# 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

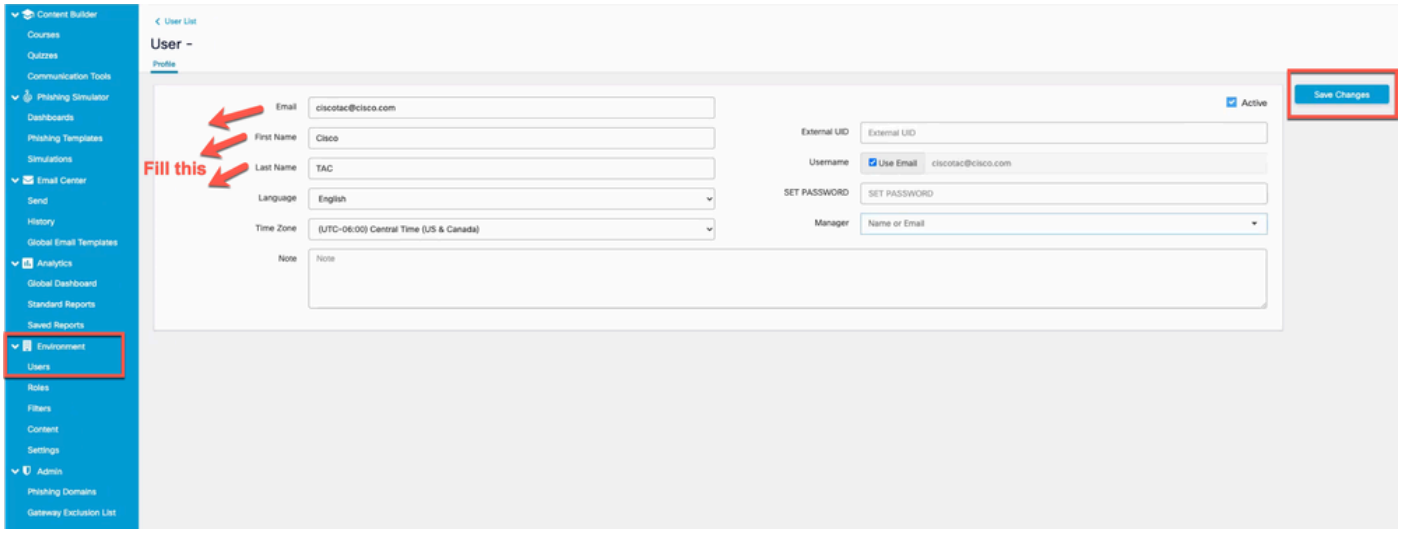
## Passaggio 1. Accedere al servizio cloud CSA

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.



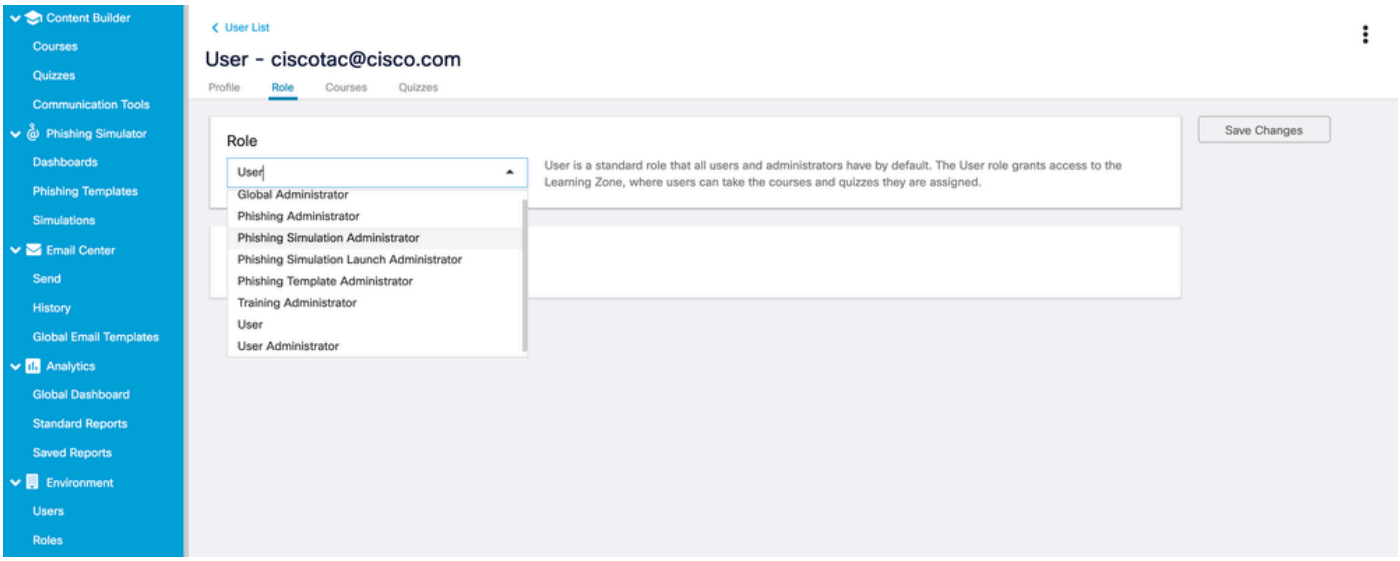

Schermata della pagina dell'interfaccia utente per aggiungere un nuovo utente

---

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

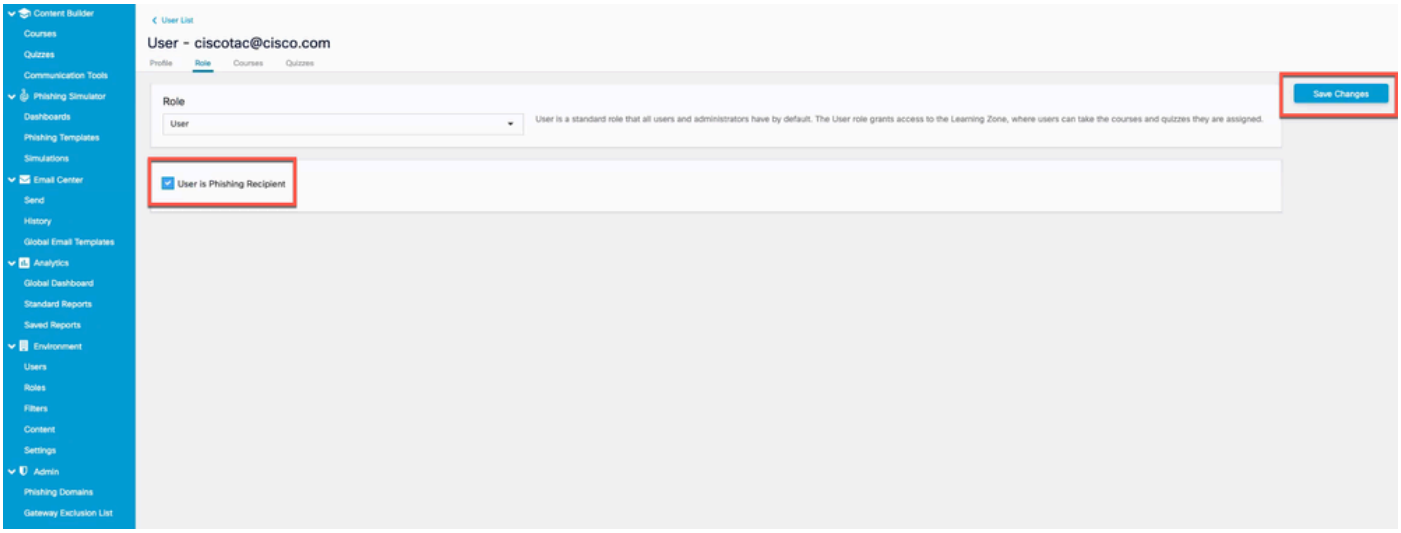
---

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:



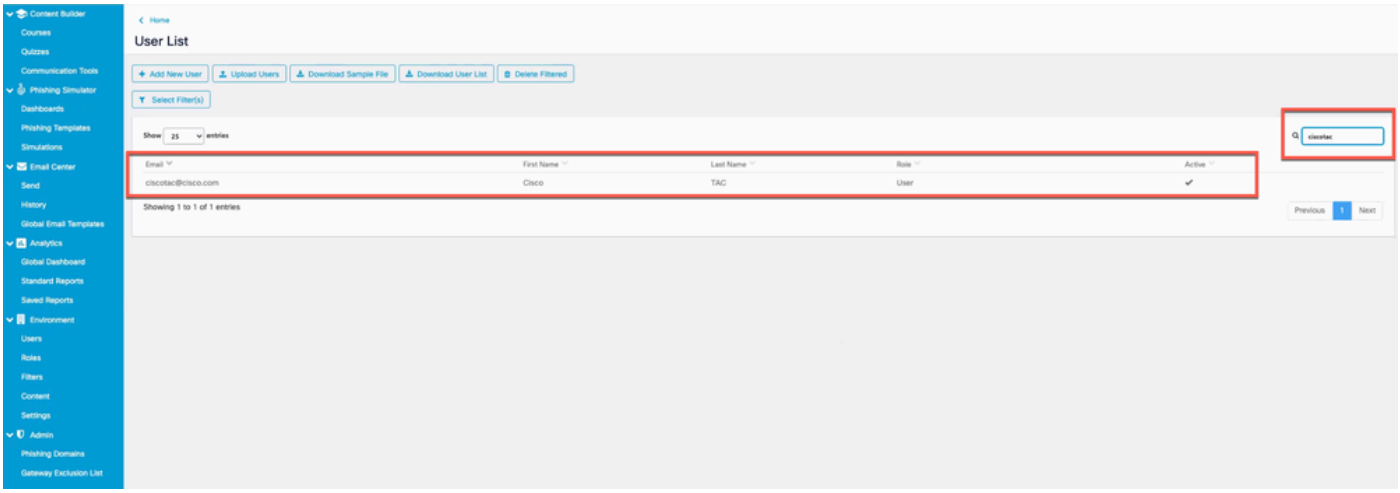

Visualizzazione delle opzioni dell'elenco a discesa del ruolo utente

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

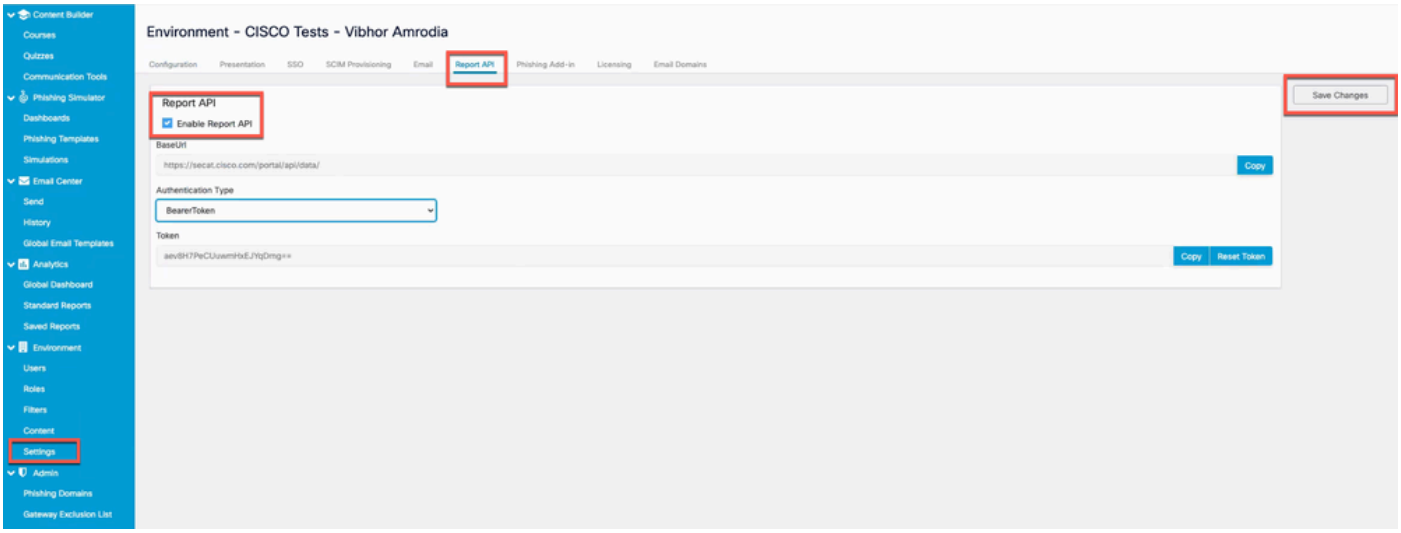
## Passaggio 3. Abilita API report

Passare alla Environments > Settings > Report API scheda e selezionareEnable Report API > Save Changes .

---

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

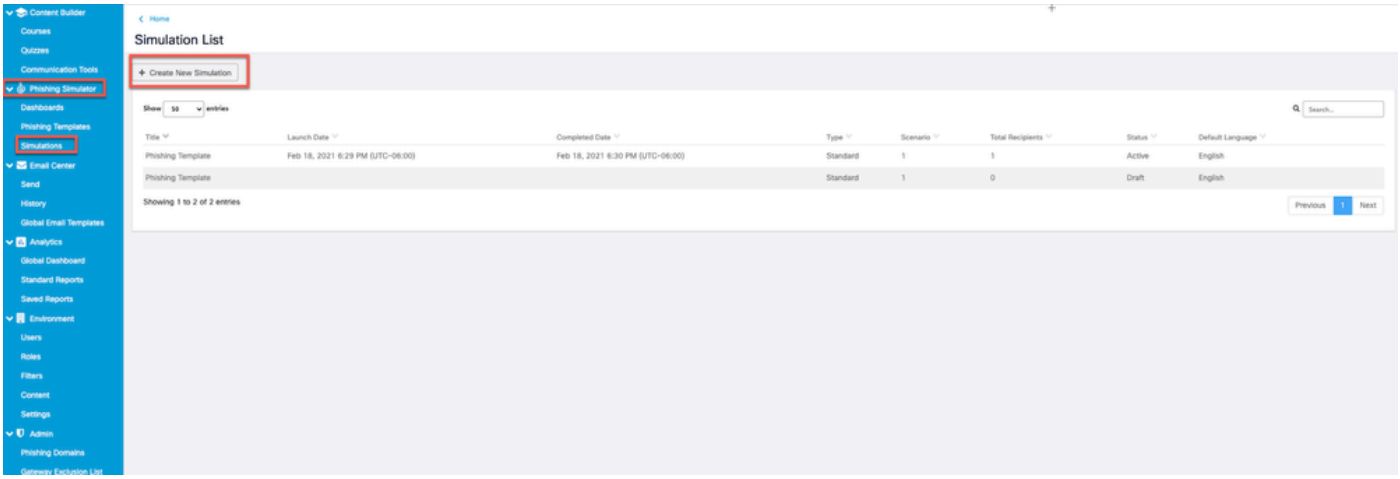
---




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.

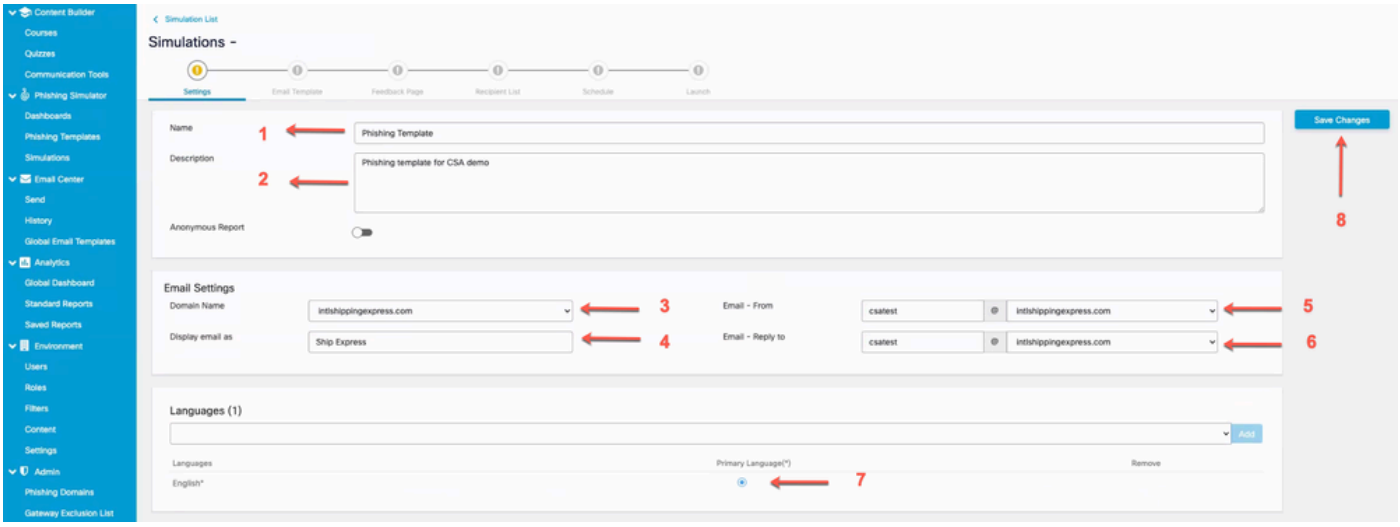



Schermata che evidenzia il pulsante "Crea nuova simulazione"

b. Inserisci queste informazioni:

