配置与思科安全邮件网关的安全感知集成

目录

简介

本文档介绍配置思科安全感知(CSA)与思科安全邮件网关集成所需的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全电子邮件网关的概念和配置
- CSA云服务

使用的组件

本文档中的信息基于AsyncOS for SEG 14.0及更高版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

从CSA云服务创建和发送网络钓鱼模拟

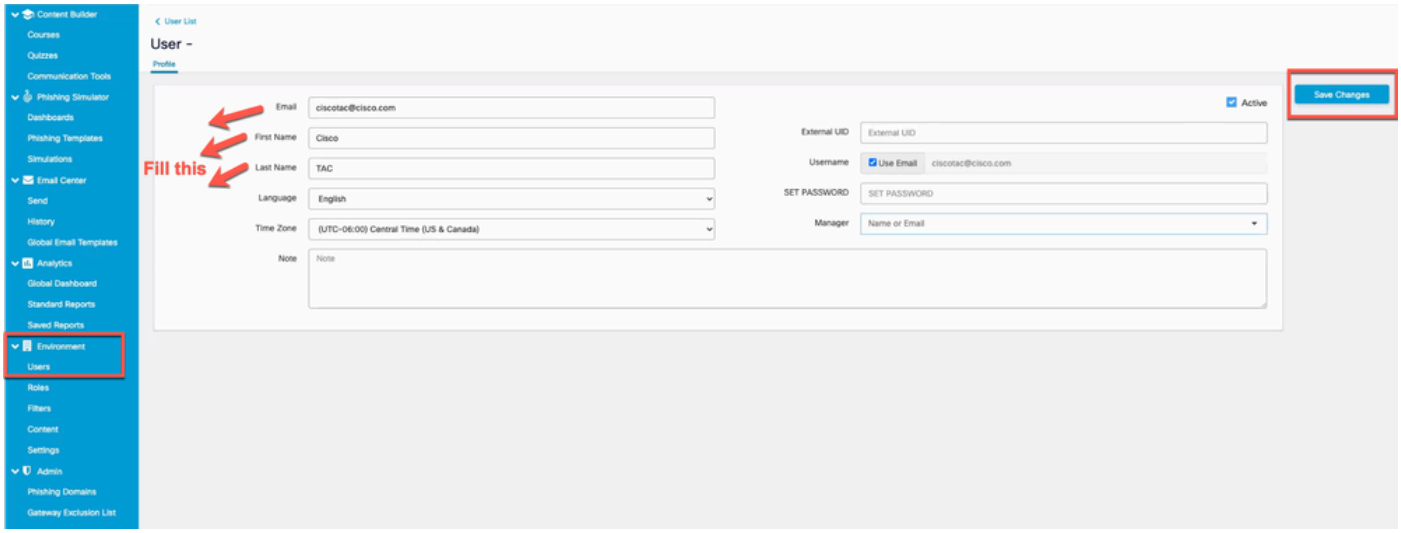
步骤1.登录CSA云服务

请参阅：
1. https://secat.cisco.com/（美洲地区）

2.欧洲地区的https://secat-eu.cisco.com/

步骤2.创建网络钓鱼邮件收件人

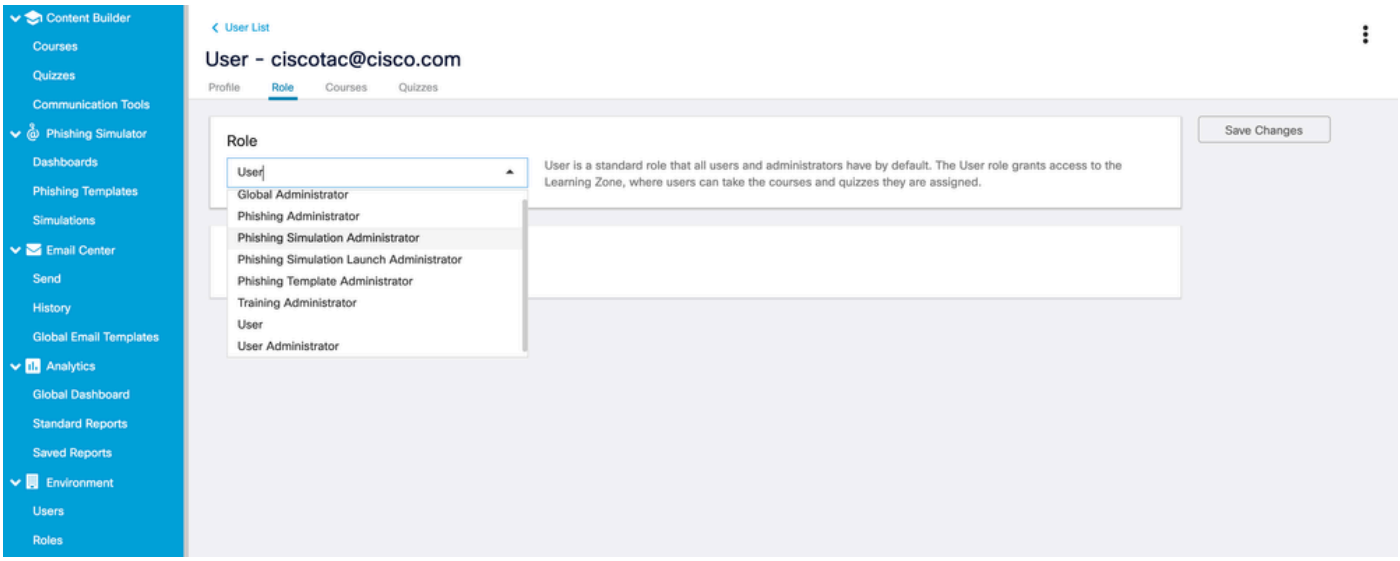
导航至**Environment > Users > Add New User**并填写“电子邮件”、“名字”、“姓氏”和“语言”字段，然后点**Save Changes**击（如图所示）。



