

Configurar a integração de percepção de segurança com o Cisco Secure Email Gateway

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Criar e enviar simulações de phishing do CSA Cloud Service](#)

[Etapa 1. Fazer login no CSA Cloud Service](#)

[Etapa 2. Criar um destinatário de e-mail de phishing](#)

[Etapa 3. Habilitar a API de Relatório](#)

[Etapa 4. Criar Simulações de Phishing](#)

[Etapa 5. Verificação de Simulações Ativas](#)

[O que é visto no lado do destinatário?](#)

[Verificar no CSA](#)

[Configurar o Secure Email Gateway](#)

[Etapa 1. Ativar o recurso Cisco Security Awareness no Secure Email Gateway](#)

[Etapa 2. Permitir e-mails simulados de phishing do CSA Cloud Service](#)

[Etapa 3. Executar Ação no Clique de Repetição do SEG](#)

[Guia de solução de problemas](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve as etapas necessárias para configurar a integração do Cisco Security Awareness (CSA) com o Cisco Secure Email Gateway.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conceitos e configuração do Cisco Secure Email Gateway
- Serviço em nuvem CSA

Componentes Utilizados

As informações neste documento são baseadas no AsyncOS para SEG 14.0 e posterior.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Criar e enviar simulações de phishing do CSA Cloud Service

Etapa 1. Fazer login no CSA Cloud Service

Consulte:

1. <https://secat.cisco.com/> para a região AMÉRICAS
2. <https://secat-eu.cisco.com/> para a região Europa

Etapa 2. Criar um destinatário de e-mail de phishing

Navegue até **Environment > Users > Add New User** os campos E-mail, Nome, Sobrenome e Idioma, preencha-os e clique **Save Changes** conforme mostrado na imagem.

The screenshot displays the 'User - Profile' configuration page in the CSA Cloud Service interface. The left-hand navigation menu has 'Environment' and 'Users' highlighted. The main form area contains the following fields and options:

- Email:** ciscotac@cisco.com
- First Name:** Cisco
- Last Name:** TAC
- Language:** English
- Time Zone:** (UTC-06:00) Central Time (US & Canada)
- Note:** (empty text area)
- External UID:** External UID
- Username:** Use Email ciscotac@cisco.com
- SET PASSWORD:** SET PASSWORD
- Manager:** Name or Email
- Active:**

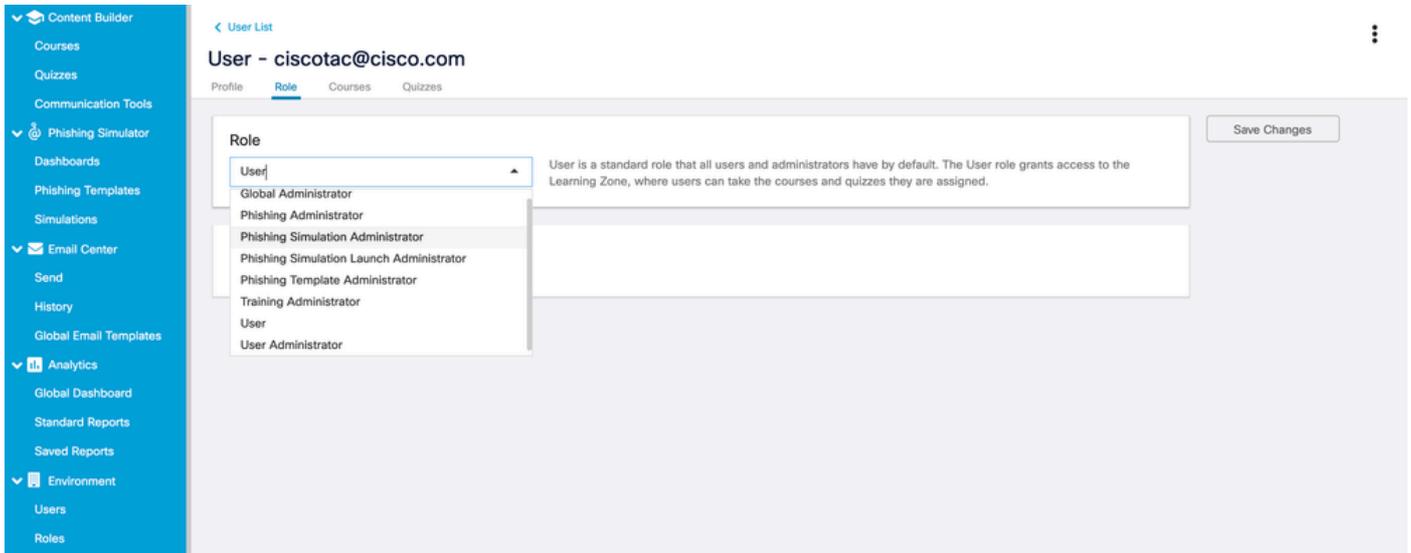
A red box highlights the 'Save Changes' button in the top right corner. Red arrows point to the Email, First Name, and Last Name fields with the text 'Fill this'.

Captura de tela da página da interface do usuário para adicionar um novo usuário



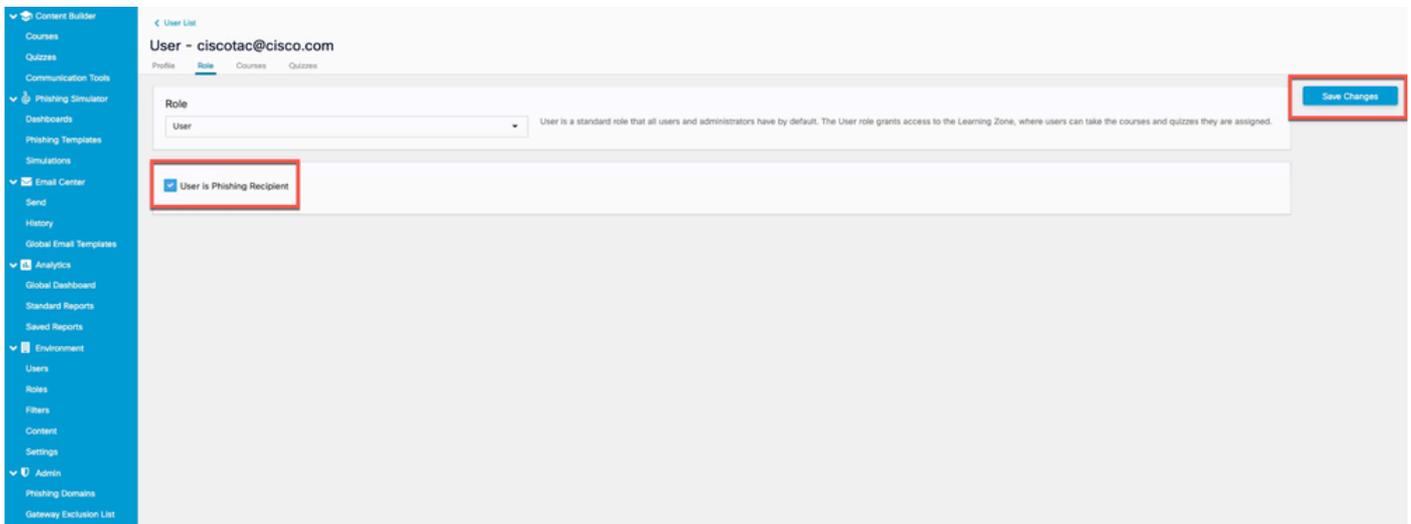
Note: Uma senha precisa ser definida apenas para um usuário administrador do CSA que está autorizado a criar e iniciar simulações.

