OSTENDO

One system . **Complete** operations

Ostendo
Continuum Edition

Amazon Simple Email Service

(SES) Integration Setup Guide

21/01/2026

Revision 1.0.0

Table Of Contents

1. Introduction to Amazon SES

Amazon Simple Email Service (SES) is a cloud-based email sending service designed for sending transactional emails, marketing messages, and other types of high-quality content to customers.

Key Features

- **Cost-effective:** Pay only for what you use with no upfront costs
- **Scalable:** Send millions of emails per day
- **High deliverability:** Built on Amazon's reliable infrastructure
- **Authentication:** Full support for SPF, DKIM, and DMARC
- **Analytics:** Track deliveries, opens, clicks, bounces, and complaints

Use Cases

- Transactional emails (order confirmations, password resets, notifications)
- Marketing campaigns and newsletters
- Automated system notifications and alerts
- Bulk email delivery

Pricing Overview

SES pricing is based on the number of emails sent. As of the time of writing:

Item	Cost (USD)
First 62,000 emails/month (from EC2)	Free
Emails sent	$0.10 per 1,000 emails
Attachments	$0.12 per GB

> ***Note**:* Check the AWS SES pricing page for current rates as these may change.

2. Understanding the SES Sandbox

All new SES accounts start in **sandbox mode**. This is a restricted environment designed to prevent abuse and help you test your setup before sending to real customers.

Sandbox Restrictions

Restriction	Details
Recipient addresses	Can only send to verified email addresses
Sending quota	Maximum 200 emails per 24-hour period
Sending rate	Maximum 1 email per second
From address	Must use verified email or domain

Verifying Email Addresses for Testing

While in the sandbox, you must verify each recipient email address:

1. Go to SES Console → Verified Identities
2. Click Create Identity
3. Select "Email address"
4. Enter the email address and click Create
5. The recipient must click the verification link in the email they receive

> **Tip**: Verifying a domain (covered in Section 4) allows you to send FROM any address on that domain without individual email verification. However, in sandbox mode you still need to verify recipient addresses.

3. Setting Up SES

3.1 Accessing the SES Console

1. Sign in to the AWS Management Console at https://console.aws.amazon.com
2. Search for "SES" or "Simple Email Service" in the search bar
3. Click on "Amazon Simple Email Service"

3.2 Selecting a Region

SES is available in multiple AWS regions. Choose a region based on:

- **Proximity:** Choose a region close to your application servers
- **Data residency:** Consider regulatory requirements for email data
- **Feature availability:** Some features may vary by region

Available Regions

Region Name	Region Code
US East (N. Virginia)	us-east-1
US West (Oregon)	us-west-2
EU (Ireland)	eu-west-1
EU (Frankfurt)	eu-central-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Singapore)	ap-southeast-1

> **Important:** **SES settings are region-specific. Verified identities, sending limits, and configuration sets do not transfer between regions. If you change regions, you must set up everything again.**

4. Domain Verification and Authentication

Verifying your domain in SES allows you to send emails from any address on that domain and enables proper email authentication.

4.1 Why Domain Verification Matters

- Send from any address on the domain (e.g., noreply@, support@, sales@)
- Enable DKIM signing with your domain (critical for deliverability)
- Prove ownership to receiving mail servers
- Prevent emails being flagged as phishing or spam

4.2 Creating a Domain Identity

1. In the SES Console, go to **Verified Identities**
2. Click **Create Identity**
3. Select **Domain** as the identity type
4. Enter your domain name (e.g., yourdomain.com)

Optional Settings

Setting	Recommendation
Assign a default configuration set	Skip for now - can be added later for tracking
Assign to a tenant	Skip - only needed for multi-tenant architectures
Use a custom MAIL FROM domain	Optional - provides full SPF alignment

DKIM Settings (Critical)

Setting	Value
Easy DKIM	Enabled (use this option)
DKIM signing key length	2048-bit (recommended for security)
DKIM signatures	Enabled
Publish DNS records to Route 53	Only if your domain uses Route 53 for DNS

5. Click Create Identity

SES will generate the DNS records you need to add to your domain's DNS configuration.

5. Configuring DNS Records

After creating a domain identity, you must add several DNS records to your domain. These records enable domain verification and email authentication.

5.1 Domain Verification (TXT Record)

This record proves you own the domain:

Type	Name/Host	Value
TXT	_amazonses	[verification string from SES]

5.2 DKIM Records (3 CNAME Records)

These records enable DKIM signing with your domain. SES provides 3 CNAME records:

Type	Name/Host	Value/Points To
CNAME	[token1]._domainkey	[token1].dkim.amazonses.com
CNAME	[token2]._domainkey	[token2].dkim.amazonses.com
CNAME	[token3]._domainkey	[token3].dkim.amazonses.com

> **DNS Provider Note:** Most DNS providers auto-append your domain name. If SES shows abc123._domainkey.yourdomain.com, enter only abc123._domainkey in the Name field.

