# Integratie van beveiligingsbewustzijn configureren met Cisco Secure Email Gateway

## Inhoud



## Inleiding

In dit document worden de stappen beschreven die nodig zijn om de integratie van Cisco Security Awareness (CSA) met de Cisco Secure Email Gateway te configureren.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Email Gateway-concepten en -configuratie
- CSA-cloudservice

### Gebruikte componenten

De informatie in dit document is gebaseerd op AsyncOS voor SEG 14.0 en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

# Phishing-simulaties maken en verzenden vanuit CSA Cloud Service

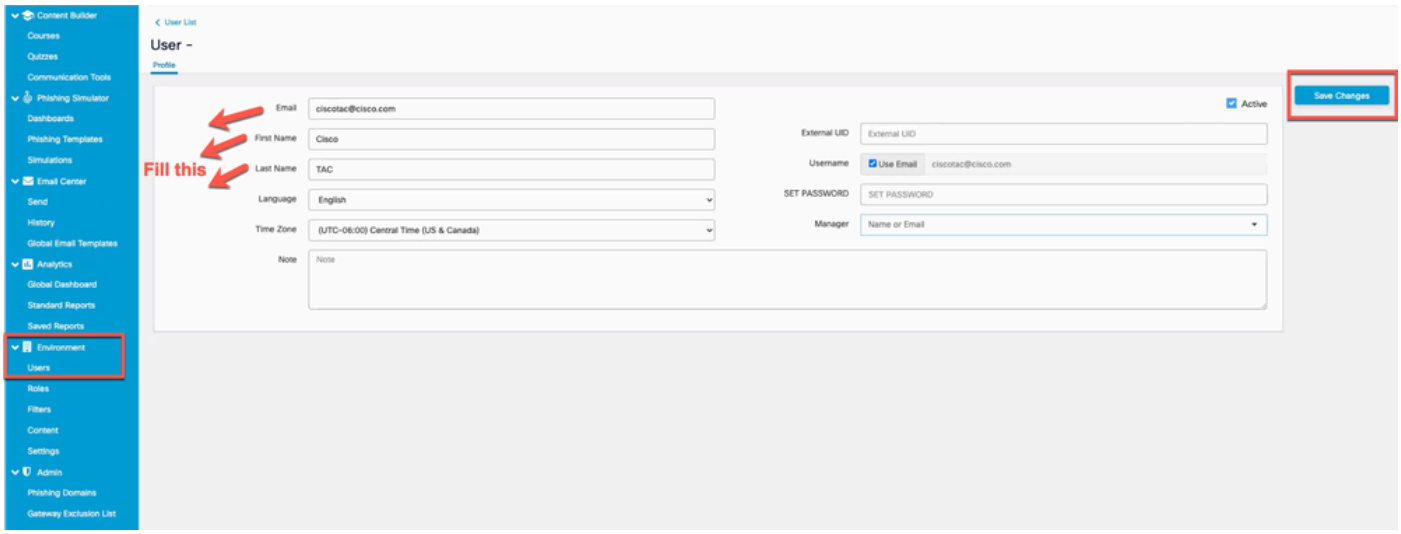
## Stap 1. Meld u aan bij CSA Cloud Service

Raadpleeg:
1. https://secat.cisco.com/ voor de regio AMERICAS

2. https://secat-eu.cisco.com/ voor de regio EUROPA

## Stap 2. Een phishing-e-mailontvanger maken

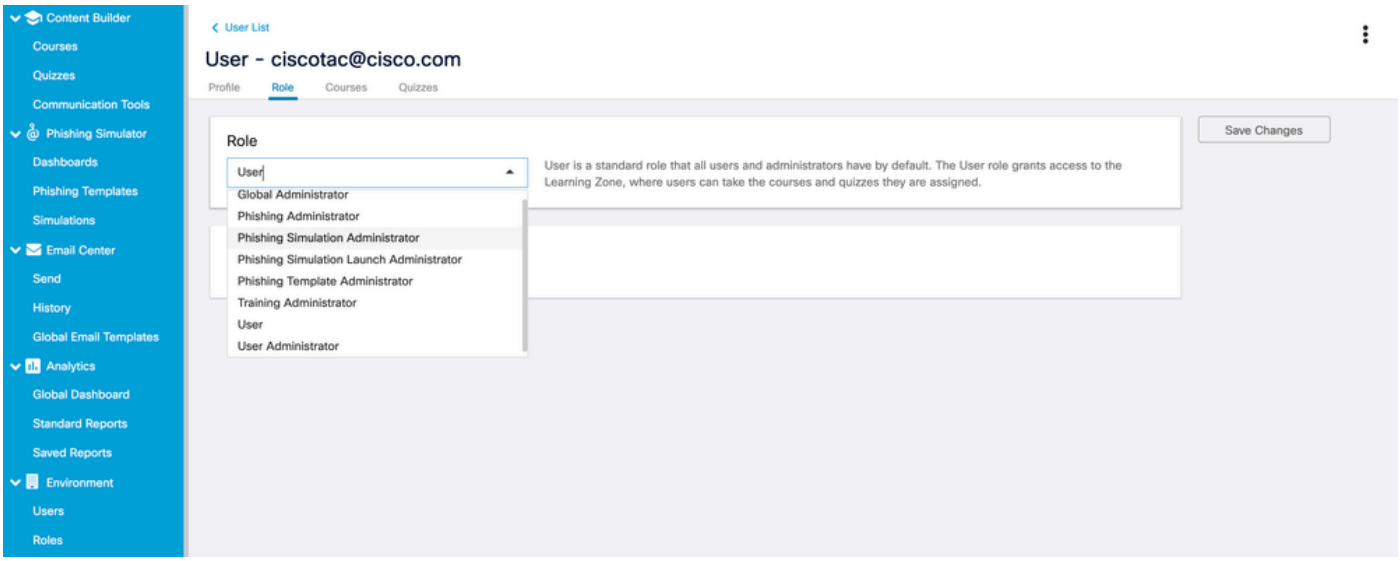
Navigeer naar **Environment** > **Users** > **Add New User** en vul de velden E-mail, Voornaam, Achternaam en Taal in en klik vervolgens op **Save Changes**zoals weergegeven in de afbeelding.




Schermafbeelding van de gebruikersinterfacepagina om nieuwe gebruiker toe te voegen

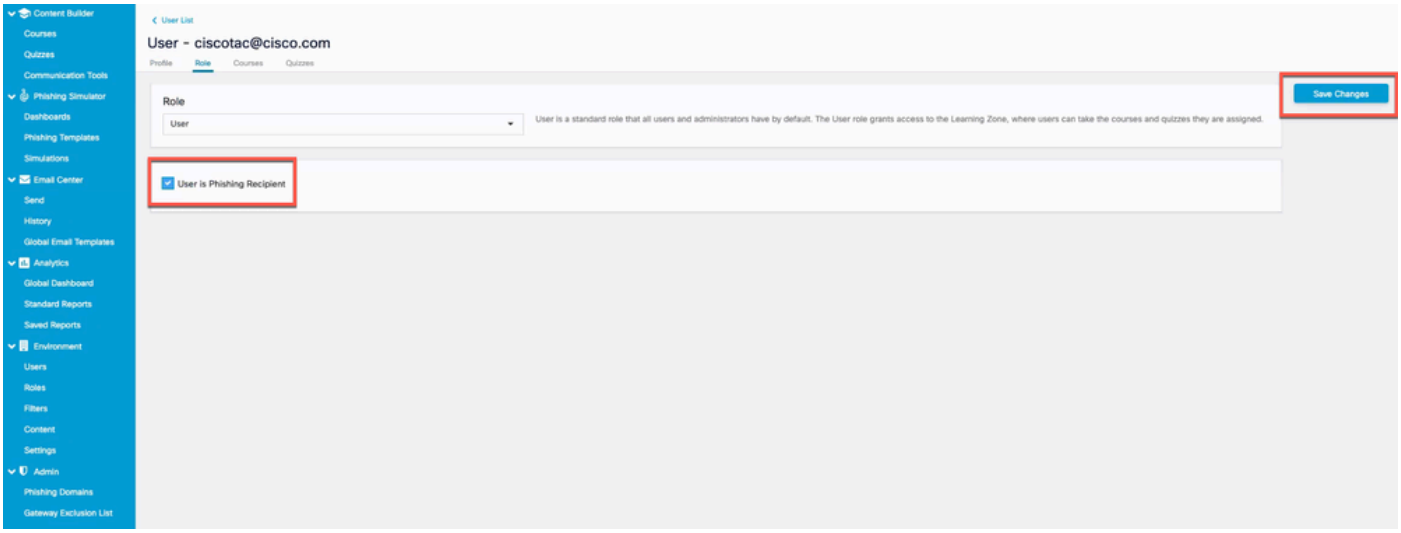
Opmerking: een wachtwoord hoeft alleen te worden ingesteld voor een CSA-beheerdersgebruiker die gemachtigd is om simulaties te maken en te starten.

