Configuration de l'intégration Security Awareness avec Cisco Secure Email Gateway

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Créer et envoyer des simulations d'hameçonnage à partir du service cloud CSA
  - Étape 1. Connexion au service cloud CSA
  - Étape 2. Création d'un destinataire d'e-mail hameçonnage
  - Étape 3 : activation de l'API de rapport
  - Étape 4. Création de simulations d'hameçonnage
  - Étape 5. Vérification des simulations actives
- Que voyez-vous du côté du destinataire ?
- Vérifier sur CSA
- Configuration de la passerelle de messagerie sécurisée
  - Étape 1 : activation de la fonctionnalité Cisco Security Awareness dans la passerelle de messagerie sécurisée
  - Étape 2. Autoriser les e-mails d'hameçonnage simulés du service cloud CSA
  - Étape 3. Action sur le clic de répétition à partir du SEG
- Guide de dépannage
- Informations connexes

Introduction

Ce document décrit les étapes nécessaires pour configurer l'intégration de Cisco Security Awareness (CSA) à la passerelle de messagerie sécurisée Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Concepts et configuration de Cisco Secure Email Gateway
- Service cloud CSA

Composants utilisés

Les informations de ce document sont basées sur AsyncOS pour SEG 14.0 et versions

ultérieures.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Créer et envoyer des simulations d'hameçonnage à partir du service cloud CSA

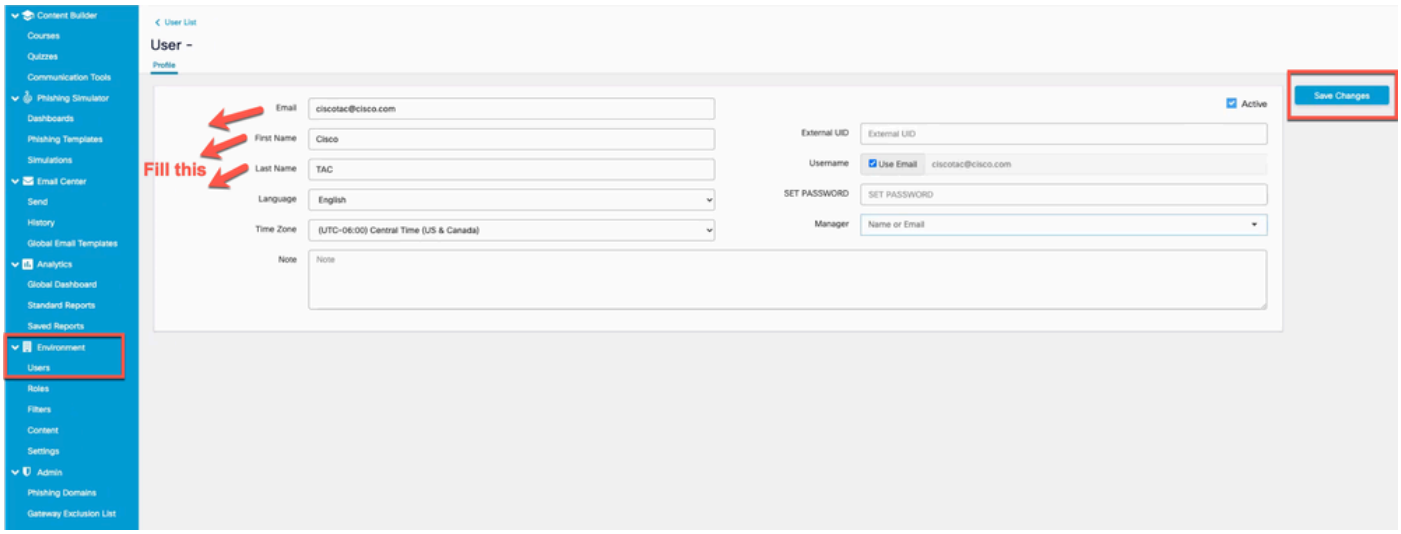
Étape 1. Connexion au service cloud CSA

Reportez-vous à :
1. https://secat.cisco.com/ pour la région AMÉRIQUES

2. https://secat-eu.cisco.com/ pour la région EUROPE

Étape 2. Création d'un destinataire d'e-mail hameçonnage

Naviguez jusqu'**Environment** > **Users** > **Add New User**aux champs E-mail, Prénom, Nom et Langue, puis cliquez sur **Save Changes**comme indiqué dans l'image.

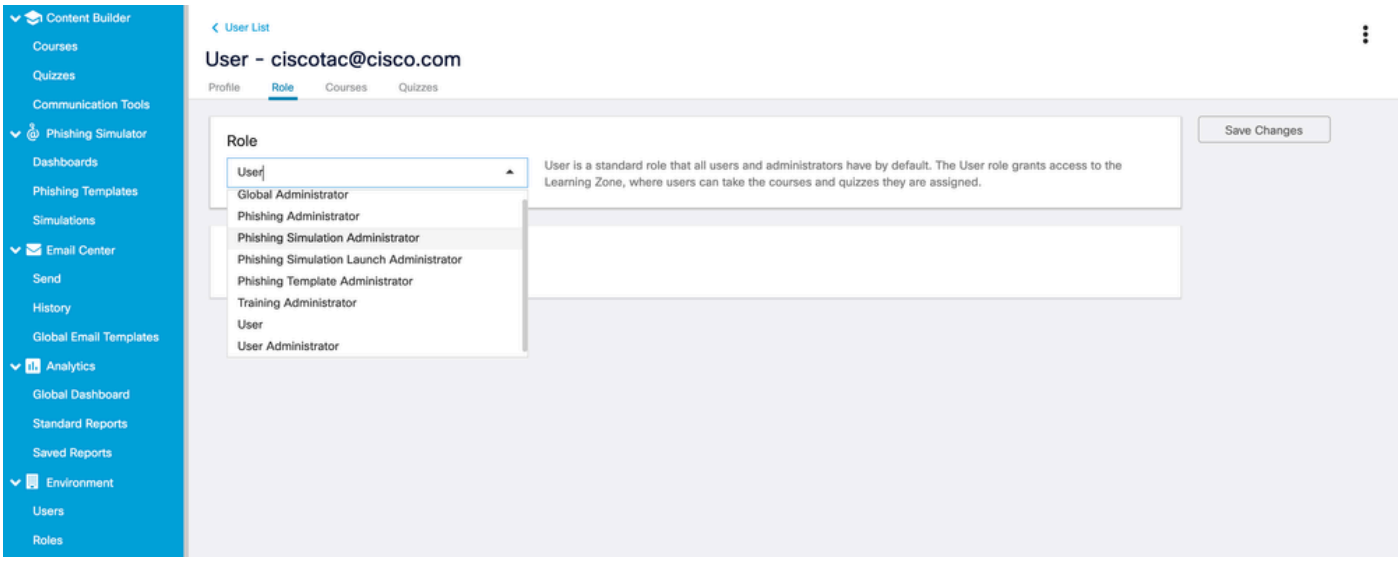


Capture d'écran de l'interface utilisateur pour ajouter un nouvel utilisateur

---

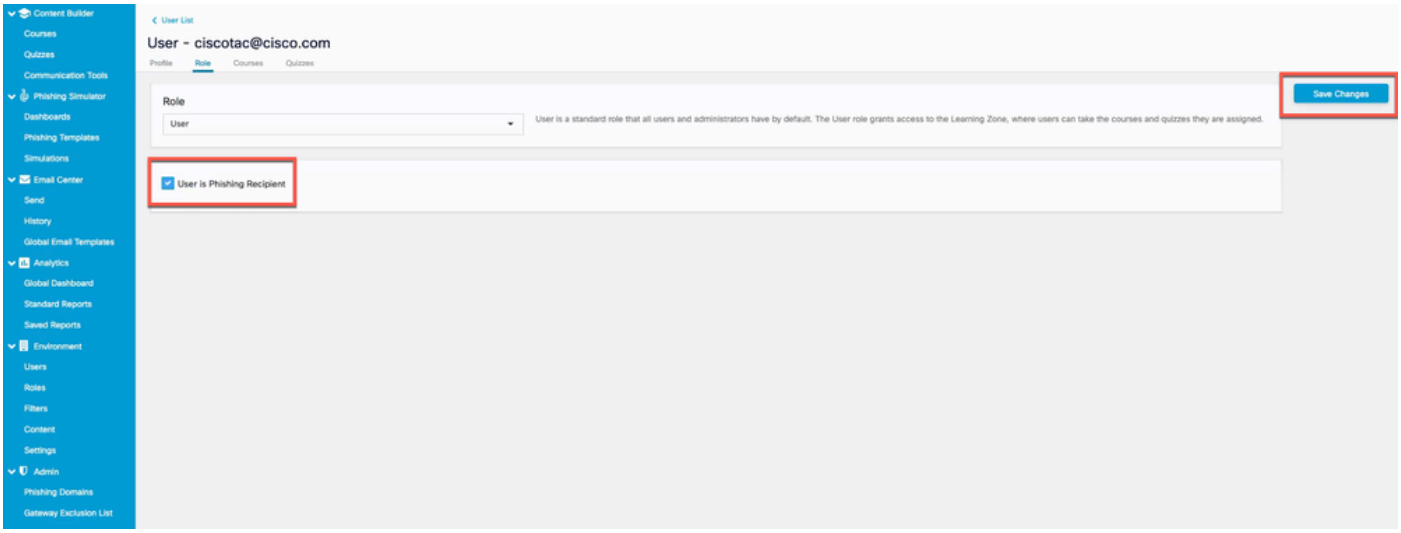
Remarque : Un mot de passe doit être défini uniquement pour un utilisateur admin CSA autorisé à créer et à lancer des simulations.