用于添加新用户的用户界面页面的截图

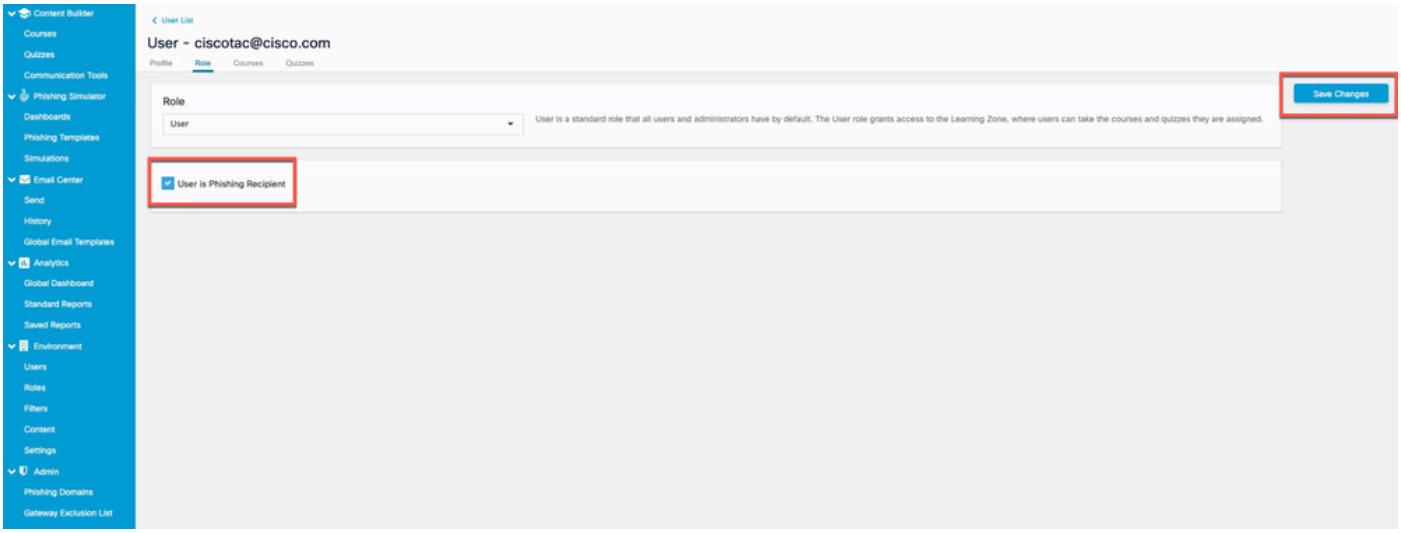
注意：只需为有权创建和启动模拟的CSA管理员用户设置密码。

创建用户后，即可选择用户的角色。您可以从下拉列表中选择角色，如下图所示：



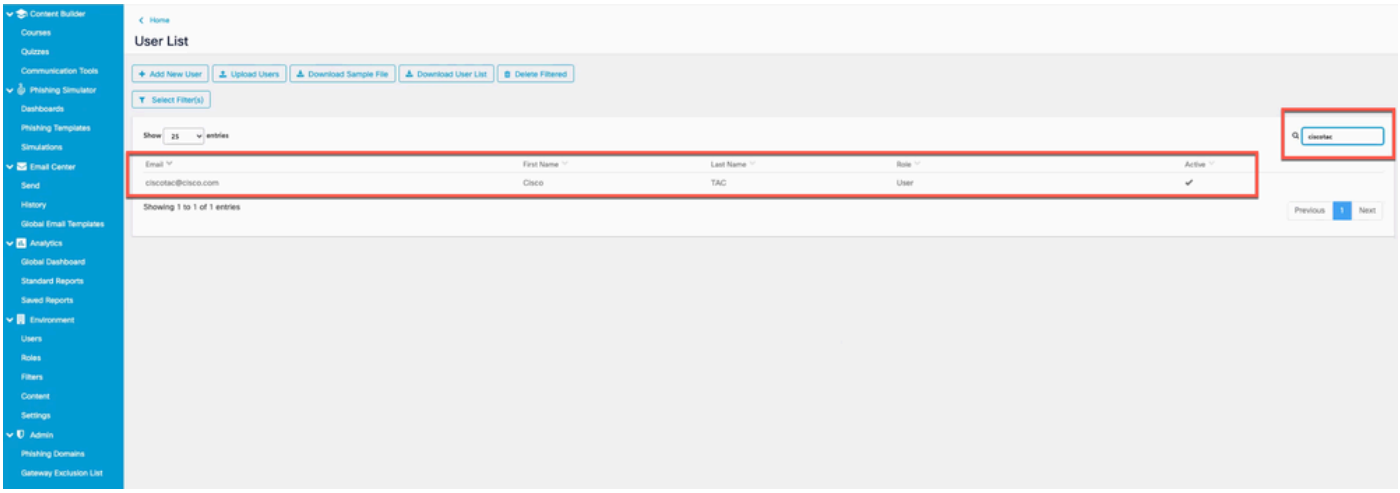
用户角色下拉选项视图

选择复User is Phishing Recipient > Save Changes选框，如图所示。



屏幕截图显示“User is Phishing Recipient”复选框已启用

确认已成功添加用户，并在根据过滤器中的邮件地址搜索时列出，如图所示。

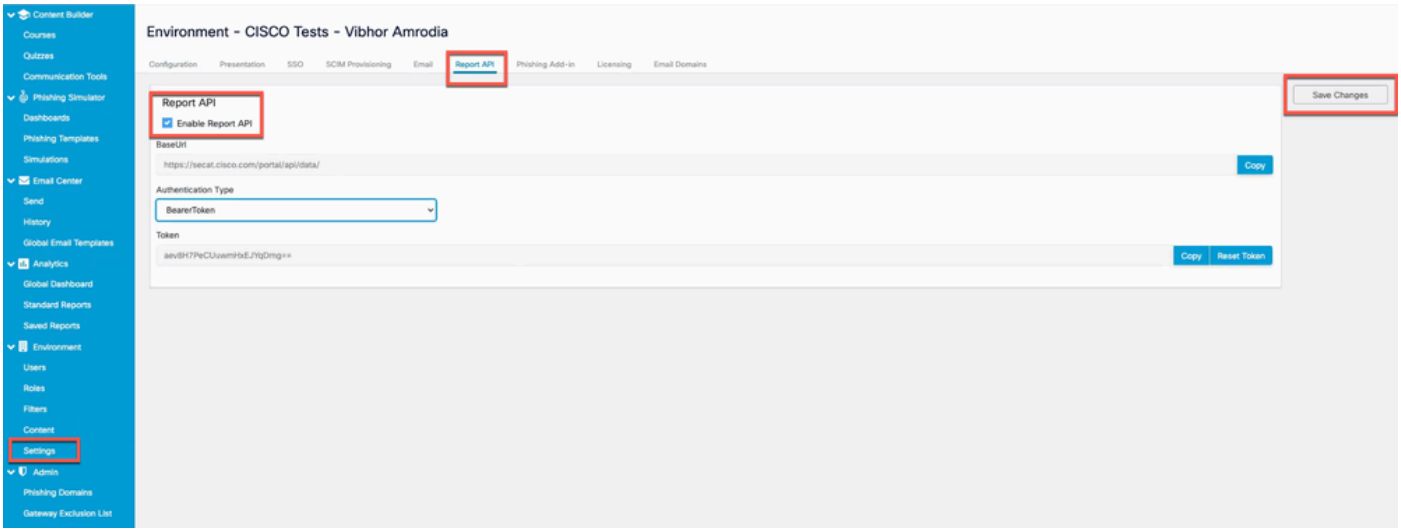


用户列表中新用户的截图

步骤3.启用报告API

导航到Environments > Settings > Report API 选项卡并选中Enable Report API > Save Changes 。

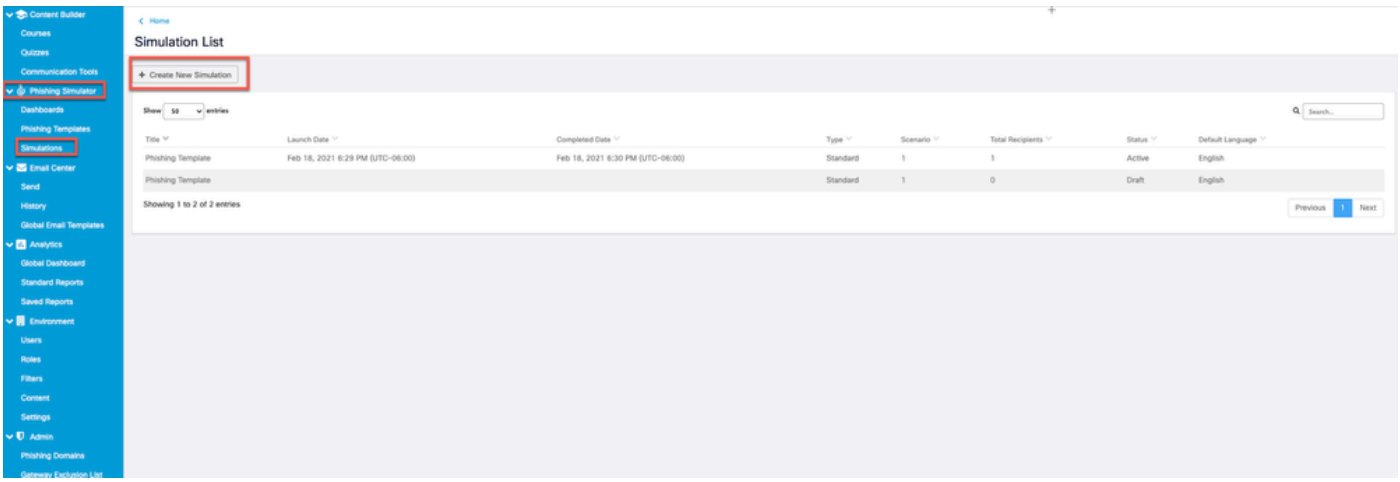
注意：记下承载令牌。您需要此操作才能将SEG与CSA集成。



屏幕截图显示“启用报告API”复选框已启用。

步骤4.创建网络钓鱼模拟

a.导航到Phishing Simulator > Simulations > Create New Simulation 可用列表Template ，并从列表中选择一个选项，如图所示。