De rol van de gebruiker kan worden geselecteerd zodra de gebruiker is gemaakt. U kunt de rol selecteren in de vervolgkeuzelijst zoals aangegeven in deze afbeelding:



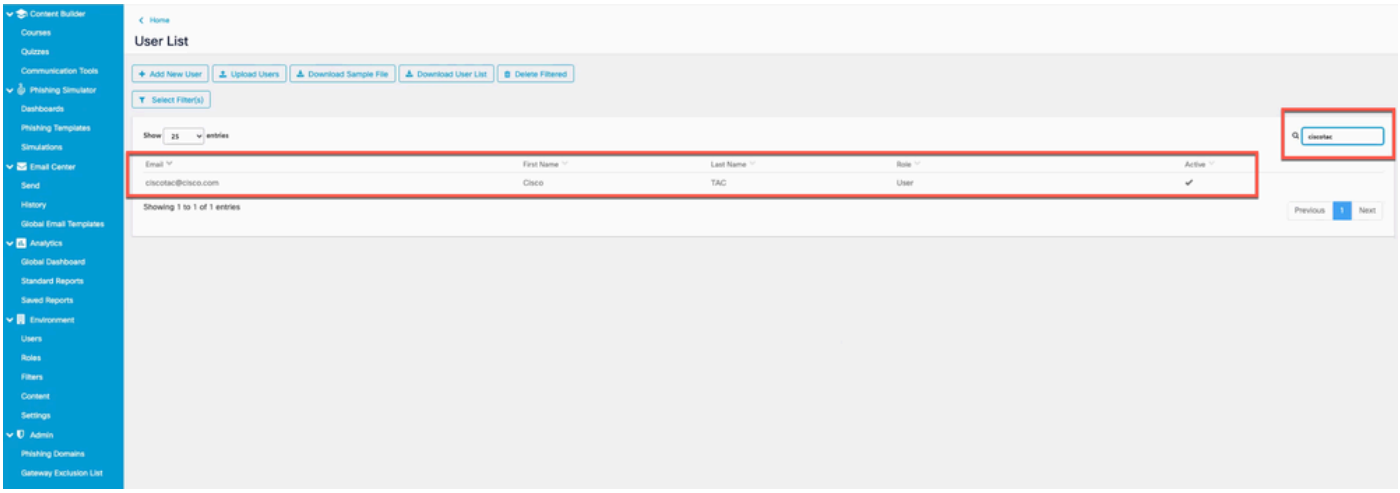

Opties voor de vervolgkeuzelijst Gebruikersrol weergeven

Schakel het User is Phishing Recipient > Save Changes selectievakje in dat in de afbeelding wordt weergegeven.




schermafbeelding met het selectievakje "Gebruiker is phishing-ontvanger" is ingeschakeld

Controleer of de gebruiker is toegevoegd en wordt vermeld wanneer wordt gezocht op basis van het e-mailadres in het filter zoals weergegeven in de afbeelding.

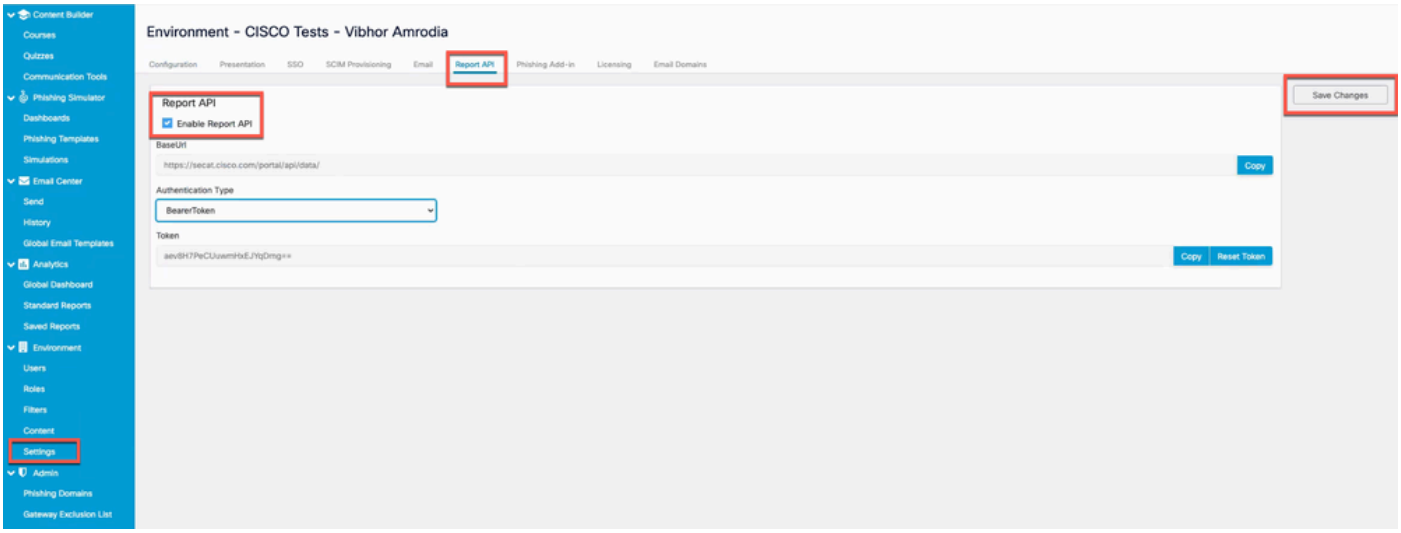


Screenshot van de nieuwe gebruiker in de gebruikerslijst

## Stap 3. Rapport-API inschakelen

Navigeer naar het Environments > Settings > Report API tabblad en controleerEnable Report API > Save Changes .

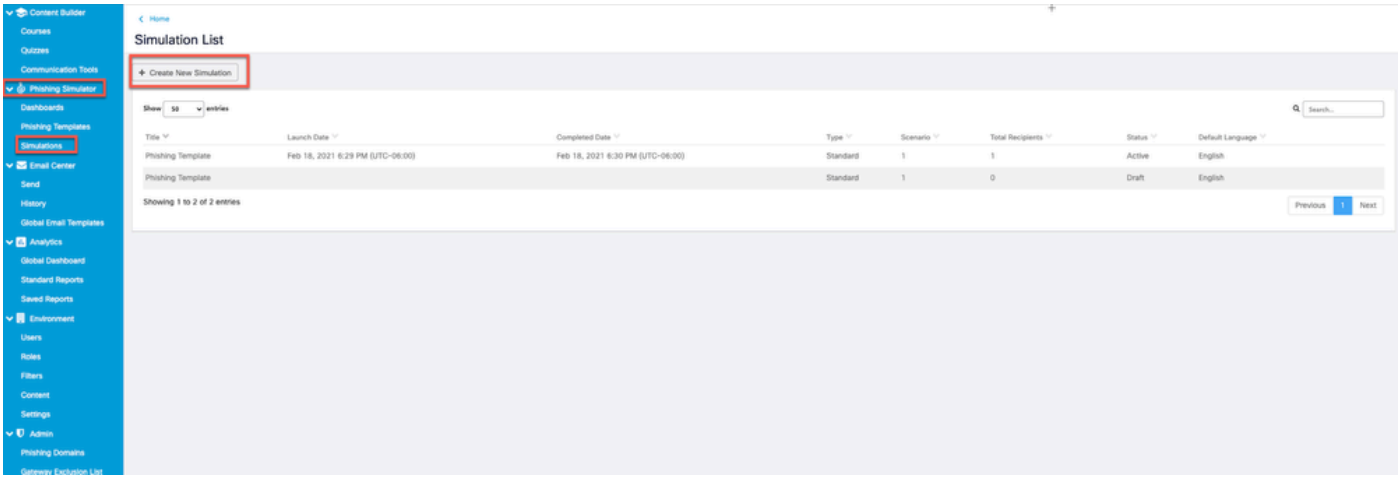
Opmerking: maak een notitie van het token aan toonder. Dit heb je nodig om de SEG te integreren met CSA.




Schermafbeelding met het selectievakje "Rapport-API inschakelen" is ingeschakeld.

## Stap 4. Phishing-simulaties maken

a. Navigeer naar Phishing Simulator > Simulations > Create New Simulation en selecteer een Template van de beschikbare lijst zoals weergegeven in de afbeelding.

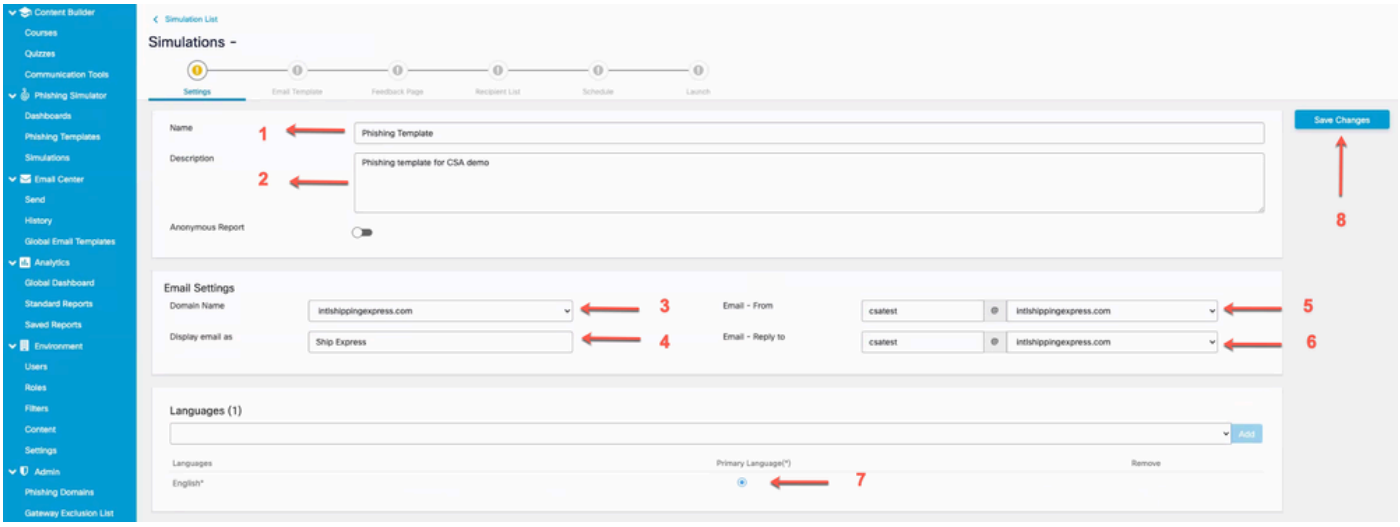



Screenshot met de knop "Nieuwe simulatie maken"

b. Vul deze informatie in:

