

Configuración de la integración del reconocimiento de seguridad con Cisco Secure Email Gateway

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Crear y enviar simulaciones de phishing desde el servicio en la nube CSA](#)

[Paso 1. Inicie sesión en CSA Cloud Service](#)

[Paso 2. Crear un destinatario de correo electrónico de phishing](#)

[Paso 3. Habilitar la API de informes](#)

[Paso 4. Crear simulaciones de phishing](#)

[Paso 5. Verificación de simulaciones activas](#)

[¿Qué se ve en el lado del destinatario?](#)

[Verificar en CSA](#)

[Configuración de Secure Email Gateway](#)

[Paso 1. Habilite la función Cisco Security Awareness en Secure Email Gateway](#)

[Paso 2. Permitir correos electrónicos de phishing simulados desde el servicio en la nube CSA](#)

[Paso 3. Actúe en Repeat Clicker de SEG](#)

[Guía de Troubleshooting](#)

[Información Relacionada](#)

Introducción

Este documento describe los pasos necesarios para configurar la integración de Cisco Security Awareness (CSA) con Cisco Secure Email Gateway.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conceptos y configuración de Cisco Secure Email Gateway
- Servicio CSA Cloud

Componentes Utilizados

La información de este documento se basa en AsyncOS para SEG 14.0 y versiones posteriores.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Crear y enviar simulaciones de phishing desde el servicio en la nube CSA

Paso 1. Inicie sesión en CSA Cloud Service

Consulte:

1. <https://secat.cisco.com/> para la región de AMÉRICA
2. <https://secat-eu.cisco.com/> para la región de EUROPA

Paso 2. Crear un destinatario de correo electrónico de phishing

Desplácese hasta **Environment > Users > Add New User** los campos Correo electrónico, Nombre, Apellidos e Idioma y rellénelos y, a continuación, haga clic en **Save Changes** como se muestra en la imagen.

The screenshot shows the 'Add New User' form in the CSA Cloud Service interface. The form is titled 'User - Profile' and contains the following fields:

- Email: ciscotac@cisco.com
- First Name: Cisco
- Last Name: TAC
- Language: English
- Time Zone: (UTC-06:00) Central Time (US & Canada)
- None: None
- External UID: External UID
- Username: Use Email ciscotac@cisco.com
- SET PASSWORD: SET PASSWORD
- Manager: Name or Email

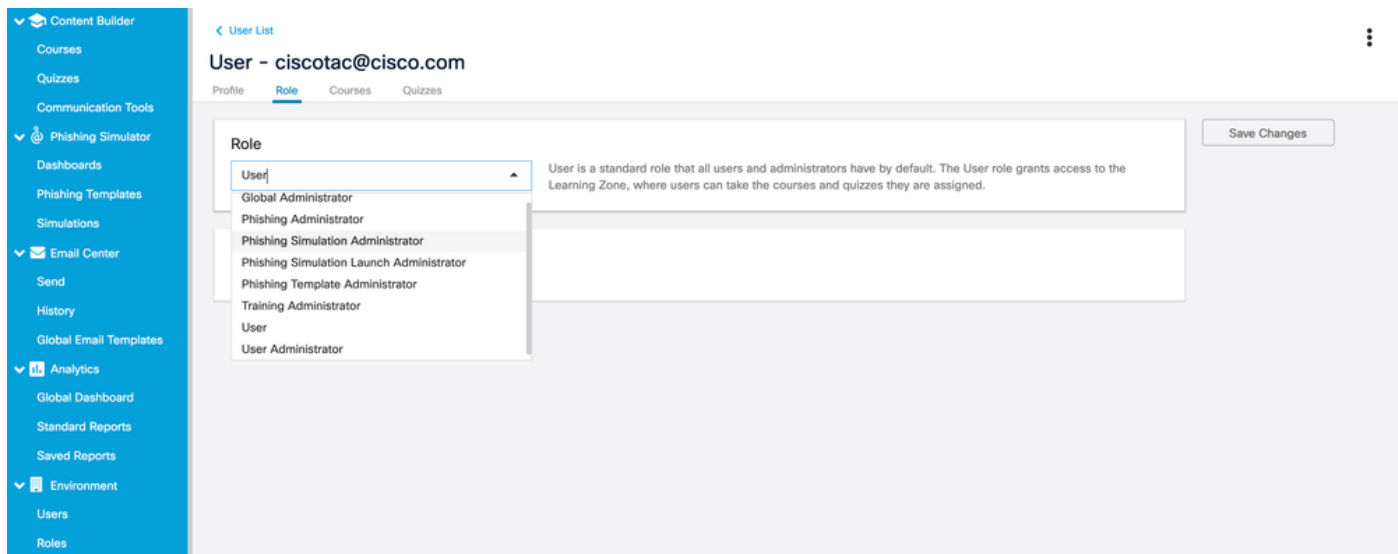
A red box highlights the 'Save Changes' button in the top right corner. Red arrows point to the 'Email', 'First Name', and 'Last Name' fields with the text 'Fill this'.

Captura de pantalla de la página de interfaz de usuario para agregar un nuevo usuario



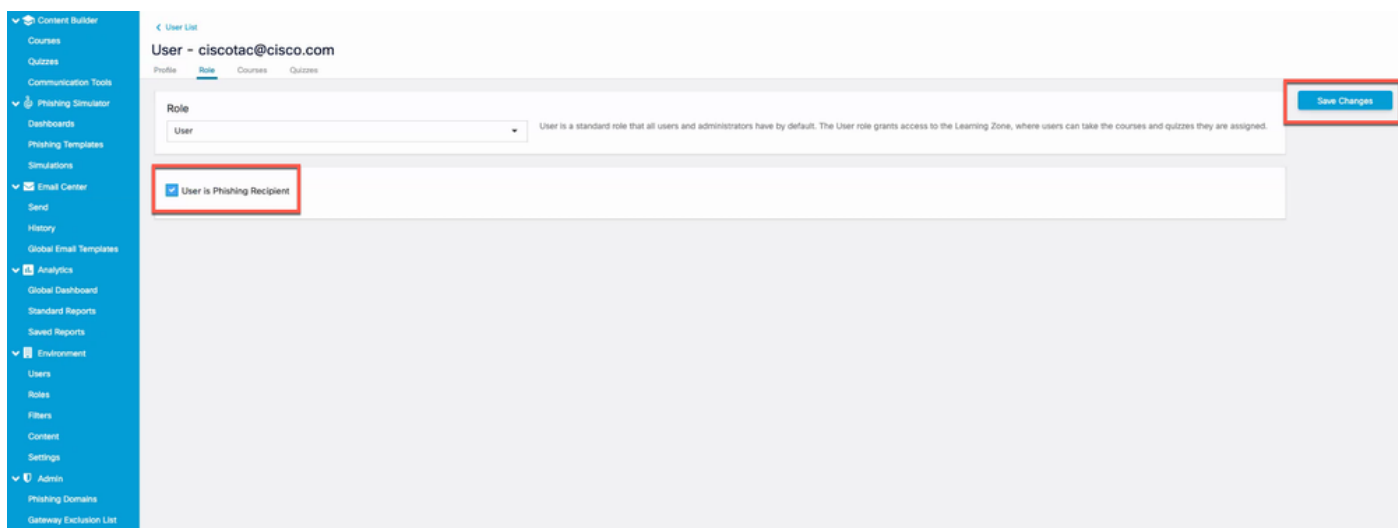
Nota: Solo se debe establecer una contraseña para un usuario administrador de CSA que esté autorizado para crear e iniciar simulaciones.

