AWS SESを使用するためのSMTPサーバの設定

内容

概要

このドキュメントでは、 **Secure Network Analytics Manager** (SNA)を使用する **Amazon Web Services Simple Email Service** (AWS SES)。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- AWS SES

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- **Stealthwatch Management Console v7.3.2**
- AWS SESサービスは2022年5月25日に提供され、 **Easy DKIM**

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

AWS SES設定のレビュー

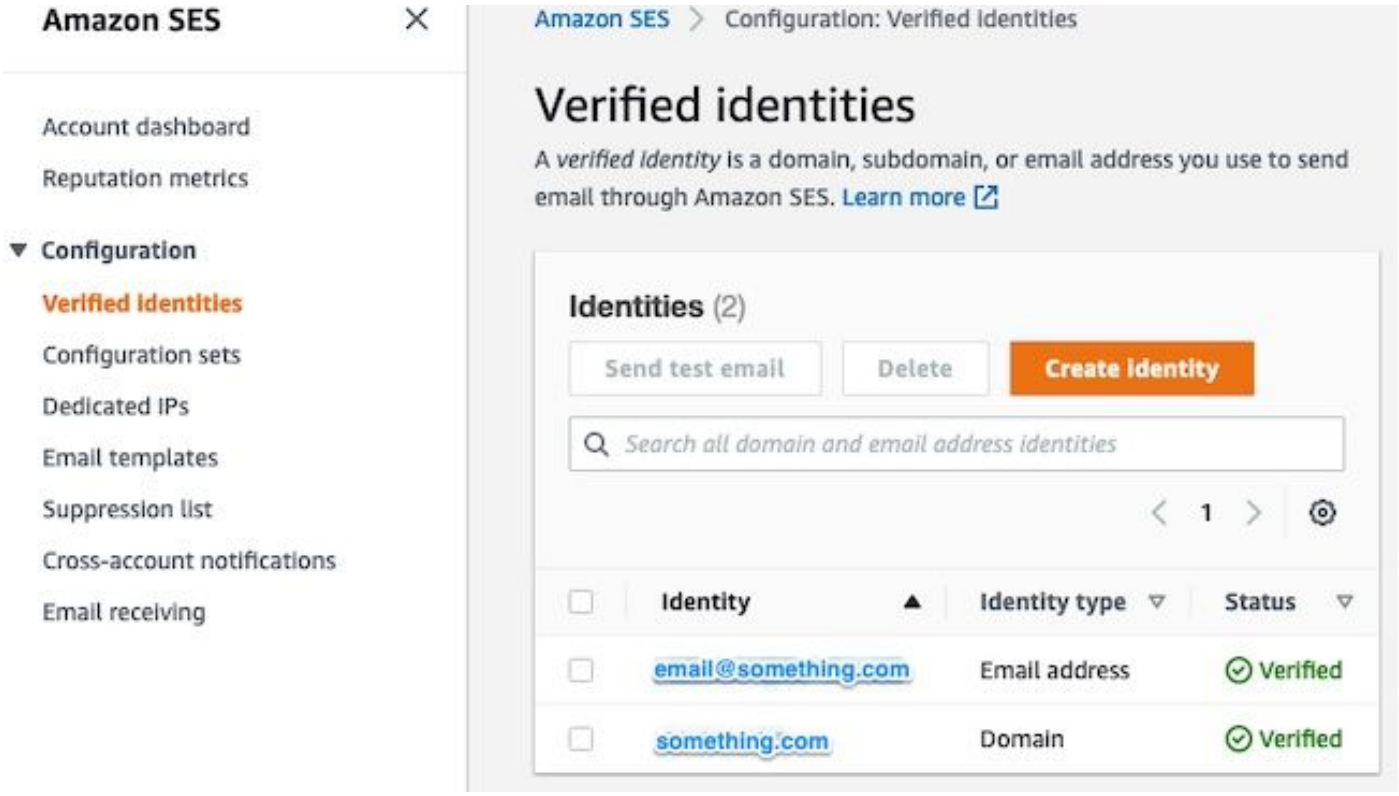