A função do usuário pode ser selecionada depois que o usuário é criado. Você pode selecionar a função no menu suspenso como indicado nesta imagem:



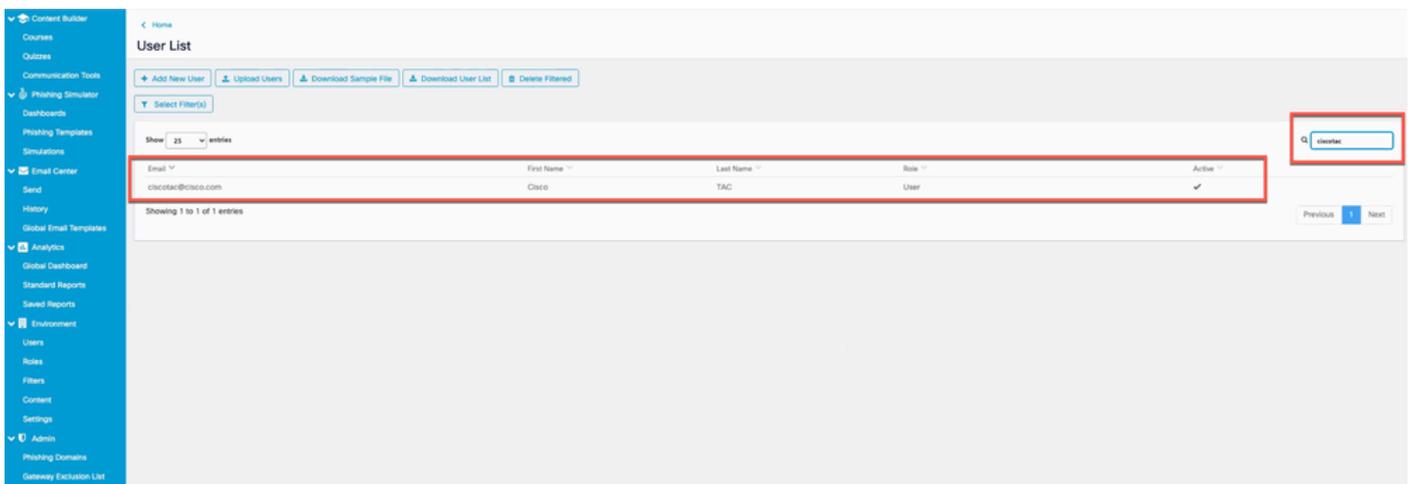
Exibição das opções suspensas de função de usuário

Marque a **User is Phishing Recipient** > Save Changes caixa de seleção conforme mostrado na imagem.



captura de tela mostrando que a caixa de seleção "O usuário é o destinatário de phishing" está ativada

Verifique se o usuário foi adicionado com êxito e se está listado quando pesquisado com base no endereço de e-mail no filtro, conforme mostrado na imagem.



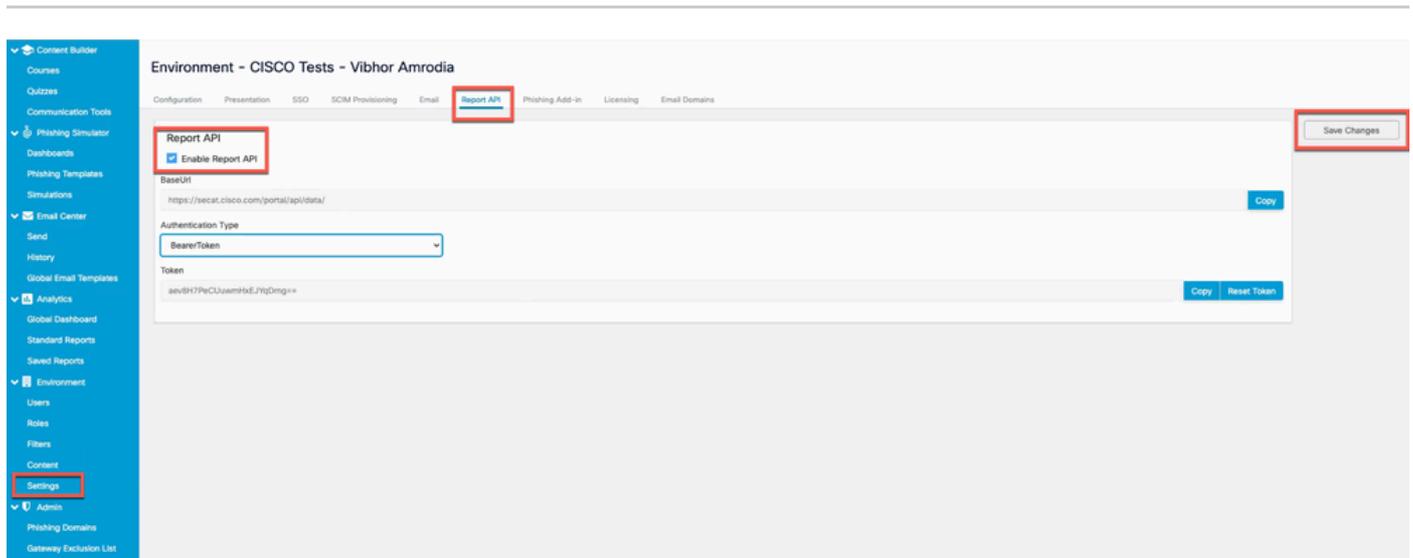
Captura de tela do novo usuário na lista de usuários

Etapa 3. Habilitar a API de Relatório

Navegue até a **Environments > Settings > Report API** guia e marque **Enable Report API > Save Changes** .



