Cisco Secure Email Gatewayとのセキュリティ認識統合の設定

内容

はじめに

このドキュメントでは、Cisco Security Awareness(CSA)とCisco Secure Email Gatewayの統合を設定するために必要な手順について説明します。

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。

- Cisco Secure Email Gatewayの概念と設定
- CSAクラウドサービス

使用するコンポーネント

このドキュメントの情報は、AsyncOS for SEG 14.0以降に基づくものです。

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たものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。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。

CSAクラウドサービスからのフィッシングシミュレーションの作成と送信

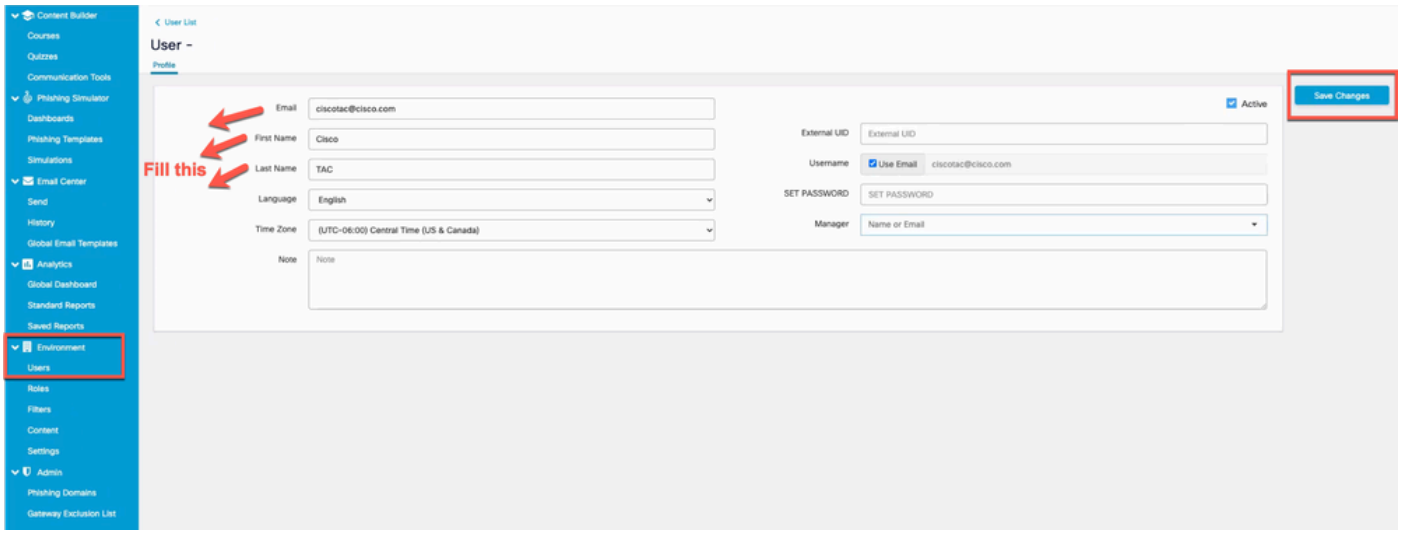
ステップ 1：CSAクラウドサービスにログインします。

次を参照してください。
1. https://secat.cisco.com/（南・北・中央アメリカ）地域

2. https://secat-eu.cisco.com/（ヨーロッパ地域）

ステップ 2フィッシングメール受信者の作成

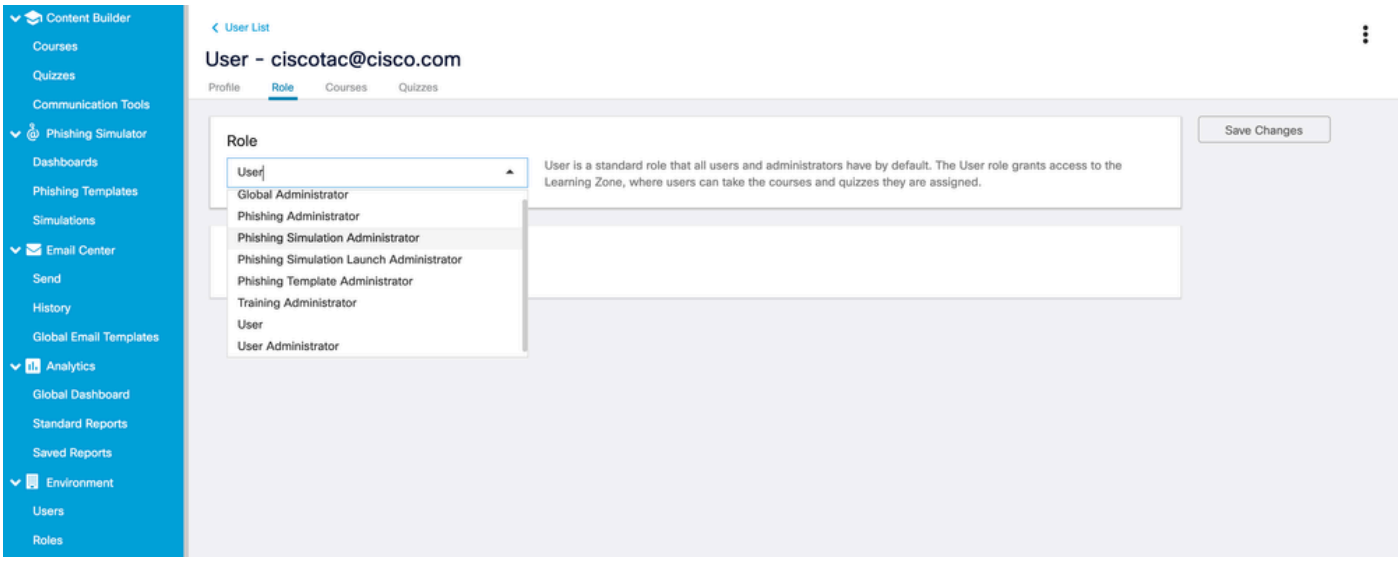
Environment > **Users** > **Add New User**の順に移動し、Email、First Name、Last Name、およびLanguageの各フィールドに入力してから、図に示すように**Save** Changesをクリックします。



新しいユーザを追加するためのユーザインターフェイスページのスクリーンショット

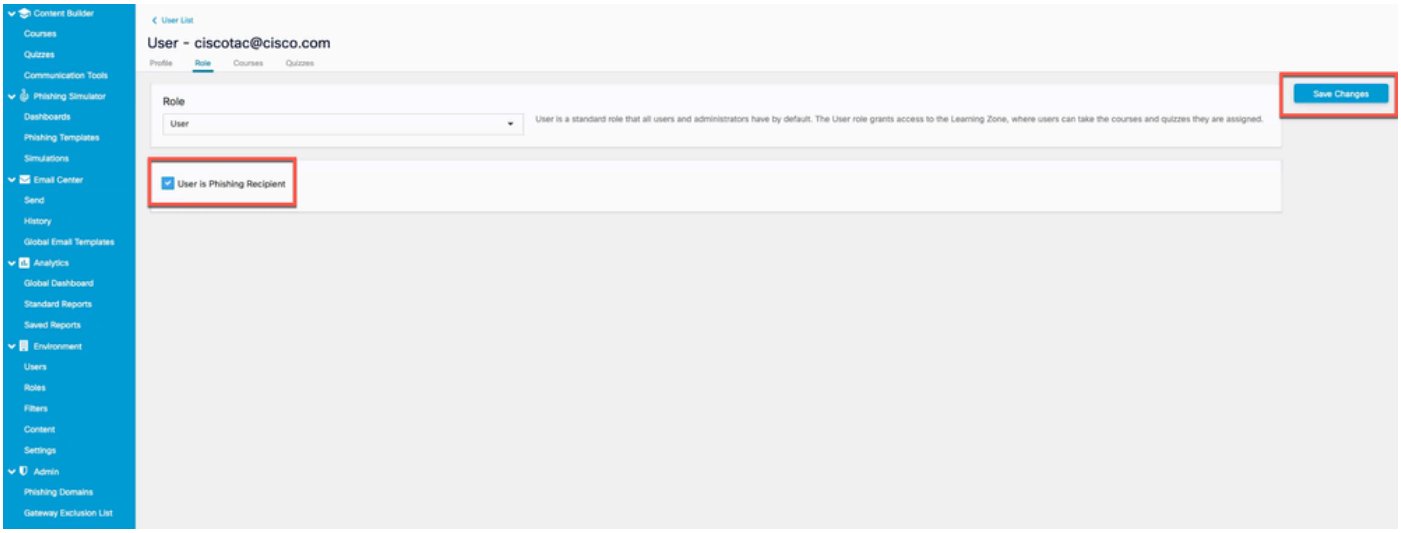
注：パスワードを設定する必要があるのは、シミュレーションの作成と起動を許可されたCSA管理者ユーザだけです。

