

# Configura server SMTP per l'utilizzo di AWS SES

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Verifica configurazione AWS SES](#)

[Crea credenziali SMTP AWS SES](#)

[Configurazione della configurazione SMTP di SNA Manager](#)

[Raccolta certificati AWS](#)

[Configura azione e-mail di Response Management](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

## Introduzione

Questo documento descrive come configurare **Secure Network Analytics Manager (SNA)** da utilizzare **Amazon Web Services Simple Email Service (AWS-SES)**.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- AWS-SES

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- **Stealthwatch Management Console v7.3.2**
- Servizi AWS SES esistenti al 25 MAGGIO 2022 con **Easy DKIM**

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Configurazione

## Verifica configurazione AWS SES

Sono richiesti tre bit di informazioni da AWS:

1. Percorso AWS-SES
2. Nome utente SMTP
3. Password SMTP

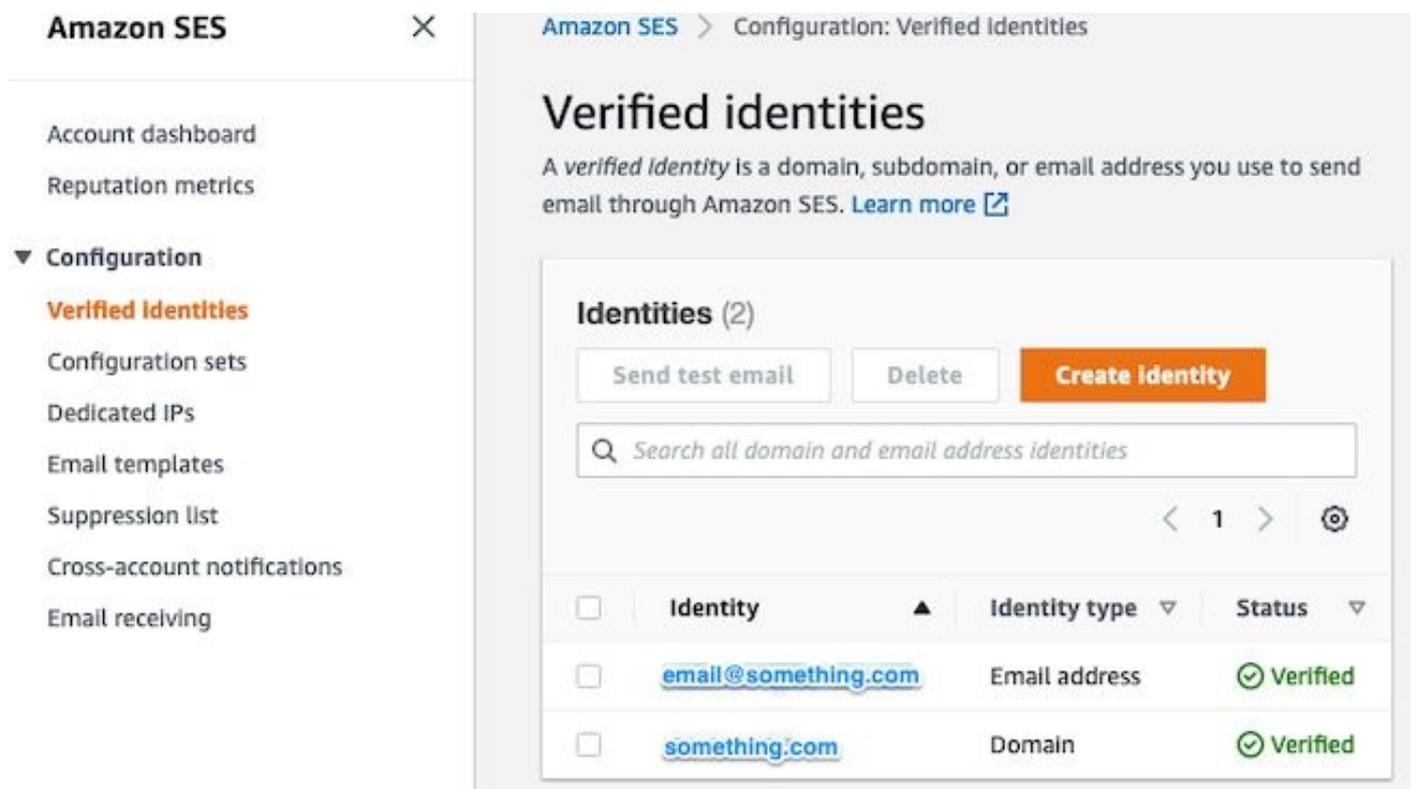
**Nota:** AWS SES, situato nella sandbox, è accettabile, ma è necessario essere consapevoli delle limitazioni per gli ambienti sandbox:

<https://docs.aws.amazon.com/ses/latest/dg/request-production-access.html>

Nella console AWS, passare a Amazon SES, quindi selezionare Configuration e fare clic su Verified Identities.

