

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

Fill this

Save Changes

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 :

User - ciscotac@cisco.com

Profile    Role    Courses    Quizzes

Role

User

Global Administrator  
Phishing Administrator  
Phishing Simulation Administrator  
Phishing Simulation Launch Administrator  
Phishing Template Administrator  
Training Administrator  
User  
User Administrator

User is a standard role that all users and administrators have by default. The User role grants access to the Learning Zone, where users can take the courses and quizzes they are assigned.

Save Changes

Affichage des options déroulantes du rôle d'utilisateur

Cochez les cases comme indiqué dans l'image.

User - ciscotac@cisco.com

Profile    Role    Courses    Quizzes

Role

User

User is a standard role that all users and administrators have by default. The User role grants access to the Learning Zone, where users can take the courses and quizzes they are assigned.

User is Phishing Recipient

Save Changes

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.

User List

Add New User    Upload Users    Download Sample File    Download User List    Delete Filtered

Select Filter(s)

Show 25 entries

| Email              | First Name | Last Name | Role | Active                              |
|--------------------|------------|-----------|------|-------------------------------------|
| ciscotac@cisco.com | Cisco      | TAC       | User | <input checked="" type="checkbox"/> |

Showing 1 to 1 of 1 entries

Q: ciscotac

Previous    Next

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.

The screenshot shows the 'Report API' configuration page. The 'Enable Report API' checkbox is checked. The 'BaseURL' field contains 'https://secat.cisco.com/portal/api/data/'. The 'Authentication Type' dropdown is set to 'BearerToken'. The 'Token' field contains a long token string. The 'Save Changes' button is highlighted with a red box.

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

## Étape 4. Crédation 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.

| Title             | Launch Date                      | Completed Date                   | Type     | Scenario | Total Recipients | Status | Default Language |
|-------------------|----------------------------------|----------------------------------|----------|----------|------------------|--------|------------------|
| Phishing Template | Feb 18, 2021 6:29 PM (UTC-06:00) | Feb 18, 2021 6:30 PM (UTC-06:00) | Standard | 1        | 0                | Active | English          |
| Phishing Template |                                  |                                  | Standard | 1        | 0                | Draft  | English          |

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.

The screenshot shows the 'Simulations - Phishing Template' settings page. The left sidebar includes sections for Content Builder, Phishing Simulator, Email Center, Analytics, and Admin. The main area has tabs for Settings, Email Template, Feedback Page, Recipient List, Schedule, and Launch. The 'Settings' tab is active. It contains fields for Name (Phishing Template, #1), Description (Phishing template for CSA demo, #2), Email Settings (Domain Name: intishippingexpress.com, #3; Display email as: Ship Express, #4), Languages (Languages: English\*, Primary Language: English\*, #5), and a Save Changes button (#8). Red arrows point to the Name, Description, Domain Name, Display email as, Primary Language, and Save Changes button.

