Konfiguration der Security Awareness Integration mit Cisco Secure Email Gateway

Inhalt

Einleitung

In diesem Dokument werden die erforderlichen Schritte zum Konfigurieren der CSA-Integration (Cisco Security Awareness) mit dem Cisco Secure Email Gateway beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konzepte und Konfiguration von Cisco Secure Email Gateway
- CSA-Cloud-Service

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf AsyncOS für SEG 14.0 und höher.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Erstellen und Senden von Phishing-Simulationen vom CSA Cloud Service

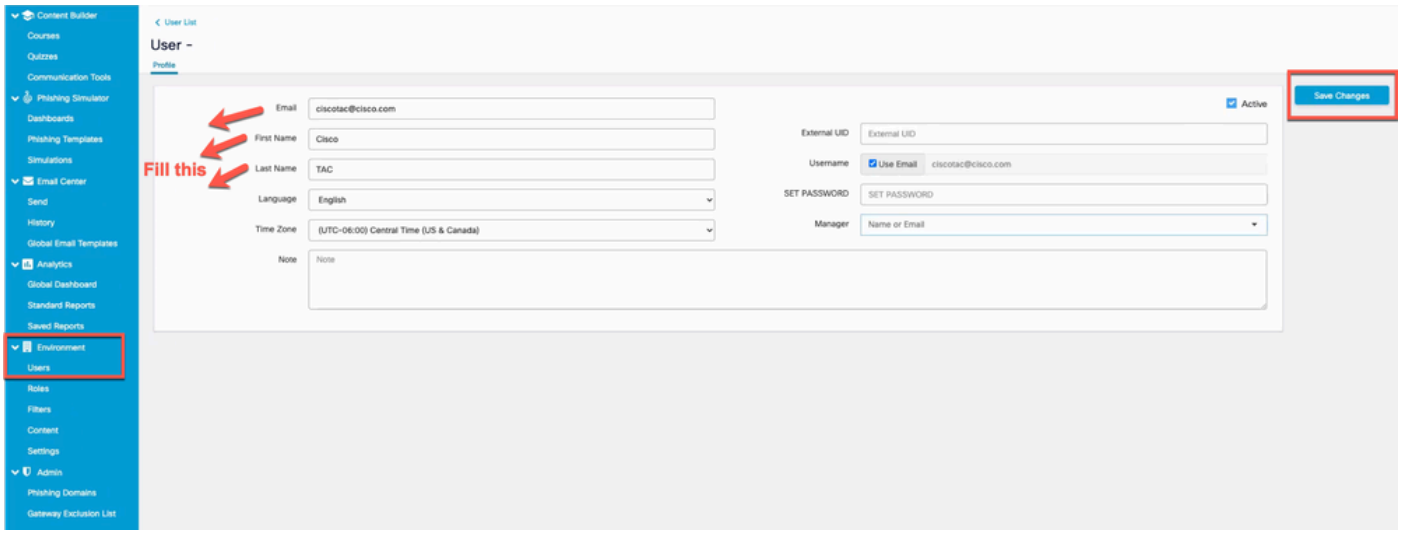
Schritt 1: Melden Sie sich beim CSA Cloud Service an.

Siehe:
1. https://secat.cisco.com/ für die Region AMERIKA

2. https://secat-eu.cisco.com/ für die Region EUROPA

Schritt 2: Phishing-E-Mail-Empfänger erstellen

Navigieren Sie zu den Feldern E-Mail, Vorname, Nachname und Sprache, **Environment** > **Users** > **Add New User** und füllen Sie diese aus. Klicken Sie dann auf, **Save Changes**wie im Bild dargestellt.

