

Configurazione dell'integrazione di consapevolezza della sicurezza con Cisco Secure Email Gateway

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Crea e invia simulazioni di phishing dal servizio cloud CSA](#)

[Passaggio 1. Accedere al servizio cloud CSA](#)

[Passaggio 2. Creazione di un destinatario di posta elettronica di phishing](#)

[Passaggio 3. Abilita API report](#)

[Passaggio 4. Creazione di simulazioni di phishing](#)

[Passaggio 5. Verifica delle simulazioni attive](#)

[Cosa si vede a lato del destinatario?](#)

[Verifica su CSA](#)

[Configurazione di Secure Email Gateway](#)

[Passaggio 1. Abilitare la funzionalità di consapevolezza della sicurezza di Cisco in Secure Email Gateway](#)

[Passaggio 2. Consenti messaggi di phishing simulati dal servizio cloud CSA](#)

[Passaggio 3. Eseguire un'azione quando si fa clic con il pulsante Ripeti da SEG](#)

[Guida alla risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare l'integrazione di Cisco Security Awareness (CSA) con Cisco Secure Email Gateway.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Concetti e configurazione di Cisco Secure Email Gateway
- Servizio cloud CSA

Componenti usati

Le informazioni di questo documento si basano su AsyncOS per SEG 14.0 e versioni successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Crea e invia simulazioni di phishing dal servizio cloud CSA

Passaggio 1. Accedere al servizio cloud CSA

Per ulteriori informazioni, fare riferimento a:

1. <https://secat.cisco.com/> per le Americhe

2. <https://secat-eu.cisco.com/> per l'Europa

Passaggio 2. Creazione di un destinatario di posta elettronica di phishing

Individuare **Environment > Users > Add New User** e compilare i campi Posta elettronica, Nome, Cognome e Lingua, quindi fare clic **Save Changes** come mostrato nell'immagine.

The screenshot shows the 'User - Profile' form in the CSA interface. The left sidebar has 'Environment' expanded, with 'Users' selected. The form fields are as follows:

Field	Value
Email	ciscotac@cisco.com
First Name	Cisco
Last Name	TAC
Language	English
Time Zone	(UTC-06:00) Central Time (US & Canada)
External UID	External UID
Username	☒ Use Email ciscotac@cisco.com
SET PASSWORD	SET PASSWORD
Manager	Name or Email

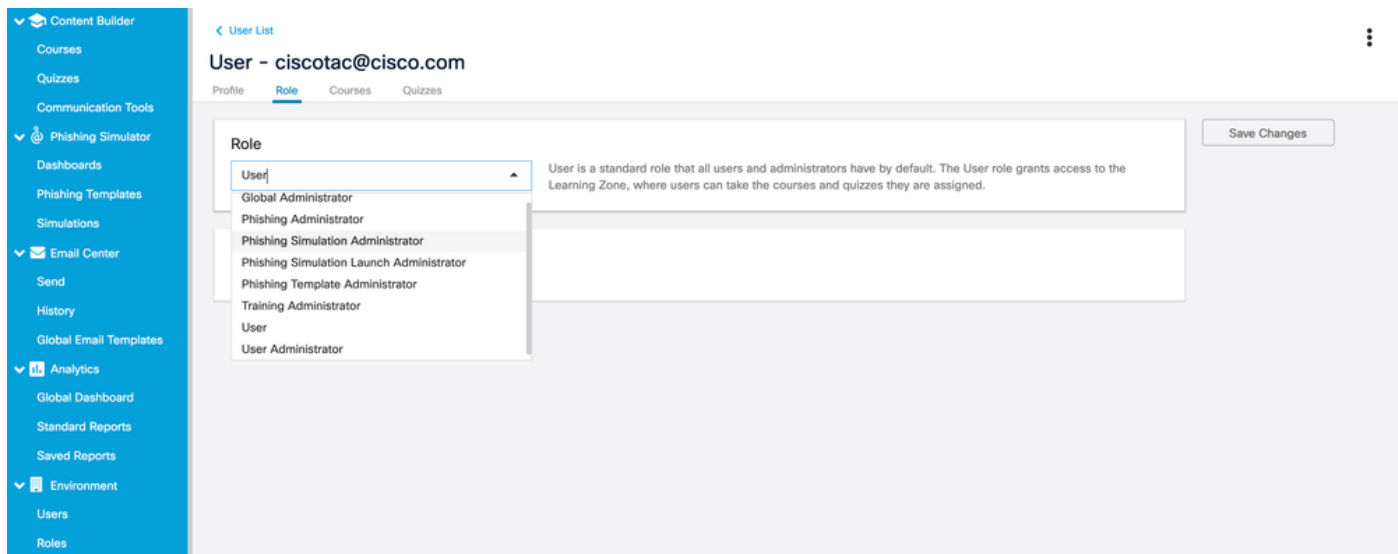
Red arrows point to the Email, First Name, and Last Name fields with the text 'Fill this'. A 'Save Changes' button is highlighted in the top right corner.