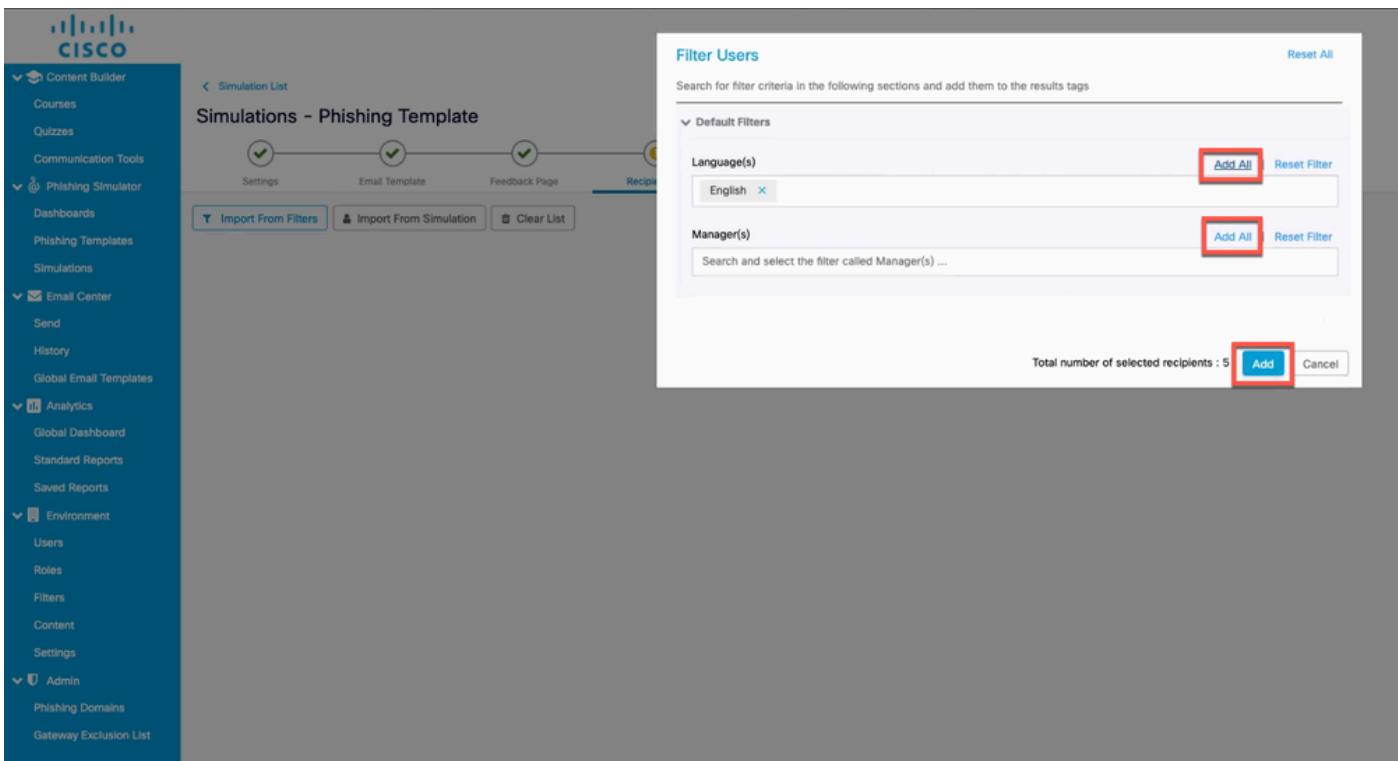
Capture d'écran mettant en évidence les champs à remplir pour configurer une nouvelle simulation

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

The screenshot shows the 'Simulations - Phishing Template' Recipient List page. The left sidebar is identical to the previous screenshot. The main area has tabs for Settings, Email Template, Feedback Page, Recipient List (which is active), Schedule, and Launch. Below the tabs are buttons for 'Import From Filters' (highlighted with a red box), 'Import From Simulation', and 'Clear List'. To the right, there's a cartoon character and the text 'It's a bit empty here.' followed by 'No recipient has been added yet.' Red arrows point to the 'Import From Filters' button and the 'Recipient List' tab.

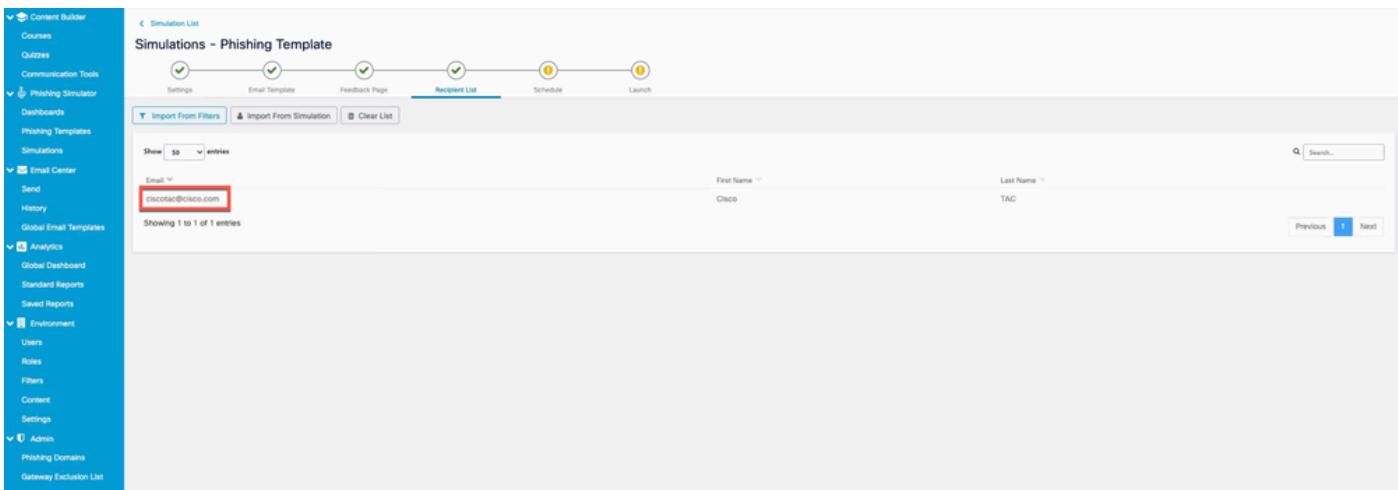
Capture d'écran montrant le bouton « Importer à partir des filtres »