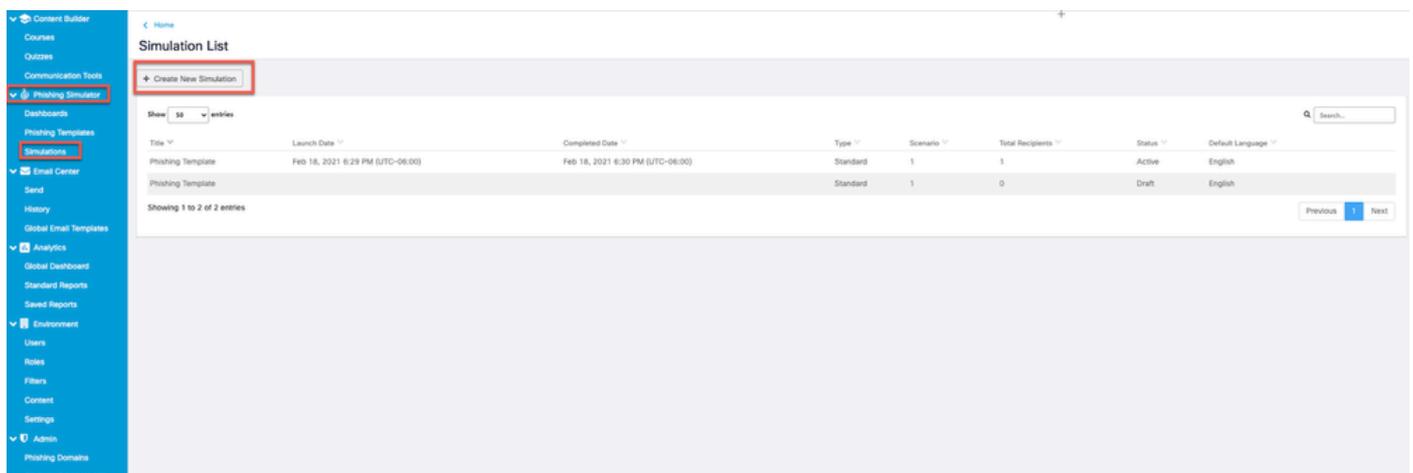
Note: Anote o Bearer Token (Token do portador). Você precisa disso para integrar o SEG ao CSA.



Captura de tela mostrando que a caixa de seleção "Habilitar API de Relatório" está habilitada.

Etapa 4. Criar Simulações de Phishing

a. Navegue até **Phishing Simulator > Simulations > Create New Simulation** e **selecione um Template** na lista disponível, conforme mostrado na imagem.

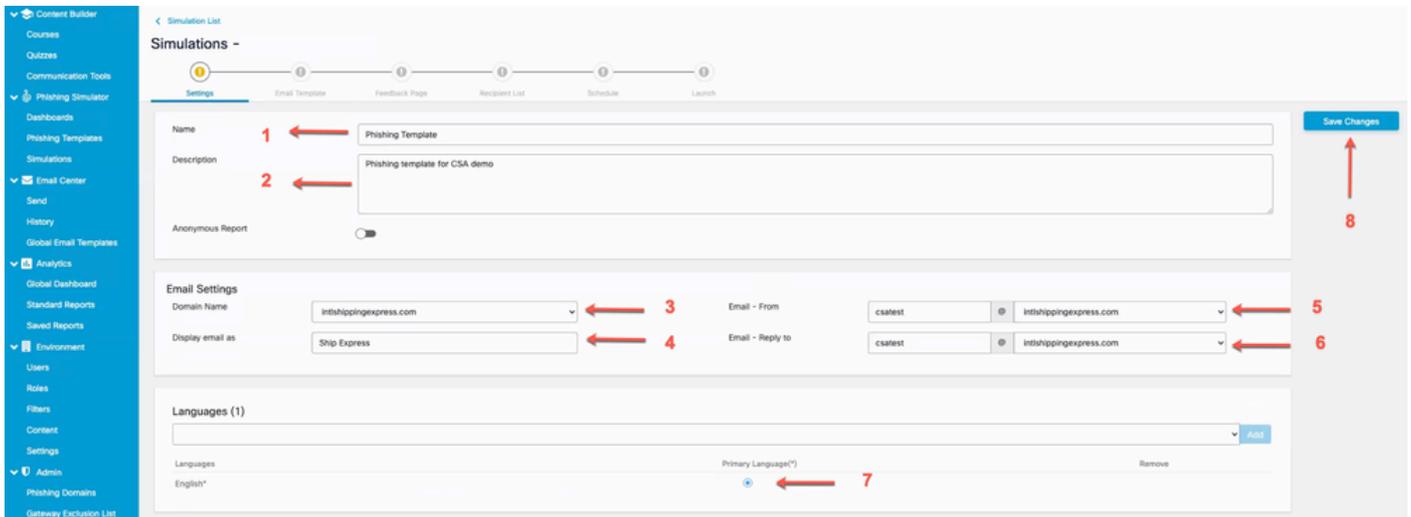


Captura de tela destacando o botão "Criar nova simulação"

b. Preencha estas informações:

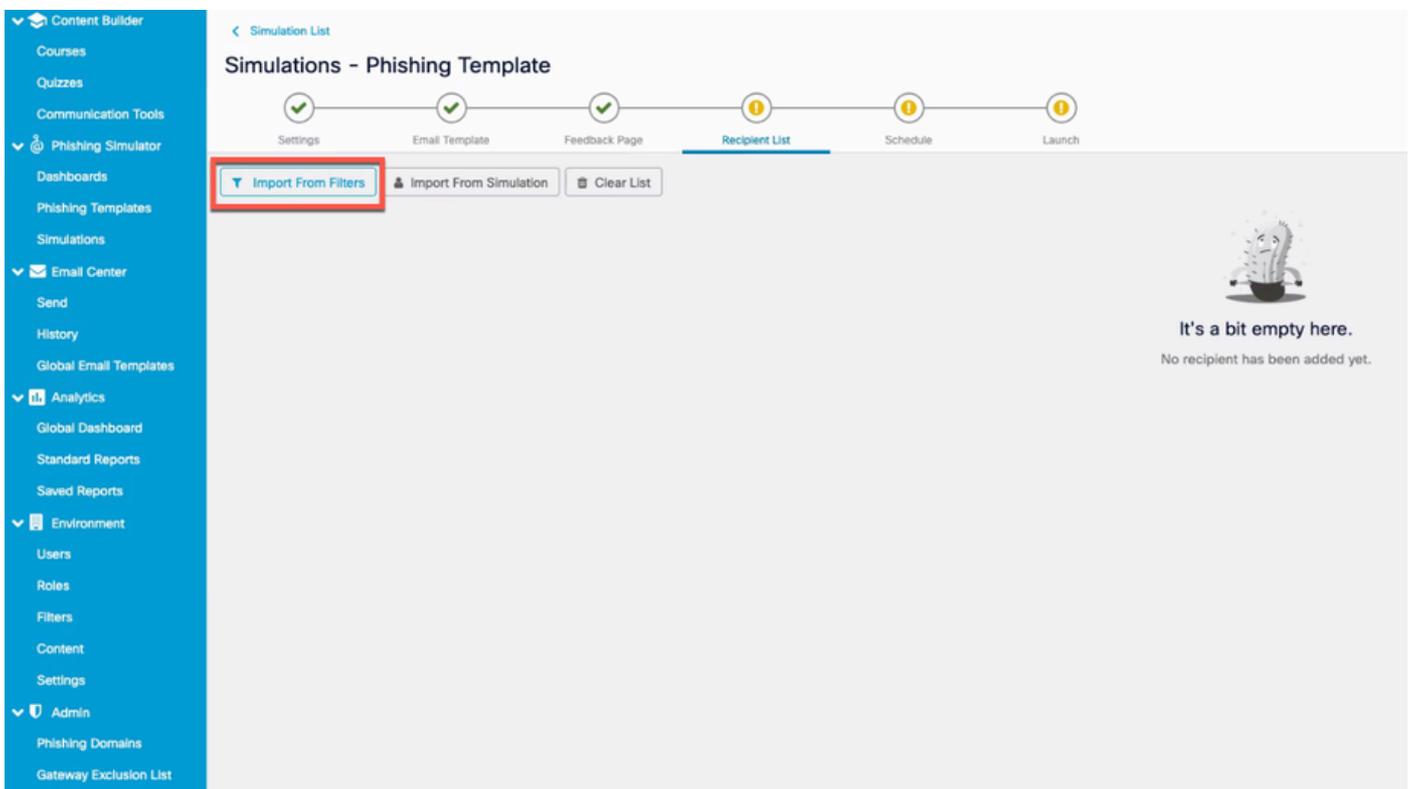
1. Selecione um nome para o modelo.