ユーザのロールは、ユーザの作成後に選択できます。次の図に示すように、ドロップダウンからロールを選択できます。



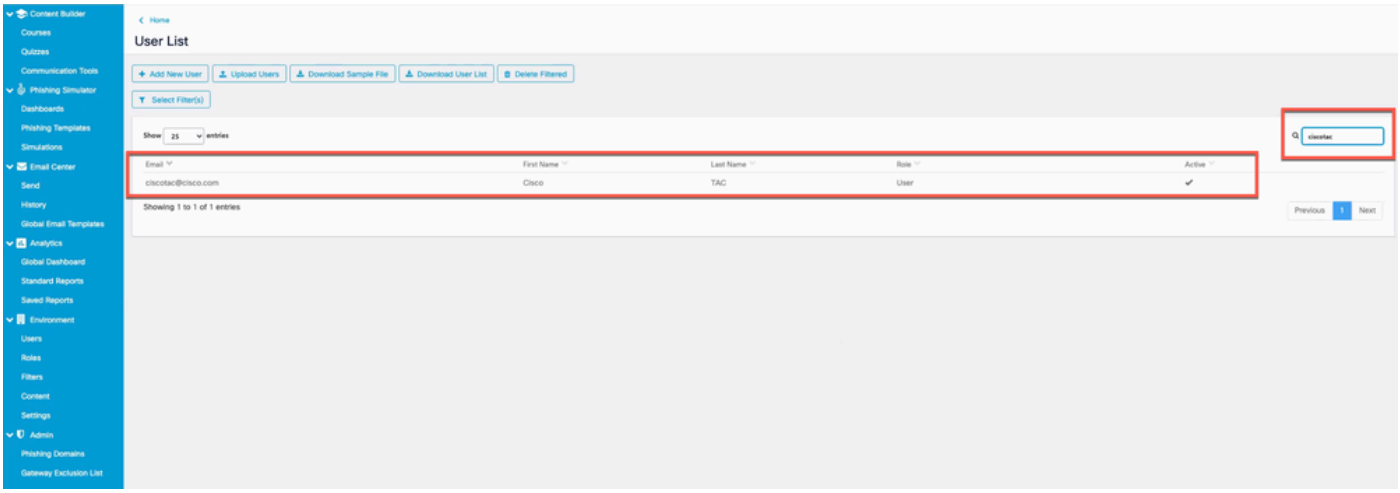
ユーザロールのドロップダウンオプションの表示

次の図に示すように、User is Phishing Recipient > Save Changesasチェックボックスをオンにします。



「ユーザがフィッシング受信者である」チェックボックスが有効になっていることを示すスクリーンショット

図に示すように、ユーザが正常に追加され、フィルタの電子メールアドレスに基づいて検索された際にリストされることを確認します。

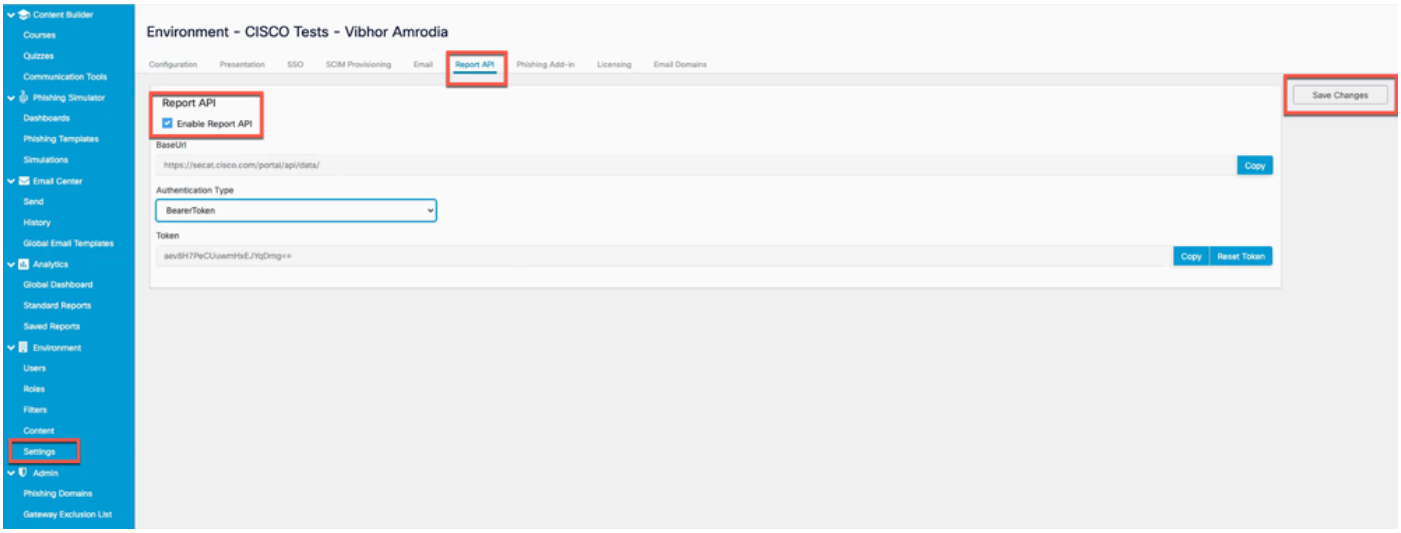


ユーザリストの新規ユーザのスクリーンショット

ステップ 3レポートAPIの有効化

Environments > Settings > Report APIタブに移動し、checkEnable Report API > Save Changesにチェックマークを付けます。

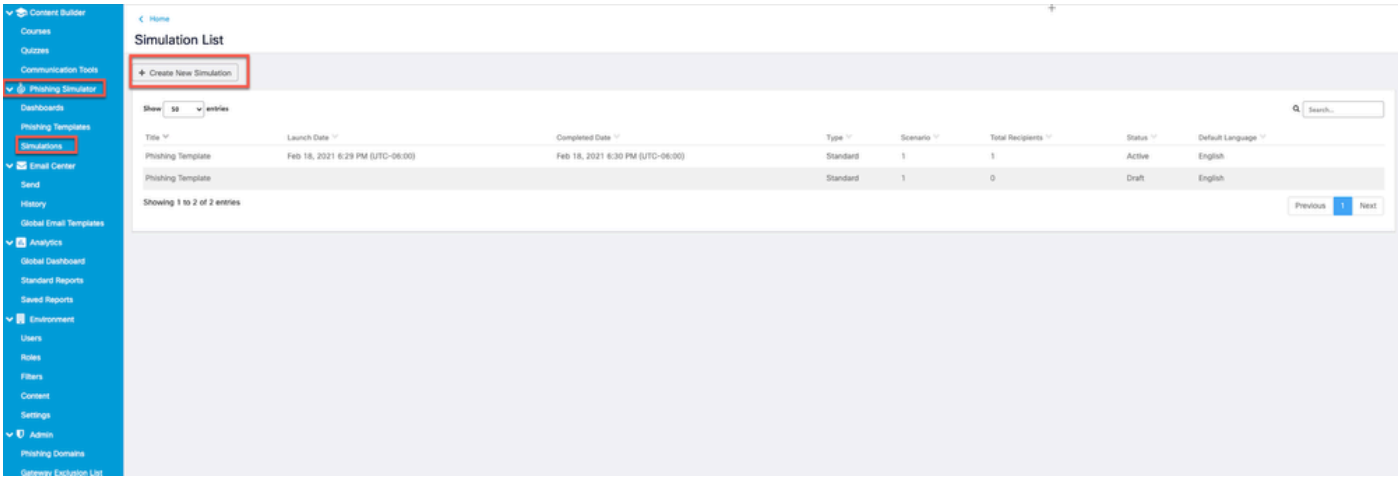
注：ベアラトークンをメモします。SEGをCSAに統合するには、これが必要です。



「レポートAPIを有効にする」チェックボックスが有効になっていることを示すスクリーンショット

ステップ 4フィッシングのシミュレーションの作成

a. Phishing Simulator > Simulations > Create New Simulationの順に選択し、図に示すように利用可能なリストからTemplateを選択します。