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. Définissez la date et les modifications pour programmer la campagne comme indiqué dans l'image.

The screenshot shows the 'Simulations - Phishing Template' configuration interface. The 'Schedule' tab is active. Key settings include:

- Maximum Email Delivery per Minute: 100
- Maximum email delivery per hour: 6000
- Delivery Default Timezone: (UTC-06:00) Central Time (US & Canada)
- Delivery Start: 2021-02-18 18:21 (highlighted by a red box)
- Restricted To Work Hours: Yes (radio button selected)
- Work hours: From 07:00 to 19:00

A red box highlights the 'Delivery Start' date input field. The 'Save Changes' button is located in the top right corner.

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

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

The screenshot shows the 'Simulations - Phishing Template' configuration interface. The 'Schedule' tab is active. Key settings include:

- Maximum Email Delivery per Minute: 100
- Maximum email delivery per hour: 6000
- Delivery Default Timezone: (UTC-06:00) Central Time (US & Canada)
- Delivery Start: 2021-02-18 18:29
- Delivery End: 2021-02-18 18:30
- Data Collect End: 2021-02-25 18:21 (highlighted by a red box)
- Restricted To Work Hours: Yes (radio button selected)
- Work hours: From 07:00 to 19:00

A red box highlights the 'Data Collect End' date input field. The 'Save Changes' button is located in the top right corner.

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.

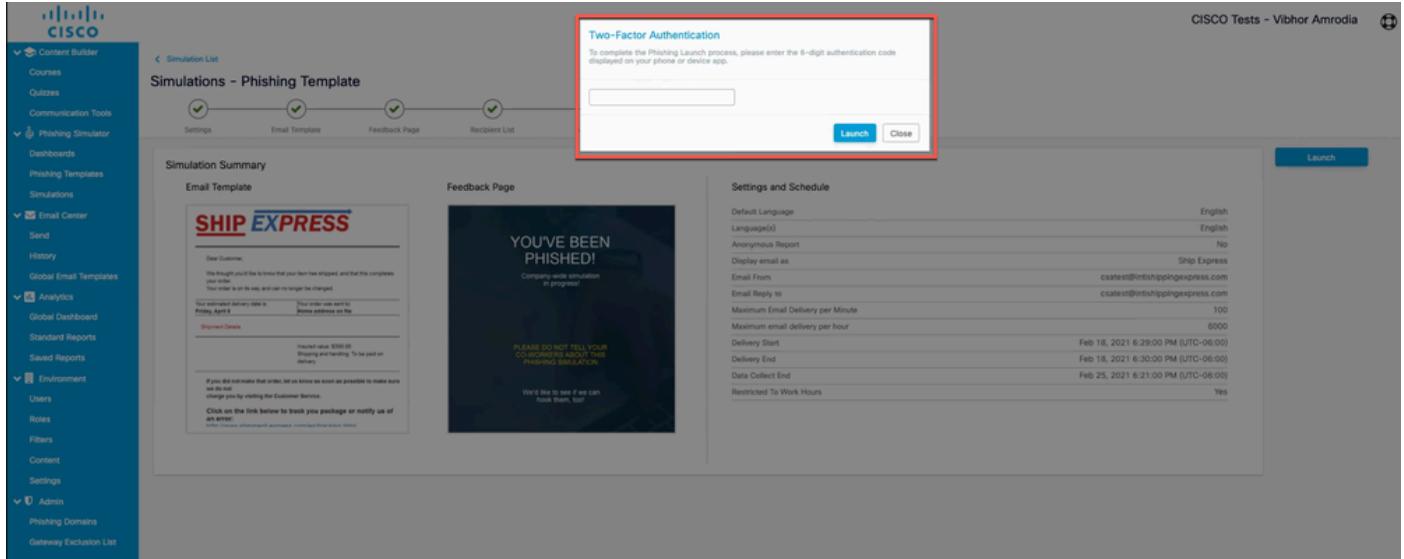
The screenshot shows the 'Simulations - Phishing Template' configuration interface. The 'Launch' tab is active. Key sections include:

- Simulation Summary:**
  - Email Template: Shows a preview of the phishing email from 'SHIP EXPRESS' with a subject line 'Your order has shipped.'
  - Feedback Page: Shows a preview of the 'YOU'VE BEEN PHISHED!' feedback page.
- Settings and Schedule:**
  - Default Language: English
  - Language(s): English
  - Anonymous Report: No
  - Display email as: Ship Express
  - Email From: csatest@fintishoppingexpress.com
  - Email Reply to: csatest@fintishoppingexpress.com
  - Maximum Email Delivery per Minute: 100
  - Maximum email delivery per hour: 6000
  - Delivery Start: Feb 18, 2021 6:29:00 PM (UTC-06:00)
  - Delivery End: Feb 18, 2021 6:30:00 PM (UTC-06:00)
  - Data Collect End: Feb 25, 2021 6:21:00 PM (UTC-06:00)
  - Restricted To Work Hours: Yes

A red box highlights the 'Launch' button. The 'Feedback Page' and 'Settings and Schedule' sections are also visible.

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 Launch comme 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 à Phishing 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.

The screenshot shows the Cisco Content Builder Dashboard. The left sidebar includes options like Content Builder, Courses, Quizzes, Communication Tools, Phishing Simulator, Dashboards, Phishing Templates, Simulations, Email Center, Analytics, and Admin. The main dashboard has sections for 'Currently active simulation list' (listing 'Phishing Template for CSA demo' with details like Launch date: Feb 18, 2021 6:29:00 PM (UTC-06:00), Completed date: Feb 18, 2021 6:30:00 PM (UTC-06:00), Type: Standard, Total Recipients: 1, Status: Active, Default Language: English) and 'Recipient actions summary' (a donut chart showing 0% total actions performed). A red box highlights the 'Export to PDF' button in the top right corner of the simulation statistics table.

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.

**Message**

Delete Archive Reply Reply to All Forward Attachment Move Junk Rules Move to Other Read/Unread Categorise Follow Up Send to OneNote

**Your Ship EXpress Order was shipped**

A **AppleService <apple-service@apple-service.com>** Today at 12:52 PM  
To: **Ramanjaneya Devi Madem (ramadem)**

**To protect your privacy, some pictures in this message were not downloaded.** [Download pictures](#)

---

Dear Customer,

We thought you'd like to know that your item has shipped, and that this completes your order. Your order is on its way, and can no longer be changed.

---

|  |  |
|--|--|
| Your estimated delivery date is:<br><b>Friday, April 8</b> | Your order was sent to:<br><b>Home address on file</b> |
|--|--|

---

**Shipment Details**

---

Insured value: \$300.00  
Shipping and handling: To be paid on delivery

---

**If you did not make that order, let us know as soon as possible to make sure we do not charge you by visiting the Customer Service.**

**Click on the link below to track you package or notify us of an error:**  
<http://www.shipment-express.com/en/tracking.html>

