Email Deliverability in Pardot

Salesforce, Winter '27

Last updated: July 22, 2026

© Copyright 2000–2026 Salesforce, Inc. All rights reserved. Salesforce is a registered trademark of Salesforce, Inc., as are other names and marks. Other marks appearing herein may be trademarks of their respective owners.

CONTENTS

Email Deliverability in Account Engagement 1

How Email Sending Works 1

Definitions 2

Best Practices for Email Deliverability 2

- Get Permission 3
- Keep Prospects Engaged 3
- Best Practices To Avoid Spam Filters 5
- Authenticating Account Engagement Emails 5
- Use a Dedicated Sending IP Address 6

Monitor Deliverability 7

Get Help 8

Common Deliverability Issues and Questions 8

EMAIL DELIVERABILITY IN ACCOUNT ENGAGEMENT

In email marketing, there's a lot that happens behind the scenes after you send an email and before it actually arrives in a recipient's inbox. To make sure emails reach your audience, it's important to understand how email delivery works and practice good deliverability habits. Use this guide to help you better understand email deliverability, troubleshoot delivery issues, and learn best practices for deliverability in Account Engagement.

Note: Account Engagement offers tools to help you meet your email marketing goals, but you're responsible for your sending reputation and deliverability. There's no tool that can help deliverability if you're not following best practices.

How Email Sending Works

When you send an email with Account Engagement, it undergoes a series of checks and transfers before it reaches your subscribers. A sent email isn't considered successfully delivered until it reaches the recipient's inbox.

Definitions

Review some key deliverability terms we use throughout this guide.

Best Practices for Email Deliverability

Let's review best practices for email deliverability.

Monitor Deliverability

Keep an eye on how your emails are performing using Account Engagement reporting tools so you can adjust your email marketing strategies accordingly.

Get Help

Account Engagement can't control your sending reputation or guarantee the delivery of your emails. However, we can help you understand how to manage your deliverability and answer any questions you have. If Salesforce Customer Support isn't able to help, we have a dedicated team of delivery specialists to assist you.

Common Deliverability Issues and Questions

Troubleshoot and find answers to the most common issues and questions around email deliverability.

How Email Sending Works

When you send an email with Account Engagement, it undergoes a series of checks and transfers before it reaches your subscribers. A sent email isn't considered successfully delivered until it reaches the recipient's inbox.

After you click send, Account Engagement validates your email, ensures merge fields or variable tags are properly formatted, and rewrites any tracked links. Then, the email moves from our outgoing server to the recipient's email server, such as Gmail or Outlook. At this point, the email is sent but not delivered.

EDITIONS

Available in: All Account Engagement Editions

Sent	Delivered
The email has gone through the Account Engagement sending process and is transferred over to the receiving email server	The receiving email server deems the email successful and places it in the recipient's inbox

After the email goes the receiving server, we no longer have any control over how it's treated or whether it's ultimately delivered. The receiving server conducts checks to validate the email before it's delivered to the recipient's inbox. The results of the delivery attempt appear in your email's report. For example, if the email is successfully delivered, you can review opens and click-through rate. If delivery is unsuccessful, you can see spam complaints or the reason for a soft or hard bounce.

Definitions

Review some key deliverability terms we use throughout this guide.

Deliverability
An industry term that refers to the likelihood of an email reaching subscriber inboxes. High deliverability means an email is unlikely to be sent to junk mail or blocked by spam filters.

Spam
Spam refers to irrelevant, inappropriate, or unsolicited messages often sent to a large group of people. Sending spam is against Permission-based email marketing policy.

Sender Reputation
How you're perceived by internet service providers (ISPs). Your sender reputation is impacted by things like spam complaints and how often your emails are opened by subscribers.

Authentication
Authentication refers to protocols internet service providers (ISPs) use to verify an email is legitimate and not spam. There are a few different types of email authentication that we go over that in the Best Practices section of this guide.

