case, message samples, or both are considered restricted or disallowed by mobile operators; prohibited content: SHAFT .	The use case, message samples provided, or both are considered restricted content under US Telecom regulations. If you believe that your content is falsely considered restricted, you can attempt to update your sample messages and use case, and resubmit the registration. Prohibited content: SHAFT .
Use case, message samples, or both are considered restricted or disallowed by mobile operators; prohibited content: gambling .	The use case, message samples provided, or both are considered restricted content under US Telecom regulations. If you believe that your content is falsely considered restricted, you can attempt to update your sample messages and use case, and resubmit the registration. Prohibited content: gambling .
Use case, message samples, or both are considered restricted or disallowed by mobile operators; prohibited content: hate .	The use case, message samples provided, or both are considered restricted content under US Telecom regulations. If you believe that your content is falsely considered restricted, you can attempt to update your sample messages and use case, and resubmit the registration. Prohibited content: hate .
Use case, message samples, or both are considered restricted or disallowed by mobile operators; prohibited content: alcohol with failure to age gate .	The use case, message samples provided, or both are considered restricted content under US Telecom regulations. If you believe that your content is falsely considered restricted, you can attempt to update your sample messages and use case, and resubmit the registration. Prohibited content: alcohol with failure to age gate .

Amazon Pinpoint SMS rejection short description	Amazon Pinpoint SMS rejection long description
<p>Use case, message samples, or both are considered restricted or disallowed by mobile operators; prohibited content: tobacco/vape with failure to age gate.</p>	<p>The use case, message samples provided, or both are considered restricted content under US Telecom regulations. If you believe that your content is falsely considered restricted, you can attempt to update your sample messages and use case, and resubmit the registration. Prohibited content: tobacco/vape with failure to age gate.</p>
<p>Use case, message samples or both are considered restricted or disallowed by mobile operators; prohibited use case: lead generation/affiliate marketing; other.</p>	<p>The use case, message samples provided or both are considered restricted content under US Telecom regulations. If you believe that your content is falsely considered restricted, you can attempt to update your sample messages and use case, and resubmit the registration. Prohibited use case: lead generation/affiliate marketing; other.</p>
<p>Use case, message samples or both are considered restricted or disallowed by mobile operators; prohibited use case: lead generation/affiliate marketing; high risk financial.</p>	<p>The use case, message samples provided or both are considered restricted content under US Telecom regulations. If you believe that your content is falsely considered restricted, you can attempt to update your sample messages and use case, and resubmit the registration. Prohibited use case: lead generation/affiliate marketing; high risk financial.</p>

Amazon Pinpoint SMS rejection short description	Amazon Pinpoint SMS rejection long description
ISV/Reseller. Company information and service information/message samples mismatch.	The company and campaign information do not match and is identified as an independent software vendor (ISV) or reseller. Register the company information that matches the service and end user. Create a new campaign that has service information aligned with company information.
Campaign appears to be Direct Lending Arrangement but appropriate Content Attribute was not selected.	The company and campaign details submitted appear to be direct lending arrangement. Edit your campaign and mark "Yes" for Direct Lending Arrangement attribute and resubmit.
Unofficial email domain for what appears to be large company that would have an official domain.	<p>The email domain provided does not appear to be official given the company information submitted with the registration. Update the registration with an official email address that matches domain of the company and resubmit.</p> <div data-bbox="829 1182 1507 1688" style="border: 1px solid #f08080; border-radius: 15px; padding: 15px; margin-top: 10px;"> <p> Important</p> <p>Campaigns are not automatically resubmitted when you resubmit your company registration. If you make any changes to your company information, then you must resubmit the company information. If you make any campaign changes, you must resubmit the campaign registration.</p> </div>

Amazon Pinpoint SMS rejection short description	Amazon Pinpoint SMS rejection long description
Opt-in process not compliant or opt-in isn't explicit.	The opt-in workflow that you have provided is either insufficient, non-compliant, or not explicit for end users to receive specific SMS messages. A compliant opt-in process will clearly specify how your recipient is able to provide their explicit consent to receive SMS messages. Some common rejection reasons: missing explicit language around SMS opt-in consent, mismatch between provided company name and message samples, receiving a text message can't be required to sign up for service, or SMS opt-in consent can't be included in the Terms of Service.
Website not provided or not working.	The company information did not include a website or the website was inaccessible. Update your company information with an accessible website and resubmit both your company and campaign for review. <div data-bbox="829 1192 1507 1696" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Important</p><p>Campaigns are not automatically resubmitted when you resubmit your company registration. If you make any changes to your company information, then you must resubmit the company information. If you make any campaign changes you must resubmit the campaign registration.</p></div>

10DLC brand or campaign registration issues

When registering a 10DLC campaign, the 3rd party downstream reviewer might find issues with the registration that results in a denied registration with a related error message. For more information on registration error messages and solutions, see [10DLC campaign registration rejection reasons](#). You should also review [10DLC Registration Best Practices to Send SMS with Amazon Pinpoint](#) and [How to Build a Compliant SMS Opt-In Process With Amazon Pinpoint](#) blog articles that have more in-depth details on how to successful register an SMS use case.

If you are still having issues getting your SMS use case approved you can reach out through AWS Support to ask for additional assistance in understanding why your use cases was rejected. **Note** that this requires downstream engagement and takes time to better understand the denial reason.

Note

If you are not based in the United States and your 10DLC brand registration fails you should:

1. Apply for [10DLC brand vetting](#), as this is a manual review of your 10DLC brand.
2. If vetting fails then follow the directions below to submit a support ticket.

To submit a request for information about a rejected 10DLC brand or campaign

1. Open the Support Center Console at <https://console.aws.amazon.com/support/home>.
2. On the **Your support cases** pane, choose **Create case**.
3. Choose the **Looking for service limit increases?** link.
4. For **Limit type**, choose **Pinpoint SMS**.
5. In the **Requests** section, do the following:
 - For **Region**, choose the AWS Region that you attempted to register the campaign in.
 - For **Resource Type**, choose **10DLC Registration**.
 - For the **Limit**, choose **Company or 10DLC Campaign Registration Rejection**.
6. For **Use case description**, enter the rejected 10DLC campaign ID.
7. Under **Contact options**, for **Preferred contact language**, choose the language that you prefer to use when communicating with the AWS Support team.

8. For **Contact method**, choose your preferred method of communicating with the AWS Support team.
9. Choose **Submit**.

The AWS Support team will provide information about the reasons that your 10DLC campaign registration was rejected in your AWS Support case.

10DLC cross-account access

Each 10DLC phone number is associated with a single account in a single AWS Region. If you want to use the same 10DLC phone number to send messages in more than one account or Region, you have two options:

1. You can register the same company and campaign in each of your AWS accounts. These registrations are managed and charged separately. If you register the same company in multiple AWS accounts, the number of messages that you can send to T-Mobile customers per day is shared across each of those accounts.
2. You can complete the 10DLC registration process in one AWS account, and use AWS Identity and Access Management (IAM) to grant other accounts permission to send through your 10DLC number.

Note

This option allows for true cross-account access to your 10DLC phone numbers. However, note that messages sent from your secondary accounts are treated as if they were sent from your primary account. Quotas and billing are counted against the primary account and not against any secondary accounts.

Setting up cross-account access using IAM policies

You can use IAM roles to associate other accounts with your main account. Then, you can delegate access permissions from your primary account to your secondary accounts by granting them access to the 10DLC numbers in the primary account.

To grant access to a 10DLC number in your primary account

1. If you haven't already done so, complete the 10DLC registration process in the primary account. This process involves three steps:
 - Register your company. For more information, see [10DLC brand registration form](#).
 - Register your 10DLC campaign (use case). For more information, see [10DLC campaign registration form](#).
 - Associate a phone number with your 10DLC campaign. For more information, see [Associating a long code with a 10DLC campaign](#).
2. Create an IAM role in your primary account that allows another account to call the `SendTextMessage` API operation for your 10DLC phone number. For more information on creating roles, see [Creating IAM roles](#) in the *IAM User Guide*.
3. Delegate and test access permission from your primary account using IAM roles with any of your other accounts that need to use your 10DLC numbers. For example, you might delegate access permission from your Production account to your Development account. For more information about delegating and testing permissions, see [Delegate access across AWS account using IAM roles](#) in the *IAM User Guide*.
4. Using the new role, send a message using a 10DLC number from a secondary account. For more information about using a role, see [Using IAM roles](#) in the *IAM User Guide*.

Configuration sets

A *configuration set* is a set of rules that are applied when you send a message. For example, a configuration set can specify a destination for events related to a message. When SMS events occur (such as delivery or failure events), they are routed to the destination associated with the configuration set that you specified when you sent the message. You're not required to use configuration sets when you send messages, but we recommend that you do. If you don't specify a configuration set with an event destination, the API doesn't emit event records. These event records are a useful way to determine how many messages you sent, how much you paid for each one, and whether or not the message was received by the recipient.

Topics

- [Managing configuration set](#)
- [Managing event destinations](#)

- [Edit a configuration sets protect configuration association](#)

Managing configuration set

This section contains information about using the AWS CLI and Amazon Pinpoint SMS console to manage configuration sets. The procedures in this section assume that you've already configured the AWS CLI. For more information, see [Getting started with the AWS CLI](#) in the *AWS Command Line Interface User Guide*.

Note

After you've created the configuration set you need to add at least one event destination to record events to. For more information, see [Managing event destinations](#).
Optionally you can associate the configuration set with a protect configuration to build custom lists of country rules for allowing or blocking messages to specific destination countries. To learn more see [Edit a configuration sets protect configuration association](#) and [Protect configuration](#).

Creating a configuration set (Console)

To create a configuration set using the Amazon Pinpoint SMS console, follow these steps:

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Configuration sets** and then **Create configuration set**.
3. For **Configuration set name** enter a descriptive name for the configuration set.
4. Choose **Create configuration set**.

Creating a configuration set (AWS CLI)

You can use the [create-configuration-set](#) command to create a new configuration set.

```
$ aws pinpoint-sms-voice-v2 create-configuration-set \  
> --configuration-set-name configurationSet
```

In the preceding command, replace *configurationSet* with the name of the configuration set that you want to create.

Deleting a configuration set (Console)

To delete a configuration set using the Amazon Pinpoint SMS console, follow these steps:

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Configuration sets**.
3. Select the **Configuration set** you want to delete and then choose **Delete**.

Deleting a configuration set (AWS CLI)

You can use the [delete-configuration-set](#) command to delete a configuration set.

```
$ aws pinpoint-sms-voice-v2 delete-configuration-set \  
> --configuration-set-name configurationSet
```

In the preceding command, replace *configurationSet* with the name of the configuration set that you want to delete.

Edit configuration set settings (Console)

To edit a configuration set using the Amazon Pinpoint SMS console, follow these steps:

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Configuration sets**.
3. On the **Configuration sets** page, choose the configuration set to edit.
4. Select the **Set settings** tab and then choose **Edit settings**.
5. In **List settings** do the following:
 - **Message type** choose either:
 - **Promotional** – Choose this option for sending marketing messages or messages promoting your business or service.
 - **Transactional** – Choose this option for sending time-sensitive messages, such as password resets or transaction alerts.
 - **Default sender ID** – Choose the default sender ID for the configuration set.
6. Choose **Save changes**.

List configuration sets (AWS CLI)

You can use the [describe-configuration-sets](#) command to view information about the configuration sets in your Amazon Pinpoint SMS account.

To view a list of the configuration sets in your account using the AWS CLI

- At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 describe-configuration-sets
```

Describe a configuration set (AWS CLI)

You can use the [describe-configuration-sets](#) command to view information about a configuration set in your Amazon Pinpoint SMS account.

To view information about specific configuration sets using the AWS CLI

- At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 describe-configuration-sets \  
> --configuration-set-names configurationSet
```

In the preceding command, replace *configurationSet* with the name of the configuration set that you want to find the details of. You can also specify multiple configuration sets by separating the name of each configuration set with a space.

Manage tags (Console)

Use the Amazon Pinpoint SMS console to add, edit or delete a Tag.

Add a Tag (Console)

- Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
- In the navigation pane, under **Configurations**, choose **Configuration sets**.
- On the **Configuration sets** page, choose the configuration set to add a tag to.
- On the **Tags** tab, choose **Manage tags**.
- Add a tag** – In **Manage tags**, choose **Add new tag** to create a new blank key/value pair.
 - Delete a tag** – In **Manage tags**, choose **Remove** next to the key/value pair.

- **Edit a tag** – In **Manage tags**, choose the **Key** or **Value** and edit the text.
6. Choose **Save changes**.

Manage tags (AWS CLI)

Use the AWS CLI to add or edit a Tag.

```
$ aws pinpoint-sms-voice-v2 tag-resource \  
  --resource-arn resource-arn \  
  --tags tags={key1=value1,key2=value2}
```

In the preceding example, do the following:

- Replace *resource-arn* with the Amazon Resource Name (ARN) that you want to add the tags to.
- Replace *key1* and *key2* with the keys of the tags that you want to add to the resource.
- Replace *value1* and *value2* with the values of the tags that you want to add for the respective keys.

Use the AWS CLI to delete a Tag.

```
$ aws pinpoint-sms-voice-v2 untag-resource \  
  --resource-arn resource-arn \  
  --tag-keys tags={key1=value1,key2=value2}
```

In the preceding example, do the following:

- Replace *resource-arn* with the Amazon Resource Name (ARN) that you want to remove the tag from.
- Replace *key1* and *key2* with the keys of the tags that you want to remove.
- Replace *value1* and *value2* with the values of the tags that you want to remove.

Managing event destinations

An *event destination* is a location (such as a CloudWatch Group, a Amazon Data Firehose stream, or an Amazon SNS topic) that SMS and voice events are sent to. To use event destinations, you first create the destination, and then associate it with a [Configuration sets](#). You can associate up to five

event destinations with a single configuration set. When you send a message, your call to the API includes a reference to the configuration set.

Prerequisites

You need to have already created a configuration set to associate the event destinations with, see [Configuration sets](#).

Topics

- [Event types for SMS, MMS, and voice](#)
- [Example event data](#)
- [Amazon CloudWatch event destinations](#)
- [Amazon Data Firehose event destinations](#)
- [Amazon SNS event destinations](#)

Event types for SMS, MMS, and voice

The easiest way to use event destinations is to send all SMS, MMS and voice events to a single destination. However, you can configure event destinations so that specific types of events are sent to different destinations. For example, you could send all delivery-related events to Firehose for storage, and all failure events to an Amazon SNS topic so that you can be notified when they occur. You can also send SMS events and voice events to different locations.

You can configure event destinations to send the following types of events:

SMS, MMS, and Voice events

- **ALL** – Sends all SMS, MMS, and voice events to the specified destination.

SMS events

- **TEXT_ALL** – Sends all SMS events to the specified destination.
- **TEXT_DELIVERED (Delivered)** – Sends all SMS delivery events to the specified destination.
- **TEXT_SUCCESSFUL (Successful)** – Sends all SMS success events to the specified destination. Success events occur when the message is accepted by the recipient's carrier.
- **TEXT_QUEUED (Queued)** – Sends all SMS queued events to the specified destination. Queued events occur when the message is queued for delivery, but not delivered yet.

- **TEXT_PENDING (Pending)** – Sends all SMS pending events to the specified destination. Pending events occur when a message is in the process of being delivered, but hasn't been delivered (or failed to be delivered) yet.
- **TEXT_BLOCKED (Blocked)** – Sends all SMS blocked events to the specified destination. Blocked events occur when the recipient's device or carrier is blocking messages to that recipient.
- **TEXT_TTL_EXPIRED (TTL expired)** – Sends all SMS TTL Expired events to the specified destination. TTL Expired events occur when the time required to deliver the message exceeds the TTL value that you specified when you sent the message.
- **TEXT_CARRIER_UNREACHABLE (Carrier unreachable)** – Sends all Carrier Unreachable events for SMS messages to the specified destination. Carrier Unreachable events occur when a transient error occurs on the carrier network of the message recipient.
- **TEXT_INVALID (SMS invalid)** – Sends all SMS invalid events to the specified destination. Invalid events occur when the destination phone number is not valid.
- **TEXT_INVALID_MESSAGE (Invalid message)** – Sends all invalid message events for SMS messages to the specified destination. Invalid message events occur when the body of the SMS message is invalid and can't be delivered.
- **TEXT_CARRIER_BLOCKED (Carrier blocked)** – Sends all carrier blocked events for SMS messages to the specified destination. Carrier blocked events occur when the recipient's carrier blocks the delivery of the message. This typically occurs when the carrier identifies the message as malicious (for example, if the message contains information related to a phishing scam) or abusive (for example, if the message is suspected of being unsolicited or prohibited content).
- **TEXT_UNREACHABLE (Unreachable)** – Sends all unreachable events for SMS messages to the specified destination. Unreachable events occur when the recipient's device is unavailable. This might occur if the device is not connected to a mobile network, or is powered off.
- **TEXT_SPAM (Spam)** – Sends all spam events for SMS messages to the specified destination. Spam events occur when the recipient's carrier identifies the message as containing unsolicited commercial content and blocks the delivery of the message.
- **TEXT_UNKNOWN (Unknown)** – Sends all unknown SMS events to the specified destination. Unknown events occur when a message fails to be delivered for a reason that isn't covered by one of the other event types. Unknown errors might be transient or permanent.

Voice events

- **VOICE_ALL** – Sends all voice events to the specified destination.

- **VOICE_COMPLETED (Completed)** – Sends all completed events for voice messages to the specified destination. Completed events occur when the audio message is played to the recipient. This status doesn't necessarily mean that the message was delivered to a human recipient. For example, it could indicate that the message was delivered to a voicemail system.
- **VOICE_ANSWERED (Answered)** – Sends all answered events for voice messages to the specified destination. Answered events occur when the recipient answers the phone.
- **VOICE_INITIATED (Initiated)** – Sends events to the specified destination each time a voice message is initiated.
- **VOICE_TTL_EXPIRED (TTL expired)** – Sends all voice TTL Expired events to the specified destination. TTL Expired events occur when the time required to deliver the message exceeds the TTL value that you specified when you sent the message.
- **VOICE_BUSY (Busy)** – Sends all busy events for voice messages to the specified destination. Busy events occur when the recipient's phone line is busy.
- **VOICE_NO_ANSWER (No answer)** – Sends all no answer events for voice messages to the specified destination. No answer events occur after the call has been placed, but the recipient (or their voicemail system) never answer.
- **VOICE_RINGING (Ringing)** – Sends all ringing events for voice messages to the specified destination. Ringing events occur after the call has been placed, but before the recipient answers.
- **VOICE_FAILED (Failed)** – Sends all voice message failure events to the specified destination. Failure events occur when the message fails to be delivered.

MMS events

- **MEDIA_ALL** – Sends all MMS events to the specified destination.
- **MEDIA_PENDING (Pending)** – Sends all MMS pending events to the specified destination. Pending events occur when a message is in the process of being delivered, but hasn't been delivered (or failed to be delivered) yet.
- **MEDIA_QUEUED (Queue)** – Sends all MMS queued events to the specified destination. Queued events occur when the message is queued for delivery, but not delivered yet.
- **MEDIA_SUCCESSFUL (Successful)** – Sends all MMS success events to the specified destination. Success events occur when the message is accepted by the recipient's carrier.
- **MEDIA_DELIVERED (Delivered)** – Sends all MMS delivery events to the specified destination.
- **MEDIA_INVALID (MMS invalid)** – Sends all MMS invalid events to the specified destination. Invalid events occur when the destination phone number is not valid.

- **MEDIA_INVALID_MESSAGE (Invalid message)** – Sends all invalid message events for MMS messages to the specified destination. Invalid message events occur when the body of the MMS message is invalid and can't be delivered.
- **MEDIA_UNREACHABLE (Unreachable)** – Sends all unreachable events for MMS messages to the specified destination. Unreachable events occur when the recipient's device is unavailable. This might occur if the device is not connected to a mobile network, or is powered off.
- **MEDIA_CARRIER_UNREACHABLE (Carrier unreachable)** – Sends all Carrier Unreachable events for MMS messages to the specified destination. Carrier Unreachable events occur when a transient error occurs on the carrier network of the message recipient.
- **MEDIA_BLOCKED (Blocked)** – Sends all MMS blocked events to the specified destination. Blocked events occur when the recipient's device or carrier is blocking messages to that recipient.
- **MEDIA_CARRIER_BLOCKED (Carrier blocked)** – Sends all carrier blocked events for MMS messages to the specified destination. Carrier blocked events occur when the recipient's carrier blocks the delivery of the message. This typically occurs when the carrier identifies the message as malicious (for example, if the message contains information related to a phishing scam) or abusive (for example, if the message is suspected of being unsolicited or prohibited content).
- **MEDIA_SPAM (Spam)** – Sends all spam events for MMS messages to the specified destination. Spam events occur when the recipient's carrier identifies the message as containing unsolicited commercial content and blocks the delivery of the message.
- **MEDIA_UNKNOWN (Unknown)** – Sends all unknown MMS events to the specified destination. Unknown events occur when a message fails to be delivered for a reason that isn't covered by one of the other event types. Unknown errors might be transient or permanent.
- **MEDIA_TTL_EXPIRED (TTL expired)** – Sends all MMS TTL Expired events to the specified destination. TTL Expired events occur when the time required to deliver the message exceeds the TTL value that you specified when you sent the message.
- **MEDIA_FILE_TYPE_UNSUPPORTED (File type unsupported)** – Sends all file type unsupported MMS events to the specified destination. File type unsupported events occur when a media file is not in a supported format. For a list of supported file types, see [MMS file types, size and character limits](#)
- **MEDIA_FILE_SIZE_EXCEEDED (File size)** – Sends all file size MMS events to the specified destination. File size exceeded event occur when the media file is larger than 600 KB in size.
- **MEDIA_FILE_INACCESSIBLE (File inaccessible)** – Sends all file inaccessible MMS events to the specified destination. File inaccessible events occur when Amazon Pinpoint SMS doesn't have permissions to access the file.

Example event data

Amazon Pinpoint SMS can stream event data about SMS, MMS, and voice message deliveries. Events generated by carriers can take up to 72 hours to be received and should not be used to determine if there is a delay in outbound message delivery. After 72 hours, if Amazon Pinpoint SMS has not received a final event from a carrier, the service will automatically return an UNKNOWN messageStatus as we do not know what happened to that message.

SMS example log

The JSON object for an SMS event contains the data shown in the following example.

```
{
  "eventType": "TEXT_SUCCESSFUL",
  "eventVersion": "1.0",
  "eventTimestamp": 1686975103470,
  "isFinal": true,
  "originationPhoneNumber": "+12065550152",
  "destinationPhoneNumber": "+14255550156",
  "isoCountryCode": "US",
  "messageId": "862a8790-60c0-4430-9b2b-658bdexample",
  "messageRequestTimestamp": 1686975103170,
  "messageEncoding": "GSM",
  "messageType": "PROMOTIONAL",
  "messageStatus": "SUCCESSFUL",
  "messageStatusDescription": "Message has been accepted by phone carrier",
  "context": {
    "account": "bar"
  },
  "totalMessageParts": 1,
  "totalMessagePrice": 0.09582,
  "totalCarrierFee": 0.0
}
```

Attribute	Description
eventType	The type of event. Values are listed in Event types for SMS, MMS, and voice
eventVersion	The version of the event JSON schema.

Attribute	Description
eventTimestamp	The time when the event was reported, shown as Unix time in milliseconds.
isFinal	True if this is the final status for the message. There are intermediate message statuses and it can take up to 72 hours for the final message status to be received.
originationPhoneNumber	The phone number that the message was sent from.
destinationPhoneNumber	The phone number that you attempted to send the message to.
isoCountryCode	The country that's associated with the recipient's phone number, shown in ISO 3166-1 alpha-2 format.
messageId	The unique ID that Amazon Pinpoint SMS generates when it accepts the message.
messageRequestTimestamp	The time when the SMS message request was received, shown as Unix time in milliseconds.
messageEncoding	The encoding of the message. Possible values are GSM and Unicode . For more information on message encoding, see SMS character limits .
messageType	The type of message. Possible values are Promotional and Transactional .