La función del usuario se puede seleccionar una vez creado el usuario. Puede seleccionar el rol en el menú desplegable como se indica en esta imagen:



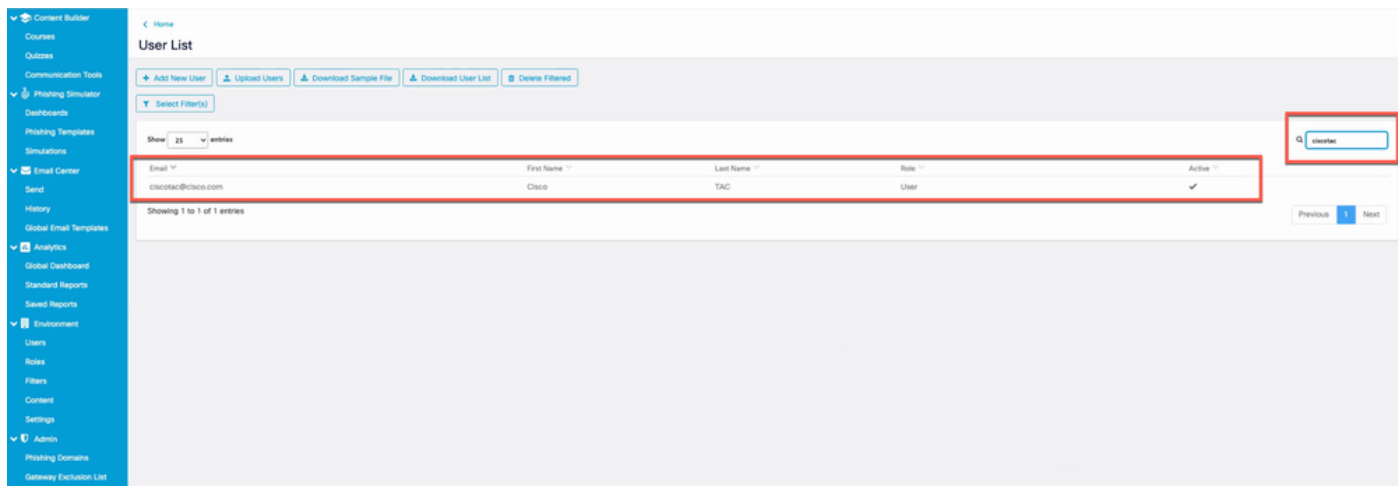
Vista de las opciones del menú desplegable de la función de usuario

Seleccione la **User is Phishing Recipient** > Save Changes casilla de verificación como se muestra en la imagen.



captura de pantalla que muestra que la casilla de verificación "El usuario es un destinatario de phishing" está activada

Compruebe que el usuario se ha agregado correctamente y que aparece en la lista cuando se realiza una búsqueda en función de la dirección de correo electrónico del filtro, como se muestra en la imagen.



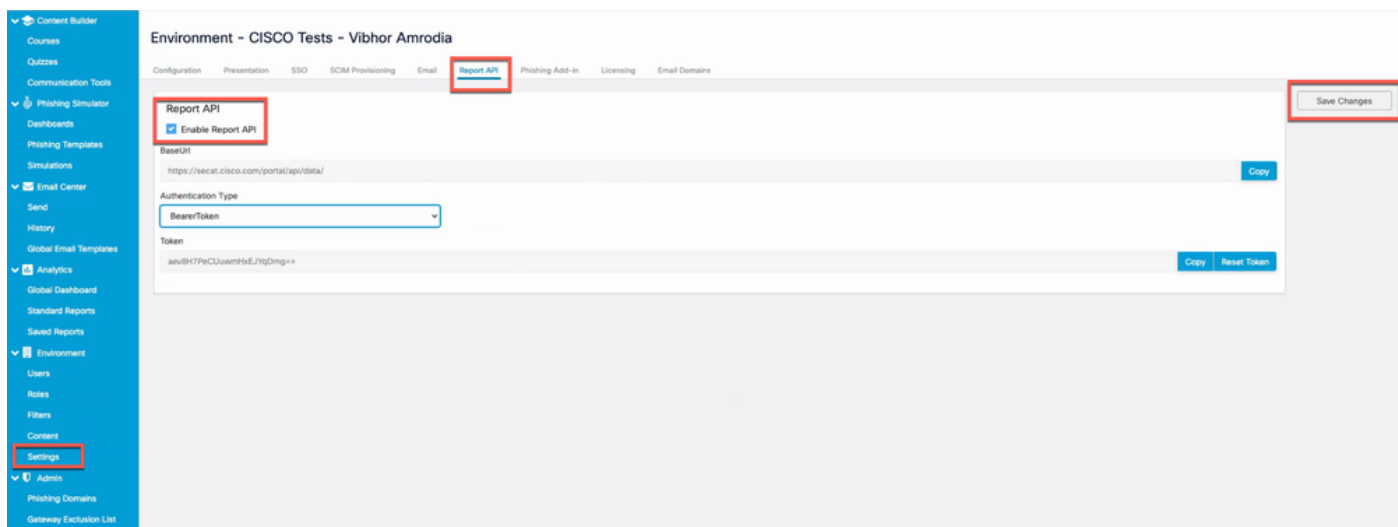
Captura de pantalla del nuevo usuario en la lista de usuarios

Paso 3. Habilitar la API de informes

Vaya a la **Environments > Settings > Report API** pestaña y active **Enable Report API > Save Changes** la opción.



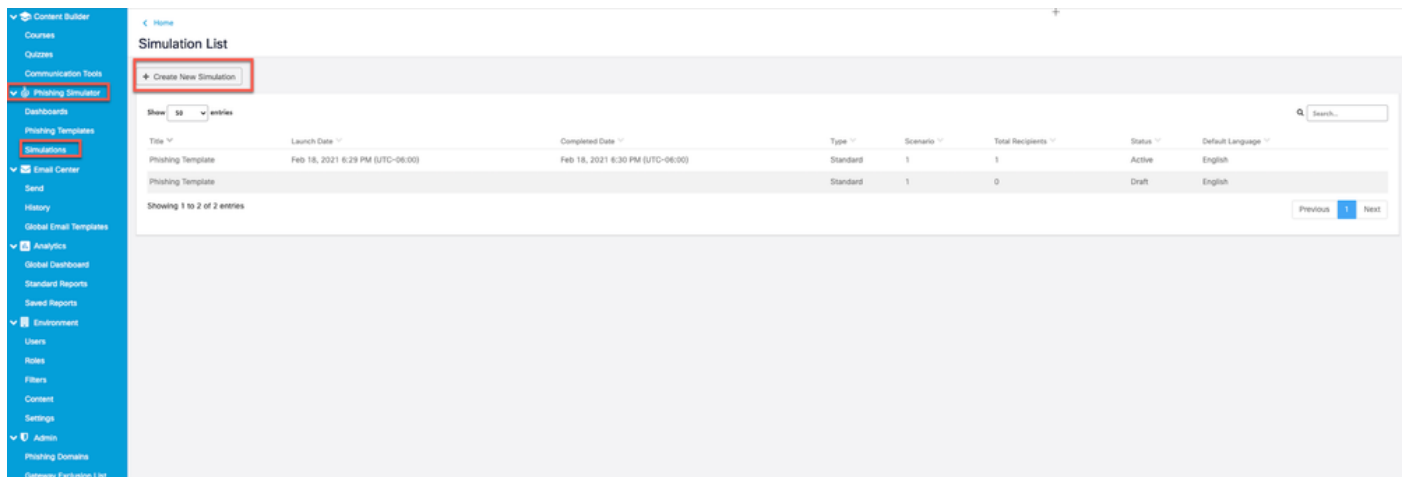
Nota: Tome nota del token portador. Esto es necesario para integrar el SEG con CSA.



