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

Contents

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

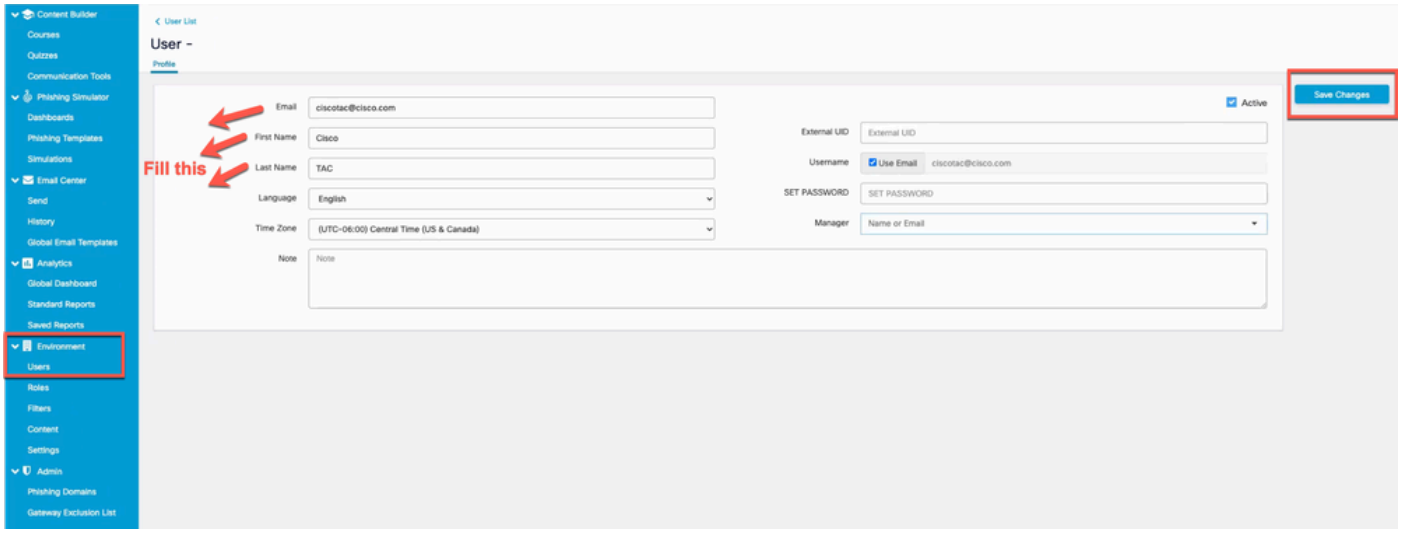
Etapa 1. Fazer login no CSA Cloud Service

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.

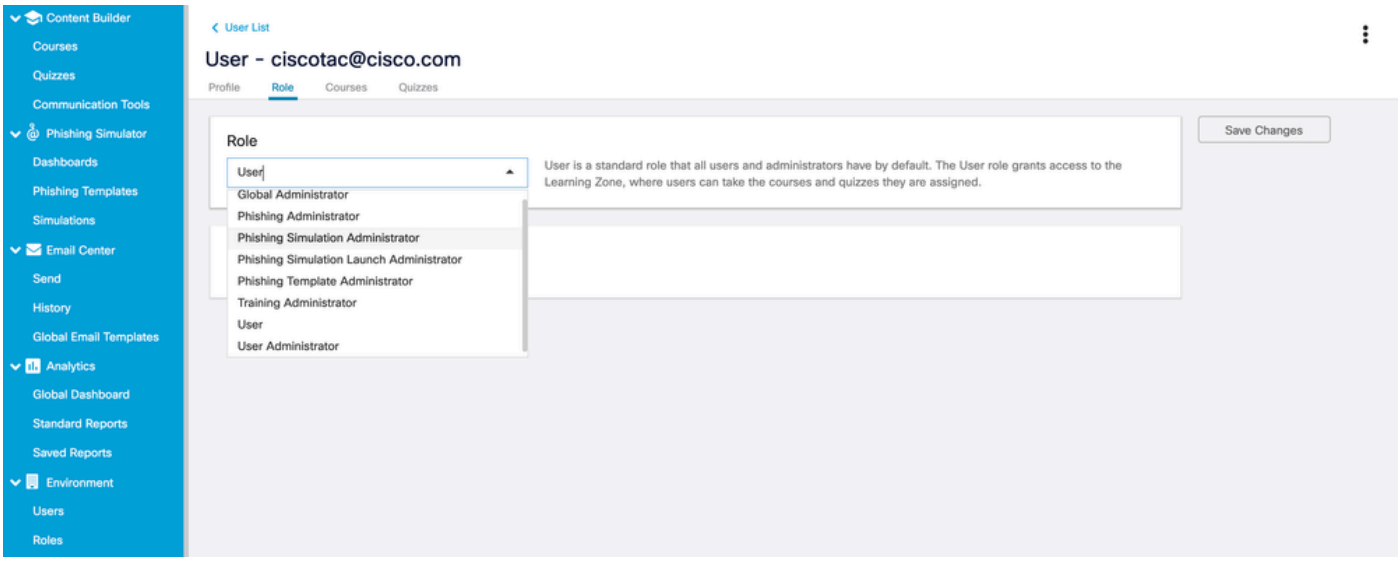


Captura de tela da página da interface do usuário para adicionar um novo usuário

---

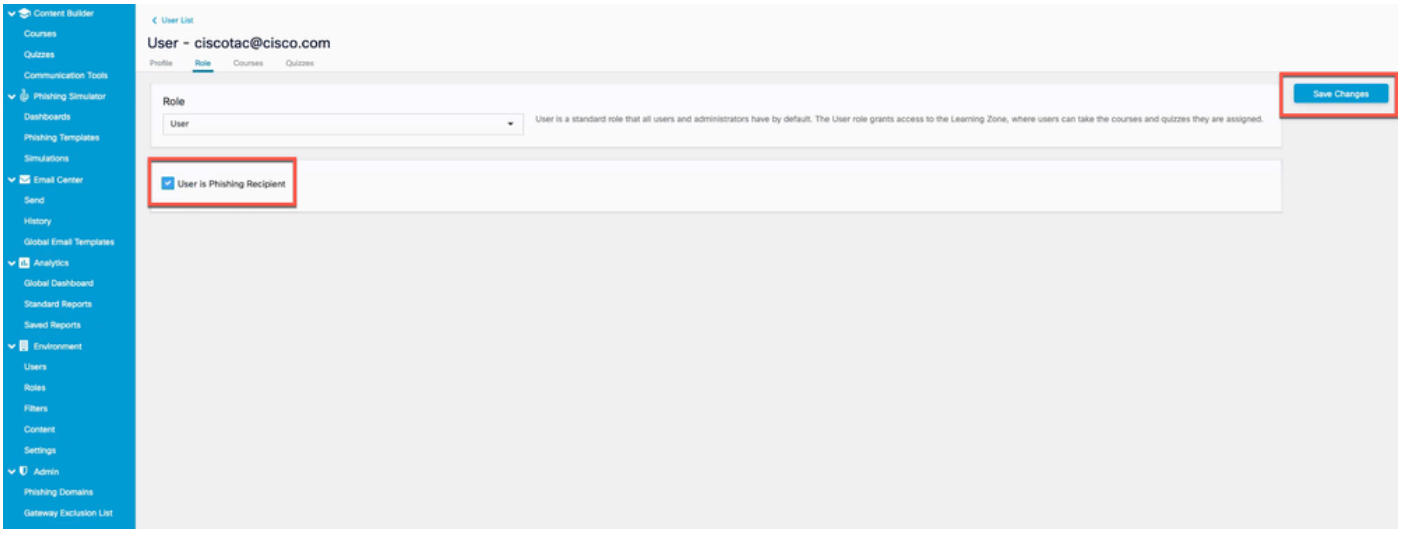
Note: Uma senha precisa ser definida apenas para um usuário administrador do CSA que está autorizado a criar e iniciar simulações.