È necessario disporre di un dominio verificato. Non è necessario un indirizzo di posta elettronica verificato. Fare riferimento alla documentazione di AWS

<https://docs.aws.amazon.com/ses/latest/dg/creating-identities.html#verify-domain-procedure>



The screenshot shows the Amazon SES console interface. On the left is a navigation sidebar with 'Configuration' expanded and 'Verified identities' selected. The main content area is titled 'Verified identities' and includes a description: 'A verified identity is a domain, subdomain, or email address you use to send email through Amazon SES. Learn more'. Below this is a section for 'Identities (2)' with buttons for 'Send test email', 'Delete', and 'Create identity'. A search bar is present with the placeholder text 'Search all domain and email address identities'. A table lists the identities:

<input type="checkbox"/>	Identity ▲	Identity type ▼	Status ▼
<input type="checkbox"/>	<a href="#">email@something.com</a>	Email address	✔ Verified
<input type="checkbox"/>	<a href="#">something.com</a>	Domain	✔ Verified

Annotare il percorso dell'endpoint SMTP. Questo valore è necessario in seguito.

**Amazon SES** X

**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
<input type="text" value="email-smtp.us-east-1.amazonaws.com"/>	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](#).

## Crea credenziali SMTP AWS SES

Nella console AWS, passare a **Amazon SES**, quindi fare clic su **Account Dashboard**.

Scorrere verso il basso fino a visualizzare "**Simple Mail Transfer Protocol (SMTP) settings**" e fare clic su **Create SMTP Credentials** per completare la configurazione.

Le credenziali non utilizzate meno recenti (circa 45 giorni) non sembrano essere errate in quanto non valide.

In questa nuova finestra, aggiornare il nome utente a qualsiasi valore e fare clic su **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": "*"}]
```

Quando la pagina presenta le credenziali, salvarle. Tieni aperta la scheda del browser.

## 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](#)

## Configurazione della configurazione SMTP di SNA Manager

Accedi a SNA Manager aperto SMTP Notifications sezione

1. Open (Aperto) **Central Management > Appliance Manager**.
2. Fare clic sul pulsante **Actions** per l'accessorio.
3. Seleziona **Edit Appliance Configuration**.
4. Selezionare il **General**.
5. Scorri verso il basso fino a **SMTP Configuration**
6. Immettere i valori raccolti da **AWS SMTP Server**: Percorso dell'endpoint SMTP raccolto dal **SMTP Settings** dal **AWS SES Account Dashboard** paginaPort: Immettere 25, 587 o 2587From Email: Può essere impostato su qualsiasi indirizzo di posta elettronica contenente **AWS Verified Domain**User Name: Si tratta del nome utente SMTP visualizzato nell'ultimo passaggio della **Review AWS SES Configuration** sezionePassword: Si tratta della password SMTP presentata nell'ultimo passaggio della **Review AWS SES Configuration** sezioneEncryption Type: Selezionare **STARTLS** (se si seleziona **SMTPS**, modificare la porta su 465 o 2465)
7. Applicare le impostazioni e attendere **SNA Manager** per tornare a un **UP** stato in **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

## Raccolta certificati AWS

Stabilire una sessione SSH per **SNA Manager** accedere come utente root.

Rivedi questi tre elementi

- Modificare la posizione dell'endpoint SMTP (ad esempio email-smtp.us-east-1.amazonaws.com)
- Modificare la porta utilizzata (ad esempio, impostare 587 per STARTTLS)
- I comandi non hanno STDOUT, il prompt viene restituito al completamento

Per STARTTLS (porta predefinita 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
```

Per SMTPS (porta predefinita 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
```

I file di certificato con estensione pem vengono creati nella directory di lavoro corrente, non accettare questa directory (output da comando pwd / ultima riga)