Le rôle de l'utilisateur peut être sélectionné une fois l'utilisateur créé. Vous pouvez sélectionner le rôle dans la liste déroulante comme indiqué dans cette image :



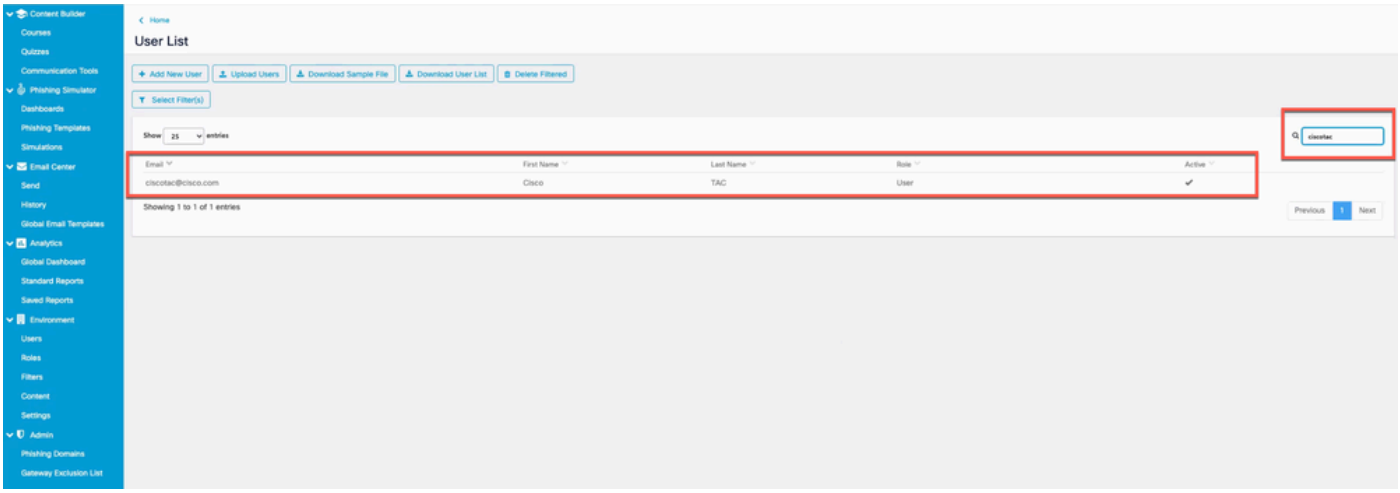
Affichage des options déroulantes du rôle d'utilisateur

Cochez lesUser is Phishing Recipient > Save Changescases comme indiqué dans l'image.



Capture d'écran montrant la case à cocher « L'utilisateur est un destinataire d'hameçonnage » activée

Vérifiez que l'utilisateur a bien été ajouté et qu'il figure dans la liste lorsqu'une recherche est effectuée en fonction de l'adresse e-mail dans le filtre, comme illustré dans l'image.

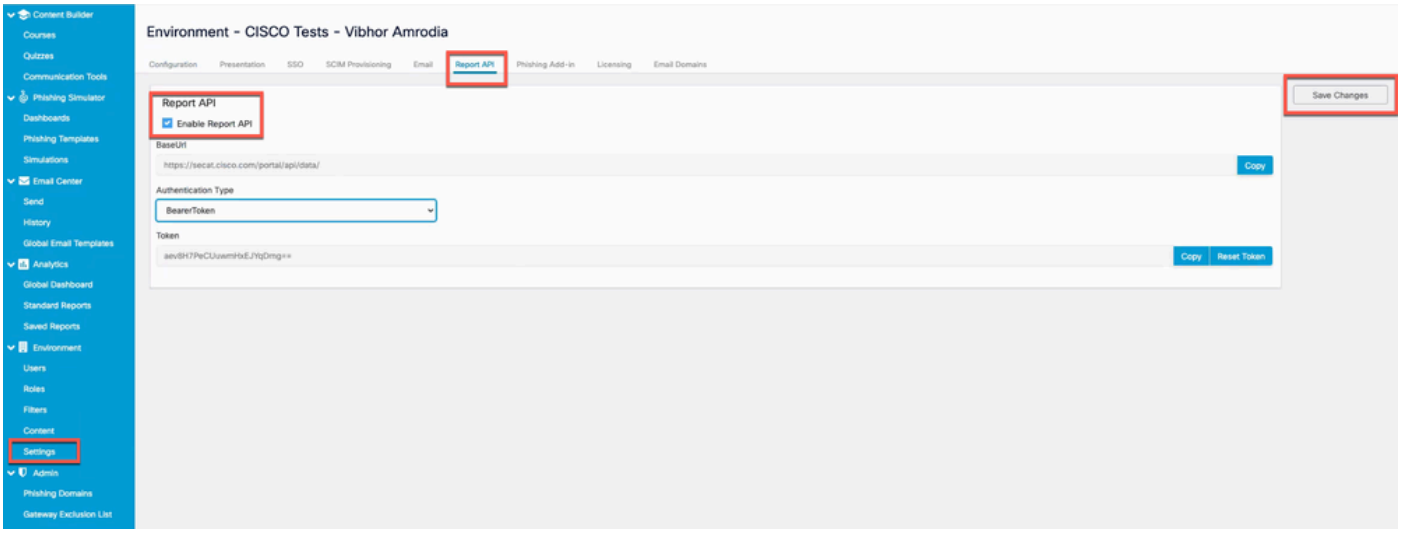


Capture d'écran du nouvel utilisateur dans la liste des utilisateurs

Étape 3 : activation de l'API de rapport

Accédez à l' Environments > Settings > Report API onglet et cochezEnable Report API > Save Changes .

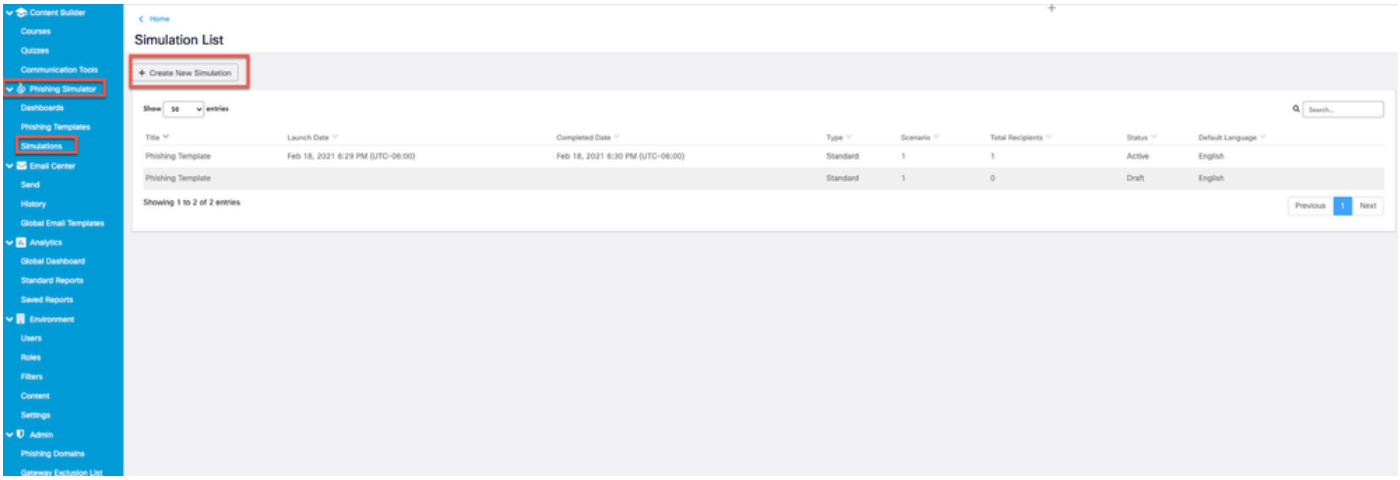
Remarque : Prenez note du jeton Bearer. Vous en avez besoin pour intégrer le SEG avec CSA.



Capture d'écran montrant la case à cocher « Activer l'API de rapport » activée.

Étape 4. Création de simulations d'hameçonnage

a. Naviguez jusqu'à Phishing Simulator > Simulations > Create New Simulation la liste disponible et sélectionnez-en un dans Template la liste, comme illustré dans l'image.