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:



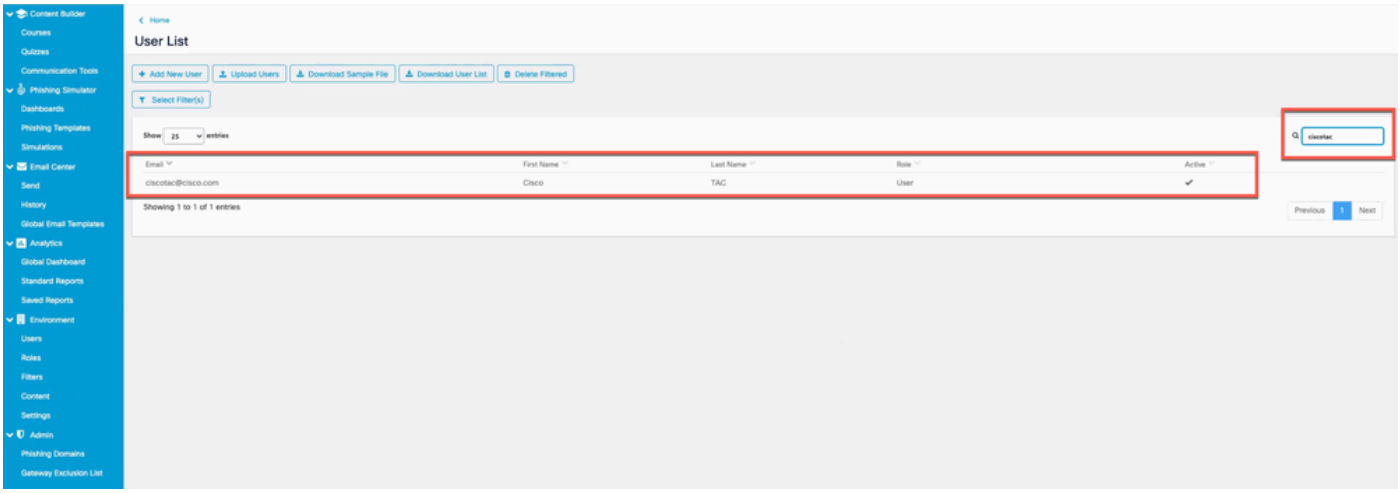
Exibição das opções suspensas de função de usuário

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.

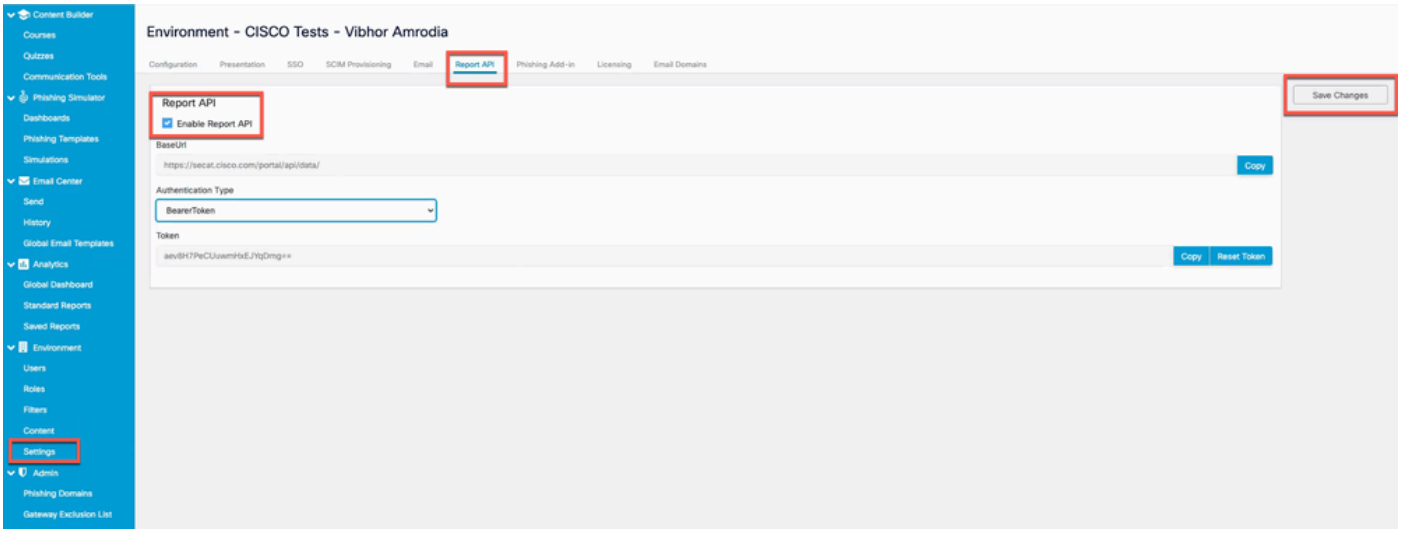


Captura de tela do novo usuário na lista de usuários

Etapa 3. Habilitar a API de Relatório

Navegue até a Environments > Settings > Report API guia e marqueEnable Report API > Save Changes .

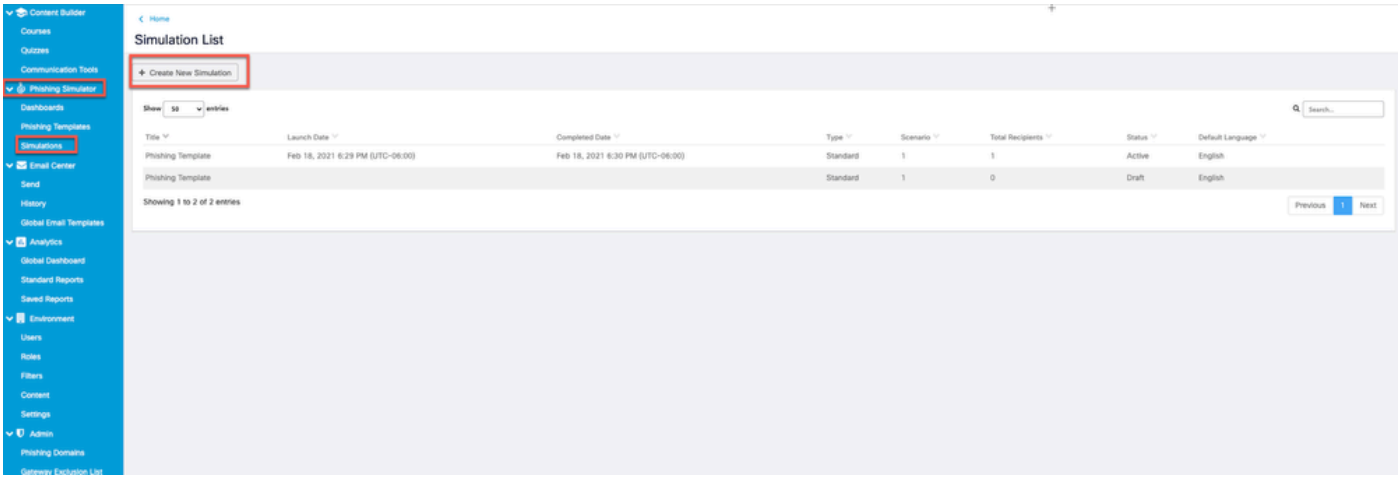
Note: Anote o Bearer Token (Token do portador). Você precisa disso para integrar o SEG ao CSA.



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.

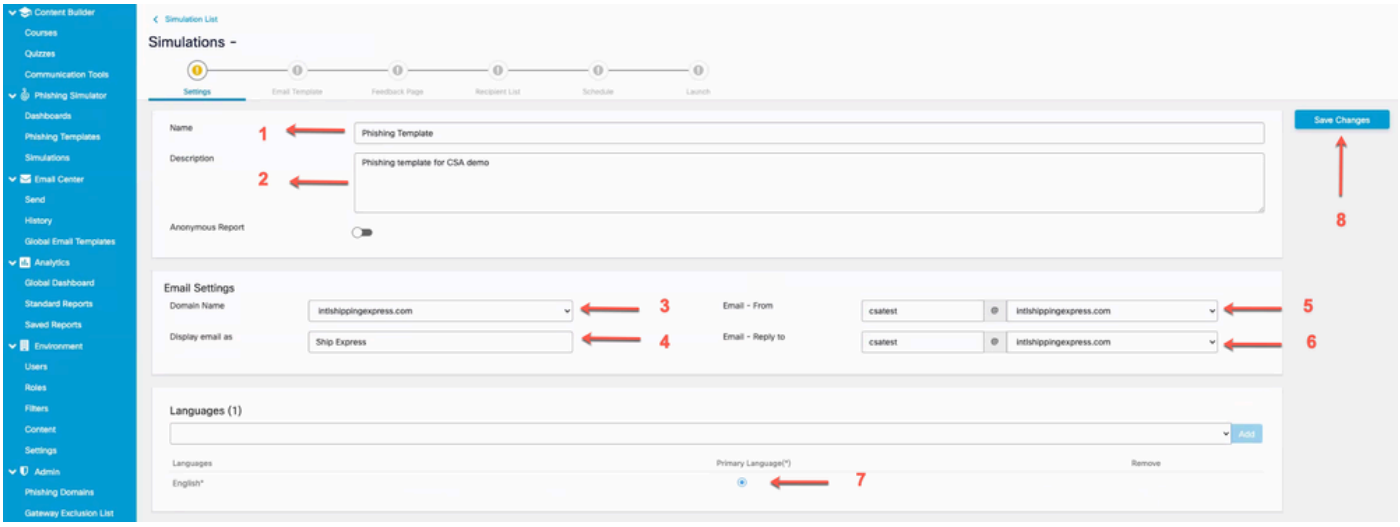


Captura de tela destacando o botão "Criar nova simulação"

b. Preencha estas informações:

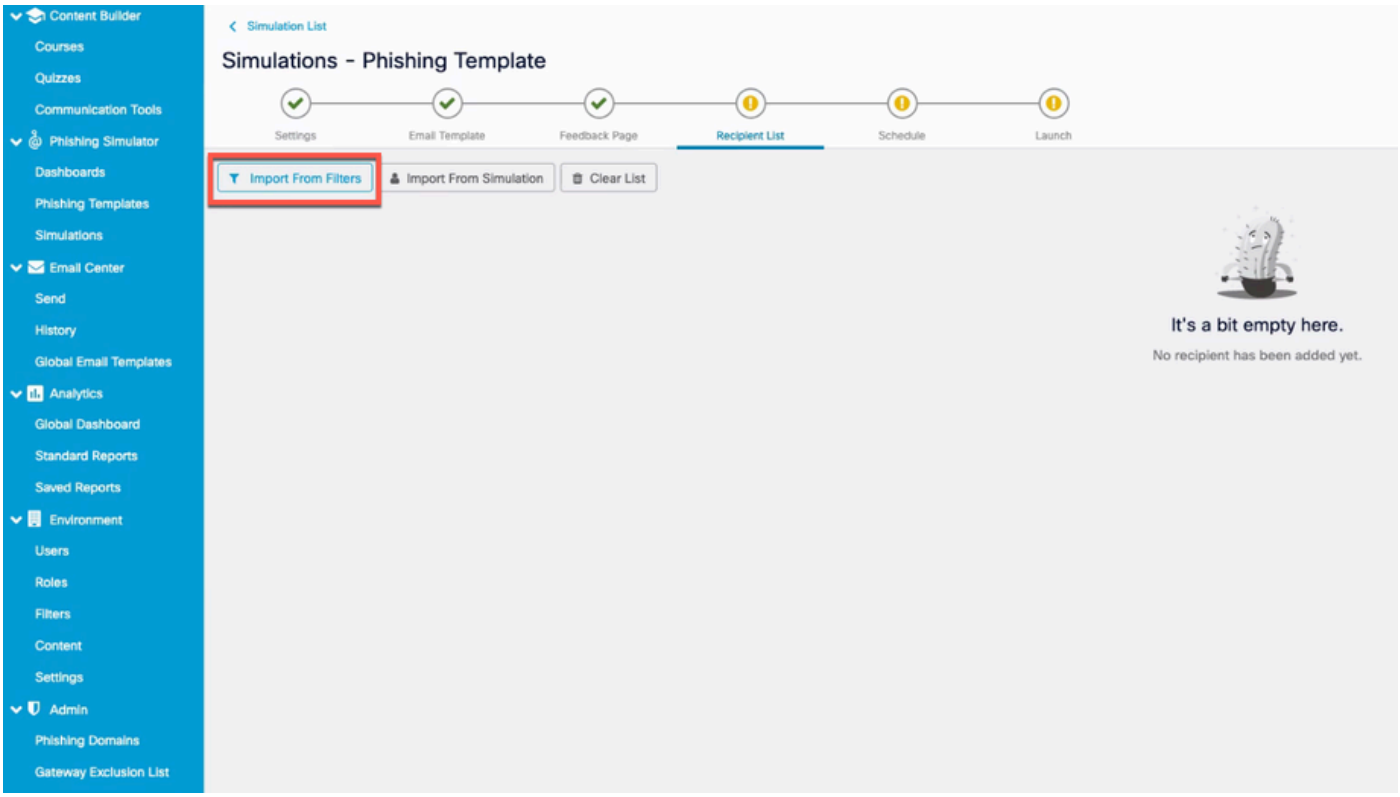
1. Selecione um nome para o modelo.

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.



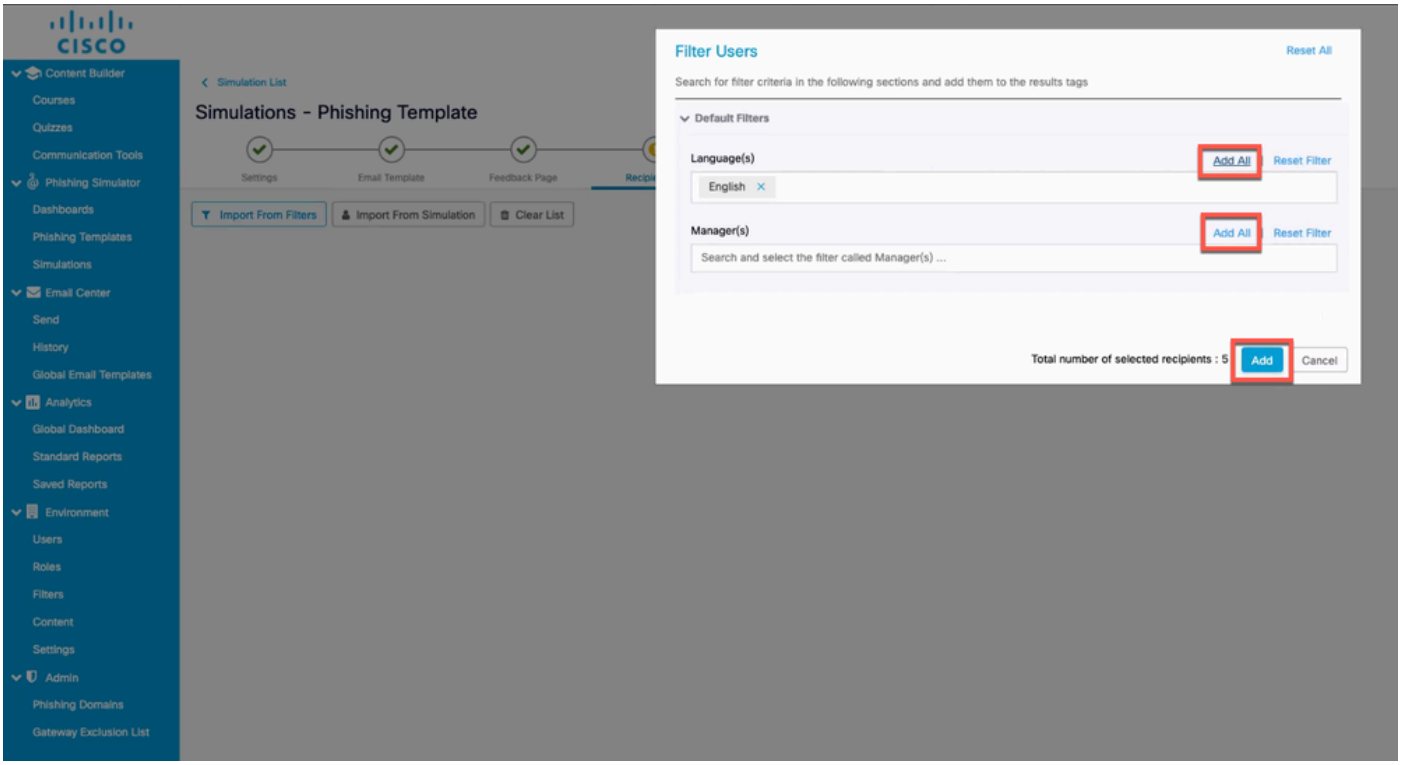
Captura de tela destacando campos que precisam ser preenchidos na configuração de uma nova simulação

