

# AWS SES를 사용하도록 SMTP 서버 구성

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[AWS SES 컨피그레이션 검토](#)

[AWS SES SMTP 자격 증명 생성](#)

[SNA Manager SMTP 구성](#)

[AWS 인증서 수집](#)

[응답 관리 이메일 작업 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

## 소개

이 문서에서는 Secure Network Analytics Manager (SNA) 사용 Amazon Web Services Simple Email Service (AWS SES).

## 사전 요구 사항

### 요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- AWS SES

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Stealthwatch Management Console v7.3.2
- AWS SES 서비스는 2022년 5월 25일에 Easy DKIM

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 구성

### AWS SES 컨피그레이션 검토

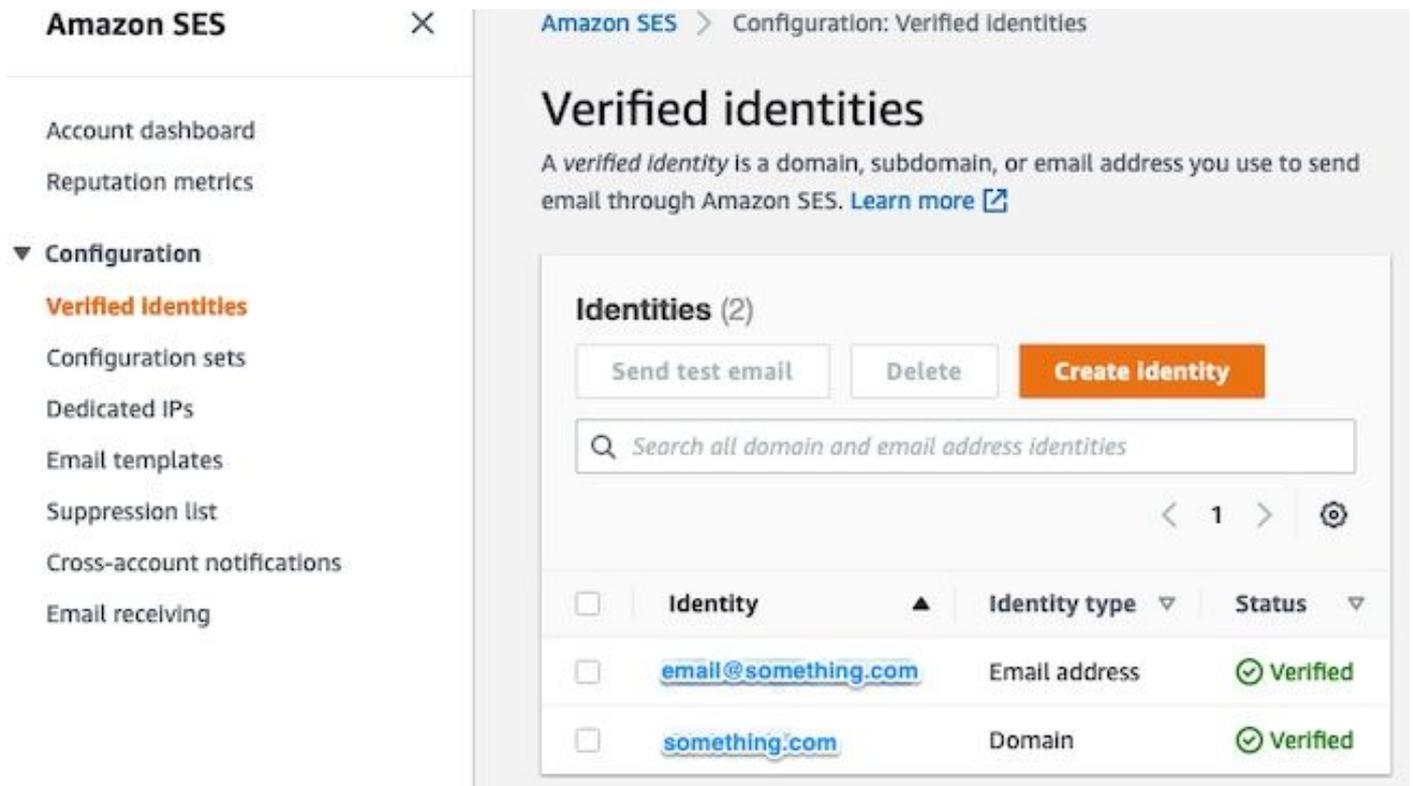
AWS에서는 다음 3비트의 정보가 필요합니다.