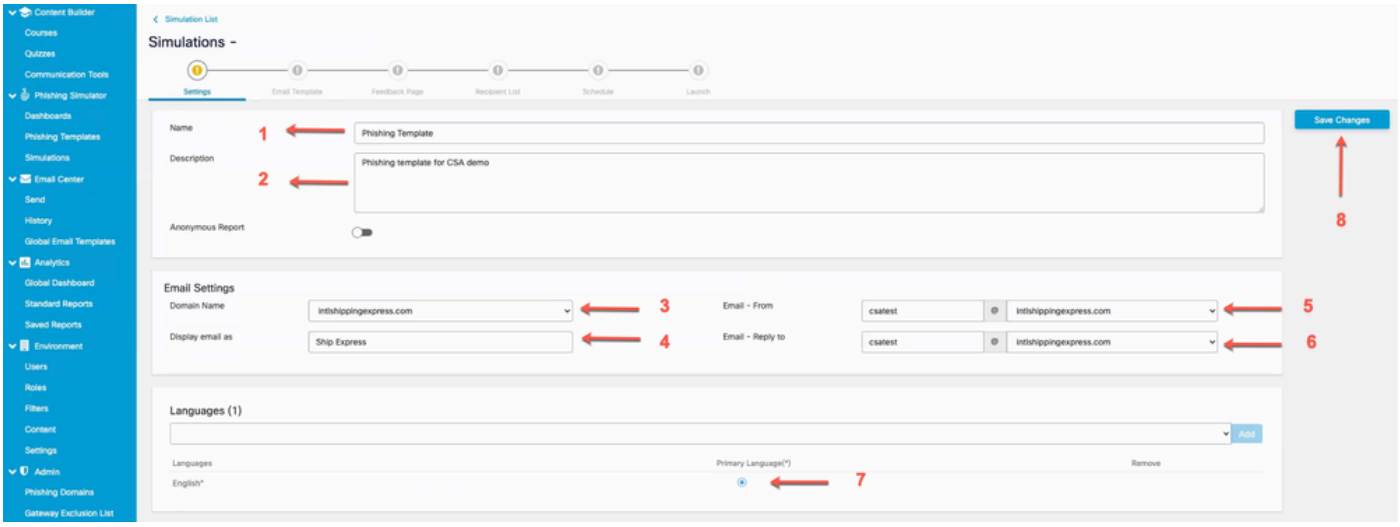


Capture d'écran montrant le bouton « Créer une nouvelle simulation »

b. Complétez ces informations :

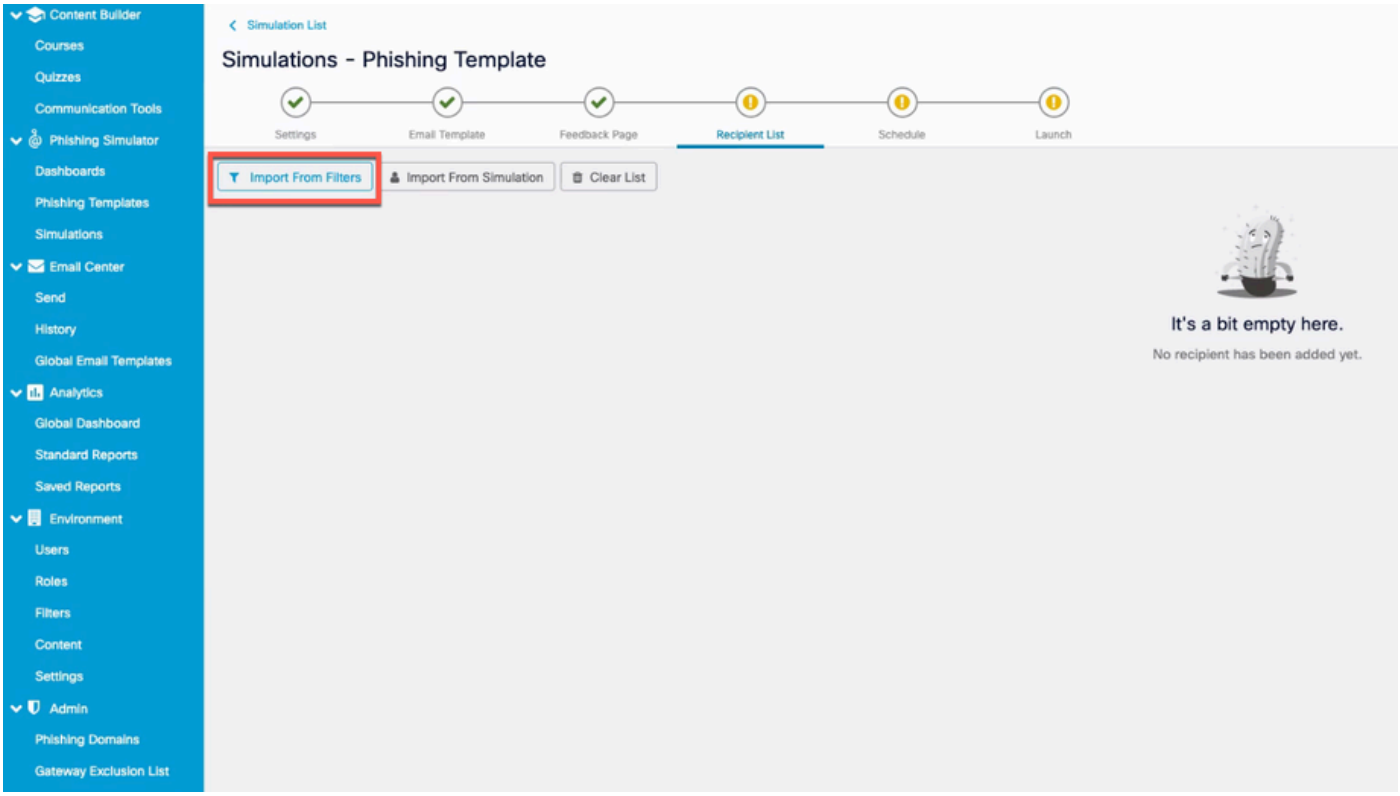
1. Sélectionnez un nom pour le modèle.

2. Décrivez le modèle.
3. Nom de domaine avec lequel l'e-mail de phishing est envoyé.
4. Nom complet de l'e-mail d'hameçonnage.
5. Adresse e-mail de (sélectionnez dans la liste déroulante).
6. Adresse de réponse (sélectionnez-la dans la liste déroulante).
7. Sélectionnez la langue.
8. Enregistrer les modifications.



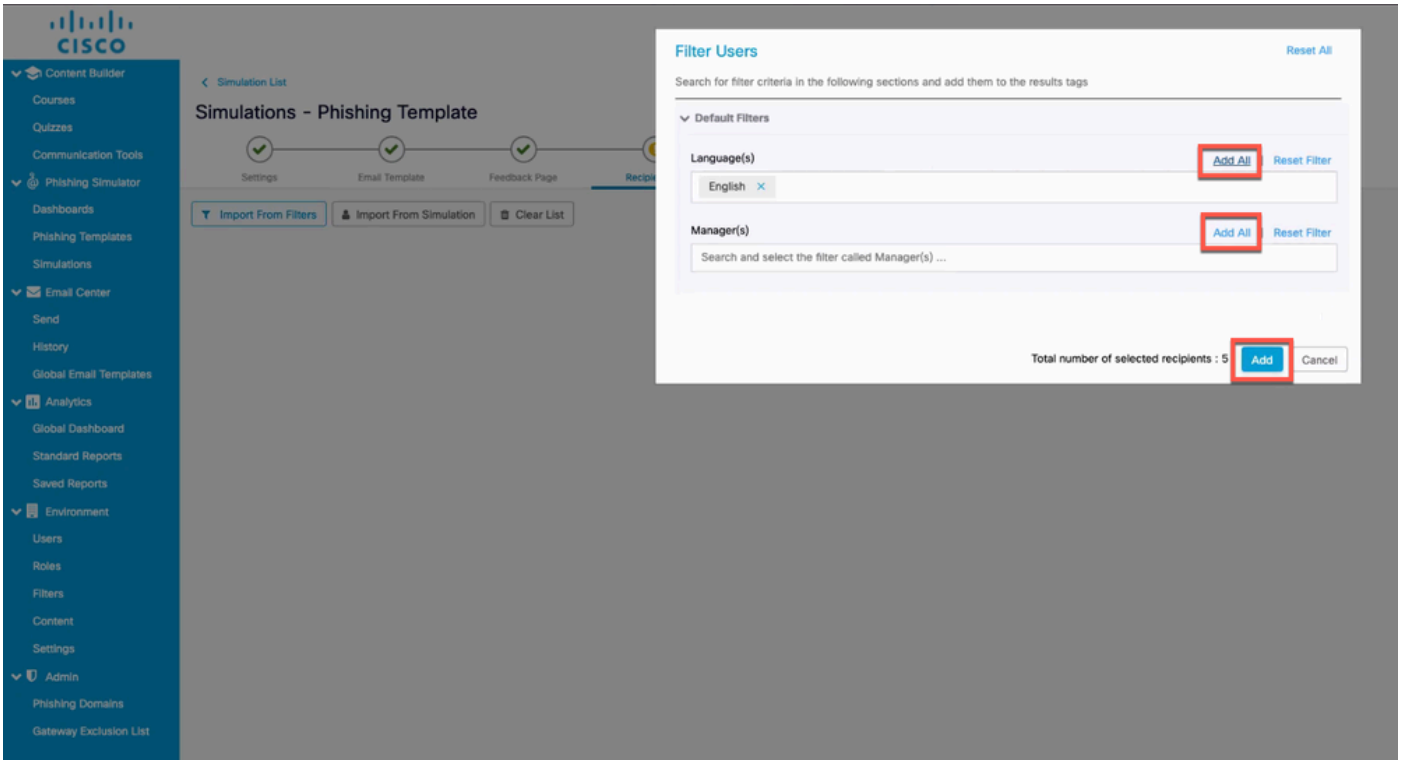
Capture d'écran mettant en évidence les champs à remplir pour configurer une nouvelle simulation

c. Cliquez sur Import from Filters et ajoutez les destinataires de l'e-mail d'hameçonnage à la Recipient Listcomme illustré dans l'image .



