

SMTP-Server für AWS SES konfigurieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[AWS SES-Konfiguration überprüfen](#)

[AWS SES SMTP-Anmeldeinformationen erstellen](#)

[Konfiguration von SNA Manager SMTP](#)

[AWS-Zertifikate erfassen](#)

[E-Mail-Aktion für das Antwortmanagement konfigurieren](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie Ihre **Secure Network Analytics Manager (SNA)** zur Verwendung **Amazon Web Services Simple Email Service (AWS SES)**.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- AWS SES

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- **Stealthwatch Management Console v7.3.2**
- AWS SES Services, wie sie am 25. Mai 2022 mit **Easy DKIM**

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konfigurieren

AWS SES-Konfiguration überprüfen

AWS benötigt drei Bit an Informationen:

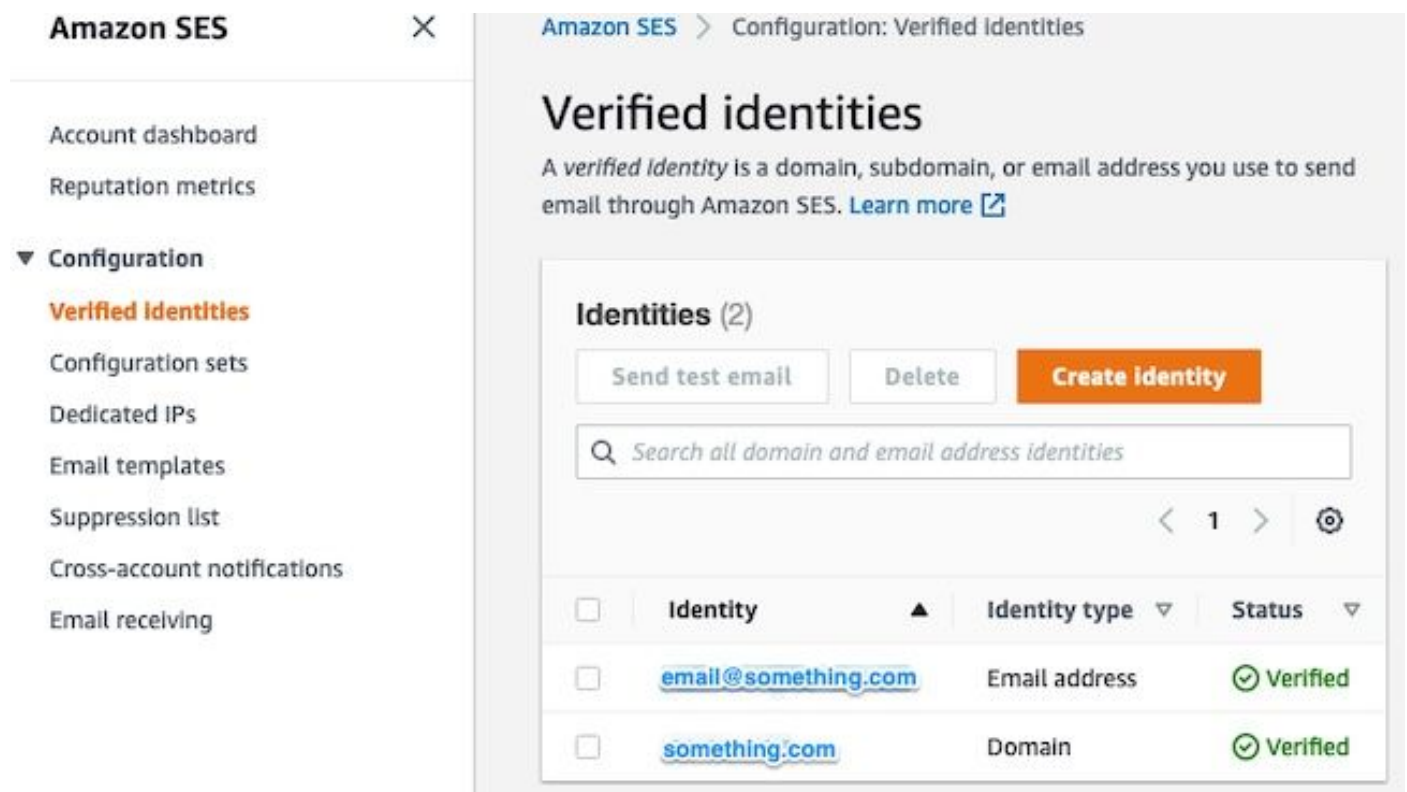
1. AWS SES-Standort
2. SMTP-Benutzername
3. SMTP-Kennwort

Anmerkung: AWS SES befindet sich in der Sandbox ist akzeptabel, aber beachten Sie die Einschränkungen für Sandbox-Umgebungen:

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

Navigieren Sie in der AWS-Konsole zu **Amazon SES**, und wählen Sie **Configuration** und klicke auf **Verified Identities**.