Attribute	Description
messageStatus	<p>The status of the message. Possible values are:</p> <ul style="list-style-type: none">• SUCCESSFUL – The message has been accepted by the phone carrier.• DELIVERED – The message has been accepted by the recipient's device.• PENDING – The message hasn't yet been delivered to the recipient's device.• INVALID – The destination phone number is invalid.• UNREACHABLE – The recipient's device is currently unreachable or unavailable. For example, the device might be powered off, or might be disconnected from the network. You can try to send the message again later.• UNKNOWN – An error occurred that prevented the delivery of the message. This error is usually transient, and you can attempt to send the message again later.• BLOCKED – The recipient's device is blocking SMS messages from the originator phone number.• CARRIER_UNREACHABLE – An issue with the mobile network of the recipient prevented the message from being delivered. This error is usually transient, and you can attempt to send the message again later.• SPAM – The recipient's mobile carrier identified the contents of the message as spam and blocked delivery of the message.• INVALID_MESSAGE – The body of the SMS message is invalid and can't be delivered.

Attribute	Description
	<ul style="list-style-type: none"> • CARRIER_BLOCKED – The recipient's carrier has blocked delivery of this message. This often occurs when the carrier identifies the contents of the message as unsolicited or malicious. • TTL_EXPIRED – The SMS message couldn't be delivered within a certain time frame. This error is usually transient, and you can attempt to send the message again later. • ACCEPTED – The SMS message was accepted. • FAILED – The SMS message failed to be delivered to the recipient's device. • SENT – The message has been sent but not delivered to the recipient's device. • UNROUTABLE – Not able to route due to a bad account configuration. • QUEUED – The message is queued for delivery
messageStatusDescription	A description of the message status.
context	Custom attributes you can specify and will be logged, when you send a message.

Attribute	Description
totalMessageParts	<p>The number of message parts that Amazon Pinpoint SMS created in order to send the message.</p> <p>Generally, SMS messages can contain only 160 GSM-7 characters or 67 non-GSM characters, although these limits can vary by country . If you send a message that exceeds these limits, Amazon Pinpoint SMS automatically splits the message into smaller parts. We bill you based on the number of message parts that you send. For more information on message parts, see Message Parts per Second (MPS) limits.</p>
totalMessagePrice	<p>The amount that we charged you to send the message. This price is shown in thousandths of a United States cent. For example, if the value of this attribute is 645, then we charged you 0.645¢ to send the message ($645 / 1000 = 0.645¢ = \\$0.00645$).</p>
totalCarrierFee	<p>The total cost of carrier fees for a message.</p>

Voice example event log

The JSON object for a Voice event contains the data shown in the following example.

```
{
  "eventType": "VOICE_COMPLETED",
  "eventVersion": "1.0",
  "eventTimestamp": 1697835373500,
  "isFinal": true,
  "originationPhoneNumber": "+12065550153",
  "destinationPhoneNumber": "+14255550159",
  "isoCountryCode": "US",
```

```

"messageId": "567f6c11-6e8b-4352-9749-a42a0example",
"messageRequestTimestamp": 1697835372720,
"messageStatus": "COMPLETED",
"callDurationInSeconds": 60,
"totalDurationInMinutes": 1,
"totalMessagePrice": 0.013,
"context": {
  "account": "bar"
}
}

```

Attribute	Description
eventType	The type of event. Values are listed in Event types for SMS, MMS, and voice
eventVersion	The version of the event JSON schema.
eventTimestamp	The time when the event was reported, shown as Unix time in milliseconds.
isFinal	True if this is the final status for the message. There are intermediate message statuses.
originationPhoneNumber	The phone number that the message was sent from.
destinationPhoneNumber	The phone number that you attempted to send the message to.
isoCountryCode	The country that's associated with the recipient's phone number, shown in ISO 3166-1 alpha-2 format.
messageId	The unique ID that Amazon Pinpoint SMS generates when it accepts the message.
messageRequestTimestamp	The time when the SMS message request was received, shown as Unix time in milliseconds.
messageStatus	The status of the message. Possible values are:

Attribute	Description
	<ul style="list-style-type: none">• INITIATED – The voice message is ready to start dialing.• RINGING – Ringing events occur after the call has been placed, but before the recipient answers.• COMPLETED – Sends all completed events for voice messages to the specified destination. Completed events occur when the audio message is played to the recipient. This status doesn't necessarily mean that the message was delivered to a human recipient. For example, it could indicate that the message was delivered to a voicemail system.• ANSWERED – Answered events occur when the recipient answers the phone.• COMPLETED – The call was answered and ended.• BUSY – Busy events occur when the recipient's phone line is busy.• NO_ANSWER – No answer events occur after the call has been placed, but the recipient (or their voicemail system) never answer.• FAILED – Failure events occur when the message fails to be delivered.• TTL_EXPIRED – TTL Expired events occur when the time required to deliver the message exceeds the TTL value that you specified when you sent the message.• SPAM – The call was marked as spam and blocked.

Attribute	Description
callDurationInSeconds	The duration of the call in seconds.
totalDurationInMinutes	The duration of the call in minutes.
totalMessagePrice	The amount that we charged you to send the voice message. This price is shown in thousandths of a United States cent.
context	Custom attributes you can specify and will be logged, when you send a message.

MMS example log

The JSON object for an MMS event contains the data shown in the following example.

```
{
  "contentType": "MMS",
  "eventType": "MEDIA_DELIVERED",
  "eventVersion": "1.0",
  "eventTimestamp": 1635197695208,
  "isFinal": true,
  "originationPhoneNumber": "+12065550153",
  "destinationPhoneNumber": "+14255550159",
  "isoCountryCode": "US",
  "messageId": "b4a3196d-5b61-4884-a0d9-745acf1f6235example",
  "messageRequestTimestamp": 1635197693241,
  "messageType": "TRANSACTIONAL",
  "messageStatus": "DELIVERED",
  "messageStatusDescription": "Message has been accepted by phone",
  "context": {"foo": "bar"},
  "totalMessageParts": 1,
  "totalMessagePrice": 0.0195,
  "totalCarrierFee": 0.00266
}
```

Attribute	Description
eventType	The type of event. Values are listed in Event types for SMS, MMS, and voice
eventVersion	The version of the event JSON schema.
eventTimestamp	The time when the event was reported, shown as Unix time in milliseconds.
isFinal	True if this is the final status for the message. There are intermediate message statuses and it can take up to 72 hours for the final message status to be received.
originationPhoneNumber	The phone number that the message was sent from.
destinationPhoneNumber	The phone number that you attempted to send the message to.
isoCountryCode	The country that's associated with the recipient's phone number, shown in ISO 3166-1 alpha-2 format.
messageId	The unique ID that Amazon Pinpoint SMS generates when it accepts the message.
messageRequestTimestamp	The time when the SMS message request was received, shown as Unix time in milliseconds.
messageType	The type of message. Possible values are Promotional and Transactional .
messageStatus	The status of the message. Possible values are: <ul style="list-style-type: none">• SUCCESSFUL – The message has been accepted by the phone carrier.

Attribute	Description
	<ul style="list-style-type: none">• DELIVERED – The message has been accepted by the recipient's device.• PENDING – The message hasn't yet been delivered to the recipient's device.• INVALID – The destination phone number is invalid.• UNREACHABLE – The recipient's device is currently unreachable or unavailable. For example, the device might be powered off, or might be disconnected from the network. You can try to send the message again later.• UNKNOWN – An error occurred that prevented the delivery of the message. This error is usually transient, and you can attempt to send the message again later.• BLOCKED – The recipient's device is blocking SMS/MMS messages from the originator phone number.• CARRIER_UNREACHABLE – An issue with the mobile network of the recipient prevented the message from being delivered. This error is usually transient, and you can attempt to send the message again later.• SPAM – The recipient's mobile carrier identified the contents of the message as spam and blocked delivery of the message.• INVALID_MESSAGE – The body of the SMS/MMS message is invalid and can't be delivered.• CARRIER_BLOCKED – The recipient's carrier has blocked delivery of this message. This often occurs when the carrier identifies the

Attribute	Description
	<p>contents of the message as unsolicited or malicious.</p> <ul style="list-style-type: none"> • TTL_EXPIRED – The SMS message couldn't be delivered within a certain time frame. This error is usually transient, and you can attempt to send the message again later. • ACCEPTED – The SMS message was accepted. • FAILED – The SMS message failed to be delivered to the recipient's device. • SENT – The message has been sent but not delivered to the recipient's device. • UNROUTABLE – Not able to route due to a bad account configuration. • QUEUED – The message is queued for delivery
messageStatusDescription	A description of the message status.
context	Custom attributes you can specify and will be logged, when you send a message.
totalMessageParts	The number of message parts that Amazon Pinpoint SMS created in order to send the message. For more information on message parts, see Message Parts per Second (MPS) limits .
totalMessagePrice	The amount that we charged you to send the message. This price is shown in thousandths of a United States cent. For example, if the value of this attribute is 645, then we charged you 0.645¢ to send the message (645 / 1000 = 0.645¢ = \$0.00645).

Attribute	Description
totalCarrierFee	The total cost of carrier fees for a message.

Amazon CloudWatch event destinations

Amazon CloudWatch Logs is an AWS service that you can use to monitor, store, and access log files. When you create a CloudWatch event destination, Amazon Pinpoint SMS sends the types of events you specified in the event destination to a CloudWatch group. To learn more about CloudWatch, see the [Amazon CloudWatch Logs User Guide](#).

Prerequisites

1. Before you can create a CloudWatch event destination, you must first create a CloudWatch group. For more information about creating log groups, see [Working with log groups and log streams](#) in the *Amazon CloudWatch Logs User Guide*.

Important

You will need the Amazon Resource Name (ARN) of the CloudWatch group to create the event destination.

2. You must create an IAM role that allows Amazon Pinpoint SMS to write to the log group. The following section contains information about the requirements for this role.

Important

You will need the Amazon Resource Name (ARN) of the IAM role to create the event destination.

3. You also have setup a configuration set to associate the event destinations with, see [Managing configuration set](#).

IAM policy for Amazon CloudWatch

Use the following example to create a policy for sending events to a CloudWatch group.

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "logs:CreateLogStream",
      "logs:DescribeLogStreams",
      "logs:PutLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:us-east-1:111122223333:log-group:log-group-name:*"
    ]
  }
]
}

```

For more information about IAM policies, see [Policies and permissions in IAM](#) in the *IAM User Guide*.

The following example statement uses the, optional but recommended, `SourceAccount` and `SourceArn` conditions to check that only the Amazon Pinpoint SMS owner account has access to the configuration set. In this example, replace *accountId* with your AWS account id, *region* with the AWS Region name and *ConfigSetName* with the name of the Configuration Set.

After you create the policy, create a new IAM role, and then attach the policy to it. When you create the role, also add the following trust policy to it:

```

{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "Service": "sms-voice.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "accountId"
      },
      "ArnLike": {
        "aws:SourceArn": "arn:aws:sms-voice:region:accountId:configuration-  
set/ConfigSetName"
      }
    }
  }
}

```

```
}  
}
```

For more information about creating IAM roles, see [Creating IAM roles](#) in the *IAM User Guide*.

Managing Amazon CloudWatch event destinations

After you create the IAM role and the CloudWatch group, you can create the event destination.

Create event destination (Console)

To create an event destination using the Amazon Pinpoint SMS console, follow these steps:

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Configuration sets**.
3. On the **Configuration sets** page, choose the configuration set to add an event destination to.
4. On the **Configuration set details** page, choose **Add destination event**.
5. Under the **Event details** section, enter a friendly name for **Event destination name**.
6. From the **Destination type** dropdown choose Amazon CloudWatch.
7. For **IAM role arn** enter the ARN of the IAM role. For more information on the IAM role arn, see [IAM policy for Amazon CloudWatch](#).
8. For **Log group arn** enter the ARN of the Amazon CloudWatch log group to deliver the events to.
9. Turn on **Event publishing**.
10. Under **Event types**, choose:
 - **All SMS events (Recommended)** – Choose this option to send all SMS events listed in [Event types for SMS, MMS, and voice](#) to Amazon CloudWatch.
 - **Custom SMS events** – Choose specific SMS events to send to CloudWatch. To edit the list of events choose **Edit SMS event selection**. On **Edit SMS event selection** check only the events you want to send to Amazon CloudWatch. Choose **Save selection**.
 - **All voice events (Recommended)** – Choose this option to send all voice events listed in [Event types for SMS, MMS, and voice](#) to Amazon CloudWatch.
 - **Custom voice events** – Choose specific voice events to send to CloudWatch. To edit the list of events choose **Edit voice event selection**. On **Edit voice event selection** check only the events you want to send to Amazon CloudWatch. Choose **Save selection**.

- **All MMS events (Recommended)** – Choose this option to send all MMS events listed in [Event types for SMS, MMS, and voice](#) to Amazon CloudWatch.
- **Custom MMS events** – Choose specific MMS events to send to CloudWatch. To edit the list of events choose **Edit MMS event selection**. On **Edit MMS event selection** check only the events you want to send to Amazon CloudWatch. Choose **Save selection**.

11. Choose **Create event**.

Create event destination (AWS CLI)

You can use the [create-event-destination](#) command to create an event destination.

At the command line, run the following command:

```
$ aws pinpoint-sms-voice-v2 create-event-destination \  
> --event-destination-name eventDestinationName \  
> --configuration-set-name configurationSet \  
> --matching-event-types eventTypes \  
> --cloud-watch-logs-destination  
  IamRoleArn=arn:aws:iam::111122223333:role/CWLSMSRole,LogGroupArn=arn:aws:logs:us-  
east-1:111122223333:log-group:MyCWLLogGroup
```

In the preceding command, make the following changes:

- Replace *eventDestinationName* with a name that describes the event destination.
- Replace *configurationSet* with the name of the configuration set that you want to associate the event destination with.
- Replace *eventTypes* with one or more of the event types listed in [Event types for SMS, MMS, and voice](#).
- Replace the value of `IamRoleArn` with the Amazon Resource Name (ARN) of an IAM role that has the policies described in [IAM policy for Amazon CloudWatch](#).
- Replace the value of `LogGroupArn` with the ARN of the CloudWatch group that you want to send events to.

Update event destination (Console)

To update an event destination using the Amazon Pinpoint SMS console, follow these steps:

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.

2. In the navigation pane, under **Configurations**, choose **Configuration sets**.
3. On the **Configuration sets** page, choose the configuration set to edit.
4. On the **Event settings** tab, choose a Amazon CloudWatch event destination and then **Edit**.
5. For **IAM role arn** enter the ARN of the IAM role. For more information about the IAM role arn, see [IAM policy for Amazon CloudWatch](#).
6. For **Log group arn** enter the ARN of the Amazon CloudWatch log group to deliver the events to.
7. Under **Event types**, choose:
 - **All SMS events (Recommended)** – Choose this option to send all SMS events listed in [Event types for SMS, MMS, and voice](#) to Amazon CloudWatch.
 - **Custom SMS events** – Choose this option choose specific SMS events to send to CloudWatch. To edit the list of events choose **Edit SMS event selection**. On **Edit SMS event selection** check only the events you want to send to Amazon CloudWatch. Choose **Save selection**.
 - **All voice events (Recommended)** – Choose this option to send all voice events listed in [Event types for SMS, MMS, and voice](#) to Amazon CloudWatch.
 - **Custom voice events** – Choose this option choose specific voice events to send to CloudWatch. To edit the list of events choose **Edit voice event selection**. On **Edit voice event selection** check only the events you want to send to Amazon CloudWatch. Choose **Save selection**.
 - **All MMS events (Recommended)** – Choose this option to send all MMS events listed in [Event types for SMS, MMS, and voice](#) to Amazon CloudWatch.
 - **Custom MMS events** – Choose this option choose specific MMS events to send to CloudWatch. To edit the list of events choose **Edit MMS event selection**. On **Edit MMS event selection** check only the events you want to send to Amazon CloudWatch. Choose **Save selection**.
8. Choose **Edit event**.

Update event destination AWS CLI)

You can use the [update-event-destination](#) command to update an event destination.

The procedure for updating a CloudWatch event destination is similar to the process for creating an event destination. At the command line, run the following command:

```
$ aws pinpoint-sms-voice-v2 update-event-destination \  
> --event-destination-name eventDestinationName \  
> --configuration-set-name configurationSet \  
> --matching-event types eventTypes \  
> --cloud-watch-logs-destination  
  IamRoleArn=arn:aws:iam::111122223333:role/CWLSMSRole,LogGroupArn=arn:aws:logs:us-  
east-1:111122223333:log-group:MyCWLLogGroup
```

In the preceding command, make the following changes:

- Replace *eventDestinationName* with a name of the event destination that you want to modify.
- Replace *configurationSet* with the name of the configuration set that you want to associate the event destination with. You can associate the event destination with a different configuration set.
- Replace *eventTypes* with one of the event types listed in [Event types for SMS, MMS, and voice](#).
- Replace the value of `IamRoleArn` with the Amazon Resource Name (ARN) of an IAM role that has the policies described in [Event types for SMS, MMS, and voice](#).
- Replace the value of `LogGroupArn` with the ARN of the CloudWatch group that you want to send events to.

Delete an CloudWatch event destination (Console)

The process for deleting an event destination is the same regardless of the type of event destination that you want to delete.

To delete an CloudWatch event destination in the Console

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Configuration sets**.
3. On the **Configuration sets** page, choose the configuration set to remove an event destination from.
4. In the **All destinations** section choose an event destination and then choose **Delete**.

Delete an CloudWatch event destination (AWS CLI)

You can use the [delete-event-destination](#) command to delete an event destination.

The process for deleting an event destination is the same regardless of the type of event destination that you want to delete.

To delete an CloudWatch event destination in the AWS CLI

- At the command line, run the following command:

```
$ aws pinpoint-sms-voice-v2 delete-event-destination \  
> --event-destination-name eventDestinationName \  
> --configuration-set-name configurationSetName
```

In the preceding command, make the following changes:

- Replace *eventDestinationName* with the name or Amazon Resource Name (ARN) of the event destination that you want to delete.
- Replace *configurationSetName* with the name or ARN of the configuration set that the event destination is associated with.

Amazon Data Firehose event destinations

Amazon Data Firehose is a fully managed service for delivering real-time streaming data to multiple types of destinations. Amazon Data Firehose is part of the Kinesis streaming data platform. To learn more about Amazon Data Firehose, see the [Amazon Data Firehose Developer Guide](#).

Some of the examples in this section assume that you've already installed and configured the AWS Command Line Interface. For more information about setting up the AWS CLI, see the [AWS Command Line Interface User Guide](#).

Prerequisites

1. Before you can create a Amazon Data Firehose event destination, you must first create a Amazon Data Firehose delivery stream. For more information about creating streams, see [Creating an Amazon Data Firehose Delivery Stream](#) in the *Amazon Data Firehose Developer Guide*.

⚠ Important

You will need the Amazon Resource Name (ARN) of the Amazon Data Firehose delivery stream to create the event destination.

2. You have to create an IAM role that allows Amazon Pinpoint SMS to write to the delivery stream, see [IAM policy for Amazon Data Firehose](#).

⚠ Important

You will need the Amazon Resource Name (ARN) of the IAM role to create the event destination.

3. You also have setup a configuration set to associate the event destinations with, see [Managing configuration set](#).

Topics in this section:

- [Creating Amazon Data Firehose event destinations](#)
- [Managing Amazon Data Firehose event destination](#)

Creating Amazon Data Firehose event destinations

Before you can create a Amazon Data Firehose event destination, you must first create a Amazon Data Firehose stream. For more information about creating log groups, see [Creating an Amazon Data Firehose Delivery Stream](#) in the *Amazon Data Firehose Developer Guide*.

You have to create an IAM role that allows the Amazon Pinpoint SMS and Voice v2 API to send data to the stream. The following section contains information about the requirements for this role.

You also have already setup a configuration set to associate the event destinations with, see [Configuration sets](#).

IAM policy for Amazon Data Firehose

Use the following example to create a policy for sending events to a Amazon Data Firehose stream.

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": "firehose:PutRecord",
    "Resource": "arn:aws:firehose:us-
east-1:111122223333:deliverystream/DeliveryStreamName"
  }
]
}

```

For more information about IAM policies, see [Policies and permissions in IAM](#) in the *IAM User Guide*.

The following example statement uses the, optional but recommended, `SourceAccount` and `SourceArn` conditions to check that only the Amazon Pinpoint SMS owner account has access to the configuration set. In this example, replace *accountId* with your AWS account id, *region* with the AWS Region name and *ConfigSetName* with the name of the Configuration Set.

After you create the policy, create a new IAM role, and then attach the policy to it. When you create the role, also add the following trust policy to it:

```

{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "Service": "sms-voice.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "accountId"
      },
      "ArnLike": {
        "aws:SourceArn": "arn:aws:sms-voice:region:accountId:configuration-
set/ConfigSetName"
      }
    }
  }
}

```

For more information about creating IAM roles, see [Creating IAM roles](#) in the *IAM User Guide*.

Managing Amazon Data Firehose event destination

Create Amazon Data Firehose event destination (Console)

To create an Amazon Data Firehose event destination using the Amazon Pinpoint SMS console, follow these steps:

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Configuration sets**.
3. On the **Configuration sets** page, choose the configuration set to add an event destination to.
4. On the **Configuration set details** page, choose **Add destination event**.
5. Under the **Event details** section, enter a friendly name for **Event destination name**.
6. From the **Destination type** dropdown choose Amazon Data Firehose.
7. For **IAM role arn** enter the ARN of the IAM role. For more information on the IAM role arn, see [IAM policy for Amazon Data Firehose](#).
8. For **Delivery stream arn** enter the ARN of the Amazon Data Firehose log group to deliver the events to.
9. Turn on **Event publishing**.
10. Under **Event types**, choose:
 - **All SMS events (Recommended)** – Choose this option to send all SMS events listed in [Event types for SMS, MMS, and voice](#) to Amazon Data Firehose.
 - **Custom SMS events** – Choose specific SMS events to send to Amazon Data Firehose. To edit the list of events choose **Edit SMS event selection**. On **Edit SMS event selection** check only the events you want to send to Amazon Data Firehose. Choose **Save selection**.
 - **All voice events (Recommended)** – Choose this option to send all voice events listed in [Event types for SMS, MMS, and voice](#) to Amazon Data Firehose.
 - **Custom voice events** – Choose specific voice events to send to Amazon Data Firehose. To edit the list of events choose **Edit voice event selection**. On **Edit voice event selection** check only the events you want to send to Amazon Data Firehose. Choose **Save selection**.
 - **All MMS events (Recommended)** – Choose this option to send all MMS events listed in [Event types for SMS, MMS, and voice](#) to Amazon Data Firehose.

- **Custom MMS events** – Choose t specific MMS events to send to Amazon Data Firehose. To edit the list of events choose **Edit MMS event selection**. On **Edit MMS event selection** check only the events you want to send to Amazon Data Firehose. Choose **Save selection**.

11. Choose **Create event**.

Create Amazon Data Firehose event destination (AWS CLI)

After you create the IAM role and the Amazon Data Firehose delivery stream, you can create the event destination.

You can use the [create-event-destination](#) command to create an event destination.

```
$ aws pinpoint-sms-voice-v2 create-event-destination \  
> --event-destination-name eventDestinationName \  
> --configuration-set-name configurationSet \  
> --matching-event-types eventTypes \  
> --kinesis-firehose-destination  
  IamRoleArn=arn:aws:iam::111122223333:role/  
  AKFSMSRole,DeliveryStreamArn=arn:aws:firehose:us-  
  east-1:111122223333:deliverystream/MyDeliveryStream
```

In the preceding command, make the following changes:

- Replace *eventDestinationName* with a name that describes the event destination.
- Replace *configurationSet* with the name of the configuration set that you want to associate the event destination with.
- Replace *eventTypes* with one or more of the event types listed in [Event types for SMS, MMS, and voice](#).
- Replace the value of `IamRoleArn` with the Amazon Resource Name (ARN) of an IAM role that has the policies described in [IAM policy for Amazon Data Firehose](#).
- Replace the value of `DeliveryStreamArn` with the ARN of the Amazon Data Firehose stream that you want to send events to.