AWSから3ビットの情報が必要です。

1. AWS SESロケーション
2. SMTPユーザ名
3. SMTPパスワード

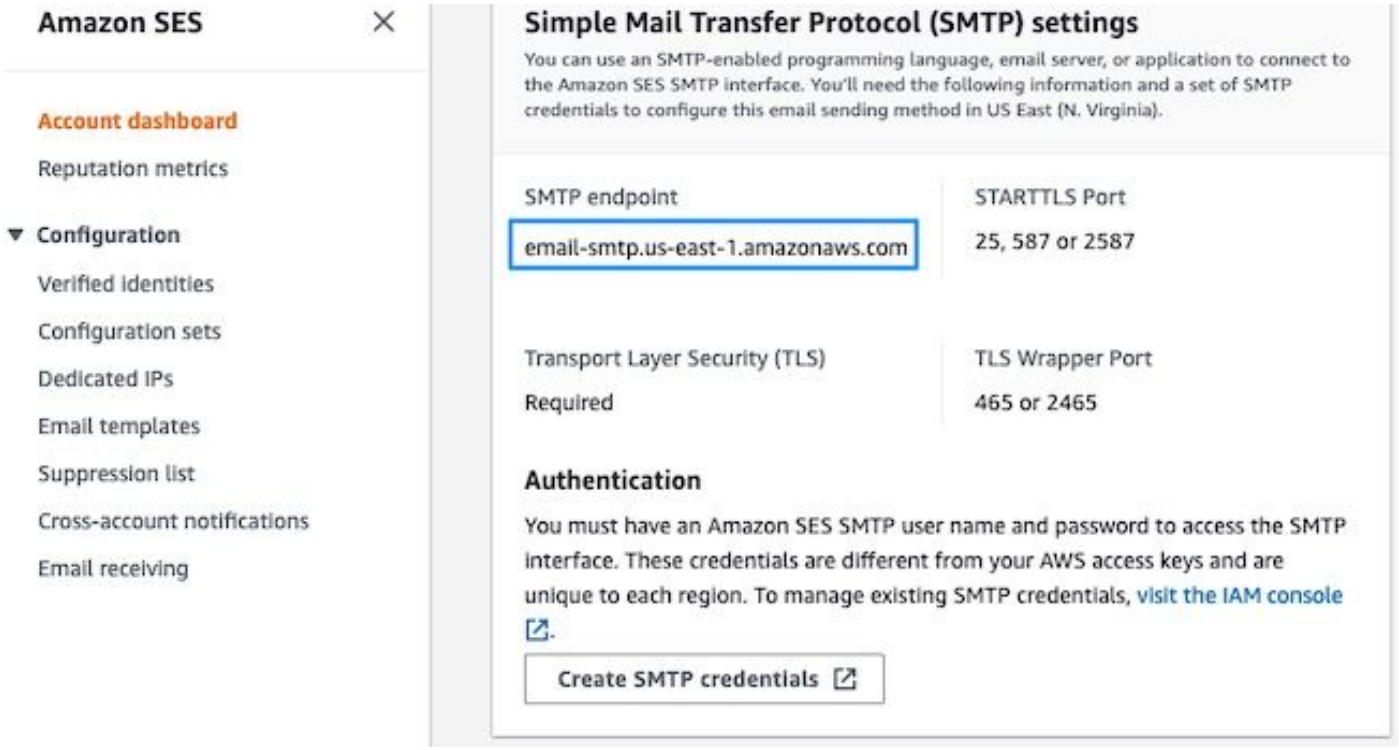
注：サンドボックスにあるAWS SESは許容されますが、サンドボックス環境の制限に注意してください。https://docs.aws.amazon.com/ses/latest/dg/request-production-access.html

AWSコンソールで、 **Amazon SES**を選択し、 **Configuration** をクリックし、 **Verified Identities.**

確認済みのドメインが必要です。確認された電子メールアドレスは必要ありません。AWSのドキュメントhttps://docs.aws.amazon.com/ses/latest/dg/creating-identities.html#verify-domain-procedure