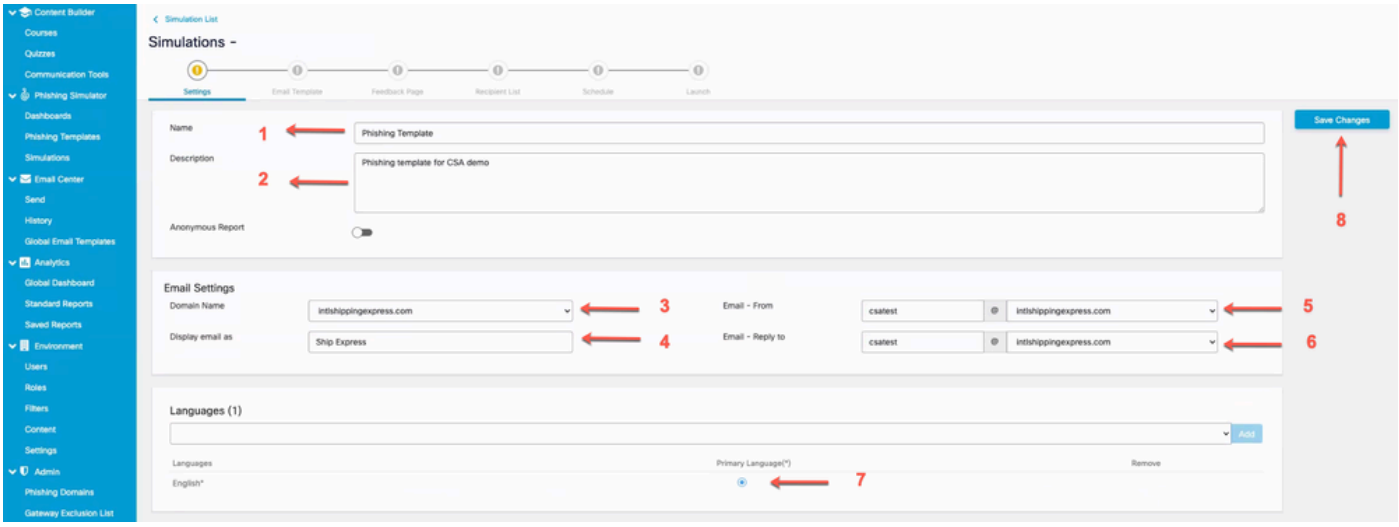


「新しいシミュレーションの作成」ボタンを強調表示するスクリーンショット

b.次の情報を入力します。

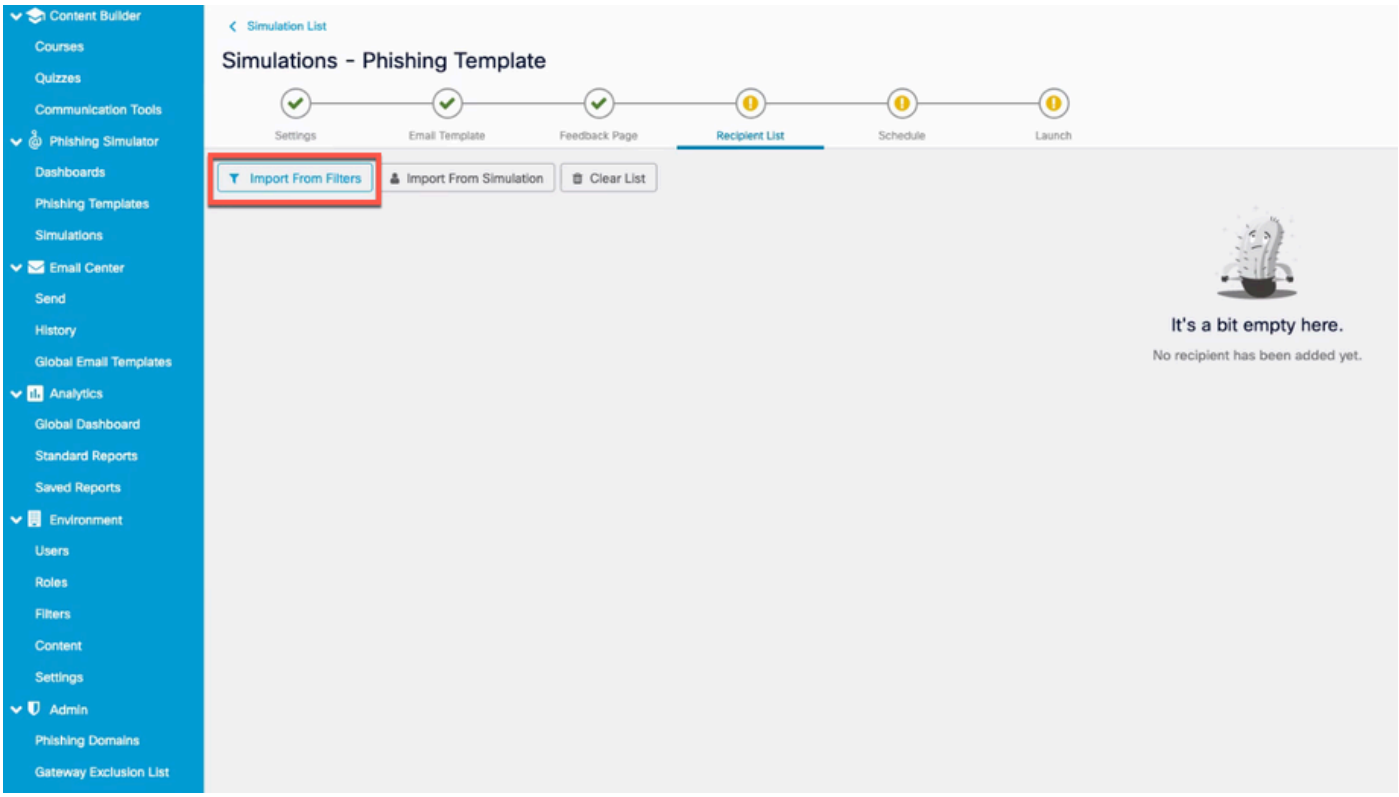
1. テンプレートの名前を選択します。

2. テンプレートについて説明します。
3. フィッシングメールの送信に使用されるドメイン名。
4. フィッシングメールの表示名。
5. 電子メール送信者のアドレス (ドロップダウンから選択) 。
6. 返信先住所 (ドロップダウンから選択)
7. [Language] を選択します。
8. 変更を保存します。



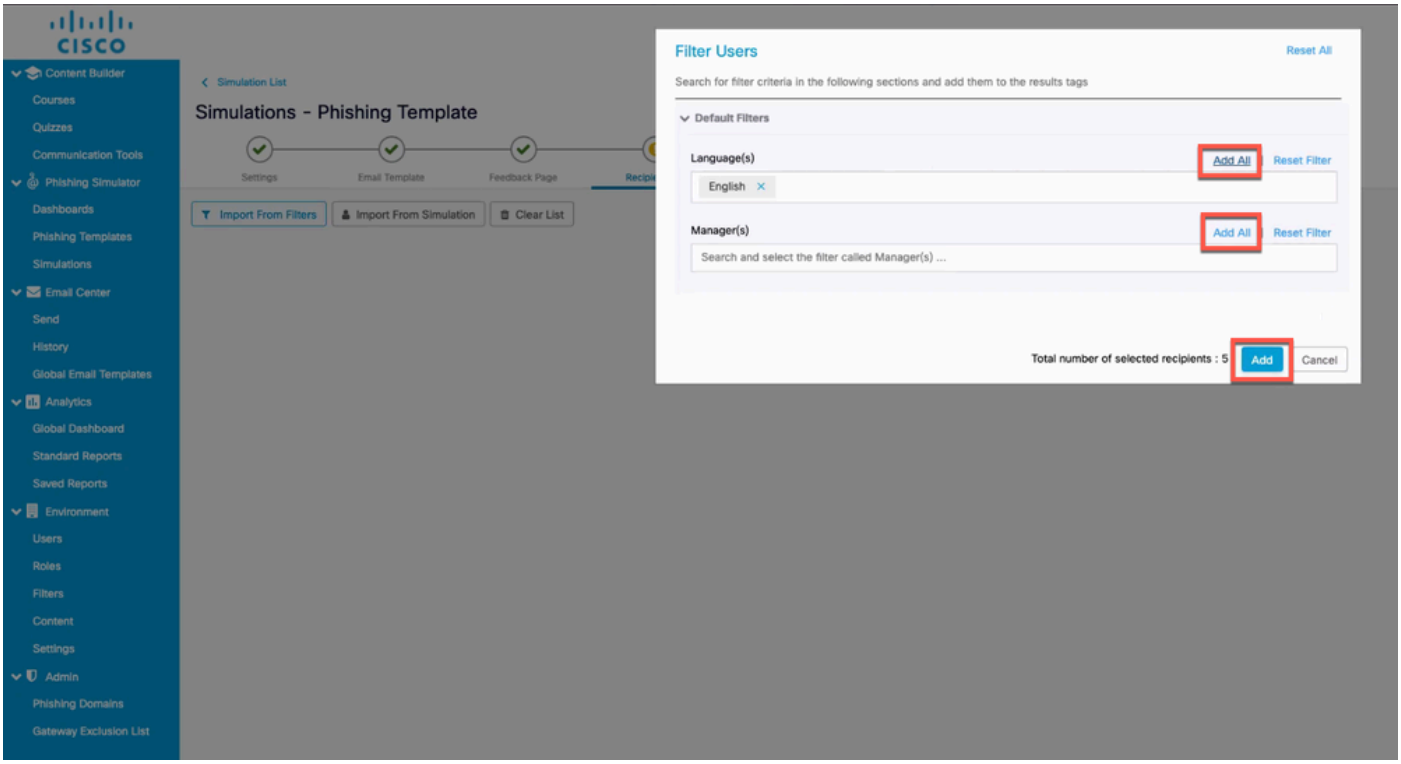
新しいシミュレーションの構成に入力する必要があるフィールドを強調表示するスクリーンショット