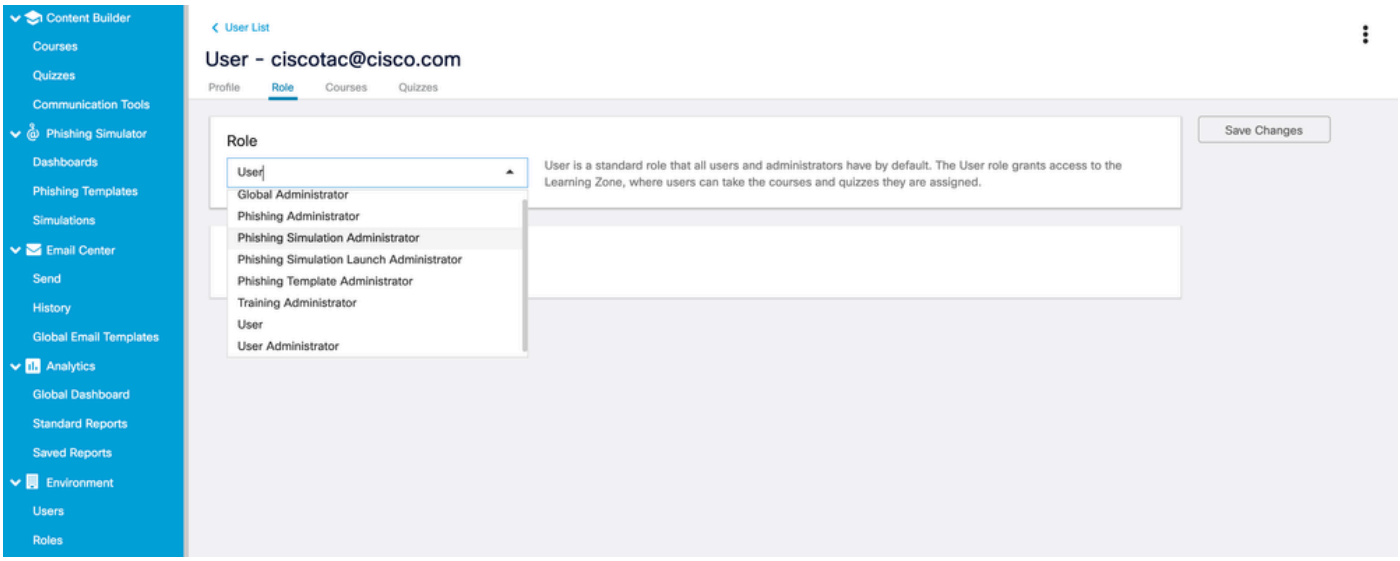


Screenshot der Benutzeroberflächenseite zum Hinzufügen eines neuen Benutzers

---

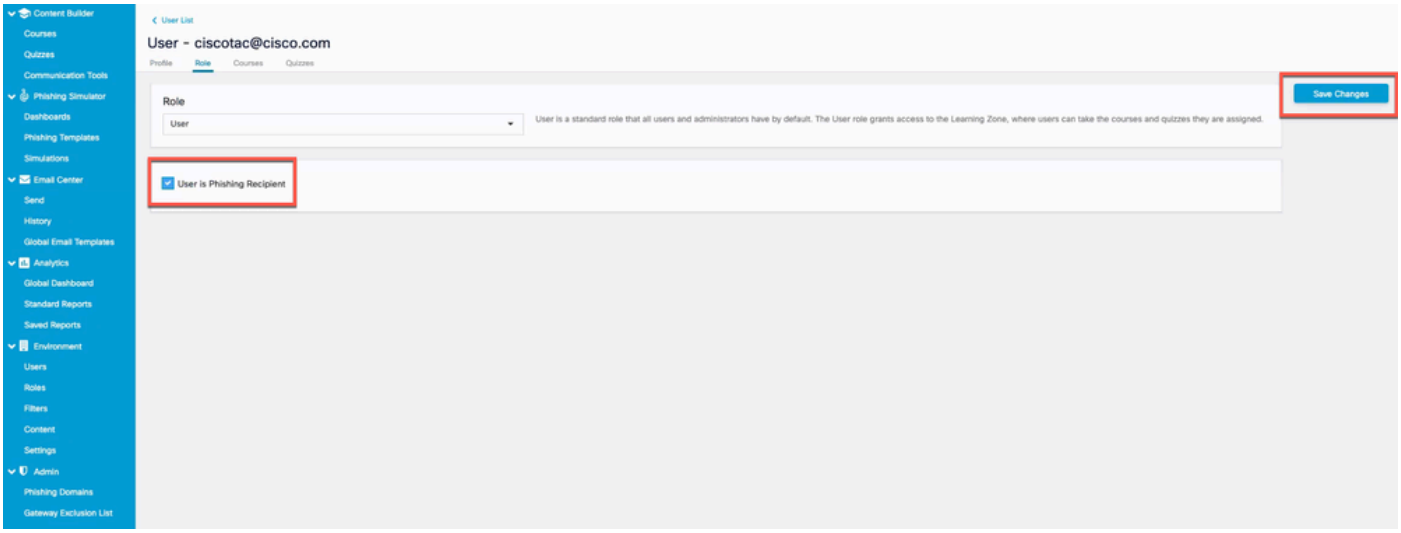
Anmerkung: Ein Kennwort muss nur für einen CSA-Administrator festgelegt werden, der berechtigt ist, Simulationen zu erstellen und zu starten.