2. Descrever o modelo.
3. Nome de domínio para o qual o email de phishing é enviado.
4. O nome de exibição do email de phishing.
5. Endereço de e-mail de (selecione no menu suspenso).
6. Endereço para resposta (selecione no menu suspenso).
7. Selecione o idioma.
8. Salvar alterações.



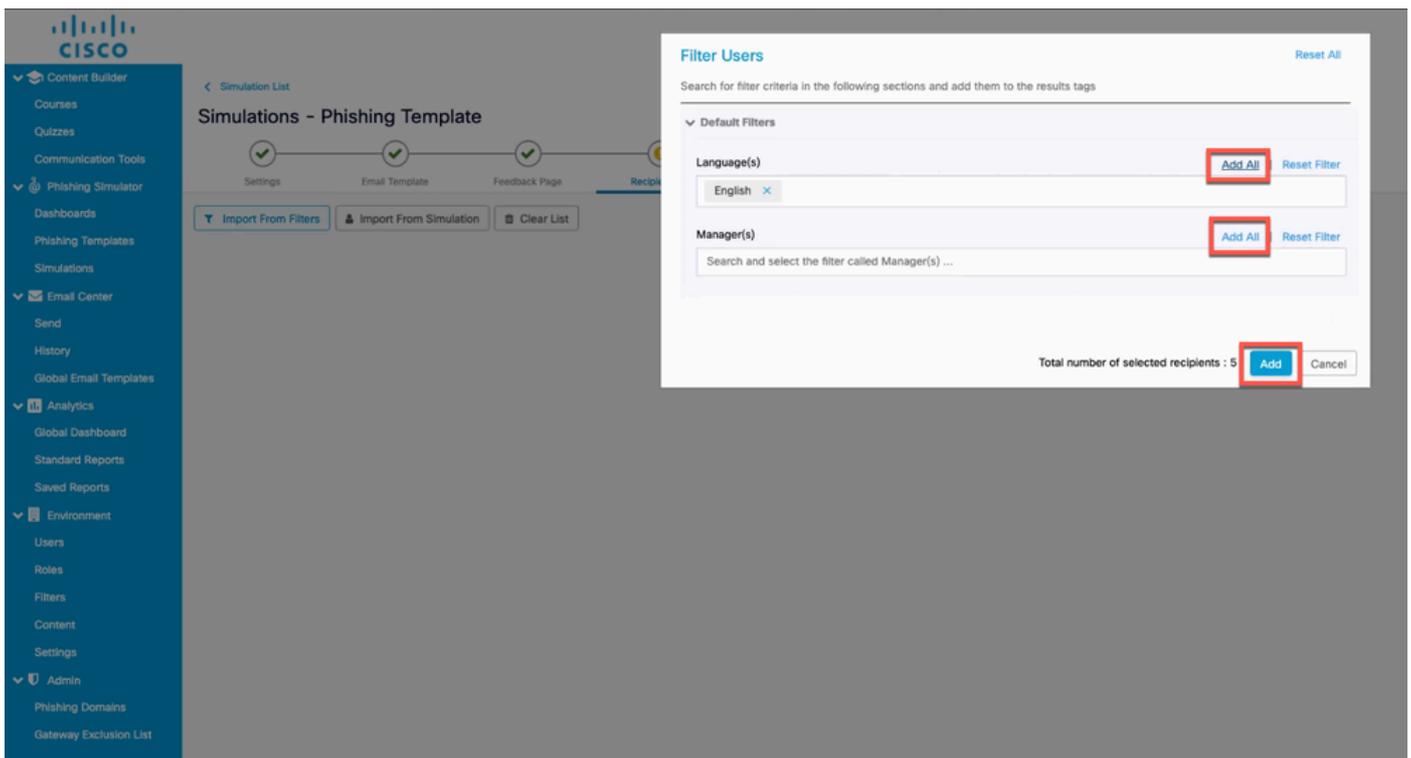
Captura de tela destacando campos que precisam ser preenchidos na configuração de uma nova simulação

c. Clique em **Import from Filters** e adicione os destinatários do e-mail de phishing à **Recipient List** conforme mostrado na imagem .



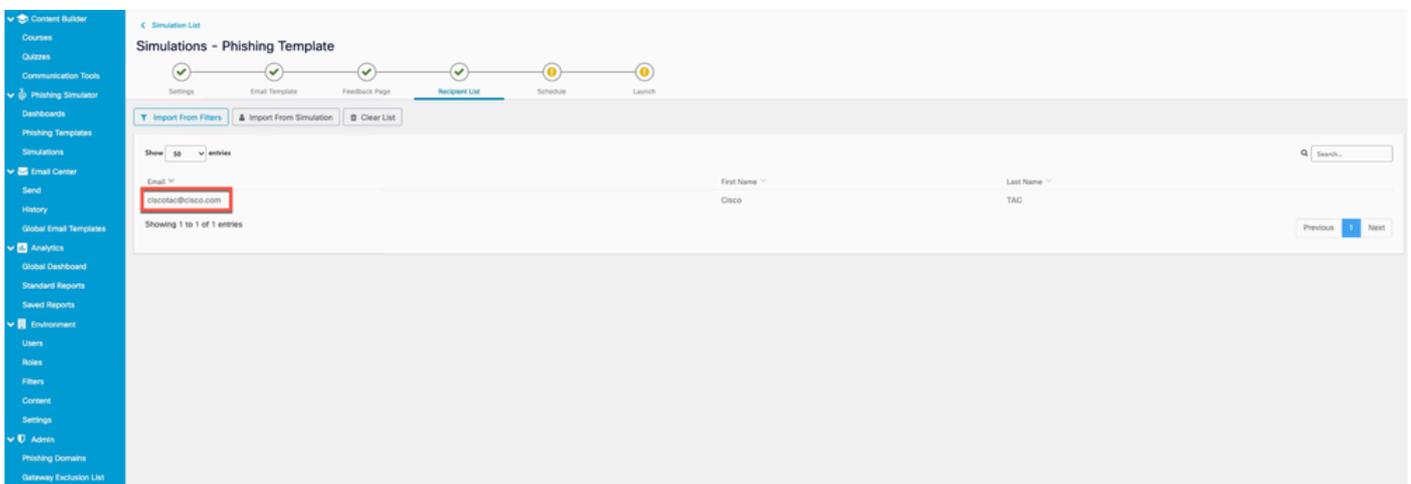
Captura de tela destacando o botão "Importar de filtros"

Você pode filtrar usuários por idioma ou gerentes. Clique em Add como mostrado na imagem.