Update Amazon Data Firehose event destination (Console)

To update an Amazon Data Firehose event destination using the Amazon Pinpoint SMS console, follow these steps:

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Configuration sets**.
3. On the **Configuration sets** page, choose the configuration set to add an event destination to.
4. On the **Configuration sets** page, choose the configuration set to edit.
5. On the **Configuration set details** page, choose a Amazon Data Firehose event destination and then **Edit**.
6. For **IAM role arn** enter the ARN of the IAM role. For more information on the IAM role arn, see [IAM policy for Amazon Data Firehose](#).
7. For **Delivery stream arn** enter the ARN of the Amazon Data Firehose log group to deliver the events to.
8. Under **Event types**, choose:
 - **All SMS events (Recommended)** – Choose this option to send all SMS events listed in [Event types for SMS, MMS, and voice](#) to Amazon Data Firehose.
 - **Custom SMS events** – Choose this option choose specific SMS events to send to CloudWatch. To edit the list of events choose **Edit SMS event selection**. On **Edit SMS event selection** check only the events you want to send to Amazon Data Firehose. Choose **Save selection**.
 - **All voice events (Recommended)** – Choose this option to send all voice events listed in [Event types for SMS, MMS, and voice](#) to Amazon Data Firehose.
 - **Custom voice events** – Choose this option choose specific voice events to send to Amazon Data Firehose. To edit the list of events choose **Edit voice event selection**. On **Edit voice event selection** check only the events you want to send to Amazon Data Firehose. Choose **Save selection**.
 - **All MMS events (Recommended)** – Choose this option to send all MMS events listed in [Event types for SMS, MMS, and voice](#) to Amazon Data Firehose.
 - **Custom MMS events** – Choose this option choose specific MMS events to send to CloudWatch. To edit the list of events choose **Edit MMS event selection**. On **Edit MMS event selection** check only the events you want to send to Amazon Data Firehose. Choose **Save selection**.
9. Choose **Edit event**.

Update Amazon Data Firehose event destination (AWS CLI)

You can use the [update-event-destination](#) command to update an event destination.

The procedure for updating a Amazon Data Firehose event destination is similar to the process for creating an event destination.

```
$ aws pinpoint-sms-voice-v2 create-event-destination \  
> --event-destination-name eventDestinationName \  
> --configuration-set-name configurationSet \  
> --matching-event-types eventTypes \  
> --kinesis-firehose-destination  
  IamRoleArn=arn:aws:iam::111122223333:role/  
  AKFSMSRole,DeliveryStreamArn=arn:aws:firehose:us-  
  east-1:111122223333:deliverystream/MyDeliveryStream
```

In the preceding command, make the following changes:

- Replace *eventDestinationName* with a name of the event destination that you want to modify.
- Replace *configurationSet* with the name of the configuration set that you want to associate the event destination with. You can associate the event destination with a different configuration set.
- Replace *eventTypes* with one of the event types listed in [Event types for SMS, MMS, and voice](#).
- Replace the value of `IamRoleArn` with the Amazon Resource Name (ARN) of an IAM role that has the policies described in [IAM policy for Amazon Data Firehose](#).
- Replace the value of `DeliveryStreamArn` with the ARN of the Amazon Data Firehose stream that you want to send events to.

Delete an Amazon Data Firehose event destination (Console)

The process for deleting an event destination is the same regardless of the type of event destination that you want to delete.

To delete an Amazon Data Firehose event destination in the Console

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.

2. In the navigation pane, under **Configurations**, choose **Configuration sets**.
3. On the **Configuration sets** page, choose the configuration set to remove an event destination from.
4. In the **All destinations** section choose an event destination and then choose **Delete**.

Delete an Amazon Data Firehose event destination (AWS CLI)

You can use the [delete-event-destination](#) command to delete an event destination.

The process for deleting an event destination is the same regardless of the type of event destination that you want to delete.

To delete an Amazon Data Firehose event destination in the AWS CLI

- At the command line, run the following command:

```
$ aws pinpoint-sms-voice-v2 delete-event-destination \  
> --event-destination-name eventDestinationName \  
> --configuration-set-name configurationSetName
```

In the preceding command, make the following changes:

- Replace *eventDestinationName* with the name or Amazon Resource Name (ARN) of the event destination that you want to delete.
- Replace *configurationSetName* with the name or ARN of the configuration set that the event destination is associated with.

Amazon SNS event destinations

Amazon Simple Notification Service (Amazon SNS) is a web service that enables applications, end-users, and devices to instantly send and receive notifications. To learn more about Amazon SNS, see the [Amazon Simple Notification Service Developer Guide](#).

Some of the examples in this section assume that you've already installed and configured the AWS Command Line Interface. For more information about setting up the AWS CLI, see the [AWS Command Line Interface User Guide](#).

Topics in this section:

- [Creating Amazon SNS event destinations](#)
- [Managing Amazon SNS event destination](#)

Creating Amazon SNS event destinations

Before you can create an Amazon SNS event destination, you must first create an Amazon SNS topic. For more information about creating Amazon SNS topics, see [Creating a topic](#) in the *Amazon Simple Notification Service Developer Guide*.

You must also have already setup a configuration set to associate the event destinations with, see [Configuration sets](#).

Amazon SNS access policy

Access to an Amazon SNS topic is controlled by a *resource policy* attached to the Amazon SNS topic, this is also called an *access policy*. For more information about Amazon SNS *access policies*, see [Identity and access management](#) in the *Amazon SNS Developer Guide*. Update the *access policy* with the following statement to permit Amazon Pinpoint SMS to publish to the Amazon SNS topic.

- Replace `111122223333` with the unique ID for your AWS account.
- Replace `TopicName` with the name of the Amazon SNS topic.
- Replace `Region` with the AWS Region that contains the Amazon SNS topic and configuration set.
- Replace `ConfigSetName` with the name of the configuration set.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "sms-voice.amazonaws.com"
      },
      "Action": "sns:Publish",
      "Resource": "arn:aws:sns:Region:111122223333:TopicName",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "accountId"
        },
        "ArnLike": {
```

```

    "aws:SourceArn": "arn:aws:sms-voice:Region:111122223333:configuration-
set/ConfigSetName"
  }
}
]
}

```

Managing Amazon SNS event destination

Create an Amazon SNS event destination (Console)

To create an Amazon SNS event destination using the Amazon Pinpoint SMS console, follow these steps:

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Configuration sets**.
3. On the **Configuration sets** page, choose the configuration set to add an event destination to.
4. On the **Configuration set details** page, choose **Add destination event**.
5. Under the **Event details** section, enter a name.
6. From the **Destination type** dropdown choose Amazon SNS.
 - a. **New Amazon SNS topic** – Choose this option, for Amazon Pinpoint SMS to create a topic in your account. The topic is automatically created with all of the required permissions. For more information on Amazon SNS topics see [Configuring Amazon SNS](#) in the [Amazon Simple Notification Service Developer Guide](#).
 - b. **Existing Amazon SNS topic** – Choose this option if you have an existing Amazon SNS topic in the **Topic arn** dropdown.
7. Under **Event types**, choose:
 - **All SMS events (Recommended)** – Choose this option to send all SMS events listed in [Event types for SMS, MMS, and voice](#) to Amazon SNS.
 - **Custom SMS events** – Choose t specific SMS events to send to Amazon SNS. To edit the list of events choose **Edit SMS event selection**. On **Edit SMS event selection** check only the events you want to send to Amazon SNS. Choose **Save selection**.
 - **All voice events (Recommended)** – Choose this option to send all voice events listed in [Event types for SMS, MMS, and voice](#) to Amazon SNS.

- **Custom voice events** – Choose t specific voice events to send to Amazon SNS. To edit the list of events choose **Edit voice event selection**. On **Edit voice event selection** check only the events you want to send to Amazon SNS. Choose **Save selection**.
- **All MMS events (Recommended)** – Choose this option to send all MMS events listed in [Event types for SMS, MMS, and voice](#) to Amazon SNS.
- **Custom MMS events** – Choose specific MMS events to send to Amazon SNS. To edit the list of events choose **Edit MMS event selection**. On **Edit MMS event selection** check only the events you want to send to Amazon SNS. Choose **Save selection**.

8. Choose **Create event**.

Create an Amazon SNS event destination (AWS CLI)

You can use the [create-event-destination](#) command to create an event destination.

```
$ aws pinpoint-sms-voice-v2 create-event-destination \  
> --event-destination-name eventDestinationName \  
> --configuration-set-name configurationSet \  
> --matching-event-types eventTypes \  
> --sns-destination TopicArn=arn:aws:sns:us-east-1:111122223333:snsTopic
```

In the preceding command, make the following changes:

- Replace *eventDestinationName* with a descriptive name for the event destination.
- Replace *configurationSet* with the name of the configuration set that you want to associate the event destination with.
- Replace *eventTypes* with one of the event types listed in [Event types for SMS, MMS, and voice](#).
- Replace the value of TopicArn with the Amazon Resource Name (ARN) of the Amazon SNS topic that you want to send events to.

Update an Amazon SNS event destination (Console)

To update an Amazon Pinpoint SMS event destination using the Amazon Pinpoint SMS console, follow these steps:

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.

2. In the navigation pane, under **Configurations**, choose **Configuration sets**.
3. On the **Configuration sets** page, choose the configuration set to add an event destination to.
4. On the **Configuration sets** page, choose the configuration set to edit.
5. On the **Configuration set details** page, choose a Amazon SNS event destination and then **Edit**.
6. From the **Destination type** dropdown choose Amazon SNS.
 - a. **New Amazon SNS topic** – Choose this option, Amazon Pinpoint SMS creates a topic in your account. The topic is automatically created with all of the required permissions. For more information on Amazon SNS topics see [Configuring Amazon SNS](#) in the [Amazon Simple Notification Service Developer Guide](#).
 - b. **Existing Amazon SNS topic** – Choose this option if you have an existing Amazon SNS topic in the **Topic arn** dropdown.
7. Under **Event types**, choose:
 - **All SMS events (Recommended)** – Choose this option to send all SMS events listed in [Event types for SMS, MMS, and voice](#) to Amazon SNS.
 - **Custom SMS events** – Choose this option choose specific SMS events to send to Amazon SNS. To edit the list of events choose **Edit SMS event selection**. On **Edit SMS event selection** check only the events you want to send to Amazon SNS. Choose **Save selection**.
 - **All voice events (Recommended)** – Choose this option to send all voice events listed in [Event types for SMS, MMS, and voice](#) to Amazon SNS.
 - **Custom voice events** – Choose this option choose specific voice events to send to Amazon SNS. To edit the list of events choose **Edit voice event selection**. On **Edit voice event selection** check only the events you want to send to Amazon SNS. Choose **Save selection**.
 - **All MMS events (Recommended)** – Choose this option to send all MMS events listed in [Event types for SMS, MMS, and voice](#) to Amazon SNS.
 - **Custom MMS events** – Choose this option choose specific MMS events to send to Amazon SNS. To edit the list of events choose **Edit MMS event selection**. On **Edit MMS event selection** check only the events you want to send to Amazon SNS. Choose **Save selection**.
8. Choose **Edit event**.

Update an Amazon SNS event destination (AWS CLI)

You can use the [update-event-destination](#) command to update an event destination.

The procedure for updating an Amazon SNS event destination is similar to the process for creating an event destination.

To update an Amazon SNS event destination in the AWS CLI

- At the command line, run the following command:

```
$ aws pinpoint-sms-voice-v2 update-event-destination \  
> --event-destination-name eventDestinationName \  
> --configuration-set-name configurationSet \  
> --matching-event types eventTypes \  
> --sns-destination TopicArn=arn:aws:sns:us-east-1:111122223333:snsTopic
```

In the preceding command, make the following changes:

- Replace *eventDestinationName* with a name of the event destination that you want to modify.
- Replace *configurationSet* with the name of the configuration set that you want to associate the event destination with. You can associate the event destination with a different configuration set.
- Replace *eventTypes* with one or more of the event types listed in [Event types for SMS, MMS, and voice](#).
- Replace the value of `TopicArn` with the Amazon Resource Name (ARN) of the Amazon SNS topic that you want to send events to.

Delete an Amazon SNS event destination (Console)

The process for deleting an event destination is the same regardless of the type of event destination that you want to delete.

To delete an Amazon SNS event destination in the Console

- Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
- In the navigation pane, under **Configurations**, choose **Configuration sets**.

3. On the **Configuration sets** page, choose the configuration set to remove an event destination from.
4. In the **All destinations** section choose an event destination and then choose **Delete**.

Delete an Amazon SNS event destination (AWS CLI)

You can use the [delete-event-destination](#) command to delete an event destination.

The process for deleting an event destination is the same regardless of the type of event destination that you want to delete.

To delete an Amazon SNS event destination in the AWS CLI

- At the command line, run the following command:

```
$ aws pinpoint-sms-voice-v2 delete-event-destination \  
> --event-destination-name eventDestinationName \  
> --configuration-set-name configurationSetName
```

In the preceding command, make the following changes:

- Replace *eventDestinationName* with the name or Amazon Resource Name (ARN) of the event destination that you want to delete.
- Replace *configurationSetName* with the name or ARN of the configuration set that the event destination is associated with.

Edit a configuration sets protect configuration association

To change a configuration set's associated protect configuration, you can use the Amazon Pinpoint SMS console, the `AssociateProtectConfiguration` action in the Amazon Pinpoint SMS and voice v2 API, or the `aws sms-voice associate-protect-configuration` command in the AWS CLI. This section shows how to change a configuration set's protect configuration using the Amazon Pinpoint SMS console and the AWS CLI.

To learn more about protect configurations see [Protect configuration](#).

Edit a configuration set's protect configuration association (Console)

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.

2. In the navigation pane, under **Configurations**, choose **Configuration sets**.
3. On the **Configuration sets** page, choose a configuration set.
4. On the **Configuration set details page** choose the **Protect configuration** tab and then **Edit settings**.
5. Under **Protect configuration management** for **Protect configuration**, choose the protect configuration to associate with the configuration set. This replaces the current protect configuration association. Choose **No association** to disassociate the configuration set from a protect configuration.
6. Choose **Save changes**

Edit a configuration set's protect configuration association (AWS CLI)

To change a configuration set's protect configuration association in the AWS CLI follow the direction in [Change a protection configuration association](#) on the Edit a protect configuration association (AWS CLI) tab.

Opt-Out lists

An *opt-out list* is list of destination phone numbers that should not have messages sent to them. When you send SMS messages, destination identities are automatically added to the opt-out list if they reply to your originator phone number with the keyword STOP (unless you enable the self-managed opt-out option). If you attempt to send a message to a destination number that is on an opt-out list, and the opt-out list is associated with the phone number used to send the message, Amazon Pinpoint SMS doesn't attempt to send the message.

Topics


- [Opt-out list keywords](#)
- [Managing opt-out lists](#)
- [Managing opt-out list phone numbers](#)
- [Tags](#)

Opt-out list keywords

Where required by local laws and regulations (such as in the US and Canada), SMS and MMS recipients can use their devices to opt out by replying to the message with any of the following:

- ARRET
- CANCEL
- END
- OPT-OUT
- OPTOUT
- QUIT
- REMOVE
- STOP
- TD
- UNSUBSCRIBE

To opt out, the recipient must reply to the same long code or short code that Amazon Pinpoint SMS used to deliver the message. After opting out, the recipient no longer receives SMS or MMS messages from your AWS account.

 **Note**

For US toll-free numbers, opt-outs are managed at the carrier level. The only supported opt-out keyword for a US toll-free number is STOP. You can't add additional opt-out keywords, or change the response message that your recipients get when they opt-out.

Managing opt-out lists

Use the Amazon Pinpoint SMS console or AWS CLI to manage your opt-out lists.

Create opt-out list (Console)

To create an opt-out list using the Amazon Pinpoint SMS console, follow these steps:

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Opt-out lists**.
3. On the **Opt-out lists** page, choose an opt-out list and then choose **Edit**.
4. On the **List details** page enter a **List name**.

5. Choose **Create list**.

Create opt-out list (AWS CLI)

At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 create-opt-out-list \  
> --opt-out-list-name optOutListName
```

In the preceding example, replace *optOutListName* with a name that makes the opt-out list easy to identify.

Describe opt-out lists (AWS CLI)

You can use the [describe-opt-out-lists](#) command to view information about the opt-out lists in your Amazon Pinpoint SMS account.

To view information about all of your opt-out lists using the AWS CLI

- At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 describe-opt-out-lists
```

You can also view information about specific opt-out lists by using the `OptOutListNames` parameter.

To view information about specific opt-out lists using the AWS CLI

- At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 describe-opt-out-lists \  
> --opt-out-list-names optOutListName
```

In the preceding command, replace *optOutListName* with the name or Amazon Resource Name (ARN) of the opt-out list that you want to find more information about. You can also specify multiple opt-out lists by separating each list name with a space.

The AWS CLI returns the following information about all of the opt-out lists in your account.

Delete opt-out list (Console)

To delete an opt-out list using the Amazon Pinpoint SMS console, follow these steps:

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Opt-out lists**.
3. On the **Opt-out lists** page, choose an opt-out list, choose **Delete**.

Delete opt-out list (AWS CLI)

You can use the [delete-opt-out-list](#) command to delete an opt-out list

At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 delete-opt-out-list \  
> --opt-out-list-name optOutListName
```

In the preceding example, replace *optOutListName* with a name that makes the opt-out list easy to identify.

View linked originators (Console)

You can view all of the origination identities that are linked to the opt-out list using the Amazon Pinpoint SMS console, follow these steps:

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Opt-out lists**.
3. On the **Opt-out lists** page, choose an opt-out list.
4. Choose **Linked origination numbers** to view all origination identities.

Managing opt-out list phone numbers

Use the Amazon Pinpoint SMS console or AWS CLI to add or remove destination phone numbers from your opt-out list or to view the origination identities associated with the opt-out list.

Add a destination number (Console)

When you add a phone number to an opt-out list that phone number will no longer receive messages sent from an origination identity that is linked to the opt-out list.

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Opt-out lists**.
3. On the **Opt-out lists** page, choose an opt-out list.
4. On the **Opted-out numbers** tab, choose **Add number**.
5. On the **Add opt-out number** page, for **Destination number** enter in the phone number to add to the opt-out list. The phone number must be in E.164 format, for example +12065550150.
6. Choose **Add number**

Search for an opted-out destination number (Console)

You can search an opt-out list to see if the opt-out list contains a destination number.

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Opt-out lists**.
3. On the **Opt-out lists** page, choose an opt-out list.
4. On the **Opted-out numbers** tab enter a phone number into the search field. The phone number must be in E.164 format for example **+12065550149**.
5. Choose **Search**.

View originators (Console)

Multiple origination identities can use the same opt-out list. You can view a list of origination identities associated with an opt-out list in the **Linked origination numbers** tab.

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Opt-out lists**.
3. On the **Opt-out lists** page, choose an opt-out list.
4. On the **Linked origination numbers** tab you can view all origination identities associated with the opt-out list.

Add a destination number (AWS CLI)

When you add a phone number to an opt-out list that phone number will no longer receive messages sent from an origination identity that is linked to the opt-out list.

You can use the [put-opted-out-number](#) command add a phone number to an opt-out list.

At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 put-opted-out-number \  
> --opt-out-list-name optOutListName \  
> --opted-out-number +12065550123
```

In the preceding example, make the following changes:

- Replace *optOutListName* with the name or Amazon Resource Name (ARN) of the opt-out list that you want to add the destination identity to.
- Replace *+12065550123* with phone number that you want to add to the opt-out list. The phone number must be formatted in E.164 format.

Remove a destination number (Console)

When you remove a phone number to an opt-out list that phone number will receive messages sent from an origination identity that is linked to the opt-out list.

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Opt-out lists**.
3. On the **Opt-out lists** page, choose an opt-out list.
4. On the **Opted-out numbers** tab enter the phone number to remove and then **Search**.
5. If the phone number is found use it can be removed from the opt-out list by using **Remove number**.
6. In the **Remove opted-out number** window enter **release** and then **Remove number**.

Remove a destination number (AWS CLI)

When you remove a phone number to an opt-out list that phone number will receive messages sent from an origination identity that is linked to the opt-out list.

You can use the [delete-opted-out-number](#) command remove a phone number to an opt-out list.

At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 delete-opted-out-number \  
> --opt-out-list-name optOutListName \  
> --opted-out-number +12065550123
```

```
> --opt-out-list-name optOutListName \  
> --opted-out-number +12065550123
```

In the preceding example, make the following changes:

- Replace *optOutListName* with the name or Amazon Resource Name (ARN) of the opt-out list that you want to add the destination identity to.
- Replace *+12065550123* with phone number that you want to add to the opt-out list. The phone number must be formatted in E.164 format.

Tags

Tags are pairs of keys and values that you can optionally apply to your AWS resources to control access or usage.

Manage tags (Console)

Use the Amazon Pinpoint SMS console to add or edit a Tag in your pool.

Manage tags (Console)

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Configurations**, choose **Opt-out list**.
3. On the **Opt-out lists** page, choose the opt-out list to add a tag to.
4. On the **Tags** tab, choose **Manage tags**.
 - **Add a tag** – In **Manage tags**, choose **Add new tag** to create a new blank key/value pair.
 - **Delete a tag** – In **Manage tags**, choose **Remove** next to the key/value pair.
 - **Edit a tag** – In **Manage tags**, choose the **Key** or **Value** and edit the text.
5. Choose **Save changes**.

Manage tags (AWS CLI)

Use the AWS CLI to add or edit a Tag.

```
$ aws pinpoint-sms-voice-v2 tag-resource \  
--resource-arn resource-arn \  
--tags tags={key1=value1,key2=value2}
```

In the preceding example, do the following:

- Replace *resource-arn* with the Amazon Resource Name (ARN) that you want to add the tags to.
- Replace *key1* and *key2* with the keys of the tags that you want to add to the resource.
- Replace *value1* and *value2* with the values of the tags that you want to add for the respective keys.

Use the AWS CLI to delete a Tag.

```
$ aws pinpoint-sms-voice-v2 untag-resource \  
  --resource-arn resource-arn \  
  --tag-keys tags={key1=value1,key2=value2}
```

In the preceding example, do the following:

- Replace *resource-arn* with the Amazon Resource Name (ARN) that you want to remove the tag from.
- Replace *key1* and *key2* with the keys of the tags that you want to remove.
- Replace *value1* and *value2* with the values of the tags that you want to remove.

Example sending SMS or voice messages

You can use the Amazon Pinpoint SMS API to send messages directly from your apps. Transactional messages are messages that you send to specific recipients.

This section includes code examples for sending both [SMS messages](#) and [voice messages](#).

Topics in this section:

- [Sending SMS Messages](#)
- [Sending Voice Messages](#)

Sending SMS Messages

You can use the following code example to send an SMS message using the AWS SDK for Python (Boto3).