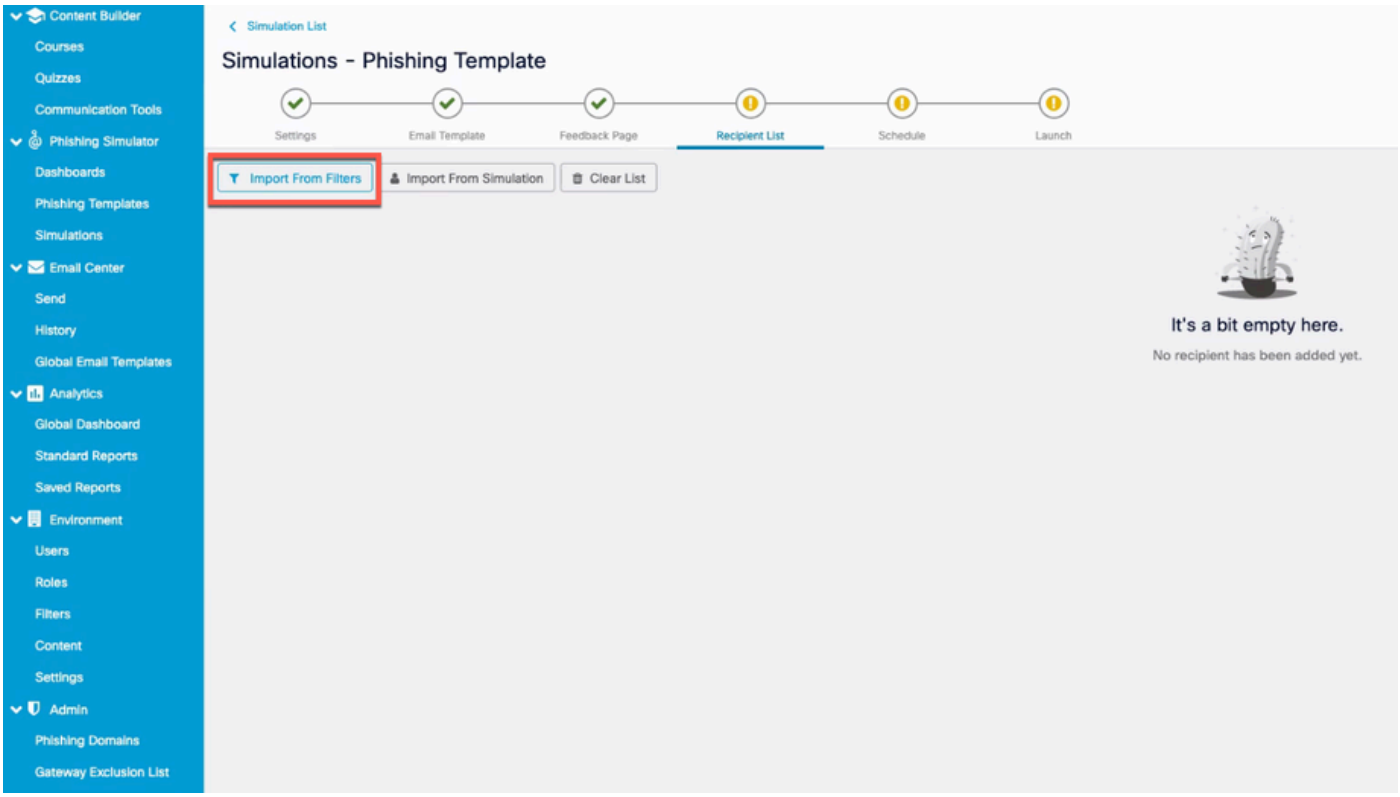
1. Selezionare un nome per il modello.

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.



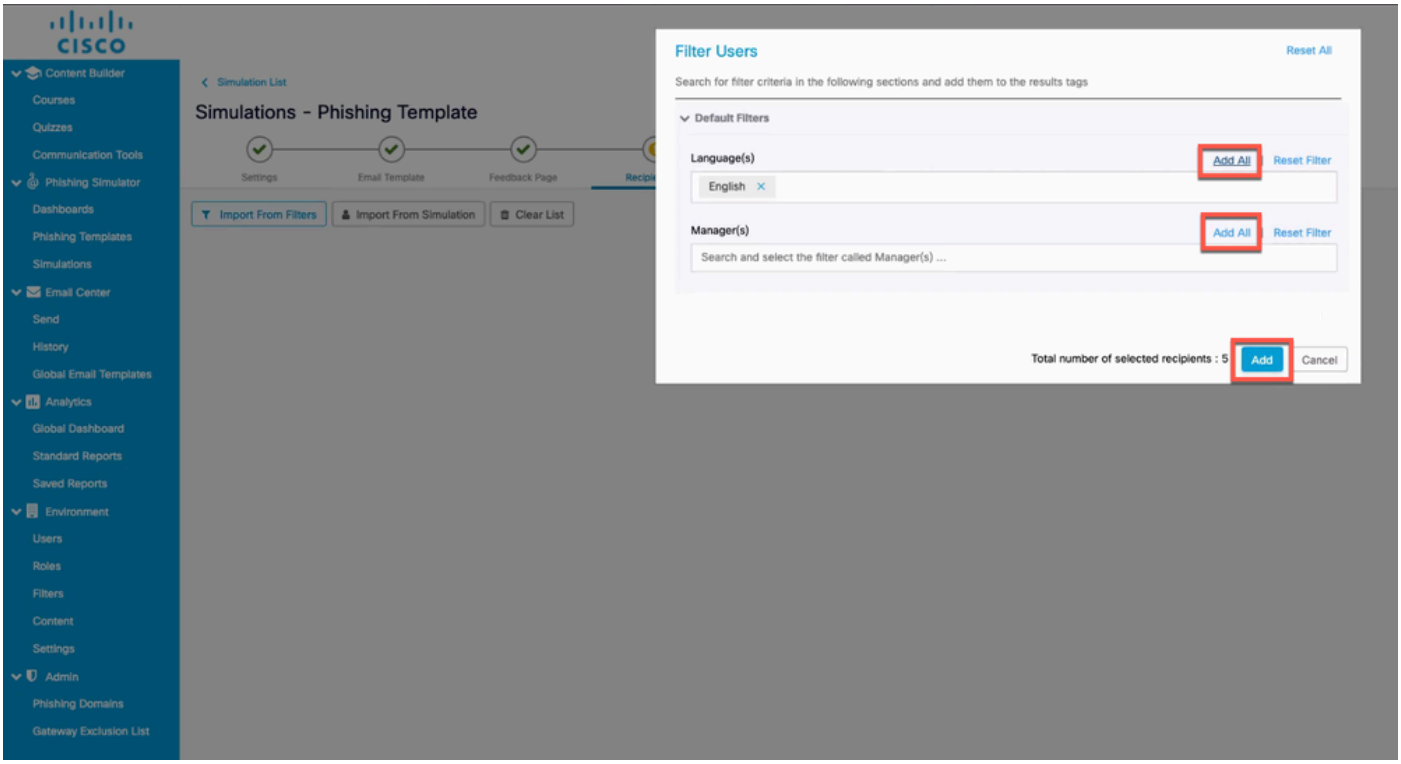

Schermata che evidenzia i campi da compilare per configurare la nuova simulazione

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



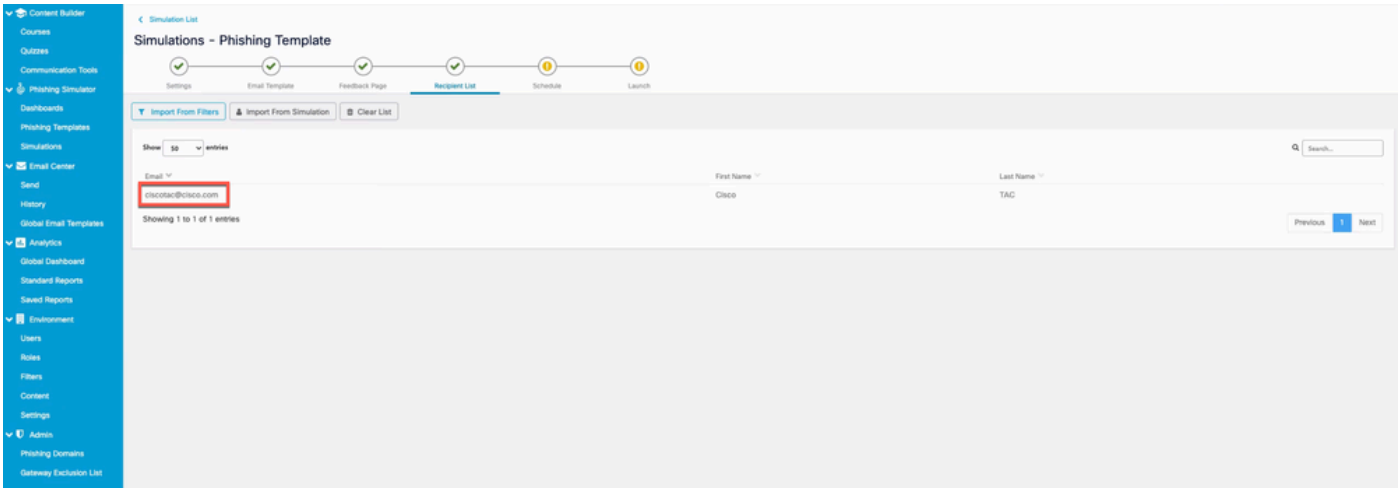

Schermata con il pulsante "Import from Filters" (Importa da filtri)