SMTPエンドポイントの場所をメモします。この値は後で必要になります。



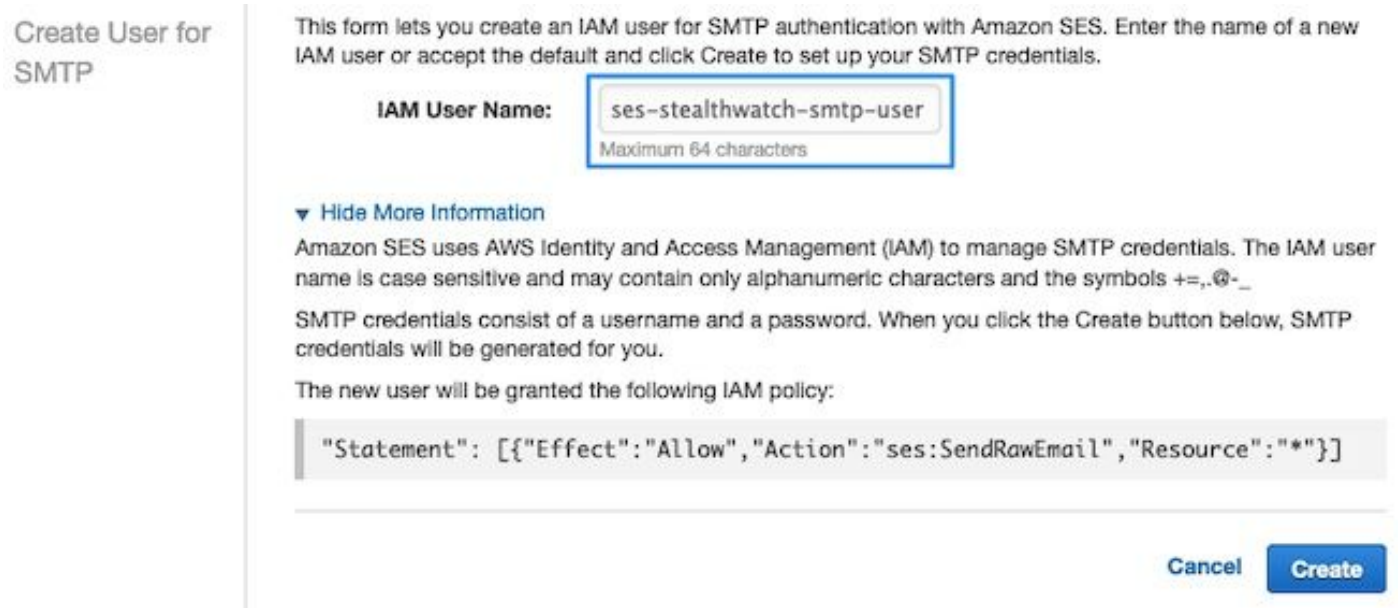
Aws SES SMTP認証情報の作成

AWSコンソールで、 **Amazon SES**をクリックし、 **Account Dashboard**.

下にスクロールして「**Simple Mail Transfer Protocol (SMTP) settings**」をクリックし、 **Create SMTP Credentials** この設定を完了する準備ができたら、

古い未使用のクレデンシャル（約45日）では、無効なクレデンシャルとしてエラーが発生しないようです。

この新しいウィンドウで、ユーザ名を任意の値に更新し、 **Create**.