1. AWS SES 위치
2. SMTP 사용자 이름
3. SMTP 비밀번호

**참고:** 샌드박스에 있는 AWS SES는 허용되지만 샌드박스 환경의 제한 사항에 유의해야 합니다. <https://docs.aws.amazon.com/ses/latest/dg/request-production-access.html>

AWS 콘솔에서 Amazon SES를 선택한 다음 Configuration 및 Verified Identities.

확인된 도메인이 있어야 합니다. 확인된 이메일 주소는 필요하지 않습니다. AWS 설명서 참조 <https://docs.aws.amazon.com/ses/latest/dg/creating-identities.html#verify-domain-procedure>



SMTP 엔드포인트의 위치를 확인합니다. 이 값은 나중에 필요합니다.

**Amazon SES** ×

### Simple Mail Transfer Protocol (SMTP) settings

You can use an SMTP-enabled programming language, email server, or application to connect to the Amazon SES SMTP interface. You'll need the following information and a set of SMTP credentials to configure this email sending method in US East (N. Virginia).

SMTP endpoint	STARTTLS Port
<b>email-smtp.us-east-1.amazonaws.com</b>	25, 587 or 2587
Transport Layer Security (TLS)	TLS Wrapper Port
Required	465 or 2465

#### Authentication

You must have an Amazon SES SMTP user name and password to access the SMTP interface. These credentials are different from your AWS access keys and are unique to each region. To manage existing SMTP credentials, [visit the IAM console](#).

[Create SMTP credentials](#)

## AWS SES SMTP 자격 증명 생성

AWS 콘솔에서 Amazon SES를 클릭한 다음 Account Dashboard.

아래로 스크롤하여 "Simple Mail Transfer Protocol (SMTP) settings" 및 "Create SMTP Credentials" 이 구성을 완료할 준비가 되었을 때

사용하지 않는 이전 자격 증명(약 45일)은 잘못된 자격 증명으로 오류가 발생하지 않습니다.

이 새 창에서 사용자 이름을 임의의 값으로 업데이트하고 **Create**.

**Create User for SMTP**

This form lets you create an IAM user for SMTP authentication with Amazon SES. Enter the name of a new IAM user or accept the default and click Create to set up your SMTP credentials.

**IAM User Name:**  (Maximum 64 characters)

▼ Hide More Information

Amazon SES uses AWS Identity and Access Management (IAM) to manage SMTP credentials. The IAM user name is case sensitive and may contain only alphanumeric characters and the symbols +, -, @, \_.

SMTP credentials consist of a username and a password. When you click the Create button below, SMTP credentials will be generated for you.

The new user will be granted the following IAM policy:

```
"Statement": [{"Effect": "Allow", "Action": "ses:SendRawEmail", "Resource": "*"}]
```

[Cancel](#) [Create](#)

페이지에서 인증서를 제공하면 저장합니다. 이 브라우저 탭을 열어 둡니다.

## Create User for SMTP

☑ Your 1 User(s) have been created successfully.

This is the only time these SMTP security credentials will be available for download. Credentials for SMTP users are only available when creating the user. For your protection, you should never share your SMTP credentials with anyone.