Die Rolle des Benutzers kann nach dem Erstellen des Benutzers ausgewählt werden. Sie können die Rolle aus der Dropdown-Liste auswählen, wie in dieser Abbildung dargestellt:



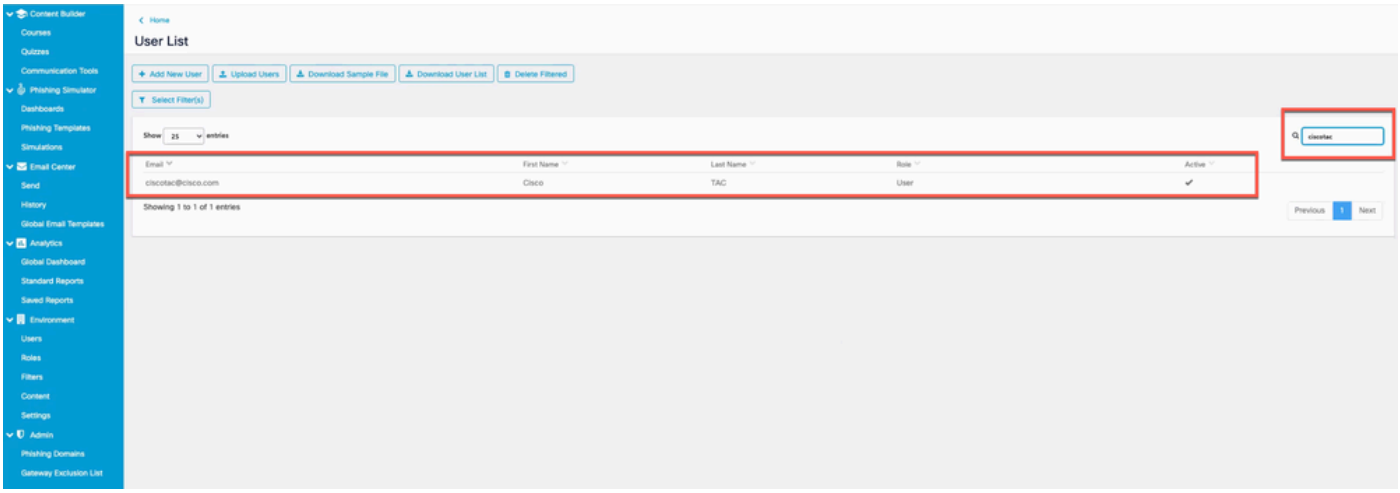
Anzeigen der Dropdown-Optionen für Benutzerrollen

Aktivieren Sie dasUser is Phishing Recipient > Save ChangesKontrollkästchen, wie im Bild dargestellt.



Screenshot, in dem das Kontrollkästchen "Benutzer ist Phishing-Empfänger" aktiviert ist.

Überprüfen Sie, ob der Benutzer erfolgreich hinzugefügt wurde und aufgeführt wird, wenn die Suche anhand der E-Mail-Adresse im Filter durchgeführt wird, wie im Bild gezeigt.

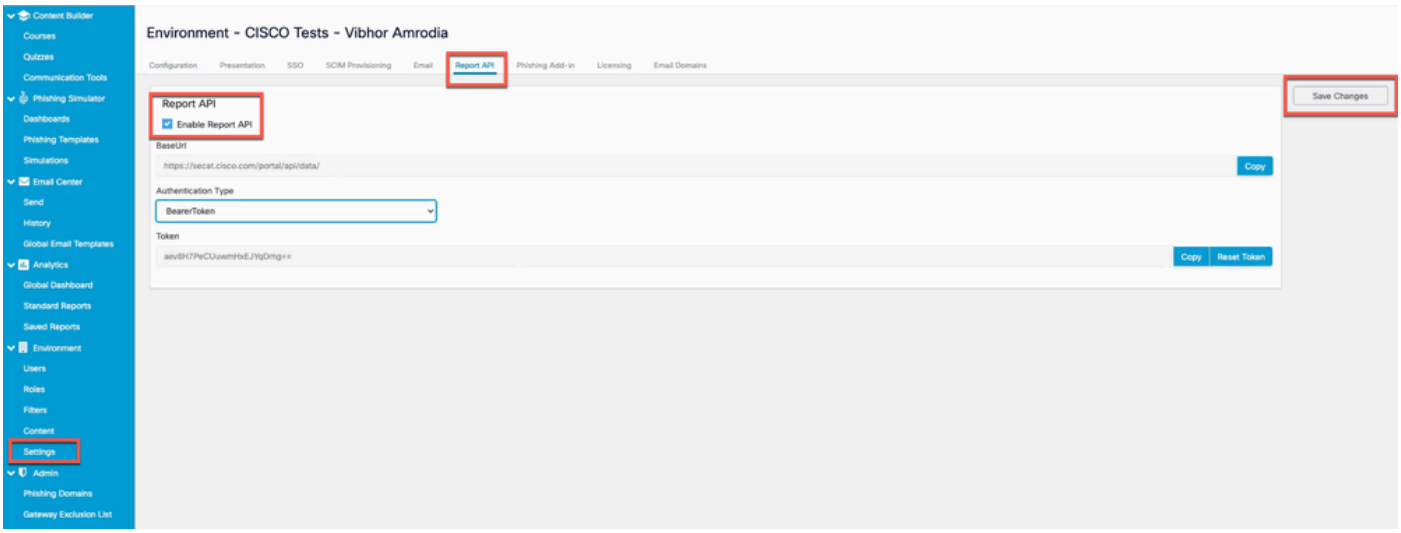


Screenshot des neuen Benutzers in der Benutzerliste

Schritt 3: Berichts-API aktivieren

Navigieren Sie zur Environments > Settings > Report API Registerkarte, und aktivieren Sie das KontrollkästchenEnable Report API > Save Changes .