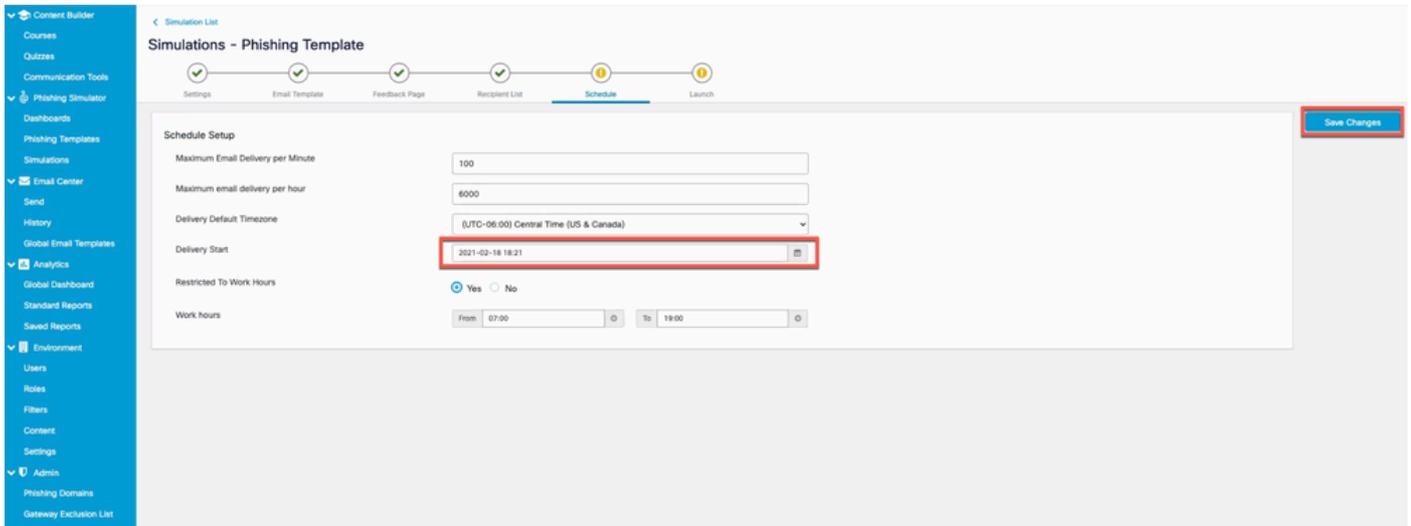
Captura de tela da caixa de diálogo Filtrar usuários para filtrar por idioma ou gerente

Aqui está um exemplo do usuário que foi criado na Etapa 2, que agora foi adicionado à lista de destinatários como mostrado na imagem.



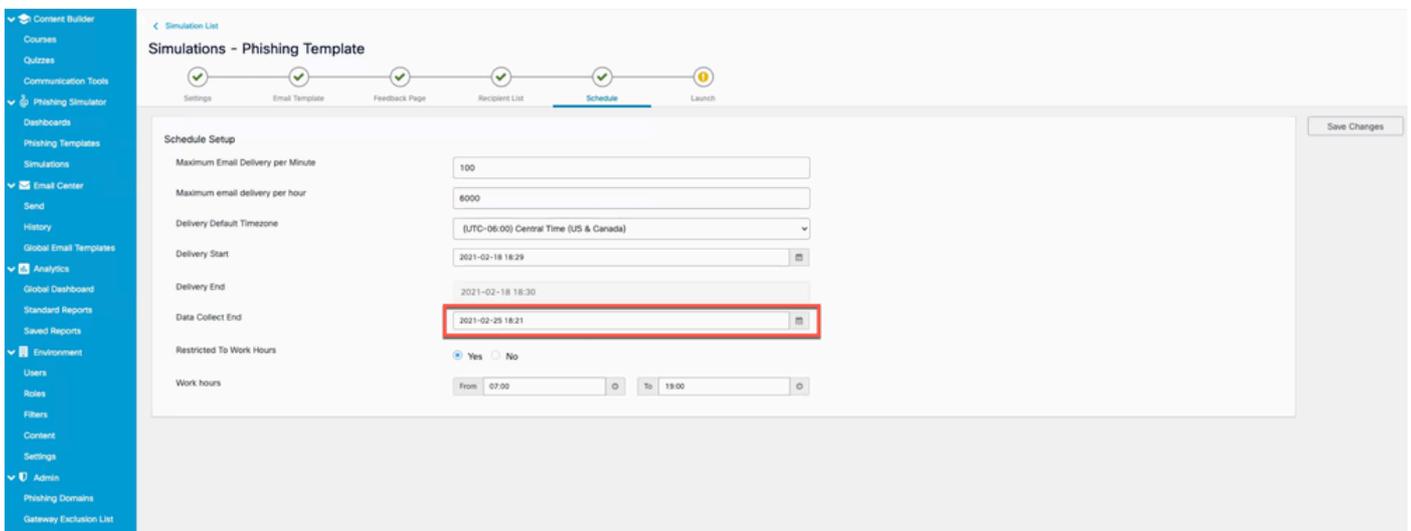
Captura de tela do usuário criado anteriormente listado como um destinatário para a simulação de phishing

d. Defina a data e as alterações para agendar a campanha, conforme mostrado na imagem.



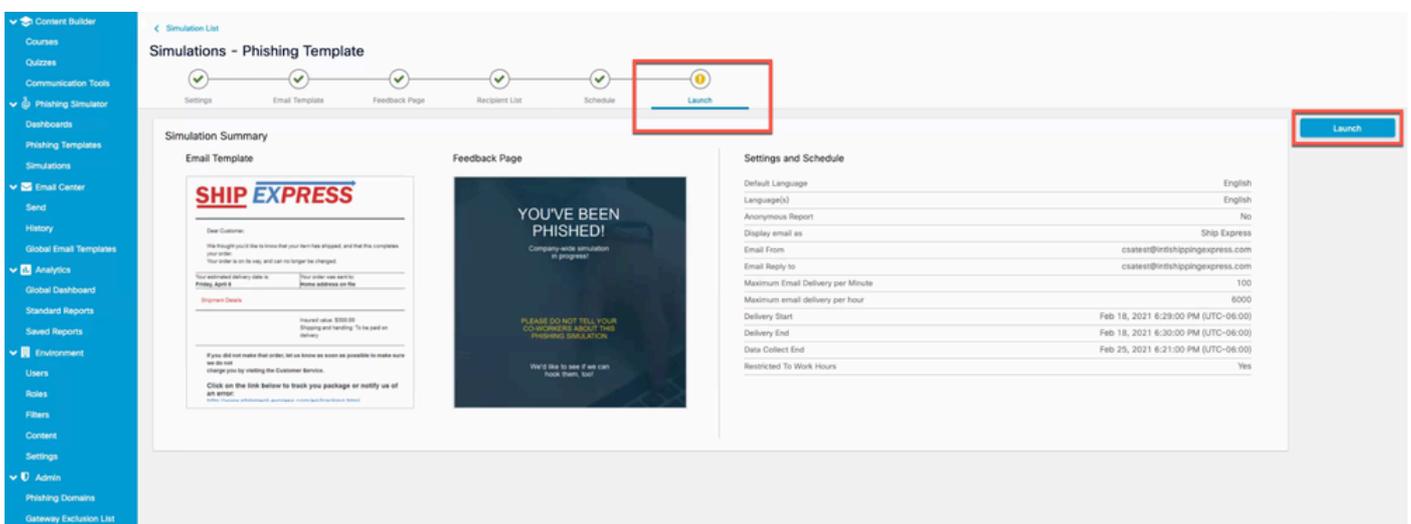
Captura de tela destacando o campo Início da entrega

Depois que a data de início é escolhida, a opção de selecionar o end date para a campanha é habilitada conforme mostrado na imagem.