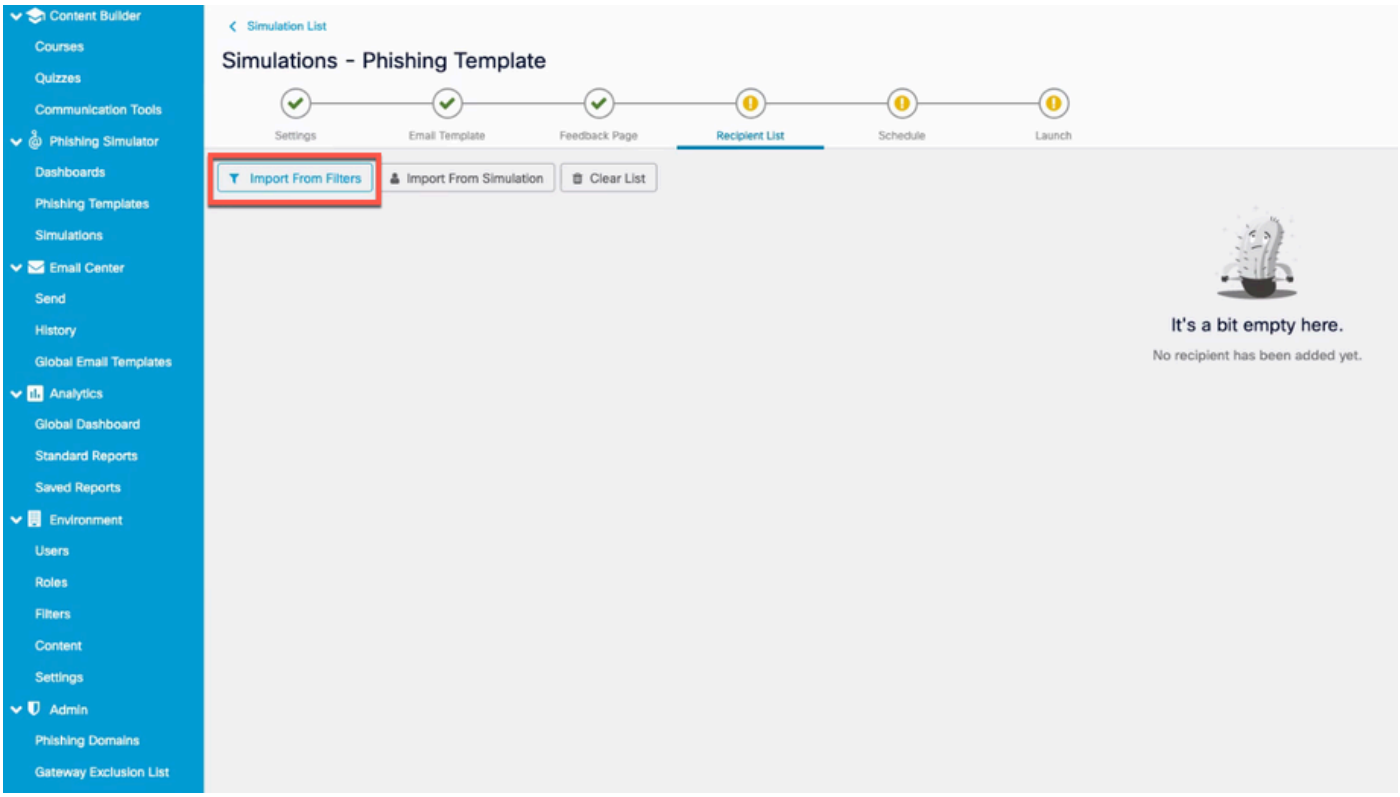
1. Selecteer een naam voor de template.

2. Beschrijf de template.
3. Domeinnaam waarmee de phishing-e-mail wordt verzonden.
4. De naam van de phishing-e-mail.
5. E-mailadres van (selecteer uit dropdown).
6. Antwoord-naar-adres (selecteer uit dropdown).
7. Selecteer de taal.
8. Wijzigingen opslaan.



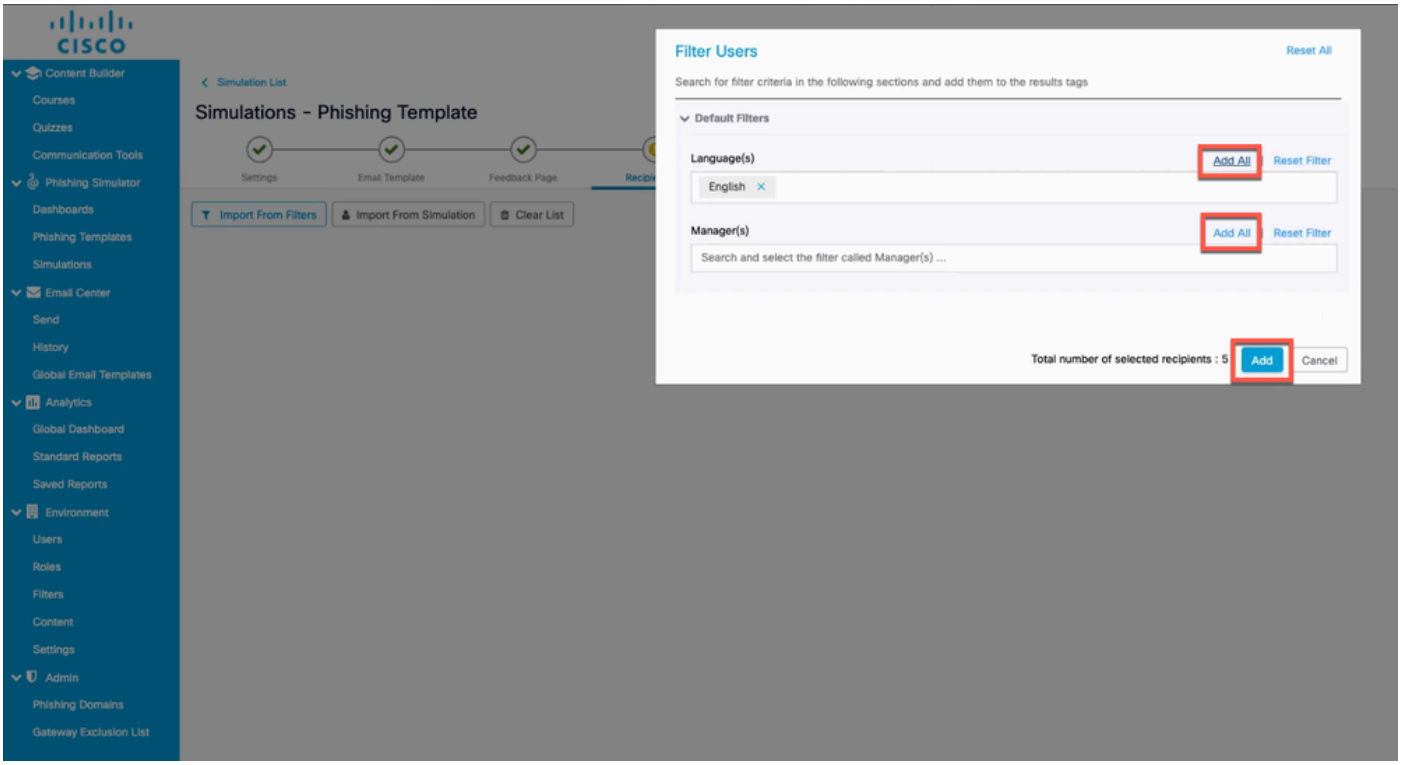

Schermafdruk met velden die moeten worden ingevuld om nieuwe simulatie te configureren

c. Klik op Import from Filters en voeg de ontvangers van phishing-e-mail toe aan de Recipient Listlijst zoals weergegeven in de afbeelding.



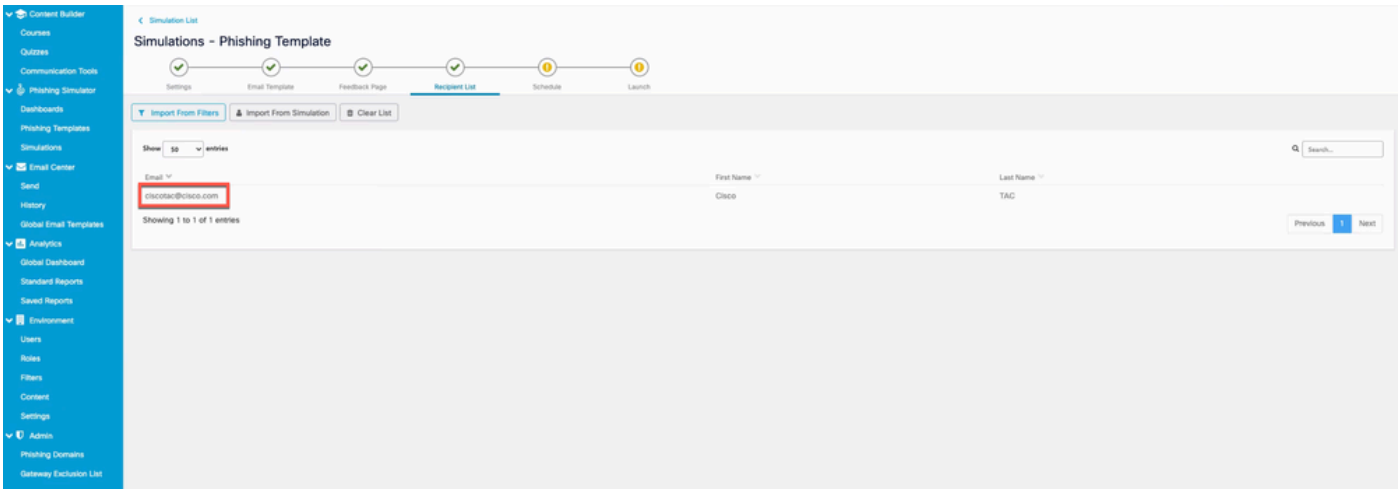

Screenshot met de knop "Importeren uit filters"

U kunt gebruikers filteren op taal of op beheer. Klik op Add zoals getoond in de afbeelding.