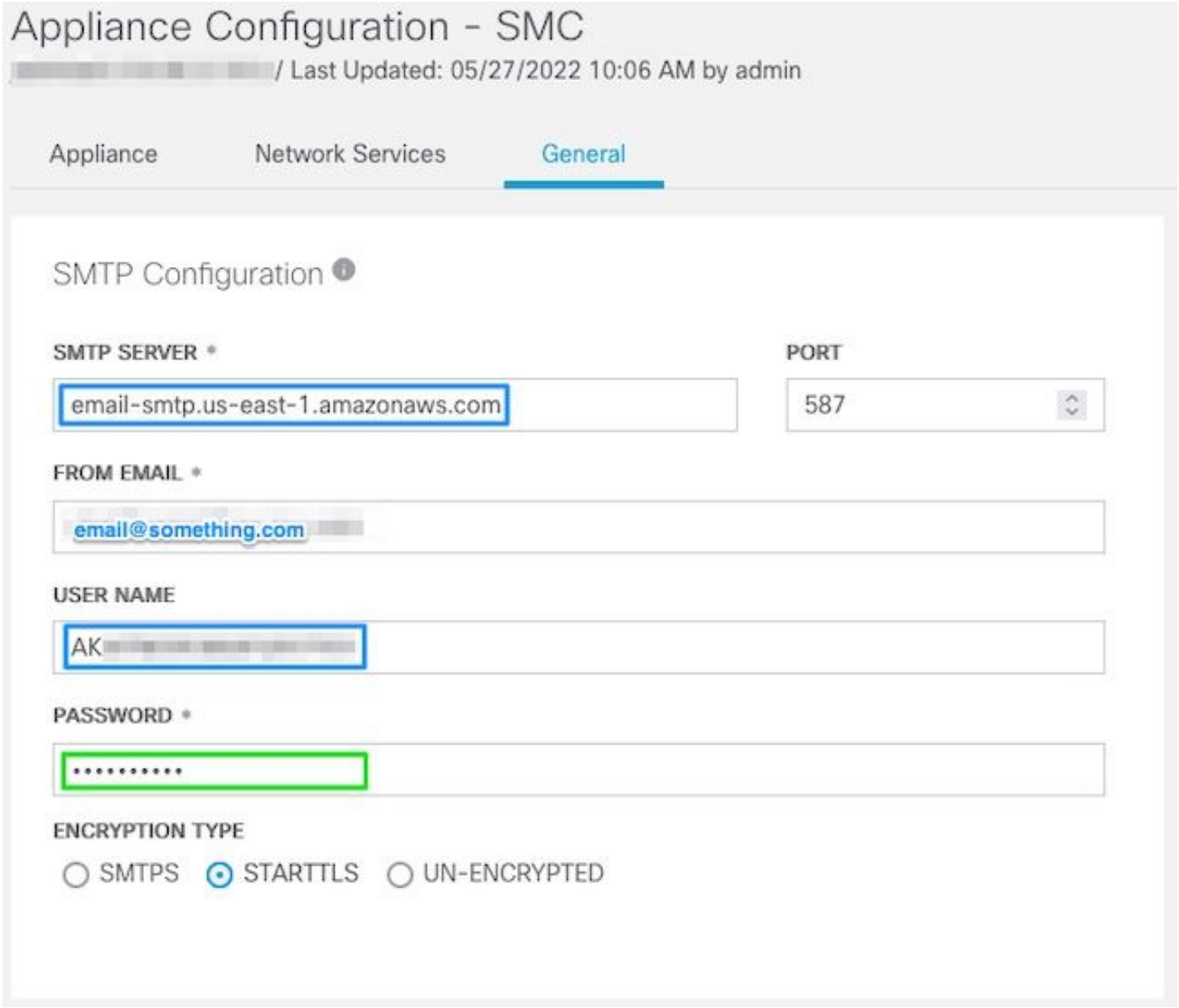


ページにクレデンシャルが表示されたら、保存します。このブラウザタブは開いたままにしておきます。

SNAマネージャSMTP設定の設定

Cisco Unified Communications Managerにログインし、 **SNA Manager**、およびopen **SMTP Notifications** セクションの「EULA not accepted」を確認します。