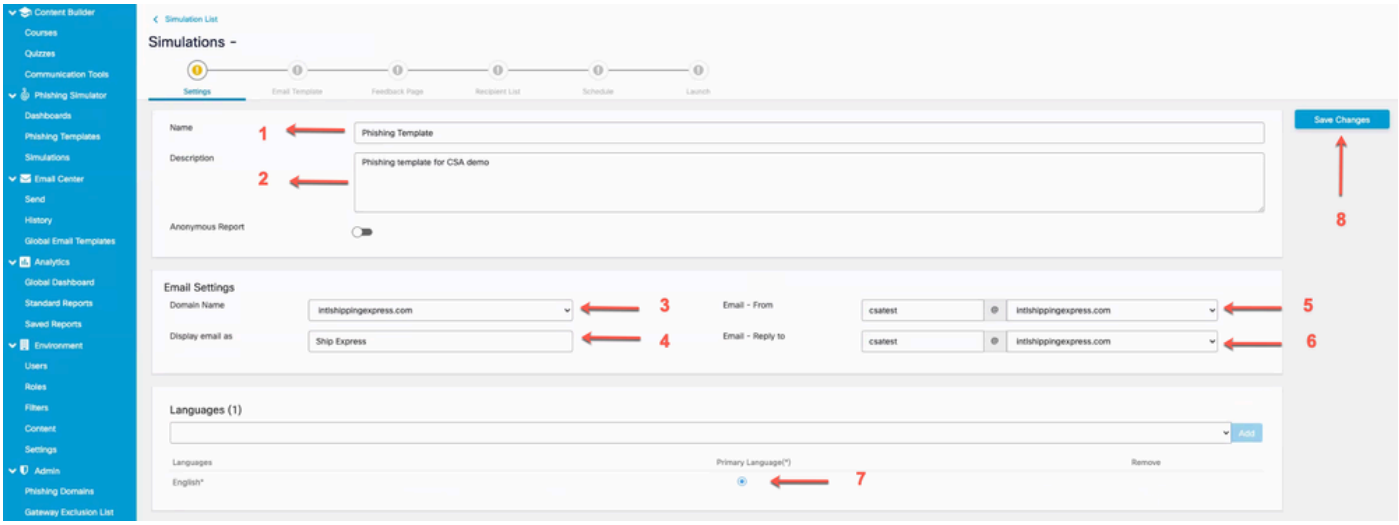


屏幕截图突出显示“创建新模拟”按钮

b.填写以下信息：

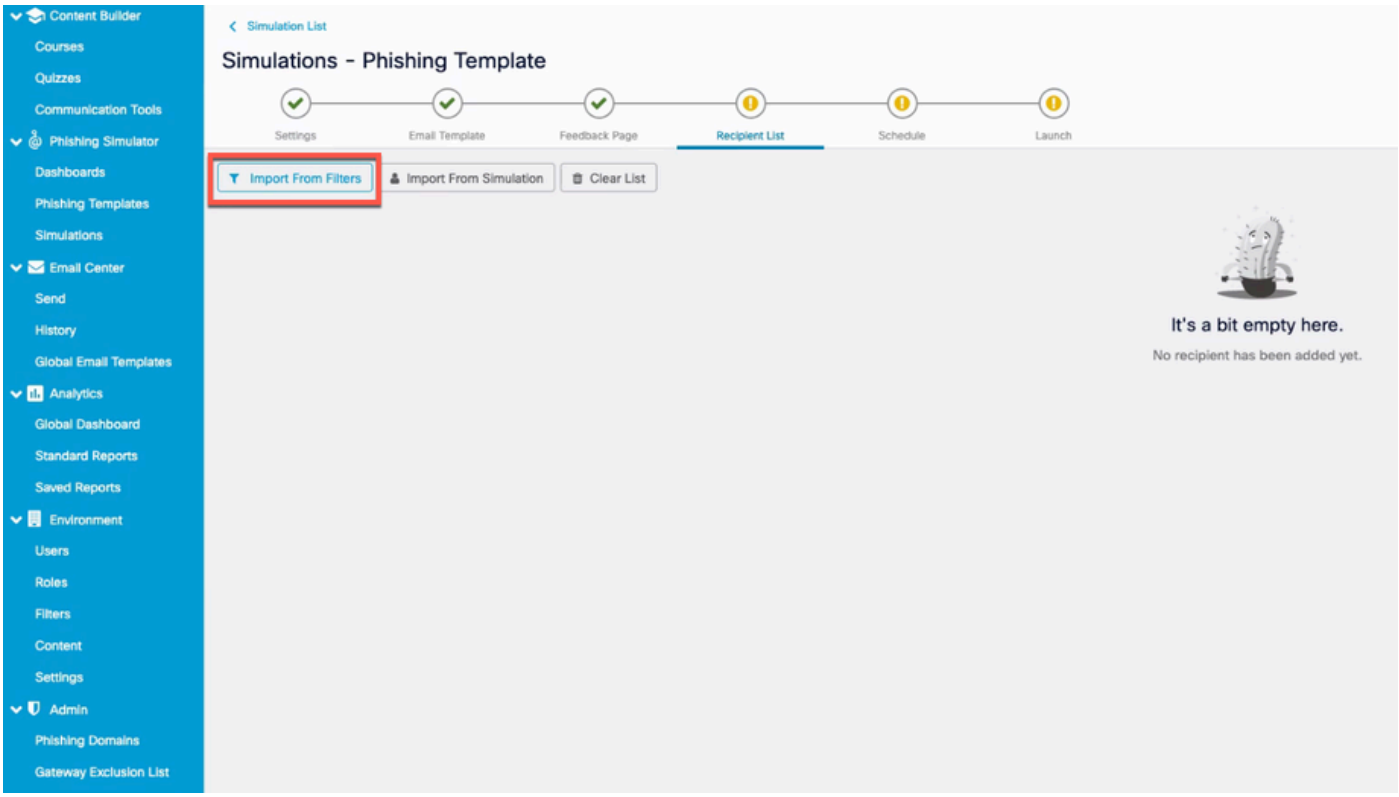
1. 选择模板的名称。
2. 描述模板。
3. 发送网络钓鱼邮件的域名。

4. 网络钓鱼邮件的显示名称。
5. 邮件发件人地址（从下拉列表中选择）。
6. 回复地址（从下拉列表中选择）。
7. 选择 Language。
8. 保存更改。