```
import boto3
from botocore.exceptions import ClientError

def send_sms_message(sms_voice_v2_client, configuration_set, context_keys,
                    country_parameters, destination_number, dry_run, keyword,
                    max_price, message_body, message_type, origination_number,
                    ttl):
    try:
        response = sms_voice_v2_client.send_text_message(
            ConfigurationSetName=configuration_set,
            Context=context_keys,
            DestinationCountryParameters=country_parameters,
            DestinationPhoneNumber=destination_number,
            DryRun=dry_run,
            Keyword=keyword,
            MaxPrice=max_price,
            MessageBody=message_body,
            MessageType=message_type,
            OriginationIdentity=origination_number,
            TimeToLive=ttl
        )

    except ClientError as e:
        print(e.response)
    else:
        return response['MessageId']

def main():
    configuration_set = "MyConfigurationSet"
    context_keys = {"key1": "value1"}
    country_parameters = {
        "IN_TEMPLATE_ID": "TEMPLATE01234",
        "IN_ENTITY_ID": "ENTITY98765"
    }
    destination_number = "+14255550168"
    dry_run = False
    keyword = "MyKeyword"
    max_price = "2.00"
    message_body = ("This is a test message sent from Amazon Pinpoint SMS "
                   "using the AWS SDK for Python (Boto3). ")
    message_type = "TRANSACTIONAL"
```

```
origination_number = "+12065550183"
ttl = 120

print(
    f"Sending text message to {destination_number}.")

message_id = send_sms_message(
    boto3.client('pinpoint-sms-voice-v2'), configuration_set, context_keys,
    country_parameters, destination_number, dry_run, keyword, max_price,
    message_body, message_type, origination_number, ttl)

print(f"Message sent!\nMessage ID: {message_id}")

if __name__ == '__main__':
    main()
```

In the preceding code example, make the following changes in the `main()` function:

- Change the value of `configuration_set` to the name or Amazon Resource Name (ARN) of the configuration set that you want to use to send this message.
- Change the value of `context_keys` to the keys and values that you want to use when sending this message. These keys appear in the event records associated with this message.
- If you use a registered sender ID to send messages to customers in India, change the value of `country_parameters` to match the registered Entity ID and Template ID that you received when you registered your sender ID.

Important

If you don't use a registered sender ID to send messages to customers in India, omit this parameter completely. If you do, you must also remove the corresponding line in the `send_sms_message` function.

- Change the value of `destination_number` to the phone number that you want to send the message to.
- If you want to execute this operation without sending any messages, change the value of `dry_run` to `True`.

- Change the value of `max_price` to the maximum amount of money that you want to spend, in US Dollars, to send each message part this message. A message part contains up to 140 bytes of information. For more information, see [SMS character limits](#).
- Change the value of `message_body` to include the message that you want to send. The maximum length of a message depends on which characters the message contains. For more information about SMS character encoding, see [SMS character limits](#).
- Change the value of `message_type` to represent the appropriate message category. Valid values are TRANSACTIONAL (for messages that are critical or time-sensitive) and PROMOTIONAL (for messages that aren't critical or time-sensitive).
- Change the value of `origination_number` to the phone number that you want to use to send the message. The phone number must be in E.164 format.
- Change the value of `ttl` to the amount of time, in seconds, that Amazon Pinpoint SMS should attempt to deliver the message. You can set the TTL value up to 259200 seconds (72 hours).

Sending Voice Messages

You can use the following code example to send a voice message using the AWS SDK for Python (Boto3).

```
import boto3
from botocore.exceptions import ClientError

def send_voice_message(sms_voice_v2_client, configuration_set, context_keys,
                      destination_number, dry_run, max_price, message_body,
                      message_type, origination_number, ttl, voice_id):
    try:
        response = sms_voice_v2_client.send_voice_message(
            ConfigurationSetName=configuration_set,
            Context=context_keys,
            DestinationPhoneNumber=destination_number,
            DryRun=dry_run,
            MaxPricePerMinute=max_price,
            MessageBody=message_body,
            MessageBodyTextType=message_type,
            OriginationIdentity=origination_number,
            TimeToLive=ttl,
            VoiceId=voice_id
        )
```

```
except ClientError as e:
    print(e.response)
else:
    return response['MessageId']

def main():
    configuration_set = "MyConfigurationSet"
    context_keys = {"key1": "value1"}
    destination_number = "+12065550123"
    dry_run = False
    max_price = "2.00"
    message_body = (
        "<speak>"
        "This is a test message sent from <emphasis>Amazon Pinpoint SMS</emphasis>"
        "using the <break strength='weak' /> AWS SDK for Python (Boto3). "
        "<amazon:effect phonation='soft'>Thank you for listening."
        "</amazon:effect>"
        "</speak>")
    message_type = "SSML"
    origination_number = "+18445550142"
    ttl = 120
    voice_id = "MATTHEW"

    print(
        f"Sending voice message with Amazon Pinpoint SMS from {origination_number} to
        {destination_number}.")

    message_id = send_voice_message(
        boto3.client('pinpoint-sms-voice-v2'), configuration_set, context_keys,
        destination_number, dry_run, max_price, message_body, message_type,
        origination_number, ttl, voice_id)

    print(f"Message sent!\nMessage ID: {message_id}")

if __name__ == '__main__':
    main()
```

In the preceding code example, make the following changes in the `main()` function:

- Change the value of `configuration_set` to the name or Amazon Resource Name (ARN) of the configuration set that you want to use to send this message.
- Change the value of `context_keys` to the keys and values that you want to use when sending this message. These keys appear in the event records associated with this message.
- Change the value of `destination_number` to the phone number that you want to send the message to.
- Change the value of `max_price` to the maximum amount of money that you want to spend per minute sending this message.
- Change the value of `message_body` to include the message that you want to send. Your message can contain up to 6,000 characters.
- If you want to use a plain text script rather than an SSML-formatted one, change the value of `message_type` to `TEXT`.
- Change the value of `origination_number` to the phone number that you want to use to send the message. The phone number must be in E.164 format.
- If you want to execute this operation without sending any messages, change the value of `dry_run` to `True`.
- Change the value of `ttl` to the amount of time, in seconds, that Amazon Pinpoint SMS should attempt to deliver the message. You can set the TTL value up to 259200 seconds (72 hours).
- Replace `MATTHEW` with the name of the Amazon Polly voice that you want to use to send the message. For a complete list of supported voices, see [SendVoiceMessage](#) in the *SMS and Voice, version 2 API Reference*. If you don't specify a voice, your message is sent using the "MATTHEW" voice.

Sending an MMS message

You can use the AWS CLI or Amazon Pinpoint SMS and voice v2 API to send MMS messages to your customers.

Use the [send-media-message](#) AWS CLI command to send an MMS message. For more information on configuring the AWS CLI, see [Configure the AWS CLI](#) in the [AWS Command Line Interface User Guide](#).

⚠ Important

MMS capabilities are only available in some countries. For more information on supported countries for SMS and MMS, see [Supported countries and regions for SMS messaging](#) and [Supported countries and regions for MMS messaging](#).

To check if your origination identity is MMS capable, see [Phone number status and capabilities](#).

Before sending an MMS message you need to upload your media files to an Amazon S3 bucket that is in the same AWS Region as your MMS capable origination identity, see [Setting up a bucket in S3 for MMS files](#).

The identity used to call `send-media-message` must have read access to the Amazon S3 bucket that contains your media files. For more information on setting read access, see [Identity-based policy examples for Amazon S3](#) in the [Amazon S3 User Guide](#).

To send an MMS message

- At the command line, enter the following command:

```
aws pinpoint-sms-voice-v2 --region 'us-east-1' send-media-message --destination-  
phone-number +12065550150 --origination-identity +14255550120 --message-body 'text  
body' --media-urls 's3://s3-bucket/media_file.jpg'
```

In the preceding command, make the following changes:

- Replace `us-east-1` with the AWS Region that your origination identity is stored in.
- Replace `+12065550150` with the destination phone number.
- Replace `+14255550120` with your origination identity. The origination identity must be ACTIVE and able to send the destination phone number.
- Replace `text body` with your text message.
- Replace `s3://s3-bucket/media_file.jpg` with the S3 URI of the media file. Supported media file formats are listed in [MMS file types, size and character limits](#). For more information about creating an S3 bucket and managing objects, see [Setting up a bucket in S3 for MMS files](#) or [Creating a bucket](#) and [Uploading objects](#) in the [Amazon S3 User Guide](#).

If Amazon Pinpoint SMS accepts the command you will receive the MessageID. This only means the command was successfully received and not that the destination device has received the message yet. For a list of error codes, see [SendMediaMessage Errors](#).

```
{
  "MessageId": "string"
}
```

Setting up a bucket in S3 for MMS files

Your MMS files must be stored in an Amazon S3 bucket. The Amazon S3 bucket must be in the same AWS account and AWS Region as your MMS capable origination identity. These directions show how to create an Amazon S3 bucket, upload a file, and build the URI to the file. For more information on Amazon S3 commands, see [Use high-level \(s3\) commands with the AWS CLI](#). For more information on configuring the AWS CLI, see [Configure the AWS CLI](#) in the [AWS Command Line Interface User Guide](#).

To create an Amazon S3 bucket use the [create-bucket](#) AWS CLI command. At the command line, enter the following command:

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

In the preceding command:

- Replace *us-east-1* with the AWS Region your MMS capable origination identity is in.
- Replace *BucketName* with the name of the new bucket.

To copy a file to the Amazon S3 bucket use the [cp](#) AWS CLI command. At the command line, enter the following command:

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

In the preceding command:

- Replace *SourceFilePathAndName* with the file path and name of the file to copy.
- Replace *BucketName* with the name of the bucket.
- Replace *FileName* with the name to use for the file.

The URI to use when sending is:

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

Understanding SMS billing and usage reports

The AWS Amazon Pinpoint SMS channel generates a usage type that contains five fields in the following format: *Region code*-*MessagingType*-*ISO*-*RouteType*-*OriginationID*-*MessageCount*/*Fee*. For example, SMS messages sent from the Asia Pacific (Tokyo) Region to a Japanese phone number would appear as **APN1-OutboundSMS-JP-Standard-Senderid-MessageCount**.

The following table displays the possible values and descriptions for the fields in the usage type. For more information about SMS pricing, see [Amazon Pinpoint SMS Pricing](#).

Field	Options	Description
<i>Region code</i>	<ul style="list-style-type: none"> APN1 – Asia Pacific (Tokyo) Region APN2 – Asia Pacific (Seoul) Region APS1 – Asia Pacific (Singapore) Region APS2 – Asia Pacific (Sydney) Region APS3 – Asia Pacific (Mumbai) Region CAN1 – Canada (Central) Region EUC1 – Europe (Frankfurt) Region EU – Europe (Ireland) Region EUW2 – Europe (London) Region 	The AWS Region prefix that indicates where the SMS message was sent from.

Field	Options	Description
	<ul style="list-style-type: none"> • UGW1 – AWS GovCloud (US-West) • USE1 (or no prefix) – US East (N. Virginia) Region • USE2 – US East (Ohio) Region • USW2 – US West (Oregon) Region 	
<i>MessagingType</i>	OutboundSMS	This field lists the message type being sent. For Outbound SMS, it reads OutboundSMS .
<i>ISO</i>	See Supported countries and regions for SMS messaging for the list of ISO country codes supported by Amazon Pinpoint SMS.	The two-digit ISO country code that the message was sent to.
<i>RouteType</i>	Standard	The route type that the message was sent through. Currently, all messages are sent through the Standard route type.
<i>OriginationID</i>	TollFree, 10DLC, Shortcode, Longcode, Senderid, Sharedroute	This field specifies the origination identity that was used to send the message. See Choosing a phone number or sender ID for more information about supported origination identities.

Field	Options	Description
<i>MessageCount/Fee</i>	MessageCount, MessageFees, CarrierFeeCount, CarrierFees	<p>This field displays either the number of messages sent or the cost associated with sending those messages.</p> <ul style="list-style-type: none"> • MessageCount – The number of messages sent using Amazon Pinpoint SMS • CarrierFeeCount – The number of messages sent using Amazon Pinpoint SMS that had carrier fee • MessageFees – The cost of sending messages sent using Amazon Pinpoint SMS • CarrierFees – The cost of carrier fees to send messages using Amazon Pinpoint SMS

Messages sent through Amazon Pinpoint SMS for Outbound SMS generate 2 – 4 usage types per combination of ISO country and origination identity. View the following examples to better understand how the usage types appear on your bill.

Example 1: Sending messages to the United Kingdom

Suppose you sent 10 messages to the United Kingdom (ISO code GB) using a short code from USE1. Then you can expect the following two usage types in your bill:

1. USE1-OutboundSMS-GB-Standard-Shortcode-MessageCount
2. USE1-OutboundSMS-GB-Standard-Shortcode-MessageFee

Example 2: Sending messages to the United States

Suppose you sent 10 messages to the United States (ISO code US) using a 10DLC number from CAN1. Then you can expect the following four usage types in your bill:

1. CAN1-OutboundSMS-US-Standard-10DLC-MessageCount
2. CAN1-OutboundSMS-US-Standard-10DLC-MessageFee
3. CAN1-OutboundSMS-US-Standard-10DLC-CarrierFeeCount
4. CAN1-OutboundSMS-US-Standard-10DLC-CarrierFees

Requesting support for SMS, MMS, and voice messaging

Certain SMS options in Amazon Pinpoint SMS can only be configured by creating a case in the [AWS Support Center](#). Open a case to request any of the following:

- **An increase to your monthly SMS, MMS, or Voice spending threshold**

By default, the monthly spending threshold is \$1.00 (USD). Your spending threshold determines the volume of messages that you can send with Amazon Pinpoint SMS. Request a spending threshold that meets the expected monthly message volume for your SMS, MMS, or voice use case. To change your spending threshold, see [Change your spending threshold](#).

- **Moving from the sandbox to production**

New Amazon Pinpoint SMS accounts are placed into an SMS or voice sandbox. The sandbox protects both AWS customers and recipients from fraud and abuse. The sandbox also creates a safe environment for test, development, and QA accounts. To move your account out of the sandbox and into production, see [SMS/MMS sandbox](#) and [Voice sandbox](#).

When you create your case in the AWS Support Center, include all the information that's required for the type of request you're submitting. If you don't, AWS Support will contact you to obtain this information before proceeding. By submitting a detailed case, you help to make sure that your request is fulfilled quickly. For the details that are required for specific types of SMS requests, see the topics in this section.

Topics

- [Requesting increases to your monthly SMS, MMS, or Voice spending quota](#)

Requesting increases to your monthly SMS, MMS, or Voice spending quota

Your spending quota determines how much money you can spend sending SMS, MMS, or voice messages through Amazon Pinpoint SMS each month. When Amazon Pinpoint SMS determines that sending an SMS, MMS, or voice message would incur a cost that exceeds your spending quota for the current month, it stops publishing SMS, MMS, or voice messages within minutes.

Important

Because Amazon Pinpoint SMS is a distributed system, it stops sending SMS, MMS, or voice messages within minutes of the spending quota being exceeded. During this period, if you continue to send SMS, MMS, or voice messages, you might incur costs that exceed your quota.

We set the maximum spending quota for all accounts in the Sandbox at \$1.00 (USD) per month. This quota is intended to let you test the message-sending capabilities of Amazon Pinpoint SMS. This quota also reduces the risk of sending large amounts of messages before you're ready to use Amazon Pinpoint SMS for your production workloads and is necessary to prevent malicious users from abusing Amazon Pinpoint SMS.

You can request an increase to the SMS, MMS, or voice spending quota for your account by opening a quota increase case in the AWS Support Center. Spending limits vary by region. Because of this you must specify the AWS Regions where you require an increase.

Change your spending threshold

You can request an increase to your maximum monthly spending quota by opening a quota increase case in the AWS Support Center. Changing your SMS spending threshold also applies to your MMS spending threshold.

Note

Some of the fields on the request form are marked as "optional." However, AWS Support requires all of the information that's mentioned in the following steps in order to process your request. If you don't provide all of the required information, you might experience delays in processing your request.

To request a spending quota increase

1. Open the Support Center Console at <https://console.aws.amazon.com/support/home>.
2. In the left hand navigation choose **Your support cases**.
3. Choose **Create case**.
4. Choose the **Looking for service quota increases?** link.
5. In the **Looking for service quota increases?** window choose **Create a case instead**.
6.
 - For **Service**, choose **Pinpoint SMS**.
 - (Optional) For **Provide a link to the site or app which will be sending SMS messages**, provide information about the website, application, or service that will send SMS messages.
 - (Optional) For **What type of messages do you plan to send**, choose the type of message that you plan to send:
 - **One Time Password** – Messages that provide passwords that your customers use to authenticate with your website or application.
 - **Promotional** – Noncritical messages that promote your business or service, such as special offers or announcements.
 - **Transactional** – Important informational messages that support customer transactions, such as order confirmations or account alerts. Transactional messages must not contain promotional or marketing content.
 - (Optional) For **Which AWS Region will you be sending messages from**, choose the region that you will be sending messages from.
 - (Optional) For **Which countries do you plan to send messages to**, enter the country or region that you want to increase your spending limit in.
 - (Optional) For **How do your customers opt to receive messages from you**, provide details about your opt-in process.
 - (Optional) For **Please provide the message template that you plan to use to send messages to your customers** field, include the template that you will be using.
7. Under **Requests**, complete the following sections:
 - For the **Region**, choose the Region from which you will be sending messages.

Note

The Region is required in the **Requests** section. Even if you provided this information in the **Case details** section you must also include it here.

- For **Resource Type**, choose **General Limits**.
 - For **Quota**, choose **Account Spend Threshold Increase**.
8. For **New quota value**, enter the maximum amount (in USD) that you can spend on SMS each calendar month.
 9. Under **Case description**, for **Use case description**, provide the following details:
 - The website or app of the company or service that's sending SMS messages.
 - The service that's provided by your website or app, and how your SMS messages contribute to that service.
 - How users opt in to receive your SMS messages on your website, app, or other location.

If your requested spending quota (the value you specified for **New quota value**) exceeds \$10,000 (USD), provide the following additional details for each country that you're messaging:

- Whether you're using a sender ID, short code, or both. If you're using a sender ID, provide:
 - The sender ID.
 - Whether the sender ID is registered with wireless carriers in the country.
 - The maximum expected transactions-per-second (TPS) for your messaging.
 - The average message size.
 - The template for the messages that you send to the country.
 - (Optional) Character encoding needs, if any.
10. (Optional) If you want to submit any further requests, choose **Add another request**. If you include multiple requests, provide the required information for each. For the required information, see the other sections within [Requesting support for SMS, MMS, and voice messaging](#).
 11. Under **Contact options**, for **Preferred contact language**, choose whether you want to receive communications for this case in **English** or **Japanese**.

12. When you finish, choose **Submit**.

The AWS Support team provides an initial response to your request within 24 hours.

In order to prevent our systems from being used to send unsolicited or malicious content, we have to consider each request carefully. If we're able to do so, we'll grant your request within this 24-hour period. However, if we need to obtain additional information from you, it might take longer to resolve your request.

We might not be able to grant your request if your use case doesn't align with our policies.

Protect

Protect is a set of capabilities that allow you to only send messages to countries where your customers are.

Use Amazon Pinpoint SMS protect configurations to build a list of country rules that allow or block messages to each destination country. Each country rules list can be applied to SMS, MMS, and voice messages sent from your AWS account.

Topics

- [Protect configuration](#)

Protect configuration

Use protect configurations to control which destination countries Amazon Pinpoint SMS can send your messages to. By controlling which countries you allow messages to be sent to, you can avoid sending to countries with high message prices or countries you don't operate in. Each protect configuration contains individual allow and block country rules for SMS, MMS, and voice.

You can use a protect configurations as the *account default*, with a configuration set, or in the *ProtectConfigurationId* parameter of the `SendMediaMessage`, `SendTextMessage`, or `SendVoiceMessage` commands. When set as an *account default*, a protect configuration will also affect messages sent through Amazon SNS, Amazon Cognito and `SendMessage`s.

The selection process for the *effective* protection configuration for a sending request is as follows:

1. *ProtectConfigurationId* – If a protection configuration is specified in the API request parameters, it will be used.
2. *ConfigurationSetName* – If no protection configuration is specified in the API request parameters, but a configuration set is specified and it has an associated protection configuration, then the protection configuration associated with this configuration set will be used.
3. *Account default* – If a protection configuration is not specified or available from 1 or 2, the *account default* protection configuration will be used.
4. *None* – If no *account default* is configured, then no protection configuration will be applied.

A protect configuration can be associated to multiple configuration sets, while a configuration set can only be associated with one protect configuration. There can only be one *account default* protect configuration at any time.

The following example for `SendMediaMessage` has both a configuration set and protect configuration specified in the command. The protect configuration specified in the `ProtectConfigurationId` parameter is used regardless of whether the configuration set has an associated protect configuration or if there is an *account default* protect configuration.

```
aws pinpoint-sms-voice-v2 --region 'us-east-1' send-media-message --destination-phone-number +12065550150 --origination-identity +14255550120 --message-body 'text body' --media-urls 's3://s3-bucket/media_file.jpg' --configuration-set-name ConfigSetName --protect-configuration-id ProtectConfigId
```

Depending on your use case we recommend the following:

- If you only need one set of country rules for all SMS, MMS, and voice you should create a protect configuration and associate it as your account *account default*.
 1. Create a protect configuration by following the directions in [Create a protect configuration](#) and set the association as *account default*.
 2. Edit the Allow and Blocked country rules for SMS, MMS, and voice by following the directions in [Change protect configuration country rules](#).
 3. Your *account default* protect configuration is now used for any message you send unless overridden by using the `ConfigurationSetName` or `ProtectConfigurationId`.
- If your use case requires more granular controls and event logging you can associate the protect configuration with a configuration set.
 1. If you don't already have a configuration set created then follow the directions at [Managing configuration set](#) and we also recommend you setup an event destination to log SMS, MMS, and voice events.
 2. Create a protect configuration by following the directions in [Create a protect configuration](#) and set the association as *configuration set* and choose one or more configuration sets.
 3. Edit the Allow and Blocked country rules for SMS, MMS, and voice by following the directions in [Change protect configuration country rules](#).
 4. To use the protect configuration you need to pass the `ConfigurationSetName` in the of the `SendMediaMessage`, `SendTextMessage`, or `SendVoiceMessage` commands.

- If your use case requires more granular controls you can create the protect configuration and use the protect configuration in the *ProtectConfigurationId* API parameter.
 1. Create a protect configuration by following the directions in [Create a protect configuration](#) and set the association as *No association*.
 2. Edit the Allow and Blocked country rules for SMS, MMS, and voice by following the directions in [Change protect configuration country rules](#).
 3. To use the protect configuration you need to pass the *ProtectConfigurationId* in the of the *SendMessage*, *SendTextMessage*, or *SendVoiceMessage* commands.

Topics

- [Create a protect configuration](#)
- [Change protect configuration country rules](#)
- [Change a protection configuration association](#)
- [Delete a protect configuration](#)
- [Manage deletion protection](#)
- [Change a protect configuration's name](#)
- [Tags](#)

Create a protect configuration

To create a new protect configuration, you can use the Amazon Pinpoint SMS console, the *CreateProtectConfiguration* action in the Amazon Pinpoint SMS and voice v2 API, or the `aws sms-voice create-protect-configuration` command in the AWS CLI. This section shows how to create protect configurations using the Amazon Pinpoint SMS console and the AWS CLI.

By default you can have up to 25 protect configurations in your AWS account.

When a protect configuration is created all country rules for SMS, MMS, and voice, are set to ALLOW. We recommend you edit the country rules before using the protect configuration. To learn more about editing the country rules, see [Change protect configuration country rules](#).

Note

The name of your protect configuration is saved as a tag key/value pair. If you don't specify a "Name" tag then the name for the protect configuration will appear as –.

Create a protect configuration (Console)

To create a protect configuration using the Amazon Pinpoint SMS console, follow these steps:

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Protect**, choose **Protect configuration** and then **Create configuration**.
3. For **Protect configuration name** enter a descriptive name for the protect configuration.
4. By default you can send messages to all countries. For **SMS country rules**, choose the countries to block sending messages to and then choose **Block**. You can sort and filter the country list based on **Country**, **Region** and **Rule**.
5. In **Protect configuration associations** for **Association type**, choose:
 - **Account default** – To use the protect configuration as your account default. If you already have an **Account default** protect configuration then it is replaced.
 - **Configuration set** – To associate the protect configuration with an existing configuration set. For **Configuration sets available for association**, choose one or more configuration sets to associate the protect configuration to. This replaces the existing protect configuration association.
 - **No association** – The protect configuration is not associated to your account default or a configuration set.
6. Choose **Create configuration**.

Now you have created your protect configuration you should edit the country rules list for MMS and voice. To learn more about editing the country rules, see [Change protect configuration country rules](#).

Create a protect configuration (AWS CLI)

You can use the create-protect-configuration command to create a new protect configuration.

To create a protect configuration

- At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 create-protect-configuration --tags  
Key=Name,Value=ProtectConfigName
```

In the preceding command, make the following changes:

- Replace *ProtectConfigName* with a friendly name for your protect configuration.