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



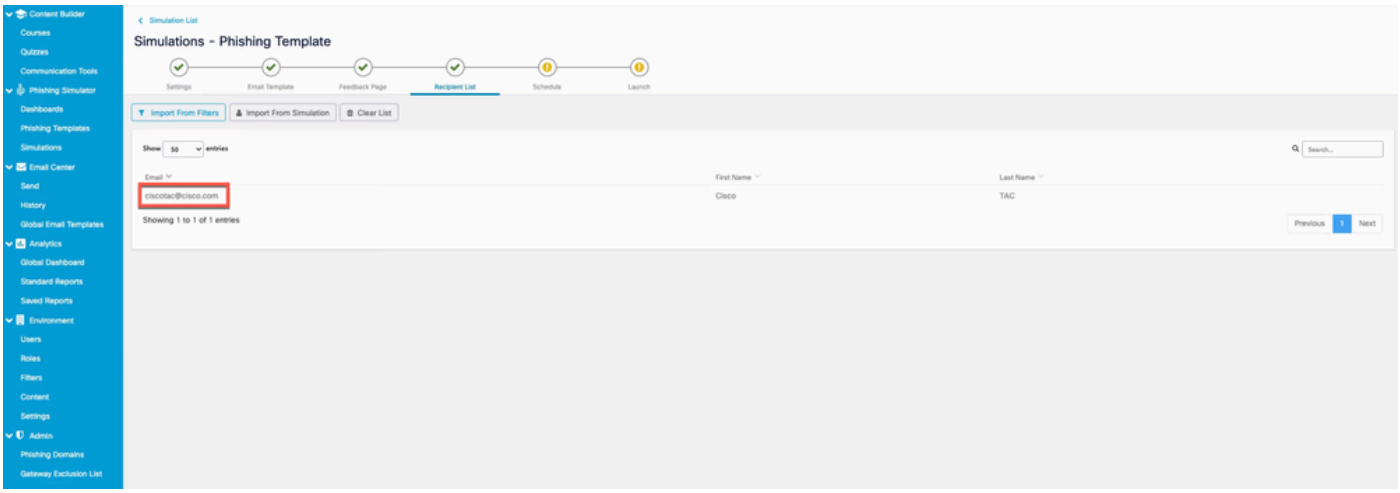
Captura de tela destacando o botão "Importar de filtros"

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



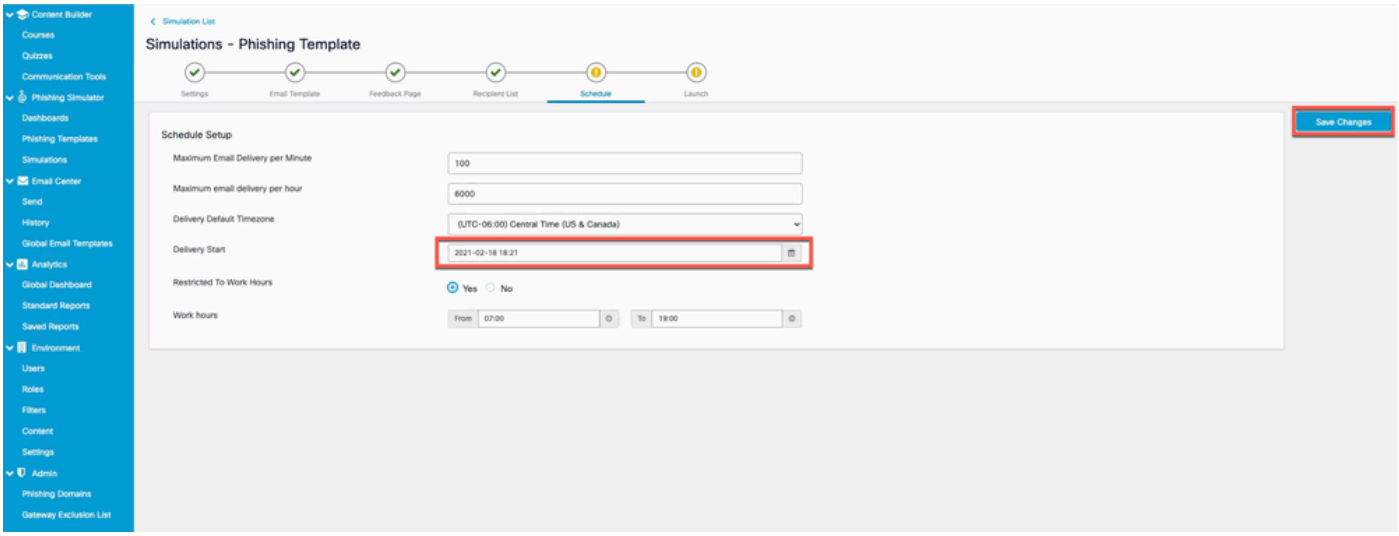
Captura de tela da caixa de diálogo Filtrar usuários para filtrar por idioma ou gerente

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



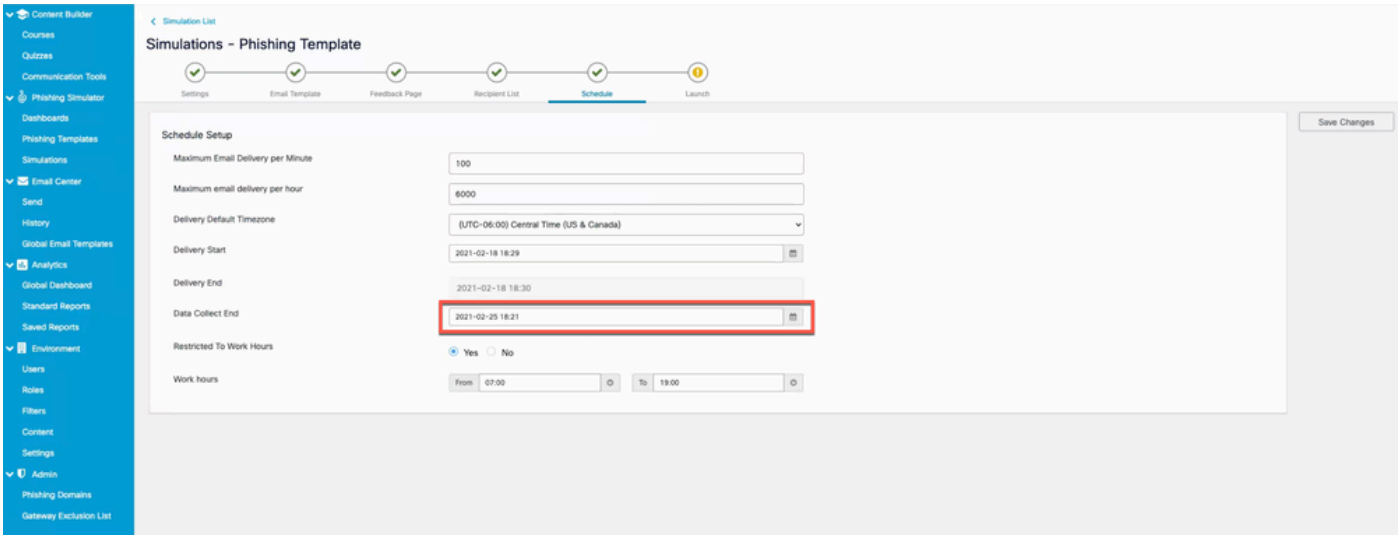
Captura de tela do usuário criado anteriormente listado como um destinatário para a simulação de phishing

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



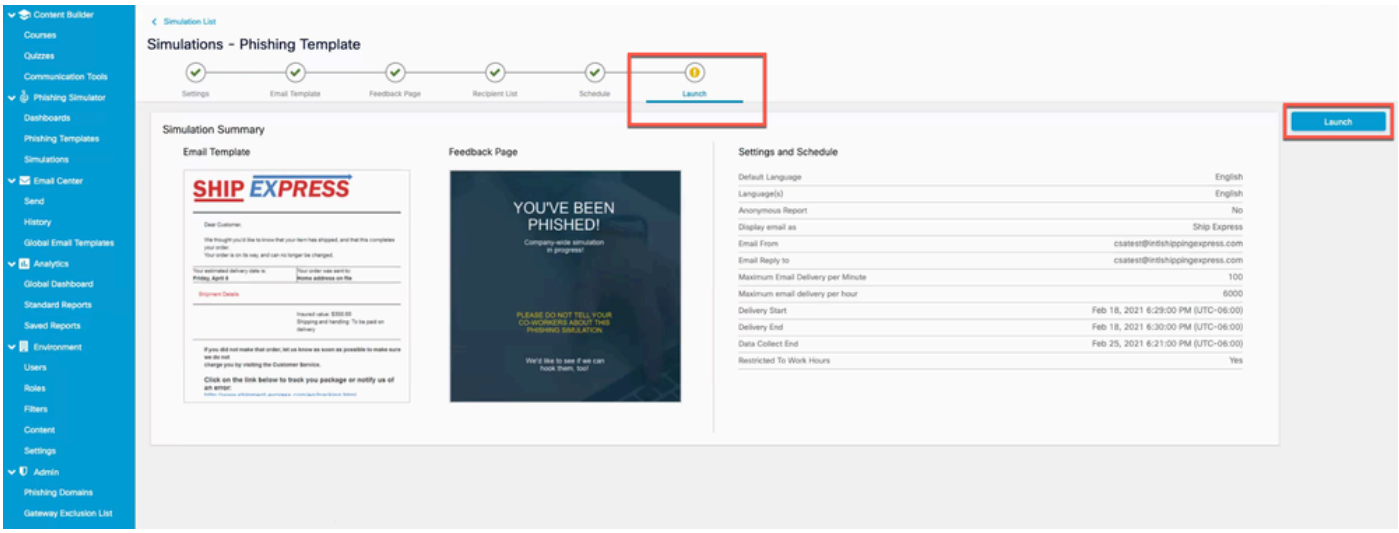
Captura de tela destacando o campo Início da entrega