SEE ALSO:

Email Reputation and Deliverability Glossary

Best Practices for Email Deliverability

Let's review best practices for email deliverability.

EDITIONS

Available in: All Account Engagement Editions

Get Permission

Account Engagement maintains an email marketing policy that's permission based. That means that you can only send to prospects who have expressly opted in to receive marketing emails from you. Permission-based email marketing is a baseline best practice and it's vital to achieving good deliverability. Use tools like Account Engagement forms and landing pages to allow prospects to opt in to marketing emails. You can also set up custom email preference center pages to allow prospects to manage their list subscriptions.

Keep Prospects Engaged

The best thing you can do for your deliverability is maintain a permission-based list of engaged subscribers. Engagement means subscribers are actively opening and clicking your emails. Internet service providers (ISPs) monitor for activity, so if your marketing emails are consistently left unopened, they start treating them as spam.

Best Practices To Avoid Spam Filters

Some spam filters evaluate your email's subject and body text when determining whether a message is spam. To keep your emails from triggering spam filters, here are some best practices.

Authenticating Account Engagement Emails

To help you achieve good email deliverability, Account Engagement requires that you verify ownership for each sending domain. Sender Policy Framework (SPF) authentication is configured for you by default. We recommend that you also set up these additional authentication methods: DomainKeys Identified Mail (DKIM) and Domain-Based Message Authentication, Reporting, and Conformance (DMARC).

Use a Dedicated Sending IP Address

A dedicated sending IP address gives you full control of your email sending, so you're fully responsible for the reputation of your own IP address.

Get Permission

Account Engagement maintains an email marketing policy that's permission based. That means that you can only send to prospects who have expressly opted in to receive marketing emails from you. Permission-based email marketing is a baseline best practice and it's vital to achieving good deliverability. Use tools like Account Engagement forms and landing pages to allow prospects to opt in to marketing emails. You can also set up custom email preference center pages to allow prospects to manage their list subscriptions.

SEE ALSO:

Create a Custom Email Preference Center Page

Salesforce Help: Set Up a Confirmed Opt-In Process in Account Engagement

Account Engagement's Permission-Based Email Marketing Policy

Keep Prospects Engaged

The best thing you can do for your deliverability is maintain a permission-based list of engaged subscribers. Engagement means subscribers are actively opening and clicking your emails. Internet service providers (ISPs) monitor for activity, so if your marketing emails are consistently left unopened, they start treating them as spam.

Account Engagement includes tools to help you identify and suppress unengaged prospects who could harm your sending reputation.

Create a Dynamic Suppression List

To prevent your customers from experiencing marketing fatigue, space out the timing of your emails with a suppression list. Create a dynamic list with a rule type that filters based on the recency and frequency of email sends.

Identify and Suppress Unengaged Prospects

Keep your deliverability high by practicing good list management and not emailing unengaged prospects. Use a dynamic list to suppress an unengaged prospect from receiving marketing emails.

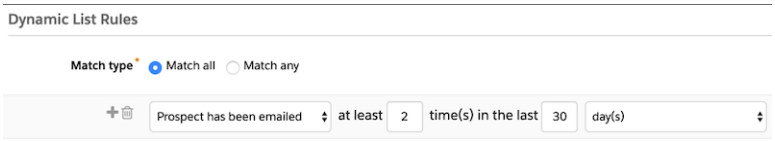
Create a Dynamic Suppression List

To prevent your customers from experiencing marketing fatigue, space out the timing of your emails with a suppression list. Create a dynamic list with a rule type that filters based on the recency and frequency of email sends.

During the setup for a dynamic list, you choose which rules to match prospects against. To use the dynamic list as a suppression list, select the **Prospect has been emailed** rule. Enter the number of sends and the time frame, and run the rule. Include the dynamic suppression list when you send marketing emails and to remove prospects who meet the criteria you set.