Now you have created your protect configuration you need to edit the country rules list for SMS, MMS, and voice. . To learn more about editing the country rules, see [Change protect configuration country rules](#). Optionally you can associate the protect configuration with the *account default* protect configuration or a configuration set.

Change protect configuration country rules

Protect configuration country rules either allow or block messages for each destination country. To update protect configuration country rules, you can use the Amazon Pinpoint SMS console or the `aws sms-voice update-protect-configuration-country-rule-set` command in the AWS CLI. This section shows how to update the protect configuration country rules using the Amazon Pinpoint SMS console and the AWS CLI.

Note

You can only change your MMS country rules list through the Amazon Pinpoint SMS and voice v2 API or AWS CLI.

Edit a protect configuration (Console)

To edit a protect configuration using the Amazon Pinpoint SMS console, follow these steps:

- Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
- In the navigation pane, under **Protect**, choose **Protect configuration**.
- On the **Protect configuration** page, choose a protect configuration and then choose **Edit**.
- In the protect configuration details table choose the **SMS rules** or **Voice rules** tab.

5. In the **SMS/Voice country rules** tab check the countries to change the rules for and then choose **Block** or **Allow**. You can sort and filter the country list based on **Country**, **Region** and **Rule**.
6. In the **Status change confirmation** window review your changes and then choose **Confirm** to apply them.

The new country rule set is now used for the protect configuration.

Edit a protect configuration (AWS CLI)

You can use the `update-protect-configuration-country-set` command to change a protect configuration's country rules. You can change up to 300 country rules at a time.

To edit a protect configuration

- To edit two country rules at the command line, enter the following command:

```
aws pinpoint-sms-voice-v2 update-protect-configuration-country-rule-set
--protect-configuration-id ProtectConfigId --number-capability Capability
--country-rule-set-updates '{"CountryISO1":{"ProtectStatus": "Rule1"},
"CountryISO2": {"ProtectStatus": "Rule2"}}'
```

In the preceding command, make the following changes:

- Replace *ProtectConfigId* with the unique identifier of the protect configuration.
- Replace *Capability* with SMS, MMS, or VOICE.
- Replace *CountryISO1* with the two letter ISO country code. For a list of ISO country codes, see [Supported countries and regions for SMS messaging](#).
- Replace *Rule1* with ALLOW or BLOCK.
- Replace *CountryISO2* with the two letter ISO country code. For a list of ISO country codes, see [Supported countries and regions for SMS messaging](#).
- Replace *Rule2* with ALLOW or BLOCK.

Change a protection configuration association

To use the country rules contained in a protect configuration, you need to associate the protect configuration as the *account default*, a configuration set, or use it directly with a

message send. If you only have one message sending use case, using an *account default* is the simplest option. If you have several use cases, you can use configuration sets to control which countries Amazon Pinpoint SMS sends to, and for the most control, you can associate a protect configuration directly in a message send. To change a protect configuration's association, you can use the Amazon Pinpoint SMS console, the `AssociateProtectConfiguration` or `SetAccountDefaultProtectConfiguration` action in the Amazon Pinpoint SMS and voice v2 API, or the `aws sms-voice associate-protect-configuration` or `aws sms-voice set-account-default-protect-configuration` commands in the AWS CLI. This section shows how to change a protect configuration's association using the Amazon Pinpoint SMS console and the AWS CLI.

The selection process for the *effective* protection configuration for a sending request is as follows:

1. *ProtectConfigurationId* – If a protection configuration is specified in the API request parameters, it will be used.
2. *ConfigurationSetName* – If no protection configuration is specified in the API request parameters, but a configuration set is specified and it has an associated protection configuration, then the protection configuration associated with this configuration set will be used.
3. *Account default* – If a protection configuration is not specified or available from 1 or 2, the *account default* protection configuration will be used.
4. *None* – If no *account default* is configured, then no protection configuration will be applied.

A protect configuration can be associated to multiple configuration sets, while a configuration set can only be associated with one protect configuration. There can only be one *account default* protect configuration.

Edit a protect configuration association (Console)

To edit a protect configuration using the Amazon Pinpoint SMS console, follow these steps:

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Protect**, choose **Protect configuration**.
3. On the **Protect configurations** page, choose a protect configuration.
4. Choose the **Associations** tab.
5. Choose **Edit settings**.
6. On the **Edit setting** page, choose one of the following options:

- **Account default** – Use the protect configuration as your *account default* protect configuration. This replaces the current *account default* protect configuration.
- **Configuration set** – Associate the protect configuration with one or more configuration sets.
 - In **Configuration sets available for association** check one or more configuration sets that do not already have a protect configuration association.
- **No association** – The protect configuration is not associated with the *account default* or a configuration set.

7. Choose **Save changes**.

Edit a protect configuration association (AWS CLI)

You can use the `associate-protect-configuration` command to associate the protect configuration with a configuration set. To change the *account default* protect configuration use the `set-account-default-protect-configuration` command.

To change a configuration sets association to a protect configuration at the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 associate-protect-configuration --configuration-set-name ConfigurationSetName --protect-configuration-id ProtectConfigurationID
```

In the preceding command, make the following changes:

- Replace *ConfigurationSetName* with the name of the configuration set.
- Replace *ProtectConfigurationID* with the unique identifier of the protect configuration.

To change the account default protect configuration at the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 set-account-default-protect-configuration --protect-configuration-id ProtectConfigurationID
```

In the preceding command, make the following changes:

- Replace *ProtectConfigurationID* with the unique identifier of the protect configuration.

Disassociate a protect configuration (AWS CLI)

You can use the `disassociate-protect-configuration` command to disassociate the protect configuration with a configuration set. To remove the *account default* protect configuration use the `delete-account-default-protect-configuration` command.

To remove a configuration sets association to a protect configuration at the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 disassociate-protect-configuration --configuration-set-name ConfigurationSetName --protect-configuration-id ProtectConfigurationID
```

In the preceding command, make the following changes:

- Replace *ConfigurationSetName* with the name of the configuration set.
- Replace *ProtectConfigurationID* with the unique identifier of the protect configuration.

To remove the *account default* protect configuration at the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 delete-account-default-protect-configuration
```

Delete a protect configuration

To delete a protect configuration, you can use the Amazon Pinpoint SMS console, the `DeleteProtectConfiguration` action in the Amazon Pinpoint SMS and voice v2 API, or the `aws sms-voice delete-protect-configuration` command in the AWS CLI. This section shows how to delete a protect configuration using the Amazon Pinpoint SMS console and the AWS CLI.

Important

Deletion protection has to be disabled before you can delete a protect configuration. The protect configuration has to be disassociated from any configuration sets or the *account default* protect configuration before you can delete it.

Delete a protect configuration (Console)

To delete a protect configuration using the Amazon Pinpoint SMS console, follow these steps:

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Protect**, choose **Protect configuration**.
3. Choose the protect configuration to delete and then choose **Delete**.
4. On the **Delete protect configurations** enter **confirm** and choose **Delete**.

Note

If your protect configuration is still associated with a configuration set or as the account default choose **Remove associations**, then enter **confirm**, and choose **Delete**.

The protect configuration has now been removed from your account.

Delete a protect configuration (AWS CLI)

You can use the `delete-protect-configuration` command to delete a protect configuration.

To delete a protect configuration

- At the command line, enter the following command:

```
$ aws pinpoint-sms-voice-v2 delete-protect-configuration --protect-configuration-id ProtectConfigId
```

In the preceding command, make the following changes:

- Replace *ProtectConfigId* with the unique identifier of the protect configuration.

Manage deletion protection

When you turn on deletion protection for a protect configuration you will not be able to delete the protect configuration until deletion protection is disabled and the protect configuration is no longer associated with a configuration set or the *account default* protect configuration. By default, deletion protection is disabled.

To enable deletion protection for a protect configuration, you can use the Amazon Pinpoint SMS console, the `DeleteProtectConfiguration` action in the Amazon Pinpoint SMS and voice v2 API, or the `aws sms-voice delete-protect-configuration` command in the AWS CLI. This section shows how to delete a protect configuration using the Amazon Pinpoint SMS console and the AWS CLI.

Enable deletion protection (Console)

Enable deletion protection

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Protect**, choose **Protect configuration**.
3. On the **Protect configurations** page, choose the protect configuration that will have deletion protection enabled.
4. On the **Deletion protection** tab, choose **Edit settings**.
5. Check **Enable deletion protection** and then **Save changes**.

Enable or disable deletion protection (AWS CLI)

You can use the `update-protect-configuration` command to enable deletion protection.

Enable deletion protection

- At the command line, enter the following command:

```
$ update-protect-configuration --protect-configuration-id ProtectConfigurationId
--deletion-protection-enabled Status
```

In the preceding command, make the following changes:

- Replace *ProtectConfigId* with the unique identifier of the protect configuration.
- Replace *Status* with *true* to enable or *false* to disable deletion protection.

Disable deletion protection (Console)

Disable deletion protection

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.

2. In the navigation pane, under **Protect**, choose **Protect configuration**.
3. On the **Protect configurations** page, choose the protect configuration that will have deletion protection disabled.
4. On the **Deletion protection** tab, choose **Edit settings**.
5. Uncheck **Enable deletion protection** and then **Save changes**.

Change a protect configuration's name

To help manage your protect configurations you should give them descriptive names. You can add or edit the name of a protect configuration at any time. You need to add a tag with the **Key** set to **Name** and the **Value** set to the name to use.

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Protect**, choose **Protect configuration**.
3. On the **Protect configuration** page, choose the protect configuration to add a tag to.
4. On the **Tags** tab, choose **Manage tags**. In **Manage tags**, choose **Add new tag**.
5. For **Key** enter **Name** and for **Value** enter a friendly name.
6. Choose **Save changes**.

Tags

Tags are pairs of keys and values that you can optionally apply to your AWS resources to control access or usage. Adding a tag to a resource can help you categorize and manage resources in different ways, such as by purpose, owner, environment, or other criteria. You can use tags to easily find existing resources, or to control which users can access specific resources.

To manage tags for a protect configuration, you can use the Amazon Pinpoint SMS console, the `TagResource` and `UntagResource` actions in the Amazon Pinpoint SMS and voice v2 API, or the `aws sms-voice tag-resource` and `aws sms-voice untag-resource` commands in the AWS CLI. This section shows how to tag and untag a protect configuration using the Amazon Pinpoint SMS console and the AWS CLI.

Manage tags (Console)

Use the Amazon Pinpoint SMS console to add, edit or delete a Tag.

Manage tags (Console)

1. Open the Amazon Pinpoint SMS console at <https://console.aws.amazon.com/sms-voice/>.
2. In the navigation pane, under **Protect**, choose **Protect configurations**.
3. On the **Protect configurations** page, choose the protect configurations to add a tag to.
4. On the **Tags** tab, choose **Manage tags**.
 - **Add a tag** – In **Manage tags**, choose **Add new tag** to create a new blank key/value pair.
 - **Delete a tag** – In **Manage tags**, choose **Remove** next to the key/value pair.
 - **Edit a tag** – In **Manage tags**, choose the **Key** or **Value** and edit the text.
5. Choose **Save changes**.

Manage tags (AWS CLI)

Use the AWS CLI to add or edit a Tag.

```
$ aws pinpoint-sms-voice-v2 tag-resource \  
  --resource-arn resource-arn \  
  --tags tags={key1=value1,key2=value2}
```

In the preceding example, do the following:

- Replace *resource-arn* with the Amazon Resource Name (ARN) that you want to add the tags to.
- Replace *key1* and *key2* with the keys of the tags that you want to add to the resource.
- Replace *value1* and *value2* with the values of the tags that you want to add for the respective keys.

Use the AWS CLI to delete a Tag.

```
$ aws pinpoint-sms-voice-v2 untag-resource \  
  --resource-arn resource-arn \  
  --tag-keys tags={key1=value1,key2=value2}
```

In the preceding example, do the following:

- Replace *resource-arn* with the Amazon Resource Name (ARN) that you want to remove the tag from.
- Replace *key1* and *key2* with the keys of the tags that you want to remove.
- Replace *value1* and *value2* with the values of the tags that you want to remove.

Security in Amazon Pinpoint SMS

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from data centers and network architectures that are built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The [shared responsibility model](#) describes this as security *of* the cloud and security *in* the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the [AWS Compliance Programs](#). To learn about the compliance programs that apply to Amazon Pinpoint SMS, see [AWS Services in Scope by Compliance Program](#).
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Amazon Pinpoint SMS. The following topics show you how to configure Amazon Pinpoint SMS to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Amazon Pinpoint SMS resources.

Topics

- [Data protection in Amazon Pinpoint SMS](#)
- [Identity and access management for Amazon Pinpoint SMS](#)
- [Compliance validation for Amazon Pinpoint SMS](#)
- [Resilience in Amazon Pinpoint SMS](#)
- [Infrastructure Security in Amazon Pinpoint SMS](#)
- [Configuration and vulnerability analysis in Amazon Pinpoint SMS](#)
- [Cross-service confused deputy prevention](#)
- [Security best practices](#)

Data protection in Amazon Pinpoint SMS

The AWS [shared responsibility model](#) applies to data protection in Amazon Pinpoint SMS. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. You are also responsible for the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the [Data Privacy FAQ](#). For information about data protection in Europe, see the [AWS Shared Responsibility Model and GDPR](#) blog post on the *AWS Security Blog*.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual users with AWS IAM Identity Center or AWS Identity and Access Management (IAM). That way, each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We require TLS 1.2 and recommend TLS 1.3.
- Set up API and user activity logging with AWS CloudTrail.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing sensitive data that is stored in Amazon S3.
- If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see [Federal Information Processing Standard \(FIPS\) 140-2](#).

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form text fields such as a **Name** field. This includes when you work with Amazon Pinpoint SMS or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form text fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

Data encryption

Amazon Pinpoint SMS data is encrypted in transit and at rest. When you submit data to Amazon Pinpoint SMS, it encrypts the data as it receives and stores it. When you retrieve data from Amazon Pinpoint SMS, it transmits the data to you by using current security protocols.

Encryption at rest

Amazon Pinpoint SMS encrypts all the data that it stores for you. This includes configuration data, registration data, and any data that you add into Amazon Pinpoint SMS. To encrypt your data, Amazon Pinpoint SMS uses internal AWS Key Management Service (AWS KMS) keys that the service owns and maintains on your behalf. We rotate these keys on a regular basis. For information about AWS KMS, see the [AWS Key Management Service Developer Guide](#).

Encryption in transit

Amazon Pinpoint SMS uses HTTPS and Transport Layer Security (TLS) 1.2 to communicate with your clients and applications. To communicate with other AWS services, Amazon Pinpoint SMS uses HTTPS and TLS 1.2. In addition, when you create and manage Amazon Pinpoint SMS resources by using the console, an AWS SDK, or the AWS Command Line Interface, all communications are secured using HTTPS and TLS 1.2.

Key management

To encrypt your Amazon Pinpoint SMS data, Amazon Pinpoint SMS uses internal AWS KMS keys that the service owns and maintains on your behalf. We rotate these keys on a regular basis. You can't provision and use your own AWS KMS or other keys to encrypt data that you store in Amazon Pinpoint SMS.

Inter-network traffic privacy

Internetwork traffic privacy refers to securing connections and traffic between Amazon Pinpoint SMS and your on-premises clients and applications, and between Amazon Pinpoint SMS and other AWS resources in the same AWS Region . The following features and practices can help you secure internetwork traffic privacy for Amazon Pinpoint SMS.

Traffic between Amazon Pinpoint SMS and on-premises clients and applications

To establish a private connection between Amazon Pinpoint SMS and clients and applications on your on-premises network, you can use AWS Direct Connect. This enables you to link your network

to an AWS Direct Connect location by using a standard, fiber-optic Ethernet cable. One end of the cable is connected to your router. The other end is connected to an AWS Direct Connect router. For more information, see [What is AWS Direct Connect?](#) in the *AWS Direct Connect User Guide*.

To help secure access to Amazon Pinpoint SMS through published APIs, we recommend that you comply with Amazon Pinpoint SMS requirements for API calls. Amazon Pinpoint SMS requires clients to use Transport Layer Security (TLS) 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS), such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). Most modern systems such as Java 7 and later support these modes.

In addition, requests must be signed using an access key ID and a secret access key that's associated with an AWS Identity and Access Management (IAM) principal for your AWS account. Alternatively, you can use the [AWS Security Token Service](#) (AWS STS) to generate temporary security credentials to sign requests.

Traffic between Amazon Pinpoint SMS and other AWS resources

To secure communications between Amazon Pinpoint SMS and other AWS resources in the same AWS Region, Amazon Pinpoint SMS uses HTTPS and TLS 1.2 by default.

Creating an interface VPC endpoint for Amazon Pinpoint SMS

You can establish a private connection between your virtual private cloud (VPC) and an endpoint in Amazon Pinpoint SMS by creating an interface VPC endpoint.

Interface endpoints are powered by [AWS PrivateLink](#), a technology that allows you to privately access Amazon Pinpoint SMS APIs without an internet gateway, NAT device, VPN connection, or AWS Direct Connect. Instances in your VPC don't need public IP addresses to communicate with the Amazon Pinpoint SMS APIs that integrate with AWS PrivateLink.

For more information, see the [AWS PrivateLink Guide](#).

Creating an interface VPC endpoints

You can create an interface endpoint using either the Amazon VPC console or the AWS Command Line Interface (AWS CLI). For more information, see [Create an interface endpoint](#) in the AWS PrivateLink Guide.

Amazon Pinpoint SMS supports the following service names:

- `com.amazonaws.region.sms-voice`

If you turn on private DNS for an interface endpoint, you can make API requests to Amazon Pinpoint SMS using the default DNS name for the AWS Region, for example, `com.amazonaws.us-east-1.sms-voice`. For more information, see [DNS hostnames](#) in the *AWS PrivateLink Guide*.

Creating a VPC endpoint policy

You can attach an endpoint policy to your VPC endpoint that controls access. The policy specifies the following information:

- The principal that can perform actions.
- The actions that can be performed.
- The resources on which actions can be performed.

For more information, see [Control access to services using endpoint policies](#) in the *AWS PrivateLink Guide*.

Example: VPC endpoint policy

The following VPC endpoint policy grants access to the listed Amazon Pinpoint SMS actions for all principals on all resources.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Action": [
        "sms-voice:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Identity and access management for Amazon Pinpoint SMS

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in)

and *authorized* (have permissions) to use Amazon Pinpoint SMS resources. IAM is an AWS service that you can use with no additional charge.

Topics

- [Audience](#)
- [Authenticating with identities](#)
- [Managing access using policies](#)
- [How Amazon Pinpoint SMS works with IAM](#)
- [Identity-based policy examples for Amazon Pinpoint SMS](#)
- [Troubleshooting Amazon Pinpoint SMS identity and access](#)
- [Amazon Pinpoint SMS actions for IAM policies](#)

Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work that you do in Amazon Pinpoint SMS.

Service user – If you use the Amazon Pinpoint SMS service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Amazon Pinpoint SMS features to do your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator. If you cannot access a feature in Amazon Pinpoint SMS, see [Troubleshooting Amazon Pinpoint SMS identity and access](#).

Service administrator – If you're in charge of Amazon Pinpoint SMS resources at your company, you probably have full access to Amazon Pinpoint SMS. It's your job to determine which Amazon Pinpoint SMS features and resources your service users should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with Amazon Pinpoint SMS, see [How Amazon Pinpoint SMS works with IAM](#).

IAM administrator – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to Amazon Pinpoint SMS. To view example Amazon Pinpoint SMS identity-based policies that you can use in IAM, see [Identity-based policy examples for Amazon Pinpoint SMS](#).

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. You must be *authenticated* (signed in to AWS) as the AWS account root user, as an IAM user, or by assuming an IAM role.

You can sign in to AWS as a federated identity by using credentials provided through an identity source. AWS IAM Identity Center (IAM Identity Center) users, your company's single sign-on authentication, and your Google or Facebook credentials are examples of federated identities. When you sign in as a federated identity, your administrator previously set up identity federation using IAM roles. When you access AWS by using federation, you are indirectly assuming a role.

Depending on the type of user you are, you can sign in to the AWS Management Console or the AWS access portal. For more information about signing in to AWS, see [How to sign in to your AWS account](#) in the *AWS Sign-In User Guide*.

If you access AWS programmatically, AWS provides a software development kit (SDK) and a command line interface (CLI) to cryptographically sign your requests by using your credentials. If you don't use AWS tools, you must sign requests yourself. For more information about using the recommended method to sign requests yourself, see [Signing AWS API requests](#) in the *IAM User Guide*.

Regardless of the authentication method that you use, you might be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see [Multi-factor authentication](#) in the *AWS IAM Identity Center User Guide* and [Using multi-factor authentication \(MFA\) in AWS](#) in the *IAM User Guide*.

AWS account root user

When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see [Tasks that require root user credentials](#) in the *IAM User Guide*.

Federated identity

As a best practice, require human users, including users that require administrator access, to use federation with an identity provider to access AWS services by using temporary credentials.

A *federated identity* is a user from your enterprise user directory, a web identity provider, the AWS Directory Service, the Identity Center directory, or any user that accesses AWS services by using credentials provided through an identity source. When federated identities access AWS accounts, they assume roles, and the roles provide temporary credentials.

For centralized access management, we recommend that you use AWS IAM Identity Center. You can create users and groups in IAM Identity Center, or you can connect and synchronize to a set of users and groups in your own identity source for use across all your AWS accounts and applications. For information about IAM Identity Center, see [What is IAM Identity Center?](#) in the *AWS IAM Identity Center User Guide*.

IAM users and groups

An [IAM user](#) is an identity within your AWS account that has specific permissions for a single person or application. Where possible, we recommend relying on temporary credentials instead of creating IAM users who have long-term credentials such as passwords and access keys. However, if you have specific use cases that require long-term credentials with IAM users, we recommend that you rotate access keys. For more information, see [Rotate access keys regularly for use cases that require long-term credentials](#) in the *IAM User Guide*.

An [IAM group](#) is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named *IAMAdmins* and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see [When to create an IAM user \(instead of a role\)](#) in the *IAM User Guide*.

IAM roles

An [IAM role](#) is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. You can temporarily assume an IAM role in the AWS Management Console by [switching roles](#). You can assume a role by calling an AWS CLI or

AWS API operation or by using a custom URL. For more information about methods for using roles, see [Using IAM roles](#) in the *IAM User Guide*.

IAM roles with temporary credentials are useful in the following situations:

- **Federated user access** – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see [Creating a role for a third-party Identity Provider](#) in the *IAM User Guide*. If you use IAM Identity Center, you configure a permission set. To control what your identities can access after they authenticate, IAM Identity Center correlates the permission set to a role in IAM. For information about permissions sets, see [Permission sets](#) in the *AWS IAM Identity Center User Guide*.
- **Temporary IAM user permissions** – An IAM user or role can assume an IAM role to temporarily take on different permissions for a specific task.
- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see [Cross account resource access in IAM](#) in the *IAM User Guide*.
- **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.
- **Forward access sessions (FAS)** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. When you use some services, you might perform an action that then initiates another action in a different service. FAS uses the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. FAS requests are only made when a service receives a request that requires interactions with other AWS services or resources to complete. In this case, you must have permissions to perform both actions. For policy details when making FAS requests, see [Forward access sessions](#).
- **Service role** – A service role is an [IAM role](#) that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see [Creating a role to delegate permissions to an AWS service](#) in the *IAM User Guide*.

- **Service-linked role** – A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.
- **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see [Using an IAM role to grant permissions to applications running on Amazon EC2 instances](#) in the *IAM User Guide*.

To learn whether to use IAM roles or IAM users, see [When to create an IAM role \(instead of a user\)](#) in the *IAM User Guide*.