Captura de pantalla que muestra que la casilla de verificación "Activar API de informe" está activada.

Paso 4. Crear simulaciones de phishing

a. Desplácese hasta **Phishing Simulator > Simulations > Create New Simulation** y **seleccione un Template** en la lista disponible, como se muestra en la imagen.



Captura de pantalla que resalta el botón "Crear nueva simulación"

b. Rellene esta información:

1. Seleccione un nombre para la plantilla.
2. Describa la plantilla.
3. Nombre de dominio con el que se envía el correo electrónico de suplantación de identidad.
4. El nombre para mostrar del correo electrónico de suplantación de identidad.
5. Dirección de correo electrónico del remitente (seleccione en el menú desplegable).
6. Dirección de respuesta (seleccione en el menú desplegable).
7. Seleccione el idioma.
8. Guarde los cambios.

Simulation List

Simulations -

Name 1 → Phishing Template

Description 2 → Phishing template for CSA demo

Anonymous Report ☐

Email Settings

Domain Name 3 → intshippingexpress.com

Display email as 4 → Ship Express

Email - From 5 → csatest @ intshippingexpress.com

Email - Reply to 6 → csatest @ intshippingexpress.com

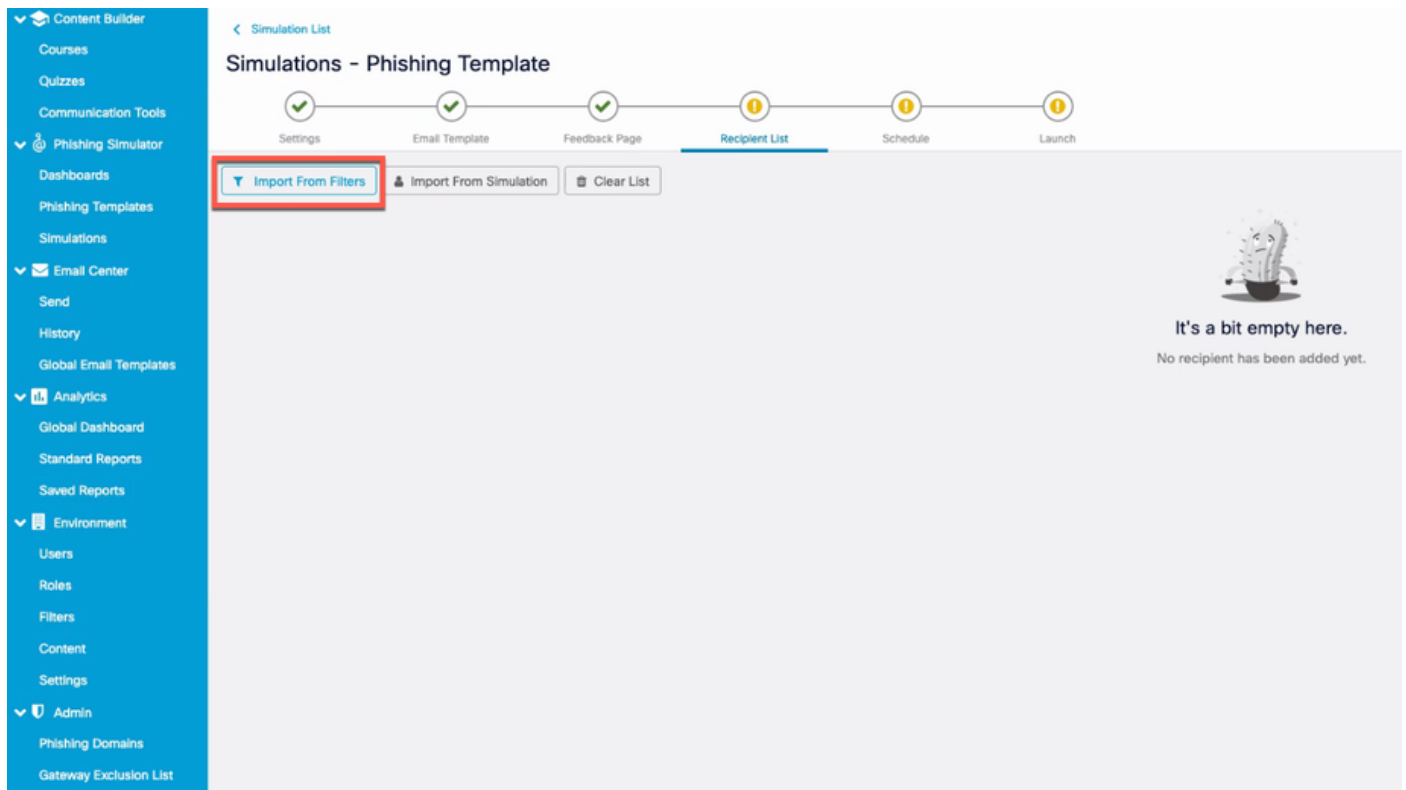
Languages (1)