Schermata della pagina dell'interfaccia utente per aggiungere un nuovo utente



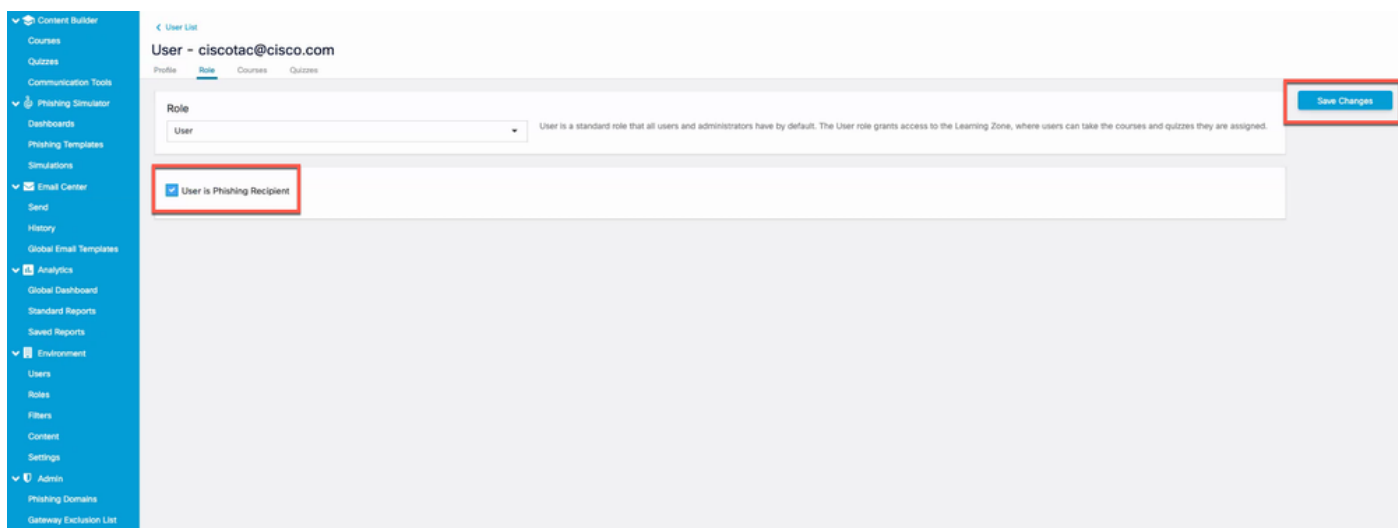
Nota: La password deve essere impostata solo per un utente amministratore CSA autorizzato a creare e avviare simulazioni.

Una volta creato l'utente, è possibile selezionare il ruolo dell'utente. È possibile selezionare il ruolo dall'elenco a discesa come indicato in questa immagine:



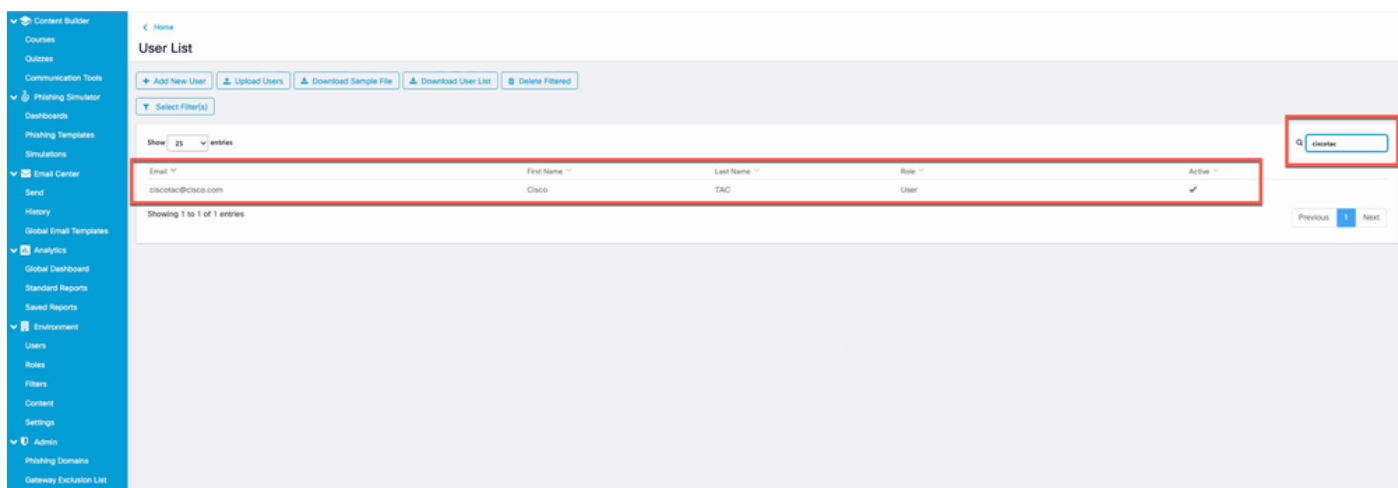
Visualizzazione delle opzioni dell'elenco a discesa del ruolo utente

Selezionare le User is Phishing Recipient > Save Changes caselle di controllo come illustrato nell'immagine.



schermata che mostra la casella di controllo "L'utente è destinatario di phishing" abilitata

Verificare che l'utente sia stato aggiunto correttamente e sia elencato quando viene eseguita la ricerca in base all'indirizzo di posta elettronica nel filtro, come mostrato nell'immagine.



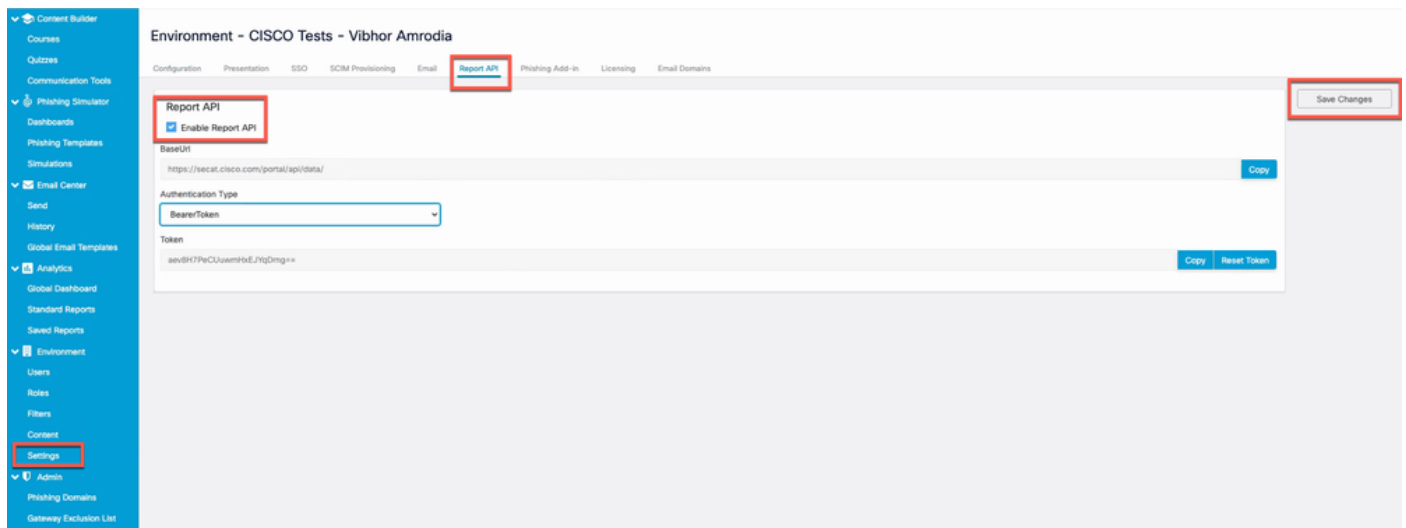
Schermata del nuovo utente nell'elenco degli utenti

Passaggio 3. Abilita API report

Passare alla **Environments > Settings > Report API** scheda e selezionare **Enable Report API > Save Changes**.