▼ Hide User SMTP Security Credentials

ses-stealthwatch-smtp-user	
SMTP Username:	AK
SMTP Password:	BC

Close

Download Credentials

## SNA Manager SMTP 구성

에 로그인합니다. SNA Manager, 및 열기 SMTP Notifications 섹션

1. 열기 Central Management > Appliance Manager.
2. 다음을 클릭합니다. Actions 를 선택합니다.
3. 선택 Edit Appliance Configuration.
4. 다음을 선택합니다. General 탭.
5. 아래로 스크롤하여 SMTP Configuration
6. AWS에서 수집한 값 입력 SMTP Server: SMTP 엔드포인트 위치 SMTP Settings 에서 AWS SES Account Dashboard 페이지Port: 25, 587 또는 2587을 입력합니다.From Email: 이 주소는 AWS Verified DomainUser Name: 이 이름은 의 마지막 단계에서 제공된 SMTP 사용자 이름입니다. Review AWS SES Configuration 섹션Password: 이 비밀번호는 의 마지막 단계에서 제공된 SMTP 비밀번호입니다. Review AWS SES Configuration 섹션Encryption Type: STARTTLS를 선택합니다(SMTPS를 선택하는 경우 포트를 465 또는 2465로 편집).
7. 설정을 적용하고 SNA Manager 로 돌아가려면 UP 주/도 Central Management

# Appliance Configuration - SMC

/ Last Updated: 05/27/2022 10:06 AM by admin

Appliance

Network Services

General

## SMTP Configuration ⓘ

SMTP SERVER \*

email-smtp.us-east-1.amazonaws.com

PORT

587

FROM EMAIL \*

email@something.com

USER NAME

AK

PASSWORD \*

\*\*\*\*\*

ENCRYPTION TYPE

SMTPS  STARTTLS  UN-ENCRYPTED

## AWS 인증서 수집

에 대한 SSH 세션 설정 SNA Manager 루트 사용자로 로그인합니다.

다음 세 가지 항목을 검토합니다.

- SMTP 엔드포인트 위치 변경(예: email-smtp.us-east-1.amazonaws.com)
- 사용된 포트 변경(예: STARTTLS의 경우 기본값 587)
- 명령에는 STDOUT가 없으며 완료 시 프롬프트가 반환됩니다

STARTTLS의 경우(기본 포트 587):

```
openssl s_client -starttls smtp -showcerts -connect email-smtp.us-east-1.amazonaws.com:587 <<<
"Q" 2>/dev/null > mycertfile.crt awk 'split_after == 1 {n++;split_after=0} /-----END
CERTIFICATE-----/ {split_after=1} {print > "cacert" n ".pem"}' < mycertfile.crt for i in `ls -t1
*.pem`; do cp $i $(awk -F "CN=" '/s:/ {gsub(/ /,x ); print $NF}' $i).pem ; done ; rm -f cacert*
mycertfile.crt
```

SMTPS의 경우(기본 포트 465):

```
openssl s_client -showcerts -connect email-smtp.us-east-1.amazonaws.com:465 <<< "Q" 2>/dev/null
```

```
> mycertfile.crt awk 'split_after == 1 {n++;split_after=0} /-----END CERTIFICATE-----/
{split_after=1} {print > "cacert" n ".pem"}' < mycertfile.crt for i in `ls -tl *.pem`; do cp $i
$(awk -F "CN=" '/s:/ {gsub(/ /,x ); print $NF}' $i).pem ; done ; rm -f cacert* mycertfile.crt
```

pem 확장명을 가진 인증서 파일은 현재 작업 디렉토리에 만들어지며 이 디렉토리는 가져오지 않습니다(pwd 명령의 출력/마지막 행).

```
sna_manager:~# openssl s_client -starttls smtp -showcerts -connect email-smtp.us-east-1.amazonaws.com:587 <<< "Q" 2>/dev/null > mycertfile.crt
sna_manager:~# awk 'split_after == 1 {n++;split_after=0} /-----END CERTIFICATE-----/
{split_after=1} {print > "cacert" n ".pem"}' < mycertfile.crt
sna_manager:~# for i in `ls -tl *.pem`; do cp $i $(awk -F "CN=" '/s:/ {gsub(/ /,x ); print $NF}'
$i).pem ; done ; rm -f cacert* mycertfile.crt
sna_manager:~# ll
total 16
-rw-r--r-- 1 root root 1648 May 27 14:54 Amazon.pem
-rw-r--r-- 1 root root 1829 May 27 14:54 AmazonRootCA1.pem
-rw-r--r-- 1 root root 2387 May 27 14:54 email-smtp.us-east-1.amazonaws.com.pem
-rw-r--r-- 1 root root 1837 May 27 14:54 StarfieldServicesRootCertificateAuthority-G2.pem
sna_manager:~# pwd
/root
```

에서 만든 파일 다운로드 **SNA Manager** 원하는 파일 전송 프로그램(Filezilla, winscp 등)을 사용하여 로컬 시스템에 이 인증서를 **SNA Manager trust store** 에서 **Central Management**.