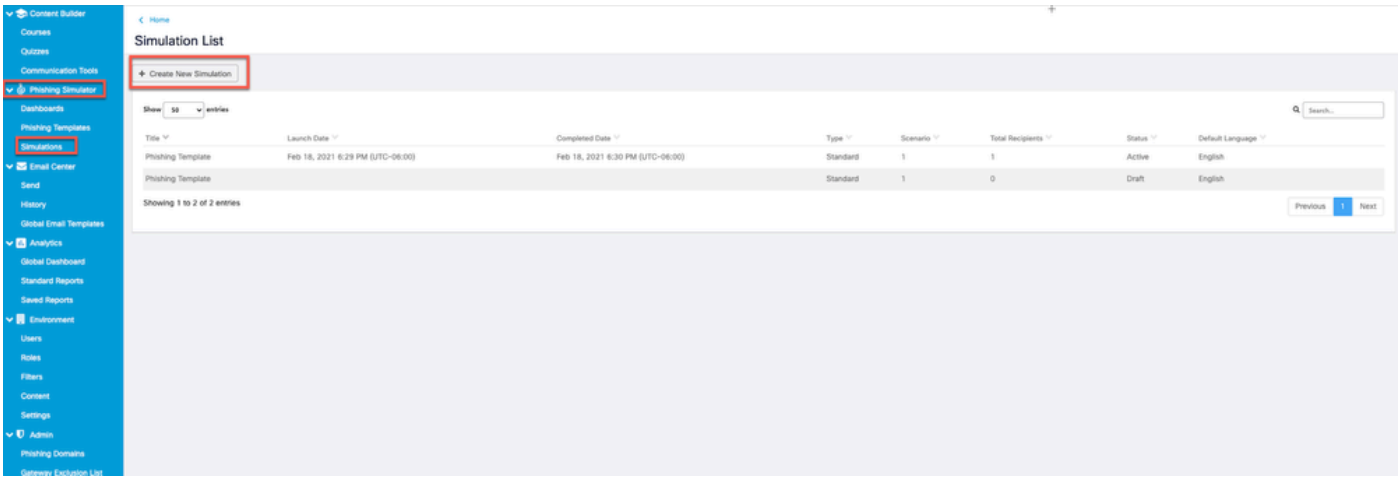
Anmerkung: Notieren Sie sich das Träger-Token. Sie benötigen diese, um die SEG mit CSA zu integrieren.



Screenshot, der das Kontrollkästchen "Report API aktivieren" anzeigt, ist aktiviert.

Schritt 4: Erstellen von Phishing-Simulationen

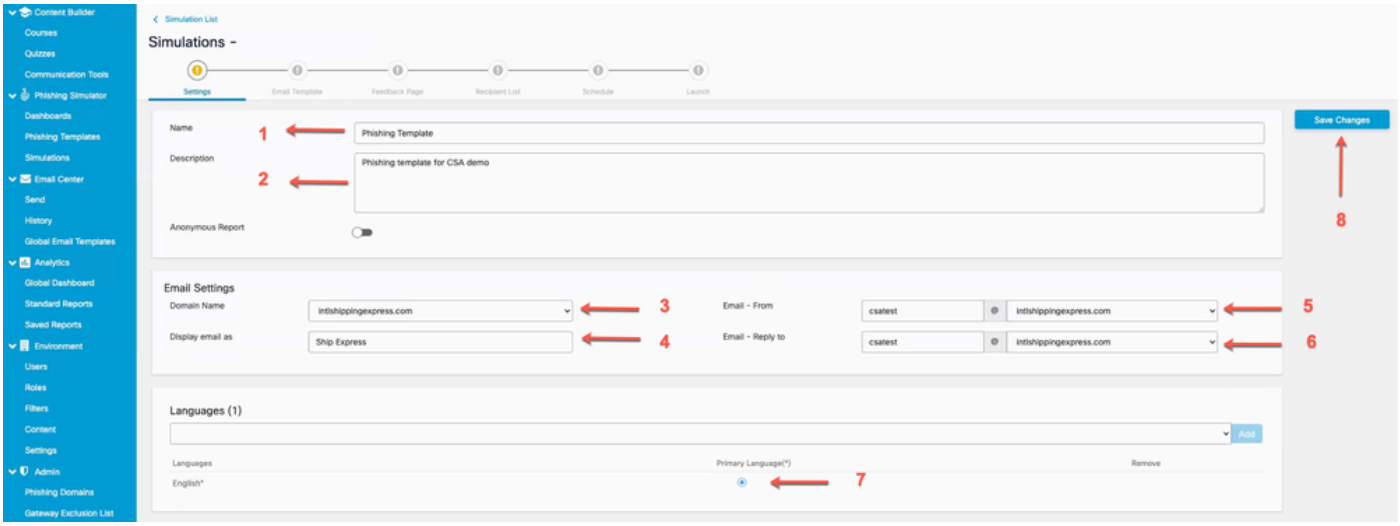
antwort: Navigieren Sie zu, Phishing Simulator > Simulations > Create New Simulation und wählen Sie eine Template aus der verfügbaren Liste aus, wie im Bild dargestellt.