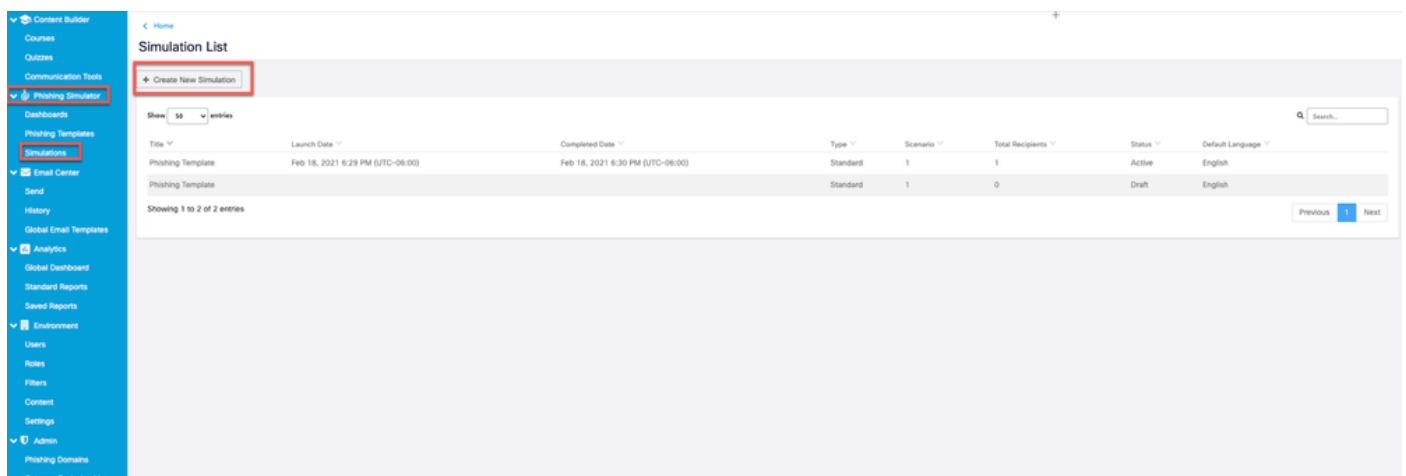
Nota: Prendere nota del token di connessione. Ciò è necessario per integrare il SEG con CSA.



Screenshot che mostra la casella di controllo "Abilita API report" abilitata.

Passaggio 4. Creazione di simulazioni di phishing

r. Individuate **Phishing Simulator > Simulations > Create New Simulation** e **selezionate una Template voce dall'elenco disponibile, come mostrato nell'immagine.**



Schermata che evidenzia il pulsante "Crea nuova simulazione"

b. Inserisci queste informazioni:

1. Selezionare un nome per il modello.

2. Descrivere il modello.
3. Nome di dominio con cui viene inviato il messaggio di phishing.
4. Nome visualizzato per l'e-mail di phishing.
5. Indirizzo da cui inviare l'e-mail (selezionare dall'elenco a discesa).
6. Indirizzo per la risposta (selezionare dall'elenco a discesa).
7. Selezionare la lingua.
8. Salvare le modifiche.

The screenshot shows the 'Simulations - Phishing Template' configuration page. The page has a sidebar on the left with various navigation options. The main content area is divided into sections: 'Name', 'Description', 'Email Settings', and 'Languages'. Red arrows and numbers 1 through 8 point to specific fields: 1 points to the 'Name' field, 2 to the 'Description' field, 3 to the 'Domain Name' dropdown, 4 to the 'Display email as' dropdown, 5 to the 'Email - From' dropdown, 6 to the 'Email - Reply to' dropdown, 7 to the 'Primary Language(*)' dropdown, and 8 to the 'Save Changes' button.

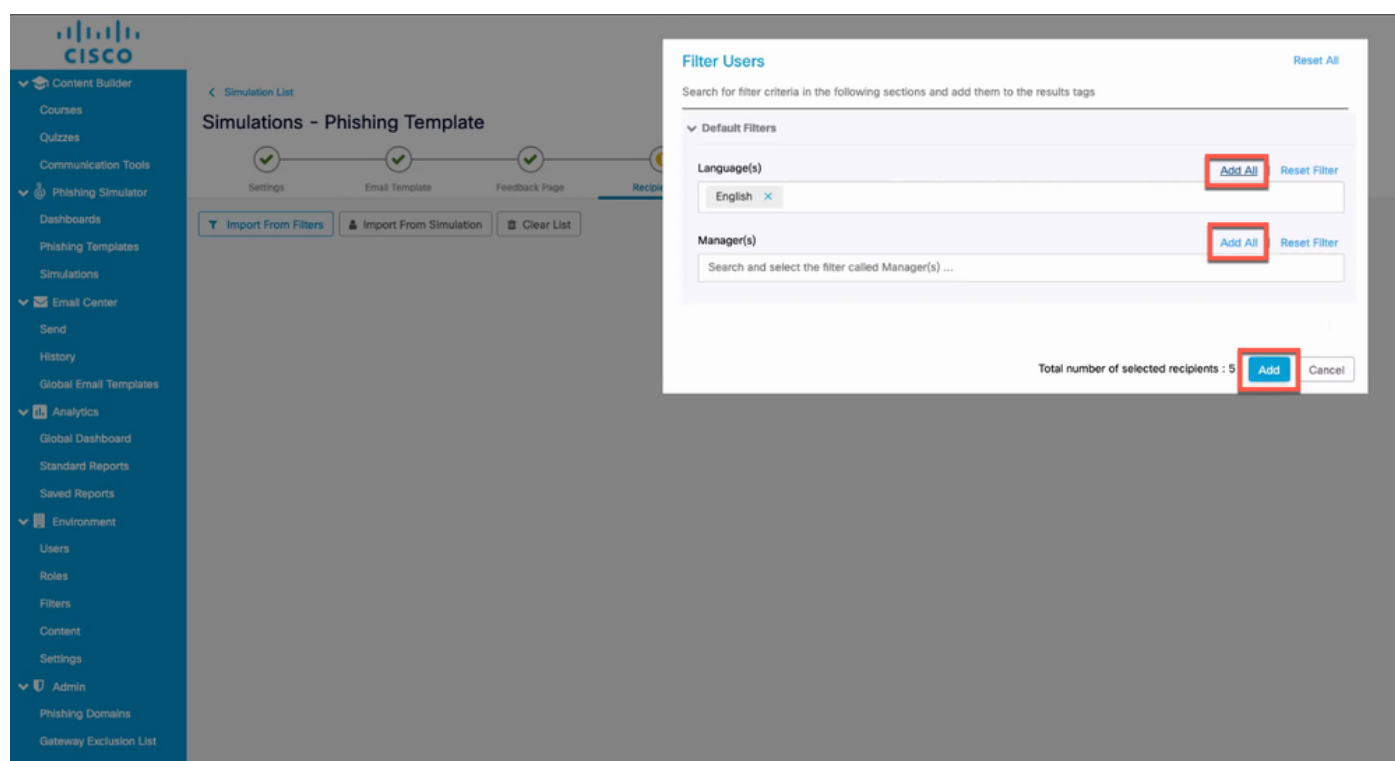
Schermata che evidenzia i campi da compilare per configurare la nuova simulazione