Primary Language(*) 7 → English

Save Changes 8

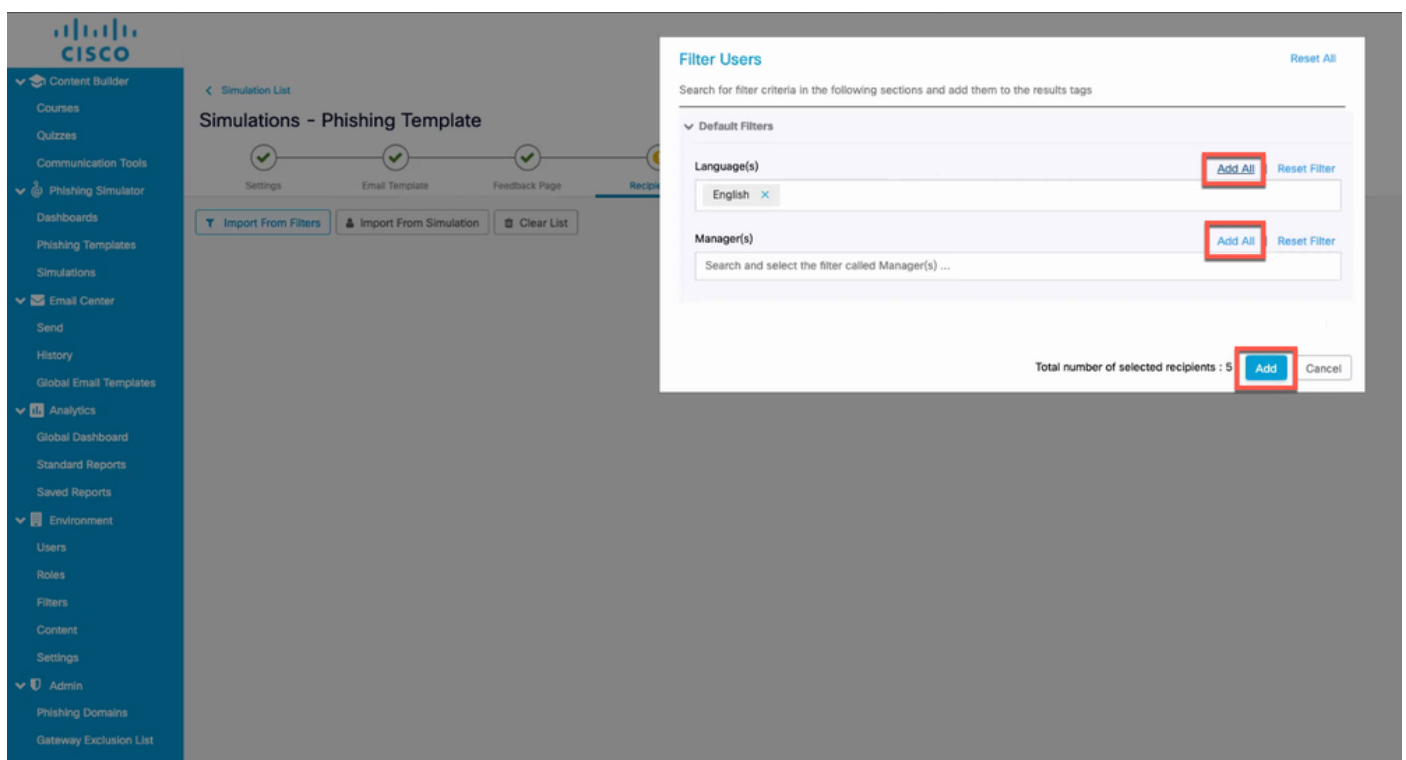
Captura de pantalla que resalta los campos que se deben rellenar para configurar una nueva simulación

c. Haga clic en Import from Filters y agregue los destinatarios de correo electrónico de suplantación de identidad a Recipient List como se muestra en la imagen .



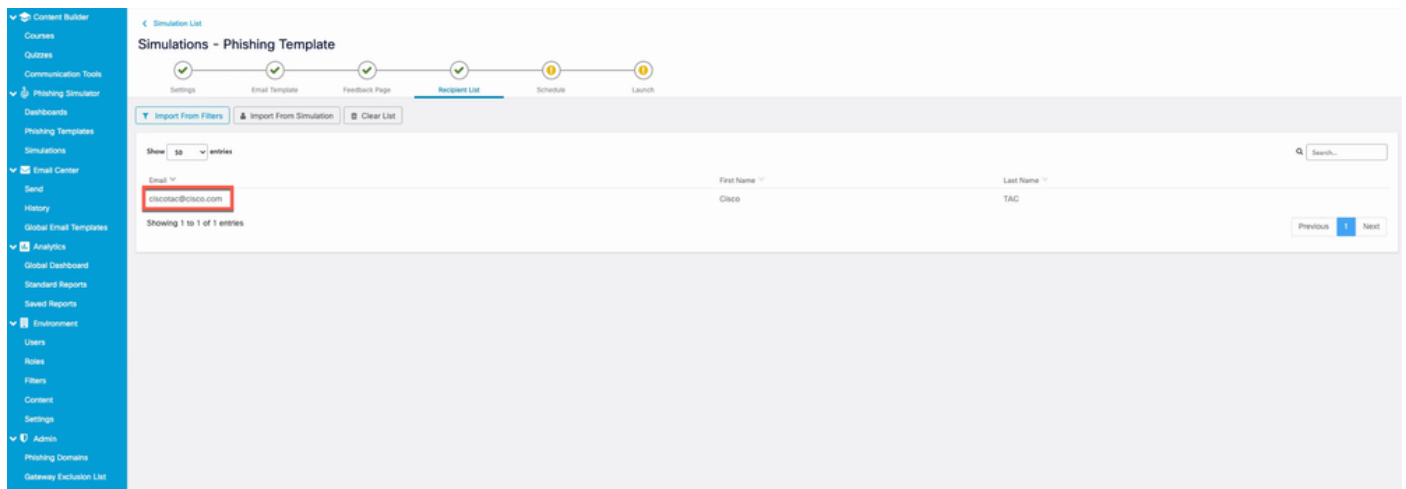
Captura de pantalla que resalta el botón "Importar de filtros"

Puede filtrar los usuarios por idioma o por jefes. Haga clic en Add como se muestra en la imagen.



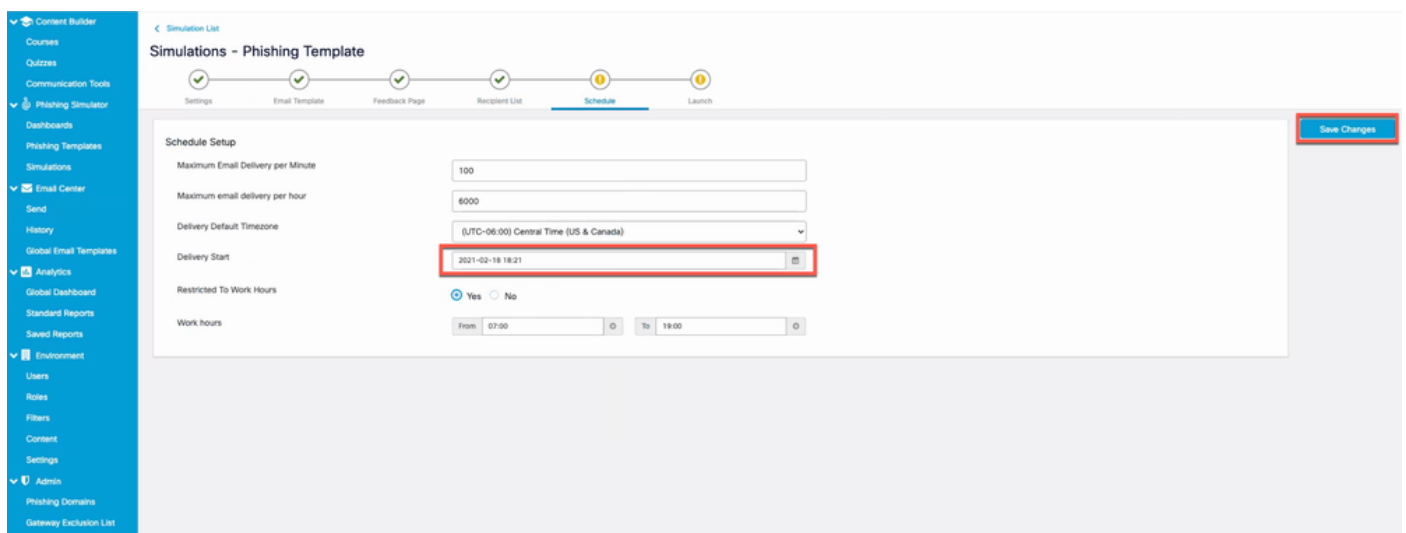
Captura de pantalla del cuadro de diálogo Filtrar usuarios para filtrar por idioma o administrador

Aquí hay un ejemplo del usuario que se creó en el Paso 2, que ahora se agrega a la lista de destinatarios como se muestra en la imagen.