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



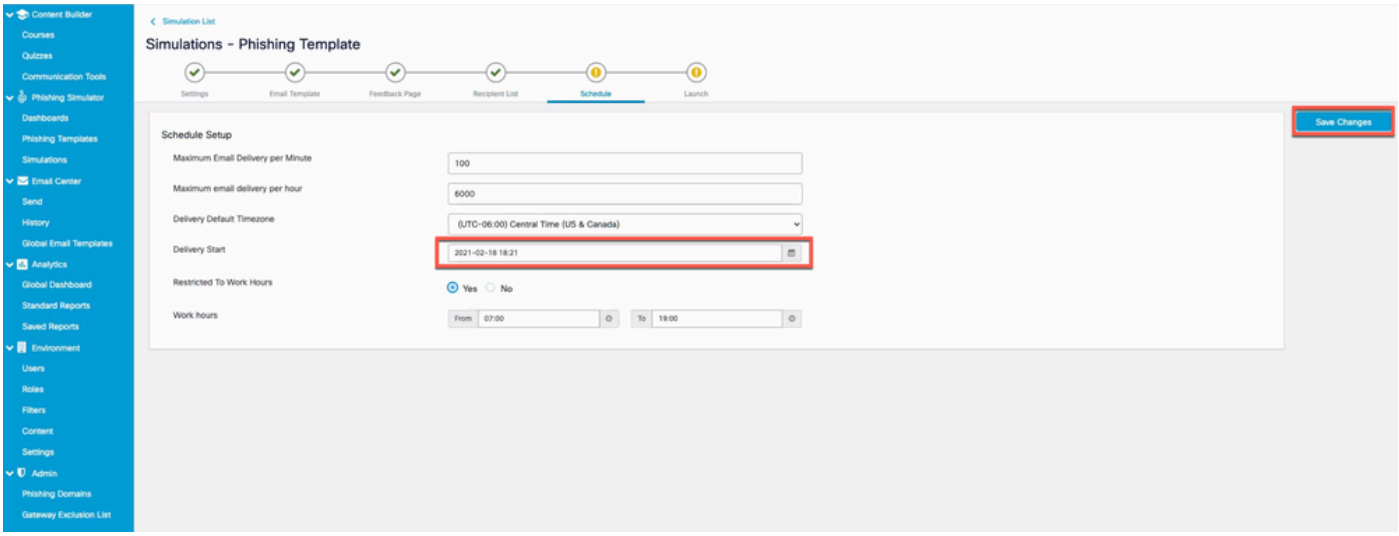

Schermata della finestra di dialogo Filtra utenti per filtrare in base alla lingua o al manager

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



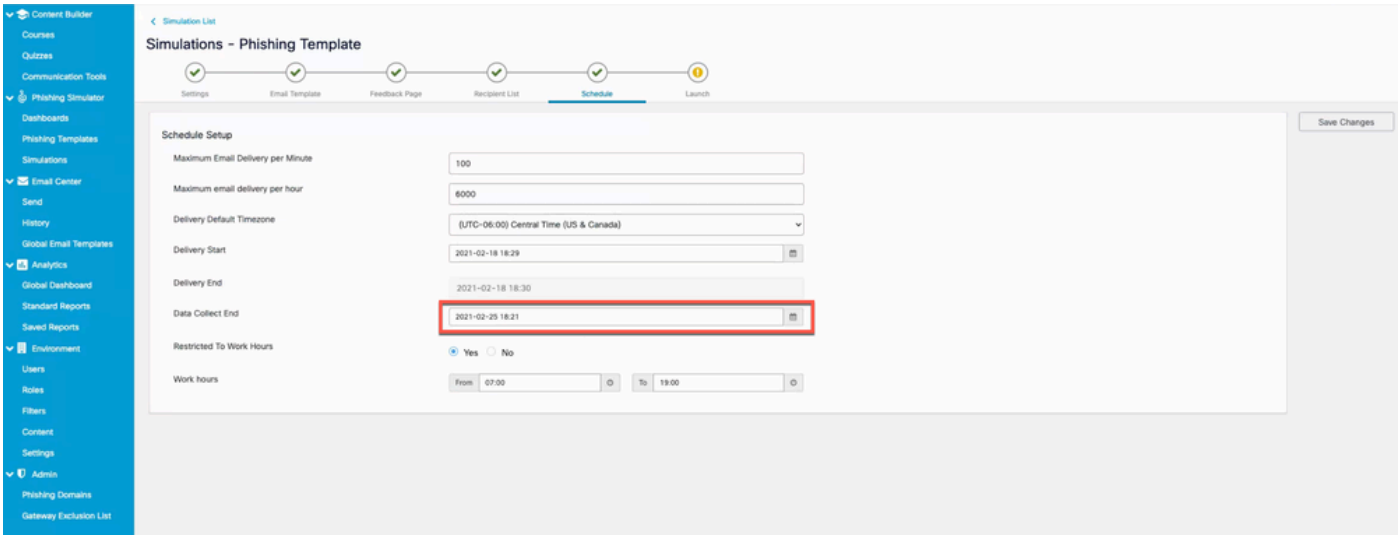

Schermata dell'utente creato in precedenza elencato come destinatario della simulazione di phishing

d. ImpostareDelivery Startla data e Save le modifiche per programmare la campagna come mostrato nell'immagine.