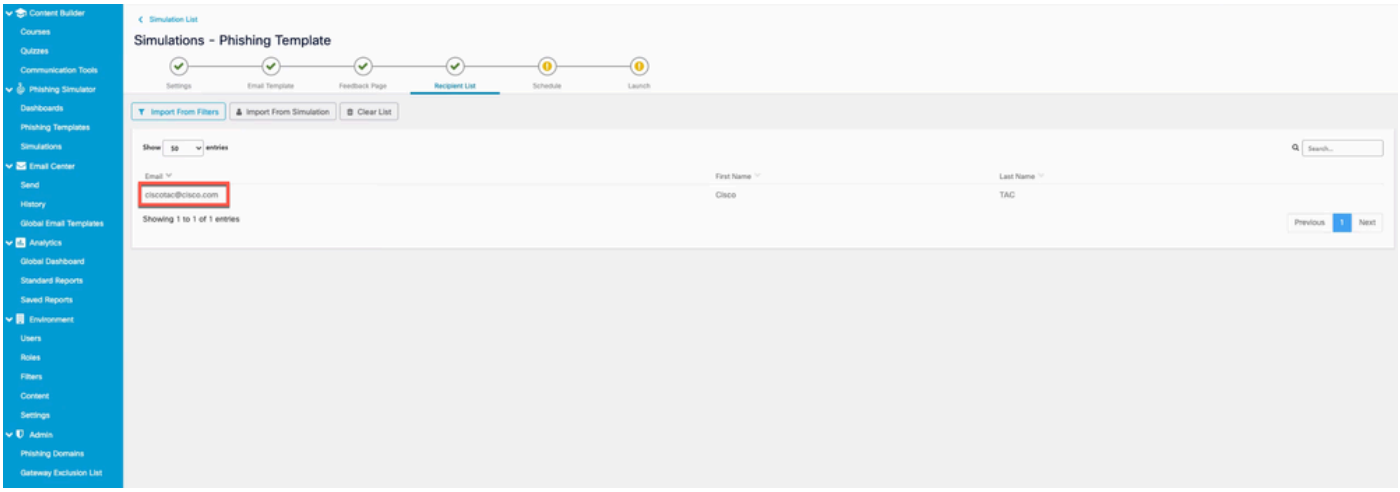
Capture d'écran montrant le bouton « Importer à partir des filtres »

Vous pouvez filtrer les utilisateurs par langue ou par gestionnaires. Cliquez sur Add comme indiqué dans l'image.



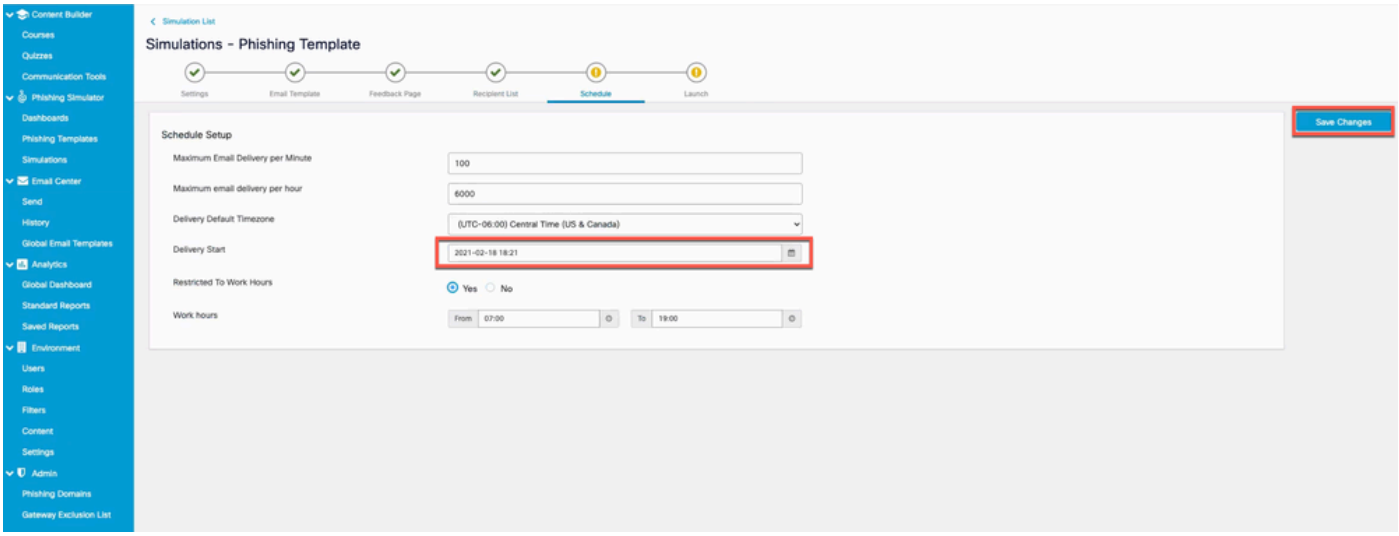
Capture d'écran de la boîte de dialogue Filtrer les utilisateurs pour le filtrage par langue ou gestionnaire

Voici un exemple de l'utilisateur créé à l'étape 2, qui est maintenant ajouté à la liste de destinataires comme illustré dans l'image.



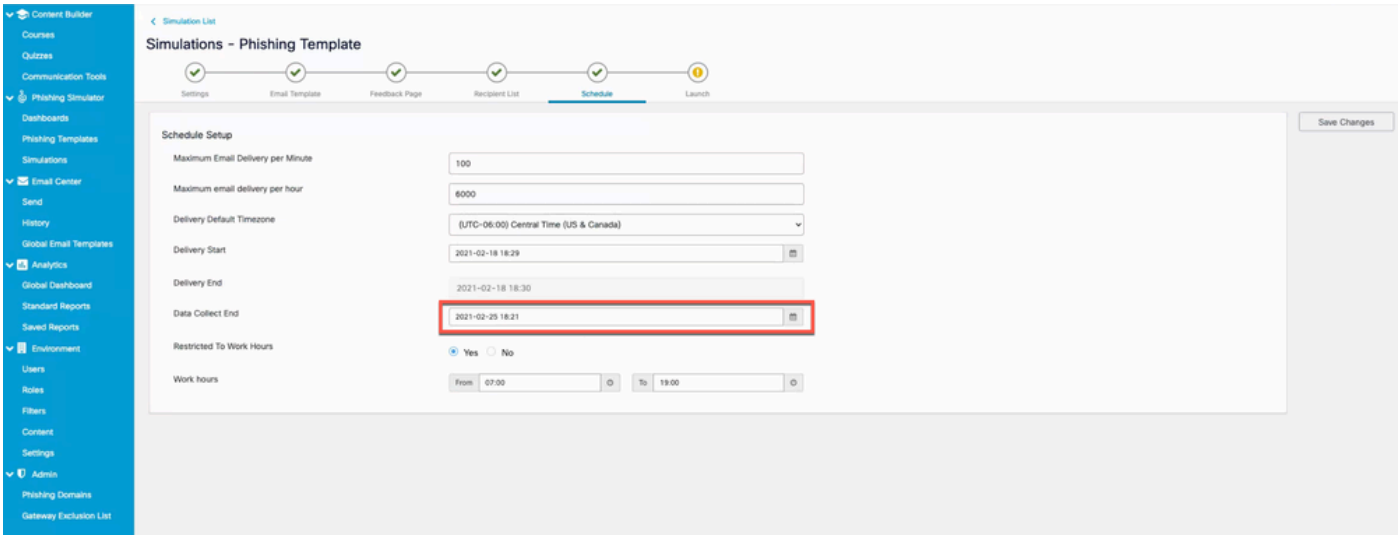
Capture d'écran de l'utilisateur créé précédemment et répertorié comme destinataire de la simulation d'hameçonnage

d. DéfinissezDelivery Startla date et les Save modifications pour programmer la campagne comme indiqué dans l'image.



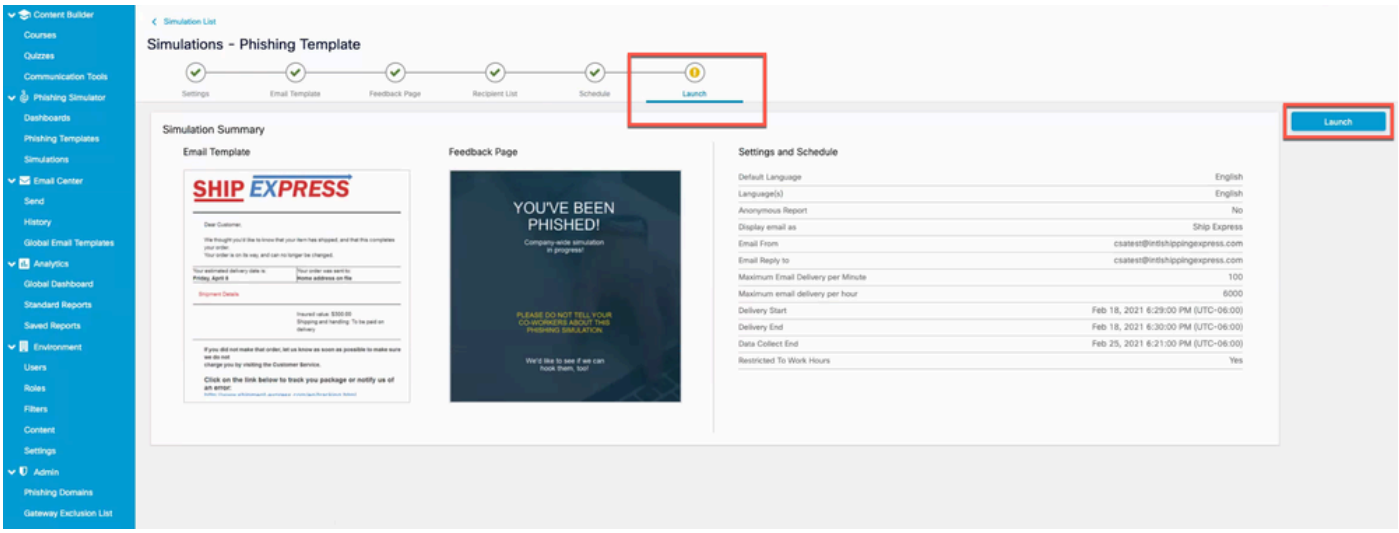
Capture d'écran mettant en évidence le champ Début de livraison

Une fois la date de début choisie, l'option permettant de sélectionner le end date pour la campagne est activée, comme illustré dans l'image.