Screenshot der Schaltfläche "Neue Simulation erstellen"

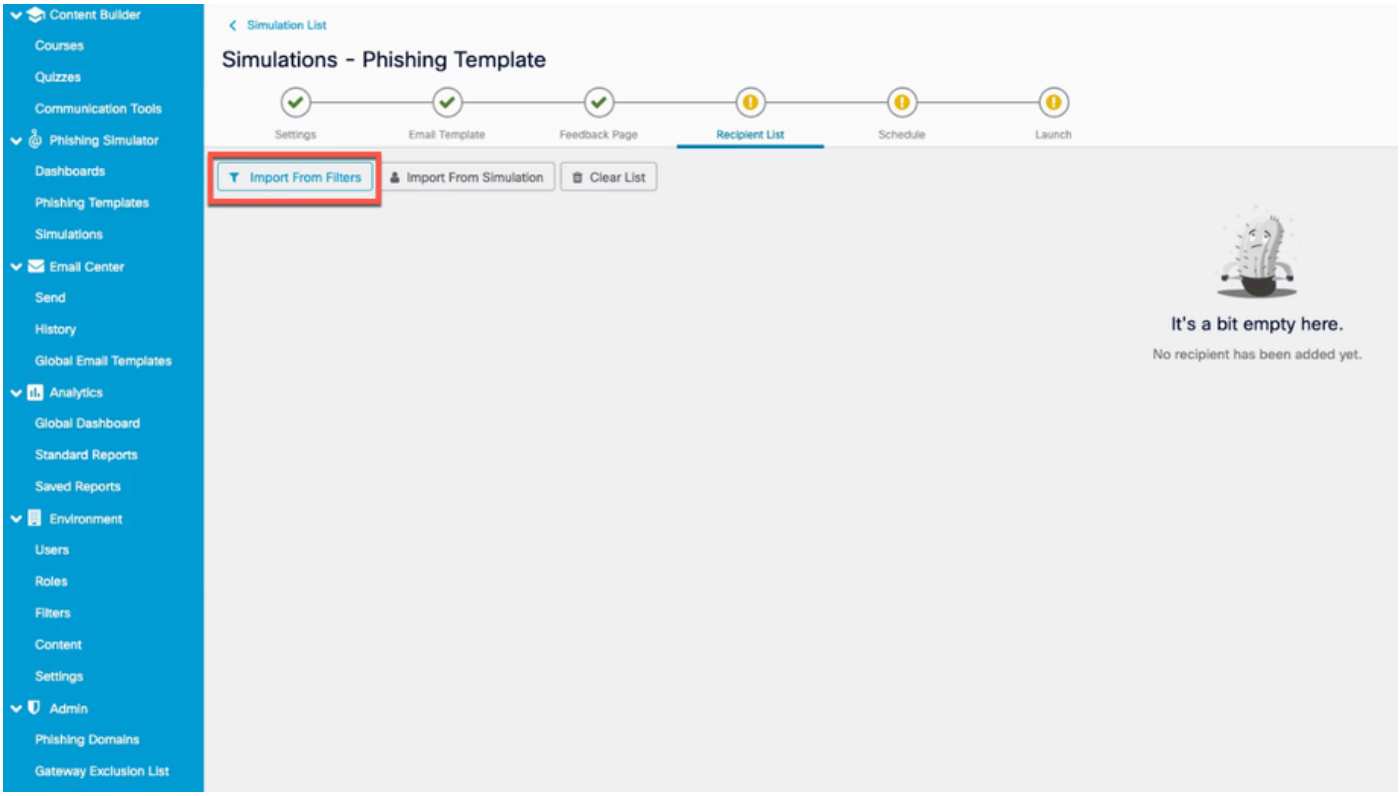
b. Geben Sie folgende Informationen ein:

1. Wählen Sie einen Namen für die Vorlage aus.
2. Beschreibung der Vorlage.
3. Domänenname, mit dem die Phishing-E-Mail gesendet wird.
4. Der Anzeigename für die Phishing-E-Mail.
5. E-Mail-Absenderadresse (in der Dropdown-Liste auswählen).
6. Antwortadresse (aus Dropdown-Liste auswählen).
7. Wählen Sie die Sprache aus.
8. Speichern Sie die Änderungen.