1. 開く **Central Management > Appliance Manager.**
2. ポリシーの横の [レポート（Report）] **Actions** アプライアンスのメニュー。
3. 選択 **Edit Appliance Configuration.**
4. 次のいずれかを選択します。 **General** tab.
5. 下にスクロールして **SMTP Configuration**
6. AWSから収集した値を入力します **SMTP Server**:これはSMTPエンドポイントの場所で、 **SMTP Settings AWS SES Account Dashboard** page**Port**:25、587、または2587と入力します。**From Email**:このフィールドには、IPアドレスを含む **AWS Verified DomainUser Name**:これは、 **Review AWS SES Configuration** セクションの「EULA not accepted」を確認します。**Password**:これは、 **Review AWS SES Configuration** セクションの「EULA not accepted」を確認します。**Encryption Type**:[STARTTLS]を選択します（[SMTPS]を選択した場合は、ポートを465または2465に編集します）。
7. 設定を適用し、 **SNA Manager** ネットワークに戻る **UP** 状態 **Central Management**



AWS証明書の収集

SSHセッションを確立し、 **SNA Manager**ルートユーザとしてログインします。

次の3つの項目を確認します

- SMTPエンドポイントの場所を変更します(email-smtp.us-east-1.amazonaws.comなど)。
- 使用するポートを変更します（たとえば、STARTTLSのデフォルトは587）。
- コマンドにはSTDOUTが含まれず、完了時にプロンプトが返されます

STARTTLS（デフォルトポート587）の場合：

```
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
```

SMTPS（デフォルトポート465）の場合：

```
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 -t1 *.pem`; do cp $i
$(awk -F "CN=" '/s:/ {gsub(/ /,x ); print $NF}' $i).pem ; done ; rm -f cacert* mycertfile.crt
```

pem拡張子が付いた証明書ファイルは、このディレクトリではなく、現在の作業ディレクトリに作成されます（pwdコマンドの出力/最終行）

```
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 -t1 *.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
```

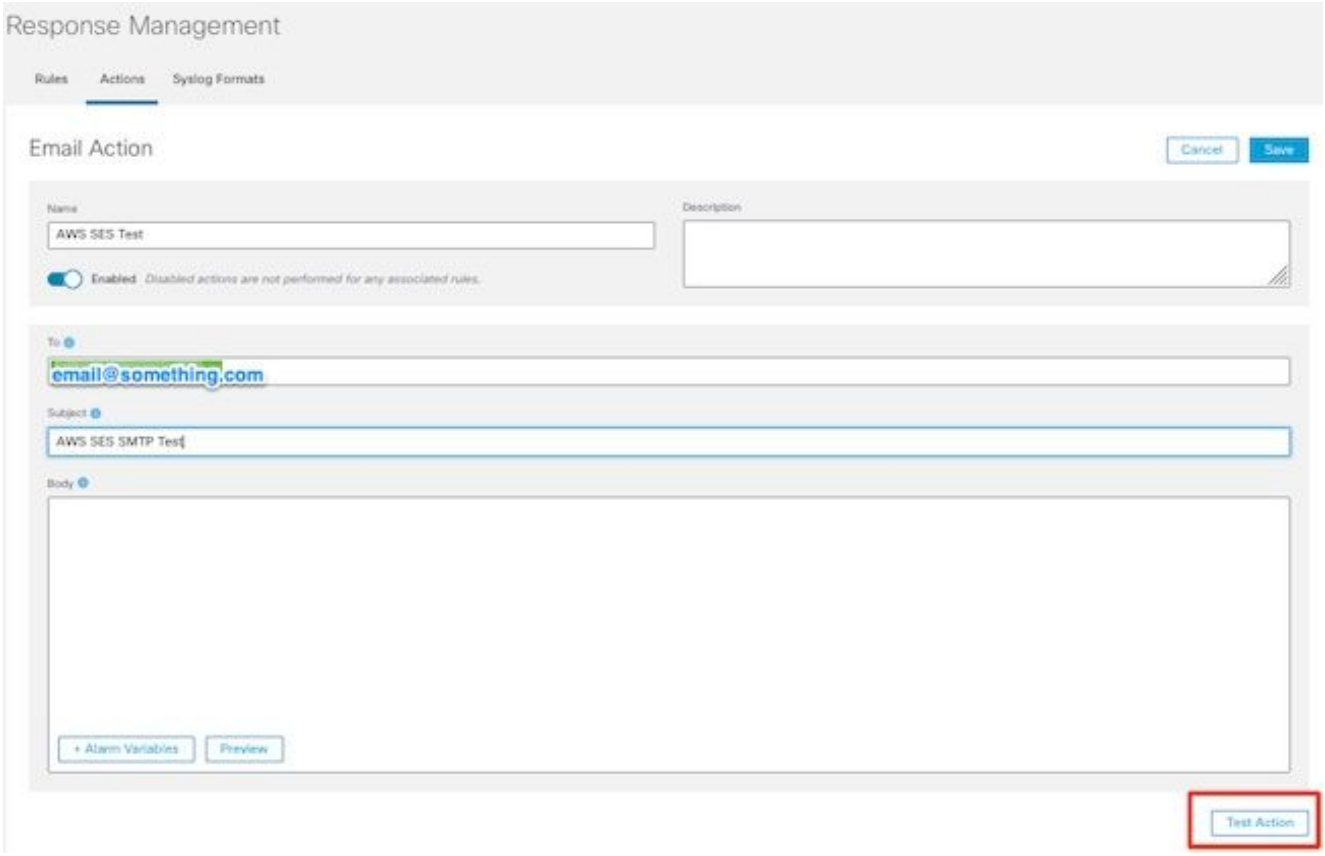
Cisco IOSソフトウェアリリース12.1Tで作成された **SNA Manager** 選択したファイル転送プログラム（Filezilla、winscpなど）を使用してローカルマシンにアクセスし、これらの証明書を **SNA Manager trust store** イン **Central Management.**