c. Import from Filtersをクリックし、図のように、フィッシングメールの受信者を受信者リストに追加します。



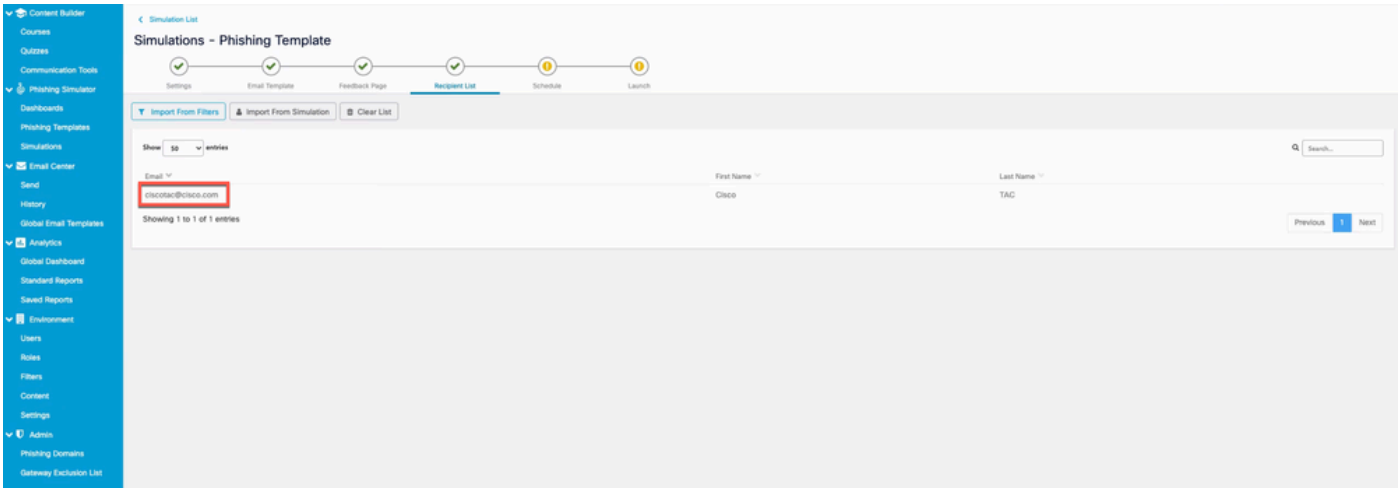
「フィルタからのインポート」ボタンを強調表示するスクリーンショット

言語またはマネージャでユーザをフィルタリングできます。図に示すように、Addをクリックします。



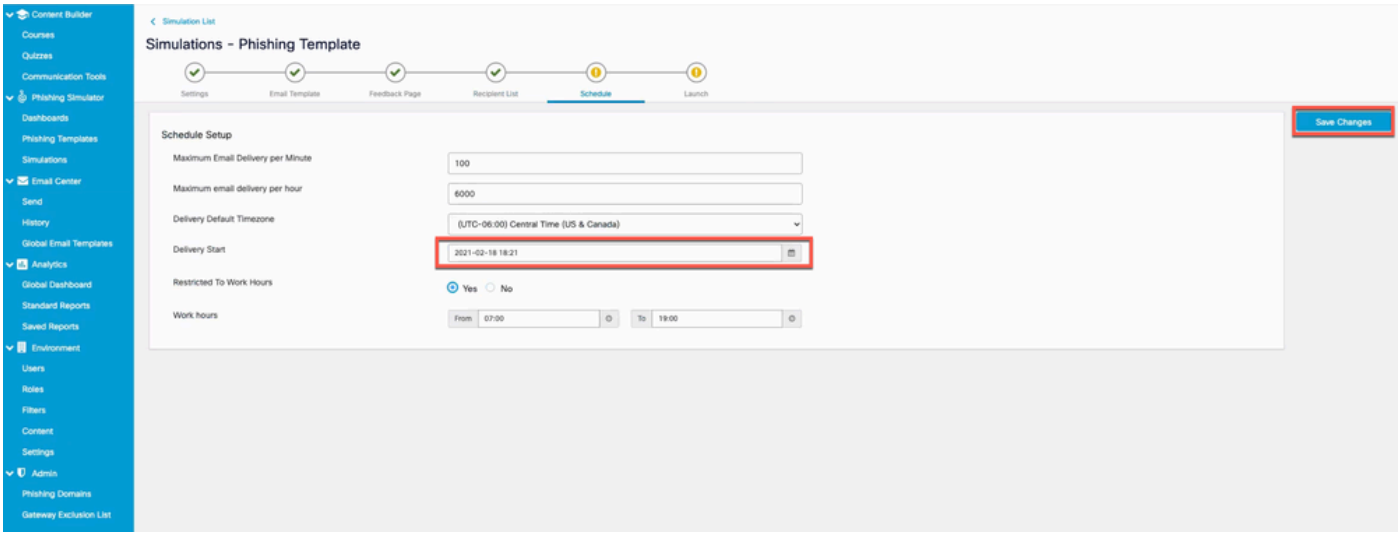
言語またはマネージャによるフィルタリング用の[フィルタユーザ]ダイアログボックスのスクリーンショット

次の図に、ステップ2で作成し、受信者リストに追加したユーザの例を示します。



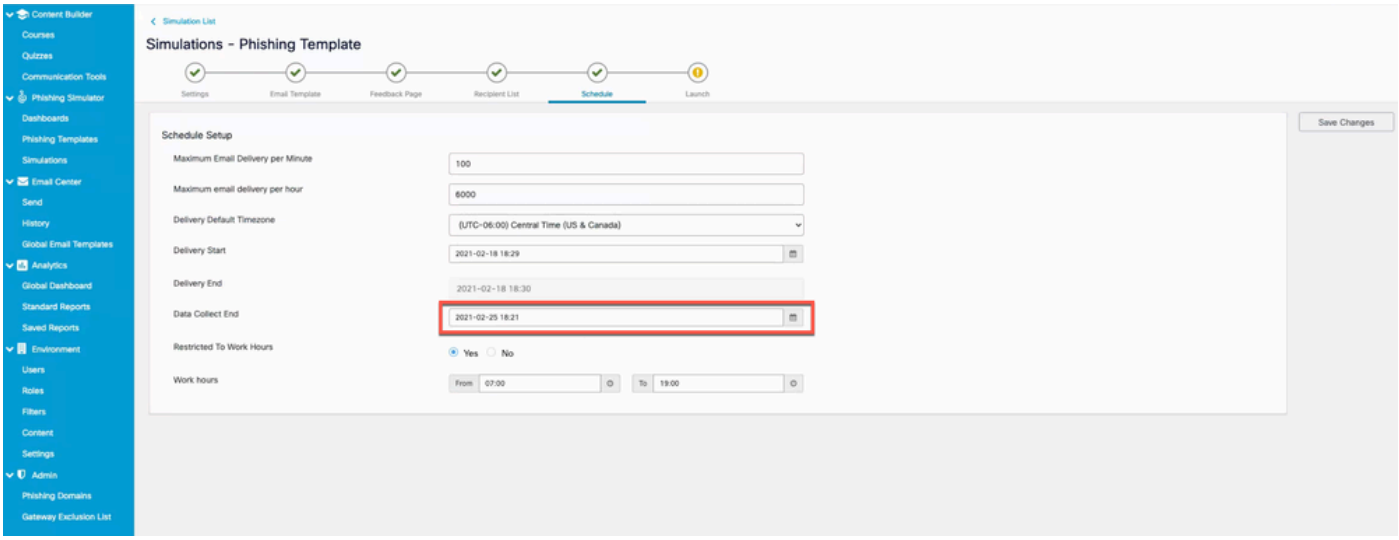
フィッシングシミュレーションの受信者としてリストされている、以前作成したユーザのスクリーンショット

d.図に示すように、配信の開始日と保存の変更を設定してキャンペーンをスケジュールします。



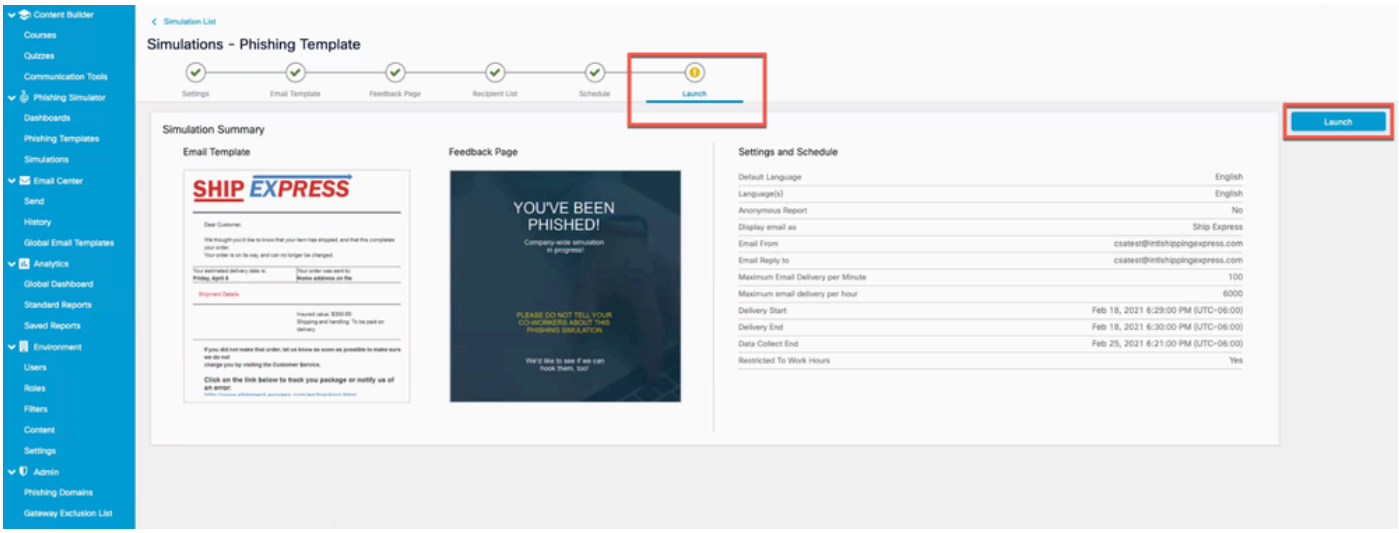
配信開始フィールドを強調表示するスクリーンショット

開始日を選択すると、図に示すように、キャンペーンの終了日を選択するオプションが有効になります。



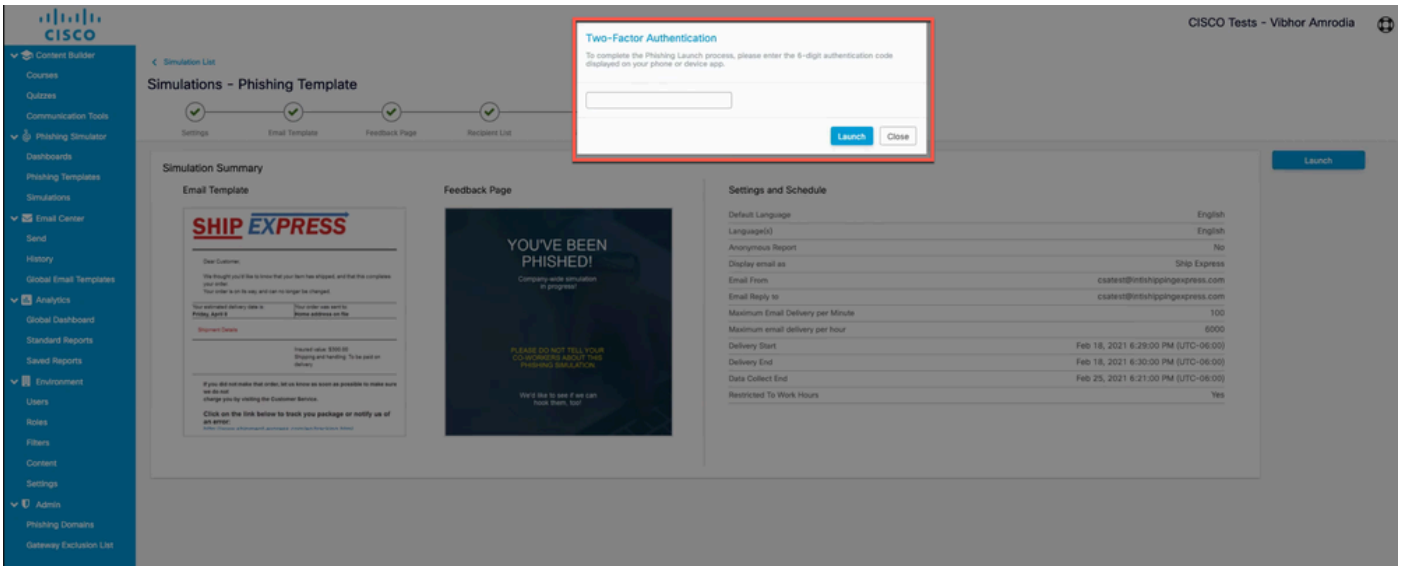
シミュレーションを終了するタイミングを指定するデータ収集終了フィールドを強調表示したスクリーンショット