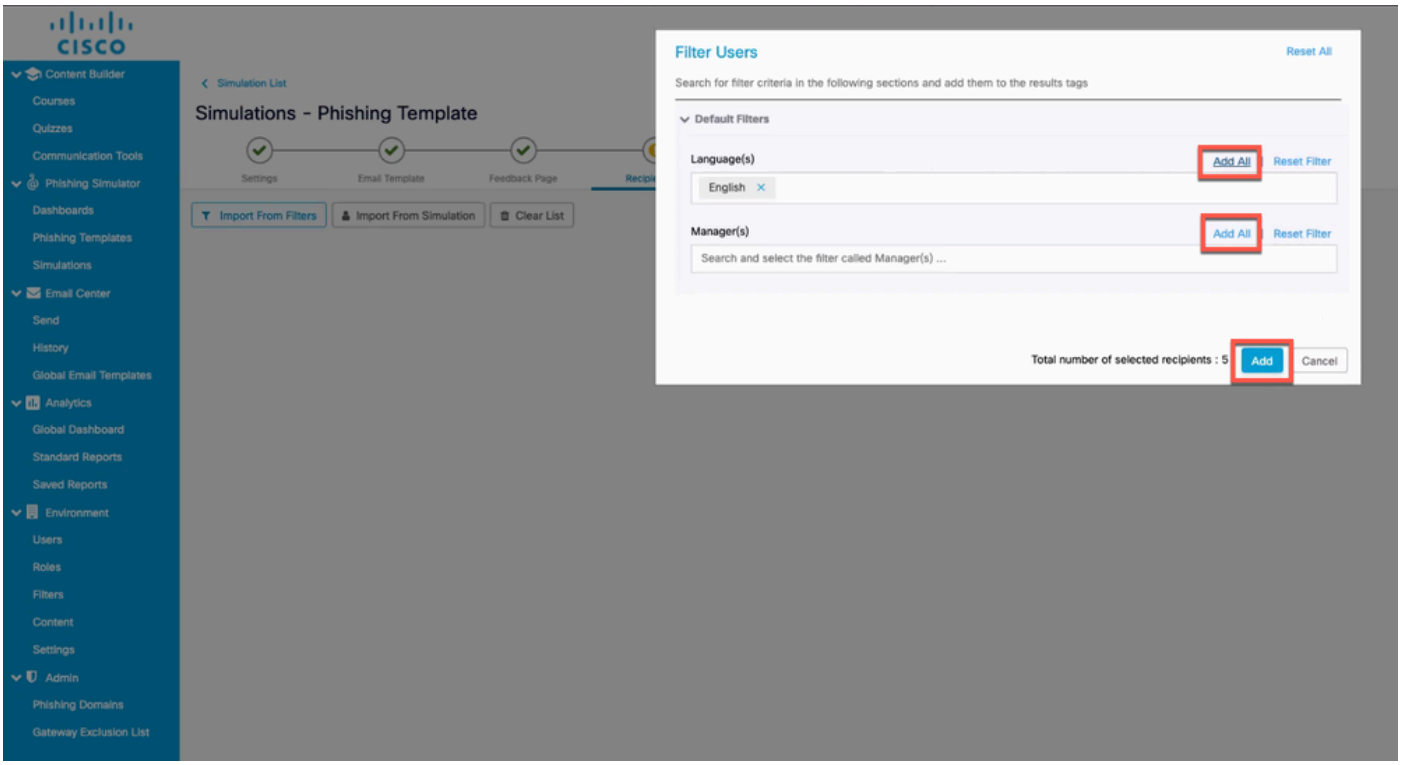
屏幕截图突出显示需要填充到配置新模拟中的字段

c.点击并Import from Filters 将网络钓鱼邮件收件人Recipient List添加到中，如图所示。



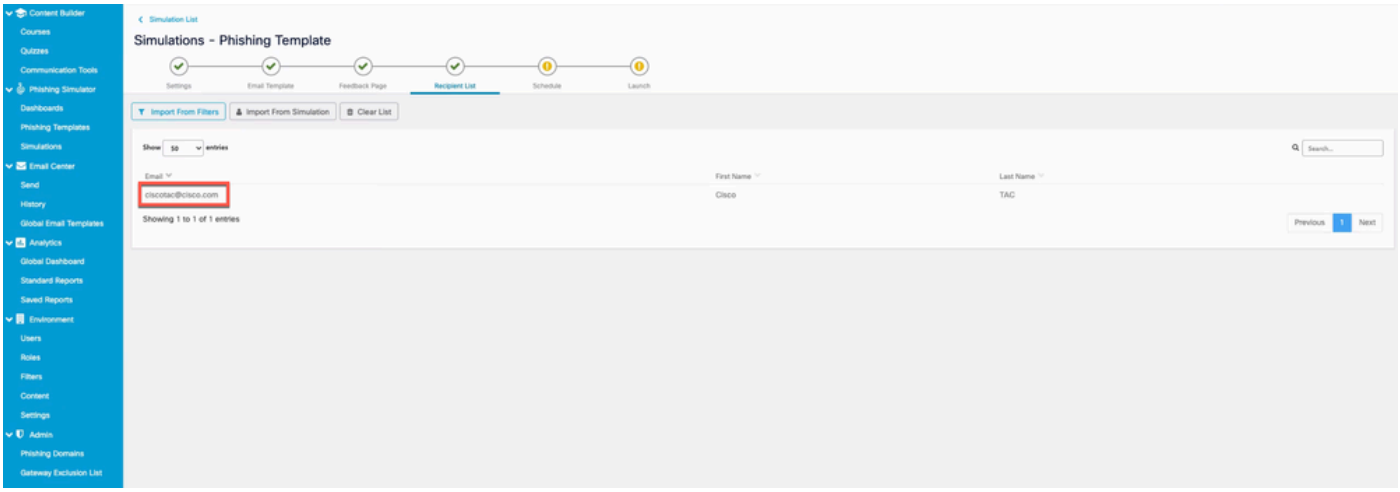
突出显示“从过滤器导入”按钮的屏幕截图

您可以按语言或管理员过滤用户。单击Add 如图所示。



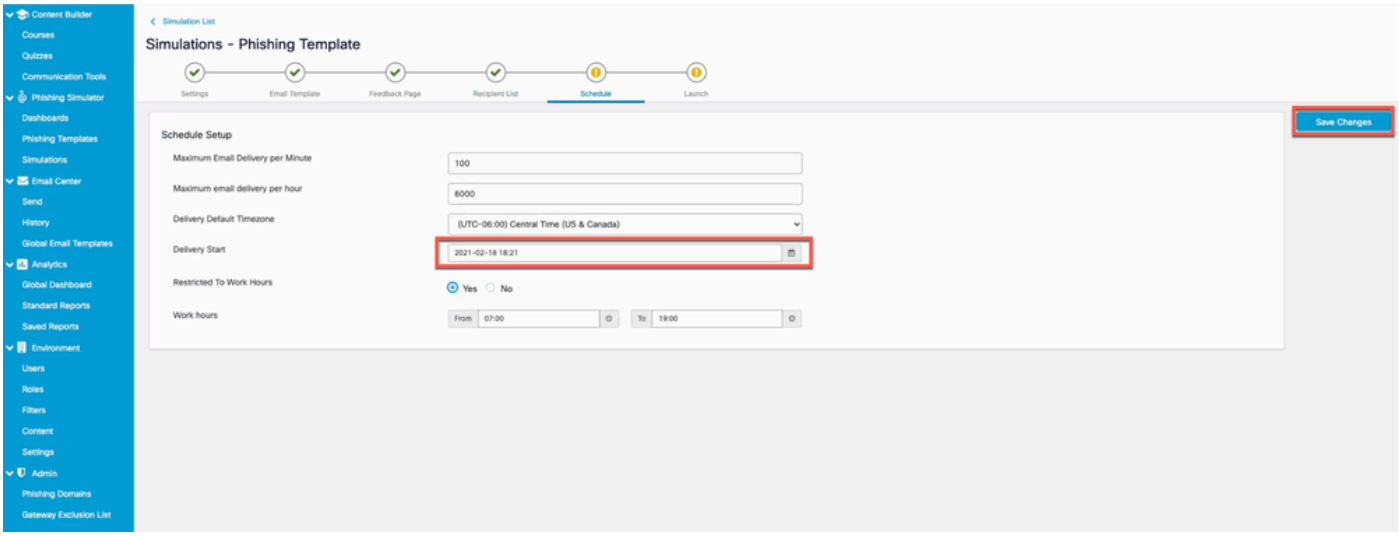
用于按语言或管理器过滤的“过滤用户”对话框的截图

以下是在步骤2中创建的用户示例，该用户现在已添加到收件人列表，如图所示。



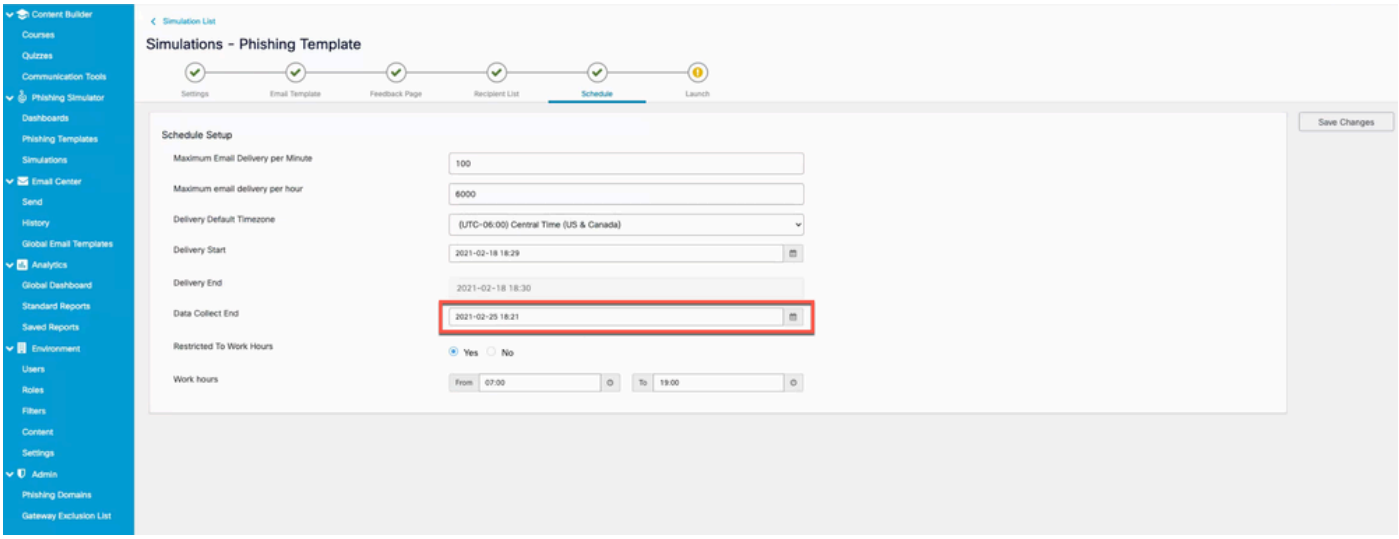
之前创建的用户的屏幕截图，该用户被列为网络钓鱼模拟的收件人

d.设置Delivery Start日期和Save更改，以计划市场活动，如图所示。