Managing access using policies

You control access in AWS by creating policies and attaching them to AWS identities or resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when a principal (user, root user, or role session) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see [Overview of JSON policies](#) in the *IAM User Guide*.

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

By default, users and roles have no permissions. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see [Creating IAM policies](#) in the *IAM User Guide*.

Identity-based policies can be further categorized as *inline policies* or *managed policies*. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see [Choosing between managed policies and inline policies](#) in the *IAM User Guide*.

Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must [specify a principal](#) in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

Access control lists (ACLs)

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs. To learn more about ACLs, see [Access control list \(ACL\) overview](#) in the *Amazon Simple Storage Service Developer Guide*.

Other policy types

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of an entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the `Principal` field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see [Permissions boundaries for IAM entities](#) in the *IAM User Guide*.
- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see [How SCPs work](#) in the *AWS Organizations User Guide*.
- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see [Session policies](#) in the *IAM User Guide*.

Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see [Policy evaluation logic](#) in the *IAM User Guide*.

How Amazon Pinpoint SMS works with IAM

Before you use IAM to manage access to Amazon Pinpoint SMS, learn what IAM features are available to use with Amazon Pinpoint SMS.

IAM features you can use with Amazon Pinpoint SMS

IAM feature	Amazon Pinpoint SMS support
Identity-based policies	Yes
Resource-based policies	No
Policy actions	Yes
Policy resources	Yes
Policy condition keys	Yes
ACLs	No
ABAC (tags in policies)	Partial
Temporary credentials	Yes
Forward access sessions (FAS)	No
Service roles	Yes
Service-linked roles	No

To get a high-level view of how Amazon Pinpoint SMS and other AWS services work with most IAM features, see [AWS services that work with IAM](#) in the *IAM User Guide*.

Identity-based policies for Amazon Pinpoint SMS

Supports identity-based policies	Yes
----------------------------------	-----

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see [Creating IAM policies](#) in the *IAM User Guide*.

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. You can't specify the principal in an identity-based policy because it applies to the user or role to which it is attached. To learn about all of the elements that you can use in a JSON policy, see [IAM JSON policy elements reference](#) in the *IAM User Guide*.

Identity-based policy examples for Amazon Pinpoint SMS

To view examples of Amazon Pinpoint SMS identity-based policies, see [Identity-based policy examples for Amazon Pinpoint SMS](#).

Resource-based policies within Amazon Pinpoint SMS

Supports resource-based policies	No
----------------------------------	----

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are *IAM role trust policies* and *Amazon S3 bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must [specify a principal](#) in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

To enable cross-account access, you can specify an entire account or IAM entities in another account as the principal in a resource-based policy. Adding a cross-account principal to a resource-based policy is only half of establishing the trust relationship. When the principal and the resource are in different AWS accounts, an IAM administrator in the trusted account must also grant the principal entity (user or role) permission to access the resource. They grant permission by attaching an identity-based policy to the entity. However, if a resource-based policy grants access to a principal in the same account, no additional identity-based policy is required. For more information, see [Cross account resource access in IAM](#) in the *IAM User Guide*.

Policy actions for Amazon Pinpoint SMS

Supports policy actions	Yes
-------------------------	-----

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Action` element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Policy actions usually have the same name as the associated AWS API operation. There are some exceptions, such as *permission-only actions* that don't have a matching API operation. There are also some operations that require multiple actions in a policy. These additional actions are called *dependent actions*.

Include actions in a policy to grant permissions to perform the associated operation.

To see a list of Amazon Pinpoint SMS actions, see [Actions Defined by Amazon Pinpoint SMS](#) in the *Service Authorization Reference*.

Policy actions in Amazon Pinpoint SMS use the following prefix before the action:

```
sms-voice
```

To specify multiple actions in a single statement, separate them with commas.

```
"Action": [  
  "sms-voice:action1",  
  "sms-voice:action2"  
]
```

You can specify multiple actions using wildcards (*). For example, to specify all actions that begin with the word `Describe`, include the following action:

```
"Action": "sms-voice:Describe*"
```

To see a list of Amazon Pinpoint SMS actions, see [Actions Defined by Amazon Pinpoint SMS](#) in the *IAM User Guide*.

However, as a best practice, you should create policies that follow the principle of *least privilege*. In other words, you should create policies that include only the permissions that are required to perform a specific action.

For a list of Amazon Pinpoint SMS actions that you can use in IAM policies, see [Amazon Pinpoint SMS actions for IAM policies](#).

To view examples of Amazon Pinpoint SMS identity-based policies, see [Identity-based policy examples for Amazon Pinpoint SMS](#).

Policy resources for Amazon Pinpoint SMS

Supports policy resources	Yes
---------------------------	-----

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The Resource JSON policy element specifies the object or objects to which the action applies. Statements must include either a Resource or a NotResource element. As a best practice, specify a resource using its [Amazon Resource Name \(ARN\)](#). You can do this for actions that support a specific resource type, known as *resource-level permissions*.

For actions that don't support resource-level permissions, such as listing operations, use a wildcard (*) to indicate that the statement applies to all resources.

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

To see a list of Amazon Pinpoint SMS resource types and their ARNs, see [Resources Defined by Amazon Pinpoint SMS](#) in the *Service Authorization Reference*. To learn with which actions you can specify the ARN of each resource, see [Actions Defined by Amazon Pinpoint SMS](#).

To view examples of Amazon Pinpoint SMS identity-based policies, see [Identity-based policy examples for Amazon Pinpoint SMS](#).

Some Amazon Pinpoint SMS actions, such as certain actions for creating resources, can't be performed on a specific resource. In those cases, you must use the wildcard (*):

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

In IAM policies, you can also specify ARNs for the following types of SMS and Voice resources:

- Configuration Set
- Opt Out List

- Phone Number
- Pool
- Registration
- Registration attachment
- Sender Id
- Verified destination phone number

For example, to create a policy statement for a phone number that has the phone number ID phone-12345678901234567890123456789012 use the following ARN:

```
"Resource": "arn:aws:sms-voice:us-east-1:123456789012:phone-number/  
phone-12345678901234567890123456789012"
```

To specify all phone numbers that belong to a specific account, use a wildcard (*) in place of the phone number ID:

```
"Resource": "arn:aws:sms-voice:us-east-1:123456789012:phone-number/*"
```

Some Amazon Pinpoint SMS and Voice actions are not performed on a specific resource, such as those for managing account-level settings like spend limits. In those cases, you must use the wildcard (*):

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

Policy condition keys for Amazon Pinpoint SMS

Supports service-specific policy condition keys	Yes
---	-----

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The **Condition** element (or *Condition block*) lets you specify conditions in which a statement is in effect. The **Condition** element is optional. You can create conditional expressions that use [condition operators](#), such as equals or less than, to match the condition in the policy with values in the request.

If you specify multiple `Condition` elements in a statement, or multiple keys in a single `Condition` element, AWS evaluates them using a logical AND operation. If you specify multiple values for a single condition key, AWS evaluates the condition using a logical OR operation. All of the conditions must be met before the statement's permissions are granted.

You can also use placeholder variables when you specify conditions. For example, you can grant an IAM user permission to access a resource only if it is tagged with their IAM user name. For more information, see [IAM policy elements: variables and tags](#) in the *IAM User Guide*.

AWS supports global condition keys and service-specific condition keys. To see all AWS global condition keys, see [AWS global condition context keys](#) in the *IAM User Guide*.

To see a list of Amazon Pinpoint SMS condition keys, see [Condition Keys for Amazon Pinpoint SMS](#) in the *Service Authorization Reference*. To learn with which actions and resources you can use a condition key, see [Actions Defined by Amazon Pinpoint SMS](#).

To view examples of Amazon Pinpoint SMS identity-based policies, see [Identity-based policy examples for Amazon Pinpoint SMS](#).

Amazon Pinpoint SMS defines its own set of condition keys and also supports some global condition keys. To see a list of all AWS global condition keys, see [AWS global condition context keys](#) in the *IAM User Guide*. To see a list of Amazon Pinpoint SMS condition keys, see [Condition Keys for Amazon Pinpoint SMS](#) in the *IAM User Guide*. To learn which actions and resources you can use a condition key with, see [Actions Defined by Amazon Pinpoint SMS](#) in the *IAM User Guide*.

ACLs in Amazon Pinpoint SMS

Supports ACLs

No

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

ABAC with Amazon Pinpoint SMS

Supports ABAC (tags in policies)

Partial

Attribute-based access control (ABAC) is an authorization strategy that defines permissions based on attributes. In AWS, these attributes are called *tags*. You can attach tags to IAM entities (users or roles) and to many AWS resources. Tagging entities and resources is the first step of ABAC. Then you design ABAC policies to allow operations when the principal's tag matches the tag on the resource that they are trying to access.

ABAC is helpful in environments that are growing rapidly and helps with situations where policy management becomes cumbersome.

To control access based on tags, you provide tag information in the [condition element](#) of a policy using the `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, or `aws:TagKeys` condition keys.

If a service supports all three condition keys for every resource type, then the value is **Yes** for the service. If a service supports all three condition keys for only some resource types, then the value is **Partial**.

For more information about ABAC, see [What is ABAC?](#) in the *IAM User Guide*. To view a tutorial with steps for setting up ABAC, see [Use attribute-based access control \(ABAC\)](#) in the *IAM User Guide*.

Using temporary credentials with Amazon Pinpoint SMS

Supports temporary credentials	Yes
--------------------------------	-----

Some AWS services don't work when you sign in using temporary credentials. For additional information, including which AWS services work with temporary credentials, see [AWS services that work with IAM](#) in the *IAM User Guide*.

You are using temporary credentials if you sign in to the AWS Management Console using any method except a user name and password. For example, when you access AWS using your company's single sign-on (SSO) link, that process automatically creates temporary credentials. You also automatically create temporary credentials when you sign in to the console as a user and then switch roles. For more information about switching roles, see [Switching to a role \(console\)](#) in the *IAM User Guide*.

You can manually create temporary credentials using the AWS CLI or AWS API. You can then use those temporary credentials to access AWS. AWS recommends that you dynamically generate temporary credentials instead of using long-term access keys. For more information, see [Temporary security credentials in IAM](#).

Forward access sessions for Amazon Pinpoint SMS

Supports forward access sessions (FAS)	No
--	----

When you use an IAM user or role to perform actions in AWS, you are considered a principal. When you use some services, you might perform an action that then initiates another action in a different service. FAS uses the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. FAS requests are only made when a service receives a request that requires interactions with other AWS services or resources to complete. In this case, you must have permissions to perform both actions. For policy details when making FAS requests, see [Forward access sessions](#).

Service roles for Amazon Pinpoint SMS

Supports service roles	Yes
------------------------	-----

A service role is an [IAM role](#) that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see [Creating a role to delegate permissions to an AWS service](#) in the *IAM User Guide*.

Warning

Changing the permissions for a service role might break Amazon Pinpoint SMS functionality. Edit service roles only when Amazon Pinpoint SMS provides guidance to do so.

Service-linked roles for Amazon Pinpoint SMS

Supports service-linked roles	No
-------------------------------	----

A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

For details about creating or managing service-linked roles, see [AWS services that work with IAM](#). Find a service in the table that includes a Yes in the **Service-linked role** column. Choose the **Yes** link to view the service-linked role documentation for that service.

Identity-based policy examples for Amazon Pinpoint SMS

By default, users and roles don't have permission to create or modify Amazon Pinpoint SMS resources. They also can't perform tasks by using the AWS Management Console, AWS Command Line Interface (AWS CLI), or AWS API. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

To learn how to create an IAM identity-based policy by using these example JSON policy documents, see [Creating IAM policies](#) in the *IAM User Guide*.

For details about actions and resource types defined by Amazon Pinpoint SMS, including the format of the ARNs for each of the resource types, see [Actions, Resources, and Condition Keys for Amazon Pinpoint SMS](#) in the *Service Authorization Reference*.

Topics

- [Policy best practices](#)
- [Using the Amazon Pinpoint SMS console](#)
- [Allow users to view their own permissions](#)
- [Examples: Providing access to Amazon Pinpoint SMS and Voice v2 API actions](#)
- [IAM role for streaming events to Kinesis](#)

Policy best practices

Identity-based policies determine whether someone can create, access, or delete Amazon Pinpoint SMS resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the *AWS managed policies* that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies that are specific to your use cases. For more information, see [AWS managed policies](#) or [AWS managed policies for job functions](#) in the *IAM User Guide*.

- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. For more information about using IAM to apply permissions, see [Policies and permissions in IAM](#) in the *IAM User Guide*.
- **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific AWS service, such as AWS CloudFormation. For more information, see [IAM JSON policy elements: Condition](#) in the *IAM User Guide*.
- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions** – IAM Access Analyzer validates new and existing policies so that the policies adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see [IAM Access Analyzer policy validation](#) in the *IAM User Guide*.
- **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users or a root user in your AWS account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see [Configuring MFA-protected API access](#) in the *IAM User Guide*.

For more information about best practices in IAM, see [Security best practices in IAM](#) in the *IAM User Guide*.

Using the Amazon Pinpoint SMS console

To access the Amazon Pinpoint SMS console, you must have a minimum set of permissions. These permissions must allow you to list and view details about the Amazon Pinpoint SMS resources in your AWS account. If you create an identity-based policy that is more restrictive than the minimum required permissions, the console won't function as intended for entities (users or roles) with that policy.

You don't need to allow minimum console permissions for users that are making calls only to the AWS CLI or the AWS API. Instead, allow access to only the actions that match the API operation that they're trying to perform.

To ensure that users and roles can still use the Amazon Pinpoint SMS console, also attach the Amazon Pinpoint SMS *ConsoleAccess* or *ReadOnly* AWS managed policy to the entities. For more information, see [Adding permissions to a user](#) in the *IAM User Guide*.

Allow users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or 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": "*"
    }
  ]
}
```

Examples: Providing access to Amazon Pinpoint SMS and Voice v2 API actions

This section provides example policies that allow access to features that are available from the Amazon Pinpoint SMS and Voice v2 API. This is a supplemental API that provides advanced options for using and managing the SMS and voice channels in Amazon Pinpoint SMS. To learn more about this API, see the [Amazon Pinpoint SMS and Voice v2 API](#).

Read-only access

The following example policy allows read-only access to all Amazon Pinpoint SMS and Voice v2 API actions and resources in your AWS account:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SMSVoiceReadOnly",
      "Effect": "Allow",
      "Action": [
        "sms-voice:List*",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeAccountLimits",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptedOutNumbers",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeRegistrationAttachments",
        "sms-voice:DescribeRegistrationFieldDefinitions",
        "sms-voice:DescribeRegistrations",
        "sms-voice:DescribeRegistrationSectionDefinitions",
        "sms-voice:DescribeRegistrationTypeDefinitions",
        "sms-voice:DescribeRegistrationVersions",
        "sms-voice:DescribeSenderId",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:DescribeVerifiedDestinationNumbers"
      ],
      "Resource": "*"
    }
  ]
}
```