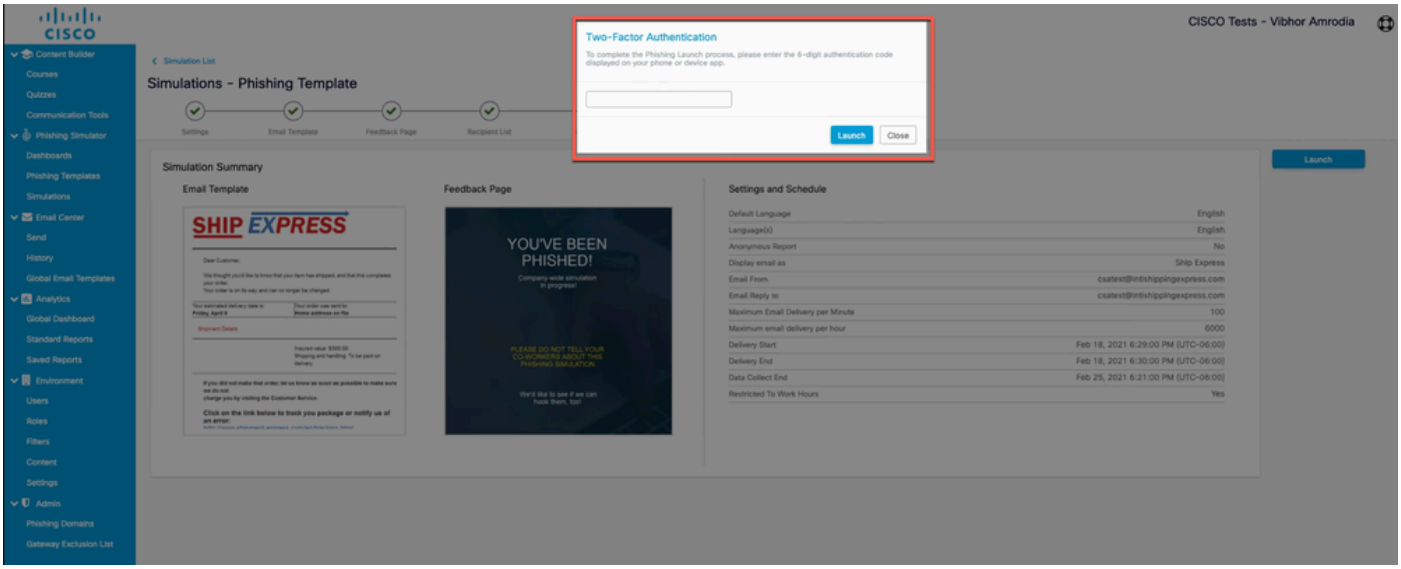
Capture d'écran mettant en surbrillance le champ Data Collect End qui indique la fin de la simulation

e. Cliquez sur Launch pour lancer la campagne, comme le montre l'image.



Capture d'écran du dernier onglet de l'assistant de création de simulation où la campagne peut être lancée

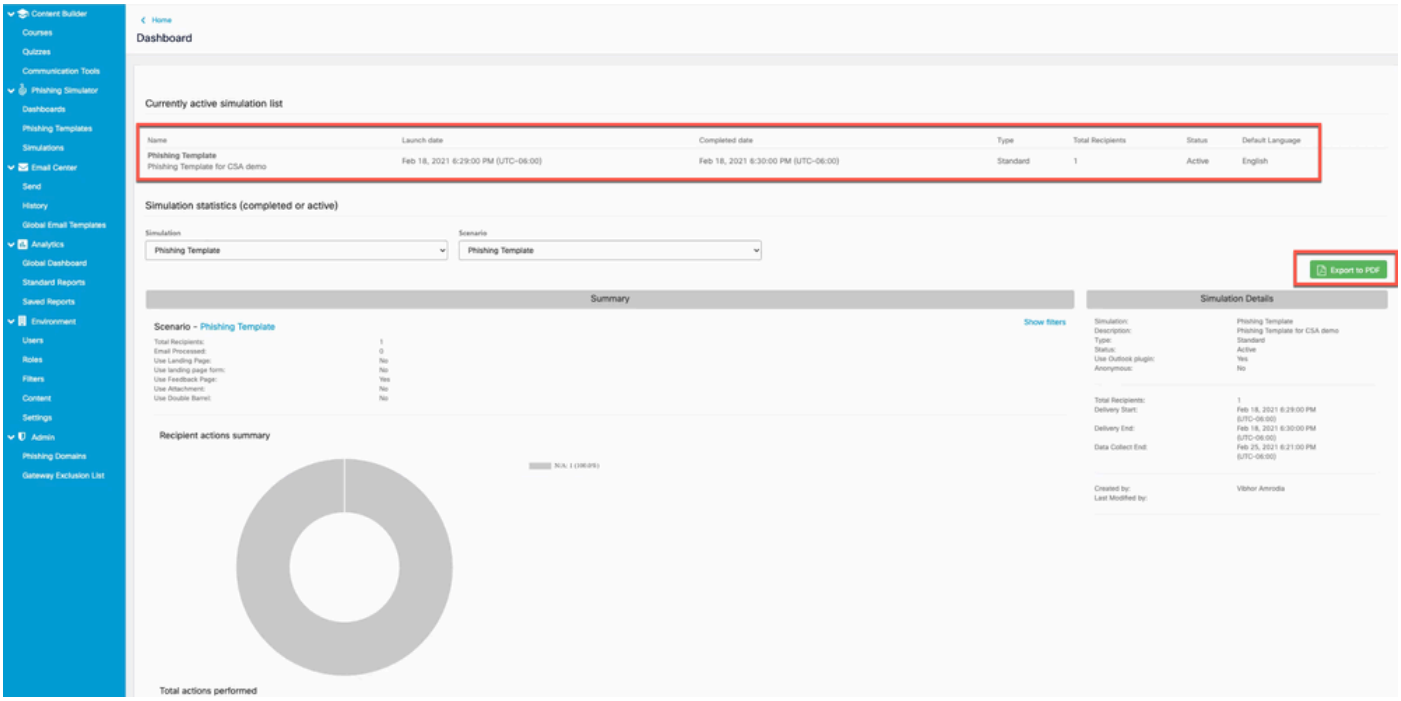
Un code d'authentification à deux facteurs peut être demandé après avoir cliqué sur le bouton de lancement. Entrez le code et cliquez sur Launchcomme indiqué dans l'image.



Capture d'écran de la fenêtre contextuelle demandant le code d'authentification à deux facteurs

Étape 5. Vérification des simulations actives

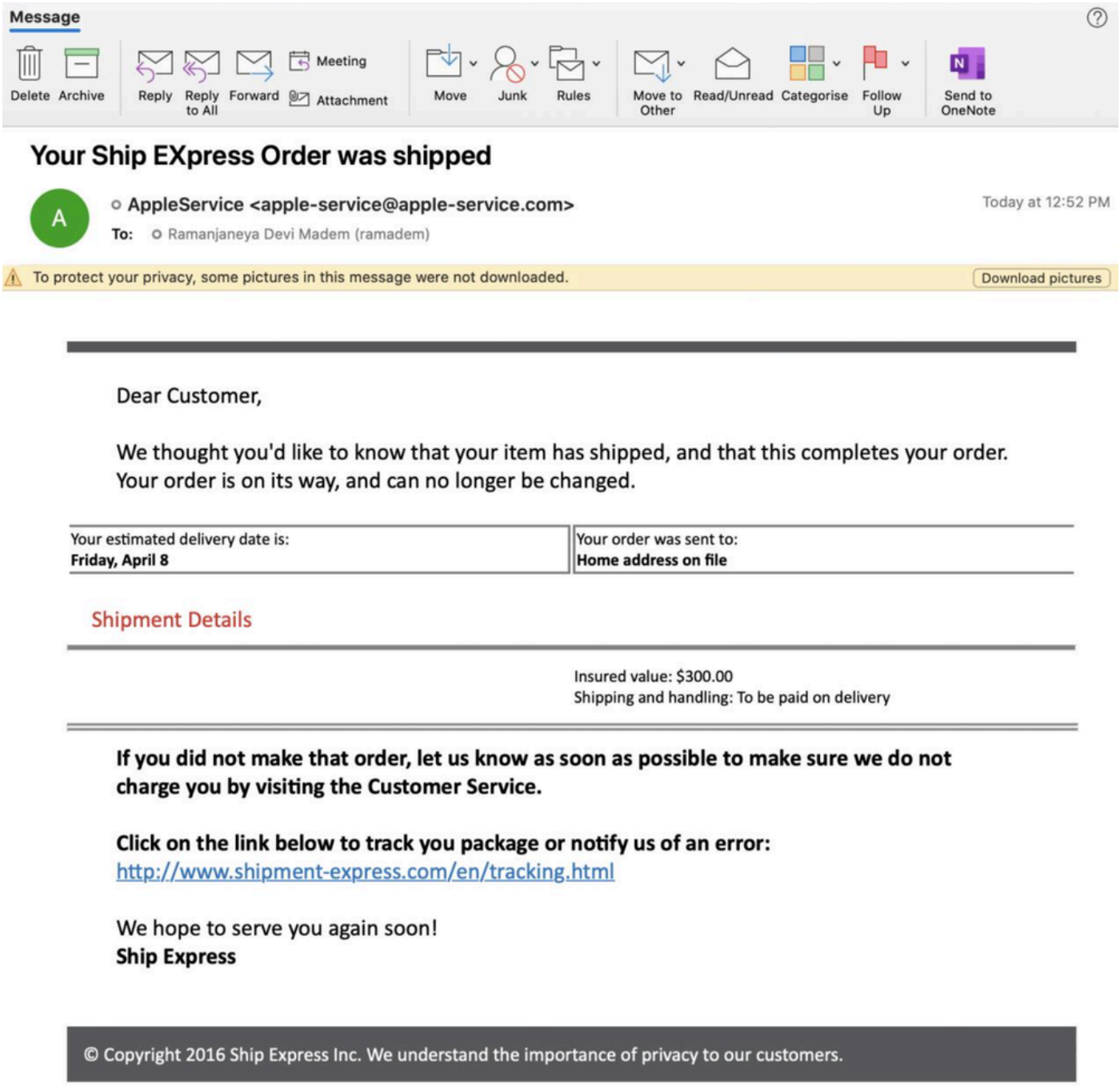
Accédez àPhishing Simulator > Dashboards. La liste des simulations actives actuelles fournit les simulations actives. Vous pouvez également cliquer sur Export as PDF et obtenir le même rapport que celui affiché dans l'image.