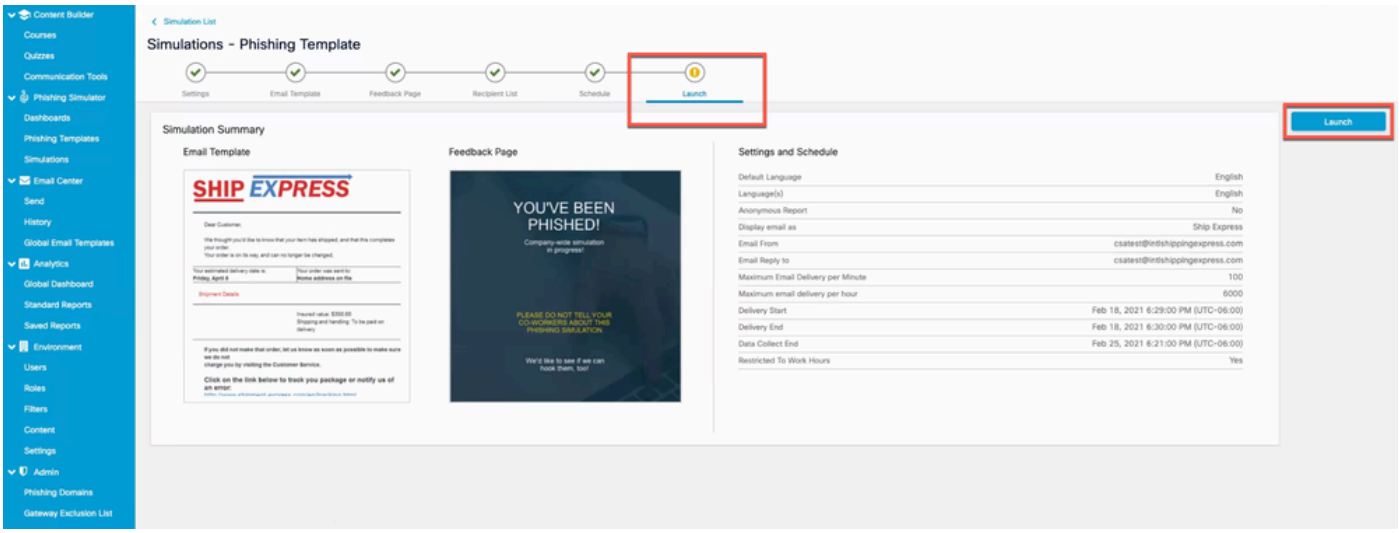

Screenshot che evidenzia il campo Inizio consegna

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



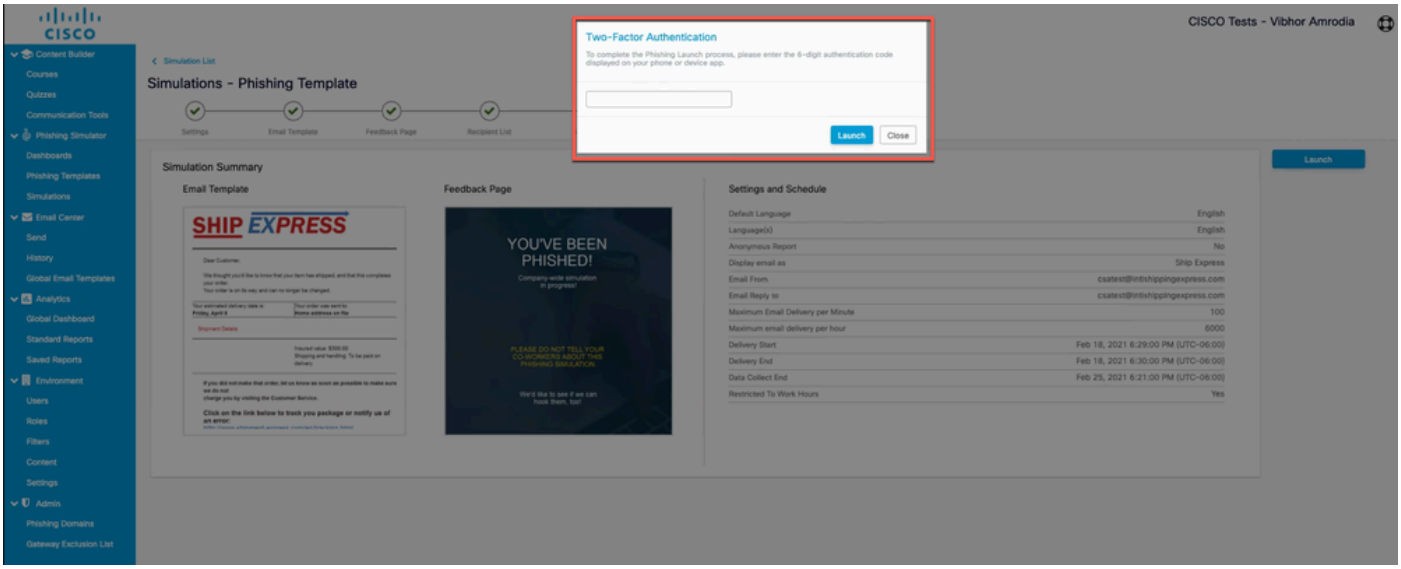

Schermata di evidenziazione del campo Data Collect End che indica quando la simulazione deve terminare

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



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

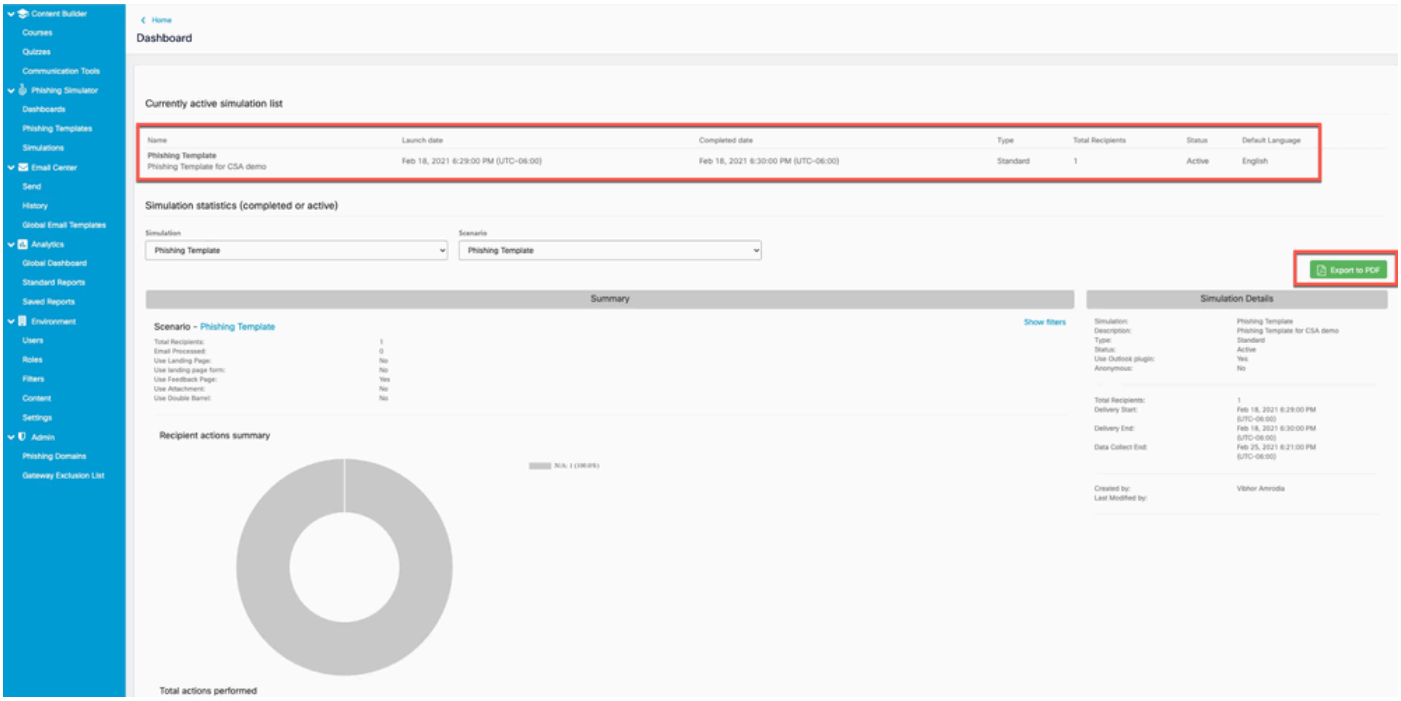
Dopo aver fatto clic sul pulsante di avvio, è possibile richiedere un codice di autenticazione a due fattori. Immettere il codice e fare clic su Launchcome mostrato nell'immagine.




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

## Passaggio 5. Verifica delle simulazioni attive

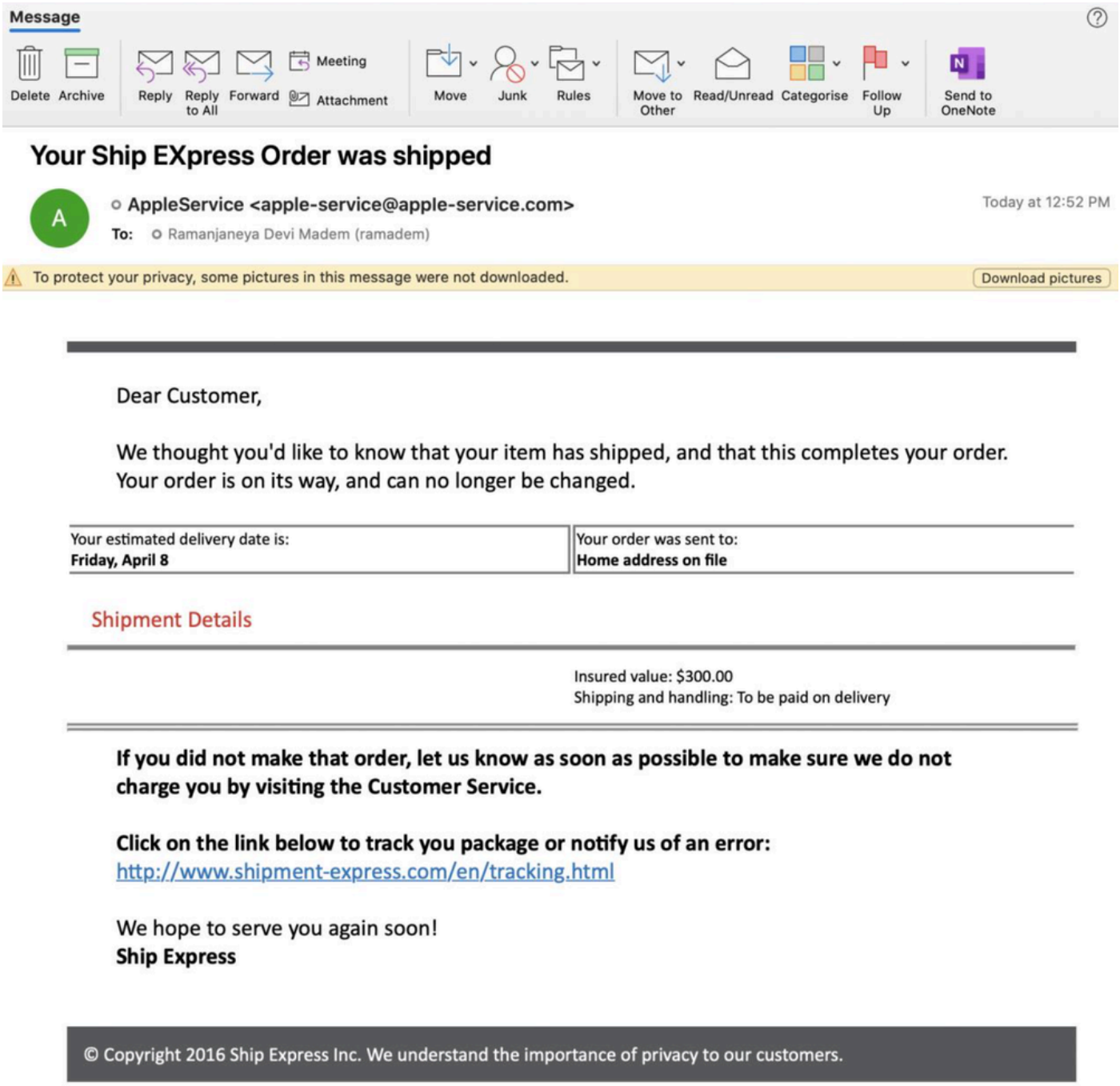
Passare aPhishing Simulator > Dashboards. L'elenco di simulazioni attive corrente fornisce le simulazioni attive. È inoltre possibile fare clic su Export as PDF e ottenere lo stesso report illustrato nell'immagine.