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



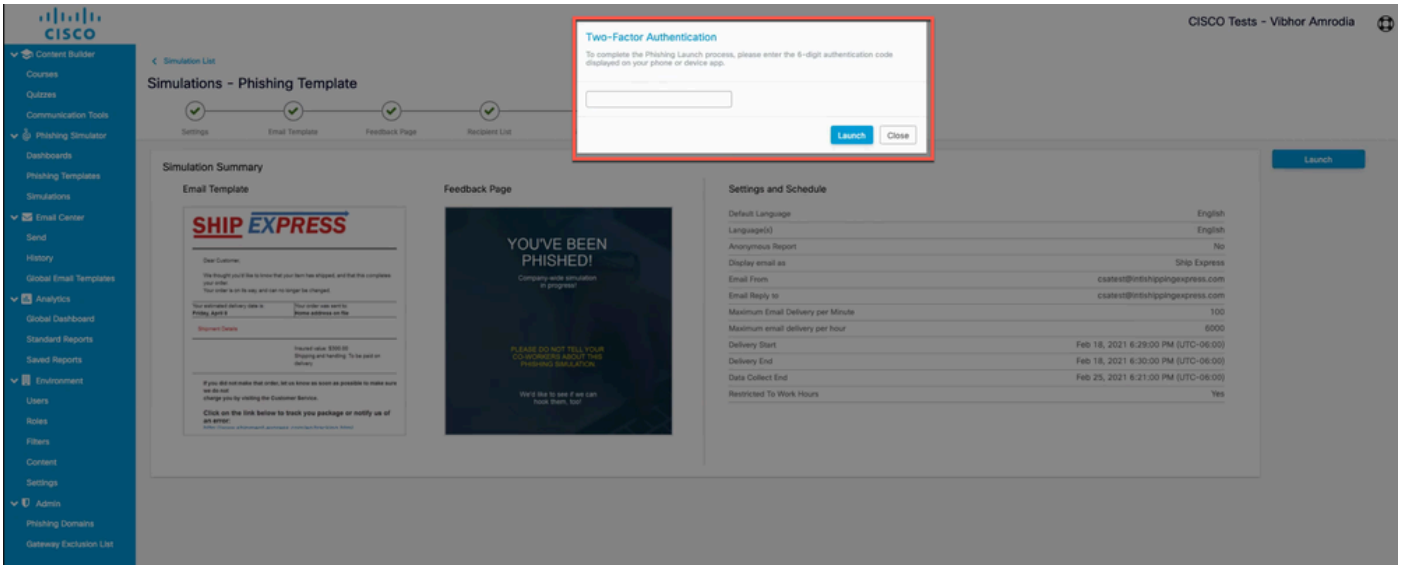
Captura de tela do realce do campo Data Collect End, que designa quando a simulação deve terminar

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

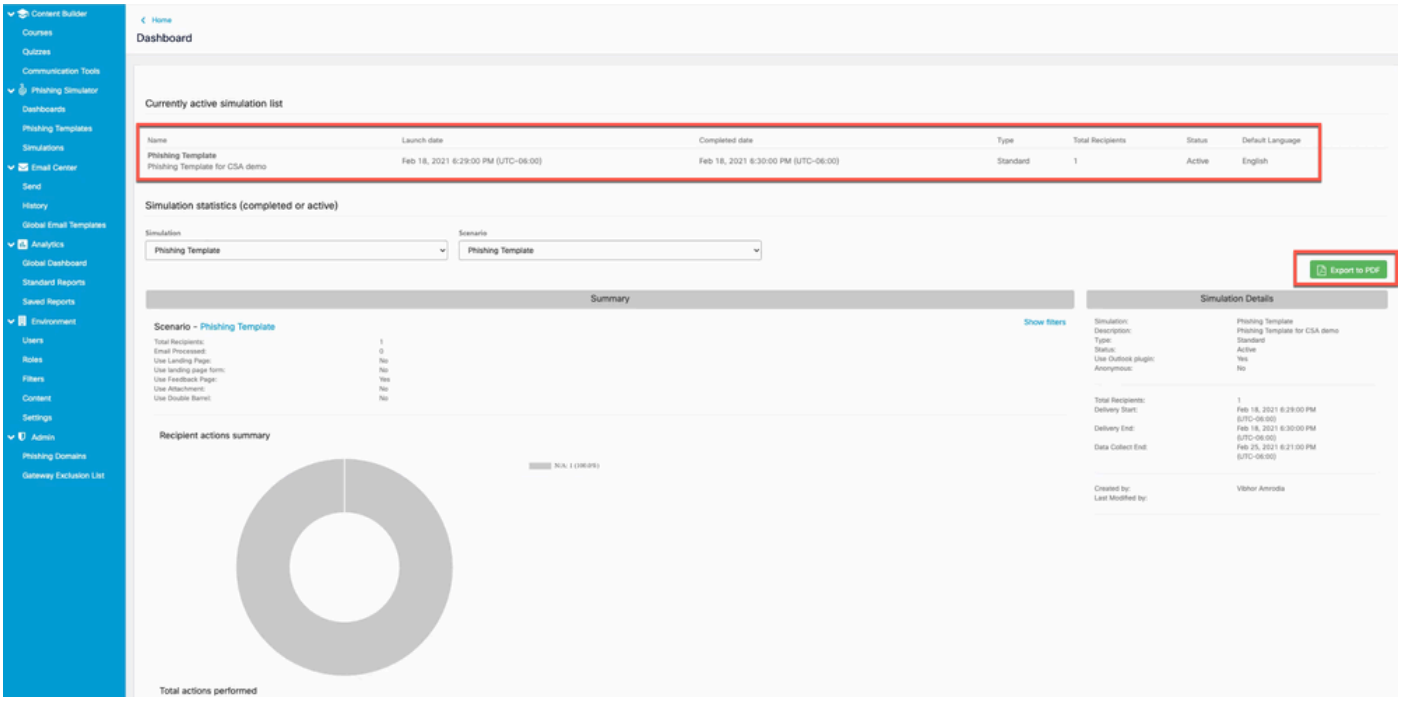
Um código de autenticação de dois fatores pode ser solicitado depois de clicar no botão Iniciar. Digite o código e clique em Launchconforme mostrado na imagem.



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

Etapa 5. Verificação de Simulações Ativas

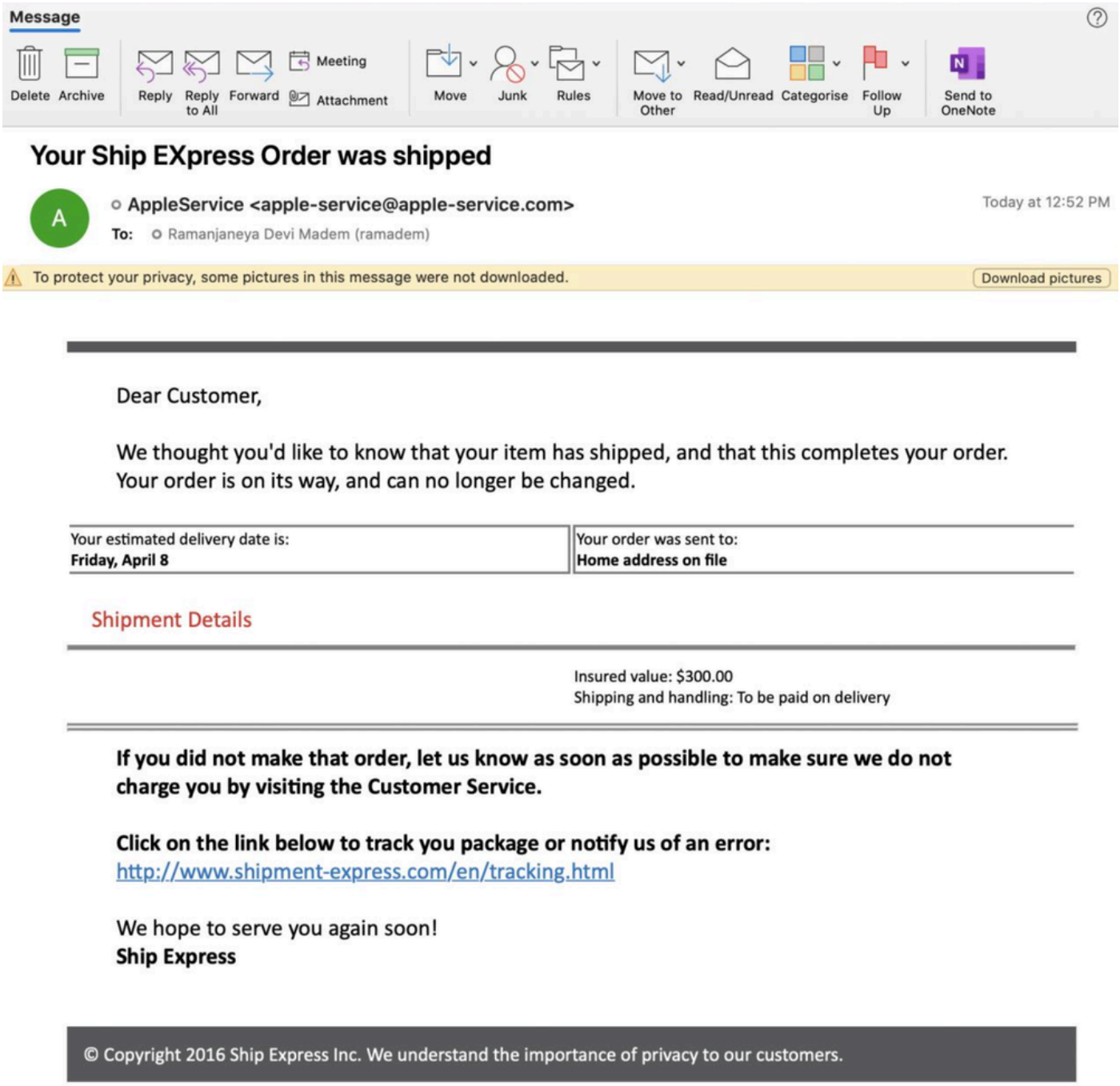
Navegue atéPhishing Simulator > Dashboards. A lista de simulação ativa atual fornece as simulações ativas. Você também pode clicar Export as PDF e obter o mesmo relatório como mostrado na imagem.