e.図に示すように、Launchをクリックしてキャンペーンを開始します。



キャンペーンを起動できるシミュレーション作成ウィザードの最後のタブのスクリーンショット

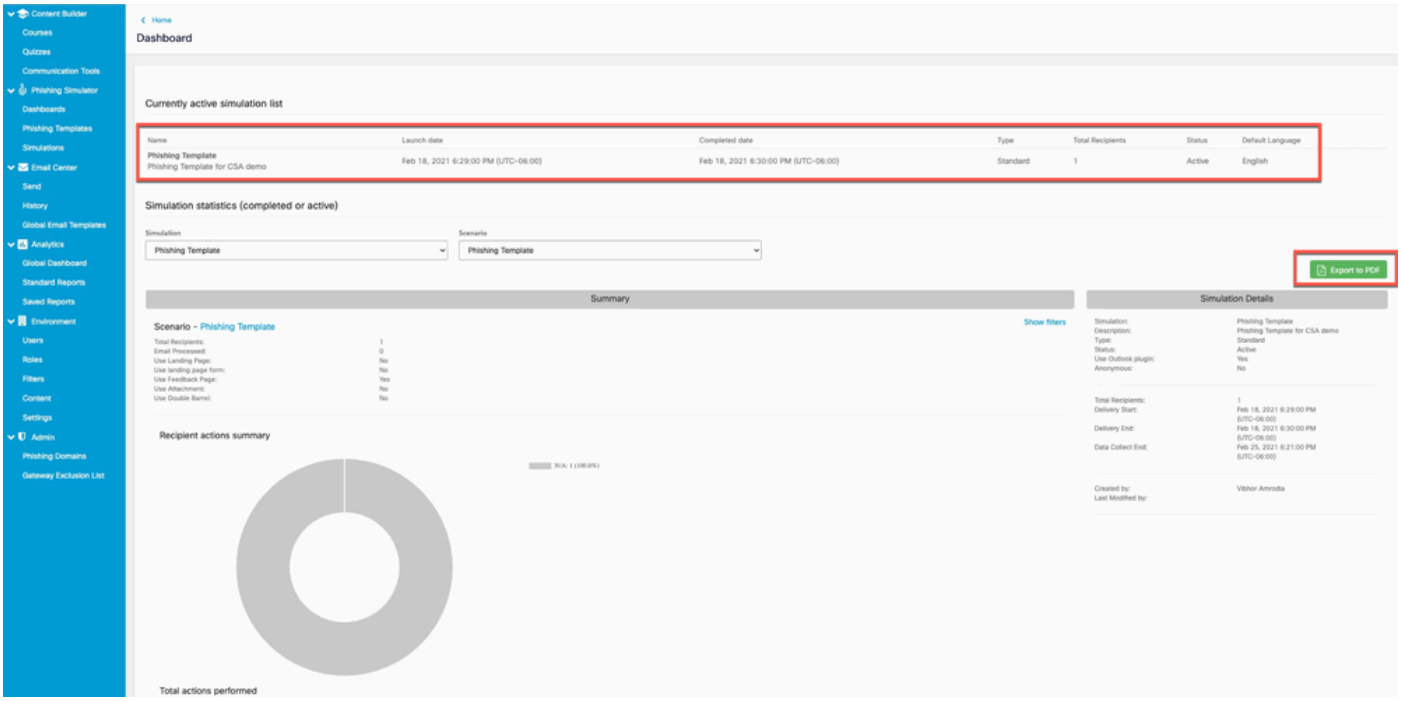
起動ボタンをクリックした後に、2要素認証コードを要求できます。コードを入力し、図に示すようにLaunchasをクリックします。



2要素認証コードを求めるポップアップのスクリーンショット

ステップ 5アクティブなシミュレーションの検証

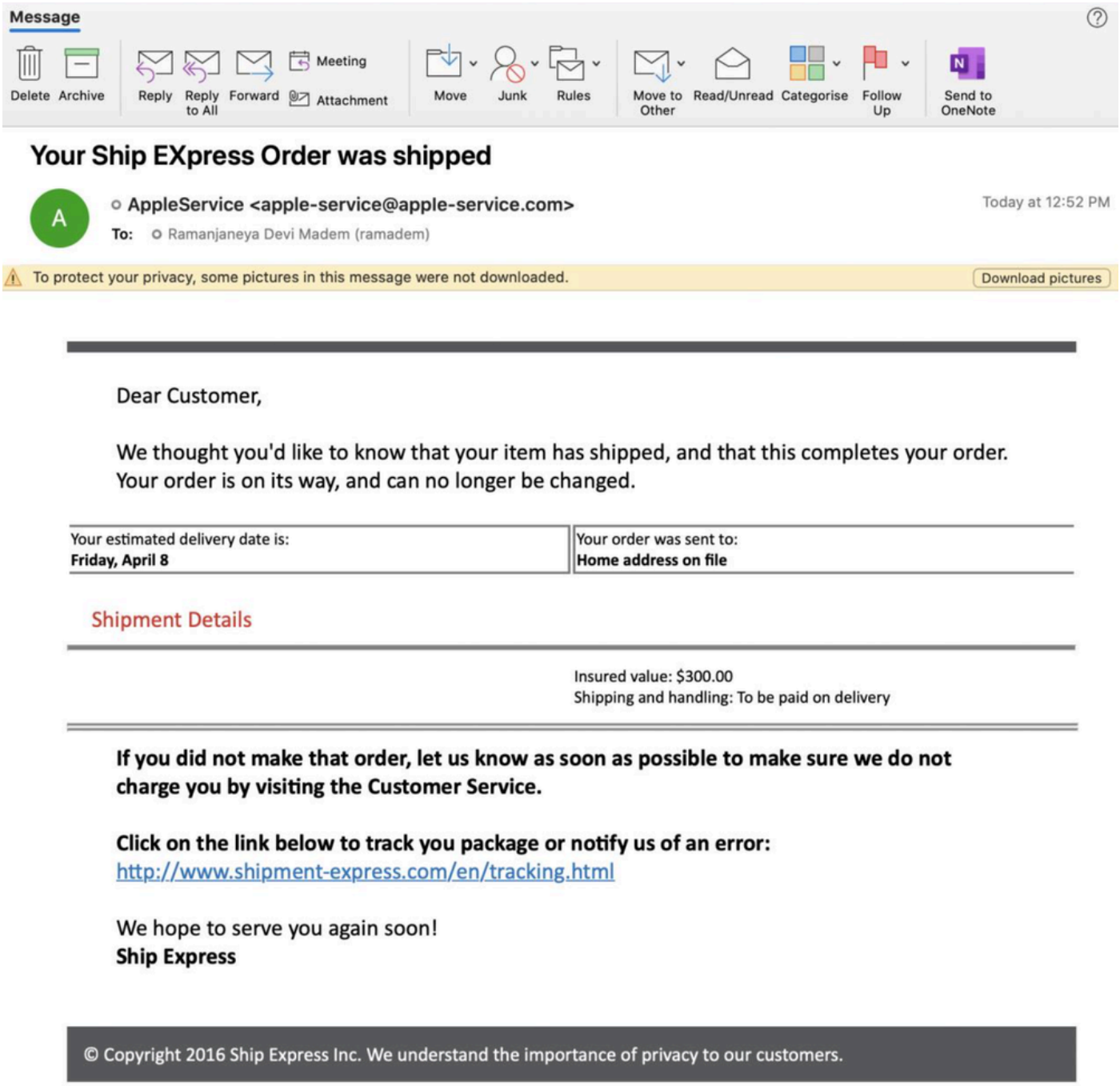
Phishing Simulator > Dashboardsの順に移動します。現在アクティブなシミュレーションリストには、アクティブなシミュレーションが表示されます。Export as PDFをクリックして、図に示すように同じレポートを取得することもできます。