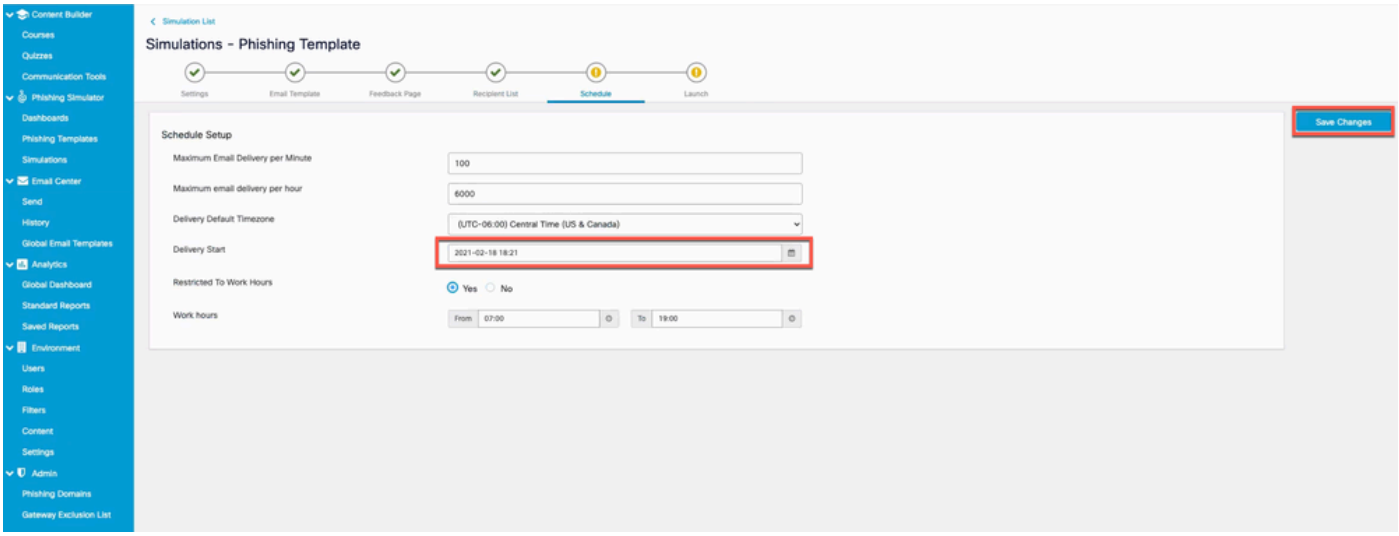

Schermafbeelding van het dialoogvenster Gebruikers filteren voor filteren op taal of beheer

Hier is een voorbeeld van de gebruiker die is gemaakt in stap 2, die nu wordt toegevoegd aan de lijst met ontvangers zoals weergegeven in de afbeelding.



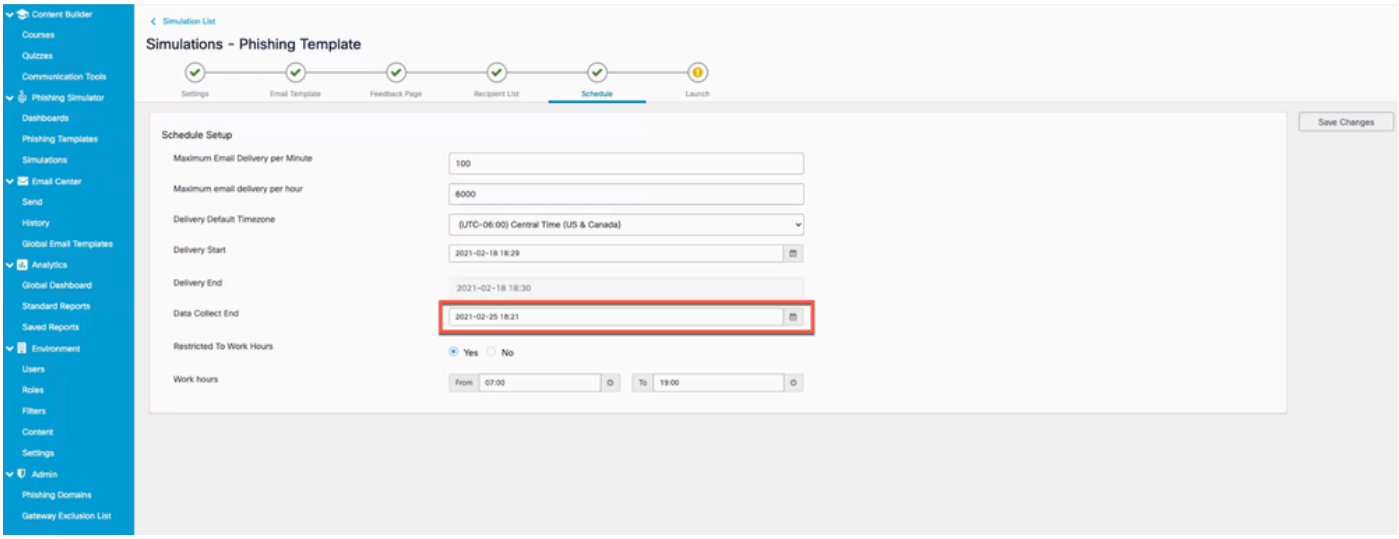

Schermafbeelding van de gebruiker die eerder is gemaakt, wordt vermeld als ontvanger voor de phishing-simulatie

d. StelDelivery Startde datum en Save wijzigingen in om de campagne te plannen zoals weergegeven in de afbeelding.



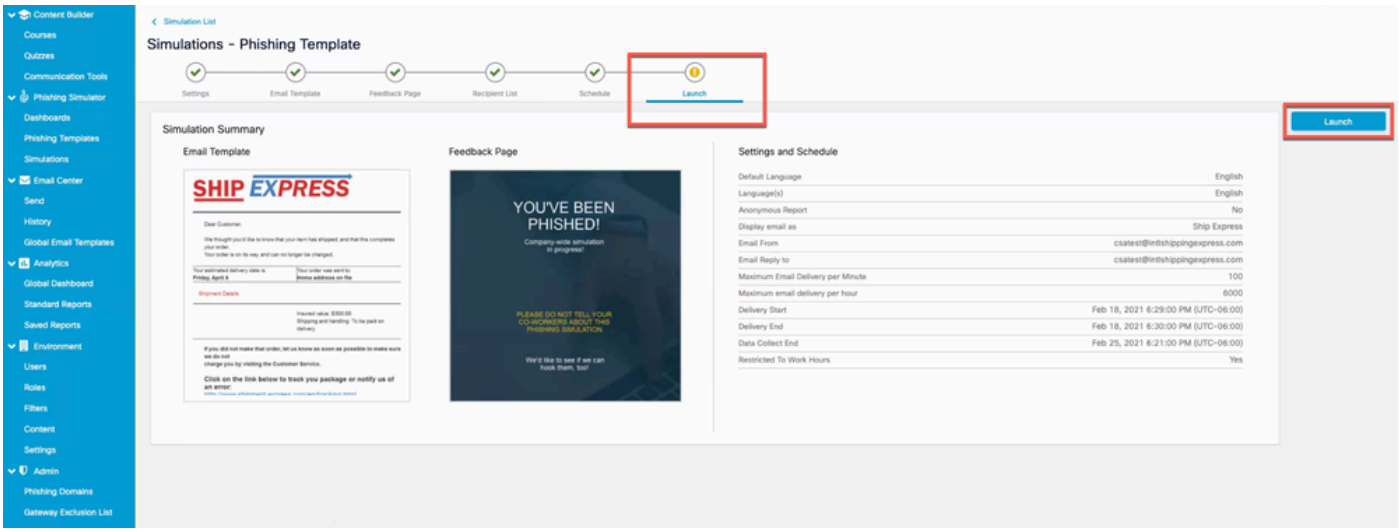

Schermafbeelding die het veld Start levering markeert

Zodra de startdatum is gekozen, is de optie om de campagne end date voor de campagne te selecteren ingeschakeld, zoals weergegeven in de afbeelding.