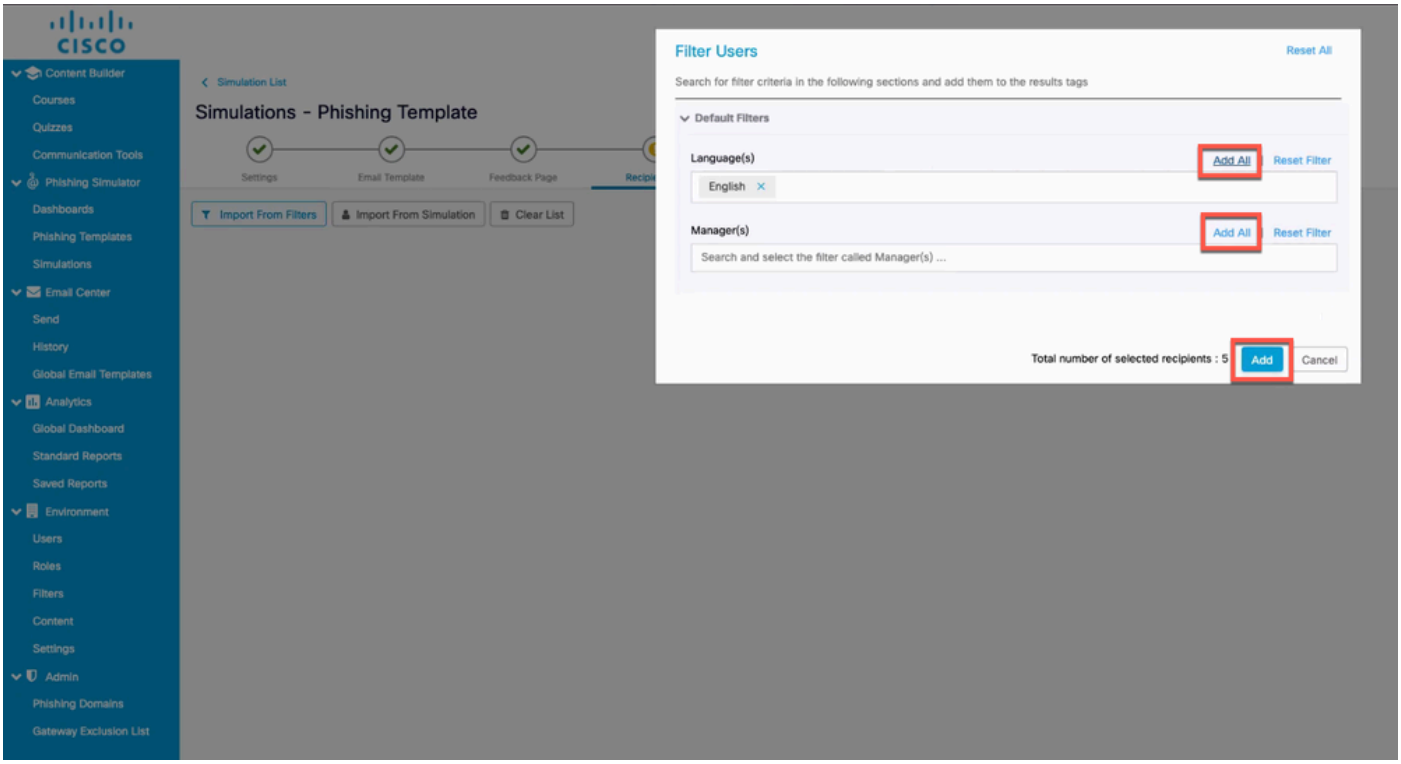
Screenshot der Felder, die für die Konfiguration einer neuen Simulation ausgefüllt werden müssen

c. Klicken Sie auf Import from Filters und fügen Sie die Phishing-E-Mail-Empfänger Recipient Listwie im Bild dargestellt zu.