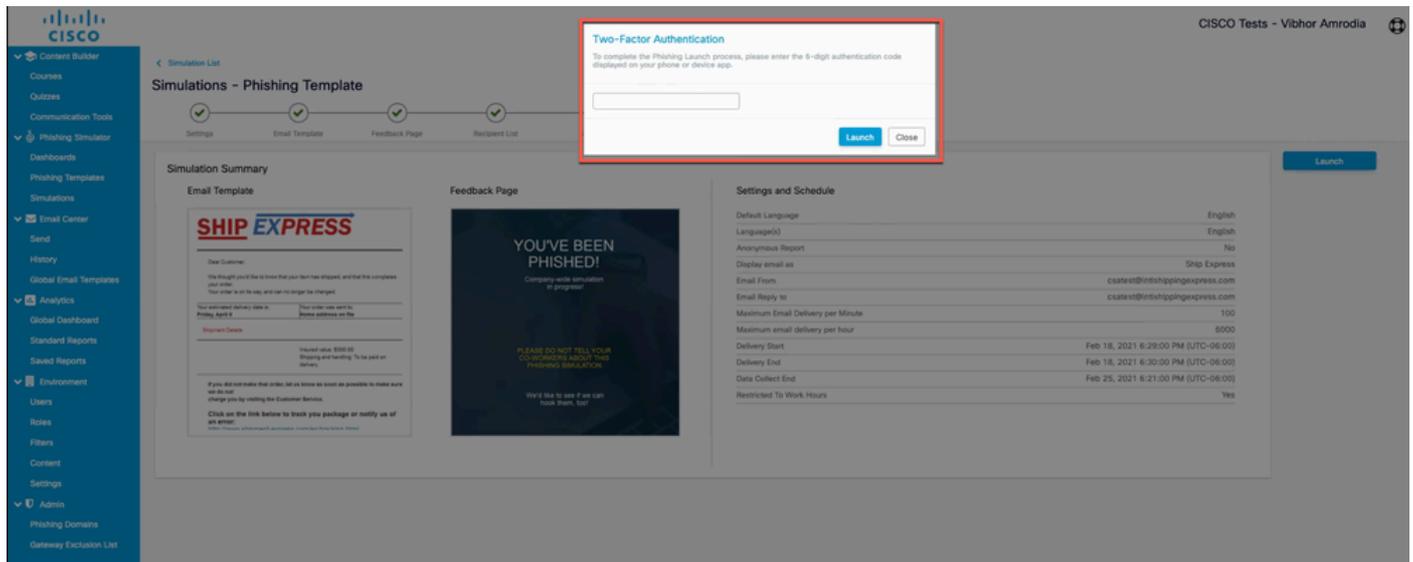
Captura de tela do realce do campo Data Collect End, que designa quando a simulação deve terminar

e. Clique em Launch para iniciar a campanha, conforme mostrado na imagem.



Captura de tela da aba final do assistente de criação de simulação onde a campanha pode ser iniciada

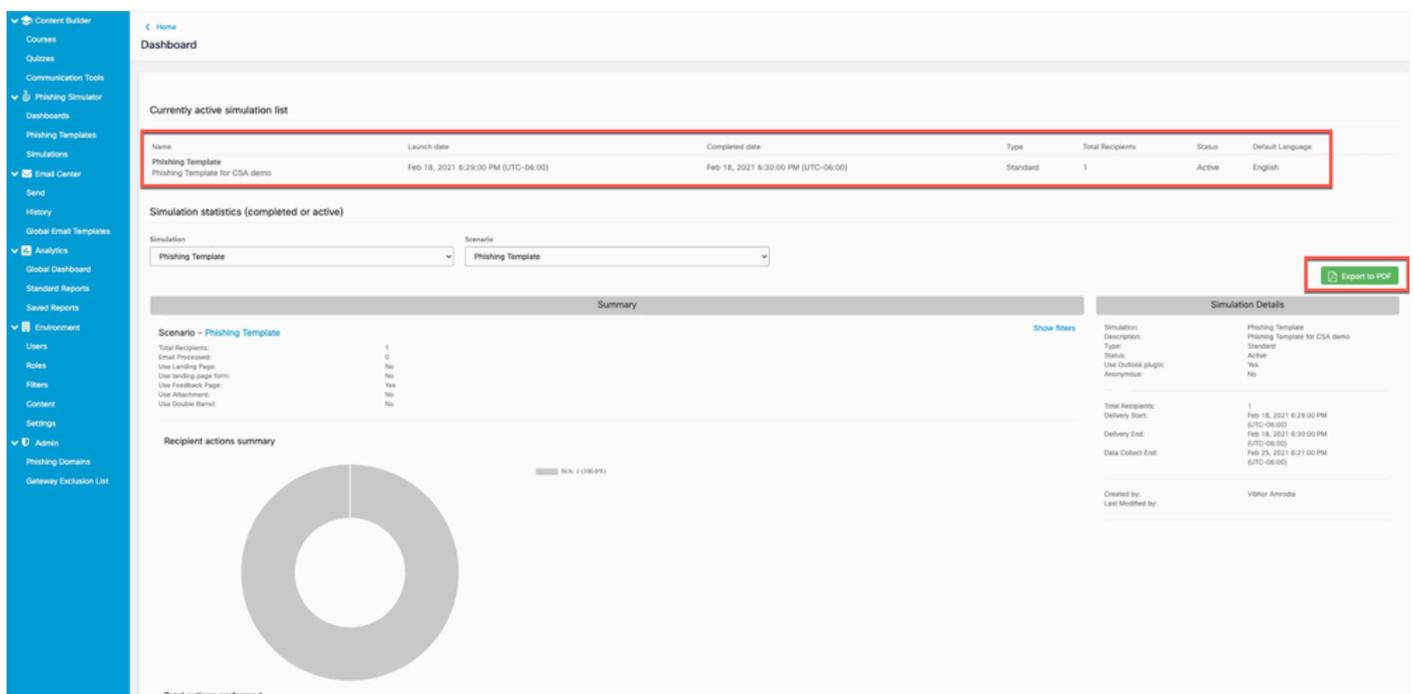
Um código de autenticação de dois fatores pode ser solicitado depois de clicar no botão Iniciar. Digite o código e clique em **Launch** conforme mostrado na imagem.