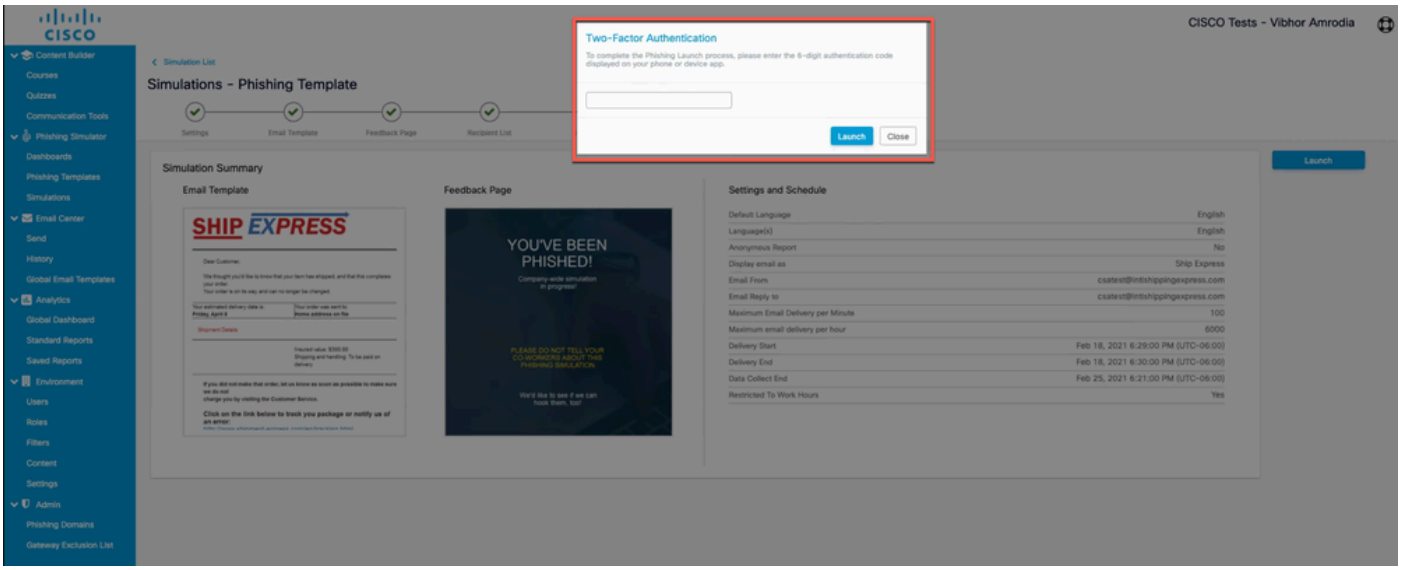

Schermafbeelding van het markeren van het veld Einde gegevensverzameling, dat aangeeft wanneer de simulatie moet worden beëindigd

e. Klik op Launch om de campagne te starten zoals weergegeven in de afbeelding.




Schermafbeelding van het laatste tabblad van de wizard Simulatie maken waar de campagne kan worden gestart

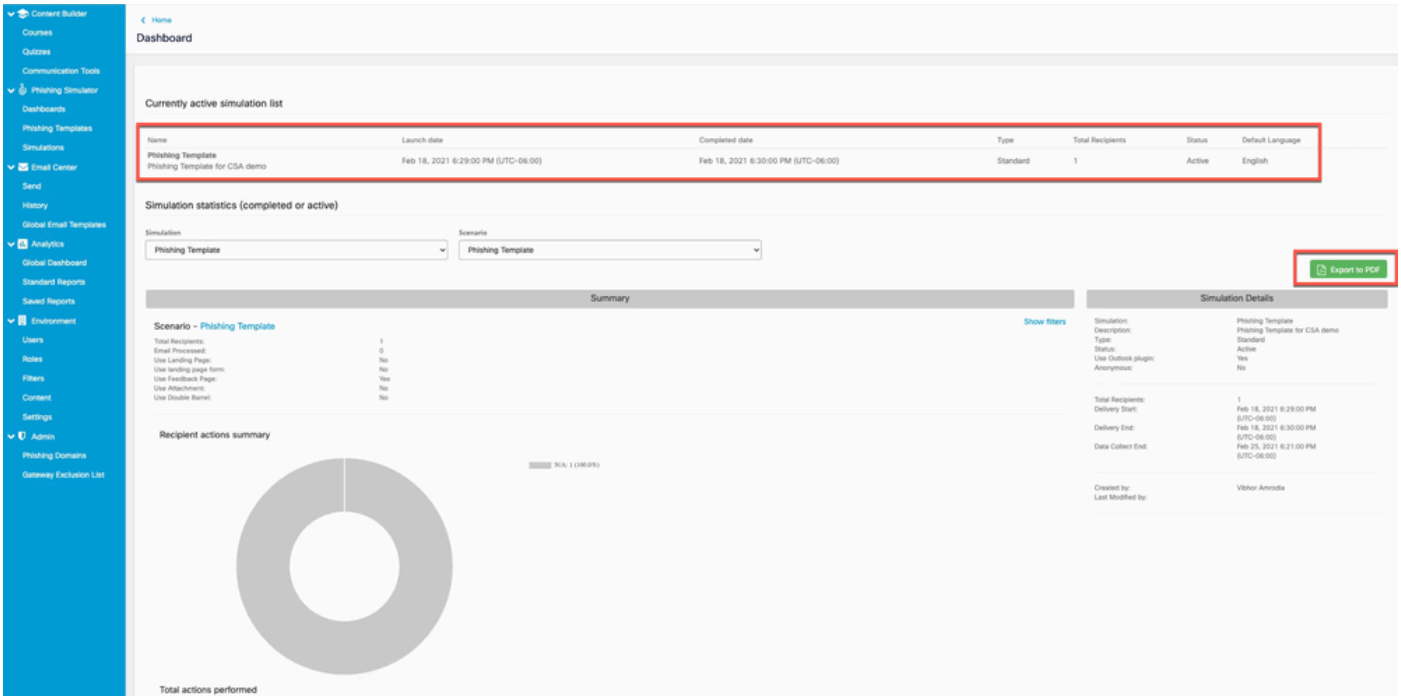
Een tweefactorauthenticatiecode kan worden aangevraagd nadat op de startknop is geklikt. Voer de code in en klik op Launchde afbeelding.




Screenshot van het pop-upvenster waarin om de tweefactorauthenticatiecode wordt gevraagd

## Stap 5. Verificatie van actieve simulaties

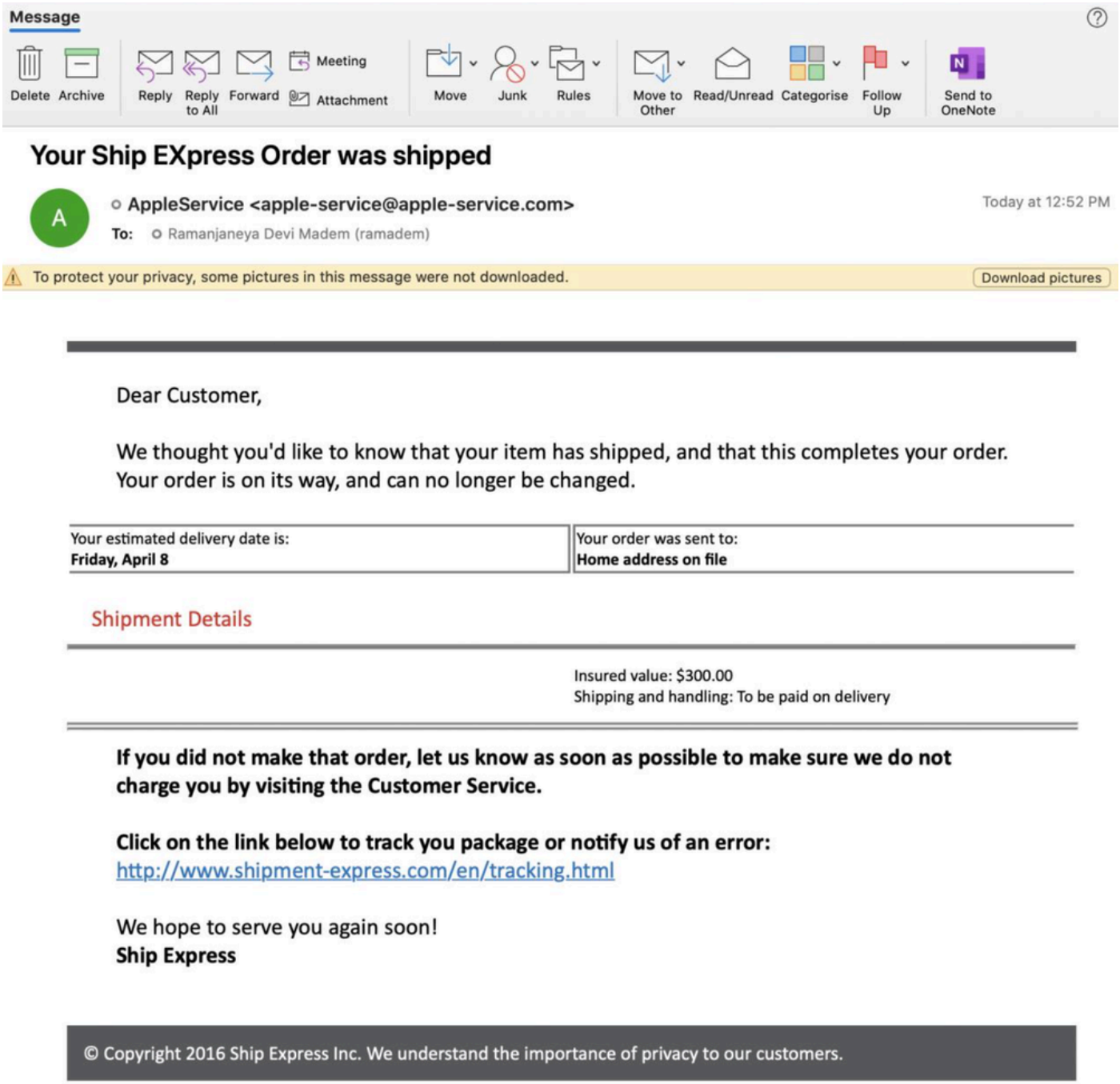
Navigeer naarPhishing Simulator > DashboardsEuropa. De huidige actieve simulatielijst bevat de actieve simulaties. U kunt ook op klikken Export as PDF en hetzelfde rapport krijgen als in de afbeelding wordt weergegeven.




