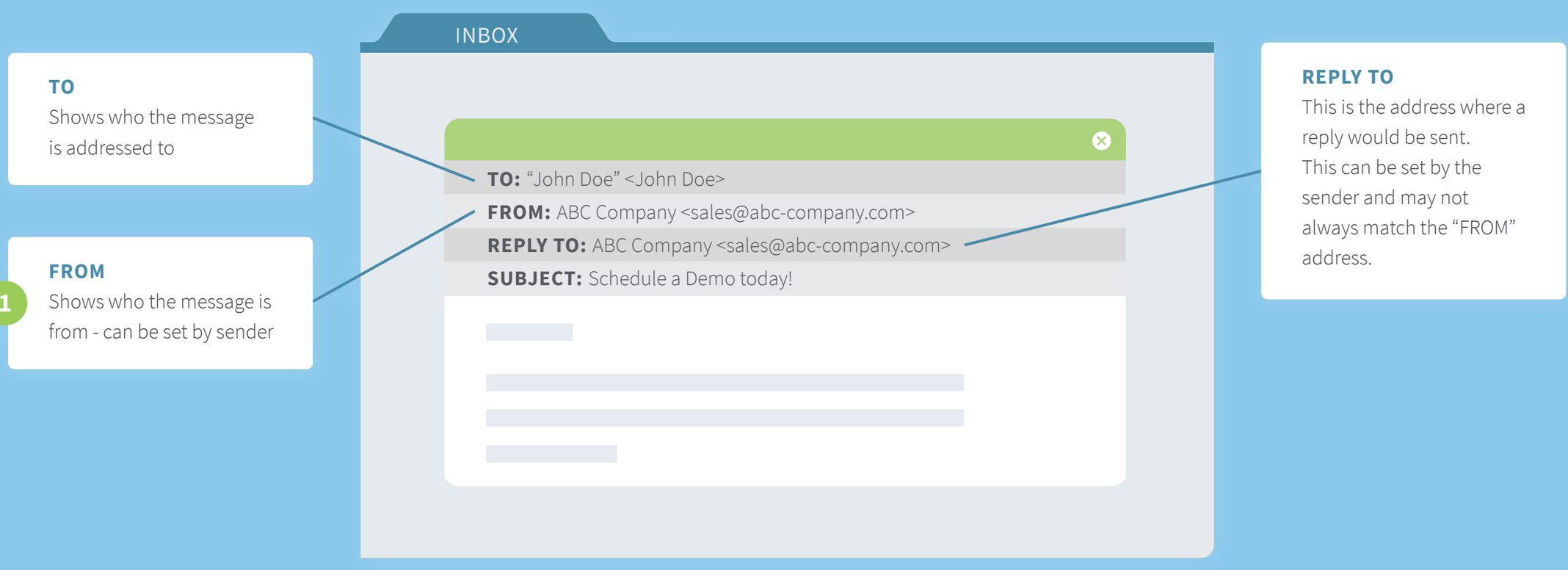
What is an Envelope Domain

Anatomy of an Email

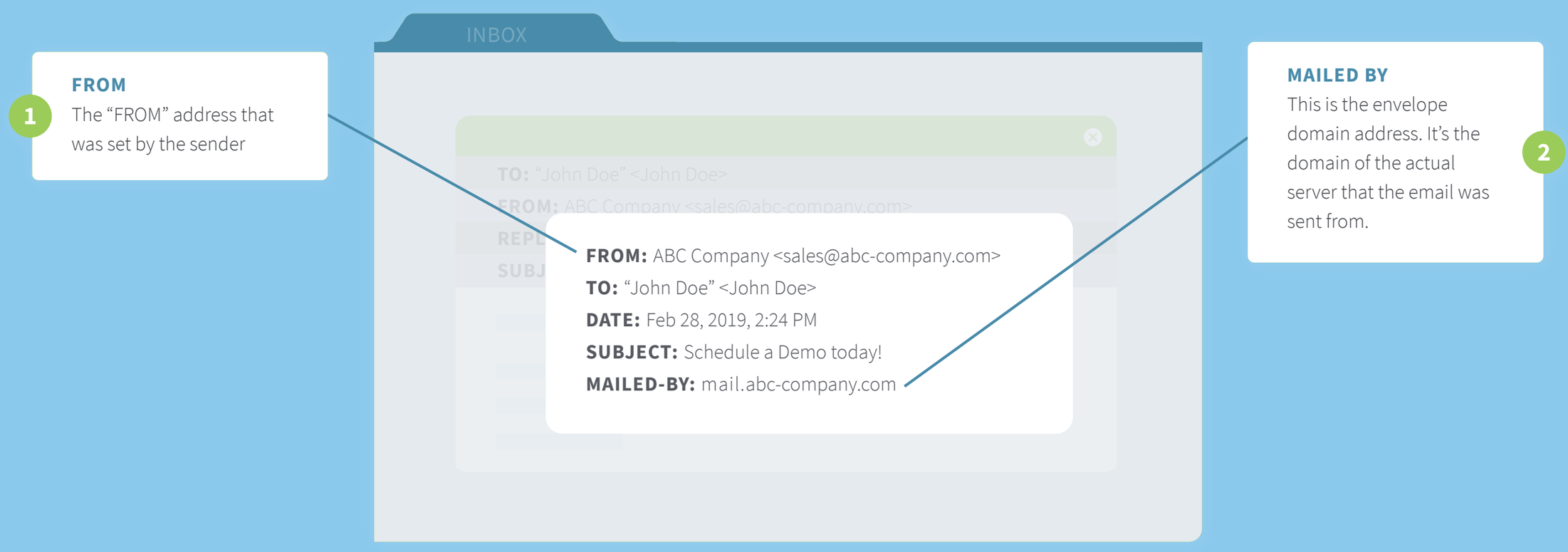
Emails contain two “from” addresses:

1. The address shown in the “FROM’ field of an email, which is visible to all email users
2. The **envelope domain address** that is hidden in the header of an email

VISIBLE TO EMAIL USERS



VISIBLE IN EMAIL HEADER



Envelope Domain Setup

When Act-On sends emails on behalf of your company, a default “mailed-by” address of ***b2b-mail.com*** is used.

For maximum deliverability, this default envelope domain should be changed to a sub-domain of your company address.

FROM: ABC Company <sales@abc-company.com>
TO: “John Doe” <John Doe>
DATE: Feb 28, 2019, 2:24 PM
SUBJECT: Schedule a Demo today!
MAILED-BY: ***b2b-mail.com***

FROM: ABC Company <sales@abc-company.com>
TO: “John Doe” <John Doe>
DATE: Feb 28, 2019, 2:24 PM
SUBJECT: Schedule a Demo today!
MAILED-BY: ***mail.abc-company.com***