フィッシングシミュレーションダッシュボードのスクリーンショット

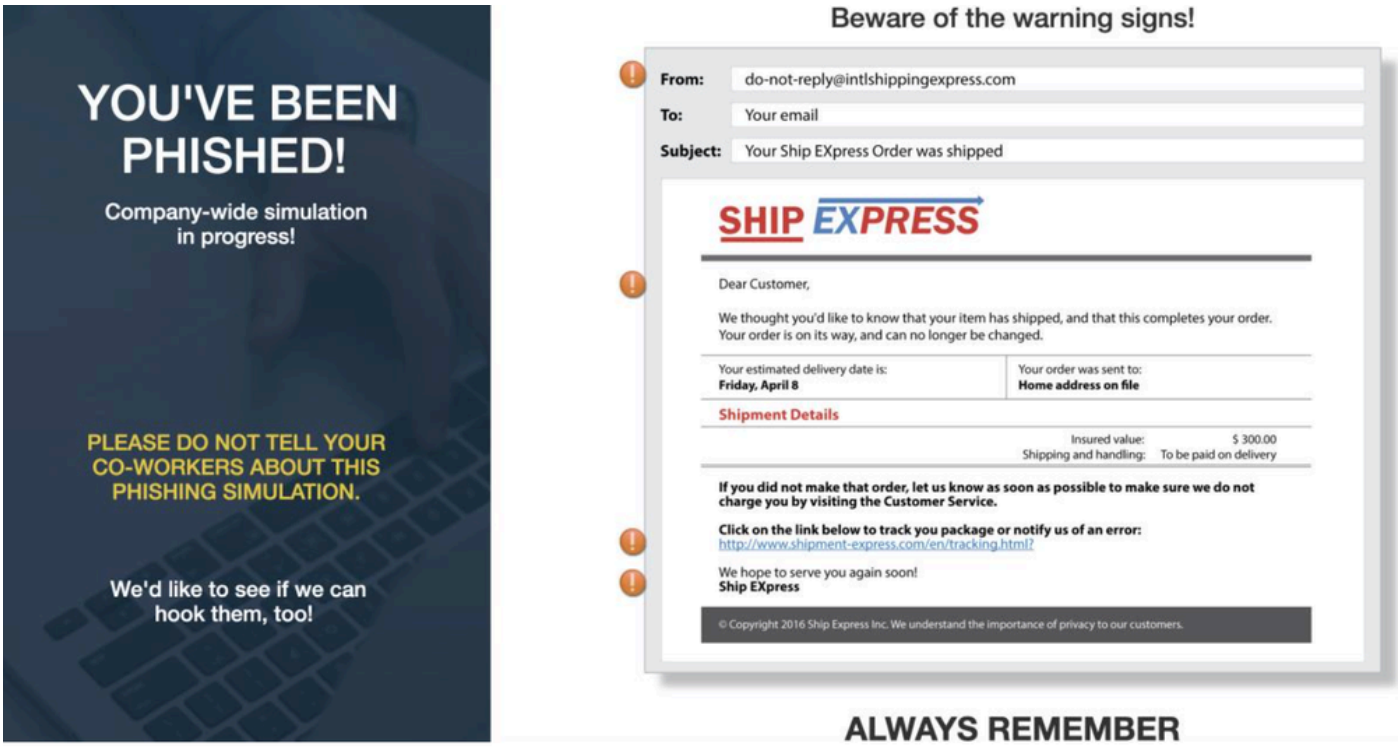
受信者の側に何が表示されますか。

受信箱のフィッシングシミュレーションメールの例。



ユーザメールボックス内のフィッシング電子メールの例

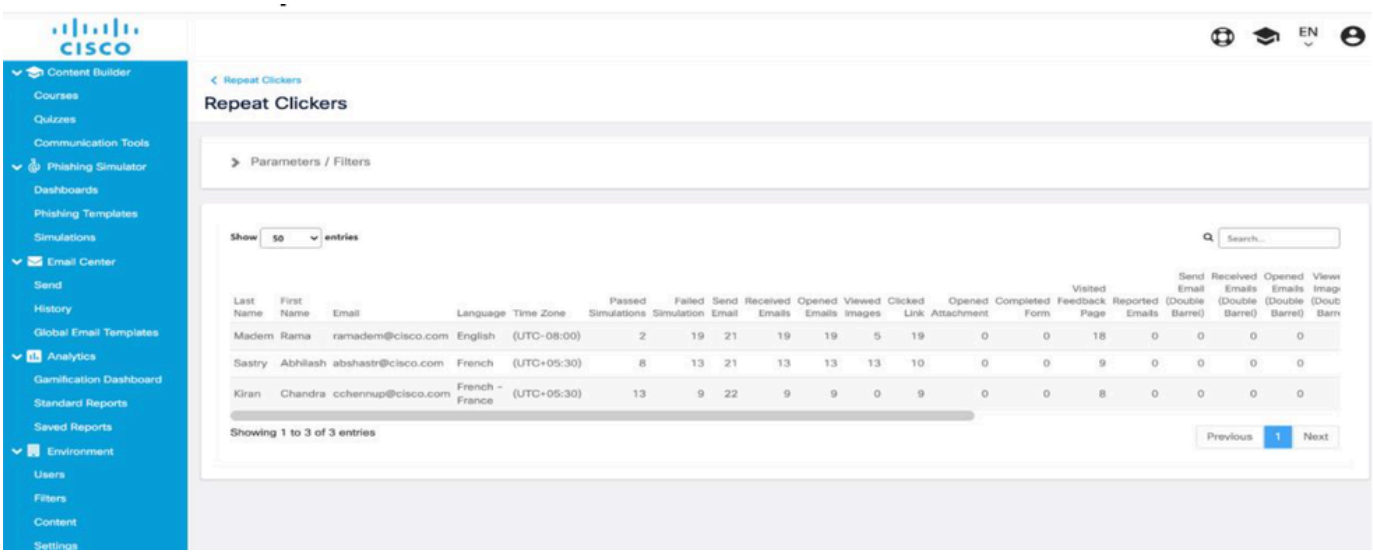
受信者がURLをクリックすると、このフィードバックページがユーザに表示され、このユーザがCSAのRepeat Clickersリスト（フィッシングURLを自由にクリックしたユーザ）の一部として表示されます。



フィッシング電子メールのURLをクリックすると表示されるフィードバックページの例

CSAでの確認

繰り返しクリックのリストは、図に示すように、**[分析]** > **[標準レポート]** > [フィッシングのシミュレーション] > **[繰り返しクリックリスト]**の下に表示されます。

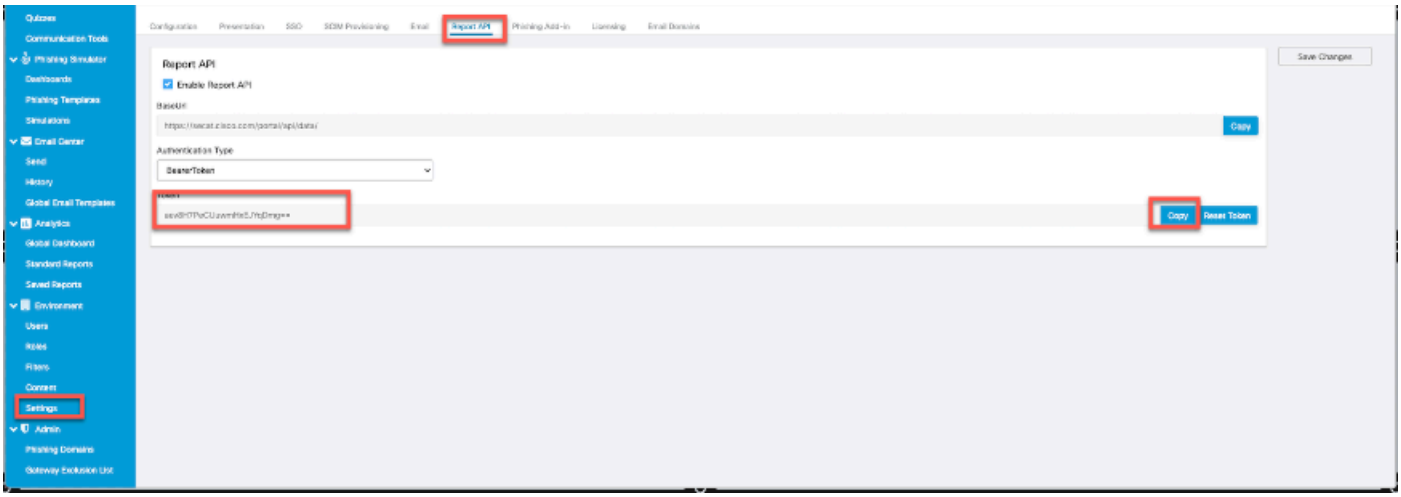


Repeat Clickersページのスクリーンショット

セキュアなEメールゲートウェイの設定

注：「CSAクラウドサービスからのフィッシングシミュレーションの作成と送信」セクションの手順3.で、Report APIを有効にすると、bearerトークンをメモしたことになります。これを手元に置い

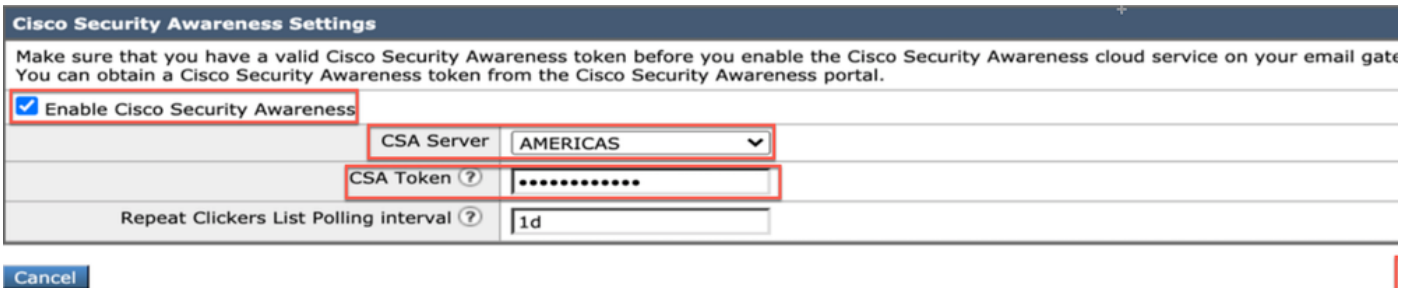
ておいて。



管理者がbearerトークンを見つけることができるレポートAPIのページのスクリーンショット

ステップ 1：Secure Email GatewayでCisco Security Awareness機能を有効にする

Secure Email GatewayのGUIで、Security Services > Cisco Security Awareness > Enable の順に移動します。リージョンとCSAトークン（前述の注に示すようにCSAクラウドサービスから取得したベアラトークン）を入力し、変更を送信して確定します。