EDITIONS

Available in: All Account Engagement Editions



Keep these considerations in mind when you use the Prospect Has Been Emailed rule.

- The rule considers list emails and email sent from Engagement Studio only.
- We recommend that you wait about 10 minutes between email sends. Allow time for the system to process an email send and mark a prospect accurately.
- Times are based on the default time zone for your business unit.
- Account Engagement evaluates time-based rules every 24 hours at midnight. For example, a rule removes a prospect when they haven't opened an email in 30 days. If a prospect meets the 30-day criteria at 9:00 AM on Monday, they remain on the list until the next evaluation at midnight.
- When you use the suppression list in an engagement program, suppressed prospects pause at the step they're on. When the time period is up, they resume the program and start receiving the paused emails.
- When multiple prospects have the same email address, the rule counts all list emails sent to prospects with that email address. For example, Prospect A and Prospect B have the same email address. You sent each prospect two emails in the last three days. The rule type counts four emails sent in the last three days.

Identify and Suppress Unengaged Prospects

Keep your deliverability high by practicing good list management and not emailing unengaged prospects. Use a dynamic list to suppress an unengaged prospect from receiving marketing emails.

Before you begin, define what an unengaged prospect looks like to your organization. Here are a few ideas to get you started.

- Have you sent 20 daily emails with no prospect activity?
- Have you sent six weekly emails with no prospect activity?
- Have you sent six monthly emails with no prospect activity?

1. Create a list.
2. Select **Dynamic List**.
3. Click **Set Rules**.
4. For Match Type, select **Match All**.
5. Add a rule, and select **Prospect has been emailed**.
6. Enter the time details for the rule.
7. Add a rule, and select **Prospect time**.
   a. From the first dropdown, select **last activity days ago**.
   b. From the second dropdown, select **is greater than**.
   c. Enter the number of days.
8. Save the list.

The list populates with unengaged prospects. Use the list as a suppression list for your email sends. If a prospect becomes active again, they're removed from the list.

EDITIONS

Available in: All Account Engagement Editions

USER PERMISSIONS

To create a dynamic list:
- Account Engagement Administrator or Marketing role

Best Practices To Avoid Spam Filters

Some spam filters evaluate your email's subject and body text when determining whether a message is spam. To keep your emails from triggering spam filters, here are some best practices.

EDITIONS

Available in: All Account Engagement Editions

Avoid Interactive Content

Some kinds of interactive content can cause your emails to be marked as spam. Including the following in your email code sometimes triggers spam filters:

- JavaScript
- RSS feeds
- Forms

Keep Your Code Clean

Copying HTML from a word processor, such as Microsoft Word, into Account Engagement adds style tags and other code that can cause rendering issues. When copying HTML content, first paste it into a text editor, such as Notepad, and remove all formatting. To add formatting back, copy the unformatted text into the editor in Account Engagement.

Keep the Image-to-Text Ratio Low

Too many images or too large of an image compared to the amount of text in an HTML email can make your message look like spam to a filter. Adding more text and reducing the number and size of images can help.

Some email clients block images by default, so your recipients don't see the images automatically. Include alt tags that describe your images in case they don't load for the recipient.

Be Careful with Links

Avoid using URL shorteners in your emails. Spammers frequently abuse them, and some shortened domains have been placed on widely used block lists. Many spam filters block emails that contain shortened links from shortened domains.

Most spam filters consider emails with links to several domains spammy, so limit the number of different domains that you link to in an email.

Include the Physical Address and a Way to Opt Out

Marketing emails must contain two things: your physical address and a way for recipients to opt out of future emails. If your marketing emails are missing an unsubscribe or email preference center link or a physical address, they can trigger spam filters. However, email templates include an unsubscribe link in the footer, so don't worry about adding this information.