c. Fai clic su **Import from Filters** e aggiungi i destinatari dell'e-mail di phishing all'elenco, **Recipient List** come mostrato nell'immagine.

The screenshot shows the 'Simulations - Phishing Template' page with the 'Recipient List' tab selected. The 'Import From Filters' button is highlighted with a red box. The page shows a message: 'It's a bit empty here. No recipient has been added yet.'

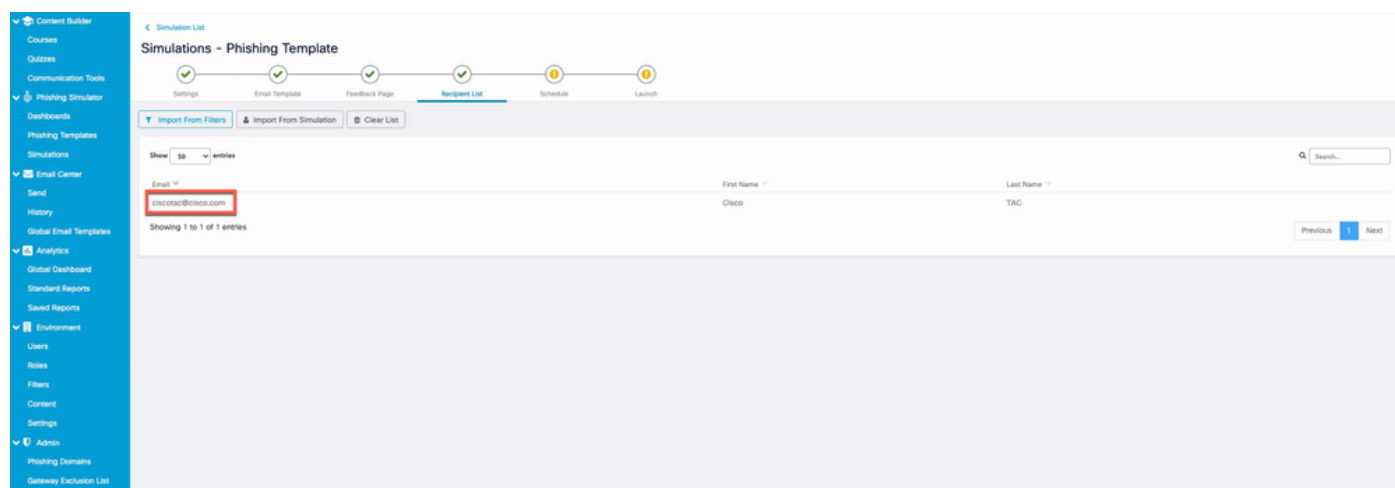
Schermata con il pulsante "Import from Filters" (Importa da filtri)

È possibile filtrare gli utenti in base alla lingua o ai manager. Fare clic su **Add** come mostrato nell'immagine.



Schermata della finestra di dialogo Filtra utenti per filtrare in base alla lingua o al manager

Di seguito è riportato un esempio dell'utente creato nel passaggio 2, che è stato aggiunto all'elenco dei destinatari come mostrato nell'immagine.



Schermata dell'utente creato in precedenza elencato come destinatario della simulazione di phishing

d. Impostare **Delivery Start** la data e **Save** le modifiche per programmare la campagna come mostrato nell'immagine.

Simulations - Phishing Template

Settings | Email Template | Feedback Page | Recipient List | **Schedule** | Launch

Schedule Setup

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

Restricted To Work Hours: ☒ Yes ☐ No

Work hours: From 07:00 To 19:00

[Save Changes](#)

Screenshot che evidenzia il campo Inizio consegna

Una volta scelta la data di inizio, l'opzione di selezione **end date** per la campagna viene abilitata, come mostrato nell'immagine.

Simulations - Phishing Template

Settings | Email Template | Feedback Page | Recipient List | **Schedule** | Launch

Schedule Setup

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

Restricted To Work Hours: ☒ Yes ☐ No

Work hours: From 07:00 To 19:00

[Save Changes](#)

Schermata di evidenziazione del campo Data Collect End che indica quando la simulazione deve terminare

e. Fare clic su **Launch** per avviare la campagna come mostrato nell'immagine.

Simulations - Phishing Template

Settings | Email Template | Feedback Page | Recipient List | Schedule | **Launch**

Simulation Summary

Email Template

SHIP EXPRESS

Dear Customer,

We thought you'd like to know that your item has shipped, and that the complete order will be on its way, and can no longer be changed.

Your estimated delivery date is: **Friday, April 9**

Shipment Details

Tracked value: \$100.00
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 ship anything and to protect your privacy.