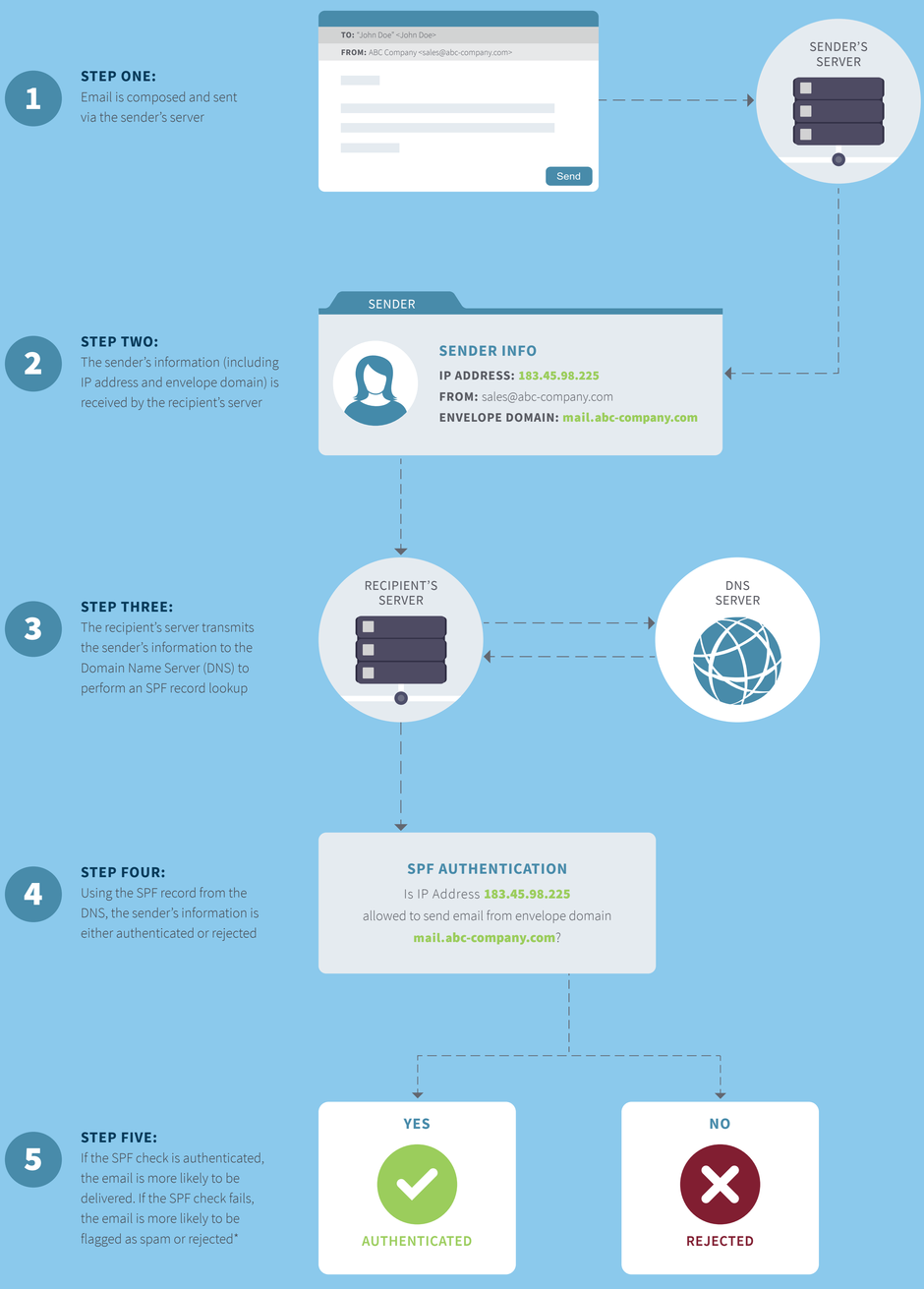
Setting up your company’s envelope domain is important for building and maintaining your company’s email reputation. If left as the default, ISPs like Google will use the reputation of ***b2b-mail.com*** to determine deliverability. If you have multiple domains, choose the one with the healthiest email reputation to set as your envelope domain.

What is SPF

Sender Policy Framework (SPF)

A Sender Policy Framework (SPF) is an email authentication system that allows the owner of a domain to specify which mail servers they use to send mail. SPF adds a layer of security to your emails by validating that the message is being sent from a legitimate source.

HERE'S HOW SPF WORKS



SPF Setup for Envelope Domain

You must enable Sender Policy Framework (SPF) for your envelope domain to let Act-On send emails on your behalf.

Work with your mail or IT team to:

1. Create the sub-domain (eg., mailer.company.com) for your email envelope
2. Create two new records under the DNS of this sub-domain:

Text record:	**MX record:**
v=spf1 include:_spf.act-on.net -all	est-mta.b2b-mail.net (priority 10)

3. Continue the steps outlined in our Required Technical Setup article

While SPF is required on your envelope domain, you can also add SPF to your primary "FROM" address domain. You can do this by following the instructions under the **"Email From Setup"** section on the Required Technical Setup page.

**SPF authentication does not guarantee inbox deliverability.*

For more information on how to maximize email deliverability, download our eBook series: Deliverability 101.

act-on

What is DKIM

DomainKeys Identified Mail (DKIM)