Capture d'écran du tableau de bord des simulations de phishing

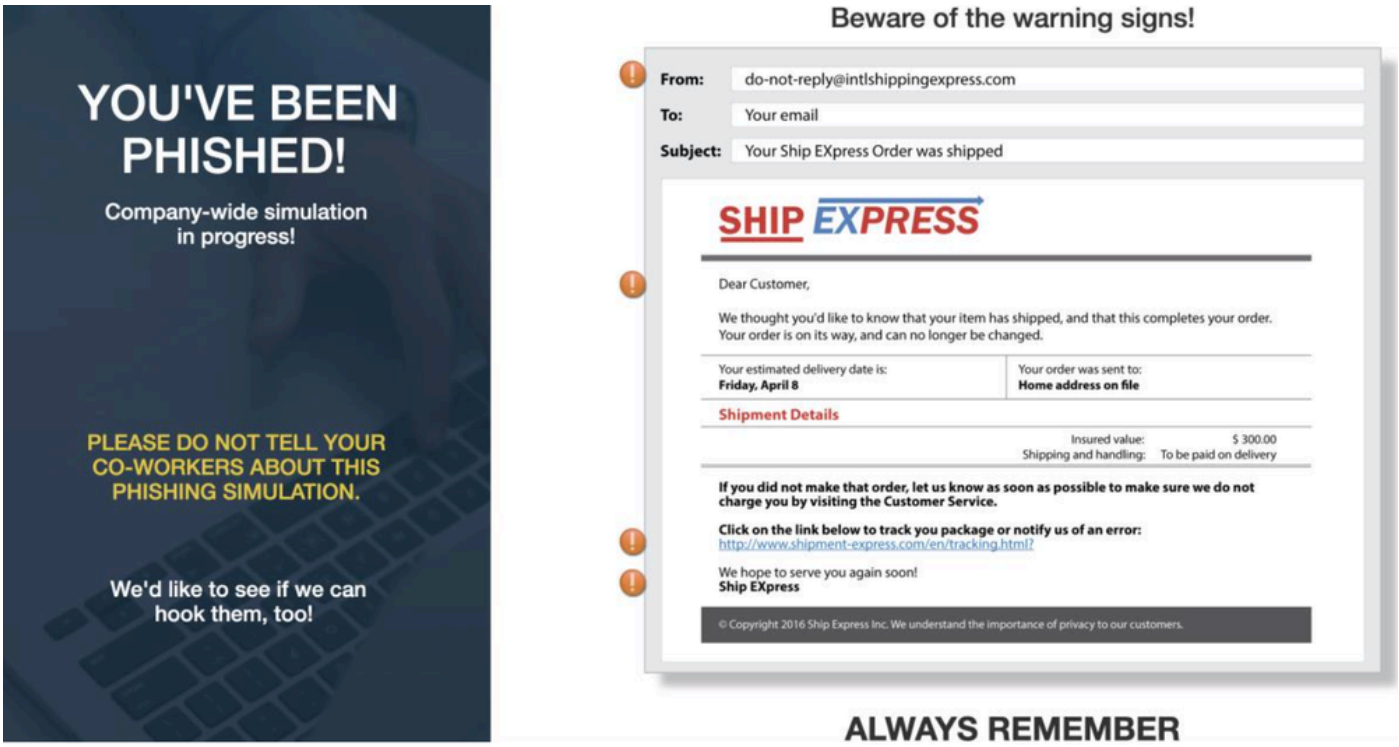
Que voyez-vous du côté du destinataire ?

Exemple d'e-mail de simulation de phishing dans la boîte de réception du destinataire.



Exemple d'e-mail de phishing simulé dans une boîte aux lettres utilisateur

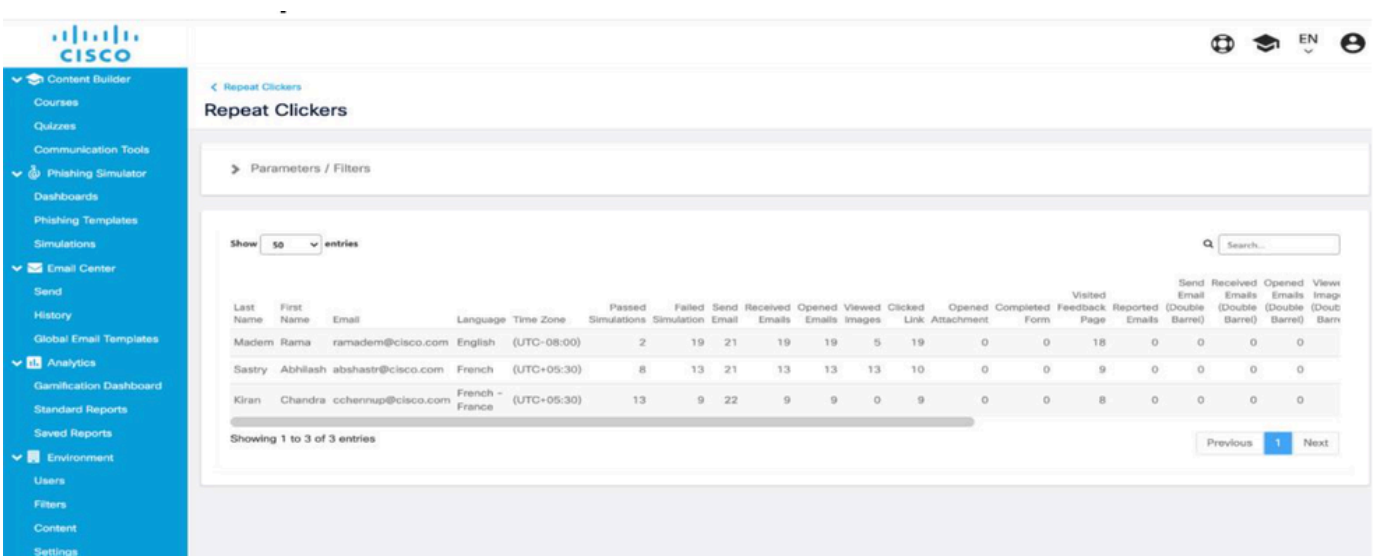
Lorsque le destinataire clique sur l'URL, cette page de commentaires est affichée à l'utilisateur et celui-ci apparaît dans la liste des clics répétés (qui a cliqué librement sur l'URL d'hameçonnage) dans CSA.



Exemple de la page de commentaires que l'utilisateur verra après avoir cliqué sur l'URL dans l'e-mail hameçonné

Vérifier sur CSA

La liste des clics répétés est affichée sousAnalytics > Standard Reports > Phishing Simulations > Repeat Clickersas shown in the image.