Click on the link below to track your package or notify us of an error.

Feedback Page

YOU'VE BEEN PHISHED!

Company-wide simulation in progress!

PLEASE DO NOT TELL YOUR CO-WORKERS ABOUT THIS PHISHED SIMULATION

World's best to see if we can hook them, too!

Settings and Schedule

Default Language: English

Language(s): English

Anonymous Report: No

Display email as: Ship Express

Email From: csatest@intshipingexpress.com

Email Reply to: csatest@intshipingexpress.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)

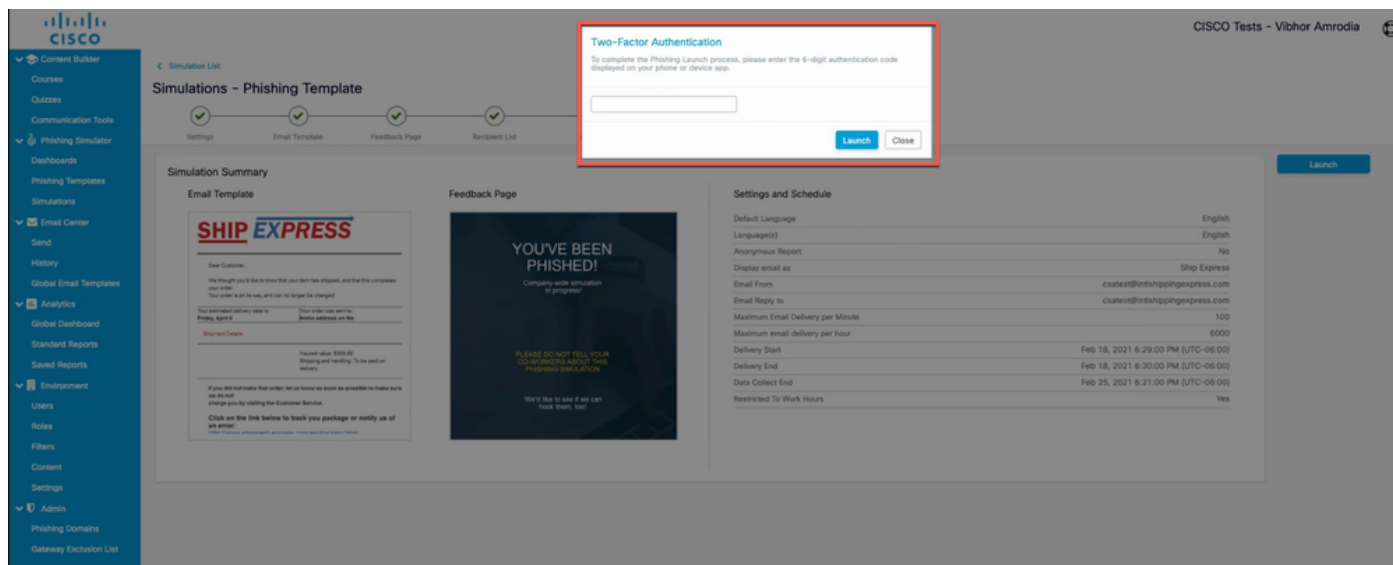
Data Collect End: Feb 25, 2021 6:21:00 PM (UTC-06:00)

Restricted To Work Hours: Yes

[Launch](#)

Schermata della scheda finale della procedura guidata per la creazione di simulazioni in cui è possibile avviare la campagna

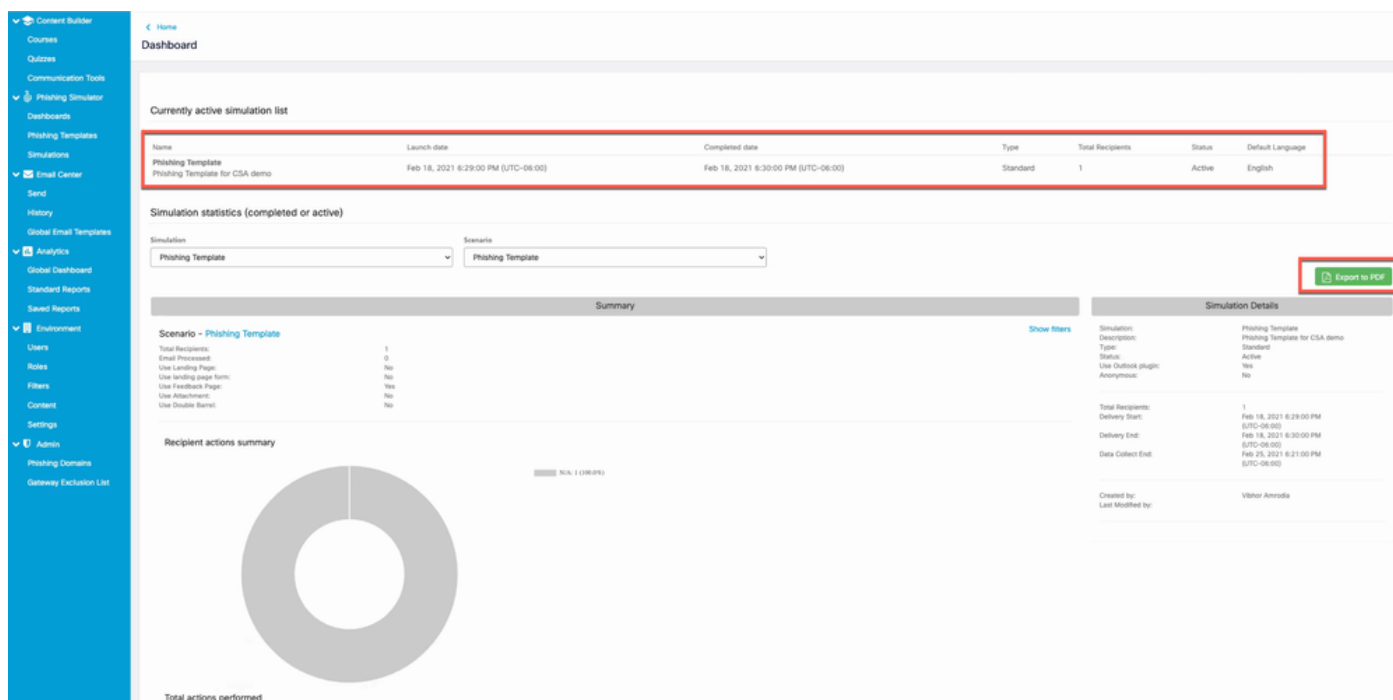
Dopo aver fatto clic sul pulsante di avvio, è possibile richiedere un codice di autenticazione a due fattori. Immettere il codice e fare clic su **Launch** come mostrato nell'immagine.