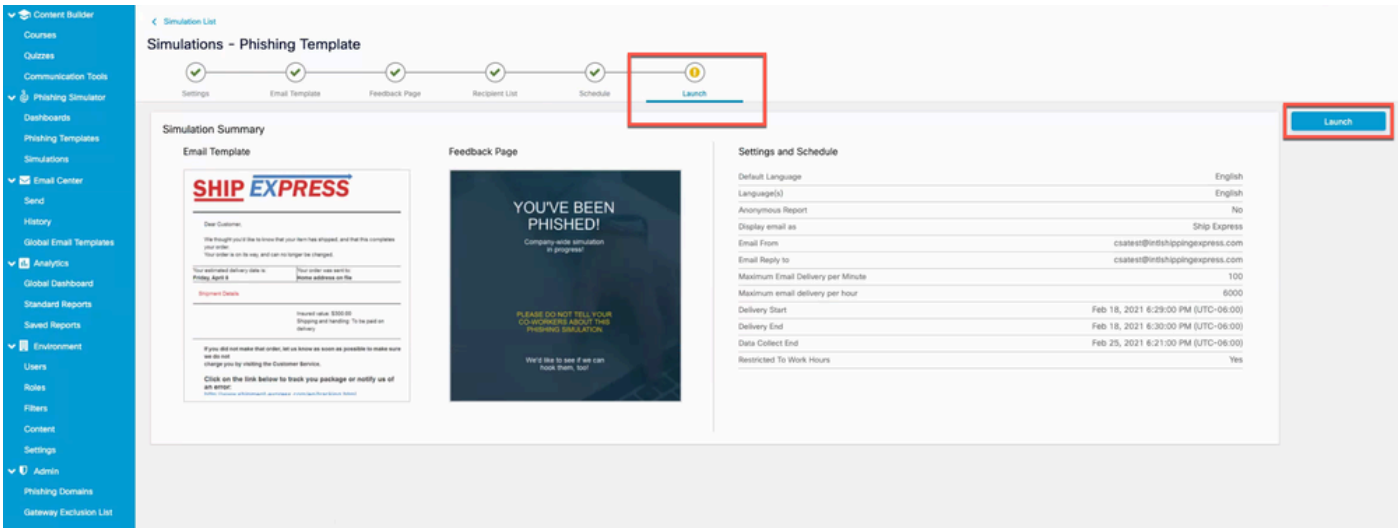
突出显示“传送开始”字段的屏幕截图

选择开始日期后，将启用为市场活end date 动选择项目的选项，如图所示。



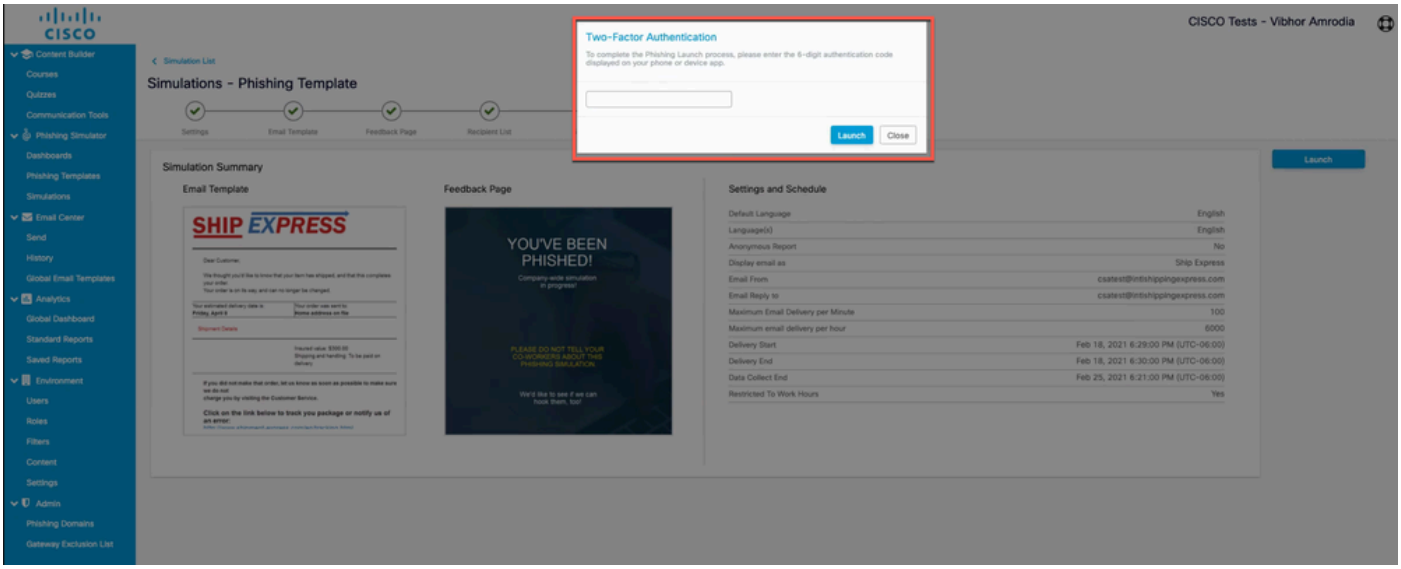
突出显示指定模拟何时结束的Data Collection End字段的截图

e.点击Launch 启动活动，如图所示。



可启动活动的模拟创建向导的最终选项卡的截图

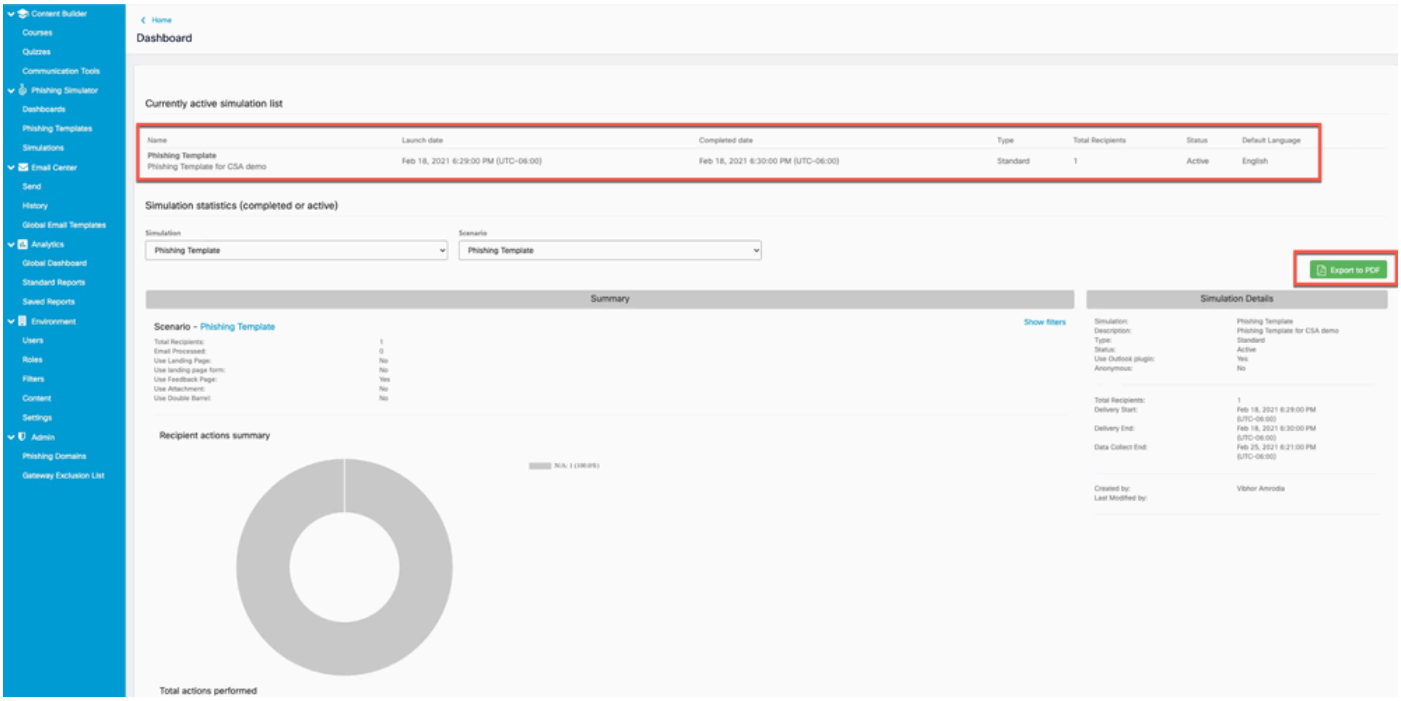
点击启动按钮后，可请求双因素身份验证代码。输入代码，然后点Launch击，如图所示。



请求双因素身份验证代码的弹出窗口截图

步骤5.主动仿真验证

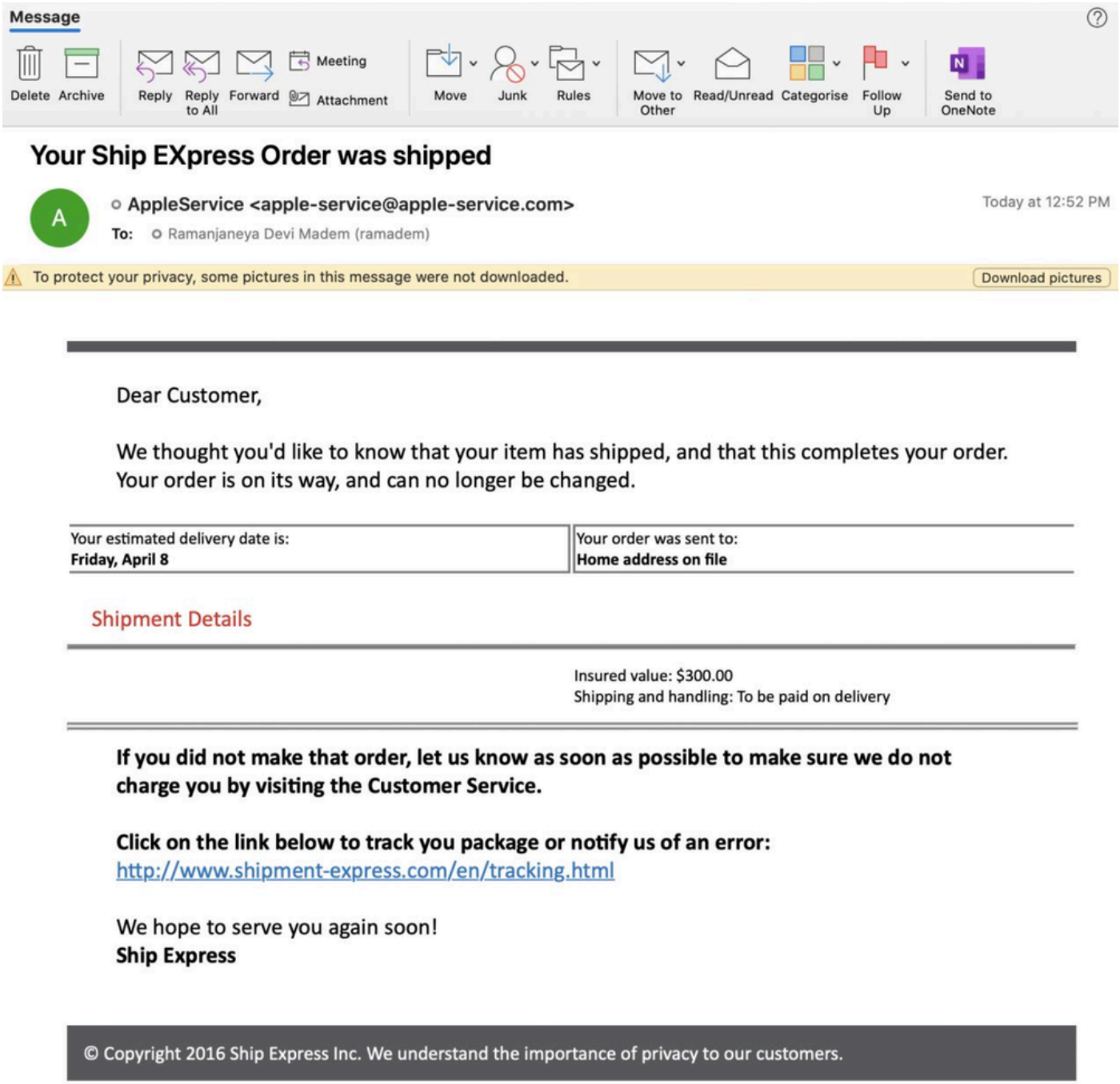
导航至。Phishing Simulator > Dashboards当前活动模拟列表提供活动模拟。您还可以单击并 Export as PDF ，获得如图所示的相同报告。