Screenshot van het dashboard voor phishing-simulaties

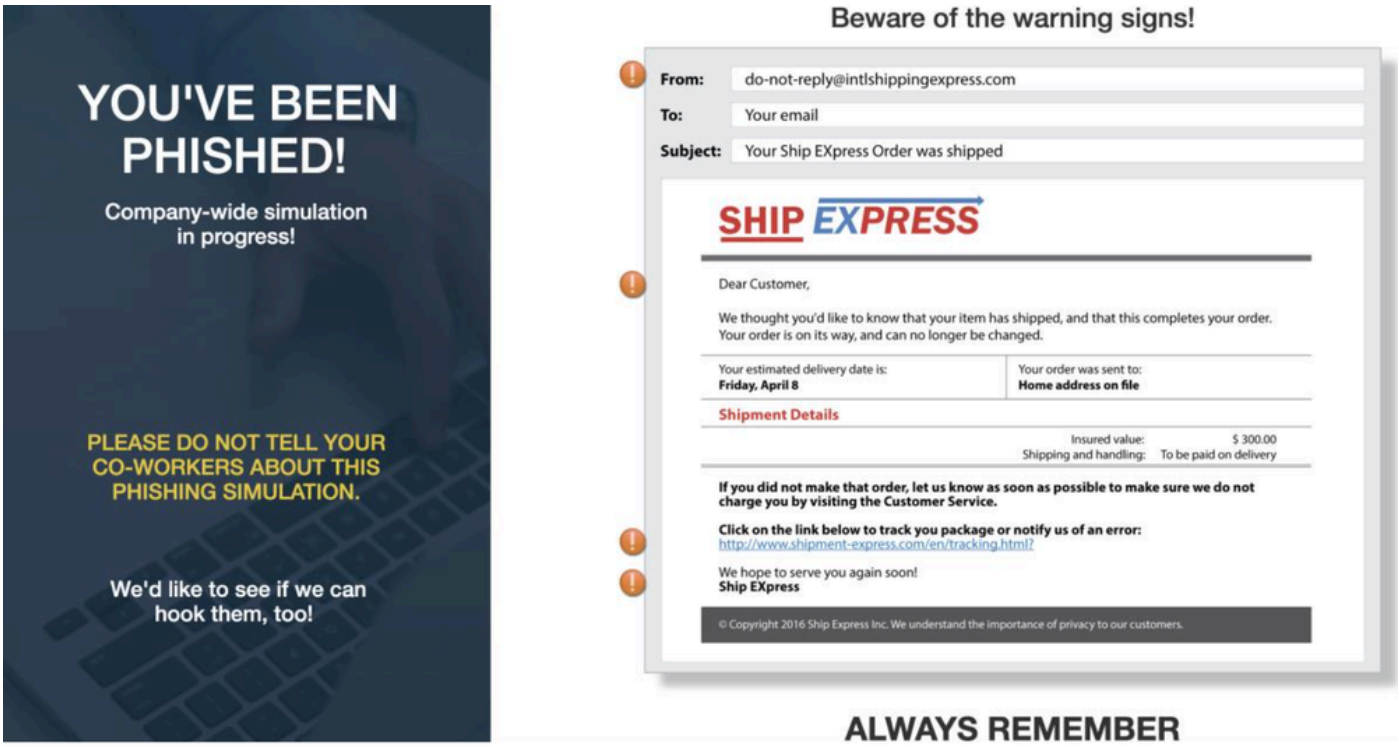
# Wat zien we aan de kant van de ontvanger?

Voorbeeld van een phishing-simulatie-e-mail in de inbox van de ontvanger.




Voorbeeld van de gesimuleerde phish-e-mail in een gebruikersmailbox

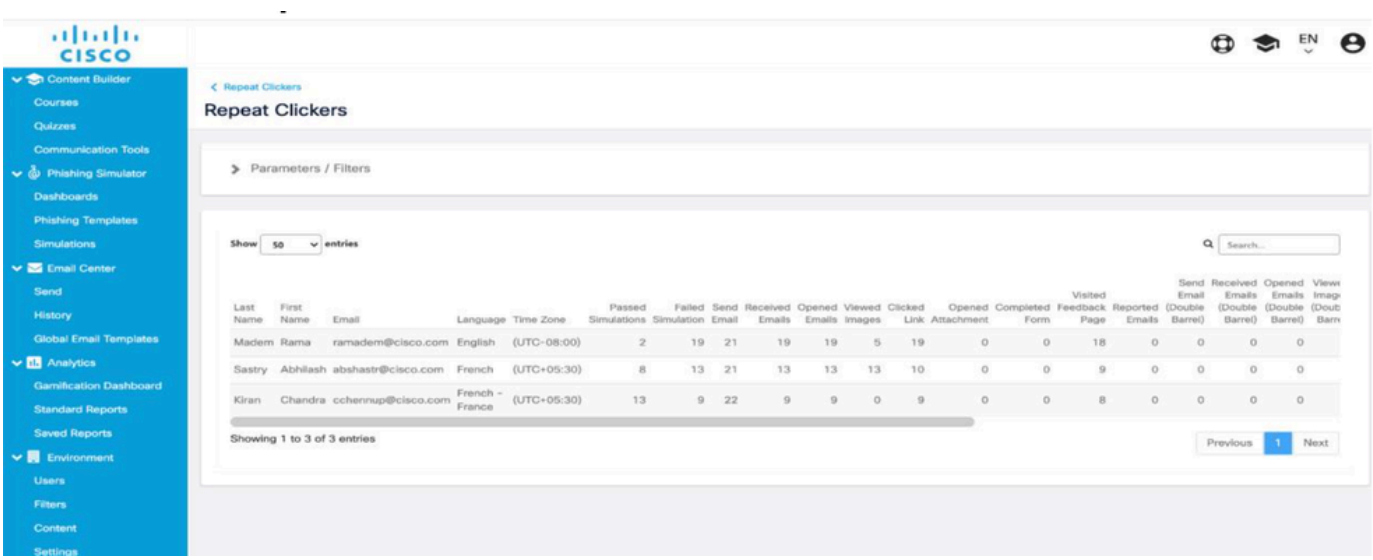
Wanneer de ontvanger op de URL klikt, wordt deze feedbackpagina aan de gebruiker getoond en deze gebruiker wordt weergegeven als onderdeel van de lijst met herhaalde clickers (die vrij op de phish-URL hebben geklikt) in CSA.




Voorbeeld van de feedbackpagina die de gebruiker te zien krijgt na het klikken op de URL in de phish-e-mail

# Controleren op CSA

De lijst met terugkerende klikken wordt weergegeven onderAnalytics > Standard Reports > Phishing Simulations > Repeat Clickersas shown in the image.

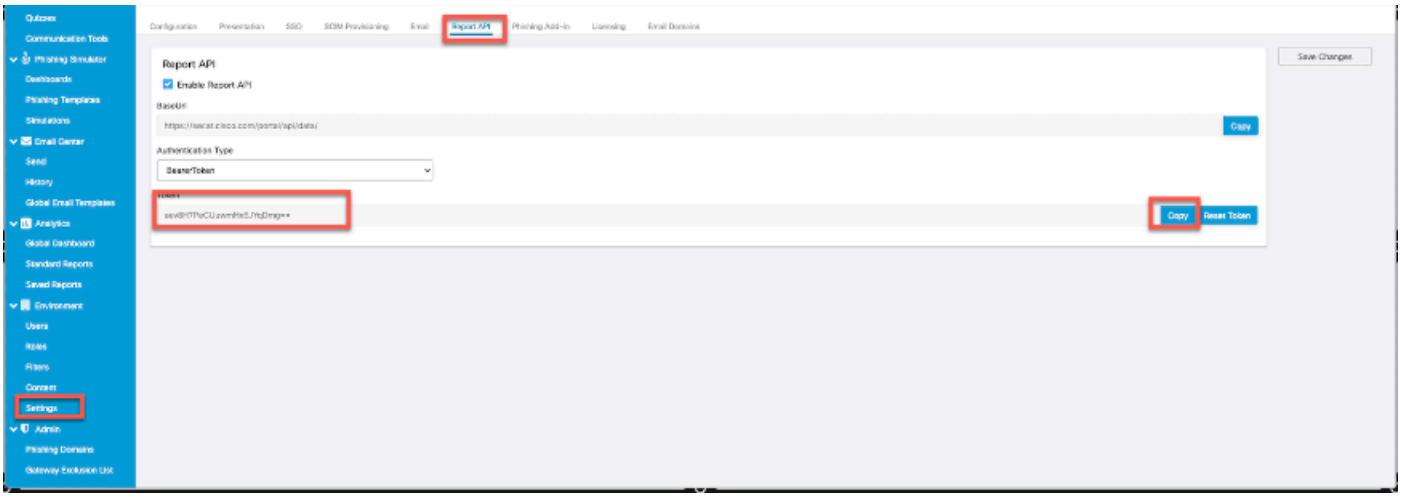



Schermafbeelding van de pagina Repeat Clickers

# De beveiligde e-mailgateway configureren

Opmerking: onder het gedeelte Create and Send Phishing Simulations van CSA Cloud Service Stap 3. wanneer u inschakeltReport API, hebt u het token aan toonder genoteerd. Houd dit bij de

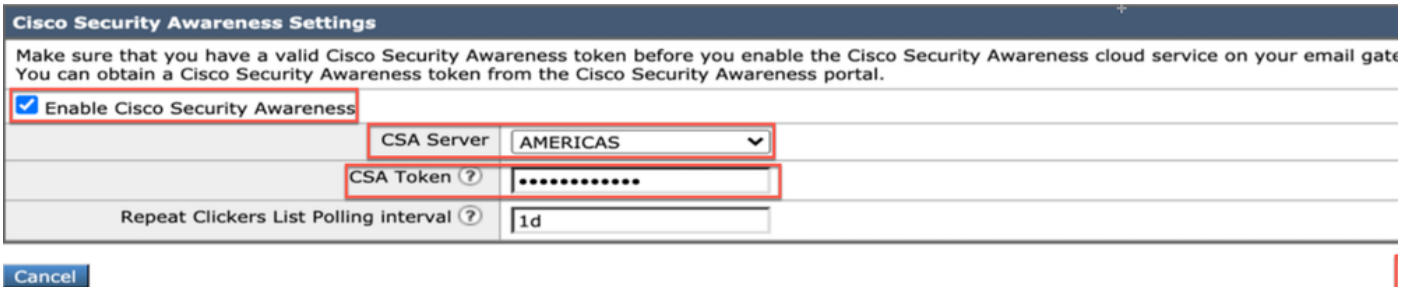
hand.