Schermata del popup che richiede il codice di autenticazione a due fattori

Passaggio 5. Verifica delle simulazioni attive

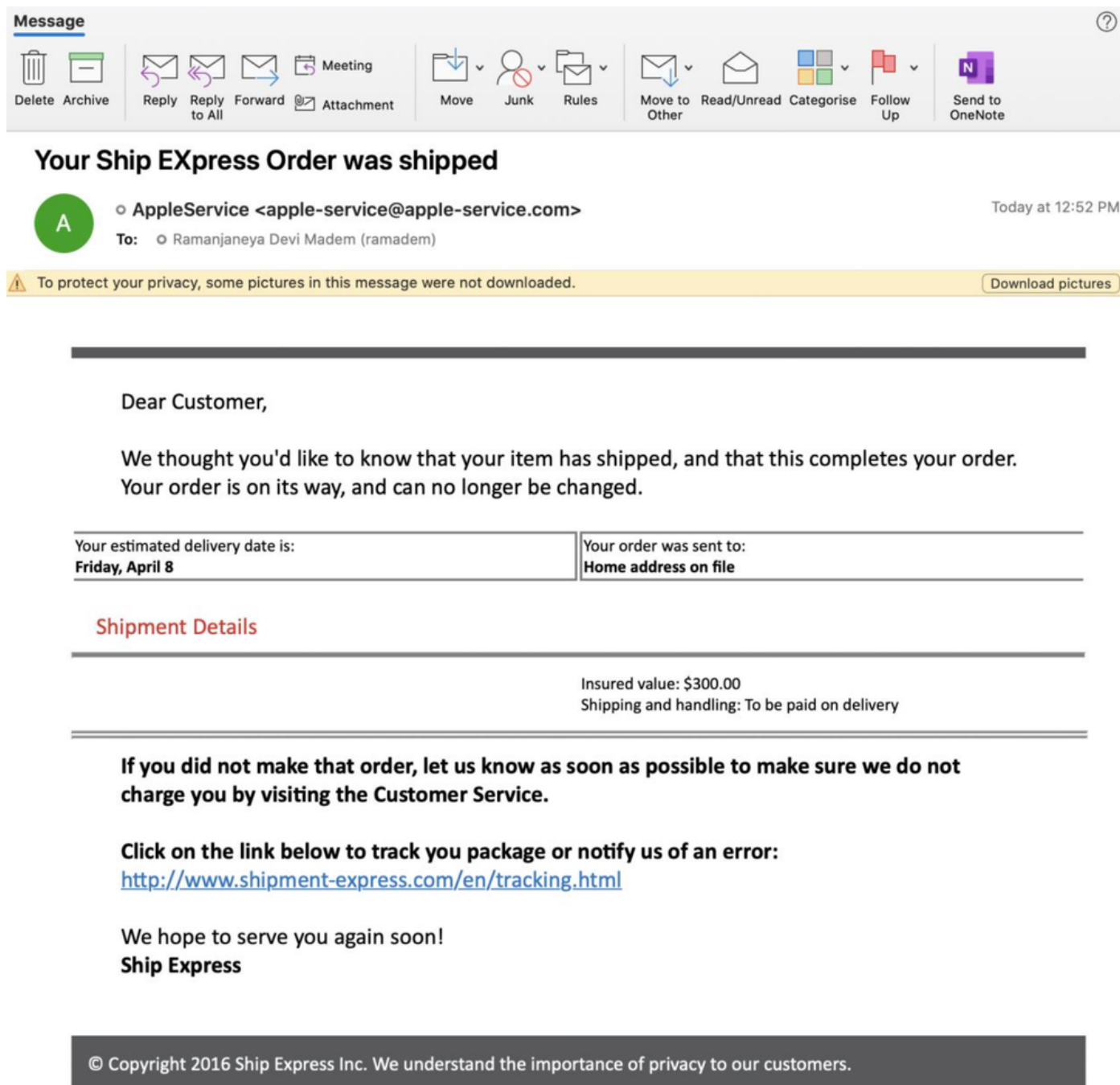
Passare a **Phishing Simulator > Dashboards**. L'elenco di simulazioni attive corrente fornisce le simulazioni attive. È inoltre possibile fare clic su **Export as PDF** e ottenere lo stesso report illustrato nell'immagine.