Cisco Secure Email GatewayのCisco Security Awareness Settingsページのスクリーンショット

CLI での設定

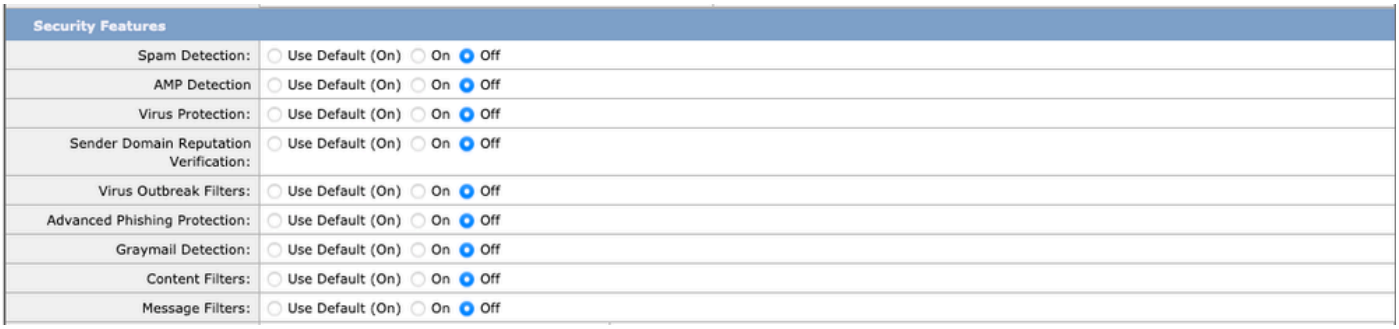
csaconfig と入力して、CLIからCSAを設定します。

```
ESA (SERVICE)> csaconfig


Choose the operation you want to perform:
- EDIT - To edit CSA settings
- DISABLE - To disable CSA service
- UPDATE_LIST - To update the Repeat Clickers list
- SHOW_LIST - To view details of the Repeat Clickers list
[]> edit

Currently used CSA Server is: https://secat.cisco.com
Available list of Servers:
1. AMERICAS
```

```
2. EUROPE
Select the CSA region to connect
[1]>

Do you want to set the token? [Y]>

Please enter the CSA token for the region selected :
The CSA token should not:
- Be blank
- Have spaces between characters
- Exceed 256 characters.

Please enter the CSA token for the region selected :

Please specify the Poll Interval
[1d]>
```

ステップ 2CSAクラウドサービスからのシミュレートされたフィッシングメールの許可

注：次に示すように、CYBERSEC_AWARENESS_ALLOWEDメールフローポリシーは、デフォルトですべてのスキャンエンジンをオフに設定して作成されます。



Security Features	
Spam Detection:	Use Default (On) On Off
AMP Detection	Use Default (On) On Off
Virus Protection:	Use Default (On) On Off
Sender Domain Reputation Verification:	Use Default (On) On Off
Virus Outbreak Filters:	Use Default (On) On Off
Advanced Phishing Protection:	Use Default (On) On Off
Graymail Detection:	Use Default (On) On Off
Content Filters:	Use Default (On) On Off
Message Filters:	Use Default (On) On Off

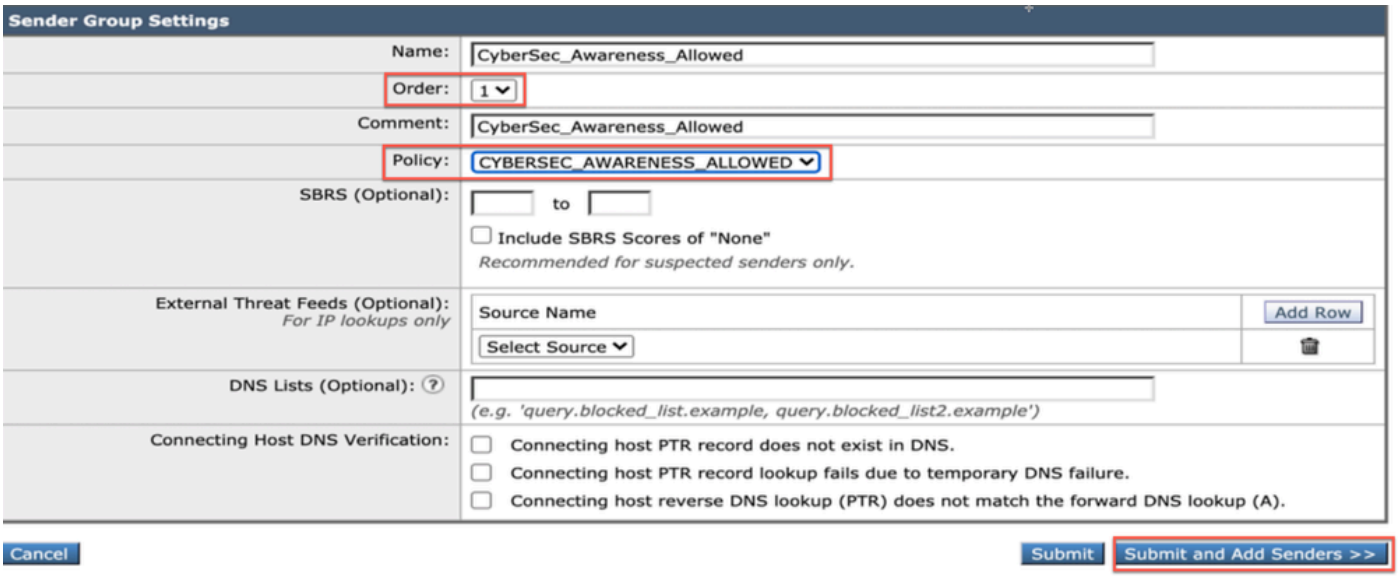
セキュリティ機能が無効になっている「CYBERSEC_AWARENESS_ALLOWED」メールフローポリシーのスクリーンショット

CSAクラウドサービスからのシミュレートされたフィッシングキャンペーンメールが、セキュアEメールゲートウェイ上のすべてのスキャンエンジンをバイパスできるようにするには、次の手順を実行します。

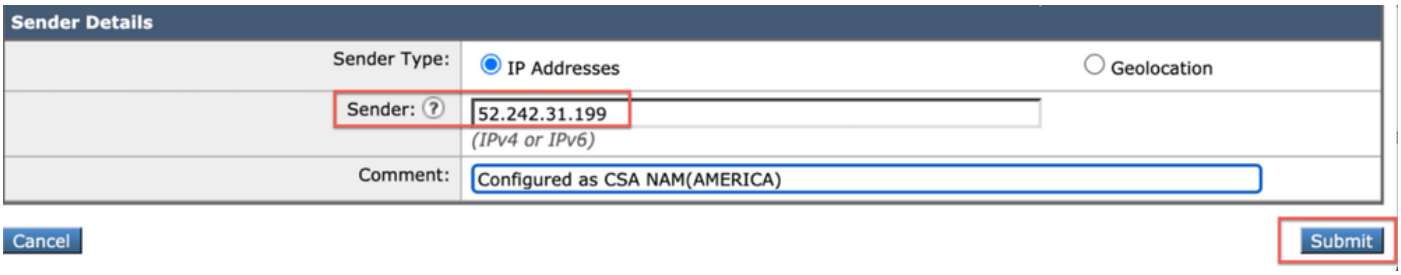
a.新しい送信者グループを作成して、CYBERSEC_AWARENESS_ALLOWEDメールフローポリシーを割り当てます。Mail Policies > HAT Overview > Add Sender Groupの順に移動し、ポリシーCYBERSEC_AWARENESS_ALLOWEDを選択して、順序を1に設定し、次にSubmit and Add Sendersを選択します。

b.フィッシングキャンペーンメールの発信元となる送信者のIP/ドメインまたは地理的位置(GEO)を追加します。

図に示すように、Mail Policies > HAT Overview > Add Sender Group > Submit and Add Sender > Add the sender IP > Submit およびCommit の順に移動して、変更を確定します。



「CYBERSEC_AWARENESS_ALLOWED」メールフローポリシーが選択されたCybersec_Awareness_Allowed送信者グループのスクリーンショット。



Cisco Secure Email GatewayのCisco Security Awareness Settingsページのスクリーンショット

CLI による設定：

1. listenerconfig > Edit > Inbound (PublicInterface) > HOSTACCESS > NEW > New Sender Group の順に移動します。

2.CYBERSEC_AWARENESS_ALLOWEDメールポリシーを使用して新しい送信者グループを作成し、フィッシングキャンペーンメールの開始元の送信者IP/ドメインを追加します。

3. 新しい送信者グループの順序を1に設定し、listenerconfig > EDIT > Inbound (PublicInterface) > HOSTACCESS > MOVE の下のMove オプションを使用します。

4. コミット

注：送信元IPはCSAのIPアドレスで、選択した地域に基づいています。使用する正しいIPアドレスについては、表を参照してください。SEG 14.0.0-xxxのポート番号443のファイアウォール内のこれらのIPアドレスまたはホスト名がCSAクラウドサービスに接続できるようにします。

AMERICA REGION

hostname	IPv4	IPv6
https://secat.cisco.com/	52.242.31.199	
Course Notification (Outbound)	167.89.98.161	
Phishing Simulation (Incoming Email Service)	207.200.3.14, 173.244.184.143	
Landing and Feedback pages (Outbound)	52.242.31.199	
Email Attachment (Outbound)	52.242.31.199	

EU REGION:

hostname	IPv4	IPv6
https://secat-eu.cisco.com/	40.127.163.97	
Course Notification (Outbound)	77.32.150.153	
Phishing Simulation (Incoming Email Service)	77.32.150.153	
Landing and Feedback pages (Outbound)	40.127.163.97	
Email Attachment (Outbound)	40.127.163.97	