Screenshot van de pagina onder Rapport API waar de beheerder de token aan toonder kan vinden

## Stap 1. Schakel de functie Cisco Security Awareness in de beveiligde e-mailgateway in

Navigeer op de Secure Email Gateway GUI naar Security Services > Cisco Security Awareness > Enable . Enter the Region en het CSA-token (token aan toonder verkregen van CSA Cloud Service zoals weergegeven in de eerder genoemde notitie) en dien de wijzigingen in en verbind deze.




Screenshot van de pagina Cisco Security Awareness-instellingen op de Cisco Secure Email Gateway

### CLI-configuratie

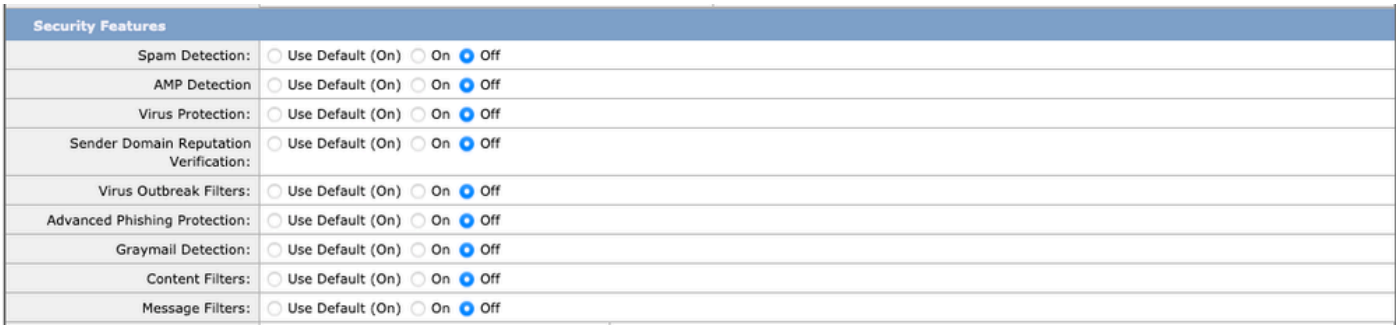
Typ om CSA csaconfig te configureren via de CLI.

```
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]>
```

## Stap 2. Gesimuleerde phishing-e-mails van CSA Cloud Service toestaan

Opmerking: het CYBERSEC_AWARENESS_ALLOWED poststroombeleid wordt standaard gemaakt, waarbij alle scanengines zijn ingesteld op Uit, zoals hier wordt weergegeven.



| 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 |

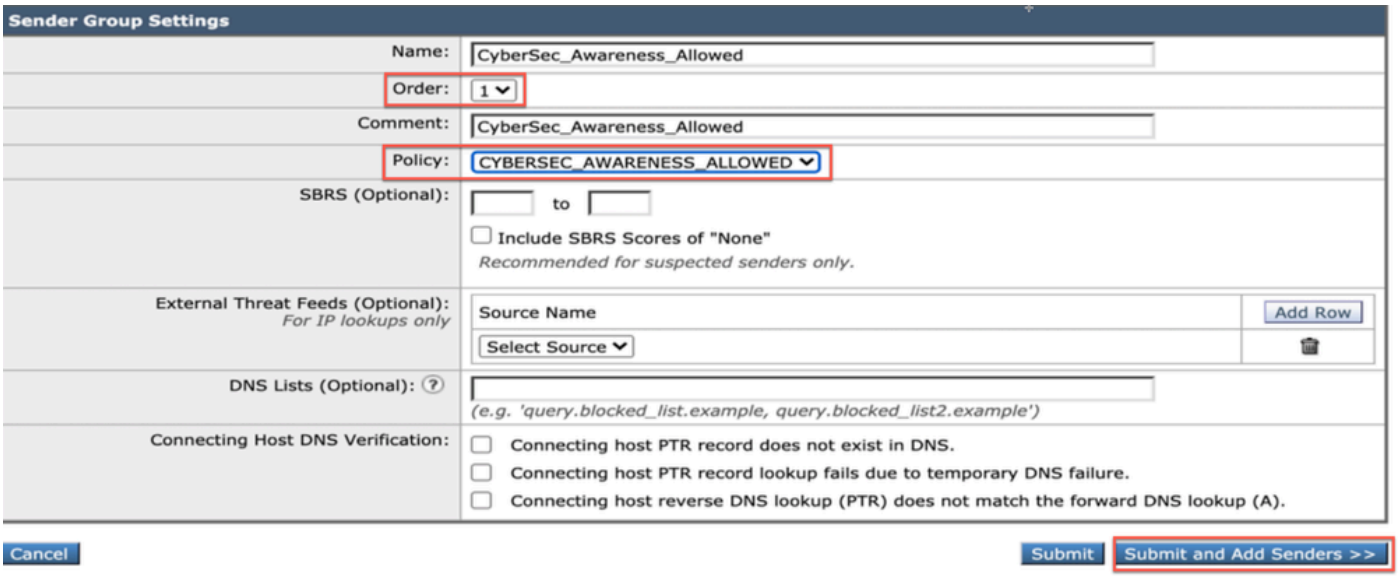
Schermafbeelding van het "CYBERSEC_AWARENESS_ALLOWED"-mailstroombeleid met uitgeschakelde beveiligingsfuncties

Om gesimuleerde e-mails van phishingcampagnes van CSA Cloud Service toe te staan om alle scanengines op Secure Email Gateway te omzeilen:

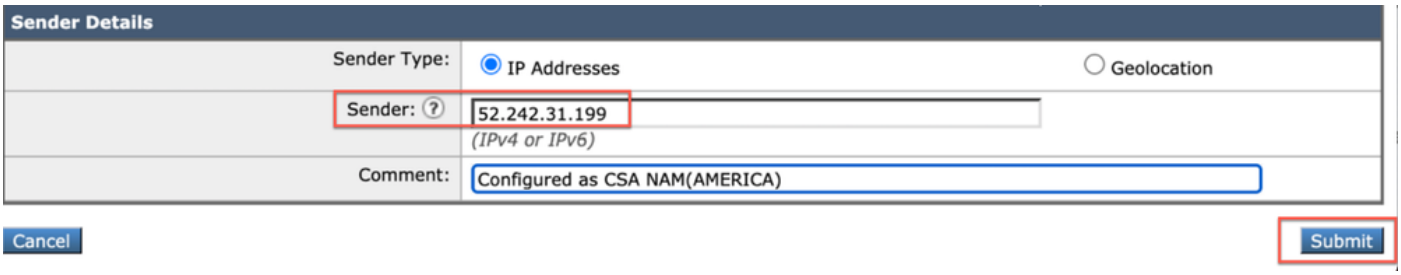
a. Een nieuwe afzendergroep maken en het beleid voor de e-mailstroom CYBERSEC_AWARENESS_ALLOWED toewijzen. Navigeer naar Mail Policies > HAT Overview > Add Sender Group en selecteer het beleid CYBERSEC_AWARENESS_ALLOWED en stel de volgorde in op 1 en vervolgens Submit and Add Senders.

b. Voeg een afzender IP/domain of afzender toeGeo Locationvan waaruit de e-mails van de Phishing-campagne worden geïnitieerd.

Navigeer naarMail Polices > HAT Overview > Add Sender Group > Submit and Add Senders > Add the sender IP > Submiten Commit wijzigingen zoals weergegeven in de afbeelding.




Screenshot van een CyberSec_Awareness_Allowed afzendergroep met het "CYBERSEC_AWARENESS_ALLOWED"-beleid voor e-mailstromen geselecteerd.




Screenshot van de pagina Cisco Security Awareness-instellingen op de Cisco Secure Email Gateway

CLI-configuratie:

1. Navigeer naar listenerconfig > Edit > Inbound (PublicInterface) > HOSTACCESS > NEW > New Sender Group .

2. Maak een nieuwe afzendergroep metCYBERSEC_AWARENESS_ALLOWEDe-mailbeleid en voeg een afzender/IP-domein toe van waaruit de e-mails van de phishingcampagne worden geïnitieerd.

3. Stel de volgorde van de nieuwe afzendergroep in op 1 en gebruik de Move Optie onder listenerconfig > EDIT > Inbound (PublicInterface) > HOSTACCESS > MOVE .