Sie müssen über eine verifizierte Domäne verfügen. Eine verifizierte E-Mail-Adresse ist nicht erforderlich. Siehe AWS-Dokumentation <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 table of identities. The table has columns for 'Identity', 'Identity type', and 'Status'. There are two identities listed: 'email@something.com' (Email address, Verified) and 'something.com' (Domain, Verified). Above the table are buttons for 'Send test email', 'Delete', and 'Create identity', along with a search bar and pagination controls.

Identity	Identity type	Status
email@something.com	Email address	Verified
something.com	Domain	Verified

Notieren Sie sich den Standort Ihres SMTP-Endpunkts. Dieser Wert wird später benötigt.

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
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](#).

[Create SMTP credentials](#)

AWS SES SMTP-Anmeldeinformationen erstellen

Navigieren Sie in der AWS-Konsole zu **Amazon SES**, und klicken Sie auf **Account Dashboard**.

Blättern Sie nach unten zum Ordner "**Simple Mail Transfer Protocol (SMTP) settings**" und klicken Sie auf **Create SMTP Credentials** um diese Konfiguration abzuschließen.

Ältere, nicht verwendete Anmeldeinformationen (ca. 45 Tage) scheinen keine ungültigen Anmeldeinformationen zu sein.

Aktualisieren Sie den Benutzernamen in diesem neuen Fenster auf einen beliebigen Wert, und klicken Sie auf **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: ses-stealthwatch-smtp-user
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](#)


Speichern Sie die Anmeldeinformationen, wenn die Seite angezeigt wird. Lassen Sie diese Browser-Registerkarte geöffnet.

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](#)

Konfiguration von SNA Manager SMTP

Melden Sie sich beim SNA Manager, und öffnen SMTP Notifications Schnitt

1. Offen **Central Management > Appliance Manager**.
2. Klicken Sie auf **Actions** für die Appliance.
3. Auswählen **Edit Appliance Configuration**.
4. Wählen Sie **General** aus.
5. Blättern Sie nach unten zu **SMTP Configuration**
6. Geben Sie die von AWS erfassten Werte ein. **SMTP Server**: Dies ist der SMTP-Endpunkt-Speicherort, der vom **SMTP Settings** von **AWS SES Account Dashboard** Seite **Port**: Geben Sie 25, 587 oder 2587 ein **From Email**: Dies kann auf jede E-Mail-Adresse festgelegt werden, die den **AWS Verified Domain** **User Name**: Dies ist der SMTP-Benutzername, der im letzten Schritt des **Review AWS SES Configuration** Schnitt **Password**: Dies ist das SMTP-Kennwort, das im letzten Schritt des **Review AWS SES Configuration** Schnitt **Encryption Type**: Wählen Sie **STARTTLS** (Wenn Sie **SMTPS** auswählen, ändern Sie den Port auf 465 oder 2465)
7. Übernehmen Sie die Einstellungen, und warten Sie auf den **SNA Manager** zurück zu einem **UP** Zustand 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

AWS-Zertifikate erfassen

Richten Sie eine SSH-Sitzung mit dem **SNA Manager**, und melden Sie sich als root an.

Diese drei Elemente überprüfen

- Ändern Sie den Speicherort des SMTP-Endpunkts (z. B. email-smtp.us-east-1.amazonaws.com).
- Ändern Sie den verwendeten Port (z. B. der Standardwert 587 für STARTTLS).
- Die Befehle haben keinen STDOUT, die Eingabeaufforderung wird nach Abschluss zurückgegeben

Für STARTTLS (Standard-Port von 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
```

Für SMTPS (Standard-Port 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
```

Die Zertifikatsdateien mit der Erweiterung pem werden im aktuellen Arbeitsverzeichnis erstellt, nicht aus diesem Verzeichnis (Ausgabe aus Befehl pwd / letzte Zeile)

```
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
```

Laden Sie die Dateien herunter, die auf dem **SNA Manager** auf Ihrem lokalen Rechner mit dem Dateiübertragungsprogramm Ihrer Wahl (Filezilla, winscp, etc.), und fügen Sie diese Zertifikate in die **SNA Manager trust store** in **Central Management**.