Schermata del dashboard simulazioni di phishing

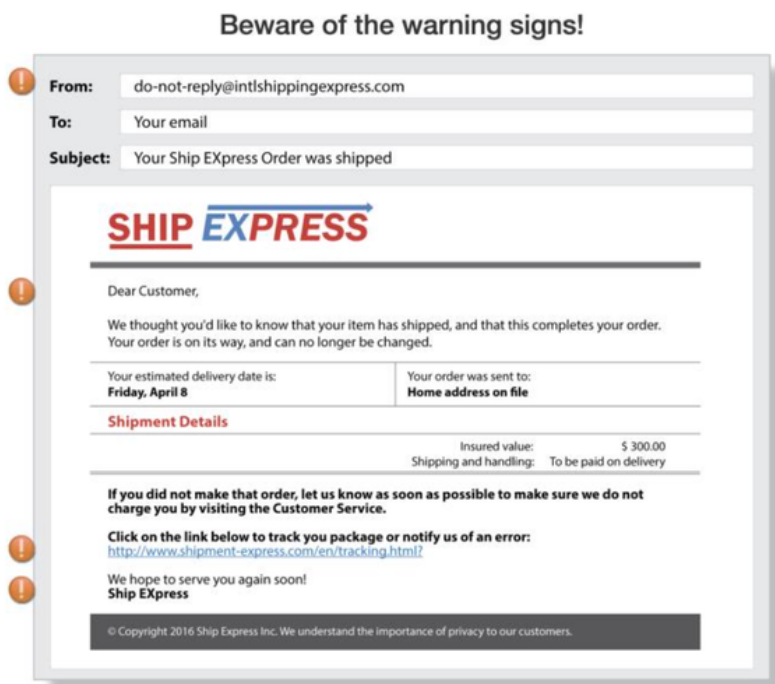
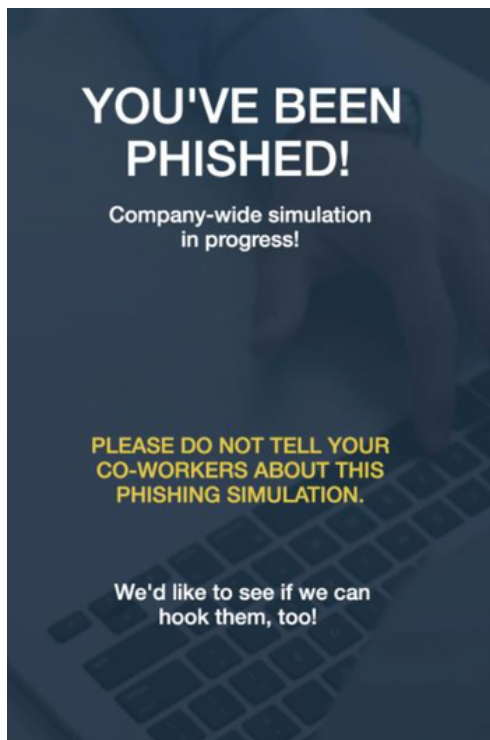
Cosa si vede a lato del destinatario?

Esempio di messaggio di simulazione di phishing nella cartella Posta in arrivo del destinatario.



Esempio di e-mail di phishing simulata in una cassetta postale utente

Quando il destinatario fa clic sull'URL, questa pagina di feedback viene mostrata all'utente che viene visualizzato come parte dell'elenco Repeat Clickers (che ha fatto clic liberamente sull'URL di phishing) in CSA.



ALWAYS REMEMBER

Esempio di pagina di feedback visualizzata dopo aver fatto clic sull'URL nell'e-mail di phishing

Verifica su CSA

L'elenco Ripeti selettori è visualizzato sotto 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

EN

Repeat Clickers

Parameters / Filters

Show50entries

Search...

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 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	cchennup@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

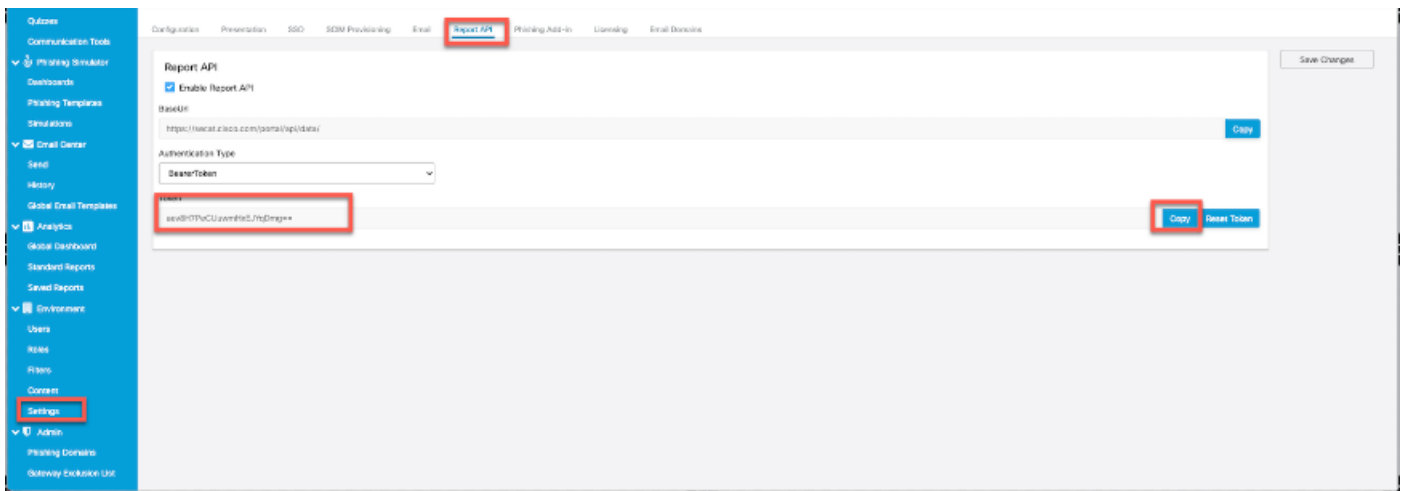
Schermata della pagina Ripeti i clic

Configurazione di Secure Email Gateway



Nota: Nella sezione Create and Send Phishing Simulations dal passaggio 3 del servizio cloud CSA. quando si abilita Report API , si è annotato il token di connessione. Tieni questo a portata di

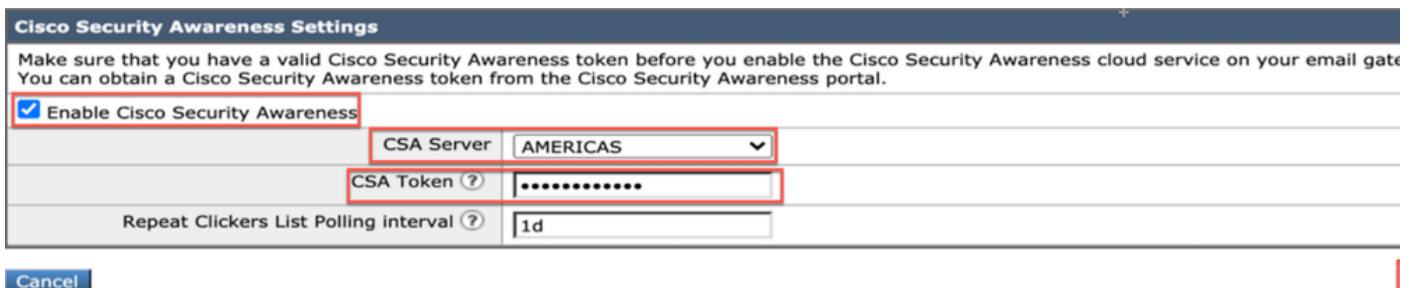
mano.