1. 開く **Central Management > Appliance Manager.**
2. ポリシーの横の [レポート（Report）] **Actions** アプライアンスのメニュー。
3. 選択 **Edit Appliance Configuration.**
4. 次のいずれかを選択します。 **General** tab.
5. 下にスクロールして **Trust Store**
6. 選択 **Add New**
7. それぞれの証明書をアップロードします。ファイル名を **Friendly Name**

応答管理の電子メールアクションの構成

Cisco Unified Communications Managerにログインし、 **SNA Manager**をクリックし、 **Response Management** セクションの「EULA not accepted」を確認します。

1. 次のいずれかを選択します。 **Configure** 画面上部のメインリボンのタブ
2. 選択 **Response Management**
3. **Response Management** ページ、選択 **Actions** tab
4. 選択 **Add New Action**
5. 選択 **Email**この電子メールアクションの名前を指定します受信者のメールアドレスを[To]フィールドに入力します（AWS SESで確認されたドメインに属している必要があります）。件名は何でもかまいません。

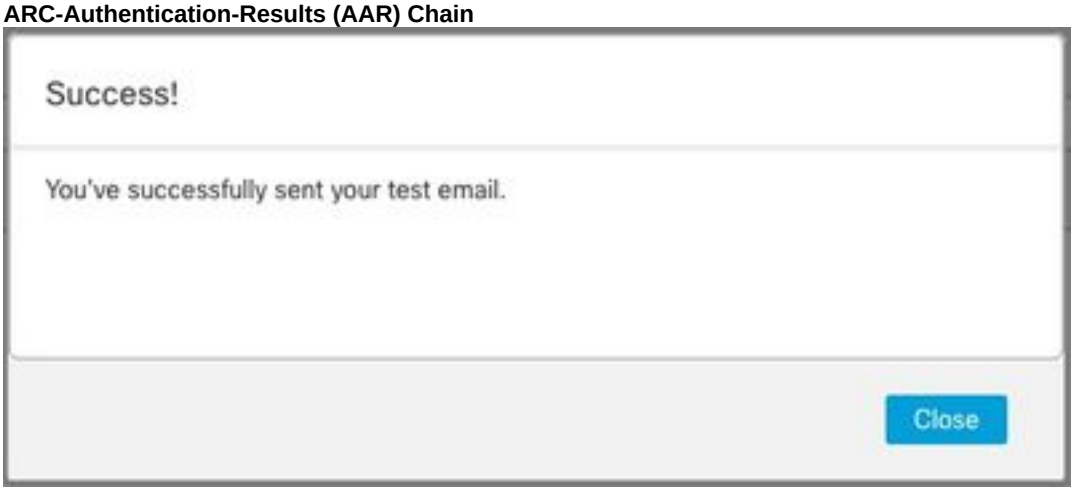


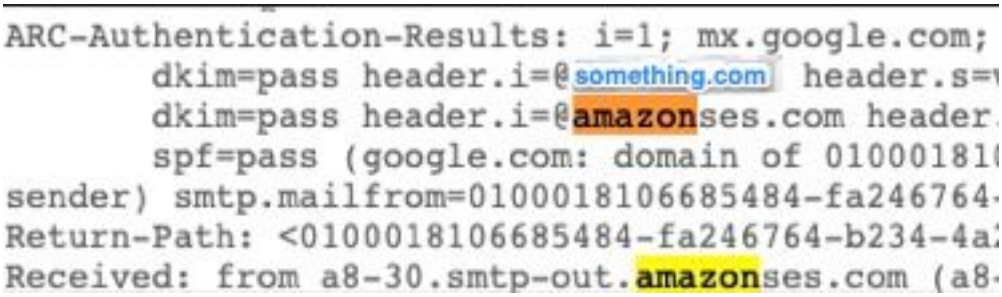
6. クリック **Save**

確認

Cisco Unified Communications Managerにログインし、 **SNA Manager**をクリックし、 **Response Management** セクション：

1. 次のいずれかを選択します。 **Configure** 画面上部のメインリボンのタブ
2. 選択 **Response Management**
3. **Response Management** ページ、選択 **Actions** tab
4. 省略記号を **Actions** で設定した電子メールアクションの行の列 **Configure Response Management Email Action** を選択し、 **Edit.**
5. 選択 **Test Action** 設定が有効であれば、成功メッセージが表示され、電子メールが配信されます。
   電子メールヘッダーの中で、amazonsesは" **Received**」フィールドとamazonsesに加え、 **ARC-Authentication-Results (AAR) Chain**