```
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
```

Scarica i file creati in **SNA Manager** sul computer locale con il programma di trasferimento file desiderato (Filezilla, winscp, ecc.) e aggiungere questi certificati al **SNA Manager trust store** in **Central Management**.

1. Open (Aperto) **Central Management > Appliance Manager**.
2. Fare clic sul pulsante **Actions** per l'accessorio.
3. Seleziona **Edit Appliance Configuration**.
4. Selezionare il **General** .
5. Scorri verso il basso fino a **Trust Store**
6. Seleziona **Add New**
7. Caricare ogni certificato, si consiglia di utilizzare il nome file come **Friendly Name**

## Configura azione e-mail di Response Management

Accedi a **SNA Manager** e aprire la **Response Management** sezione

1. Selezionare il **Configure** sulla barra multifunzione principale nella parte superiore dello schermo
2. Seleziona **Response Management**
3. Dal **Response Management** selezionare **Actions** scheda
4. Seleziona **Add New Action**
5. Seleziona **Email** Specificare un nome per l'azione di posta elettronica Immettere l'indirizzo e-mail del destinatario nel campo "A" (notare che deve appartenere al dominio verificato in AWS SES) Il soggetto può essere qualsiasi cosa.

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

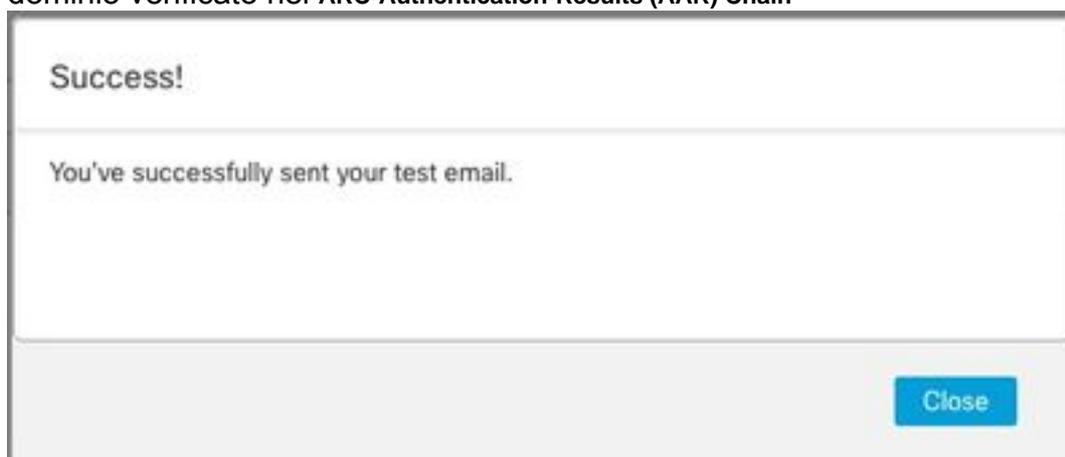
6. Clic **Save**

## Verifica

Accedi a **SNA Manager** aprire la **Response Management** sezione:

1. Selezionare il **Configure** sulla barra multifunzione principale nella parte superiore dello schermo
2. Seleziona **Response Management**
3. Dal **Response Management** selezionare **Actions** scheda
4. Selezionare i puntini di sospensione nella **Actions** per la riga dell'azione e-mail configurata nel **Configure Response Management Email Action** e selezionare **Edit**.
5. Seleziona **Test Action** e se la configurazione è valida, viene visualizzato un messaggio di operazione riuscita e viene recapitata un'e-mail.

Nell'intestazione email amazonses è mostrato nella "Received" e amazonses, insieme al dominio verificato nel **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. Se il test ha avuto esito negativo, nella parte superiore dello schermo viene visualizzato un banner - passare alla sezione Risoluzione dei problemi

## Risoluzione dei problemi

OSPF (Open Shortest Path First) `/lancope/var/logs/containers/sw-reponse-mgmt.log` contiene i messaggi di errore per le azioni di test. L'errore più comune e la correzione viene elencata nella tabella. I messaggi di errore elencati nella tabella sono solo una parte della riga del log degli errori

Errore	Fix
SMTPSendFailedException: 554 Messaggio rifiutato: Indirizzo di posta elettronica non verificato. Identità non sottoposte a controllo nella regione US-EAST-1: {indirizzo_posta_elettronica}	Aggiornare "From Email" (Da e-mail) nella configurazione SMTP di SNA Manager su un messaggio di posta elettronica appartenente al dominio verificato di AWS SES
EccezioneAutenticazioneNonRiuscita: Credenziali di autenticazione 535 non valide	Ripetere le sezioni Creare credenziali SMTP AWS SES e configurare la configurazione SMTP di SNA Manager
Eccezione SunCertPathBuilder: impossibile trovare un percorso di certificazione valido per la destinazione richiesta	Confermare che tutti i certificati AWS presentati si trovino nell'archivio attendibile di SNA Manager - eseguire l'acquisizione dei pacchetti quando viene eseguita l'azione di test e confrontare i certificati presentati sul lato server con il contenuto dell'archivio attendibile
routine SSL:tls_process_ske_dhe:chiave dh troppo piccola	Cfr. addendum
Qualsiasi altro errore	Apri richiesta TAC per revisione

Appendice: Chiave DH troppo piccola.

Questo è un problema del lato AWS, in quanto usano chiavi a 1024 bit quando si usano cifrari DHE ed EDH (suscettibili logjam) e SNA Manager rifiuta di continuare la sessione SSL. Il risultato del comando mostra i tasti temp del server dalla connessione openssl quando vengono utilizzati i cifrari DHE/EDH.

```
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

L'unica soluzione disponibile è rimuovere tutte le cifrature DHE ed EDH con il comando come utente root su SMC, AWS seleziona una suite di cifratura ECDHE e la connessione riesce.

```
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
```

## Informazioni correlate

- <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>
- [Documentazione e supporto tecnico – Cisco Systems](#)