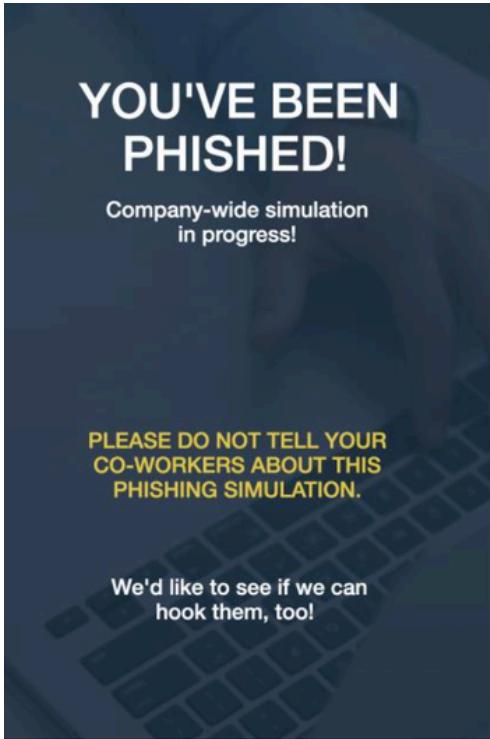
We hope to serve you again soon!  
**Ship Express**

---

© Copyright 2016 Ship Express Inc. We understand the importance of privacy to our customers.

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.



Beware of the warning signs!

**From:** do-not-reply@intlshippingexpress.com  
**To:** Your email  
**Subject:** Your Ship EXpress Order was shipped

**SHIP EXPRESS**

Dear Customer,

We thought you'd like to know that your item has shipped, and that this completes your order. Your order is on its way, and can no longer be changed.

|   |   |
|---|---|
| Your estimated delivery date is:<br>Friday, April 8 | Your order was sent to:<br>Home address on file |
|---|---|

**Shipment Details**

|   |
|---|
| Insured value: \$ 300.00                      |
| Shipping and handling: To be paid on delivery |

If you did not make that order, let us know as soon as possible to make sure we do not charge you by visiting the Customer Service.

Click on the link below to track you package or notify us of an error:  
<http://www.shipment-express.com/en/tracking.html>

We hope to serve you again soon!  
**Ship Express**

© Copyright 2016 Ship Express Inc. We understand the importance of privacy to our customers.

## ALWAYS REMEMBER

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 sous Analytics > Standard Reports > Phishing Simulations > Repeat Clickers as shown in the image.

| Last Name | First Name | Email               | Language        | Time Zone   | Passed Simulations | Failed Simulation | Send Email | Received Emails | Opened Emails | Viewed Images | Clicked Link | Opened Attachment | Completed Form | Visited Page | Feedback Form | Reported Emails | Send Email (Double Barrel) | Received Emails (Double Barrel) | Opened Emails (Double Barrel) | Viewed Images (Double Barrel) |
|-----------|------------|---------------------|-----------------|-------------|--------------------|-------------------|------------|-----------------|---------------|---------------|--------------|-------------------|----------------|--------------|---------------|-----------------|----------------------------|---------------------------------|-------------------------------|-------------------------------|
| Madem     | Rama       | ramadem@cisco.com   | English         | (UTC-08:00) | 2                  | 19                | 21         | 19              | 19            | 5             | 19           | 0                 | 0              | 18           | 0             | 0               | 0                          | 0                               | 0                             |                               |
| Sastr     | Abhilash   | abshastr@cisco.com  | French          | (UTC+05:30) | 8                  | 13                | 21         | 13              | 13            | 13            | 10           | 0                 | 0              | 9            | 0             | 0               | 0                          | 0                               | 0                             |                               |
| Kiran     | Chandra    | ccherinup@cisco.com | French - France | (UTC+05:30) | 13                 | 9                 | 22         | 9               | 9             | 0             | 9            | 0                 | 0              | 8            | 0             | 0               | 0                          | 0                               | 0                             |                               |