5.3 SPF Record (TXT Record)

SPF specifies which servers can send email for your domain:

New SPF Record

If you have no existing SPF record:

Type	Name	Value
TXT	@	v=spf1 include:amazonses.com ~all

Existing SPF Record

If you already have an SPF record, add include:amazonses.com to it:

Before: v=spf1 include:_spf.google.com ~all

After: v=spf1 include:_spf.google.com include:amazonses.com ~all

> **Warning**: You can only have ONE SPF record per domain. Multiple SPF records will cause authentication failures. Always edit the existing record rather than creating a new one.

5.4 DMARC Record (TXT Record)

DMARC tells receiving servers how to handle authentication failures:

Type	Name	Value
TXT	_dmarc	v=DMARC1; p=none;

DMARC Policy Options

Policy	Behaviour
p=none	Monitor only - recommended for initial setup and testing
p=quarantine	Send failing emails to spam/junk folder
p=reject	Reject/block emails that fail authentication completely

> **Recommendation:** Start with p=none while testing. Once you confirm all legitimate emails pass authentication, gradually move to p=quarantine and eventually p=reject for maximum protection against domain spoofing.

5.5 Verifying DNS Configuration

After adding DNS records, verify the configuration:

In SES Console

1. Go to Verified Identities → click your domain
2. Check "Identity status" shows **Verified**
3. Check "DKIM configuration" shows **Successful**

Online Tools

- **SPF:** https://mxtoolbox.com/spf.aspx
- **DKIM:** https://mxtoolbox.com/dkim.aspx
- **DMARC:** https://mxtoolbox.com/dmarc.aspx

DNS propagation typically takes 5-10 minutes but can take up to 72 hours.

6. IAM Credentials for API Access

To send emails programmatically via the SES API, you need AWS credentials with appropriate permissions.

6.1 Creating an IAM User

1. Go to the IAM Console (search "IAM" in AWS Console)
2. Click **Users** → **Create user**
3. Enter a username (e.g., ses-sender)
4. Click **Next**
5. Select **Attach policies directly**
6. Search for and select AmazonSESFullAccess
7. Click **Next** → **Create user**

6.2 Creating Access Keys

1. Click on the user you just created
2. Go to **Security credentials** tab
3. Scroll to "Access keys" → click **Create access key**
4. Select "Application running outside AWS"
5. Click **Create access key**
6. **Save the Access Key ID and Secret Access Key immediately**

> **Critical:** The Secret Access Key is only shown once. Save it securely before closing the page. If lost, you must create new credentials.

6.3 Minimal Permission Policy (Recommended)

For better security, create a custom policy with only the required permissions:

```
{
  "Version": "2012-10-17",

  "Statement": [{

    "Effect": "Allow",

    "Action": [

      "ses:SendEmail",

      "ses:SendRawEmail"

    ],
    "Resource": "*"

  }]

}
```

7. Sending Emails via the API

SES provides multiple methods for sending emails programmatically.

7.1 API Endpoints

Use the appropriate endpoint for your AWS region:

Region	Endpoint
US East (N. Virginia)	email.us-east-1.amazonaws.com
US West (Oregon)	email.us-west-2.amazonaws.com
EU (Ireland)	email.eu-west-1.amazonaws.com
Asia Pacific (Sydney)	email.ap-southeast-2.amazonaws.com

7.2 Sending Methods

Method	Use Case
SendEmail	Simple emails - SES constructs the message from parameters
SendRawEmail	Full control - you provide the complete MIME message (attachments, custom headers)
SendTemplatedEmail	Personalised emails using SES templates
SendBulkTemplatedEmail	Bulk sending with templates to multiple recipients

7.3 Required Parameters

When calling the SES API, you'll need:

Parameter	Description
Source (From)	The verified email address or domain to send from
Destination (To)	Recipient email addresses (To, CC, BCC)
Subject	Email subject line
Body	Email content (HTML and/or plain text)

7.4 AWS SDK Integration

AWS provides SDKs for most programming languages. Configure credentials using:

- **Environment variables:** AWS_ACCESS_KEY_ID, AWS_SECRET_ACCESS_KEY
- **Credentials file:** ~/.aws/credentials
- **IAM roles:** When running on AWS infrastructure (EC2, Lambda)
- **Direct configuration:** Pass credentials in code (least recommended)

8. Configuration Sets and Event Tracking

Configuration sets allow you to track email events and apply sending rules.