1. Offen **Central Management > Appliance Manager**.
2. Klicken Sie auf **Actions** für die Appliance.
3. Auswählen **Edit Appliance Configuration**.
4. Wählen Sie **General** aus.
5. Blättern Sie nach unten zu **Trust Store**
6. Auswählen **Add New**
7. Laden Sie die Zertifikate hoch. Es wird empfohlen, den Dateinamen als **Friendly Name**

E-Mail-Aktion für das Antwortmanagement konfigurieren

Melden Sie sich beim **SNA Manager**, und öffnen Sie die **Response Management** Schnitt

1. Wählen Sie **configure** Registerkarte im Hauptfenster am oberen Bildschirmrand
2. Auswählen **Response Management**
3. Über die **Response Management** Seite auswählen **Actions** Lasche
4. Auswählen **Add New Action**
5. Auswählen **Email**Namen für diese E-Mail-Aktion angebenGeben Sie die E-Mail-Adresse des Empfängers im Feld "An" ein (beachten Sie, dass diese zur in AWS SES verifizierten Domäne gehören muss).Das Thema kann alles sein.

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

Subject: AWS SES SMTP Test

Body:

+ Alarm Variables Preview

Test Action

6. Klicken Sie auf **Save**

Überprüfung

Melden Sie sich beim **SNA Manager**, und öffnen Sie die **Response Management** Abschnitt:

1. Wählen Sie **configure** Registerkarte im Hauptfenster am oberen Bildschirmrand
2. Auswählen **Response Management**
3. Über die **Response Management** Seite auswählen **Actions** Lasche
4. Wählen Sie die Ellipse im **Actions** Spalte für die Zeile der E-Mail-Aktion, die Sie im **Configure Response Management Email Action** und wählen Sie **Edit**.
5. Auswählen **Test Action** Wenn die Konfiguration gültig ist, wird eine Erfolgsmeldung angezeigt, und es wird eine E-Mail zugestellt.

Im E-Mail-Header wird amazones im "Received"-Feld und Amazonen, zusammen mit der verifizierten Domäne in der **ARC-Authentication-Results (AAR) Chain**

Success!

You've successfully sent your test email.

Close


```
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. Wenn der Test nicht erfolgreich war, wird oben im Bildschirm ein Banner angezeigt. Fahren Sie mit dem Abschnitt zur Fehlerbehebung fort.

Fehlerbehebung

Die Fehlermeldung `/lancope/var/logs/containers/sw-reponse-mgmt.log` enthält die Fehlermeldungen für die Testaktionen. Der häufigste Fehler, und die Korrektur ist in der Tabelle aufgeführt. Beachten Sie, dass die in der Tabelle aufgeführten Fehlermeldungen nur einen Teil der Zeile des Fehlerprotokolls darstellen.

Fehler	Beheben
SMTPSendFailedAusnahme: 554 Nachricht abgelehnt: E-Mail-Adresse ist nicht verifiziert. Die Identitäten wurden in der Region US-EAST-1 nicht geprüft: {email_address}	Aktualisieren Sie "Von E-Mail" in der SNA Manager SMTP-Konfiguration auf eine E-Mail, die zur AWS SES-verifizierten Domäne gehört.
AuthentifizierungFehlgeschlageneAusnahme: 535 Authentifizierungsdaten ungültig	Abschnitte wiederholen Erstellen von AWS SES SMTP-Anmeldeinformationen und Konfigurieren in SNA Manager SMTP-Konfiguration Bestätigen Sie, dass sich alle AWS-Zertifikate im Manager-Vertrauensspeicher befinden. Führen Sie eine Paketerfassung durch, wenn eine Testaktion durchgeführt wird, und vergleichen Sie die serverseitigen Zertifikate mit den Inhalten des Vertrauensspeichers.
SunCertPathBuilderAusnahme: kein gültiger Zertifizierungspfad zum angeforderten Ziel gefunden	Siehe Anhang
SSL-Routinen:tls_process_ske_dhe:dh Schlüssel zu klein	TAC-Ticket zur Überprüfung öffnen
Andere Fehler	

Nachtrag: DH-Schlüssel zu klein.

Dies ist ein AWS-Problem, da sie 1024-Bit-Schlüssel verwenden, wenn DHE- und EDH-Chiffren verwendet werden (anfällig für Logjam) und der SNA-Manager sich weigert, die SSL-Sitzung fortzusetzen. Die Befehlsausgabe zeigt die temporären Serverschlüssel der openssl-Verbindung an, wenn DHE/EDH-Verschlüsselungen verwendet werden.

```
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
```

Die einzig verfügbare Problemumgehung besteht darin, alle DHE- und EDH-Chiffren mit dem Befehl als Root-Benutzer auf der SMC zu entfernen. AWS wählt eine ECDHE-Chiffriersuite aus und die Verbindung wird erfolgreich hergestellt.

```
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
```

Zugehörige Informationen

- <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>
- [Technischer Support und Dokumentation für Cisco Systeme](#)