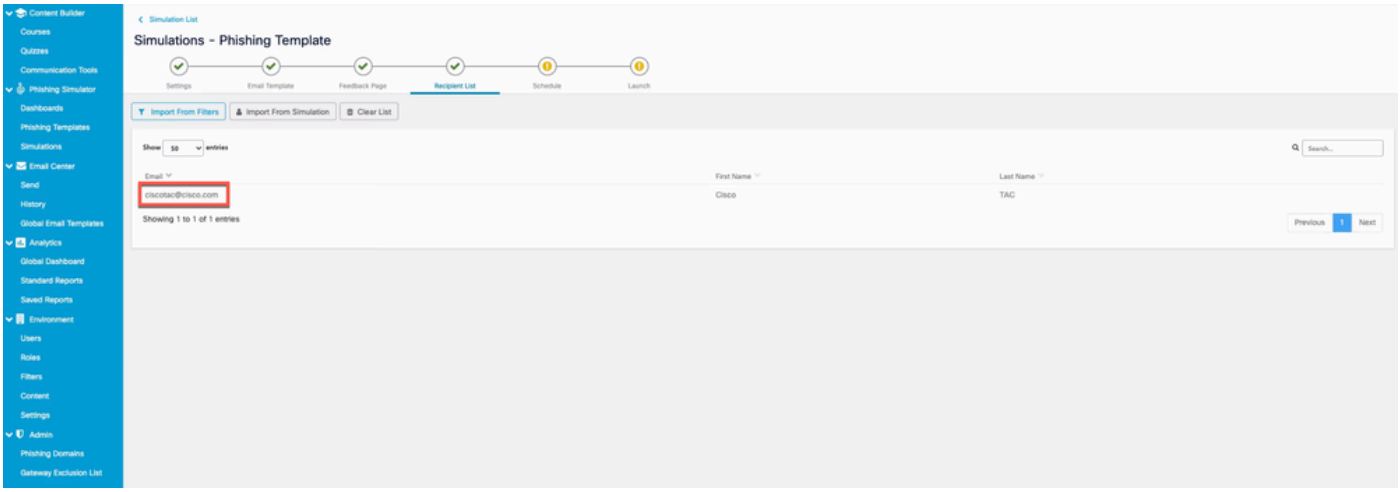
Screenshot mit der Schaltfläche "Aus Filtern importieren"

Sie können Benutzer entweder nach Sprache oder nach Managern filtern. Klicken Sie auf Add wie im Bild dargestellt.



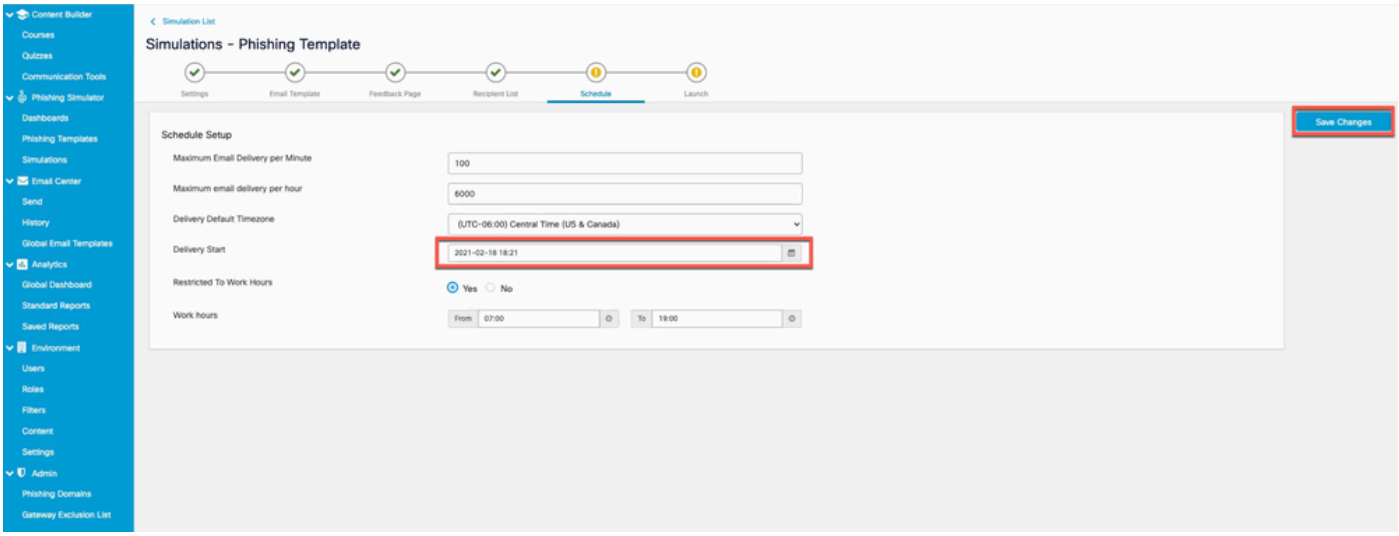
Screenshot des Dialogfelds "Benutzer filtern" zum Filtern nach Sprache oder Manager

Hier ist ein Beispiel für den Benutzer, der in Schritt 2 erstellt wurde, der nun, wie im Bild gezeigt, zur Empfängerliste hinzugefügt wird.