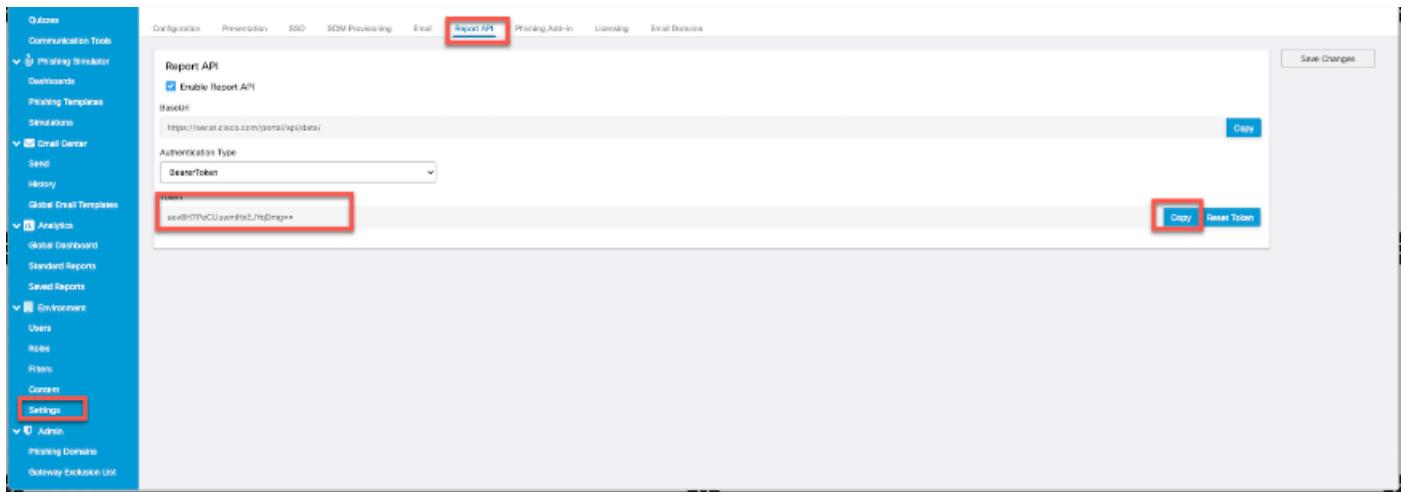
Capture d'écran de la page Repeat Clickers

## 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

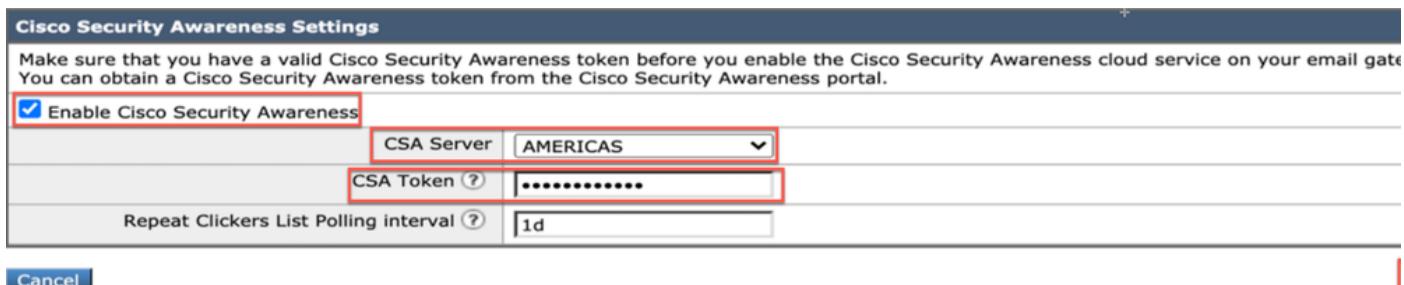
main !



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:                        | <input type="radio"/> Use Default (On) | <input type="radio"/> On <input checked="" type="radio"/> Off |
| AMP Detection:                         | <input type="radio"/> Use Default (On) | <input type="radio"/> On <input checked="" type="radio"/> Off |
| Virus Protection:                      | <input type="radio"/> Use Default (On) | <input type="radio"/> On <input checked="" type="radio"/> Off |
| Sender Domain Reputation Verification: | <input type="radio"/> Use Default (On) | <input type="radio"/> On <input checked="" type="radio"/> Off |
| Virus Outbreak Filters:                | <input type="radio"/> Use Default (On) | <input type="radio"/> On <input checked="" type="radio"/> Off |
| Advanced Phishing Protection:          | <input type="radio"/> Use Default (On) | <input type="radio"/> On <input checked="" type="radio"/> Off |
| Graymail Detection:                    | <input type="radio"/> Use Default (On) | <input type="radio"/> On <input checked="" type="radio"/> Off |
| Content Filters:                       | <input type="radio"/> Use Default (On) | <input type="radio"/> On <input checked="" type="radio"/> Off |
| Message Filters:                       | <input type="radio"/> Use Default (On) | <input type="radio"/> On <input checked="" type="radio"/> 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 Location à partir duquel les e-mails de campagne d'hameçonnage sont envoyés.

