

# Configurar o servidor SMTP para usar o AWS SES

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Revisar a configuração do AWS SES](#)

[Criar Credenciais SMTP do AWS SES](#)

[Configurar SMTP do SNA Manager](#)

[Reunir certificados AWS](#)

[Configurar Ação de Email de Gerenciamento de Resposta](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve como configurar seu **Secure Network Analytics Manager (SNA)** para usar **Amazon Web Services Simple Email Service AWS SES**.

## Prerequisites

### Requirements

A Cisco recomenda o conhecimento destes tópicos:

- AWS SES

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- **Stealthwatch Management Console v7.3.2**
- Serviços AWS SES existentes em 25 de maio de 2022 com **Easy DKIM**

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Configurar

## Revisar a configuração do AWS SES

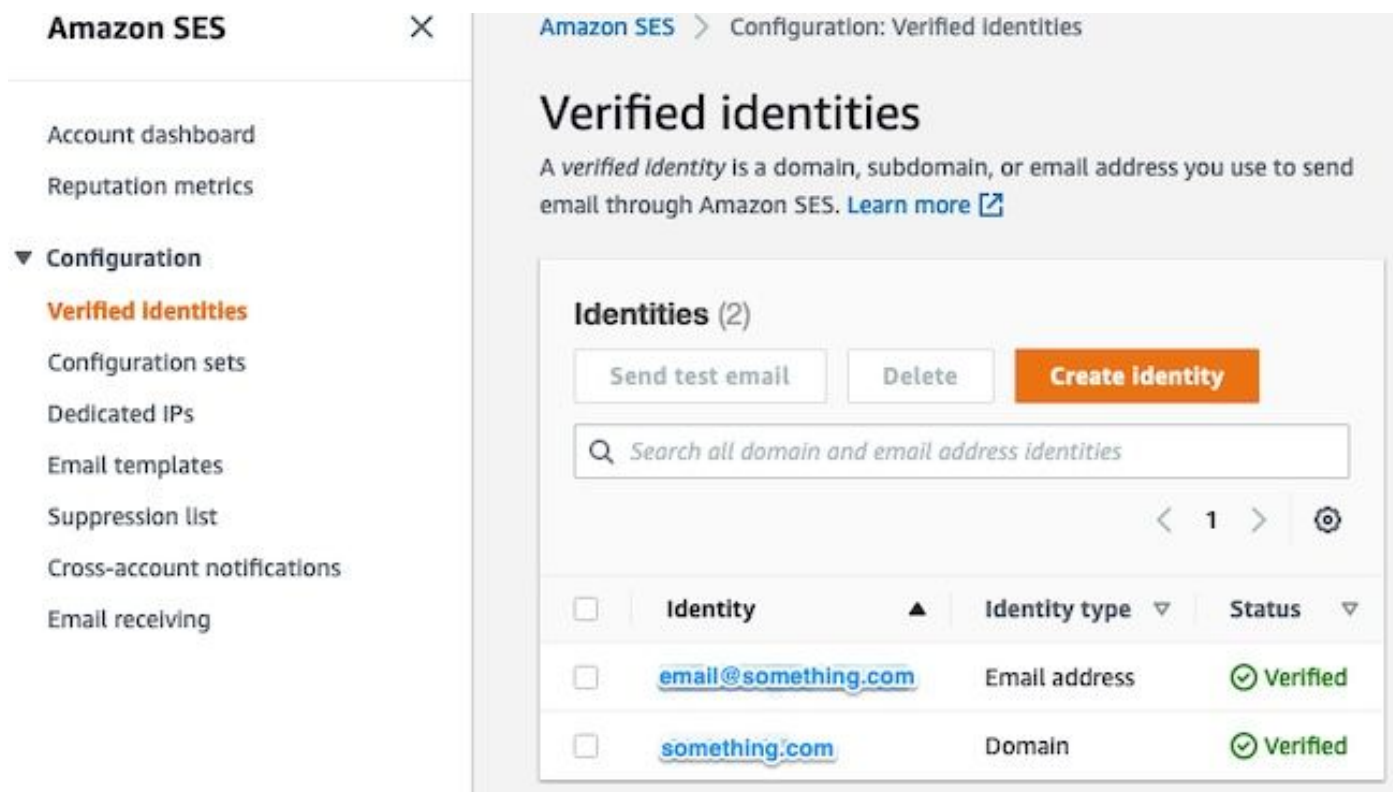
São necessários três bits de informação do AWS:

1. local AWS SES
2. Nome de usuário SMTP
3. Senha SMTP

**Note:** O AWS SES localizado no sandbox é aceitável, mas esteja ciente das limitações para ambientes de sandbox: <https://docs.aws.amazon.com/ses/latest/dg/request-production-access.html>

No console AWS, navegue até Amazon SES e selecione Configuration e clique em Verified Identities.