1. 열기 **Central Management > Appliance Manager**.
2. 다음을 클릭합니다. **Actions** 를 선택합니다.
3. 선택 **Edit Appliance Configuration**.
4. 다음을 선택합니다. **General** 탭.
5. 아래로 스크롤하여 **Trust Store**
6. 선택 **Add New**
7. 각 인증서를 업로드합니다. 파일 이름을 **Friendly Name**

## 응답 관리 이메일 작업 구성

에 로그인합니다. **SNA Manager**을 열고 **Response Management** 섹션

1. 다음을 선택합니다. **Configure** 화면 상단의 기본 리본에 있는 탭
2. 선택 **Response Management**
3. 에서 **Response Management** 페이지, 선택 **Actions** 탭
4. 선택 **Add New Action**
5. 선택 **Email**이 전자 메일 작업의 이름 제공"받는 사람" 필드에 수신자 이메일 주소를 입력합니다 (AWS SES에서 확인된 도메인에 속해야 함).주제는 무엇이든 될 수 있습니다.

Response Management

Rules Actions Syslog Formats

Email Action Cancel Save

Name: AWS SES Test Description:

Enabled Disabled actions are not performed for any associated rules.

To: [email@something.com](mailto:email@something.com)

Subject: AWS SES SMTP Test

Body:

+ Alarm Variables Preview

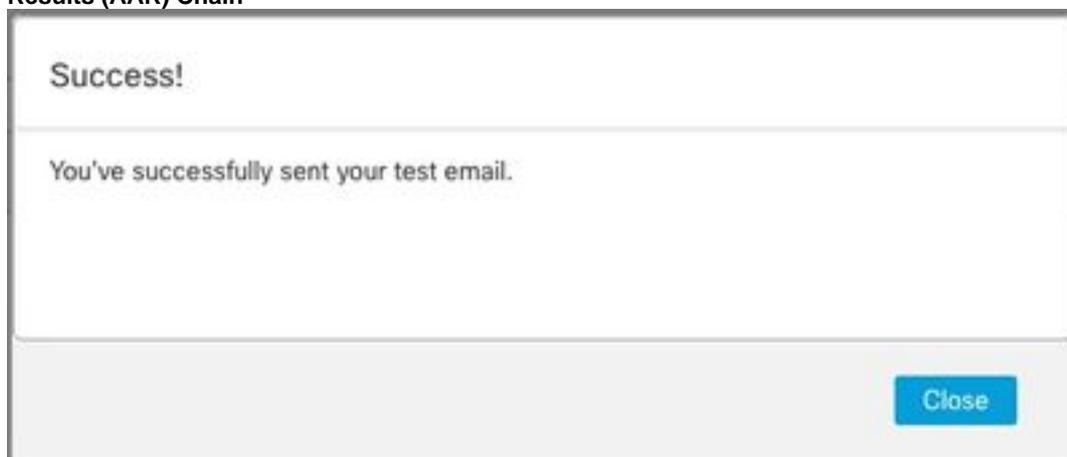
Test Action

6. 클릭 Save

## 다음을 확인합니다.

에 로그인합니다. SNA Manager을 열고 Response Management 섹션:

1. 다음을 선택합니다. Configure 화면 상단의 기본 리본에 있는 탭
2. 선택 Response Management
3. 에서 Response Management 페이지, 선택 Actions 탭
4. 에서 줄임표 선택 Actions 에서 구성한 이메일 작업의 행에 대한 열 Configure Response Management Email Action 섹션을 선택하고 Edit.
5. 선택 Test Action 구성이 유효한 경우 성공 메시지가 표시되고 이메일이 전송됩니다. 이메일 헤더에는 Amazon이 표시됩니다. Received" 필드 및 amazon과 함께 ARC-Authentication-Results (AAR) Chain



```
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@something.com header.s=
dkim=pass header.i=@amazon.es.com header.
spf=pass (google.com: domain of 010001810
sender) smtp.mailfrom=0100018106685484-fa246764-
Return-Path: <0100018106685484-fa246764-b234-4a
Received: from a8-30.smtp-out.amazon.es.com (a8-
```

6. 테스트가 실패할 경우 화면 상단에 배너가 표시됩니다. 문제 해결 섹션으로 이동합니다.