Captura de tela do pop-up solicitando o código de Autenticação de dois fatores

Etapa 5. Verificação de Simulações Ativas

Navegue até **Phishing Simulator > Dashboards**. A lista de simulação ativa atual fornece as simulações ativas. Você também pode clicar **Export as PDF** e obter o mesmo relatório como mostrado na imagem.



Captura de tela do painel de simulações de phishing

O que é visto no lado do destinatário?

Exemplo de um e-mail de simulação de phishing na caixa de entrada do destinatário.

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

 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.

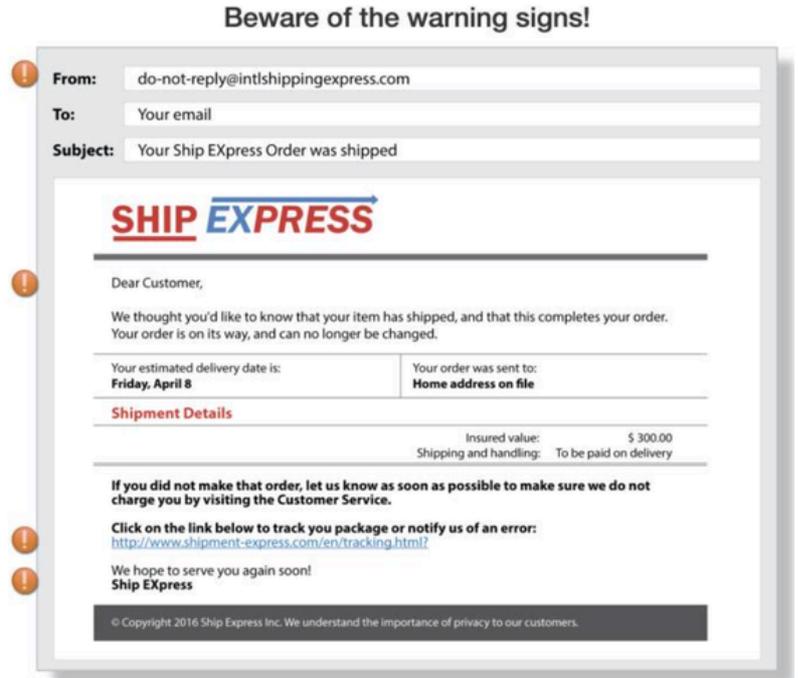
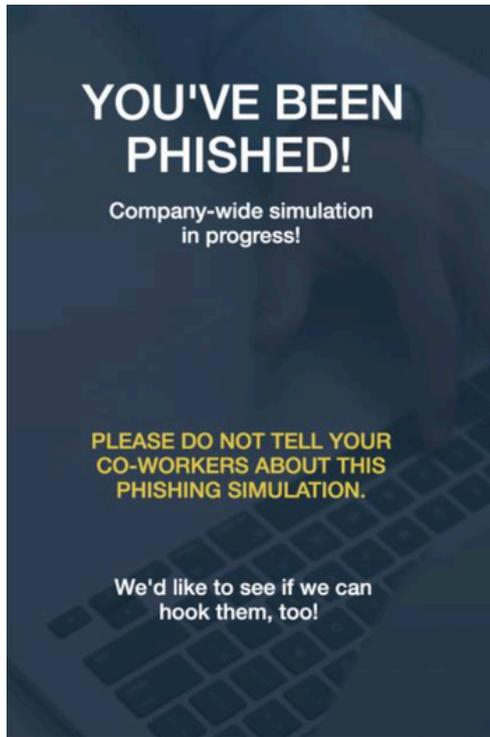
Click on the link below to track you package or notify us of an error:
<http://www.shipment-express.com/en/tracking.html>

We hope to serve you again soon!
Ship Express

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

Exemplo de e-mail simulado de phishing em uma caixa de correio de usuário

Quando o destinatário clica no URL, essa página de feedback é mostrada ao usuário e esse usuário aparece como parte da lista de Clientes Repetidos (que clicou livremente no URL do phishing) no CSA.



ALWAYS REMEMBER

Exemplo da página de comentários que o usuário verá depois de clicar no URL no e-mail de phishing

Verificar no CSA

A lista Repetir cliques é exibida em **Analytics > Standard Reports > Phishing Simulations > Repeat Clickers** as shown in the image.

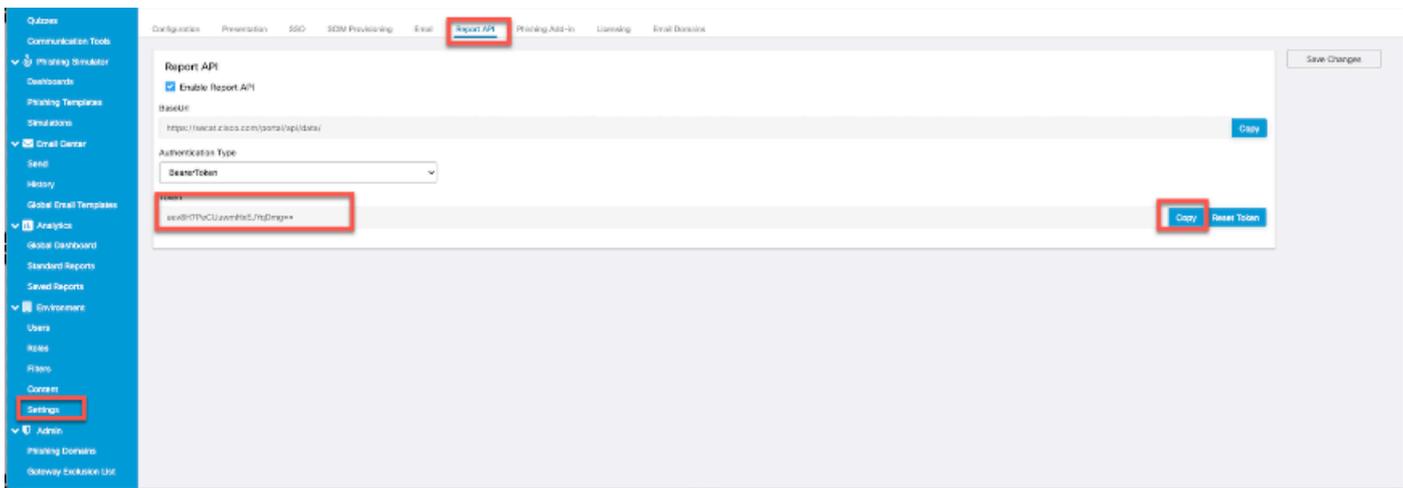
Last Name	First Name	Email	Language	Time Zone	Passed Simulations	Failed Simulation	Send Email	Received Emails	Opened Emails	Viewed Images	Clicked Link	Opened Attachment	Completed Form	Visited Page	Feedback Reported	Send Email (Double Barre)	Received Emails (Double Barre)	Opened Emails (Double Barre)	Views Image (Double Barre)
Madem	Rama	ramadem@cisco.com	English	(UTC-08:00)	2	19	21	19	19	5	19	0	0	18	0	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	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	0