Naviguez jusqu'à Mail Policies > HAT Overview > Add Sender Group > Submit and Add Senders > Add the sender IP > Submit

et Commit modifiez comme indiqué dans l'image.

| Sender Group Settings  |  |
|--|--|
| Name:  | CyberSec_Awareness_Allowed   |
| Order:   | 1  |
| Comment:   | CyberSec_Awareness_Allowed   |
| Policy:  | CYBERSEC_AWARENESS_ALLOWED   |
| SBRS (Optional):   | <input type="text"/> to <input type="text"/><br><input type="checkbox"/> Include SBRS Scores of "None"<br>Recommended for suspected senders only.  |
| External Threat Feeds (Optional):<br>For IP lookups only   | Source Name<br><input type="button" value="Add Row"/><br><input type="button" value="Select Source"/>  |
| DNS Lists (Optional): ?  | (e.g. 'query.blocked_list.example, query.blocked_list2.example')   |
| Connecting Host DNS Verification:  | <input type="checkbox"/> Connecting host PTR record does not exist in DNS.<br><input type="checkbox"/> Connecting host PTR record lookup fails due to temporary DNS failure.<br><input type="checkbox"/> Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A). |
| <input type="button" value="Cancel"/> <input type="button" value="Submit"/> <input type="button" value="Submit and Add Senders &gt;&gt;"/> |  |

Capture d'écran d'un groupe d'expéditeurs CyberSec\_Awareness\_Allowed avec la stratégie de flux de messages « CYBERSEC\_AWARENESS\_ALLOWED » sélectionnée.

| Sender Details  |   |
|---|---|
| Sender Type:  | <input checked="" type="radio"/> IP Addresses <input type="radio"/> Geolocation |
| Sender: ?   | 52.242.31.199<br>(IPv4 or IPv6)   |
| Comment:  | Configured as CSA NAM(AMERICA)  |
| <input type="button" value="Cancel"/> <input type="button" value="Submit"/> |   |

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

#### Configuration CLI :

- Accédez à listenerconfig > Edit > Inbound (PublicInterface) > HOSTACCESS > NEW > New Sender Group .
- Créez un nouveau groupe d'expéditeurs avec une stratégie de CYBERSEC\_AWARENESS\_ALLOWED messagerie et ajoutez une adresse IP/un domaine d'expéditeur à partir duquel les e-mails de campagne d'hameçonnage sont initiés.
- Définissez l'ordre du nouveau groupe d'expéditeurs sur 1 et utilisez l'option sous listenerconfig > EDIT > Inbound (PublicInterface) > HOSTACCESS > MOVE .
- 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 |
|---|----------------------------------|------|
| <a href="https://secat.cisco.com/">https://secat.cisco.com/</a> | 52.242.31.199                    |      |
| Course Notification (Outbound)                                  | 167.89.98.161                    |      |
| Phishing Simulation (Incoming Email Service)                    | 207.200.3.14,<br>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 |
|---|---------------|------|
| <a href="https://secat-eu.cisco.com/">https://secat-eu.cisco.com/</a> | 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 |      |