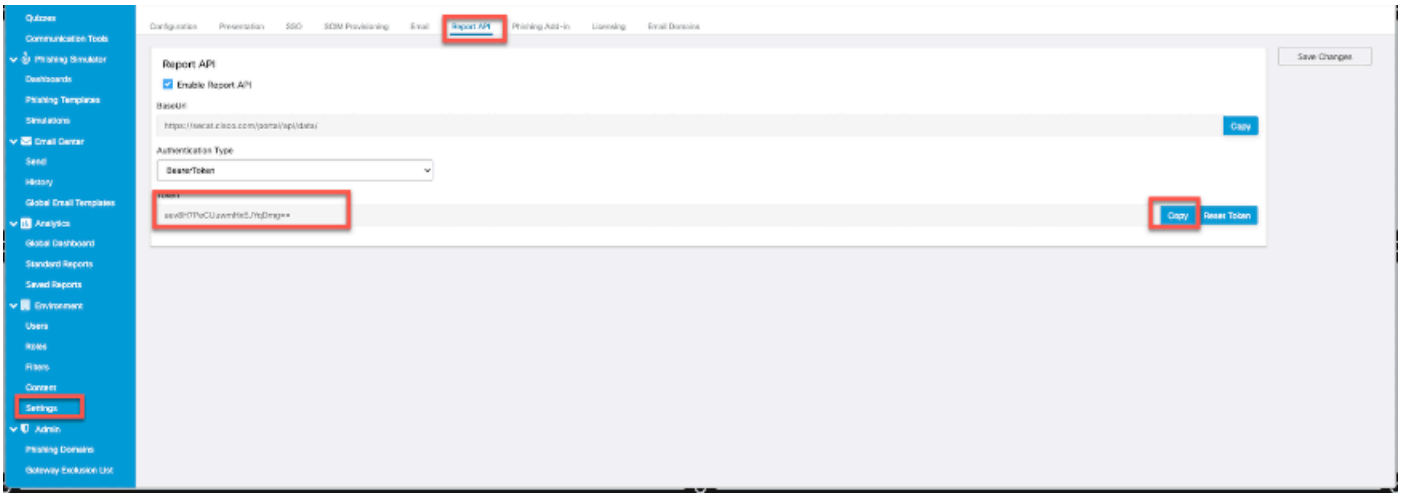


Capture d'écran de la page Repeat Clickers

Configuration de la passerelle de messagerie sécurisée

Remarque : Dans la section Create and Send Phishing Simulations de l'étape 3 du service cloud CSA, lorsque vous activez Report API , vous avez noté le jeton porteur. Gardez ceci à portée de

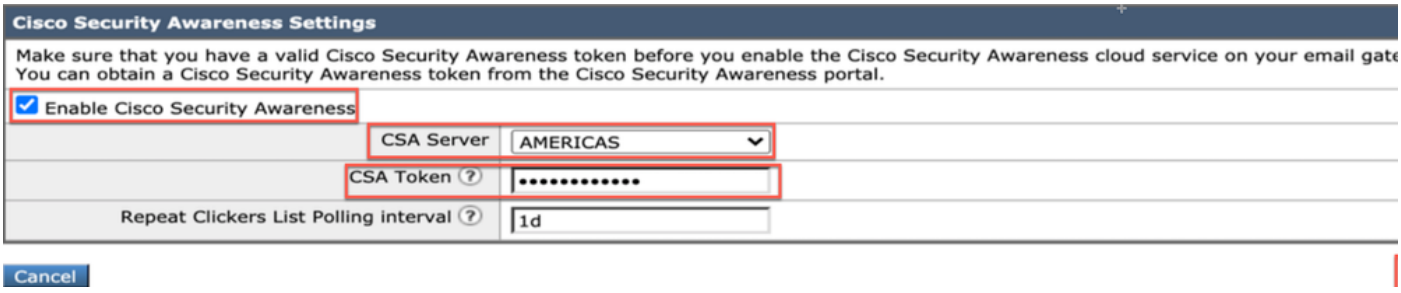
main !



Capture d'écran de la page sous l'API de rapport où l'administrateur peut trouver le jeton porteur

Étape 1 : activation de la fonctionnalité Cisco Security Awareness dans la passerelle de messagerie sécurisée

Dans l'interface utilisateur graphique de la passerelle de messagerie sécurisée, accédez à Security Services > Cisco Security Awareness > Enable . Enter the Region and the CSA Token (Jeton porteur obtenu auprès du service cloud CSA, comme indiqué dans la remarque précédente) et soumettez et validez les modifications.



Capture d'écran de la page des paramètres de Cisco Security Awareness sur la passerelle de messagerie sécurisée Cisco

Configuration CLI

Tapez csaconfig pour configurer CSA via l'interface de ligne de commande.

```
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]>
```

Étape 2. Autoriser les e-mails d'hameçonnage simulés du service cloud CSA

Remarque : La stratégie CYBERSEC_AWARENESS_ALLOWED de flux de messages est créée par défaut avec tous les moteurs d'analyse désactivés, comme illustré ici.

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

Capture d'écran de la stratégie de flux de messages « CYBERSEC_AWARENESS_ALLOWED » avec les fonctions de sécurité désactivées

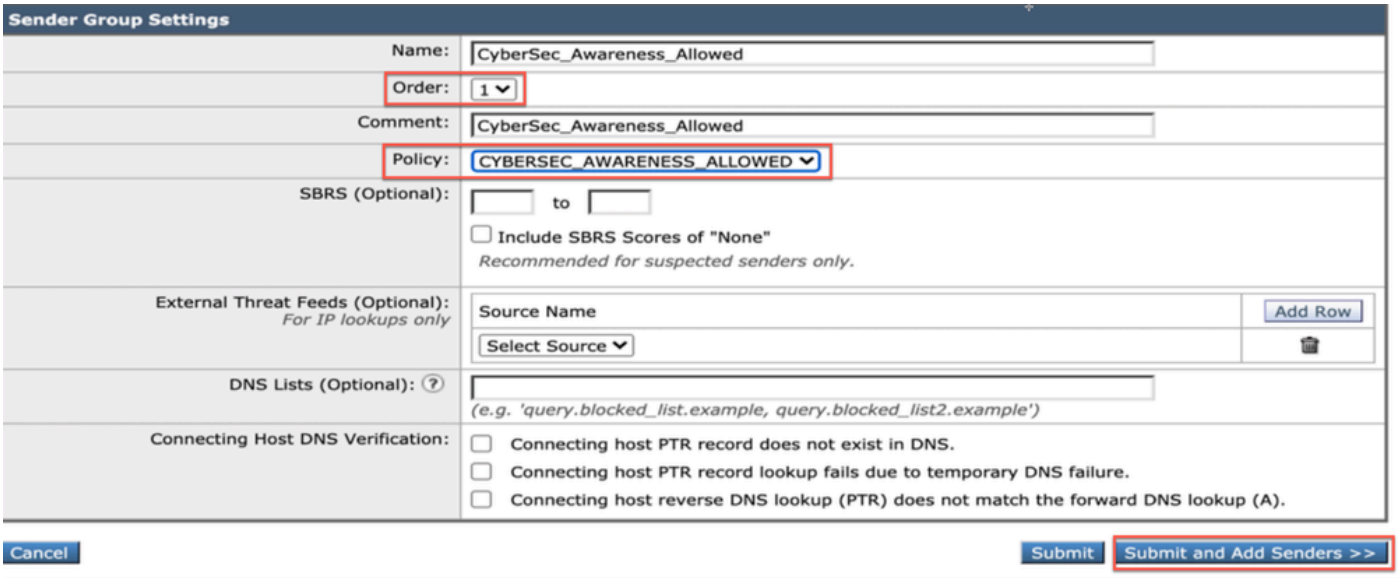
Pour permettre aux e-mails de campagne d'hameçonnage simulés du service cloud CSA de contourner tous les moteurs d'analyse sur la passerelle de messagerie sécurisée :

a. Créez un nouveau groupe d'expéditeurs et attribuez la stratégie de flux de messages CYBERSEC_AWARENESS_ALLOWED. Naviguez jusqu'à Mail Policies > HAT Overview > Add Sender Group , sélectionnez la règle CYBERSEC_AWARENESS_ALLOWED et définissez l'ordre sur 1, puis Submit and Add Senders.

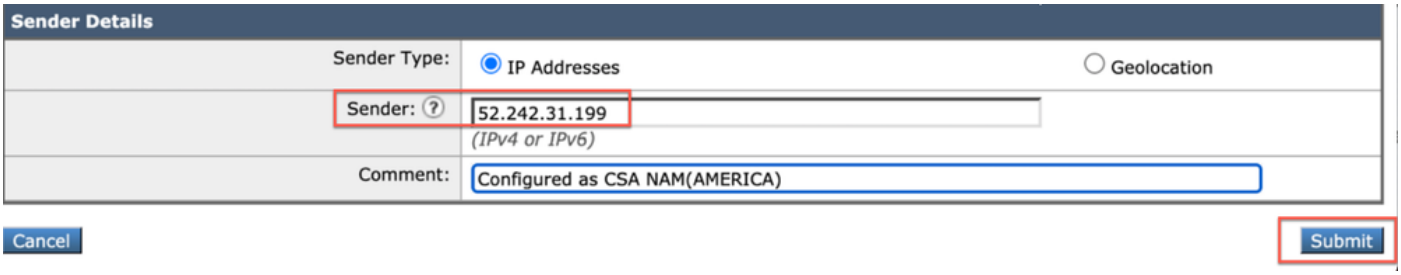
b. Ajoutez un expéditeur IP/domain ouGeo Locationà partir duquel les e-mails de campagne d'hameçonnage sont envoyés.

Naviguez jusqu'àMail Polices > HAT Overview > Add Sender Group > Submit and Add Senders > Add the sender IP > Submit

etCommitmodifiez comme indiqué dans l'image.



Capture d'écran d'un groupe d'expéditeurs CyberSec_Awareness_Allowed avec la stratégie de flux de messages « CYBERSEC_AWARENESS_ALLOWED » sélectionnée.



Capture d'écran de la page des paramètres de Cisco Security Awareness sur la passerelle de messagerie sécurisée Cisco

Configuration CLI :

1. Accédez à listenerconfig > Edit > Inbound (PublicInterface) > HOSTACCESS > NEW > New Sender Group .

2. Créez un nouveau groupe d'expéditeurs avec une stratégie deCYBERSEC_AWARENESS_ALLOWEDmessagerie et ajoutez une adresse IP/un domaine d'expéditeur à partir duquel les e-mails de campagne d'hameçonnage sont initiés.

3. Définissez l'ordre du nouveau groupe d'expéditeurs sur 1 et utilisez l'Moveoption sous listenerconfig > EDIT > Inbound (PublicInterface) > HOSTACCESS > MOVE .