Você deve ter um domínio verificado. Não é necessário um endereço de email verificado. Consulte a documentação da AWS <https://docs.aws.amazon.com/ses/latest/dg/creating-identities.html#verify-domain-procedure>



The screenshot shows the AWS SES console interface. On the left is a navigation sidebar with 'Amazon SES' at the top and a 'Configuration' section containing 'Verified Identities' (highlighted in orange), 'Configuration sets', 'Dedicated IPs', 'Email templates', 'Suppression list', 'Cross-account notifications', and 'Email receiving'. 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 'Search all domain and email address identities'. A table below shows two 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

Observe o local do seu endpoint SMTP. Esse valor será necessário posteriormente.

**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](#).

## Criar Credenciais SMTP do AWS SES

No console AWS, navegue até **Amazon SES** clique em **Account Dashboard**.

Role para baixo até "**Simple Mail Transfer Protocol (SMTP) settings**" e clique em **Create SMTP Credentials** quando estiver pronto para concluir essa configuração.

Credenciais mais antigas e não utilizadas (aproximadamente 45 dias) não parecem ter erros como credenciais inválidas.

Nessa nova janela, atualize o nome de usuário para qualquer valor e clique em **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 a página apresentar as credenciais, salve-as. Mantenha esta guia do navegador aberta.

## 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

## Configurar SMTP do SNA Manager

Faça login no SNA Manager e abra a seção SMTP Notifications

1. Abrir **Central Management > Appliance Manager**.
2. Clique no botão **Actions** para o equipamento.
3. Selecionar **Edit Appliance Configuration**.
4. Selecione o **General** guia.
5. Role para baixo até **SMTP Configuration**
6. Inserir os valores reunidos do **AWS SMTP Server**: Este é o local do Ponto de Extremidade SMTP obtido do **SMTP Settings** nos **AWS SES Account Dashboard** página  
**Port**: Digite 25, 587 ou 2587  
**From Email**: Pode ser definido para qualquer endereço de e-mail que contenha o **AWS Verified Domain**  
**User Name**: Este é o nome de usuário SMTP que foi apresentado na última etapa do **Review AWS SES Configuration** seção  
**Password**: Esta é a senha SMTP que foi apresentada na última etapa do **Review AWS SES Configuration** seção  
**Encryption Type**: Selecione **STARTTLS** (Se você selecionar **SMTPS**, edite a porta para 465 ou 2465)
7. Aplique as configurações e aguarde o **SNA Manager** para voltar a um estado **UP** em **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

## Reunir certificados AWS

Estabelecer uma sessão SSH para o **SNA Manager** faça login como o usuário raiz.

Revise estes três itens

- Alterar a localização do ponto final SMTP (por exemplo, email-smtp.us-east-1.amazonaws.com)
- Alterar a porta usada (por exemplo, padrão de 587 para STARTTLS)
- Os comandos não têm STDOUT, o prompt é retornado após a conclusão

Para STARTTLS (porta padrão de 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 -tl
*.pem`; do cp $i $(awk -F "CN=" '/s:/ {gsub(/ /,x ); print $NF}' $i).pem ; done ; rm -f cacert*
mycertfile.crt
```

Para SMTPS (porta padrão de 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
```

Os arquivos de certificado com a extensão pem são criados no diretório de trabalho atual, e não deste diretório (saída do comando pwd / última linha)

```
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
```

Faça download dos arquivos criados no **SNA Manager** à sua máquina local com o programa de transferência de arquivos de sua escolha (Filezilla, winscp, etc.) e adicione esses certificados à **SNA Manager trust store** in **Central Management**.

1. Abrir **Central Management > Appliance Manager**.
2. Clique no botão **Actions** para o equipamento.
3. Selecionar **Edit Appliance Configuration**.
4. Selecione o **General** guia.
5. Role para baixo até **Trust Store**
6. Selecionar **Add New**
7. Carregue cada um dos certificados recomendados para usar o nome de arquivo como **Friendly Name**

## Configurar Ação de Email de Gerenciamento de Resposta

Faça login no **SNA Manager** e abra o **Response Management** seção

1. Selecione o **Configure** na faixa de opções principal na parte superior da tela
2. Selecionar **Response Management**
3. Nos **Response Management** , selecione **Actions** guia
4. Selecionar **Add New Action**
5. Selecionar **Email** Forneça um nome para esta ação de Email Insira o endereço de e-mail do destinatário no campo "Para" (observe que ele deve pertencer ao domínio verificado no AWS SES)O assunto pode ser qualquer coisa.