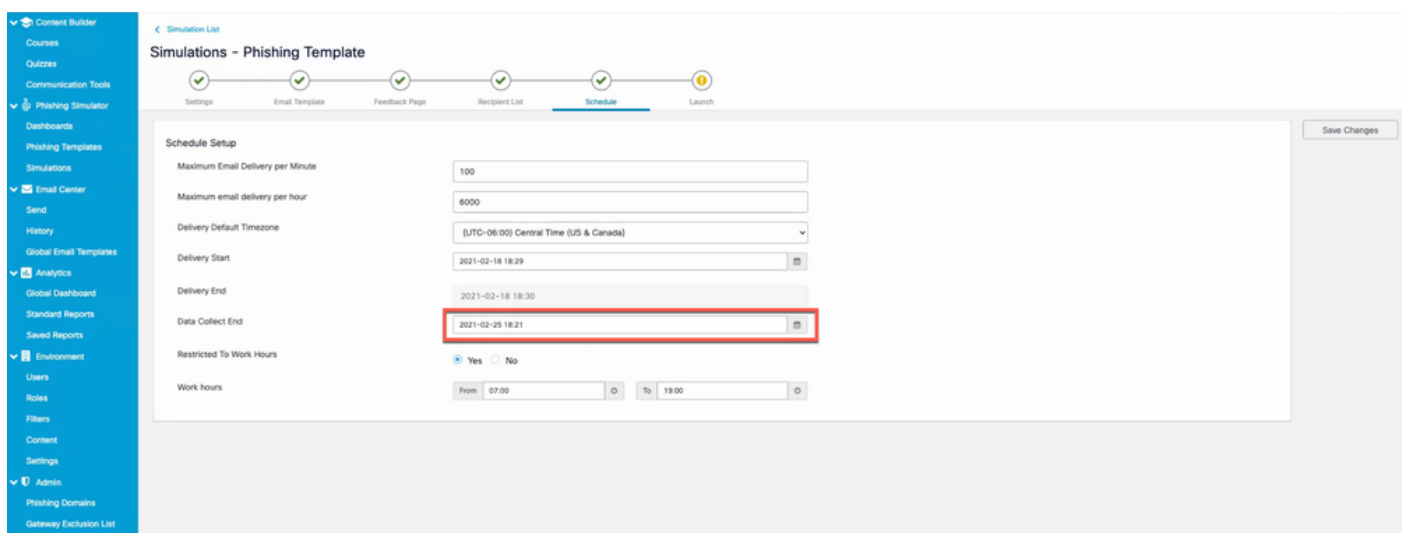
Captura de pantalla del usuario creado anteriormente que aparece como destinatario de la simulación de phishing

d. Establezca la fecha y los cambios para programar la campaña como se muestra en la imagen.



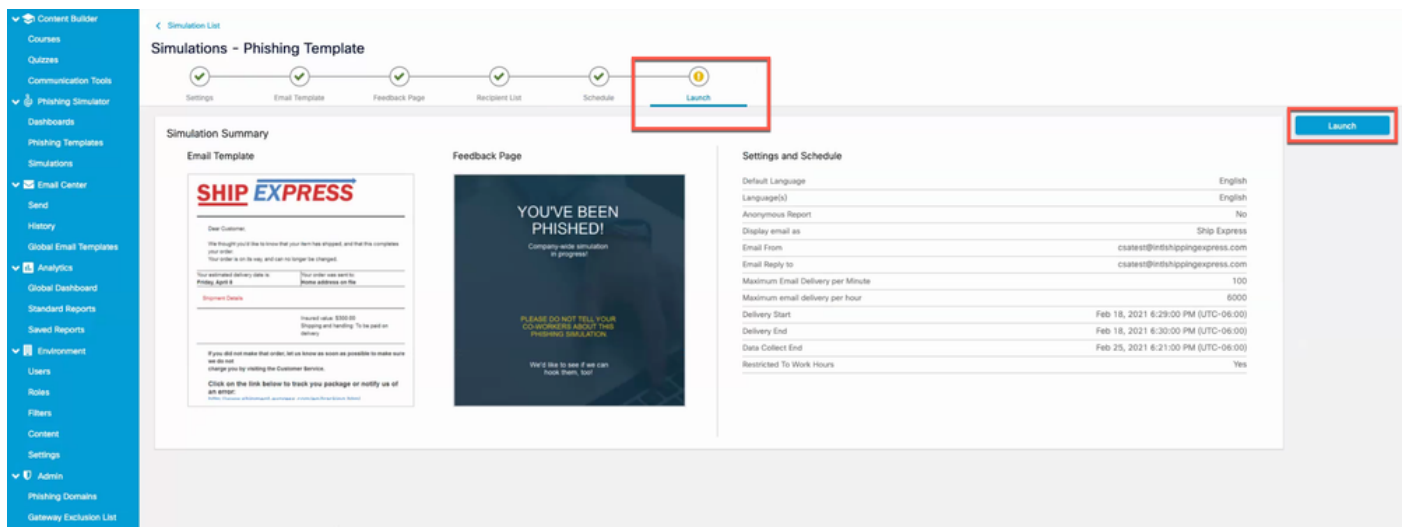
Captura de pantalla que resalta el campo de inicio de entrega

Una vez que se ha elegido la fecha de inicio, la opción **end date** para seleccionar la campaña está habilitada, como se muestra en la imagen.