Schermata del dashboard simulazioni di phishing

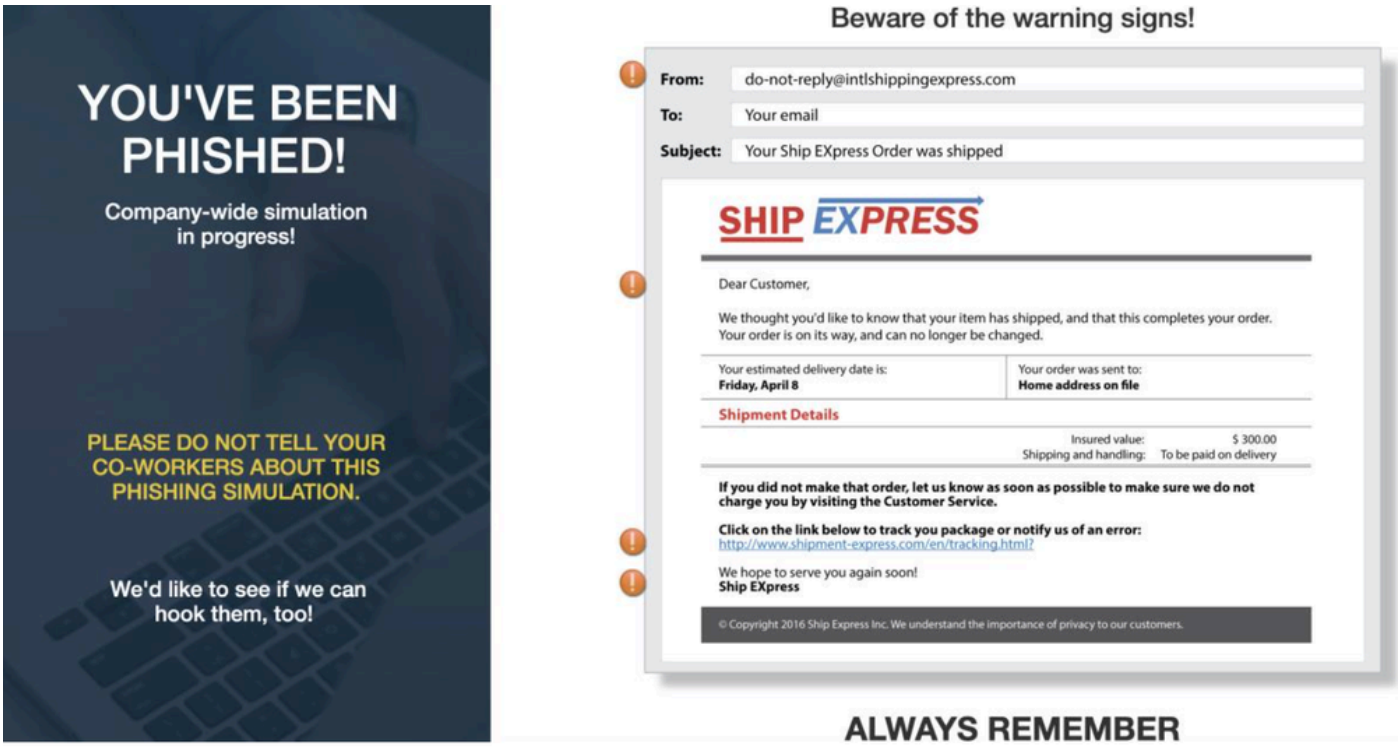
# Cosa si vede a lato del destinatario?

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

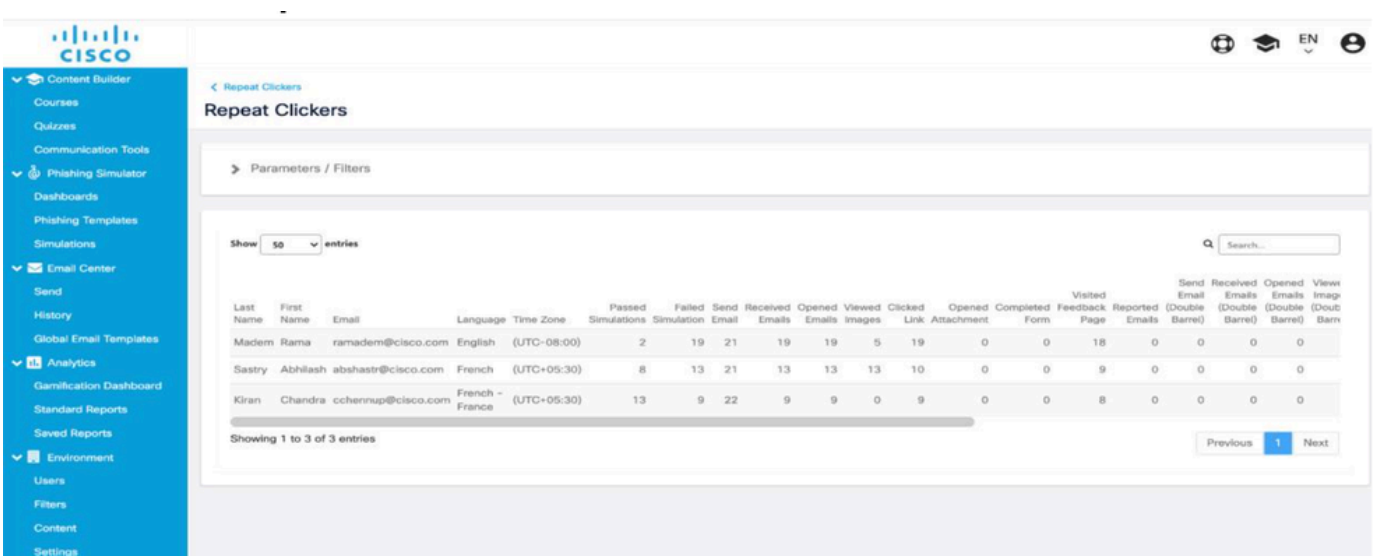
Quando il destinatario fa clic sull'URL, questa pagina di feedback viene mostrata all'utente che viene visualizzato come parte dell'elenco Repeat Clickers (che ha fatto clic liberamente sull'URL di phishing) in CSA.




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 sottoAnalytics > Standard Reports > Phishing Simulations > Repeat Clickersas shown in the image.