4. Toezeggen.

---

Opmerking: het IP-adres van de afzender is het IP-adres van de CSA en is gebaseerd op de regio die u hebt geselecteerd. Raadpleeg de tabel voor het juiste IP-adres dat moet worden gebruikt. Sta deze IP-adressen/hostnamen toe in de firewall met poortnummer 443 voor SEG 14.0.0-xxx om verbinding te maken met de CSA-cloudservice.

---

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 | |

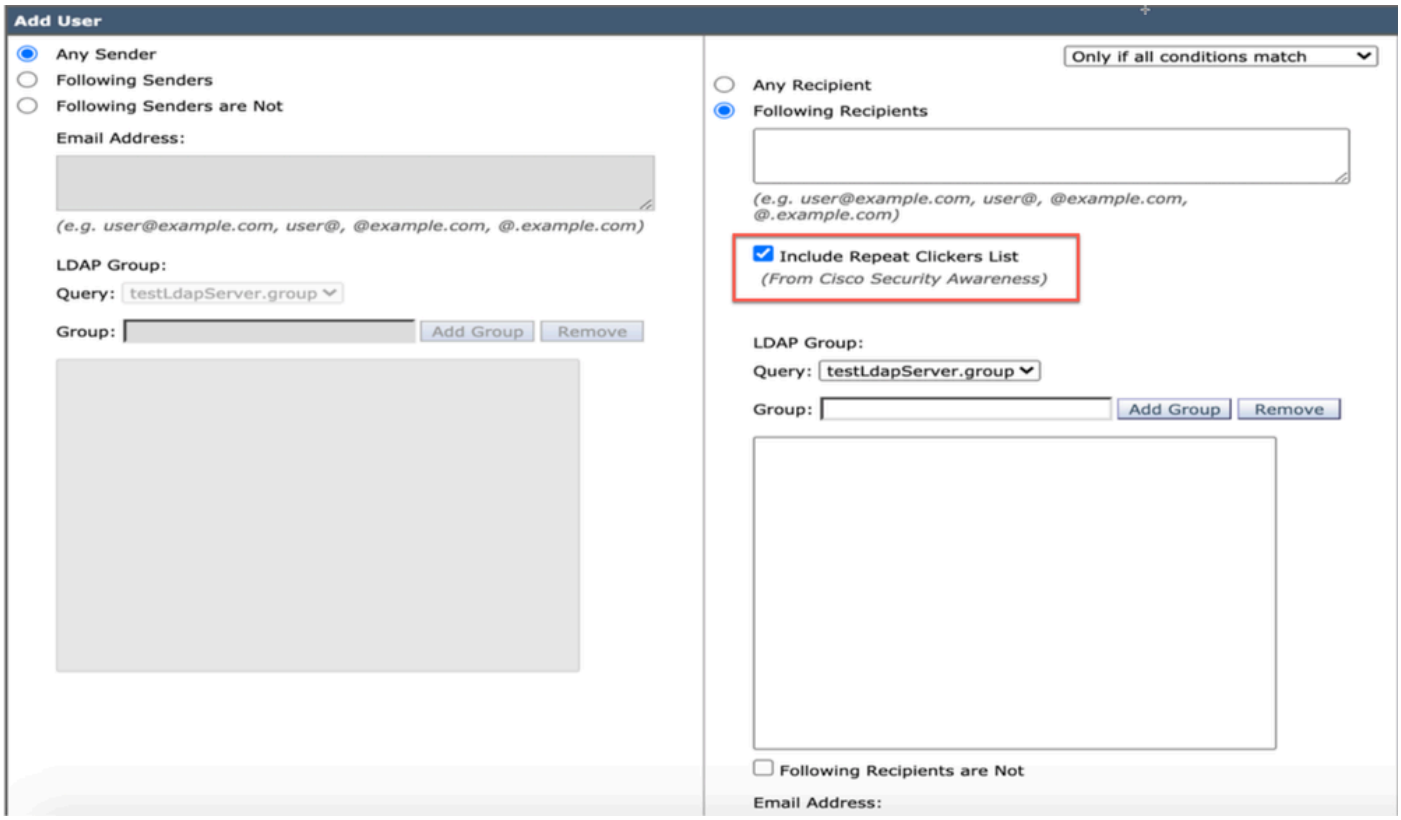
Schermafbeelding van de CSA-regio's Amerika en de EU IP-adressen en hostnamen

## Stap 3. Onderneem actie op Repeat Clicker van SEG

Zodra de phishing-e-mails zijn verzonden en de lijst met terugkerende clickers in de SEG is ingevuld, kan een agressief beleid voor inkomende e-mail worden gemaakt om actie te ondernemen op het gebied van e-mail aan die specifieke gebruikers.

Include Repeat Clickers List Maak een nieuw agressief beleid voor inkomende aangepaste e-mail en schakel het selectievakje in het gedeelte voor ontvangers in.

Van GUI, navigeer naar Mail Policies > Incoming Mail Policies > Add Policy > Add User > Include Repeat Clickers List > Submit en Commit de wijzigingen.




Schermafbeelding van aangepast beleid voor inkomende e-mail geconfigureerd om e-mail te verwerken die bestemd is voor terugkerende clickers

# Gids voor probleemoplossing

1. Navigeer naar csaconfig > SHOW_LISTom de details van de lijst met terugkerende clickers te bekijken.

```
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. Navigeer naar csaconfig > UPDATE_LIST als u de lijst met terugkerende clickers wilt forceren.

```
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.
```

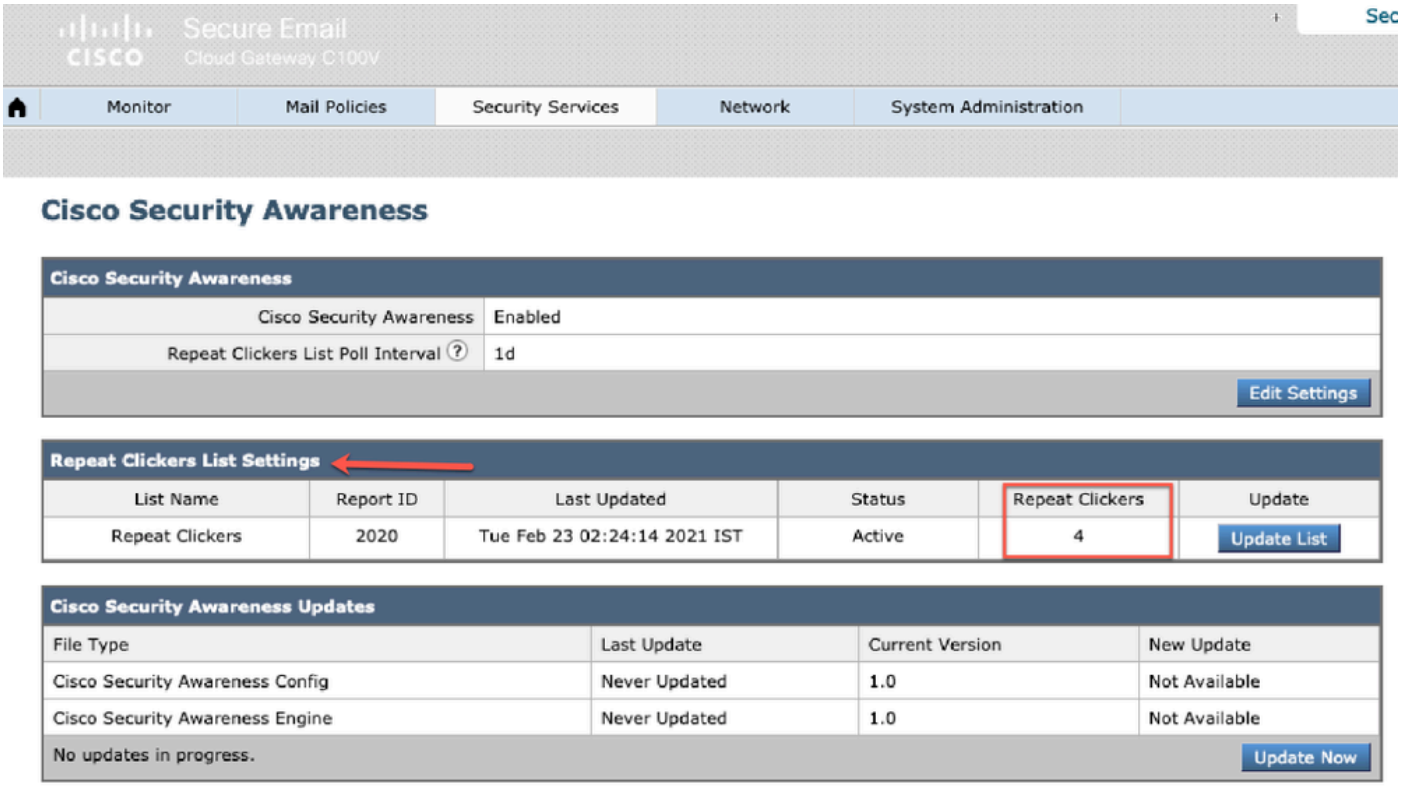
3. Sla de csa-logs op om te zien of de lijst met terugkerende clickers is gedownload of dat er een fout is opgetreden. Hier is de working setup:

```
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. Het aantal terugkerende clickers lijst kan ook worden gezien vanuit de GUI. Navigeer naar Security Services > Cisco Security Awarenesszoals getoond in de afbeelding.




Screenshot van Security Services > Cisco Security Awareness-pagina met het aantal herhaalde klikken

# Gerelateerde informatie

- [Technische ondersteuning en documentatie – Cisco Systems]

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.