8.1 What Configuration Sets Track

Event	Description
Send	Email was accepted by SES for delivery
Delivery	Email was successfully delivered to the recipient's mail server
Bounce	Email could not be delivered (hard or soft bounce)
Complaint	Recipient marked the email as spam
Reject	SES rejected the email (virus, spam content)
Open	Recipient opened the email (requires tracking pixel)
Click	Recipient clicked a link (requires link wrapping)

8.2 Creating a Configuration Set

1. Go to SES Console → Configuration sets
2. Click **Create set**
3. Enter a name (e.g., production-tracking)
4. Configure sending options as needed
5. Click **Create set**

8.3 Event Destinations

Events can be sent to various AWS services:

- **Amazon SNS:** Real-time notifications, webhooks
- **Amazon CloudWatch:** Metrics and dashboards
- **Amazon Kinesis Firehose:** Stream to S3, Redshift, or other destinations
- **Amazon EventBridge:** Event-driven workflows

9. Handling Bounces and Complaints

Properly handling bounces and complaints is critical for maintaining your sending reputation.

9.1 Types of Bounces

Type	Description
Hard Bounce	Permanent failure - address doesn't exist, domain invalid. Remove immediately.
Soft Bounce	Temporary failure - mailbox full, server unavailable. May retry.
Transient	Temporary issue - can retry after some time

9.2 Required Actions

Event	Action Required
Hard Bounce	Immediately remove address from your list. Never send again.
Complaint	Remove address and investigate. Review email content and targeting.
Soft Bounce	Retry with exponential backoff. Remove after repeated failures.

9.3 Setting Up Notifications

Configure SNS topics to receive bounce and complaint notifications:

1. Create an SNS topic for bounces and one for complaints
2. In SES, go to Verified Identities → your domain
3. Under Notifications, configure Bounce and Complaint feedback
4. Select your SNS topics
5. Subscribe your application endpoint to the SNS topics

> **Critical:** AWS requires you to handle bounces and complaints. Failure to do so can result in your SES account being suspended.

10. Requesting Production Access

To send emails to non-verified recipients, you must request production access (leave the sandbox).

10.1 Prerequisites

Before requesting production access, ensure you have:

- Verified at least one domain with DKIM enabled
- Set up bounce and complaint handling
- Tested sending within the sandbox successfully
- A legitimate use case for sending email

10.2 Submitting the Request

1. In SES Console, go to **Account dashboard**
2. Find "Request production access" and click **Request production access**
3. Select your mail type (Transactional, Marketing, or Both)
4. Enter your website URL
5. Provide a detailed use case description
6. Explain how you handle bounces and complaints
7. Submit the request

10.3 Use Case Description Tips

AWS reviews each request manually. Include:

- What type of emails you'll send (transactional, notifications, etc.)
- How recipients opt-in to receive emails
- How you maintain your mailing list
- Your process for handling unsubscribes
- How you process bounces and complaints

Requests are typically reviewed within 24 hours. If denied, you'll receive feedback on what to address.

11. Monitoring and Reputation

11.1 Account Dashboard

The SES Account Dashboard shows your current sending status and metrics:

- **Account status:** Sandbox or Production
- **Daily sending quota:** Maximum emails per 24 hours
- **Maximum send rate:** Emails per second
- **Emails sent:** Count for current period

11.2 Reputation Metrics

SES tracks your sending reputation. Keep these metrics healthy:

Metric	Target	Risk If Exceeded
Bounce Rate	< 5%	Account suspension, deliverability issues
Complaint Rate	< 0.1%	Account suspension, reputation damage

11.3 CloudWatch Metrics

SES publishes metrics to CloudWatch. Key metrics to monitor:

- **Send** - Total send attempts
- **Delivery** - Successful deliveries
- **Bounce** - Failed deliveries
- **Complaint** - Spam reports
- **Reputation.BounceRate** - Current bounce percentage
- **Reputation.ComplaintRate** - Current complaint percentage

12. Best Practices

12.1 Email Authentication

- Always verify domains rather than individual email addresses
- Enable Easy DKIM with 2048-bit keys
- Configure SPF, DKIM, and DMARC for all sending domains
- Test authentication using email header analysis

12.2 List Management

- Use confirmed opt-in (double opt-in) where possible
- Remove hard bounces immediately - never retry
- Honor unsubscribe requests promptly
- Regularly clean inactive addresses from your lists
- Never purchase email lists