Schermata della pagina in API di report in cui l'amministratore può trovare il token di connessione

Passaggio 1. Abilitare la funzionalità di consapevolezza della sicurezza di Cisco in Secure Email Gateway

Nell'interfaccia utente di Secure Email Gateway, passare a Enter the Region and the CSA Token (Bearer Token ottenuto dal servizio cloud CSA, come mostrato nella nota precedente Security Services > Cisco Security Awareness > Enable .) e inviare e confermare le modifiche.



Screenshot della pagina delle impostazioni di Cisco Security Awareness su Cisco Secure Email Gateway

Configurazione dalla CLI

Digitare `csaconfig` per configurare CSA tramite 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
- ```
[> 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]>

## Passaggio 2. Consenti messaggi di phishing simulati dal servizio cloud CSA



Nota: Il criterio del `CYBERSEC_AWARENESS_ALLOWED` flusso di posta viene creato per impostazione predefinita con tutti i motori di scansione impostati su Disattivato, come mostrato di seguito.

| 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 |

Screenshot del criterio del flusso di posta "`CYBERSEC_AWARENESS_ALLOWED`" con le funzionalità di sicurezza disabilitate

Per consentire alle e-mail della campagna di phishing simulata dal servizio cloud CSA di ignorare tutti i motori di scansione su Secure Email Gateway:

r. Creare un nuovo gruppo di mittenti e assegnare il criterio del `CYBERSEC_AWARENESS_ALLOWED` flusso di posta. Passare al criterio `Mail Policies > HAT Overview > Add Sender Group` e selezionarlo, `CYBERSEC_AWARENESS_ALLOWED` impostare l'ordine su 1 e quindi `Submit and Add Senders`.

b. Aggiungere un mittente `IP/domain` o `Geo Location` da cui vengono avviati i messaggi di posta elettronica della campagna di phishing.

Passare a `Mail Policies > HAT Overview > Add Sender Group > Submit and Add Senders > Add the sender IP > Submit` e `Commit` modificare come mostrato nell'immagine.

| 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></td> </tr> </tbody> </table>                                                                                                                                          | Source Name |  | Select Source |  |
| Source Name                                                     |                                                                                                                                                                                                                                                                                              |             |  |               |  |
| Select Source                                                   |                                                                                                                                                                                                                                                                                              |             |  |               |  |
| 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). |             |  |               |  |

[Cancel](#)
[Submit](#)
[Submit and Add Senders >>](#)

Screenshot di un gruppo di mittenti CyberSec\_Awareness\_Allowed con il criterio del flusso di posta "CYBERSEC\_AWARENESS\_ALLOWED" selezionato.

| 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)"/>                     |

[Cancel](#)
[Submit](#)

Screenshot della pagina delle impostazioni di Cisco Security Awareness su Cisco Secure Email Gateway

## Configurazione dalla CLI:

1. Passare a `listenerconfig > Edit > Inbound (PublicInterface) > HOSTACCESS > NEW > New Sender Group` .

2. Crea un nuovo gruppo di mittenti con i criteri di posta e aggiungi un dominio/IP mittente da cui vengono avviati i messaggi di posta elettronica della campagna di phishing.

3. Impostare l'ordine del nuovo gruppo di mittenti su 1 e utilizzare l'Move opzione in `listenerconfig > EDIT > Inbound (PublicInterface) > HOSTACCESS > MOVE` .

4. Esecuzione del commit.



Nota: L'IP del mittente è l'indirizzo IP dell'account CSA e si basa sulla regione selezionata. Fare riferimento alla tabella per l'indirizzo IP corretto da utilizzare. Consentire a questi indirizzi IP/nomi host nel firewall con il numero di porta 443 per la connessione di SEG 14.0.0-xxx al servizio 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,<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 |      |

Screenshot degli indirizzi IP e dei nomi host di CSA Americas e delle regioni dell'UE

### Passaggio 3. Eseguire un'azione quando si fa clic con il pulsante Ripeti da SEG

Dopo l'invio delle e-mail di phishing e l'inserimento dell'elenco di selezioni ripetute nel SEG, è possibile creare una policy per la posta in arrivo aggressiva che consenta di intervenire sulla posta inviata a tali utenti specifici.

Creare un nuovo criterio personalizzato per la posta in arrivo aggressivo e abilitare **Include Repeat Clickers List** la casella di controllo nella sezione del destinatario.

Dalla GUI, selezionare **Mail Policies > Incoming Mail Policies > Add Policy > Add User > Include Repeat Clickers List > Submit** e selezionare **Commit** le modifiche.

**Add User**

☒ Any Sender  
☐ Following Senders  
☐ Following Senders are Not

Email Address:  
  
 (e.g. user@example.com, user@, @example.com, @.example.com)

LDAP Group:  
 Query:

Group:

☐ Any Recipient  
☒ Following Recipients

☒ Include Repeat Clickers List  
 (From Cisco Security Awareness)

LDAP Group:  
 Query:

Group:

☐ Following Recipients are Not

Email Address:

Screenshot del criterio Posta in arrivo personalizzato configurato per gestire la posta destinata ai selettori di ripetizione

## Guida alla risoluzione dei problemi

1. Passare `csaconfig > SHOW_LIST` per visualizzare i dettagli dell'elenco di cliccatori ripetuti.

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. Passare a `csaconfig > UPDATE_LIST` se si desidera forzare l'aggiornamento dell'elenco di cliccatori ripetuti.

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. Esaminare i log CSA per verificare se l'elenco di cliccatori ripetuti è stato scaricato o se si è verificato un errore. Di seguito è riportata 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. L'elenco dei dispositivi che selezionano più volte il numero di utenti può essere visualizzato anche dalla GUI. Passare a `Security Services > Cisco Security Awareness` come mostrato nell'immagine.

Cisco Security Awareness

Cisco Security Awareness

Cisco Security Awareness	Enabled
Repeat Clickers List Poll Interval [?]	1d

Edit Settings

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	Update List

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. Update Now

Screenshot di Security Services > pagina di consapevolezza sulla sicurezza Cisco che evidenzia il numero di clic ripetuti

Informazioni correlate

- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).