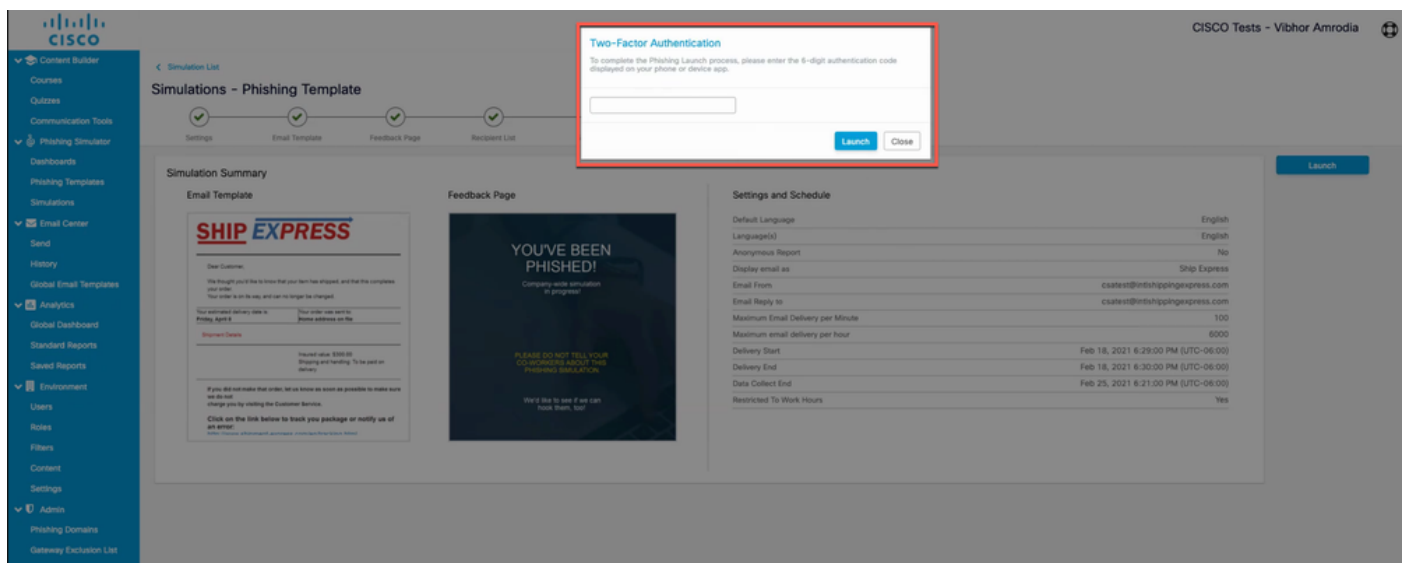
Captura de pantalla de resaltar el campo Data Collect End que designa cuándo debe terminar la simulación

e. Haga clic en Launch para iniciar la campaña, como se muestra en la imagen.



Captura de pantalla de la pestaña final del asistente de creación de simulaciones donde se puede iniciar la campaña

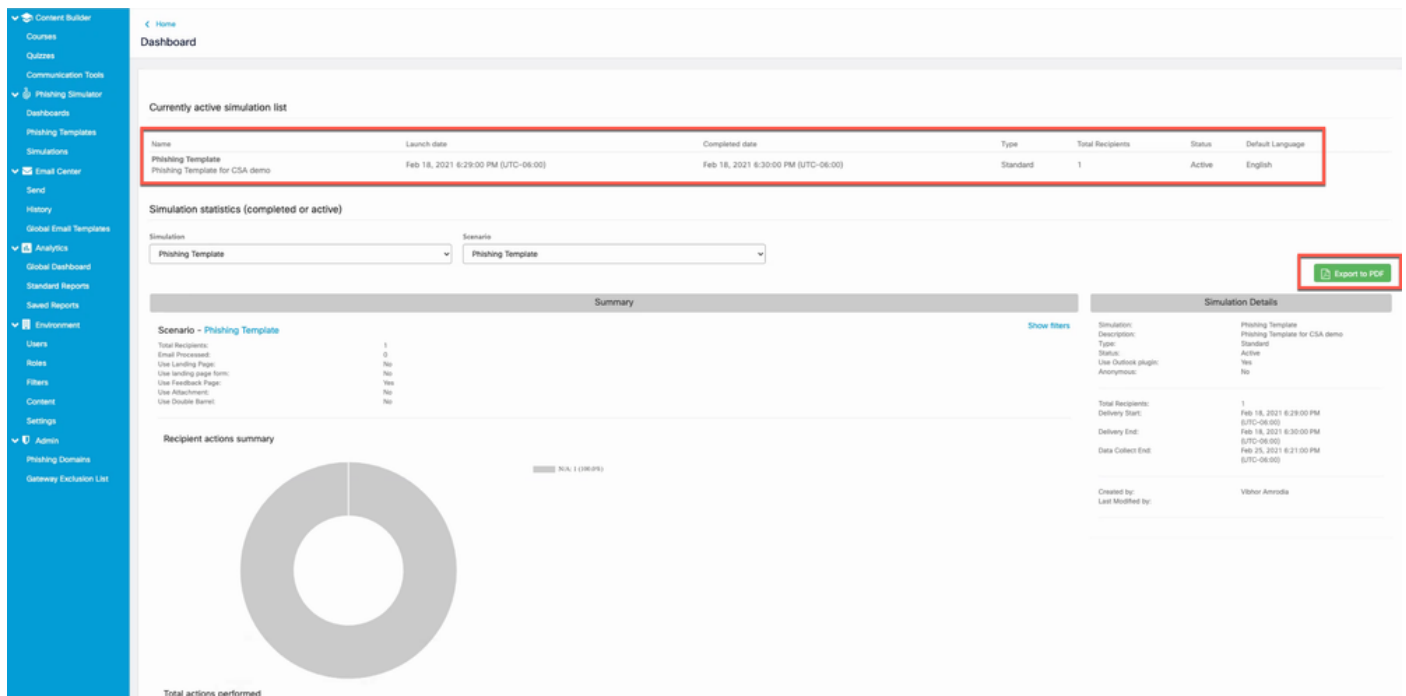
Se puede solicitar un código de autenticación de dos factores después de hacer clic en el botón de inicio. Introduzca el código y haga clic en Launch como se muestra en la imagen.



Captura de pantalla de la ventana emergente donde se solicita el código de autenticación de dos factores

Paso 5. Verificación de simulaciones activas

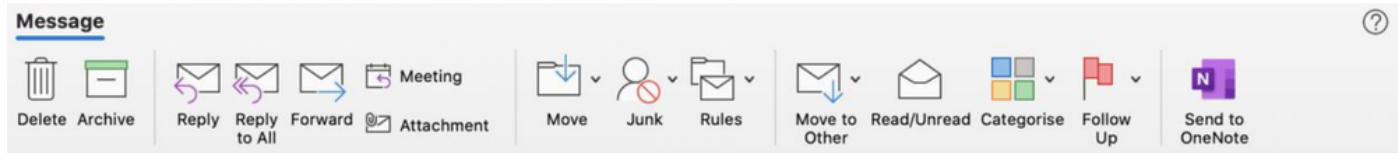
Vaya a .Phishing Simulator > Dashboards La lista actual de simulaciones activas proporciona las simulaciones activas. También puede hacer clic Export as PDF y obtener el mismo informe que se muestra en la imagen.



Captura de pantalla del panel de simulaciones de phishing

¿Qué se ve en el lado del destinatario?

Ejemplo de un correo electrónico de simulación de phishing en la bandeja de entrada del destinatario.



Your Ship EXpress Order was shipped



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:
Friday, April 8

Your order was sent to:
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.