Captura de tela do painel de simulações de phishing

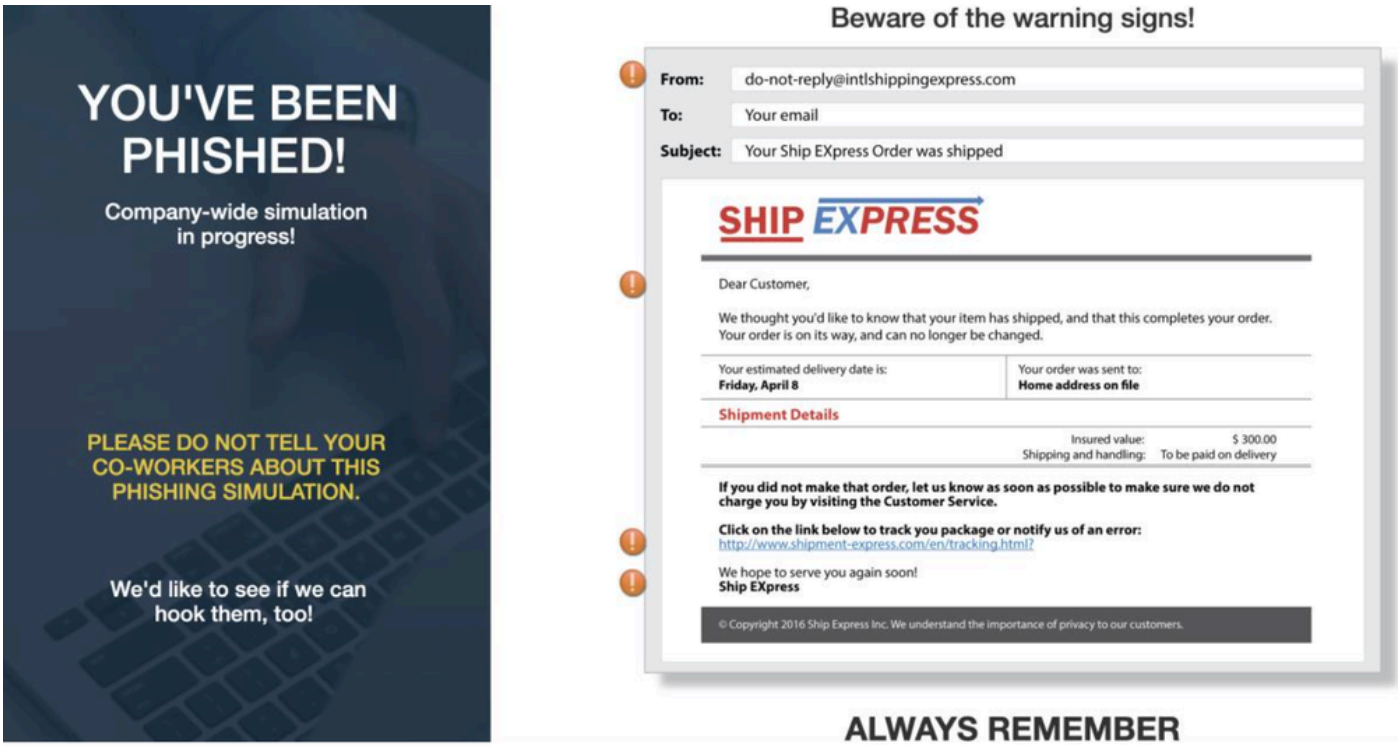
O que é visto no lado do destinatário?

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



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

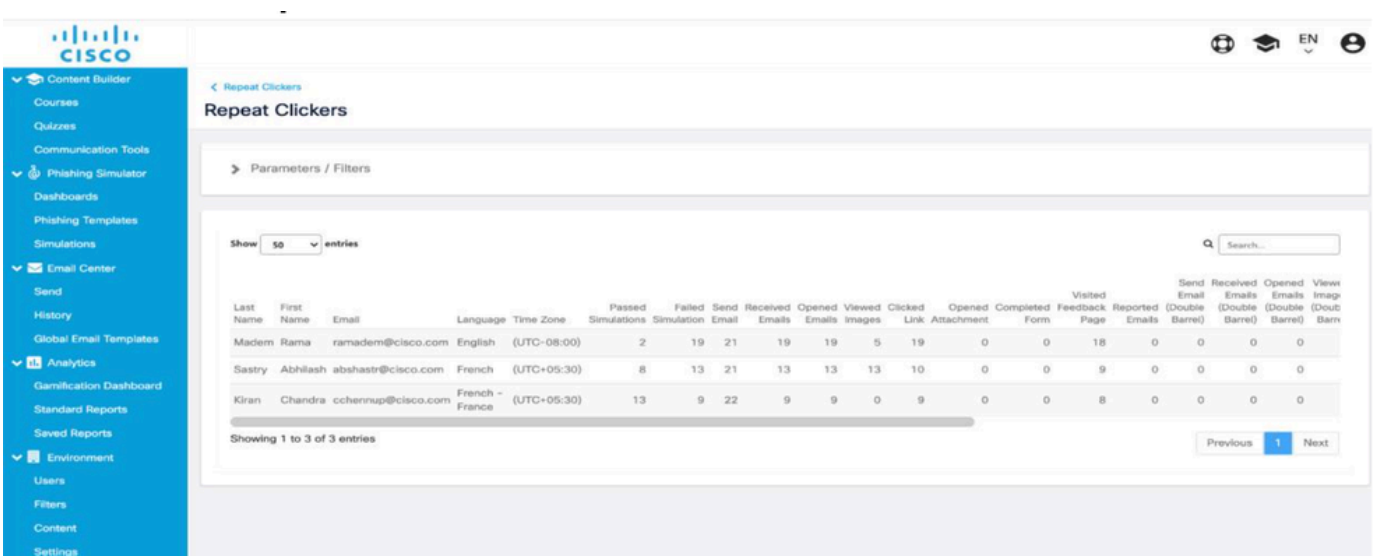
Quando o destinatário clica no URL, essa página de feedback é mostrada ao usuário e esse usuário aparece como parte da lista de Clientes Repetidos (que clicou livremente no URL do phishing) no CSA.