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

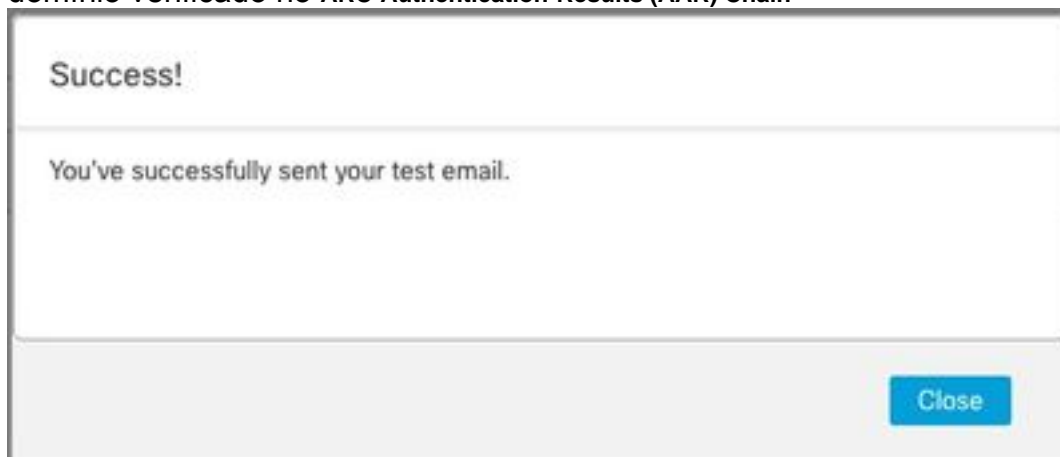
6. Clique em **Save**

## Verificar

Faça login no **SNA Manager** abra o **Response Management** seção:

1. Selecione o **Configure** na faixa de opções principal na parte superior da tela
2. Selecionar **Response Management**
3. Nos **Response Management** , selecione **Actions** guia
4. Selecione as reticências no **Actions** para a linha da ação de email configurada no **Configure Response Management Email Action** e selecione **Edit**.
5. Selecionar **Test Action** e se a configuração for válida, uma mensagem de êxito será apresentada e um e-mail será entregue.

No cabeçalho do e-mail, amazonas é mostrado na "**Received**" e amazonas, junto com o domínio verificado no **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 o teste não for bem-sucedido, um banner será apresentado na parte superior da tela - continue na seção de solução de problemas

## Troubleshoot

O `/lancope/var/logs/containers/sw-reponse-mgmt.log` contém as mensagens de erro para as ações de teste. O erro mais comum, e a correção é listada na tabela.

Observe que as mensagens de erro listadas na tabela são apenas uma parte da linha do log de erros

### Erro

SMTPSendFailedException: 554 Mensagem rejeitada: O endereço de email não foi verificado. As identidades falharam na verificação na região US-EAST-1: {email\_address}

AuthenticationFailedException: 535 Credenciais de autenticação inválidas

Exceção do SunCertPathBuilder: não é possível encontrar um caminho de certificação válido para o destino solicitado

rotinas SSL:tls\_process\_ske\_dhe:chave dh muito pequena

Qualquer outro erro

### Reparar

Atualize o "Do e-mail" na configuração SMTP do Gerenciador SNA para um e-mail que pertença a domínio verificado do AWS SES

Seções repetidas Criar Credenciais SMTP do AWS SES e Configurar Configuração SMTP do SNA Manager

Confirme se todos os certificados apresentados por AWS estão no armazenamento confiável do SNA Manager - execute a captura de pacotes quando

**Ação de Teste** for executada e compare os certificados apresentados no lado do servidor com o conteúdo do armazenamento confiável

Ver adenda

Abrir caso do TAC para revisão

Adendo: Chave DH muito pequena.

Esse é um problema do AWS, pois eles usam chaves de 1024 bits quando as cifras DHE e EDH são usadas (susceptíveis ao logjam) e o Gerenciador SNA se recusa a continuar a sessão SSL. A saída do comando mostra as chaves temporárias do servidor da conexão openssl quando cifras DHE/EDH são usadas.

```
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
```

A única solução disponível é remover todas as cifras DHE e EDH com o comando como o usuário raiz no SMC, o AWS seleciona um conjunto de cifras ECDHE e a conexão é bem-sucedida.

```
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
```

## Informações Relacionadas

- <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>
- [Suporte Técnico e Documentação - Cisco Systems](#)