Administrator access

The following example policy allows full access to all Amazon Pinpoint SMS and Voice v2 API actions and resources in your AWS account:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SMSVoiceFullAccess",
      "Effect": "Allow",
      "Action": [
        "sms-voice:*"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "accountId"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:sms-voice:region:accountId:*"
        }
      }
    }
  ]
}
```

IAM role for streaming events to Kinesis

Amazon Pinpoint SMS can automatically send app usage data, or *event data*, from your app to an Amazon Kinesis data stream or Amazon Data Firehose delivery stream in your AWS account. Before Amazon Pinpoint SMS can begin streaming the event data, you must delegate the required permissions to Amazon Pinpoint SMS.

If you use the console to set up event streaming, Amazon Pinpoint SMS automatically creates an AWS Identity and Access Management (IAM) role with the required permissions.

If you want to create the role manually, attach the following policies to the role:

- A permissions policy that allows Amazon Pinpoint SMS to send event data to your stream.
- A trust policy that allows Amazon Pinpoint SMS to assume the role.

After you create the role, you can configure Amazon Pinpoint SMS to automatically send events to your stream. For more information, see [Amazon Data Firehose event destinations](#) in this guide.

Troubleshooting Amazon Pinpoint SMS identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with Amazon Pinpoint SMS and IAM.

Topics

- [I am not authorized to perform an action in Amazon Pinpoint SMS](#)
- [I am not authorized to perform iam:PassRole](#)
- [I want to allow people outside of my AWS account to access my Amazon Pinpoint SMS resources](#)

I am not authorized to perform an action in Amazon Pinpoint SMS

If you receive an error that you're not authorized to perform an action, your policies must be updated to allow you to perform the action.

The following example error occurs when the `mateojackson` IAM user tries to use the console to view details about a fictional `my-example-widget` resource but doesn't have the fictional `sms-voice:GetWidget` permissions.

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

In this case, the policy for the `mateojackson` user must be updated to allow access to the `my-example-widget` resource by using the `sms-voice:GetWidget` action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

I am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, your policies must be updated to allow you to pass a role to Amazon Pinpoint SMS.

Some AWS services allow you to pass an existing role to that service instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named `marymajor` tries to use the console to perform an action in Amazon Pinpoint SMS. However, the action requires the service to have permissions that are granted by a service role. Mary does not have permissions to pass the role to the service.

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

In this case, Mary's policies must be updated to allow her to perform the `iam:PassRole` action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

I want to allow people outside of my AWS account to access my Amazon Pinpoint SMS resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Amazon Pinpoint SMS supports these features, see [How Amazon Pinpoint SMS works with IAM](#).
- To learn how to provide access to your resources across AWS accounts that you own, see [Providing access to an IAM user in another AWS account that you own](#) in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see [Providing access to AWS accounts owned by third parties](#) in the *IAM User Guide*.
- To learn how to provide access through identity federation, see [Providing access to externally authenticated users \(identity federation\)](#) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see [Cross account resource access in IAM](#) in the *IAM User Guide*.

Amazon Pinpoint SMS actions for IAM policies

To manage access to Amazon Pinpoint SMS resources in your AWS account, you can add Amazon Pinpoint SMS actions to AWS Identity and Access Management (IAM) policies. By using actions in policies, you can control what users can do on the Amazon Pinpoint SMS console. You can also control what users can do programmatically by using the AWS SDKs, the AWS Command Line Interface (AWS CLI), or the Amazon Pinpoint SMS APIs directly.

This topic identifies Amazon Pinpoint SMS actions that you can add to IAM policies for your AWS account. To see examples that demonstrate how you can use actions in policies to manage access to Amazon Pinpoint SMS resources, see [Identity-based policy examples for Amazon Pinpoint SMS](#).

Topics

- [Amazon Pinpoint SMS and Voice v2 API actions](#)

Amazon Pinpoint SMS and Voice v2 API actions

This section identifies actions for features that are available from the Amazon Pinpoint SMS and Voice v2 API. For the Amazon Pinpoint SMS and Voice v2 API is an API that provides advanced options for using and managing the SMS and voice channels. For a complete list of actions available in version 2, see the [Amazon Pinpoint SMS and Voice API version 2 API Reference](#).

sms-voice:AssociateOriginationIdentity

Associate the specified origination identity with a pool.

- Resource ARN – `arn:aws:sms-voice:region:accountId:pool/poolId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:phone-number/phoneNumberId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:sender-id/senderId/isoCountyCode`

sms-voice:AssociateProtectConfiguration

Associate the specified protect configuration with a configuration set.

- Resource ARN – `arn:aws:sms-voice:region:accountId:configuration-set/configurationSetName`
- Resource ARN – `arn:aws:sms-voice:region:accountId:protect-configuration/ProtectConfigurationId`

sms-voice:CreateConfigurationSet

Create a new configuration set.

- Resource ARN – `arn:aws:sms-voice:region:accountId:configuration-set/configurationSetName`

sms-voice:CreateEventDestination

Create a new event destination in a configuration set.

- Resource ARN – `arn:aws:sms-voice:region:accountId:configuration-set/configurationSetName`

sms-voice:CreateOptOutList

Create a new opt-out list.

- Resource ARN – `arn:aws:sms-voice:region:accountId:opt-out-list/optOutListName`

sms-voice:CreatePool

Create a new pool and associates the specified origination identity to the pool.

- Resource ARN – `arn:aws:sms-voice:region:accountId:pool/poolId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:phone-number/phoneNumberId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:sender-id/senderId/isoCountyCode`

sms-voice:CreateProtectConfiguration

Create a new protect configuration.

- Resource ARN – `arn:aws:sms-voice:region:accountId:protect-configuration/ProtectConfigurationId`

sms-voice:CreateRegistration

Create a registration.

- Resource ARN – `arn:aws:sms-voice:region:accountId:registration/registrationId`

sms-voice:CreateRegistrationAssociation

Associate a registration with an origination identity.

- Resource ARN – `arn:aws:sms-voice:region:accountId:registration/registrationId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:phone-number/phoneNumberId`

sms-voice:CreateRegistrationAttachment

Create an attachment for a registration.

- Resource ARN – `arn:aws:sms-voice:region:accountId:registration-attachment/registrationAttachmentId`

sms-voice:CreateRegistrationVersion

Create a new version of the registration.

- Resource ARN – `arn:aws:sms-voice:region:accountId:registration/registrationId`

sms-voice:CreateVerifiedDestinationNumber

Create a new verified destination phone number.

- Resource ARN – `arn:aws:sms-voice:region:accountId:verified-destination-number/verifiedDestinationNumberId`

sms-voice>DeleteAccountDefaultProtectConfiguration

Disassociate the account default protect configuration.

- Resource ARN – Not available. Use *.

sms-voice>DeleteConfigurationSet

Delete an existing configuration set.

- Resource ARN – `arn:aws:sms-voice:region:accountId:configuration-set/configurationSetName`

sms-voice>DeleteDefaultMessageType

Delete an existing default message type on a configuration set.

- Resource ARN – `arn:aws:sms-voice:region:accountId:configuration-set/configurationSetName`

sms-voice>DeleteDefaultSenderId

Delete an existing default sender ID on a configuration set.

- Resource ARN – `arn:aws:sms-voice:region:accountId:sender-id/configuration-set/configurationSetName`

sms-voice:DeleteEventDestination

Delete an existing event destination.

- Resource ARN – `arn:aws:sms-voice:region:accountId:configuration-set/configurationSetName`

sms-voice:DeleteKeyword

Delete an existing keyword from an origination phone number or pool.

- Resource ARN – `arn:aws:sms-voice:region:accountId:pool/poolId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:phone-number/phoneNumberId`

sms-voice:DeleteMediaMessageSpendLimitOverride

Delete an account-level monthly spending limit override for sending MMS messages.

- Resource ARN – Not available. Use *.

sms-voice:DeleteOptedOutNumber

Delete an existing opted out destination phone number from the specified opt-out list.

- Resource ARN – `arn:aws:sms-voice:region:accountId:opt-out-list/optOutListName`

sms-voice:DeleteOptOutList

Delete an existing opt-out list. All opted out phone numbers in the opt-out list are deleted.

- Resource ARN – `arn:aws:sms-voice:region:accountId:opt-out-list/optOutListName`

sms-voice:DeletePool

Delete an existing pool.

- Resource ARN – `arn:aws:sms-voice:region:accountId:pool/poolId`

sms-voice:DeleteProtectConfiguration

Delete a protect configuration.

- Resource ARN – `arn:aws:sms-voice:region:accountId:protect-configuration/ProtectConfigurationId`

sms-voice:DeleteRegistration

Delete a new version of the registration.

- Resource ARN – `arn:aws:sms-voice:region:accountId:registration/registrationId`

sms-voice:DeleteRegistrationAttachment

Delete the registration attachment.

- Resource ARN – `arn:aws:sms-voice:region:accountId:registration-attachment/registrationAttachmentId`

sms-voice:DeleteRegistrationFieldValue

Delete the value from a registration field.

- Resource ARN – `arn:aws:sms-voice:region:accountId:registration/registrationId`

sms-voice:DeleteTextMessageSpendLimitOverride

Delete an account-level monthly spending limit override for sending text messages.

- Resource ARN – Not available. Use *.

sms-voice:DeleteVerifiedDestinationNumber

Delete a verified destination phone number.

- Resource ARN – `arn:aws:sms-voice:region:accountId:verified-destination-number/verifiedDestinationNumberId`

sms-voice:DeleteVoiceMessageSpendLimitOverride

Delete an account-level monthly spend limit override for sending voice messages.

- Resource ARN – Not available. Use *.

sms-voice:DescribeAccountAttributes

Describe attributes of your AWS account.

- Resource ARN – Not available. Use *.

sms-voice:DescribeAccountLimits

Describe the current Amazon Pinpoint SMS Voice V2 resource quotas for your account.

- Resource ARN – Not available. Use *.

sms-voice:DescribeConfigurationSets

Describe the specified configuration sets or all in your account.

- Resource ARN – `arn:aws:sms-voice:region:accountId:configuration-set/configurationSetName`

sms-voice:DescribeKeywords

Describe the specified keywords or all keywords on your origination phone number or pool.

- Resource ARN – `arn:aws:sms-voice:region:accountId:pool/poolId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:phone-number/phoneNumberId`

sms-voice:DescribeOptedOutNumbers

Describe the specified opted out destination numbers or all opted out destination numbers in an opt-out list.

- Resource ARN – `arn:aws:sms-voice:region:accountId:opt-out-list/optOutListName`

sms-voice:DescribeOptOutLists

Describe the specified opt-out list or all opt-out lists in your account.

- Resource ARN – `arn:aws:sms-voice:region:accountId:opt-out-list/optOutListName`

sms-voice:DescribePhoneNumbers

Describe the specified origination phone number, or all the phone numbers in your account.

- Resource ARN – `arn:aws:sms-voice:region:accountId:phone-number/phoneNumberId`

sms-voice:DescribePools

Retrieve the specified pools or all pools associated with your AWS account.

- Resource ARN – `arn:aws:sms-voice:region:accountId:pool/poolId`

sms-voice:DescribeProtectConfiguration

Retrieve the specified protect configurations.

- Resource ARN – `arn:aws:sms-voice:region:accountId:protect-configuration/ProtectConfigurationId`

sms-voice:DescribeRegistrationAttachments

List all registration attachments.

- Resource ARN – `arn:aws:sms-voice:region:accountId:registration-attachment/registrationAttachmentId`

sms-voice:DescribeRegistrationFieldDefinitions

List the field definition for a registration.

- Resource ARN – Not available. Use *.

sms-voice:DescribeRegistrationFieldValues

List the field values for a registration.

- Resource ARN – `arn:aws:sms-voice:region:accountId:registration/registrationId`

sms-voice:DescribeRegistrations

List the registrations in your account.

- Resource ARN – `arn:aws:sms-voice:region:accountId:registration/registrationId`

sms-voice:DescribeRegistrationSectionDefinitions

List the section definition for a registration.

- Resource ARN – Not available. Use *.

sms-voice:DescribeRegistrationTypeDefinitions

List the type definitions for a registration.

- Resource ARN – Not available. Use *.

sms-voice:DescribeRegistrationVersions

List the versions for a registration.

- Resource ARN – `arn:aws:sms-voice:region:accountId:registration/registrationId`

sms-voice:DescribeSenderIds

Describe the specified SenderIds or all SenderIds associated with your AWS account.

- Resource ARN – `arn:aws:sms-voice:region:accountId:sender-id/senderId/isoCountryCode`

sms-voice:DescribeSpendLimits

Describe the current Amazon Pinpoint monthly spend limits for sending voice and text messages.

- Resource ARN – Not available. Use *.

sms-voice:DescribeVerifiedDestinationNumbers

List the verified destination phone numbers in your account.

- Resource ARN – `arn:aws:sms-voice:region:accountId:verified-destination-number/verifiedDestinationNumberId`

sms-voice:DisassociateOriginationIdentity

Remove the specified origination identity from an existing pool.

- Resource ARN – `arn:aws:sms-voice:region:accountId:pool/poolId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:phone-number/phoneNumberId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:sender-id/senderId/isoCountryCode`

sms-voice:DisassociateProtectConfiguration

Disassociate a configuration set from a protect configuration.

- Resource ARN – `arn:aws:sms-voice:region:accountId:protect-configuration/ProtectConfigurationId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:configuration-set/configurationSetName`

sms-voice:DiscardRegistrationVersion

Discard the current version of a registration.

- Resource ARN – `arn:aws:sms-voice:region:accountId:registration/registrationId`

sms-voice:GetProtectConfigurationCountryRuleSet

Get the country rule set for a protect configuration.

- Resource ARN – `arn:aws:sms-voice:region:accountId:protect-configuration/ProtectConfigurationId`

sms-voice:ListPoolOriginationIdentities

Show the origination phone numbers in a pool.

- Resource ARN – `arn:aws:sms-voice:region:accountId:pool/poolId`

sms-voice:ListRegistrationAssociations

List all resources associated with the registration.

- Resource ARN – `arn:aws:sms-voice:region:accountId:registration/registrationId`

sms-voice:ListTagsForResource

List the tags associated with a resource.

- Resource ARN – `arn:aws:sms-voice:region:accountId:configuration-set/configurationSetName`
- Resource ARN – `arn:aws:sms-voice:region:accountId:opt-out-list/optOutListName`
- Resource ARN – `arn:aws:sms-voice:region:accountId:phone-number/phoneNumberId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:pool/poolId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:sender-id/senderId/isoCountryCode`

sms-voice:ProtectConfiguration

A protect configuration controls which destination countries messages can be sent to.

- Resource ARN – `arn:aws:sms-voice:region:accountId:protect-configuration/ProtectConfigurationId`

sms-voice:PutKeyword

Add or update a keyword on an origination phone number or pool.

- Resource ARN – `arn:aws:sms-voice:region:accountId:phone-number/phoneNumberId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:pool/poolId`

sms-voice:PutOptedOutNumber

Add a destination phone number to an opt-out list.

- Resource ARN – `arn:aws:sms-voice:region:accountId:opt-out-list/optOutListName`

sms-voice:PutRegistrationFieldValue

Update a field value in the registration.

- Resource ARN – `arn:aws:sms-voice:region:accountId:registration/registrationId`

sms-voice:ReleasePhoneNumber

Remove an origination phone number from your Amazon Pinpoint SMS account.

- Resource ARN – `arn:aws:sms-voice:region:accountId:phone-number/phoneNumberId`

sms-voice:ReleaseSenderId

Remove a sender ID from your Amazon Pinpoint SMS account.

- Resource ARN – `arn:aws:sms-voice:region:accountId:sender-id/senderId/isoCountryCode`

sms-voice:RequestPhoneNumber

Request to add an origination phone number to your account.

- Resource ARN – `arn:aws:sms-voice:region:accountId:phone-number/phoneNumberId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:pool/poolId`

sms-voice:RequestSenderId

Request a new sender ID.

- Resource ARN – `arn:aws:sms-voice:region:accountId:sender-id/senderId/isoCountryCode`

sms-voice:SendDestinationNumberVerificationCode

Send an SMS or voice message containing a verification code to the destination phone number.

- Resource ARN – `arn:aws:sms-voice:region:accountId:phone-number/phoneNumberId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:pool/poolId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:sender-id/senderId/isoCountryCode`

sms-voice:SendMediaMessage

Send an MMS message.

- Resource ARN – `arn:aws:sms-voice:region:accountId:phone-number/phoneNumberId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:pool/poolId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:sender-id/senderId/isoCountryCode`

sms-voice:SendTextMessage

Send an SMS message.

- Resource ARN – `arn:aws:sms-voice:region:accountId:phone-number/phoneNumberId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:pool/poolId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:sender-id/senderId/isoCountryCode`

sms-voice:SendVoiceMessage

Send a voice message.

- Resource ARN – `arn:aws:sms-voice:region:accountId:phone-number/phoneNumberId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:pool/poolId`

sms-voice:SetAccountDefaultProtectConfiguration

Set the account protect configuration.

- Resource ARN – `arn:aws:sms-voice:region:accountId:protect-configuration/ProtectConfigurationId`

sms-voice:SetDefaultMessageType

Set the default message type for SMS messages.

- Resource ARN – `arn:aws:sms-voice:region:accountId:configuration-set/configurationSetName`

sms-voice:SetDefaultSenderId

Set the default sender ID value for voice messages.

- Resource ARN – `arn:aws:sms-voice:region:accountId:configuration-set/configurationSetName`

sms-voice:SetMediaMessageSpendLimitOverride

Set a monthly spending limit for MMS messages.

- Resource ARN – Not available. Use *.

sms-voice:SetTextMessageSpendLimitOverride

Set a monthly spending limit for SMS messages.

- Resource ARN – Not available. Use *.

sms-voice:SetVoiceMessageSpendLimitOverride

Set a monthly spending limit for voice messages.

- Resource ARN – Not available. Use *.

sms-voice:SubmitRegistrationVersion

Submit the latest version of a registration.

- Resource ARN – `arn:aws:sms-voice:region:accountId:registration/registrationId`

sms-voice:TagResource

Add a tag to a resource.

- Resource ARN – `arn:aws:sms-voice:region:accountId:configuration-set/configurationSetName`
- Resource ARN – `arn:aws:sms-voice:region:accountId:opt-out-list/optOutListName`
- Resource ARN – `arn:aws:sms-voice:region:accountId:phone-number/phoneNumberId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:pool/poolId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:sender-id/senderId/isoCountryCode`

sms-voice:UntagResource

Remove tags from a resource.

- Resource ARN – `arn:aws:sms-voice:region:accountId:configuration-set/configurationSetName`

- Resource ARN – `arn:aws:sms-voice:region:accountId:opt-out-list/optOutListName`
- Resource ARN – `arn:aws:sms-voice:region:accountId:phone-number/phoneNumberId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:pool/poolId`
- Resource ARN – `arn:aws:sms-voice:region:accountId:sender-id/senderId/isoCountryCode`

sms-voice:UpdateEventDestination

Update an existing event destination.

- Resource ARN – `arn:aws:sms-voice:region:accountId:configuration-set/configurationSetName`

sms-voice:UpdatePhoneNumber

Update the configuration of an origination phone number.

- Resource ARN – `arn:aws:sms-voice:region:accountId:phone-number/phoneNumberId`

sms-voice:UpdateProtectConfiguration

Update the protect configuration.

- Resource ARN – `arn:aws:sms-voice:region:accountId:protect-configuration/ProtectConfigurationId`

sms-voice:UpdateProtectConfigurationCountryRuleSet

Update the country rule set of a protect configuration.

- Resource ARN – `arn:aws:sms-voice:region:accountId:protect-configuration/ProtectConfigurationId`

sms-voice:UpdatePool

Update an existing phone number pool.

- Resource ARN – `arn:aws:sms-voice:region:accountId:pool/poolId`

sms-voice:UpdateSenderId

Update a sender ID.

- Resource ARN – `arn:aws:sms-voice:region:accountId:sender-id/senderId/isoCountryCode`

sms-voice:VerifyDestinationNumber

Verify a destination phone number.

- Resource ARN – `arn:aws:sms-voice:region:accountId:verified-destination-number/verifiedDestinationNumberId`

Compliance validation for Amazon Pinpoint SMS

To learn whether an AWS service is within the scope of specific compliance programs, see [AWS services in Scope by Compliance Program](#) and choose the compliance program that you are interested in. For general information, see [AWS Compliance Programs](#).

You can download third-party audit reports using AWS Artifact. For more information, see [Downloading Reports in AWS Artifact](#).

Your compliance responsibility when using AWS services is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- [Security and Compliance Quick Start Guides](#) – These deployment guides discuss architectural considerations and provide steps for deploying baseline environments on AWS that are security and compliance focused.
- [Architecting for HIPAA Security and Compliance on Amazon Web Services](#) – This whitepaper describes how companies can use AWS to create HIPAA-eligible applications.

Note

Not all AWS services are HIPAA eligible. For more information, see the [HIPAA Eligible Services Reference](#).

- [AWS Compliance Resources](#) – This collection of workbooks and guides might apply to your industry and location.
- [AWS Customer Compliance Guides](#) – Understand the shared responsibility model through the lens of compliance. The guides summarize the best practices for securing AWS services and map the guidance to security controls across multiple frameworks (including National Institute of Standards and Technology (NIST), Payment Card Industry Security Standards Council (PCI), and International Organization for Standardization (ISO)).

- [Evaluating Resources with Rules](#) in the *AWS Config Developer Guide* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- [AWS Security Hub](#) – This AWS service provides a comprehensive view of your security state within AWS. Security Hub uses security controls to evaluate your AWS resources and to check your compliance against security industry standards and best practices. For a list of supported services and controls, see [Security Hub controls reference](#).
- [Amazon GuardDuty](#) – This AWS service detects potential threats to your AWS accounts, workloads, containers, and data by monitoring your environment for suspicious and malicious activities. GuardDuty can help you address various compliance requirements, like PCI DSS, by meeting intrusion detection requirements mandated by certain compliance frameworks.
- [AWS Audit Manager](#) – This AWS service helps you continuously audit your AWS usage to simplify how you manage risk and compliance with regulations and industry standards.

Resilience in Amazon Pinpoint SMS

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see [AWS Global Infrastructure](#).

In addition to the AWS global infrastructure, Amazon Pinpoint SMS offers several features to help support your data resiliency and backup needs.

Infrastructure Security in Amazon Pinpoint SMS

As a managed service, Amazon Pinpoint SMS is protected by the AWS global network security procedures that are described in the [Amazon Web Services: Overview of Security Processes](#) whitepaper.

You use AWS published API calls to access Amazon Pinpoint SMS through the network. Clients must support Transport Layer Security (TLS) 1.0 or later. We recommend TLS 1.2. Clients must also

support cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the [AWS Security Token Service](#) (AWS STS) to generate temporary security credentials to sign requests.

Configuration and vulnerability analysis in Amazon Pinpoint SMS

As a managed service, Amazon Pinpoint SMS is protected by AWS global network security. For information about AWS security services and how AWS protects infrastructure, see [AWS Cloud Security](#). To design your AWS environment using the best practices for infrastructure security, see [Infrastructure Protection](#) in *Security Pillar AWS Well-Architected Framework*.

You use AWS published API calls to access Amazon Pinpoint SMS through the network. Clients must support the following:

- Transport Layer Security (TLS). We require TLS 1.2 and recommend TLS 1.3.
- Cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the [AWS Security Token Service](#) (AWS STS) to generate temporary security credentials to sign requests.

Cross-service confused deputy prevention

The confused deputy problem is a security issue where an entity that doesn't have permission to perform an action can coerce a more-privileged entity to perform the action. In AWS, cross-service impersonation can result in the confused deputy problem. Cross-service impersonation can occur when one service (the *calling service*) calls another service (the *called service*). The calling service can be manipulated to use its permissions to act on another customer's resources in a way it should not otherwise have permission to access. To prevent this, AWS provides tools that help you protect

your data for all services with service principals that have been given access to resources in your account.

We recommend using the [aws:SourceArn](#) and [aws:SourceAccount](#) global condition context keys in resource policies to limit the permissions that Amazon Pinpoint SMS gives another service to the resource. Use `aws:SourceArn` if you want only one resource to be associated with the cross-service access. Use `aws:SourceAccount` if you want to allow any resource in that account to be associated with the cross-service use.

The most effective way to protect against the confused deputy problem is to use the `aws:SourceArn` global condition context key with the full ARN of the resource. If you don't know the full ARN of the resource or if you are specifying multiple resources, use the `aws:SourceArn` global condition context key with wildcard characters (*) for the unknown portions of the ARN. For example, `arn:aws:servicename:*:123456789012*`.

If the `aws:SourceArn` value does not contain the account ID, such as an Amazon S3 bucket ARN, you must use both global condition context keys to limit permissions.

The value of `aws:SourceArn` must be the ARN of the phone number.

The following example shows how you can use the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in Amazon Pinpoint SMS to prevent the confused deputy problem.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "sms-voice.amazonaws.com"
    },
    "Action": "sns:Publish",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "accountId"
      },
      "ArnLike": {
        "aws:SourceArn": "arn:aws:sms-voice:region:PhoneNumberARN:*"
      }
    }
  }
}
```

}

Security best practices

Amazon Pinpoint SMS provides a number of security features to consider as you develop and implement your own security policies. The following best practices are general guidelines and don't represent a complete security solution. Because these best practices might not be appropriate or sufficient for your environment, treat them as helpful considerations rather than prescriptions.

- Create an individual user for each person who manages Amazon Pinpoint SMS resources, including yourself. Don't use AWS root credentials to manage Amazon Pinpoint resources.
- Grant each user the minimum set of permissions required to perform his or her duties.
- Use IAM groups to effectively manage permissions for multiple users.
- Rotate your IAM credentials regularly.

Monitoring Amazon Pinpoint SMS

Monitoring is an important part of maintaining the reliability, availability, and performance of Amazon Pinpoint SMS and your other AWS solutions. AWS provides the following monitoring tools to watch Amazon Pinpoint SMS, report when something is wrong, and take automatic actions when appropriate:

- **Amazon CloudWatch** monitors your AWS resources and the applications you run on AWS in real time. You can collect and track metrics, create customized dashboards, and set alarms that notify you or take actions when a specified metric reaches a threshold that you specify. For example, you can have CloudWatch track CPU usage or other metrics of your Amazon EC2 instances and automatically launch new instances when needed. For more information, see the [Amazon CloudWatch User Guide](#).
- **Amazon CloudWatch Logs** enables you to monitor, store, and access your log files from Amazon EC2 instances, CloudTrail, and other sources. CloudWatch can monitor information in the log files and notify you when certain thresholds are met. You can also archive your log data in highly durable storage. For more information, see the [Amazon CloudWatch Logs User Guide](#).
- **AWS CloudTrail** captures API calls and related events made by or on behalf of your AWS account and delivers the log files to an Amazon S3 bucket that you specify. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred. For more information, see the [AWS CloudTrail User Guide](#).
- **AWS Health Dashboards**, can check and monitor the status of your Amazon Pinpoint SMS environment. To check the status of the Amazon Pinpoint SMS service overall, use the AWS Service Health Dashboard. To check, monitor, and view historical data about any events or issues that might affect your AWS environment more specifically, use the AWS Personal Health Dashboard. To learn more about these dashboards, see the [AWS Health User Guide](#).
- **AWS Trusted Advisor** inspects your AWS environment and provides recommendations for opportunities to address security gaps, improve system availability and performance, and save money. All AWS customers have access to a core set of Trusted Advisor checks. Customers who have a Business or Enterprise support plan have access to additional Trusted Advisor checks.

Many of these checks can help you assess the security posture of your Amazon Pinpoint SMS resources as part of your AWS account overall. For example, the core set of Trusted Advisor checks includes the following:

- Logging configurations for your AWS account, for each supported AWS Region .

- Access permissions for your Amazon Simple Storage Service (Amazon S3) buckets, which might contain files that you import into Amazon Pinpoint SMS to build segments.
- Use of AWS Identity and Access Management users, groups, and roles to control access to Amazon Pinpoint SMS resources.
- IAM configurations and policy settings that might compromise the security of your AWS environment and Amazon Pinpoint SMS resources.

For more information, see [AWS Trusted Advisor](#) in the *AWS Support User Guide*.

Topics

- [Monitoring Amazon Pinpoint SMS with Amazon CloudWatch](#)
- [Monitoring SMS, MMS, and voice spending activity with Amazon Pinpoint SMS](#)
- [Logging Amazon Pinpoint SMS and voice v2 API calls using AWS CloudTrail](#)

Monitoring Amazon Pinpoint SMS with Amazon CloudWatch

You can monitor Amazon Pinpoint SMS using CloudWatch, which collects raw data and processes it into readable, near real-time metrics. These statistics are kept for 15 months, so that you can access historical information and gain a better perspective on how your web application or service is performing. You can also set alarms that watch for certain thresholds, and send notifications or take actions when those thresholds are met. For more information, see the [Amazon CloudWatch User Guide](#).

For Amazon Pinpoint SMS, you might want to watch for **TextMessageMonthlySpend**, **MediaMessageMonthlySpend** and **VoiceMessageMonthlySpend** and trigger an alarm when greater than, greater than or equal to, or equal to the threshold. The namespace is for Amazon Pinpoint SMS is `AWS/SMSVoice`.

The following tables list the metrics and dimensions for Amazon Pinpoint SMS.

Metric	Description	Recommended statistic
TextMessageMonthlySpend	The amount of money (in US Dollars) that you have spent sending SMS messages this month.	Maximum

Metric	Description	Recommended statistic
	Unit: US Dollars	
VoiceMessageMonthlySpend	The amount of money (in US Dollars) that you have spent sending Voice messages this month. Unit: US Dollars	Maximum
MediaMessageMonthlySpend	The amount of money (in US Dollars) that you have spent sending MMS messages this month. Unit: US Dollars	Maximum

Monitoring SMS, MMS, and voice spending activity with Amazon Pinpoint SMS

This topic provides information about viewing SMS, MMS, and voice spending metrics in Amazon CloudWatch. It also explains how to set up a CloudWatch alarm that sends you a notification when your monthly SMS, MMS, or voice spending exceeds a certain amount.

If you only want to view your monthly charges for using Amazon Pinpoint SMS, including the amount of money you've spent, you should use the AWS Billing and Cost Management console. The Billing and Cost Management console provides an estimate of your bill for the current month, and your final charges for previous months. For more information, see [Viewing your monthly charges](#) in the *AWS Billing User Guide*.

View your monthly SMS, MMS, and voice spending by using CloudWatch

To quickly determine how much money you've spent sending SMS, MMS, and voice messages during the current month, you can use the Metrics section of the CloudWatch console. CloudWatch retains metrics data for 15 months, so you can view real-time data and analyze historical trends.

For more information about viewing metrics in CloudWatch, see [Using Amazon CloudWatch metrics](#) in the *Amazon CloudWatch User Guide*.

To view SMS, MMS, and voice spending metrics in CloudWatch

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. In the navigation pane, choose **Metrics**.
3. On the **All metrics** tab, choose **SMSVoice**.
4. Choose **Account Metrics**.
5. Select from options **TextMessageMonthlySpend**, **MediaMessageMonthlySpend**, and **VoiceMessageMonthlySpend**. Based on your selection, the graph updates to display the amount of money spent during the current month by using Amazon Pinpoint SMS.

Note

The **TextMessageMonthlySpend**, **MediaMessageMonthlySpend**, and **VoiceMessageMonthlySpend** metrics don't appear until you send at least one message using Amazon Pinpoint SMS.

Create an SMS, MMS, or voice spending alarm by using CloudWatch

In addition to viewing your monthly SMS, MMS, and voice spending metrics, you can create CloudWatch alarms that notify you when your SMS, MMS, or voice spending exceeds a certain amount. You can set up CloudWatch to deliver these notifications to you by sending them to an Amazon SNS topic.

For more information about creating alarms in CloudWatch, see [Using Amazon CloudWatch alarms](#) in the *Amazon CloudWatch User Guide*.

To create an SMS or voice spending alarm in CloudWatch

1. If you haven't already done so, create an Amazon SNS topic and subscribe an endpoint to it. The endpoint that you subscribe to the topic should be the location where you want to receive spending notifications. For example, if you want to receive spending notifications by email, subscribe your email address to the Amazon SNS topic. If you want to receive spending notifications by text message, subscribe an SMS endpoint to the topic.

For information about creating and subscribing to topics, see [Getting started with Amazon SNS](#) in the *Amazon Simple Notification Service Developer Guide*.

2. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.

3.

 **Important**

Before you create a billing alarm, you must set your AWS Region to US East (N. Virginia). Billing metric data is stored in this AWS Region and represents worldwide charges. You also must enable billing alerts for your account or in the management/payer account (if you are using consolidated billing). For more information, see [Enabling billing alerts](#).


In the navigation pane, under **Alarms**, choose **Billing**.