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

Verificar no CSA

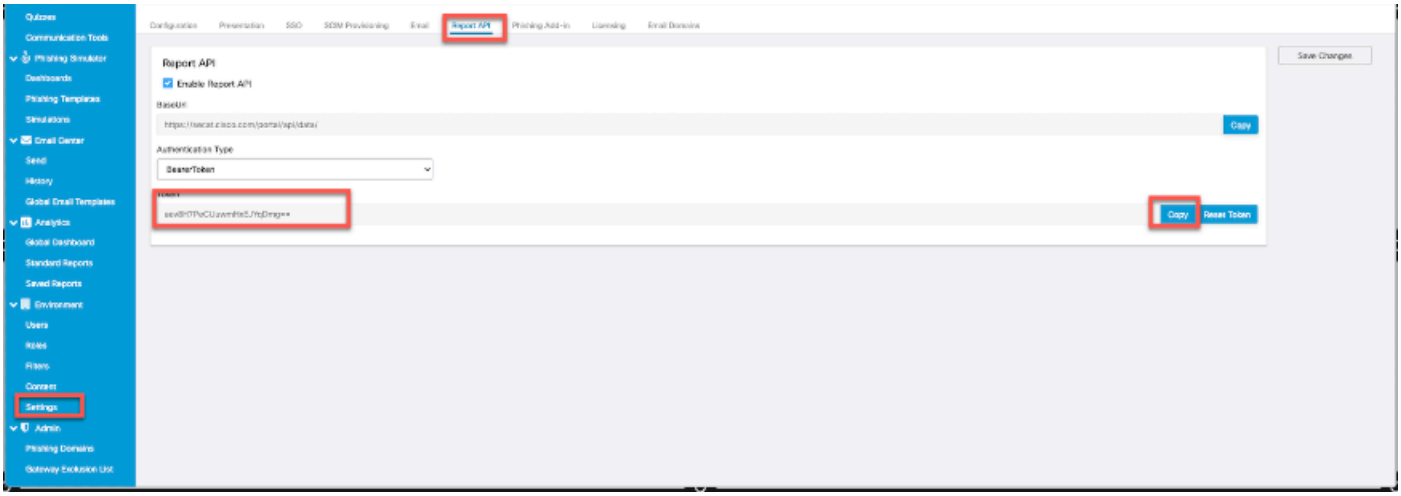
A lista Repetir cliques é exibida emAnalytics > Standard Reports > Phishing Simulations > Repeat Clickersas shown in the image.



Captura de tela da página Repetir cliques

Configurar o Secure Email Gateway

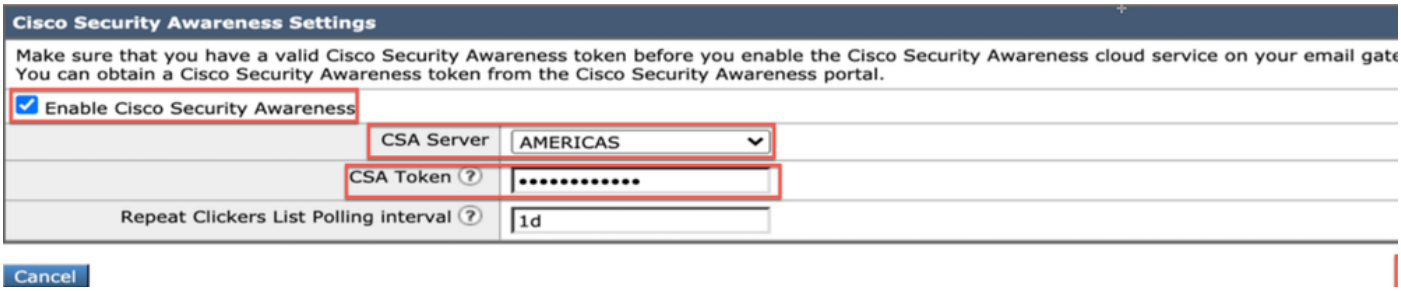
Note: Na seção Create and Send Phishing Simulations da Etapa 3 do CSA Cloud Service, quando você habilita o Report API , você anota o token do portador. Mantenha isto à mão.



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

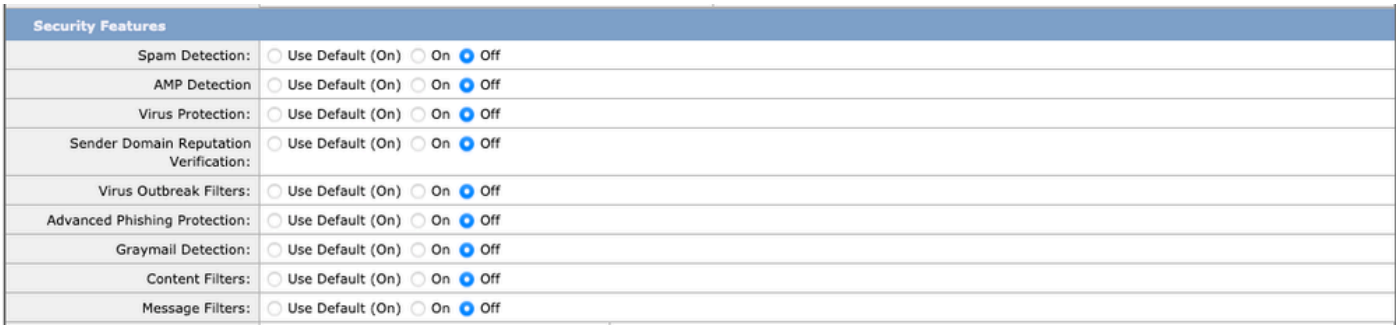
Digite csaconfig para configurar o CSA através do CLI.

```
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:	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

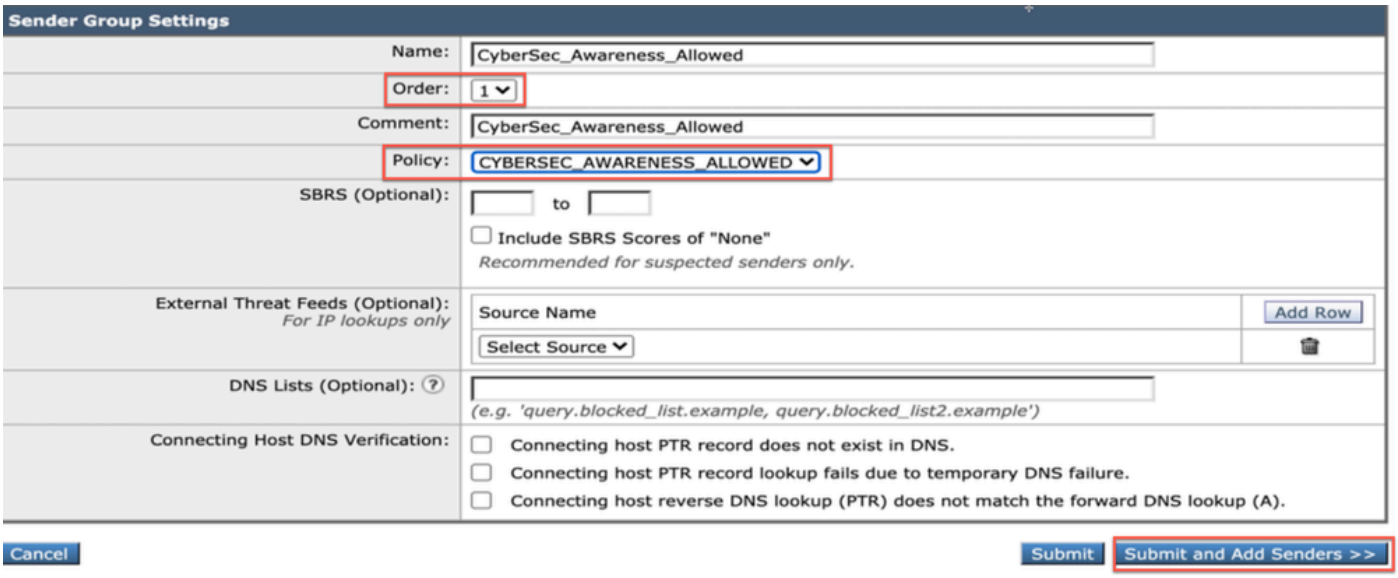
Captura de tela da política de fluxo de e-mail "CYBERSEC_AWARENESS_ALLOWED" com recursos de segurança desativados

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

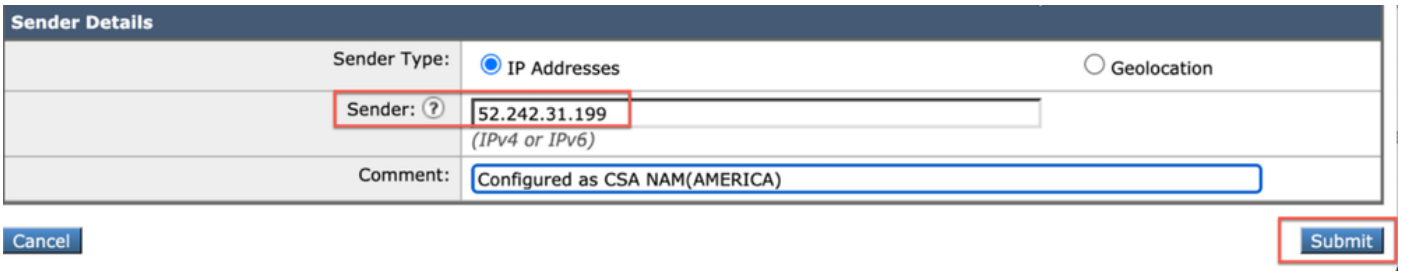
a. Crie um novo grupo de remetente e atribua a política de fluxo CYBERSEC_AWARENESS_ALLOWED de e-mail. Navegue até Mail Policies > HAT Overview > Add Sender Group e selecione a políticaCYBERSEC_AWARENESS_ALLOWED, defina a ordem como 1 e, em seguida, Submit and Add Senders.

b. Adicione um remetente IP/domain ouGeo Locationde onde os emails da campanha de Phishing foram iniciados.

Navegue atéMail Polices > HAT Overview > Add Sender Group > Submit and Add Senders > Add the sender IP > SubmiteCommitalterações conforme mostrado na imagem.



Captura de tela de um grupo de remetente CyberSec_Awareness_Allowed com a política de fluxo de mensagens "CYBERSEC_AWARENESS_ALLOWED" selecionada.



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 .

CYBERSEC_AWARENESS_ALLOWED2. 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 aMoveopção 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, 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	

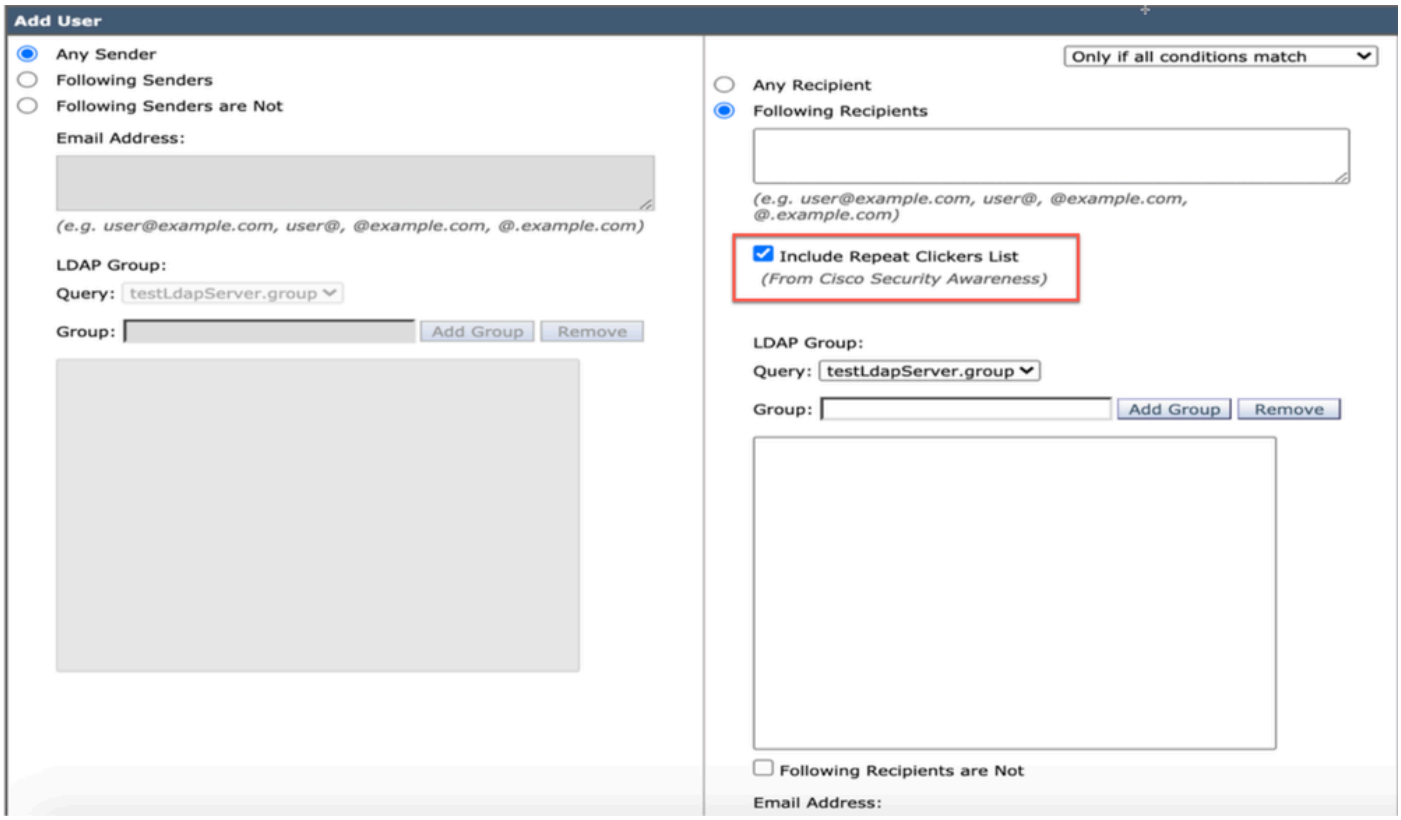
Captura de tela dos endereços IP e nomes de host das regiões CSA Americas e EU

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.



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_LISTpara 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.
```