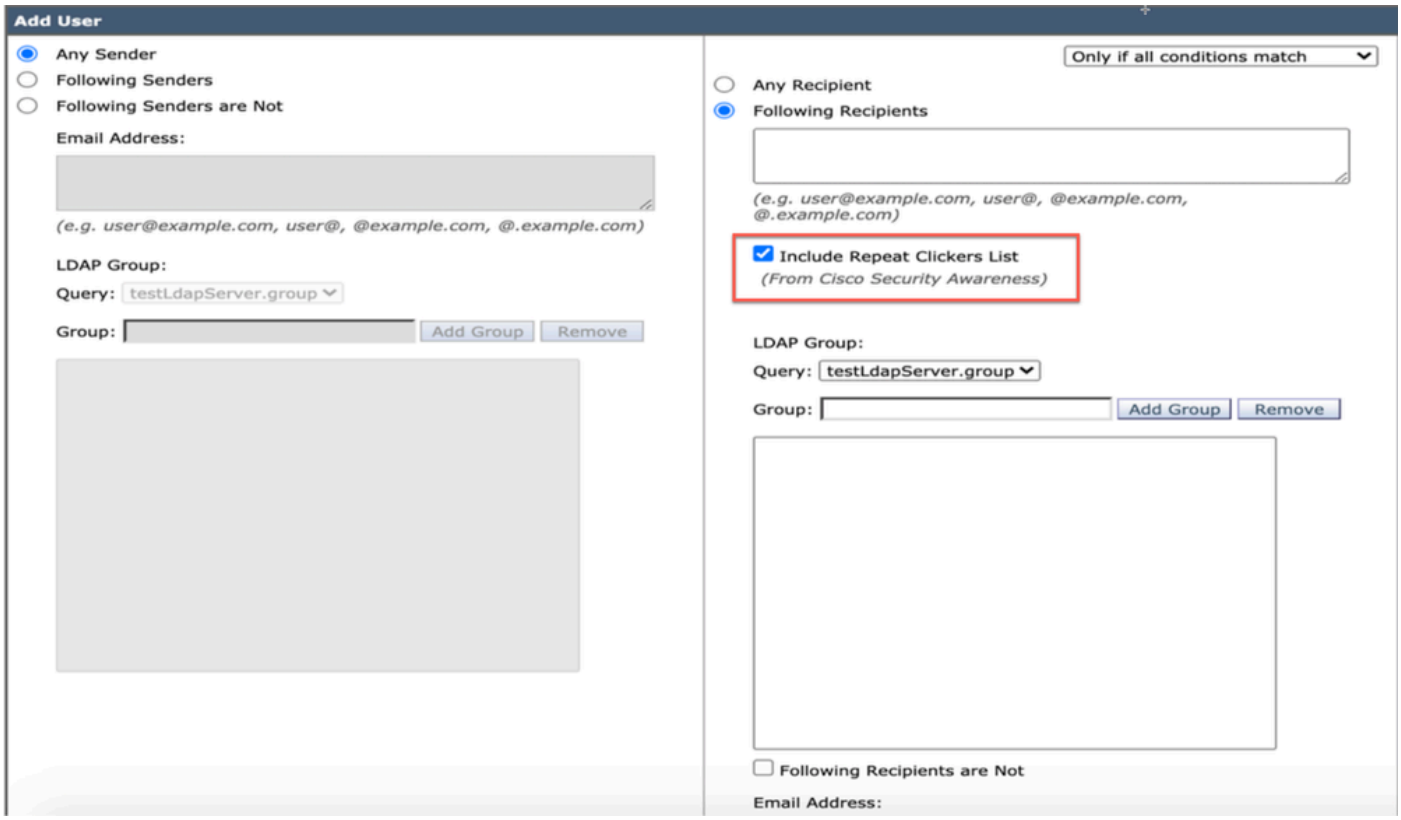
CSA AmericasおよびEU地域のIPアドレスおよびホスト名のスクリーンショット

ステップ 3SEGからの繰り返しクリックに対するアクションの実行

フィッシングメールが送信され、リピートクリッカーリストがSEGに取り込まれると、アグレッシブな着信メールポリシーを作成して、これらの特定のユーザ宛てのメールに対してアクションを実行できます。

新しい積極的な着信カスタムメールポリシーを作成し、受信者セクションのInclude Repeat Clickers Listチェックボックスを有効にします。

GUIから、Mail Policies > Incoming Mail Policies > Add Policy > Add User > Include Repeat Clickers List > Submitの順に移動し、変更を確定します。



繰り返しクリック者に送信されるメールを処理するように設定されたカスタム受信メールポリシーのスクリーンショット

トラブルシューティング ガイド

1. csaconfig > SHOW_LISTに移動し、リピートクリッカリストの詳細を確認します。

```
ESA (SERVICE)> csaconfig


Choose the operation you want to perform:
- EDIT - To edit CSA settings
- DISABLE - To disable CSA service
- UPDATE_LIST - To update the Repeat Clickers list
- SHOW_LIST - To view details of the Repeat Clickers list
[]> show_list

List Name       : Repeat Clickers
Report ID       : 2020
Last Updated    : 2021-02-22 22:19:08
List Status     : Active
Repeat Clickers : 4
```

2. リピートクリッカーリストを強制的に更新する場合は、csaconfig > UPDATE_LISTに移動します。

```
ESA (SERVICE)> csaconfig
```

```
Choose the operation you want to perform:
- EDIT - To edit CSA settings
- DISABLE - To disable CSA service
- UPDATE_LIST - To update the Repeat Clickers list
- SHOW_LIST - To view details of the Repeat Clickers list
[]> update_list

Machine: ESA An update for the Repeat Clickers list was initiated successfully.
```

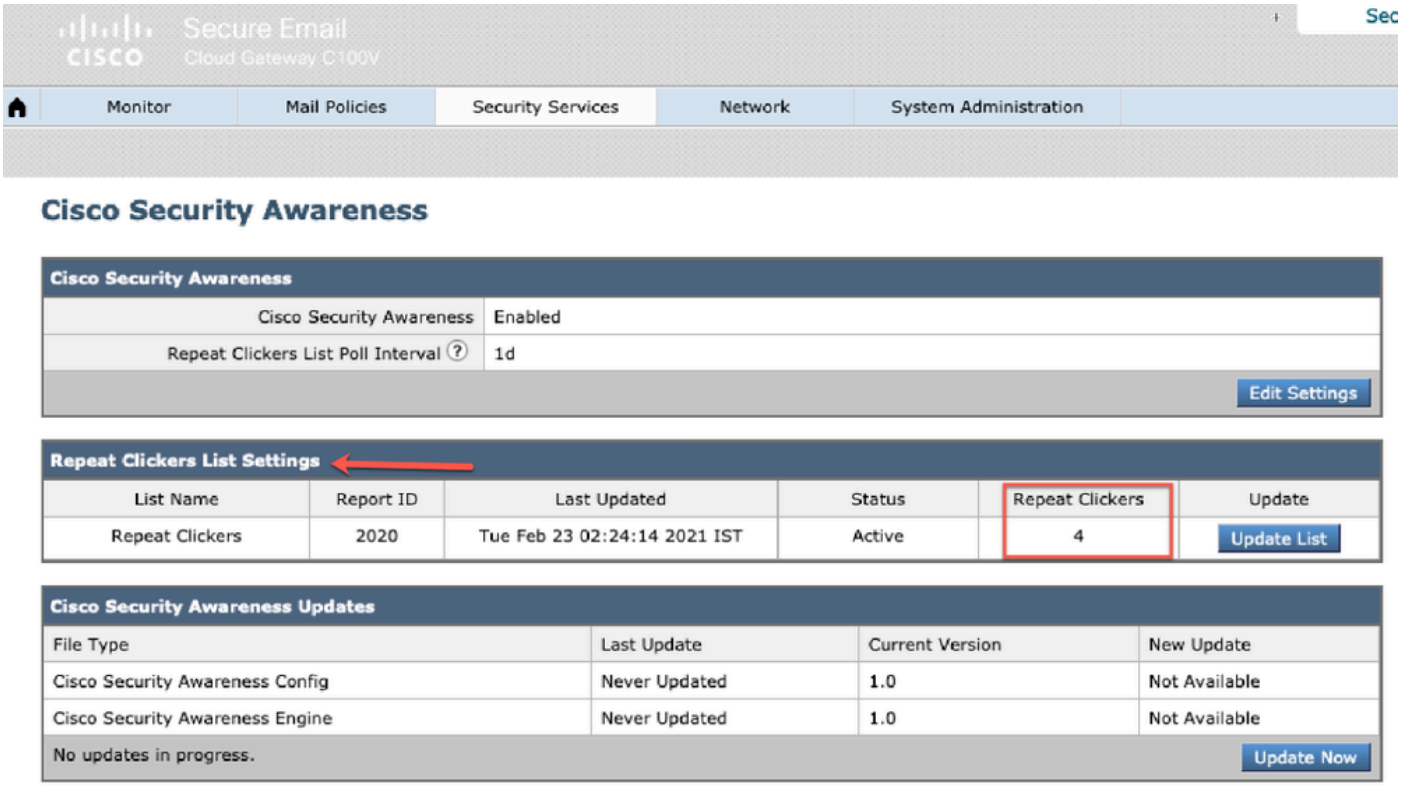
3. csaログを追跡し、リピートクリッカーリストがダウンロードされているかどうか、またはエラーが発生しているかどうかを確認します。動作する設定を次に示します。

```
tail csa
Tue Jan  5 13:20:31 2021 Info: CSA: Connecting to the Cisco Security Awareness cloud service [https://s
Tue Jan  5 13:20:31 2021 Info: CSA: Polling the Cisco Security Awareness cloud service to download the
Tue Jan  5 13:20:31 2021 Info: CSA: Trying to get the license expiry date: loop count 0
Tue Jan  5 13:20:31 2021 Info: CSA: Connecting to the Cisco Security Awareness cloud service [https://s
Tue Jan  5 13:20:31 2021 Info: CSA: Trying to download Repeat clickers list: loop count 0
Tue Jan  5 13:20:31 2021 Info: CSA: The update of the Repeat Clickers list was completed at [Tue Jan  5
Wed Jan  6 13:20:32 2021 Info: CSA: Polling the Cisco Security Awareness cloud service to download the
```

誤ったトークンを入力した場合の出力を次に示します。

```
tail csa
Fri Feb 19 12:28:39 2021 Info: CSA: Connecting to the Cisco Security Awareness cloud service [https://s
Fri Feb 19 12:28:39 2021 Info: CSA: Trying to get the license expiry date: loop count 0
Fri Feb 19 12:28:39 2021 Info: CSA: Polling the Cisco Security Awareness cloud service to download the
Fri Feb 19 12:28:43 2021 Info: CSA: Connecting to the Cisco Security Awareness cloud service [https://s
Fri Feb 19 12:28:43 2021 Info: CSA: Trying to download Repeat clickers list: loop count 0
Fri Feb 19 12:28:44 2021 Warning: CSA: The download of the Repeat Clickers list from the Cisco Security
```

4. リピートクリッカリストのカウントは、GUIからも確認できます。図に示すように、Security Services > Cisco Security Awarenessasの順に選択します。



繰り返しクリックの数を強調表示したセキュリティサービス>シスコのセキュリティ認識ページのスクリーンショット

関連情報

- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。