网络钓鱼模拟控制面板的截图

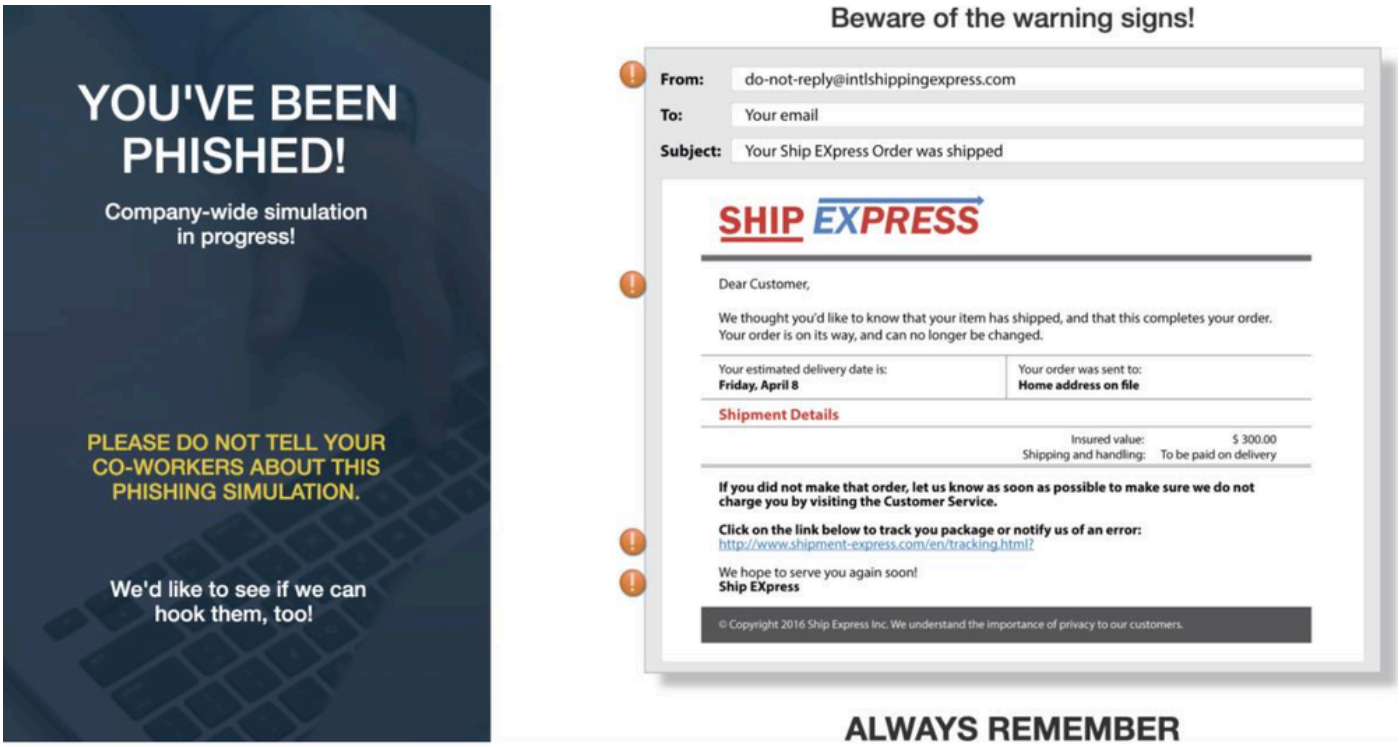
在接收方一侧看到什么？

收件人收件箱中的网络钓鱼模拟电子邮件示例。



用户邮箱中的模拟网络钓鱼邮件示例

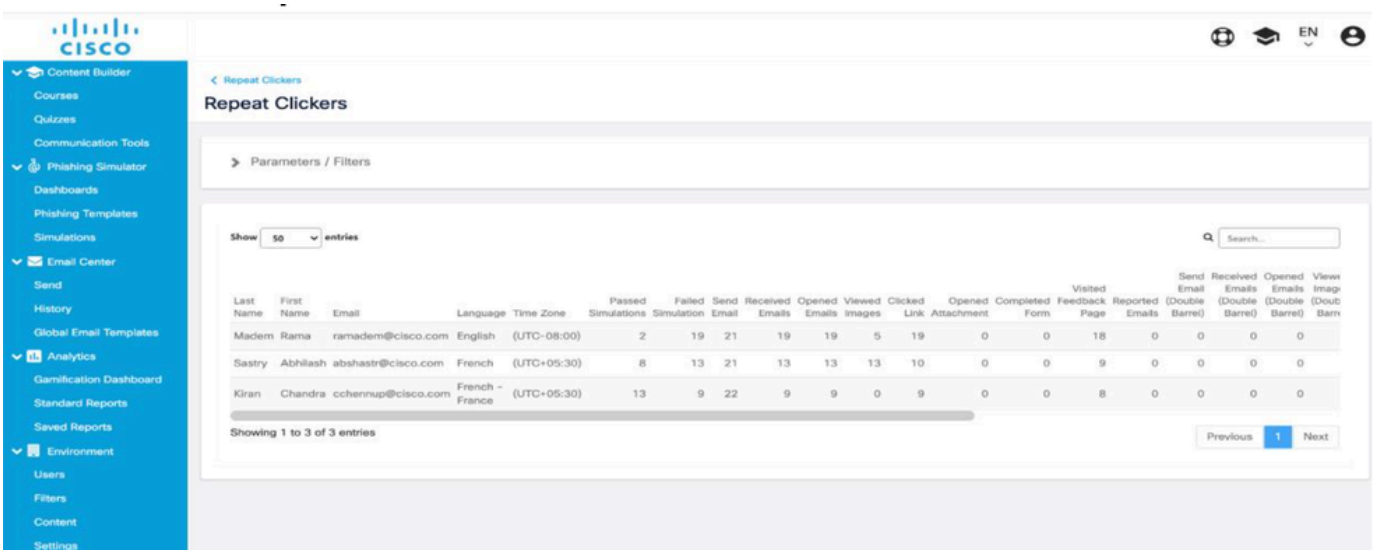
当收件人点击URL时，此反馈页面会向用户显示，并且此用户在CSA中显示为“重复点击者”(Repeat Clickers)列表（自由点击网络钓鱼URL）的一部分。



用户点击网络钓鱼邮件中的URL后看到的反馈页面示例

在CSA上验证

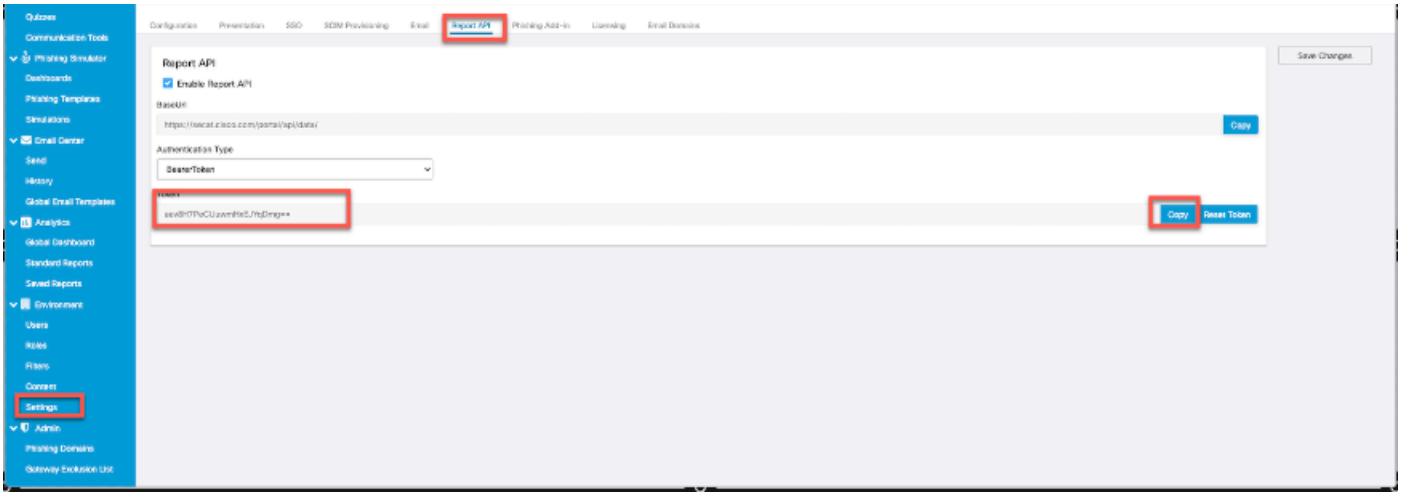
“重复点击者”列表显示在Analytics > Standard Reports > Phishing Simulations > Repeat Clickersas shown in the image.