Captura de tela da página Repetir cliques

Configurar o Secure Email Gateway



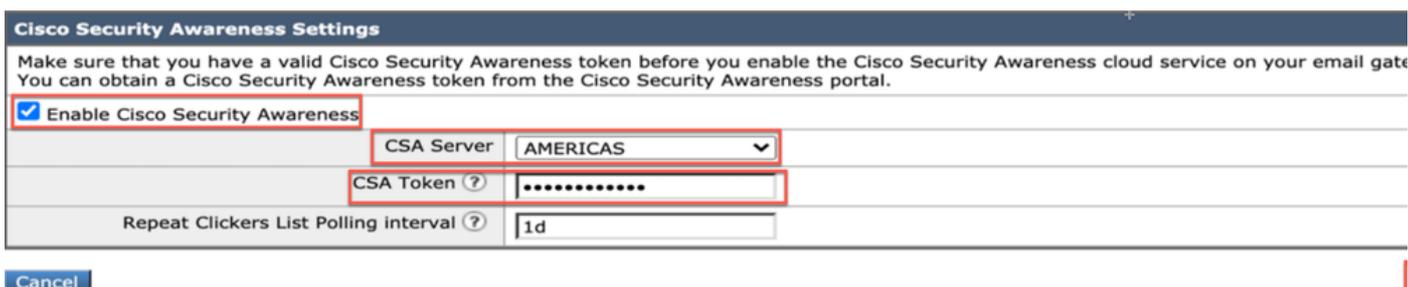
Note: Na seção **Create and Send Phishing Simulations** da Etapa 3 do CSA Cloud Service, quando você habilita o **Report API**, você anota o token do portador. Mantenha isto à mão.



Captura de tela da página na API de relatório, onde o administrador pode encontrar o token do portador

Etapa 1. Ativar o recurso Cisco Security Awareness no Secure Email Gateway

Na GUI do Secure Email Gateway, navegue para `Security Services > Cisco Security Awareness > Enable`. **Enter the Region and the CSA Token (Bearer Token obtain from CSA Cloud Service, conforme mostrado na observação mencionada anteriormente) e envie e confirme as alterações.**



Captura de tela da página de configurações do Cisco Security Awareness no Cisco Secure Email Gateway

Configuração de CLI

Digite `csaconfig` para configurar o CSA através do 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]>

## Etapa 2. Permitir e-mails simulados de phishing do CSA Cloud Service



Note: A política de fluxo de e-mail `CYBERSEC_AWARENESS_ALLOWED` é criada por padrão com todos os mecanismos de varredura definidos como Off (Desativado), conforme mostrado aqui.

| 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 tela da política de fluxo de e-mail "CYBERSEC\_AWARENESS\_ALLOWED" com recursos de segurança desativados

Para permitir que e-mails simulados de campanha de phishing do CSA Cloud Service ignorem todos os mecanismos de verificação no Secure Email Gateway:

- Crie um novo grupo de remetente e atribua a política de fluxo `CYBERSEC_AWARENESS_ALLOWED` de e-mail. Navegue até `Mail Policies > HAT Overview > Add Sender Group` e selecione a política `CYBERSEC_AWARENESS_ALLOWED`, defina a ordem como 1 e, em seguida, `Submit and Add Senders`.
- Adicione um remetente `IP/domain` ou `Geo Location` de onde os emails da campanha de Phishing foram iniciados.

Navegue até `Mail Policies > HAT Overview > Add Sender Group > Submit and Add Senders > Add the sender IP > Submit & Commit` alterações conforme mostrado na imagem.

| 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>Add Row</th> </tr> </thead> <tbody> <tr> <td>Select Source</td> <td></td> </tr> </tbody> </table>                                                                                                                                   | Source Name | Add Row | Select Source |  |
| Source Name                                                                                                                                       | Add Row                                                                                                                                                                                                                                                                                      |             |         |               |  |
| 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). |             |         |               |  |
| <p>Cancel <span style="float: right;">Submit <span style="border: 1px solid red; padding: 2px;">Submit and Add Senders &gt;&gt;</span></span></p> |                                                                                                                                                                                                                                                                                              |             |         |               |  |

Captura de tela de um grupo de remetente CyberSec\_Awareness\_Allowed com a política de fluxo de mensagens "CYBERSEC\_AWARENESS\_ALLOWED" selecionada.

| Sender Details                                                                                                    |                                                                                                                          |
|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Sender Type:                                                                                                      | <input checked="" type="radio"/> IP Addresses <span style="margin-left: 100px;"><input type="radio"/> Geolocation</span> |
| 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)"/>                                                              |
| <p>Cancel <span style="float: right;"><span style="border: 1px solid red; padding: 2px;">Submit</span></span></p> |                                                                                                                          |

Captura de tela da página de configurações do Cisco Security Awareness no Cisco Secure Email Gateway

## Configuração de CLI:

1. Navegue até `listenerconfig > Edit > Inbound (PublicInterface) > HOSTACCESS > NEW > New Sender Group` .

2. Crie um novo grupo de remetente com a política de e-mail e adicione um IP/domínio do remetente de onde os e-mails da campanha de Phishing são iniciados.

3. Defina a ordem do novo grupo de remetente como 1 e use a opção `Move` em `listenerconfig > EDIT > Inbound (PublicInterface) > HOSTACCESS > MOVE` .

4. Confirmar.



Note: O IP do remetente é o endereço IP do CSA e se baseia na região selecionada. Consulte a tabela para obter o endereço IP correto a ser usado. Permita que esses endereços IP/nomes de host no firewall com número de porta 443 para SEG 14.0.0-xxx se conectem ao serviço de nuvem 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 tela dos endereços IP e nomes de host das regiões CSA Americas e EU

### Etapa 3. Executar Ação no Clique de Repetição do SEG

Depois que os e-mails de phishing forem enviados e a lista de cliques repetidos for preenchida no SEG, uma política agressiva de recebimento de e-mail pode ser criada para agir sobre e-mails para esses usuários específicos.

Crie uma nova política agressiva de recebimento de e-mails personalizados e ative `Include Repeat Clickers List` a caixa de seleção na seção do destinatário.

Na GUI, navegue até `Mail Policies > Incoming Mail Policies > Add Policy > Add User > Include Repeat Clickers List > Submit` e faça `Commit` as alterações.

**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 Only if all conditions match ▼  
 Following Recipients

Include Repeat Clickers List  
(From Cisco Security Awareness)

LDAP Group:  
 Query:

Group:

Following Recipients are Not

Email Address:

Captura de tela da Política de recebimento de e-mails configurada para manipular e-mails destinados a cliques repetidos

## Guia de solução de problemas

1. Navegue até `csaconfig > SHOW_LIST` para ver os detalhes da lista de cliques repetidos.

```
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. Navegue até `csaconfig > UPDATE_LIST` se você deseja forçar a atualização da lista de cliques repetidos.

```
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. Localize os logs do csa para ver se a lista de cliques repetidos foi baixada ou se há um erro.

Aqui está o 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. A lista de contagens de cliques repetidos também pode ser vista na GUI. Navegue até Security

Services > Cisco Security Awareness conforme mostrado na imagem.

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](#)

Captura de tela da página Serviços de segurança > Cisco Security Awareness destacando o número de cliques repetidos

Informações Relacionadas

- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.