12.3 Content Guidelines

- Use a consistent, recognizable From name and address
- Write clear, descriptive subject lines
- Include both HTML and plain text versions
- Avoid spam trigger words ("FREE!", "Act Now!", etc.)
- Ensure links match their display text (no misleading URLs)
- Include a physical mailing address (required by CAN-SPAM)

12.4 Security

- Use IAM roles when running on AWS infrastructure
- Apply least-privilege permissions to IAM users
- Never embed credentials in source code
- Rotate access keys regularly
- Enable CloudTrail for API logging

13. Troubleshooting

13.1 Common Issues

Emails flagged as phishing (High Confidence Phish)

Cause: DKIM is signing with amazonses.com instead of your domain

Solution: Verify DKIM CNAME records are added and SES shows DKIM status as "Successful"

compauth=fail in email headers

Cause: Domain alignment failure - authentication domains don't match From address

Solution: Enable Easy DKIM and verify all 3 CNAME records are correctly configured

dmarc=none in email headers

Cause: No DMARC record published for the sending domain

Solution: Add DMARC TXT record to DNS (_dmarc)

SPF authentication fails

Cause: SPF record doesn't include SES, or multiple SPF records exist

Solution: Ensure single SPF record includes include:amazonses.com

Can't send to external recipients

Cause: Account is still in sandbox mode

Solution: Request production access (Section 10)

13.2 Verification Header Checklist

When checking email headers, verify:

Header Check	Expected Value
spf=	pass
dkim= header.d=	pass header.d=yourdomain.com
dmarc=	pass
compauth= (Microsoft)	pass reason=100
CAT: (Microsoft)	NONE

14. Quick Reference

DNS Records Summary

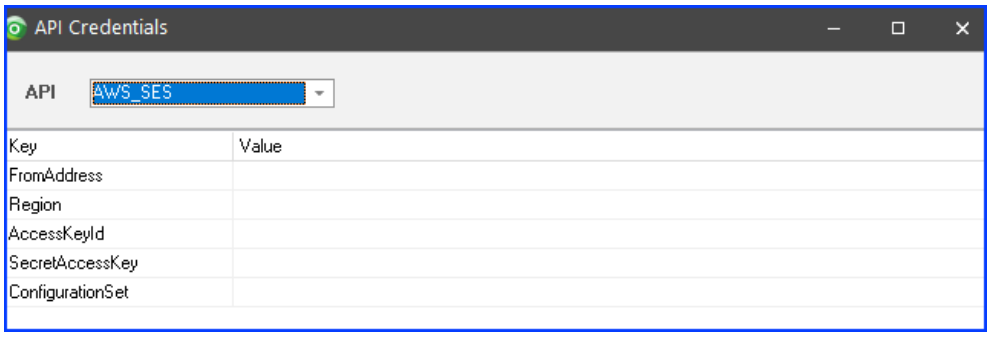
Type	Name	Value
TXT	_amazonses	[from SES]
CNAME	[token]._domainkey	[token].dkim.amazonses.com
TXT	@	v=spf1 include:amazonses.com ~all
TXT	_dmarc	v=DMARC1; p=none;

Setup Checklist

✓	Task
☐	Create domain identity in SES
☐	Enable Easy DKIM (2048-bit)
☐	Add domain verification TXT record
☐	Add 3 DKIM CNAME records
☐	Verify domain status in SES
☐	Verify DKIM status in SES
☐	Add/update SPF record
☐	Add DMARC record
☐	Create IAM user with SES permissions
☐	Generate and save access keys
☐	Configure bounce/complaint handling
☐	Test email sending in sandbox
☐	Verify email headers show pass for SPF, DKIM, DMARC
☐	Request production access

15. Configure Ostendo Continuum

1. In Ostendo, navigate to **File → System Configuration → API Credentials**
2. Select **AWS_SES** from the API dropdown
3. Enter the following values from your Azure app registration:



API Credentials

To configure AWS Simple Email Service (SES) for sending emails, select **AWS_SES** from the API dropdown and complete the following fields:

> **Note:** All credentials are stored encrypted in the Ostendo database.

Field	Description
FromAddress	The email address that will appear as the sender. This address must be verified in your AWS SES console.
Region	The AWS region where your SES service is configured (e.g., ap-southeast-2 for Sydney, us-east-1 for N. Virginia).
AccessKeyId	Your AWS IAM Access Key ID. This is obtained from the AWS IAM console when creating access credentials.
SecretAccessKey	Your AWS IAM Secret Access Key. This is only shown once when creating the access key, so ensure you have it saved securely.
ConfigurationSet	The name of your SES Configuration Set. This is used for tracking email delivery, bounces, and complaints.

Saving Credentials

Credentials are automatically saved when you exit the value list or close the screen. All fields must be competed to use the selected API.