## 문제 해결

이 `/lancope/var/logs/containers/sw-reponse-mgmt.log` 파일에 테스트 작업에 대한 오류 메시지가 있습니다. 가장 일반적인 오류와 수정 사항이 표에 나열됩니다. 표에 나열된 오류 메시지는 오류 로그 줄의 일부에 불과합니다

### 오류

SMTPSendFailedException: 554 거부된 메시지: 이메일 주소가 확인되지 않았습니다. ID가 US-EAST-1 영역에서 확인에 실패했습니다. {email\_address}

인증 실패 예외: 535 인증 자격 증명이 잘못되었습니다.

SunCertPathBuilder예외: 요청된 대상에 대한 유효한 인증 경로를 찾을 수 없습니다.

SSL 루틴:tls\_process\_ske\_dhe:dh 키가 너무 작음

기타 오류

### 수정

SNA ManagerSMTP Configuration의 "From Email" 필드를 AWS SES 검증 도메인에 속한 이메일로 업데이트

반복 섹션 AWS SES SMTP 자격 증명 생성 및 SNA Manager SMTP 구성

AWS에서 제공한 모든 인증서가 SNA Manager 트러스트 스토어에 있는지 확인합니다. 테스트 작업을 수행할 때 패키지 캡처를 수행하고, 서버측에서 제공한 인증서가 트러스트 스토어 콘텐츠와 비교합니다.

추록 참조

검토를 위해 TAC 케이스 열기

부록: DH 키가 너무 작습니다.

이는 DHE 및 EDH 암호를 사용할 때 1024비트 키를 사용하고(logjam에 취약함) SNA Manager가 SSL 세션을 계속 진행하지 않을 때 AWS에서 발생하는 문제입니다. 명령 출력은 DHE/EDH 암호가 사용될 때 openssl 연결의 서버 임시 키를 보여줍니다.

```
sna_manager:~# openssl s_client -starttls smtp -connect email-smtp.us-east-2.amazonaws.com:587 -
cipher "EDH" <<< "Q" 2>/dev/null | grep "Server Temp"
```

```
Server Temp Key: DH, 1024 bits
```

```
sna_manager:~# openssl s_client -starttls smtp -connect email-smtp.us-east-2.amazonaws.com:587 -
cipher "DHE" <<< "Q" 2>/dev/null | grep "Server Temp"
```

```
Server Temp Key: DH, 1024 bits
```

```
sna_manager:~# openssl s_client -starttls smtp -connect email-smtp.us-east-2.amazonaws.com:587
<<< "Q" 2>/dev/null | grep "Server Temp"
```

```
Server Temp Key: ECDH, P-256, 256 bits
```

사용 가능한 유일한 해결 방법은 SMC의 루트 사용자로 명령을 사용하여 모든 DHE 및 EDH 암호를 제거하는 것입니다. AWS는 ECDHE 암호 그룹을 선택하고 연결이 성공합니다.

```
cp /lancope/services/swos-compliance/security/tls-ciphers /lancope/services/swos-compliance/security/tls-ciphers.bak ; > /lancope/services/swos-compliance/security/tls-ciphers ; echo "TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_256_GCM_SHA384:TLS_AES_128_CCM_SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:AES256-GCM-SHA384" > /lancope/services/swos-compliance/security/tls-ciphers ; docker restart sw-response-mgmt
```

## 관련 정보

- <https://docs.aws.amazon.com/ses/latest/dg/setting-up.html>
- <https://docs.aws.amazon.com/ses/latest/dg/creating-identities.html#verify-domain-procedure>
- <https://docs.aws.amazon.com/ses/latest/dg/smtp-credentials.html>
- <https://docs.aws.amazon.com/ses/latest/dg/smtp-connect.html>
- [기술 지원 및 문서 - Cisco Systems](#)