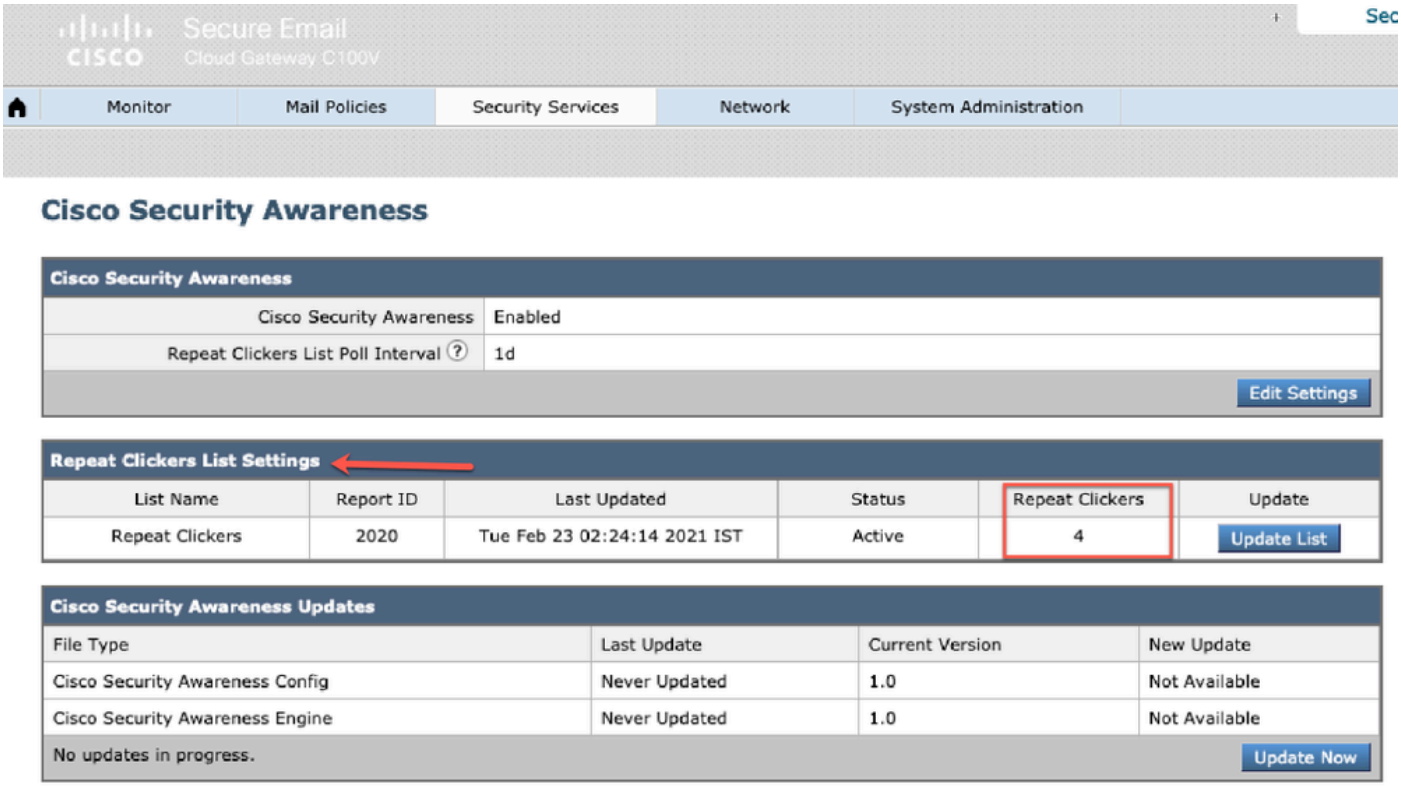
3. Localize os logs do csa para ver se a lista de cliques repetidos foi baixada ou se há um erro. Aqui está o working setup:

```
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 Awarenessconforme mostrado na imagem.



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.