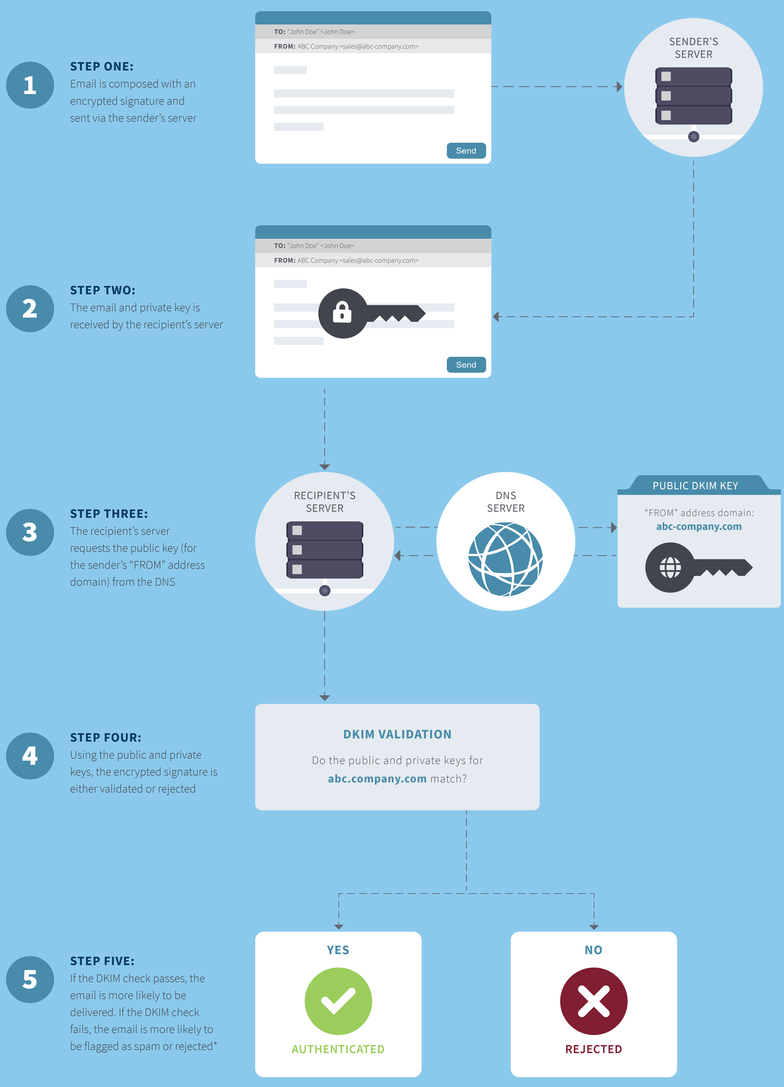
DomainKeys Identified Mail (DKIM) is a system that helps authenticate your emails. Much like SPF, DKIM is an authentication framework that tells the world that it is really you sending a given email message. DKIM does this by allowing users to add encrypted signatures to parts of emails. The encrypted signature generates a set of two keys:

PRIVATE KEY
This key is kept secret and can only be accessed by the sender. The private key is used to create the encrypted signature in the outgoing email.

PUBLIC KEY
This is published to the DNS server for ISPs to access. The public key is used to verify the encrypted signature when the email is delivered.

DKIM can combat spoofing or phishing techniques by proving that the mail server the email claims to be sent from is in fact the server that sent the email. Without DKIM, your messages will automatically be flagged as suspicious and may not be delivered to your recipients.

HERE'S HOW DKIM WORKS

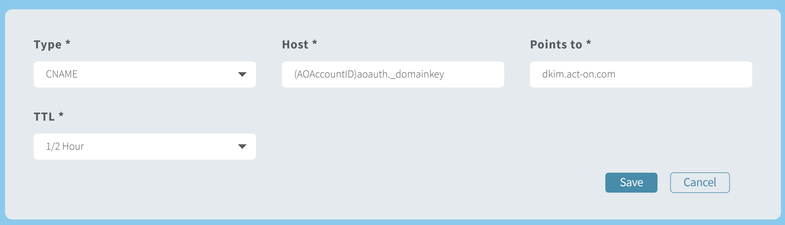


DKIM Setup for Email

You must enable DKIM for each email "FROM" domain (not on the envelope domain) to let Act-On use it as From label on your messages.

Work with your mail or IT team to:

1. Gather the list of domains you are using for your From addresses
2. From the Start page in Act-On, locate your Account ID (in the Account section, next to your Account Name)
3. For each domain create a new CNAME entry in your DNS:
   - Name or Host: (AOAccountID)aoauth._domainkey
   - Value or Points To: dkim.act-on.com



   - See Editing Your DNS to Implement DKIM for detailed steps to create this entry
   - For multiple accounts: Please use your parent account's ID for the CNAME entry on all child accounts
4. Continue the steps outlined in our Required Technical Setup article

**DKIM authentication does not guarantee inbox deliverability.*

For more information on how to maximize email deliverability, download our eBook series: Deliverability 101.

act-on