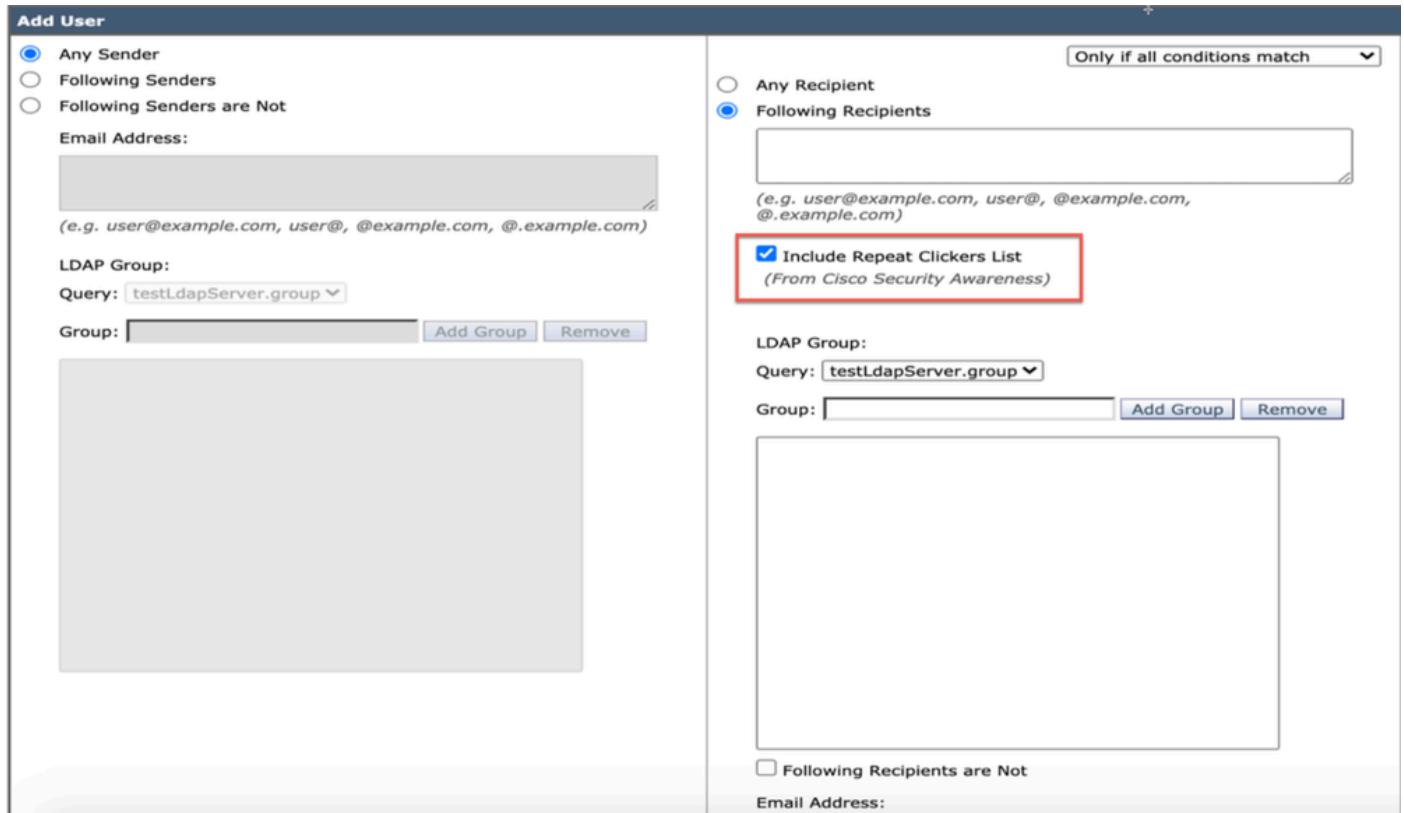
Capture d'écran des adresses IP et noms d'hôte des régions CSA Amériques et UE

### 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_LIST` pour 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 Awareness comme indiqué dans l'image.

Secure Email  
CISCO Cloud Gateway C100V

Sec

Monitor Mail Policies Security Services Network System Administration

## Cisco Security Awareness

| Cisco Security Awareness                              |         |
|---|---------|
| Cisco Security Awareness                              | Enabled |
| Repeat Clickers List Poll Interval <small>(?)</small> | 1d      |
| <a href="#">Edit Settings</a>                         |         |

| Repeat Clickers List Settings |           |                              |        |                 |                             |
|-------------------------------|-----------|------------------------------|--------|-----------------|-----------------------------|
| List Name                     | Report ID | Last Updated                 | Status | Repeat Clickers | Update                      |
| Repeat Clickers               | 2020      | Tue Feb 23 02:24:14 2021 IST | Active | 4               | <a href="#">Update List</a> |

| Cisco Security Awareness Updates |               |                 |               |                            |
|----------------------------------|---------------|-----------------|---------------|----------------------------|
| File Type                        | Last Update   | Current Version | New Update    |                            |
| Cisco Security Awareness Config  | Never Updated | 1.0             | Not Available |                            |
| Cisco Security Awareness Engine  | Never Updated | 1.0             | Not Available |                            |
| No updates in progress.          |               |                 |               | <a href="#">Update Now</a> |

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.