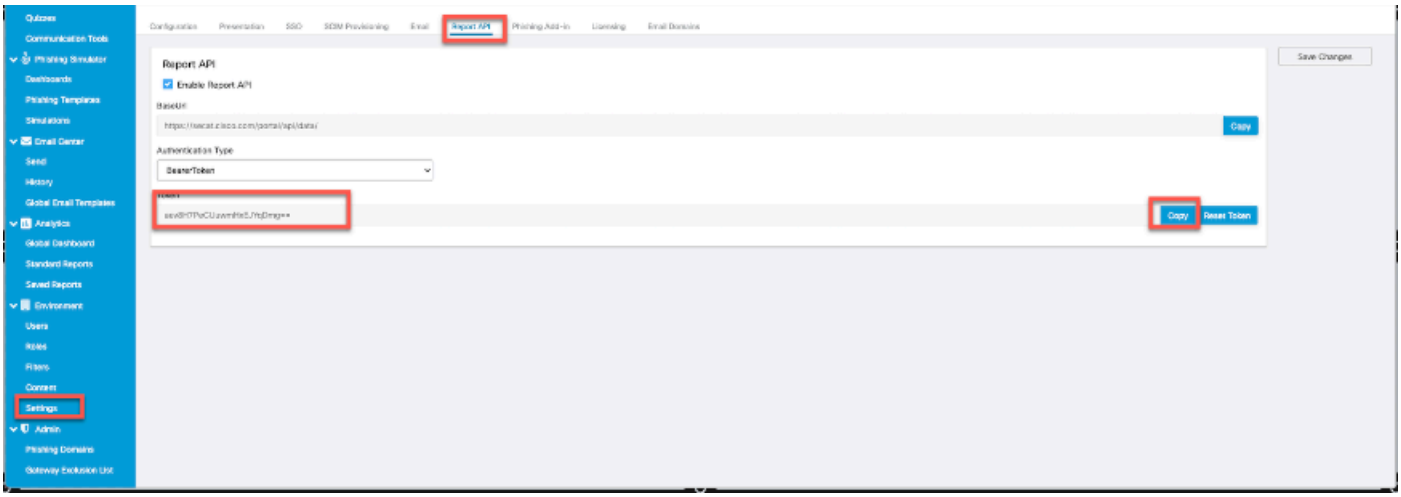



Schermata della pagina Ripeti i clic

# 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

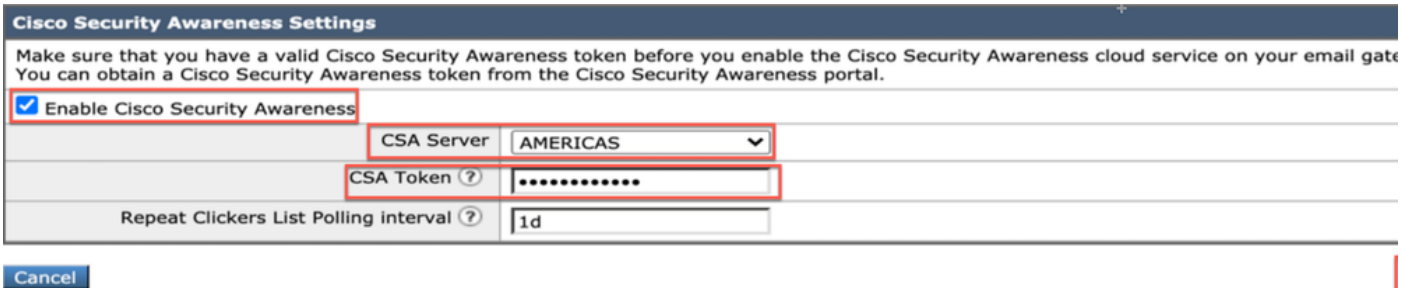
mano.




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

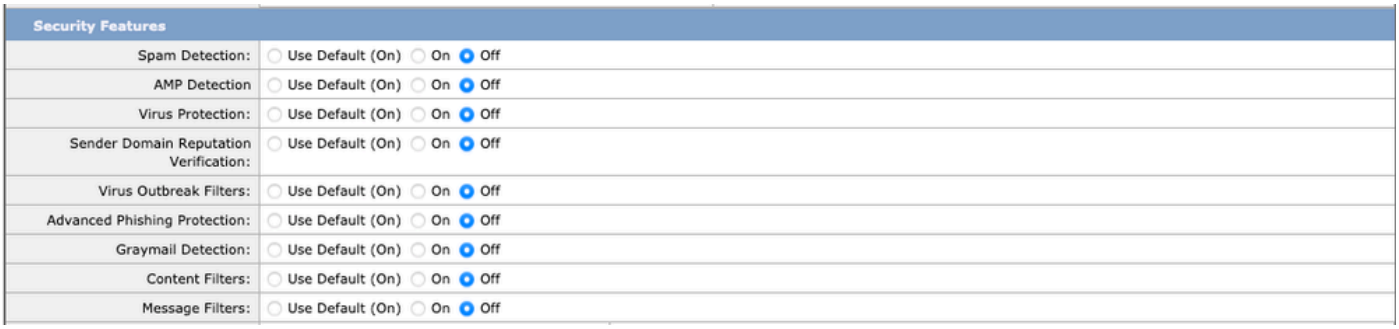
Digitare `csaconfig` per configurare CSA tramite la CLI.

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

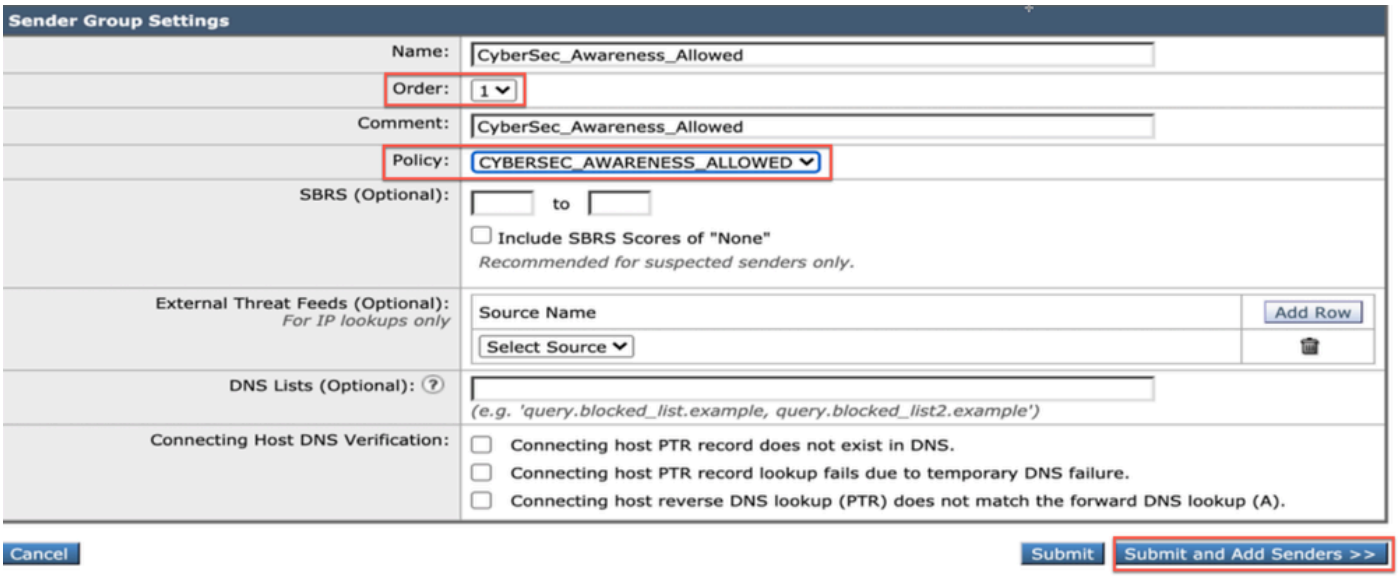
Screenshot del criterio del flusso di posta "CYBERSEC_AWARENESS_ALLOWED" con le funzionalità di sicurezza disabilitate

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:

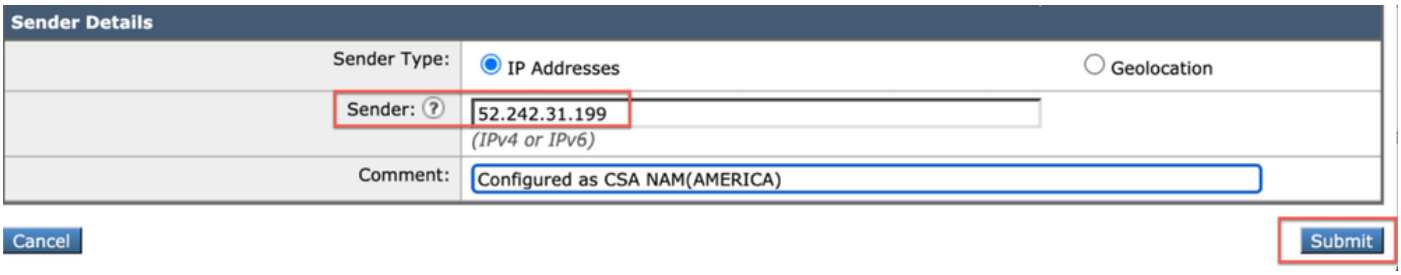
r. Creare un nuovo gruppo di mittenti e assegnare il criterio del CYBERSEC_AWARENESS_ALLOWED flusso di posta. Passare al criterio Mail Policies > HAT Overview > Add Sender Group e selezionarlo, CYBERSEC_AWARENESS_ALLOWED impostare l'ordine su 1 e quindi Submit and Add Senders.

b. Aggiungere un mittente IP/domain oGeo Locationda cui vengono avviati i messaggi di posta elettronica della campagna di phishing.