“重复单击者”页的截图

配置安全邮件网关

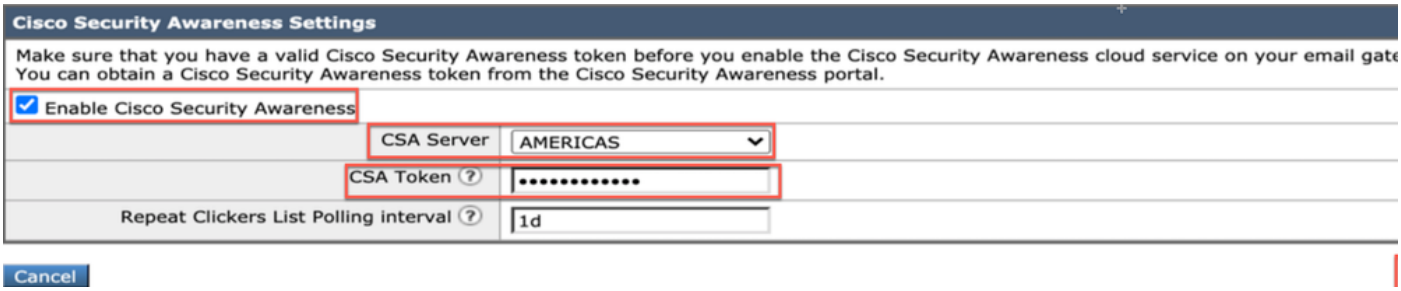
注意：Create and Send Phishing Simulations 在CSA Cloud Service Step 3(CSA云服务步骤3)部分Report API下，您记下了承载令牌。保持这个方便。



报告API下的页面截图，管理员可以在其中找到承载令牌

步骤1.在安全邮件网关中启用思科安全感知功能

在安全邮件网关GUI上，导航至Security Services > Cisco Security Awareness > Enable .“输入区域”和CSA令牌（从CSA云服务获取的承载令牌，如前文所述“备注”所示），然后提交并提交更改。



思科安全邮件网关上的思科安全感知设置页面的截图

CLI 配置

键入csaconfig ，通过CLI配置CSA。

```
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]>
```

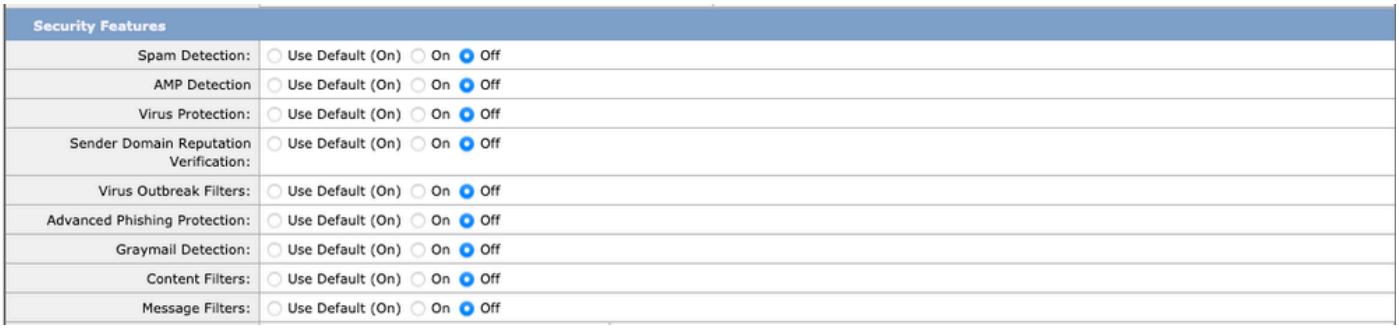
```
Please enter the CSA token for the region selected :
The CSA token should not:
- Be blank
- Have spaces between characters
- Exceed 256 characters.

Please enter the CSA token for the region selected :

Please specify the Poll Interval
[1d]>
```

步骤2.允许来自CSA云服务的模拟网络钓鱼邮件

注意：默认情况下CYBERSEC_AWARENESS_ALLOWED，系统会创建Mailflow策略，其中所有扫描引擎均设置为Off（如图所示）。



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

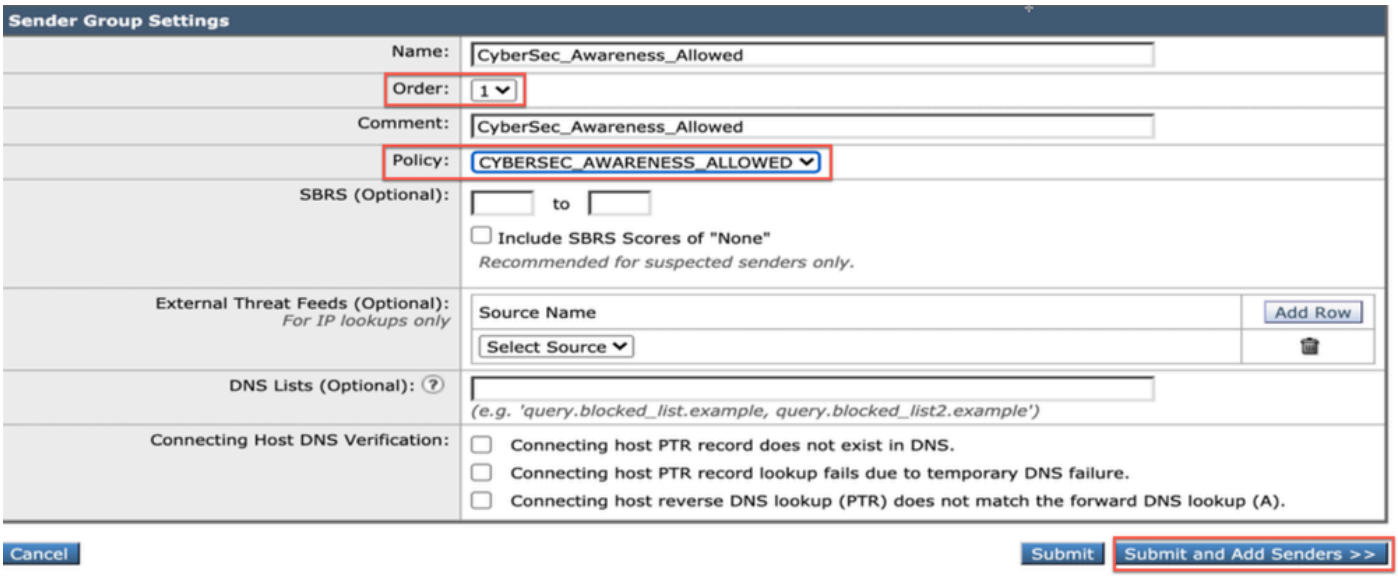
禁用安全功能的“CYBERSEC_AWARENESS_ALLOWED”邮件流策略的截图

要允许来自CSA云服务的模拟网络钓鱼活动邮件绕过安全邮件网关上的所有扫描引擎，请执行以下操作：

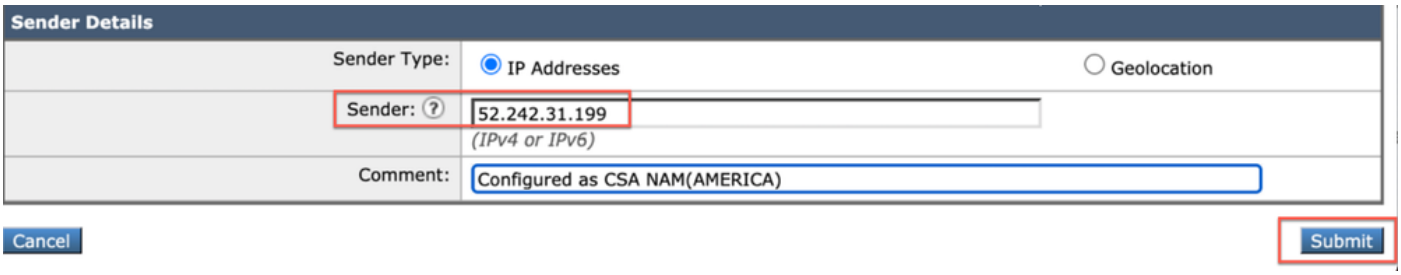
a.创建新的发件人组并分配邮件流策略CYBERSEC_AWARENESS_ALLOWED。导航至Mail Policies > HAT Overview > Add Sender Group，选择策略CYBERSEC_AWARENESS_ALLOWED，并将顺序设置为1，然后 Submit and Add Senders.

b.添加发件人IP/domain或Geo Location发起网络钓鱼活动邮件的位置。

导航至Mail Polices > HAT Overview > Add Sender Group > Submit and Add Senders > Add the sender IP > Submit并Commit更改，如图所示。



选中“CYBERSEC_AWARENESS_ALLOWED”邮件流策略的CyberSec_Awareness_Allowed发件人组的截图。



思科安全邮件网关上的思科安全感知设置页面的截图

CLI 配置：

1.导航至 listenerconfig > Edit > Inbound (PublicInterface) > HOSTACCESS > NEW > New Sender Group．