4. Engagez.

Remarque : L'adresse IP de l'expéditeur est l'adresse IP du CSA et dépend de la région que vous avez sélectionnée. Reportez-vous au tableau pour connaître l'adresse IP correcte à utiliser. Autorisez ces adresses IP/noms d'hôte dans le pare-feu avec le numéro de port 443 pour SEG 14.0.0-xxx à se connecter au service cloud CSA.

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	

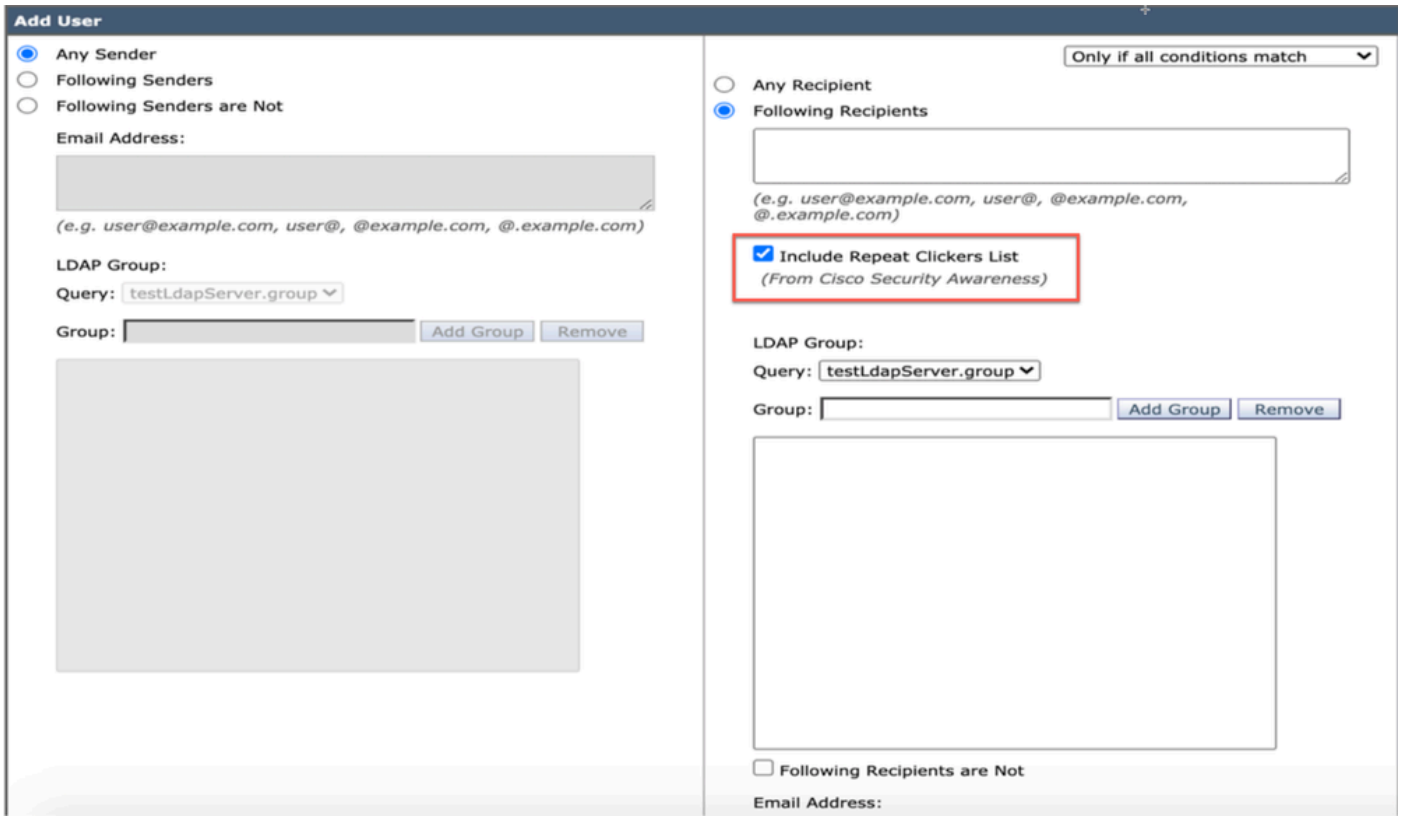
Capture d'écran des adresses IP et noms d'hôte des régions CSA Amériques et UE

Étape 3. Action sur le clic de répétition à partir du SEG

Une fois que les e-mails d'hameçonnage ont été envoyés et que la liste de clics de répétition est renseignée dans le SEG, une politique de messages entrants agressive peut être créée pour prendre des mesures sur les messages envoyés à ces utilisateurs spécifiques.

Créez une nouvelle stratégie de messages entrants personnalisés agressive et activez la case à cocher Include Repeat Clickers List dans la section du destinataire.

Dans l'interface utilisateur graphique, accédez à Mail Policies > Incoming Mail Policies > Add Policy > Add User > Include Repeat Clickers List > Submit et aux Commit modifications.



Capture d'écran d'une stratégie de messages entrants personnalisée configurée pour gérer les messages destinés aux cliqueurs répétés

Guide de dépannage

1. Accédez à csaconfig > SHOW_LISTpour afficher les détails de la liste des cliqueurs de répétition.

```
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. Accédez à csaconfig > UPDATE_LIST si vous souhaitez forcer la mise à jour de la liste des cliqueurs de répétition.

```
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.
```

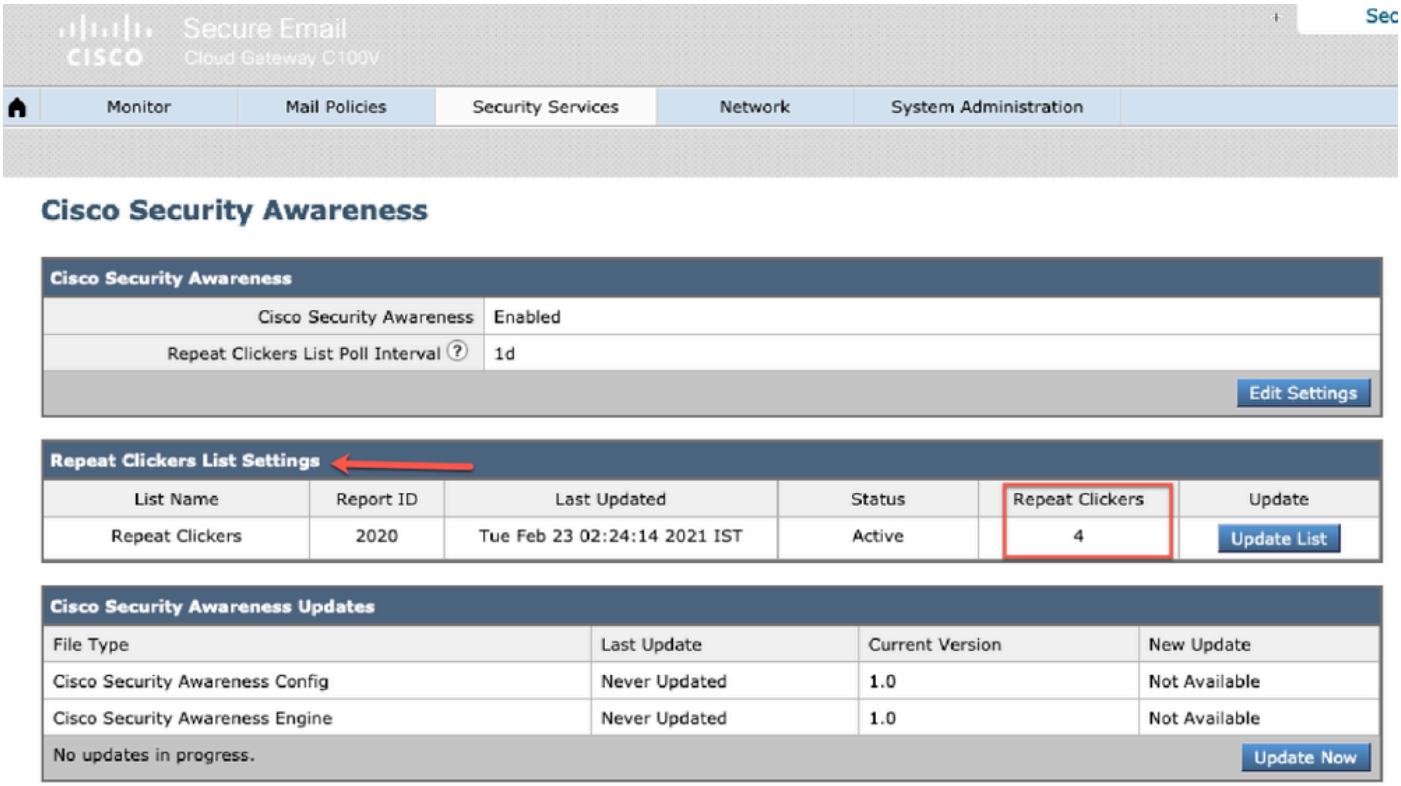
3. Suivez les journaux CSSA pour voir si la liste des cliqueurs de répétition a été téléchargée ou s'il y a une erreur. Voici la working setup:

```
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
```

Here is an output when you have entered the incorrect token:

```
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. La liste du nombre de cliqueurs de répétition est également visible depuis l'interface utilisateur graphique. Naviguez jusqu'à Security Services > Cisco Security Awarenesscomme indiqué dans l'image.



Capture d'écran de la page Security Services > Cisco Security Awareness qui indique le nombre de clics répétés

Informations connexes

- [Assistance et documentation techniques - Cisco Systems]

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.