Authenticating Account Engagement Emails

To help you achieve good email deliverability, Account Engagement requires that you verify ownership for each sending domain. Sender Policy Framework (SPF) authentication is configured for you by default. We recommend that you also set up these additional authentication methods: DomainKeys Identified Mail (DKIM) and Domain-Based Message Authentication, Reporting, and Conformance (DMARC).

Validation Key

In Account Engagement, you can only send from domains that you own. For each sending domain that you add, Account Engagement generates a validation key to add to your DNS configuration. The key verifies ownership and validates your domain for email sending.

Sender Policy Framework (SPF)

SPF is a form of email authentication that makes forging the sender of an email, or email spoofing, more difficult. SPF isn't aimed at stopping spammers. Rather, it tightens loopholes used by spammers to spoof emails. SPF provides a list of all outbound email sources for a domain as a DNS TXT record. Emails you send through Account Engagement pass SPF automatically. As a best practice, we still recommend including an SPF record for your domain in your DNS configuration.

When a receiving mail server gets a message appearing to be sent from a certain domain, it checks the sender's SPF statement to verify that information.

DomainKeys Identified Mail (DKIM)

DKIM is a common email authentication system that adds another layer of verifying ownership with DNS records. We recommend setting up DKIM because ISPs have strict security policies to prevent spam.

Domain-Based Message Authentication, Reporting, and Conformance (DMARC)

With DMARC, you notify receiving servers that your messages use SPF and DKIM and instruct them on what to do if those checks fail. Work with your IT team to set up DMARC in your DNS configuration.

SEE ALSO:

- Add and Verify a Domain for Email Sending
- Implement DKIM Authentication for Account Engagement Email
- *Knowledge Article*: DMARC Support

Use a Dedicated Sending IP Address

A dedicated sending IP address gives you full control of your email sending, so you're fully responsible for the reputation of your own IP address.

We recommend a dedicated IP if you send over 100,000 emails per month. If you send over 250,000 emails per month, a dedicated IP is required. Shared IP addresses are best for lower-volume or inconsistent senders.

A dedicated sending IP offers some benefits for high-volume senders.

- A dedicated IP address gives you more control over your sending reputation. On a shared IP address, you're affected by the sending practices of everyone on the address.
- In industries with heightened security, like banking and defense, a dedicated sending IP address is more likely to be allowlisted than a shared address. When your sending IP address is allowlisted, your emails are more likely to stay out of the spam folder.

EDITIONS

Available in: Account Engagement **Advanced** and **Premium** Editions

Available for an additional cost in: Account Engagement **Plus** Edition

Warming a Dedicated IP Address

New IP addresses are considered "cold" until they've established an email sending reputation. Mail servers tend to treat messages that are coming from a cold IP address as spam. IP warming is a process that helps you establish a reputation as a legitimate email sender. It's best to start small and gradually send to larger volumes of prospects. IP warming gives receiving servers time to observe your sending patterns and behavior and builds a solid sending reputation.

Warming a Dedicated IP Address

New IP addresses are considered "cold" until they've established an email sending reputation. Mail servers tend to treat messages that are coming from a cold IP address as spam. IP warming is a process that helps you establish a reputation as a legitimate email sender. It's best to start small and gradually send to larger volumes of prospects. IP warming gives receiving servers time to observe your sending patterns and behavior and builds a solid sending reputation.

EDITIONS

Available in: Account Engagement **Advanced** and **Premium** Editions

Available for an additional cost in: Account Engagement **Plus** Edition

Getting Started with a Dedicated IP Address

Before you can start warming your IP address, make sure you take care of these prerequisites.

- To make sure that your users can receive test emails, allowlist your new sending IP on your corporate receiving server.
- Segment out your best and most active contacts. Don't start your IP warming with old lists! Having high delivery rates with your initial campaigns helps build your IP's sending reputation.

Warming the IP Address

The key to warming your IP address is to spread out your email sends over multiple days. For example, if you plan to send 200,000 emails a week, split your lists into 20 sublists. Don't include more than 10,000 recipients in each list. Email only one sublist per day over the first few days. A consistent mail volume day-to-day is better than a large volume spike on one day of the week and no email sent on remaining days of the week.