4. Next to **Billing alarms**, choose **Create alarm**.

5. Choose **Select metric**.

6. On the **All metrics** tab, choose **SMSVoice**, and then choose **Account Metrics**.

7. Select either **TextMessageMonthlySpend**, **MediaMessageMonthlySpend**, or **VoiceMessageMonthlySpend**.

 **Note**

The **TextMessageMonthlySpend**, **MediaMessageMonthlySpend**, and **VoiceMessageMonthlySpend** metrics don't appear until you send at least one message through Amazon Pinpoint SMS.

8. Choose the **Graphed metrics** tab, and then complete the following steps:

- Under **Statistic**, choose the statistic or predefined percentile that you want to monitor, or specify a custom percentile—for example, **p99** or **p45**.
- Under **Period**, choose the evaluation period for the alarm. When evaluating the alarm, each period is aggregated into one datapoint.

9. Choose **Select metric**. The **Specify metric and conditions** page appears, showing a graph and other information about the metric and statistic for the alarm.

10. Under **Conditions**, complete the following steps:

- For **Threshold type**, choose **Static**.
 - For **Whenever (TextMessageMonthlySpend, MediaMessageMonthlySpend, or VoiceMessageMonthlySpend) is**, specify whether you want the metric to be greater than, greater than or equal to, or equal to the threshold in order to trigger the alarm. Then, under **than**, enter the threshold value, which is the dollar amount (in US Dollars) that you want to trigger the alarm.
11. Under **Additional configuration**, complete the following steps:
 - For **Datapoints to alarm**, enter the number of evaluation periods (datapoints) during which the spending amount must exceed the threshold to trigger the alarm.
 - For **Missing data treatment**, choose **Treat missing data as ignore (maintain the alarm state)**.
 12. Choose **Next**.
 13. Under **Notification**, complete the following steps:
 - For **Whenever this alarm state is**, choose **in Alarm**.
 - For **Select an SNS topic**, choose the Amazon SNS topic that you want the alarm notification to be sent to.
 14. Choose **Next**.
 15. Enter a name and, optionally, a description for the alarm, and then choose **Next**.
 16. Under **Preview and create**, review and confirm that the alarm settings are what you want, and then choose **Create alarm**.

Logging Amazon Pinpoint SMS and voice v2 API calls using AWS CloudTrail

Amazon Pinpoint SMS is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Amazon Pinpoint SMS. CloudTrail captures all API calls for Amazon Pinpoint SMS as events. The calls captured include calls from the Amazon Pinpoint SMS console and code calls to the Amazon Pinpoint SMS and voice v2 API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Amazon Pinpoint SMS. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to Amazon Pinpoint SMS, the IP address from which

the request was made, the IAM Identity Type User who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the [AWS CloudTrail User Guide](#).

Amazon Pinpoint SMS information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in Amazon Pinpoint SMS, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see [Viewing events with CloudTrail Event history](#).

For an ongoing record of events in your AWS account, including events for Amazon Pinpoint SMS, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- [Overview for creating a trail](#)
- [CloudTrail supported services and integrations](#)
- [Configuring Amazon SNS notifications for CloudTrail](#)
- [Receiving CloudTrail log files from multiple regions](#) and [Receiving CloudTrail log files from multiple accounts](#)

All Amazon Pinpoint SMS actions are logged by CloudTrail and are documented in the [Amazon Pinpoint SMS and Voice v2 API](#). For example, calls to the `CreatePool`, `UpdatePhoneNumber` and `DescribePools` actions generate entries in the CloudTrail log files.

Every event or log entry contains information about the IAM Identity Type User that generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the [CloudTrail userIdentity element](#).

You can create a trail and store your log files in your Amazon S3 bucket for as long as you want. Also, you can define Amazon S3 lifecycle rules to archive or delete log files automatically. By default, your log files are encrypted with Amazon S3 server-side encryption (SSE).

To be notified of log file delivery, configure CloudTrail to publish Amazon SNS notifications when new log files are delivered. For more information, see [Configuring Amazon SNS notifications for CloudTrail](#).

You can also aggregate Amazon Pinpoint SMS log files from multiple AWS Regions and multiple AWS accounts into a single Amazon S3 bucket. For more information, see [Receiving CloudTrail log files from multiple regions](#) and [Receiving CloudTrail log files from multiple accounts](#).

Amazon Pinpoint SMS and Voice v2 API actions that can be logged by CloudTrail

The Amazon Pinpoint SMS and Voice v2 API supports logging the following actions as events in CloudTrail log files:

- [AssociateOriginationIdentity](#)
- [AssociateProtectConfiguraiton](#)
- [CreateConfigurationSet](#)
- [CreateEventDestination](#)
- [CreateOptOutList](#)
- [CreatePool](#)
- [CreateProtectConfiguration](#)
- [CreateRegistration](#)
- [CreateRegistrationAssociation](#)
- [CreateRegistrationAttachment](#)
- [CreateRegistrationVersion](#)
- [CreateVerifiedDestinationNumber](#)
- [DeleteAccountDefaultProtectConfiguration](#)
- [DeleteConfigurationSet](#)
- [DeleteDefaultMessageType](#)

- [DeleteDefaultSenderId](#)
- [DeleteEventDestination](#)
- [DeleteKeyword](#)
- [DeleteMediaMessageSpendLimitOverride](#)
- [DeleteOptedOutNumber](#)
- [DeleteOptOutList](#)
- [DeletePool](#)
- [DeleteProtectConfiguration](#)
- [DeleteRegistration](#)
- [DeleteRegistrationAttachment](#)
- [DeleteRegistrationFieldValue](#)
- [DeleteTextMessageSpendLimitOverride](#)
- [DeleteVerifiedDestinationNumber](#)
- [DeleteVoiceMessageSpendLimitOverride](#)
- [DescribeAccountAttributes](#)
- [DescribeAccountLimits](#)
- [DescribeConfigurationSets](#)
- [DescribeKeywords](#)
- [DescribeOptedOutNumbers](#)
- [DescribeOptOutLists](#)
- [DescribePhoneNumbers](#)
- [DescribePools](#)
- [DescribeProtectConfigurations](#)
- [DescribeRegistrationAttachments](#)
- [DescribeRegistrationFieldDefinitions](#)
- [DescribeRegistrationFieldValues](#)
- [DescribeRegistrations](#)
- [DescribeRegistrationSectionDefinitions](#)
- [DescribeRegistrationTypeDefinitions](#)
- [DescribeRegistrationVersions](#)

- [DescribeSenderIds](#)
- [DescribeSpendLimits](#)
- [DescribeVerifiedDestinationNumbers](#)
- [DisassociateOriginationIdentity](#)
- [DisassociateProtectConfiguration](#)
- [DiscardRegistrationVersion](#)
- [GetProtectConfigurationCountryRuleSet](#)
- [ListPoolOriginationIdentities](#)
- [ListRegistrationAssociations](#)
- [ListTagsForResource](#)
- [PutKeyword](#)
- [PutOptedOutNumber](#)
- [PutRegistrationFieldValue](#)
- [ReleasePhoneNumber](#)
- [ReleaseSenderId](#)
- [RequestPhoneNumber](#)
- [RequestSenderId](#)
- [SendDestinationNumberVerificationCode](#)
- [SetAccountDefaultProtectConfiguration](#)
- [SetDefaultMessageType](#)
- [SetDefaultSenderId](#)
- [SetMediaMessageSpendLimitOverride](#)
- [SetTextMessageSpendLimitOverride](#)
- [SetVoiceMessageSpendLimitOverride](#)
- [SubmitRegistrationVersion](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateEventDestination](#)
- [UpdatePhoneNumber](#)
- [UpdatePool](#)

- [UpdateProtectConfiguration](#)
- [UpdateProtectConfigurationCountryRuleSet](#)
- [UpdateSenderId](#)
- [VerifyDestinationNumber](#)

The following Amazon Pinpoint SMS and Voice version 2 API actions **aren't** logged in CloudTrail:

- [SendTextMessage](#)
- [SendVoiceMessage](#)
- [SendMediaMessage](#)

Understanding Amazon Pinpoint SMS log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the `CreateConfigurationSet` and `CreateEventDestination` action.

```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIHTRCDA62EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/SampleUser",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "SampleUser"
      },
      "eventTime": "2018-11-06T21:45:55Z",
      "eventSource": "sms-voice.amazonaws.com",
      "eventName": "CreateConfigurationSet",
      "awsRegion": "us-east-1",
```

```

    "sourceIPAddress": "192.0.0.1",
    "userAgent": "PostmanRuntime/7.3.0",
    "requestParameters": {
      "ConfigurationSetName": "MyConfigurationSet"
    },
    "responseElements": null,
    "requestID": "56dcc091-e20d-11e8-87d2-9994aexample",
    "eventID": "725843fc-8846-41f4-871a-7c52dexample",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
  },
  {
    "eventVersion": "1.05",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDAIHTRCDA62EXAMPLE",
      "arn": "arn:aws:iam::111122223333:user/SampleUser",
      "accountId": "111122223333",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName": "SampleUser"
    },
    "eventTime": "2018-11-06T21:47:08Z",
    "eventSource": "sms-voice.amazonaws.com",
    "eventName": "CreateEventDestination",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.0.1",
    "userAgent": "PostmanRuntime/7.3.0",
    "requestParameters": {
      "EventDestinationName": "CloudWatchEventDestination",
      "ConfigurationSetName": "MyConfigurationSet",
      "EventDestination": {
        "Enabled": true,
        "MatchingEventTypes": [
          "INITIATED_CALL",
          "INITIATED_CALL"
        ],
        "CloudWatchLogsDestination": {
          "IamRoleArn": "arn:aws:iam::111122223333:role/iamrole-01",
          "LogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:clientloggroup-01"
        }
      }
    }
  },

```

```
    "responseElements":null,  
    "requestID":"81de1e73-e20d-11e8-b158-d5536example",  
    "eventID":"fcafc21f-7c93-4a3f-9e72-fca2dexample",  
    "readOnly":false,  
    "eventType":"AwsApiCall",  
    "recipientAccountId":"111122223333"  
  }  
]  
}
```

Access Amazon Pinpoint SMS using an interface endpoint (AWS PrivateLink)

You can use AWS PrivateLink to create a private connection between your VPC and Amazon Pinpoint SMS. You can access Amazon Pinpoint SMS as if it were in your VPC, without the use of an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC don't need public IP addresses to access Amazon Pinpoint SMS.

You establish this private connection by creating an *interface endpoint*, powered by AWS PrivateLink. We create an endpoint network interface in each subnet that you enable for the interface endpoint. These are requester-managed network interfaces that serve as the entry point for traffic destined for Amazon Pinpoint SMS.

For more information, see [Access AWS services through AWS PrivateLink](#) in the *AWS PrivateLink Guide*.

Considerations for Amazon Pinpoint SMS

Before you set up an interface endpoint for Amazon Pinpoint SMS, review [Considerations](#) in the *AWS PrivateLink Guide*.

Amazon Pinpoint SMS supports making calls to all of its API actions through the interface endpoint.

VPC endpoint policies are not supported for Amazon Pinpoint SMS. By default, full access to Amazon Pinpoint SMS is allowed through the interface endpoint. Alternatively, you can associate a security group with the endpoint network interfaces to control traffic to Amazon Pinpoint SMS through the interface endpoint.

Create an interface endpoint for Amazon Pinpoint SMS

You can create an interface endpoint for Amazon Pinpoint SMS using either the Amazon VPC console or the AWS Command Line Interface (AWS CLI). For more information, see [Create an interface endpoint](#) in the *AWS PrivateLink Guide*.

Create an interface endpoint for Amazon Pinpoint SMS using the following service name:


```
com.amazonaws.region.pinpoint-sms-voice-v2
```

If you enable private DNS for the interface endpoint, you can make API requests to Amazon Pinpoint SMS using its default Regional DNS name. For example, `sms-voice.us-east-1.amazonaws.com`.

Create an endpoint policy for your interface endpoint

An endpoint policy is an IAM resource that you can attach to an interface endpoint. The default endpoint policy allows full access to Amazon Pinpoint SMS through the interface endpoint. To control the access allowed to Amazon Pinpoint SMS from your VPC, attach a custom endpoint policy to the interface endpoint.

An endpoint policy specifies the following information:

- The principals that can perform actions (AWS accounts, IAM users, and IAM roles).
- The actions that can be performed.
- The resources on which the actions can be performed.

For more information, see [Control access to services using endpoint policies](#) in the *AWS PrivateLink Guide*.

Example: VPC endpoint policy for Amazon Pinpoint SMS actions

The following is an example of a custom endpoint policy. When you attach this policy to your interface endpoint, it grants access to the listed Amazon Pinpoint SMS actions for all principals on all resources.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "sms-voice:SendTextMessage",
        "sms-voice:RequestPhoneNumber",
        "sms-voice>DeletePool"
      ],
      "Resource": "*"
    }
  ]
}
```

```
}  
  ]  
}
```

Quotas for Amazon Pinpoint SMS

Your AWS account has default quotas, formerly referred to as limits, for each AWS service. Unless otherwise noted, each quota is Region-specific. You can request increases for some quotas, and other quotas cannot be increased.

To request a quota increase, see [Requesting a quota increase](#).

Your AWS account has the following quotas related to Amazon Pinpoint SMS.

The following table lists the Requests Per Second (RPS) quota for each resource of the Amazon Pinpoint SMS and Voice v2 API. All Resources are eligible for a rate increase by following the directions by following the directions in [Requesting a quota increase](#).

Resource	Default quota rate (requests per second)
AssociateOriginationIdentity	1
AssociateProtectConfiguration	1
CreateConfigurationSet	1
CreateEventDestination	1
CreateOptOutList	1
CreatePool	1
CreateProtectConfiguration	1
CreateRegistration	1
CreateRegistrationAssociation	1
CreateRegistrationAttachment	1
CreateRegistrationVersion	1
CreateVerifiedDestinationNumber	1
DeleteAccountDefaultProtectConfiguration	1

Resource	Default quota rate (requests per second)
DeleteConfigurationSet	1
DeleteDefaultMessageType	1
DeleteDefaultSenderId	1
DeleteEventDestination	1
DeleteKeyword	1
DeleteMediaMessageSpendLimitOverride	1
DeleteOptedOutNumber	10
DeleteOptOutList	1
DeletePool	1
DeleteProtectConfiguration	1
DeleteRegistration	1
DeleteRegistrationAttachment	1
DeleteRegistrationFieldValue	1
DeleteTextMessageSpendLimitOverride	1
DeleteVerifiedDestinationNumber	1
DeleteVoiceMessageSpendLimitOverride	1
DescribeAccountAttributes	1
DescribeAccountLimits	1
DescribeConfigurationSets	1
DescribeKeywords	1

Resource	Default quota rate (requests per second)
DescribeOptedOutNumbers	1
DescribeOptOutLists	1
DescribePhoneNumbers	1
DescribePools	1
DescribeProtectConfiguration	1
DescribeRegistrationAttachments	1
DescribeRegistrationFieldDefinitions	1
DescribeRegistrationFieldValues	1
DescribeRegistrations	1
DescribeRegistrationSectionDefinitions	1
DescribeRegistrationTypeDefinitions	1
DescribeRegistrationVersions	1
DescribeSenderIds	1
DescribeSpendLimits	1
DescribeVerifiedDestinationNumbers	1
DisassociateOriginationIdentity	1
DisassociateProtectConfiguration	1
DiscardRegistrationVersion	1
GetProtectConfigurationCountryRuleSet	1
ListPoolOriginationIdentities	1

Resource	Default quota rate (requests per second)
ListRegistrationAssociations	1
ListTagsForResource	10
ProtectConfiguration	1
PutKeyword	1
PutOptedOutNumber	10
PutRegistrationFieldValue	1
ReleasePhoneNumber	1
ReleaseSenderId	1
RequestPhoneNumber	1
RequestSenderId	1
SendDestinationNumberVerificationCode	1
SendMediaMessage	1
SendTextMessage	1
SendVoiceMessage	1
SetAccountDefaultProtectConfiguration	1
SetDefaultMessageType	1
SetDefaultSenderId	1
SetMediaMessageSpendLimitOverride	1
SetTextMessageSpendLimitOverride	1
SetVoiceMessageSpendLimitOverride	1

Resource	Default quota rate (requests per second)
SubmitRegistrationVersion	1
TagResource	1
UntagResource	1
UpdateEventDestination	1
UpdatePhoneNumber	1
UpdateProtectConfiguration	1
UpdateProtectConfigurationCountryRuleSet	1
UpdatePool	1
UpdateSenderId	1
VerifyDestinationNumber	1

SMS and MMS quotas

The following quotas apply to the SMS and MMS channel.

Resource	Default quota	Eligible for increase
Spending threshold	USD \$1.00 per account	Yes , but spending limits vary by region. You must specify the region(s) in which you require an increase.
Number of SMS messages that can be sent each second (<i>sending rate</i>)	Varies depending on destination country and originating phone number. For more information, see Message parts per second limits in the <i>Amazon Pinpoint User Guide</i> .	Yes , however, you might need to obtain a phone number that supports higher throughput. If you're unsure of which number type to use, contact AWS Support or your

Resource	Default quota	Eligible for increase
		<p>AWS Account Manager for more information</p> <p>If you use an alphanumeric Sender ID to send messages, you might be able to increase your throughput rate. To find out if a throughput increase is available for your Sender ID, Open an Amazon Pinpoint SMS support case to request a sender ID in the Support Center Console. In your request, include your existing Sender ID, the country in which you use that Sender ID, and the throughput rate you want to request.</p>
Number of SMS and MMS messages that can be sent to a single recipient each second	1 message per second	No
Number of Amazon SNS topics for two-way SMS	100,000 per account	Yes
Number of Keywords for two-way SMS	30 Keywords per number	Yes
Number of SMS, MMS, and Voice numbers	25 per account	Yes
Number of dedicated phone numbers	25 per account	Yes

Resource	Default quota	Eligible for increase
Number of opt-out lists Note: The required Default opt-out list counts against this quota.	25 per account	Yes
Number of configuration sets	25 per account	Yes
Number of event destinations	5 per configuration set	No
Number of verified destinations on phone numbers while in SMS sandbox	10 per account	Yes
Number of phone number pools	25 per account	Yes
Number of origination identities that can be associated with a phone number pool	100 per phone number pool	Yes

10DLC quotas

The following quotas apply to SMS messages sent using 10DLC phone numbers. 10DLC numbers can only be used to send messages to recipients in the United States.

Resource	Default quota	Eligible for increase
Max 10DLC companies per AWS account	25	Yes
Max 10DLC campaigns per 10DLC brand	10	Yes

Resource	Default quota	Eligible for increase
Max 10DLC numbers per 10DLC campaign	49	No

Protect configuration quotas

The following quotas apply to protect configurations.

Resource	Default quota	Eligible for increase
Number of protect configurations	25	No

Voice quotas


The following quotas apply to the voice channel.

Note

When your account is removed from the sandbox, you automatically qualify for the maximum quotas shown in the following table.

Resource	Default quota	Eligible for increase
Number of voice messages that can be sent during a 24-hour period	If your account is in the sandbox: 20 messages	No
Number of voice messages that can be sent to a single recipient during a 24-hour period	5 messages	No

Resource	Default quota	Eligible for increase
Number of voice messages that can be sent per minute	If your account is in the sandbox: 5 calls per minute If your account is out of the sandbox: 20 calls per minute	No
Number of voice messages that can be sent from a single originating phone number per second	1 message per second	No
Voice message length	If your account is in the sandbox: 30 seconds If your account is out of the sandbox: 5 minutes	No

Resource	Default quota	Eligible for increase
Ability to send voice messages to international phone numbers	<p>If your account is in the sandbox, you can send messages to recipients in only the following countries:</p> <ul style="list-style-type: none">• Australia• Canada• Germany• Hong Kong• Israel• Japan• Mexico• Singapore• Sweden• United States• United Kingdom <p>If your account is out of the sandbox, you can send messages to recipients in any country.</p> <div data-bbox="591 1352 1029 1717"><p> Note</p><p>International calls are subject to additional fees, which vary by destination country or region.</p></div>	No

Resource	Default quota	Eligible for increase
Number of characters in a voice message	3,000 billable characters, in words that are spoken 6,000 characters total, including billable characters and SSML tags	No
Number of configuration sets	10,000 voice configuration sets	No

Requesting a quota increase

If the value in the **Eligible for Increase** column in any of the preceding tables is **Yes**, you can request an increase for that quota.

To request a quota increase

1. Open the Support Center Console at <https://console.aws.amazon.com/support/home>.
2. In the left hand navigation choose **Your support cases**.
3. Choose **Create case**.
4. Choose the **Looking for service quota increases?** link.
5. In the **Looking for service quota increases?** window choose **Create a case instead**.
6. Under **Service quota increase**, do the following:
 - For **Service**, choose **Pinpoint SMS**.
 - (Optional) For **Provide a link to the site or app which will be sending SMS messages**, provide information about the website, application, or service that will send SMS messages.
 - (Optional) For **What type of messages do you plan to send**, choose the type of message that you plan to send using your long code:
 - **One Time Password** – Messages that provide passwords that your customers use to authenticate with your website or application.
 - **Promotional** – Noncritical messages that promote your business or service, such as special offers or announcements.

- **Transactional** – Important informational messages that support customer transactions, such as order confirmations or account alerts. Transactional messages must not contain promotional or marketing content.
 - (Optional) For **Which AWS Region will you be sending messages from**, choose the AWS Region that you will be sending messages from.
 - (Optional) For **Which countries do you plan to send messages to**, enter the country or region that you want to purchase short codes in.
 - (Optional) In the **How do your customers opt to receive messages from you**, provide details about your opt-in process.
 - (Optional) In the **Please provide the message template that you plan to use to send messages to your customers** field, include the template that you will be using.
7. Under **Requests**, do one of the following:
 - For **Region**, choose your AWS Region.
 - For **Resource Type**, choose **General Limits**.
 - For **Quota**, choose the quota to change.
 - For **New quota value** enter a new value for the quota.
 - To request an increase to the same quota in an additional AWS Region, choose **Add another request**, and then choose the additional AWS Region and fill out the new request.
 8. Under **Case description**, for **Use case description**, explain why you're requesting the quota increase.
 9. Under **Contact options**, for **Preferred contact language**, choose the language that you prefer to use when communicating with the AWS Support team.
 10. For **Contact method**, choose your preferred method of communicating with the AWS Support team.
 11. Choose **Submit**.

The AWS Support team provides an initial response to your request within 24 hours.

In order to prevent our systems from being used to send unsolicited or malicious content, we have to consider each request carefully. If we're able to do so, we'll grant your request within this 24-hour period. However, if we need to obtain additional information from you, it might take longer to resolve your request.

We might not be able to grant your request if your use case doesn't align with our policies.

Document history for the Amazon Pinpoint SMS User Guide

The following table describes the documentation releases for Amazon Pinpoint SMS.

Change	Description	Date
Regional availability	Added Canada West (Calgary) to the list of supported regions. For more information, see Regional availability .	July 2, 2024
United Kingdom sender ID registration	Added a form for registering your sender ID in the United Kingdom. For more information, see Request a phone number .	June 27, 2024
Request a phone number	Requesting a phone number for the United States has been updated with a new flow for 10DLC. For more information, see Request a phone number .	June 24, 2024
Protect configuration	Use protect configurations to control which destination countries Amazon Pinpoint SMS can send your messages to. For more information, see Protect configurations .	April 30, 2024
Multimedia messaging service (MMS) support	Amazon Pinpoint SMS now supports sending multimedia messages and files from an MMS capable origination identity. For more informati	April 30, 2024

	on, see Sending an MMS message .	
Set a spend limit	You can set an Enforced and Account spend limits for SMS and voice messages. For more information, see Set a spend limit .	March 27, 2024
SMS Sandbox	You are charged for SMS verification messages after the first verification message is sent. For more information, see SMS Sandbox .	November 28, 2023
Phone numbers two-way messaging	Amazon Pinpoint SMS now supports sending two-way SMS messages to Amazon Connect for processing. For more information, see Two-way SMS messaging .	November 28, 2023
Initial release	Initial release of the Amazon Pinpoint SMS User Guide	November 16, 2023