Passare aMail Polices > HAT Overview > Add Sender Group > Submit and Add Senders > Add the sender IP > SubmiteCommitmodificare come mostrato nell'immagine.




Screenshot di un gruppo di mittenti CyberSec_Awareness_Allowed con il criterio del flusso di posta "CYBERSEC_AWARENESS_ALLOWED" selezionato.




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 .

CYBERSEC_AWARENESS_ALLOWED2. 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.2.

3. Impostare l'ordine del nuovo gruppo di mittenti su 1 e utilizzare l'Moveopzione 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 | |

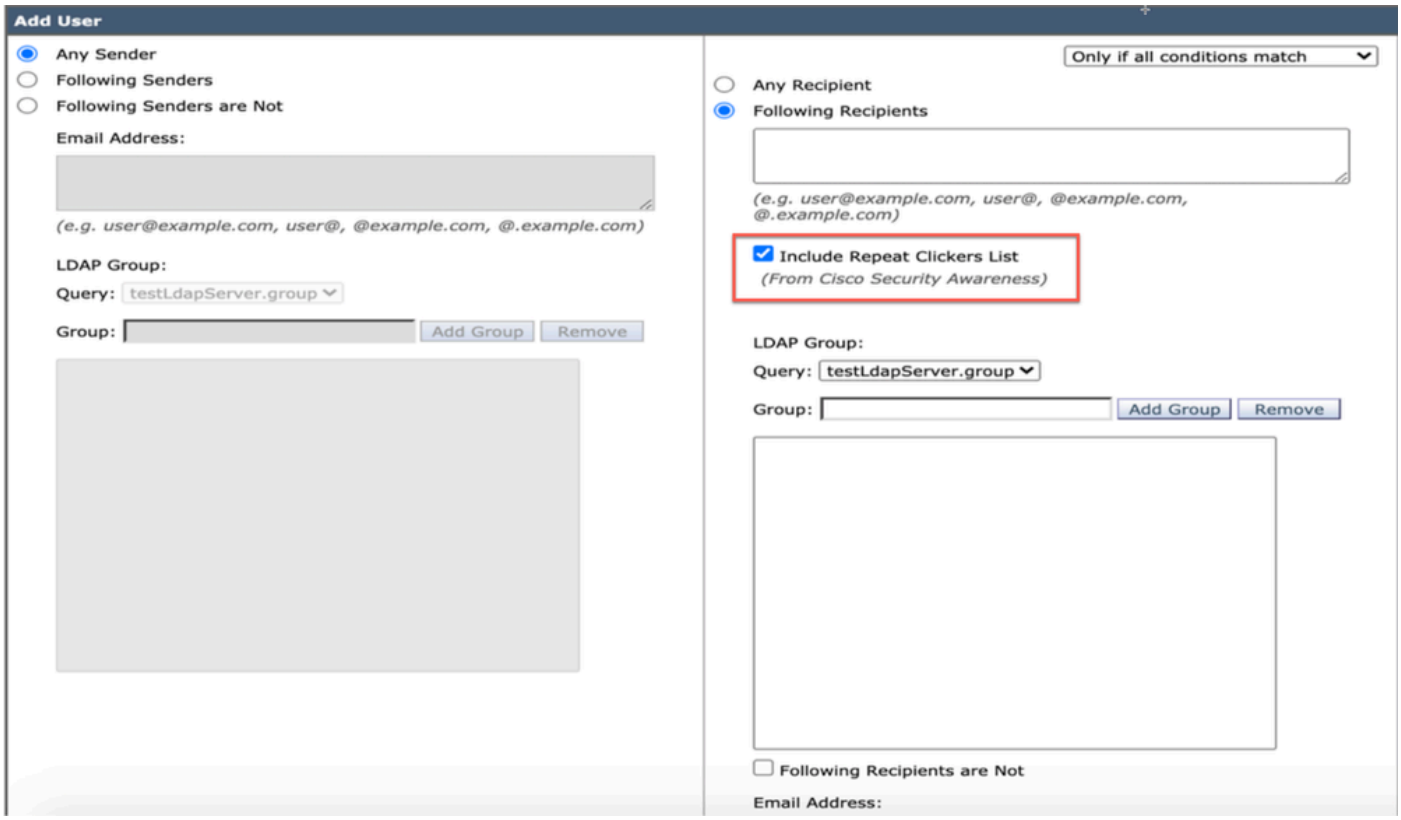
Screenshot degli indirizzi IP e dei nomi host di CSA Americas e delle regioni dell'UE

## 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.




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_LISTper 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.
```

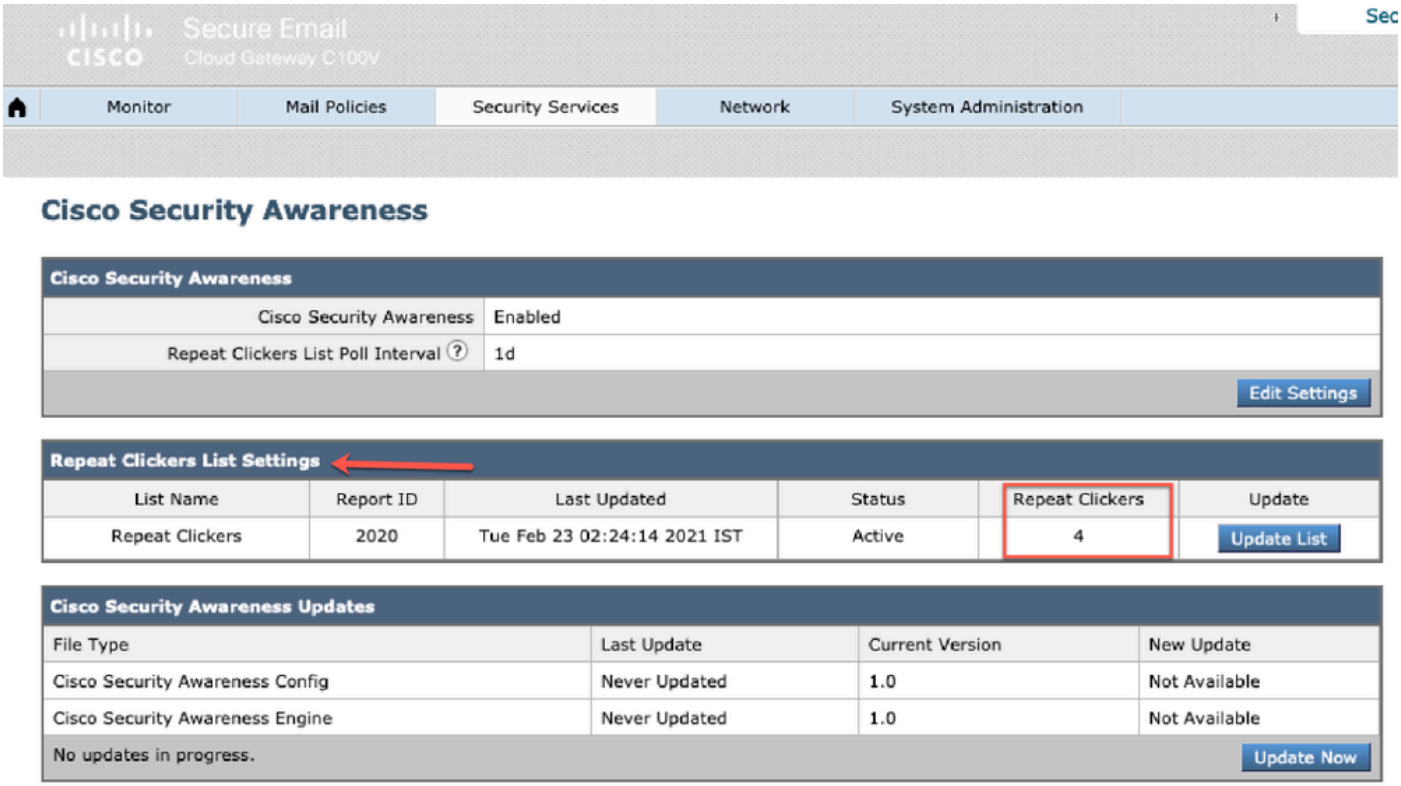
3. Esaminare i log CSA per verificare se l'elenco di cliccatori ripetuti è stato scaricato o se si è verificato un errore. Di seguito è riportata la working setup:

```
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 Awarenesscome mostrato nell'immagine.




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).