A good rule for larger ramp-ups is to start with 10,000 prospects per day. If your bounce rate stays below 10% and your spam complaint rate stays below 0.1%, double your sending per day over the next few weeks. Continue this rate until you reach your desired sending volume.

This example shows how to ramp up to sending 200,000 emails a week.

Week	Emails Per Day	Total Per Week
Week 1	10k per day x 4 days	40k
Week 2	20k per day x 5 days	100k
Week 3	40k per day x 5 days	200k
Week 4	50k/day x 4 days	200k

Monitor Deliverability

Keep an eye on how your emails are performing using Account Engagement reporting tools so you can adjust your email marketing strategies accordingly.

There are also third-party tools available on the web where you can check your sender score and find out if you are on any known blocklists. If you do find your IP on a public blocklist, Salesforce Customer Support can usually help resolve the issue. If you are on a private blocklist for a specific organization, work directly with that organization's IT team to determine next steps.

SEE ALSO:

- Account Engagement Campaign Reporting
- List Email Report

Get Help

Account Engagement can't control your sending reputation or guarantee the delivery of your emails. However, we can help you understand how to manage your deliverability and answer any questions you have. If Salesforce Customer Support isn't able to help, we have a dedicated team of delivery specialists to assist you.

Contact Salesforce Customer Support

Common Deliverability Issues and Questions

Troubleshoot and find answers to the most common issues and questions around email deliverability.

EDITIONS

Available in: All Account Engagement Editions

Your internal tests are going to spam.

When you send an email from your company domain to your company domain but from an unfamiliar IP address, it can flag spam filters. To avoid this problem, allowlist your business unit's sending IP and remove it from any other spam or security filters that you have in place.

Your emails go to spam when sent from Account Engagement but not Gmail.

Gmail is built for individual, or 1:1, email sends while Account Engagement is a marketing platform. These classifications play a critical role in how email servers consider emails that come from each. To help stop malicious spam, spam filters take a closer look at emails sent through bulk email services like Account Engagement.

To help prevent your emails from being marked as spam, ask your prospects to allowlist your sending IP, just as you did internally. Add a line of text to your emails that explains what to do if they don't want to miss your emails. For example: "Sometimes email providers like Gmail or Yahoo! don't deliver marketing emails because they mistake them for spam. To avoid this problem, please add [sender email address] to your list of preferred senders."

Locate email bounce codes

Navigate to the email report in your business unit and click the number of soft or hard bounces. Bounce codes are generated by the recipient's email server. Account Engagement translates the more common bounce codes, but you can find more information with a quick web search.

Confirm that your domain validation key is correct. If you use DomainKeys Identified Mail (DKIM) authentication, confirm that your DomainKey entry is correct.

In standalone Account Engagement, go to **Admin** > **Domain Management**. In the Lightning App, go to **Account Engagement** > **Domain Management**. If everything is verified and working correctly, each column shows green checkmarks. If you generated a DomainKey outside of Account Engagement or your TXT entry was added in the last 24 hours, it's possible that the checkmarks don't appear.

You can also send a test email to yourself and inspect the email headers to diagnose the problem. A successful email has a PASS value under SPF and DKIM. Depending on your email client, the location of headers and the way they look can be different. If it doesn't pass, make sure that you're using your business unit's sending IP and that the domain matches your Domain Management page.

If the email shows both PASS values but still goes to spam, contact Salesforce Customer Support for further investigation.

Your emails are being placed in Gmail's Promotional tab.

Account Engagement doesn't have control over which tab Gmail chooses for your email. Keep in mind that the Promotional tab is still your recipient's inbox. In fact, it can actually reduce the number of spam complaints and opt-outs. When recipients know that they're looking at a marketing email, they're sometimes more likely to react positively.