6. テストに失敗した場合は、画面上部にバナーが表示されます。トラブルシューティングセクションに進みます

トラブルシュート

「 **/lancope/var/logs/containers/sw-reponse-mgmt.log** ファイルには、テストアクションのエラーメッセージが含まれています。最も一般的なエラーと修正を表に示します。
表に示されているエラーメッセージは、エラーログ行の一部に過ぎないことに注意してください

エラー	修正
SMTPSendFailedException:554 Message rejected:メールアドレスが確認されていません。IDがリージョンUS-EAST-1のチェックに失敗しました。{email_address}	SNA ManagerSMTP設定の「From Email」をAWS SES検証済みドメインに属する電子メールに更新します
AuthenticationFailedException:535認証資格情報が無効です	セクション「AWS SES SMTP認証情報の作成」SNA Manager SMTP設定の設定」を繰り返します
SunCertPathBuilderException:要求されたターゲットへの有効な証明パスが見つかりません	AWSから提示されたすべての証明書がSNA Manager信頼ストアにあることを確認します。**テストアクション**の実行時にパケットキャプチャを実行サーバ側から提示された証明書を信頼ストアの内比較します。
SSLルーチン：tls_process_ske_dhe:dhキーが小さすぎます	別紙を参照
その他のエラー	TACケースを開いて確認する

付録:DHキーが小さすぎます。

これはAWS側の問題です。DHEとEDHの暗号を使用する場合（ログが詰まる可能性がある）、1024ビットキーを使用し、SNAマネージャがSSLセッションの続行を拒否します。コマンド出力には、DHE/EDH暗号が使用されている場合のopenssl接続からのサーバの一時キーが表示されます。

```
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
```

唯一の回避策は、SMCでrootユーザとしてコマンドを使用してすべてのDHEおよびEDH暗号を削除することです。AWSはECDHE暗号スイートを選択し、接続が成功します。

```
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_SHA2
56: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
```

関連情報

- 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
- テクニカル サポートとドキュメント – Cisco Systems