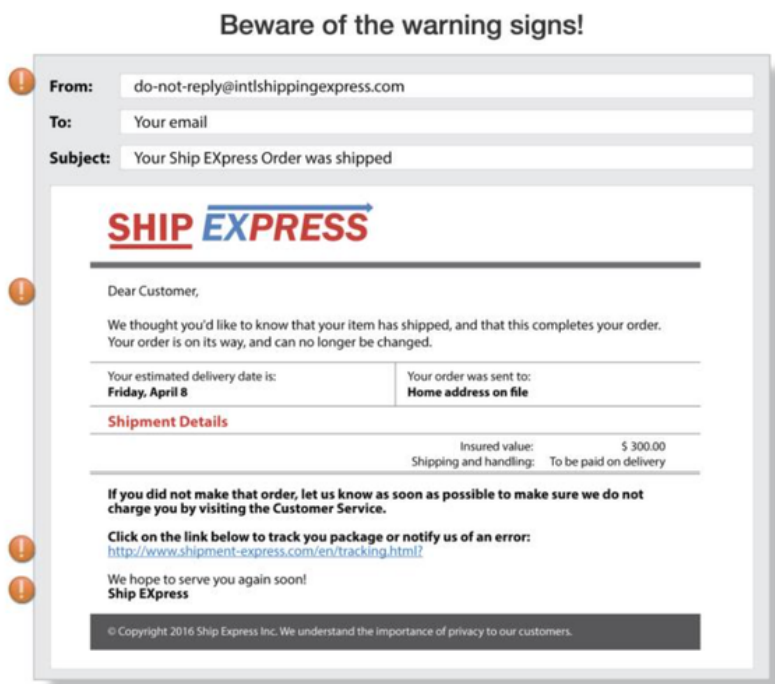
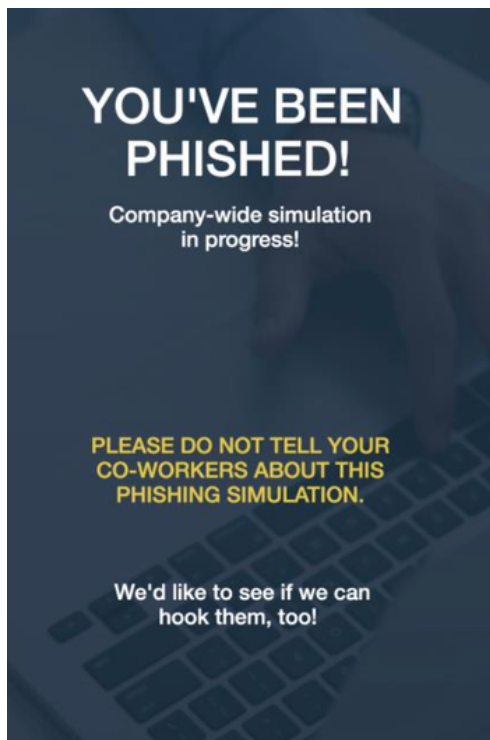
Click on the link below to track you package or notify us of an error:
<http://www.shipment-express.com/en/tracking.html>

We hope to serve you again soon!
Ship Express

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

Ejemplo de correo electrónico simulado de phishing en un buzón de correo de usuario

Cuando el destinatario hace clic en la URL, se muestra esta página de comentarios al usuario y este usuario aparece como parte de la lista Repetir clickers (que ha hecho clic libremente en la URL de phish) en CSA.



ALWAYS REMEMBER

Ejemplo de la página de comentarios que verá el usuario después de hacer clic en la URL del correo electrónico de phishing

Verificar en CSA

La lista Repetir clics se muestra debajo de Analytics > Standard Reports > Phishing Simulations > Repeat Clickers as shown in the image.

CISCO

Content Builder

Courses

Quizzes

Communication Tools

Phishing Simulator

Dashboards

Phishing Templates

Simulations

Email Center

Send

History

Global Email Templates

Analytics

Gamification Dashboard

Standard Reports

Seved Reports

Environment

Users

Filters

Content

Repeat Clickers

Parameters / Filters

Show50entries

Search...

Last Name	First Name	Email	Language	Time Zone	Passed Simulations	Failed Simulation	Sent Email	Received Emails	Opened Emails	Viewed Images	Clicked Link	Opened Attachment	Completed Form	Visited Feedback Page	Reported Emails	Send Email (Double Barrel)	Received Emails (Double Barrel)	Opened Emails (Double Barrel)	Views Image (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	
Sastry	Abhilash	abshastr@cisco.com	French	(UTC+05:30)	8	13	21	13	13	13	10	0	0	9	0	0	0	0	
Kiran	Chandra	ccchennup@cisco.com	French - France	(UTC+05:30)	13	9	22	9	9	0	9	0	0	8	0	0	0	0	

Showing 1 to 3 of 3 entries

Previous

1

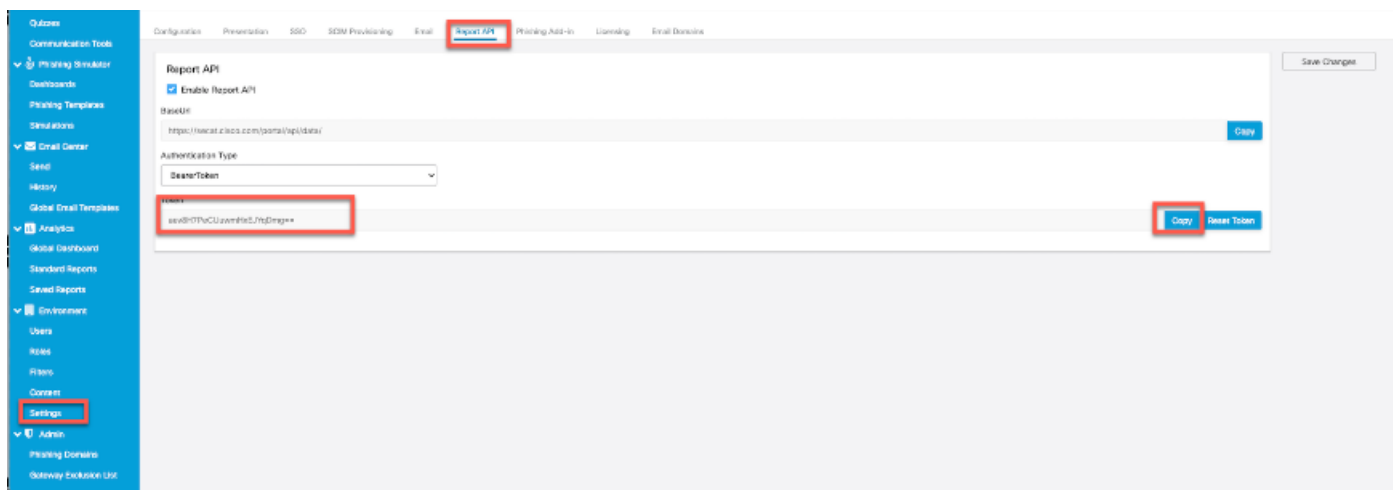
Next

Captura de pantalla de la página Repeat Clickers

Configuración de Secure Email Gateway



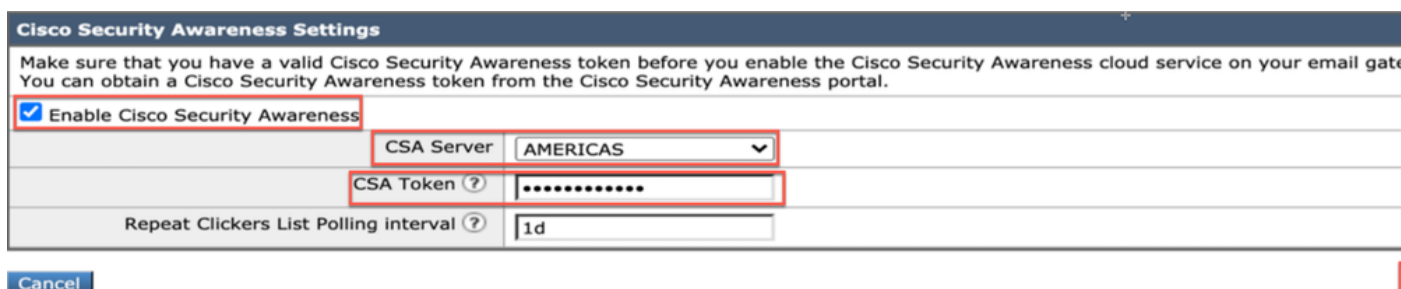
Nota: En la sección Create and Send Phishing Simulations de CSA Cloud Service Paso 3. cuando habilita Report API , ha anotado el token portador. Mantén esto a mano.