2.使用邮件策略创建一个新CYBERSEC_AWARENESS_ALLOWED的发件人组，并添加发起网络钓鱼活动邮件的发件人IP/域。

3.将新发件人组的顺序设置为1，并使用下面的Move选项 listenerconfig > EDIT > Inbound (PublicInterface) > HOSTACCESS > MOVE．

4.确认。

注意：发送方IP是CSA的IP地址，基于您选择的区域。请参考表，了解要使用的正确IP地址。在防火墙中允许这些IP地址/主机名（SEG 14.0.0-xxx的端口号为443）连接到CSA云服务。

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	

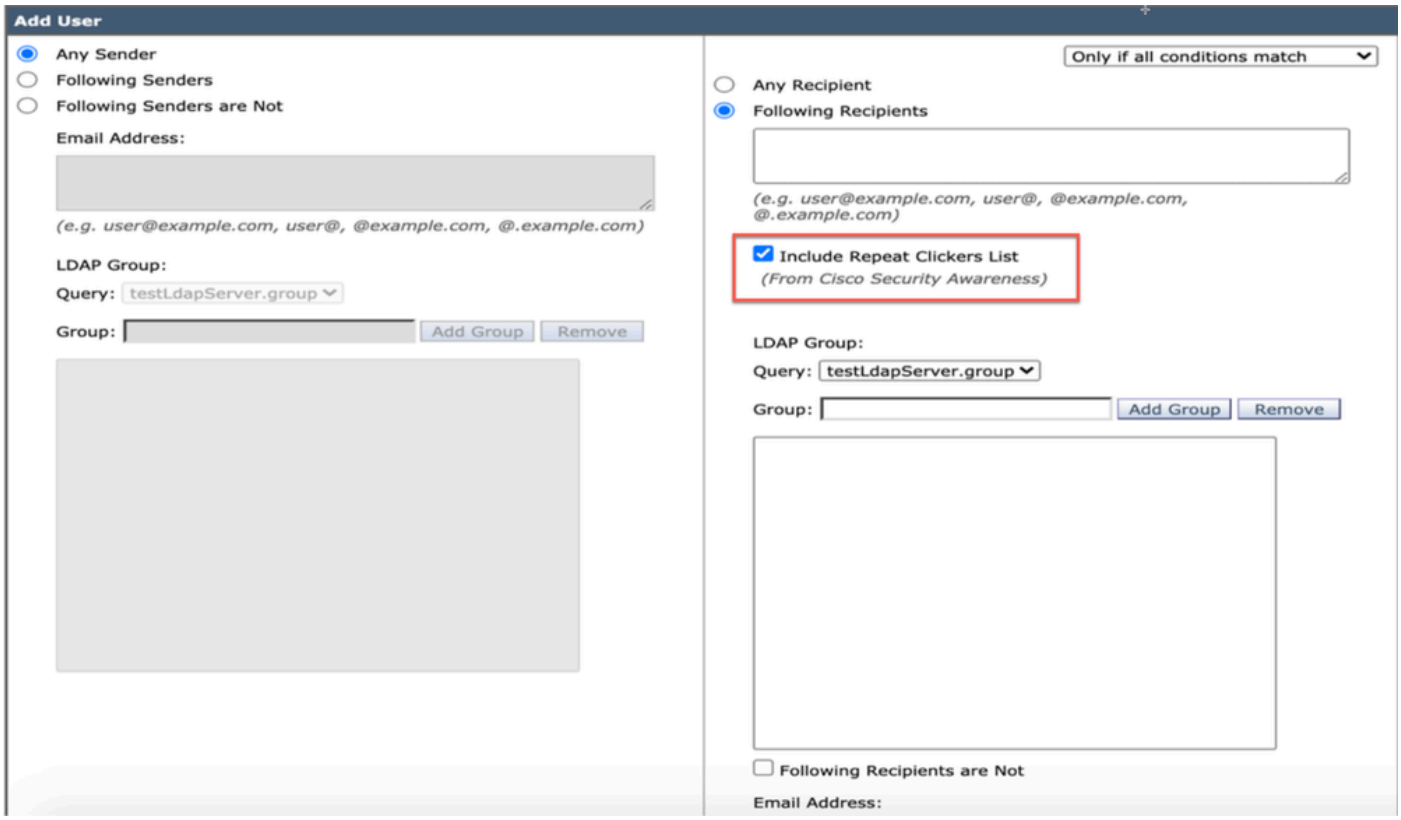
CSA美洲和欧盟地区IP地址和主机名的截图

步骤3.对SEG的Repeat Clicker采取行动

一旦网络钓鱼邮件已发送且重复点击者列表已填充在SEG中，即可创建积极的传入邮件策略，以对发送给这些特定用户的邮件执行操作。

在收件人部分创建新的主动传入自定义邮件策略Include Repeat Clickers List(Aggressive Incoming Custom Mail Policy and enable)复选框。

从GUI导航到Mail Policies > Incoming Mail Policies > Add Policy > Add User > Include Repeat Clickers List > Submit和Commit“更改”。



自定义传入邮件策略的屏幕截图，该策略配置为处理发往重复点击的邮件

故障排除指南

1.定位至csaconfig > SHOW_LIST以查看重复单击者列表的详细信息。

```
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.如果要强制更新重复单击者列表csaconfig > UPDATE_LIST ，请导航至。

```
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.
```

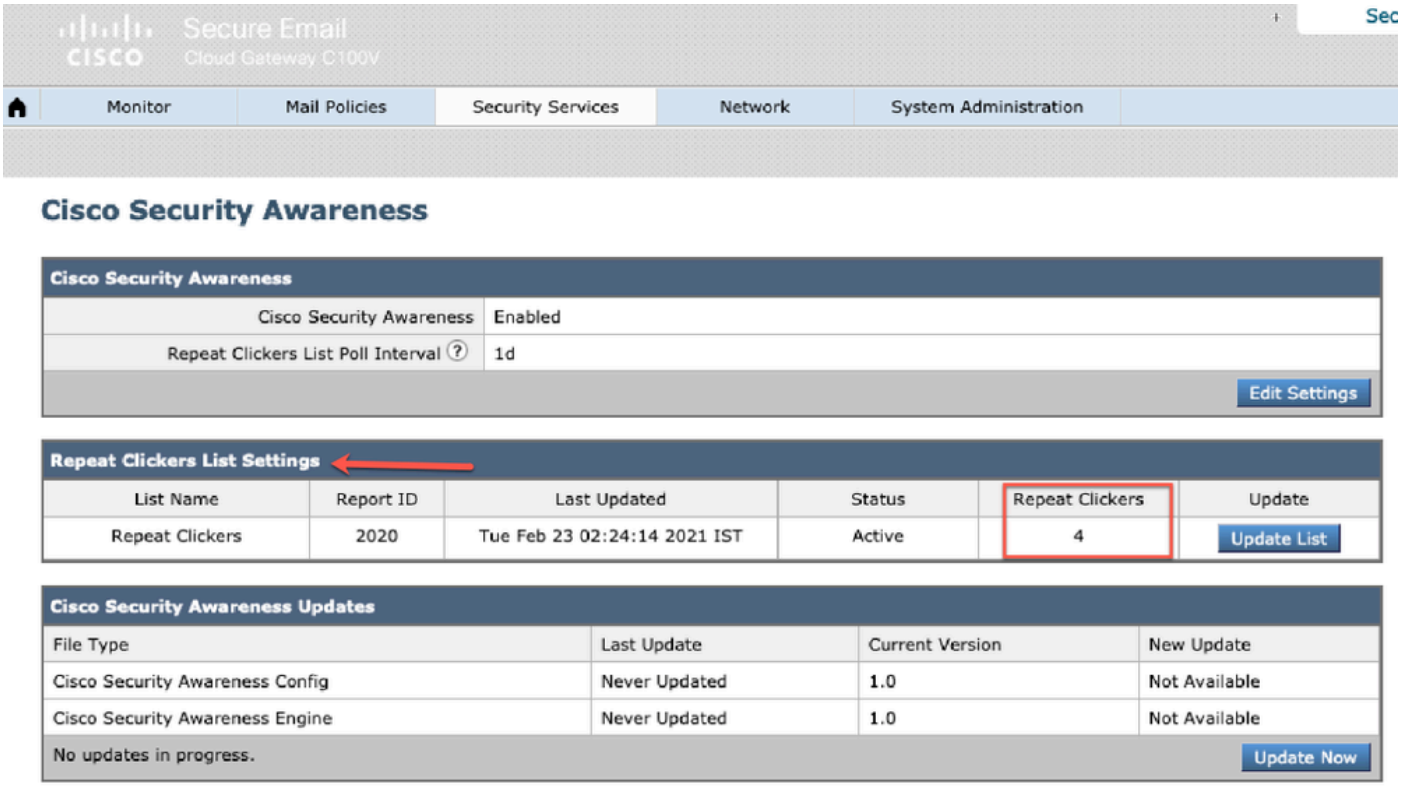
3.跟踪csa日志，查看是否已下载重复点击者列表或是否存在错误。以下是 working setup:

```
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.在GUI中也可以看到重复点击者列表的计数。导航至Security Services > Cisco Security Awareness如图所示。



“安全服务”(Security Services)>“思科安全感知”(Cisco Security Awareness)页面的截图，突出显示重复点击的数量

相关信息

- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。