Captura de pantalla de la página de la API de informe, donde el administrador puede encontrar el token portador

Paso 1. Habilite la función Cisco Security Awareness en Secure Email Gateway

En la GUI de Secure Email Gateway, navegue hasta **Security Services > Cisco Security Awareness > Enable**. Enter the Region and the CSA Token (Bearer Token obtenido de CSA Cloud Service como se muestra en la nota mencionada anteriormente) y envíe y confirme los cambios.



Captura de pantalla de la página de configuración de reconocimiento de seguridad de Cisco en Cisco Secure Email Gateway.

Configuración de CLI

Escriba `csaconfig` para configurar CSA a través de la CLI.

```
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
- ```
[1]> 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]>

## Paso 2. Permitir correos electrónicos de phishing simulados desde el servicio en la nube CSA



**Nota:** La `CYBERSEC_AWARENESS_ALLOWED` política Mailflow se crea de forma predeterminada con todos los motores de escaneo desactivados, como se muestra aquí.

| 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 |

Captura de pantalla de la política de flujo de correo "CYBERSEC\_AWARENESS\_ALLOWED" con las funciones de seguridad desactivadas

Para permitir que los correos electrónicos de campaña de phishing simulados del servicio en la nube CSA omitan todos los motores de análisis de Secure Email Gateway:

a. Cree un nuevo grupo de remitentes y asigne la política de flujo `CYBERSEC_AWARENESS_ALLOWED` de correo. Desplácese hasta `Mail Policies > HAT Overview > Add Sender Group` y seleccione la directiva `CYBERSEC_AWARENESS_ALLOWED` y establezca el orden en 1 y, a continuación, `Submit and Add Senders`.

b. Agregue un remitente `IP/domain` o un remitente `Geo Location` desde el que se inician los correos electrónicos de la campaña de phishing.

Desplácese hasta `Mail Polices > HAT Overview > Add Sender Group > Submit and Add Senders > Add the sender IP > Submit/Commit` cambia tal y como se muestra en la imagen.

| 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><i>Recommended for suspected senders only.</i>                                                                                                                                     |             |  |               |                                                                              |
| External Threat Feeds (Optional):<br><i>For IP lookups only</i> | <table border="1"> <thead> <tr> <th>Source Name</th> <th></th> </tr> </thead> <tbody> <tr> <td>Select Source</td> <td> <input type="button" value="Add Row"/> <input type="button" value="Delete"/> </td> </tr> </tbody> </table>                                                            | Source Name |  | Select Source | <input type="button" value="Add Row"/> <input type="button" value="Delete"/> |
| Source Name                                                     |                                                                                                                                                                                                                                                                                              |             |  |               |                                                                              |
| Select Source                                                   | <input type="button" value="Add Row"/> <input type="button" value="Delete"/>                                                                                                                                                                                                                 |             |  |               |                                                                              |
| DNS Lists (Optional): ?                                         | <input type="text"/><br><i>(e.g. 'query.blocked_list.example, query.blocked_list2.example')</i>                                                                                                                                                                                              |             |  |               |                                                                              |
| 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). |             |  |               |                                                                              |

Captura de pantalla de un grupo de remitentes CyberSec\_Awareness\_Allowed con la política de flujo de correo "CYBERSEC\_AWARENESS\_ALLOWED" seleccionada.

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

Captura de pantalla de la página de configuración de reconocimiento de seguridad de Cisco en Cisco Secure Email Gateway.

## Configuración de CLI:

1. Acceda a `listenerconfig > Edit > Inbound (PublicInterface) > HOSTACCESS > NEW > New Sender Group`.
2. Cree un nuevo grupo de remitentes con política de correo CYBERSEC\_AWARENESS\_ALLOWED y agregue una dirección IP/dominio de remitente desde donde se inician los correos electrónicos de la campaña de phishing.
3. Establezca el orden del nuevo grupo de remitentes en 1 y utilice la Move opción de `listenerconfig > EDIT > Inbound (PublicInterface) > HOSTACCESS > MOVE`.
4. Confirmar.



Nota: La IP del remitente es la dirección IP de la CSA y se basa en la región seleccionada. Consulte la tabla para obtener la dirección IP correcta que se debe utilizar. Permita que estas direcciones IP/nombres de host en el firewall con el número de puerto 443 para SEG 14.0.0-xxx se conecten al servicio en la nube 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,<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 |
|----------------------------------------------|---------------|------|
| 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 |      |

Captura de pantalla de las direcciones IP y los nombres de host de las regiones de CSA América y UE

### Paso 3. Actúe en Repeat Clicker de SEG

Una vez que se han enviado los correos electrónicos de suplantación de identidad (phishing) y la lista de repetidores de clickers se ha rellenado en el SEG, se puede crear una política de correo entrante agresiva para realizar acciones sobre el correo a esos usuarios específicos.

Cree una nueva y agresiva política de correo personalizado entrante y active la **Include Repeat Clickers List** casilla de verificación en la sección de destinatarios.

En GUI, desplácese hasta **Mail Policies > Incoming Mail Policies > Add Policy > Add User > Include Repeat Clickers List > Submit y Commit** los cambios.

Captura de pantalla de la política de correo entrante personalizada configurada para manejar el correo destinado a clickers repetidos

## Guía de Troubleshooting

1. Desplácese hasta `csaconfig > SHOW_LIST` para ver los detalles de la lista de pulsadores de repetición.

```
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. Desplácese hasta `csaconfig > UPDATE_LIST` si desea forzar la actualización de la lista de repetidores.

```
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. Siga los registros de csa para ver si se ha descargado la lista de repetidores de clickers o si hay un error. Aquí está el `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. El conteo de la lista de clickers repetidos también se puede ver desde la GUI. Desplácese hasta `Security Services > Cisco Security Awareness` como se muestra en la imagen.

### Cisco Security Awareness

| Cisco Security Awareness                                                                                             |         |
|----------------------------------------------------------------------------------------------------------------------|---------|
| Cisco Security Awareness                                                                                             | Enabled |
| Repeat Clickers List Poll Interval  | 1d      |
| <div>Edit Settings</div>                                                                                             |         |

| 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               | <div>Update List</div> |

| 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.          |               |                 | <div>Update Now</div> |

Captura de pantalla de la página Servicios de seguridad > Reconocimiento de seguridad de Cisco que destaca el número de clickers repetidos

### Información Relacionada

- [Soporte Técnico y Documentación - Cisco Systems](#)

#### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).