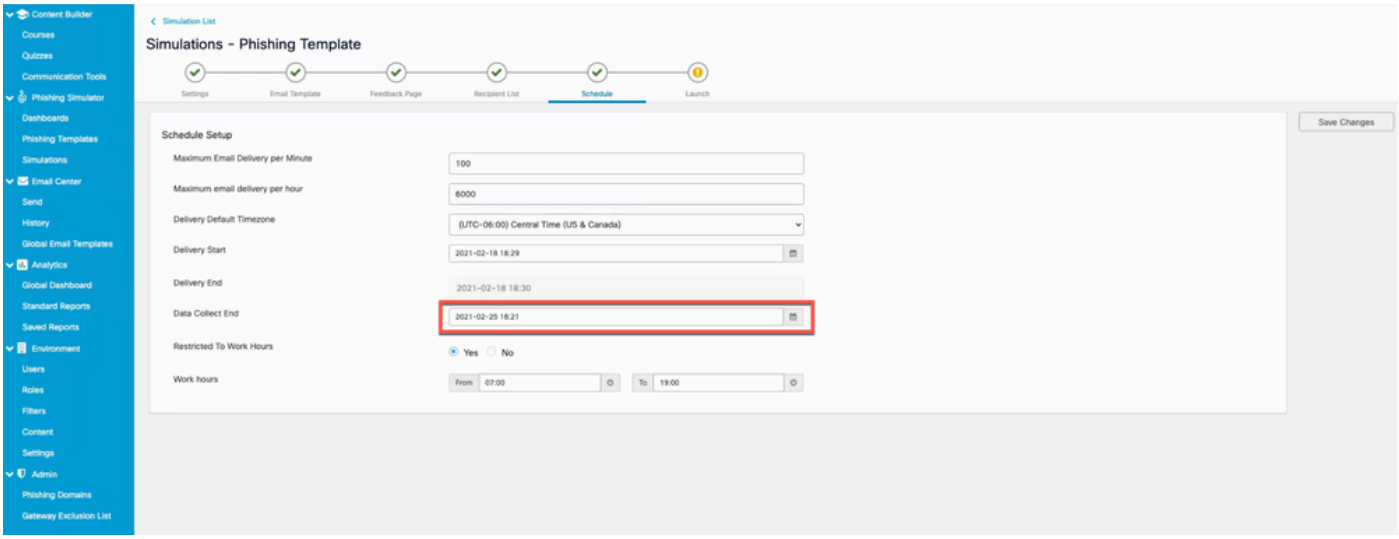
Screenshot des zuvor erstellten Benutzers, der als Empfänger für die Phishing-Simulation aufgeführt ist

d. Legen SieDelivery Startdas Datum und die Save Änderungen so fest, dass die Kampagne wie im Bild dargestellt geplant wird.



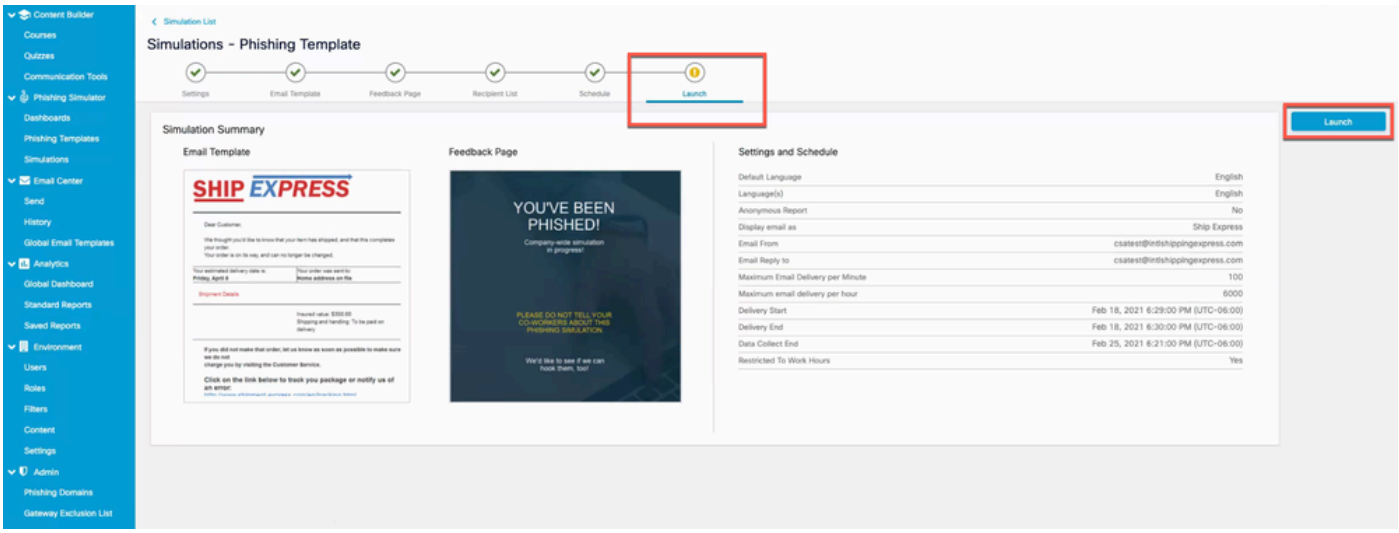
Screenshot des Felds Lieferanfang

Nach der Auswahl des Startdatums wird die Option end date zur Auswahl der Kampagne aktiviert (siehe Bild).



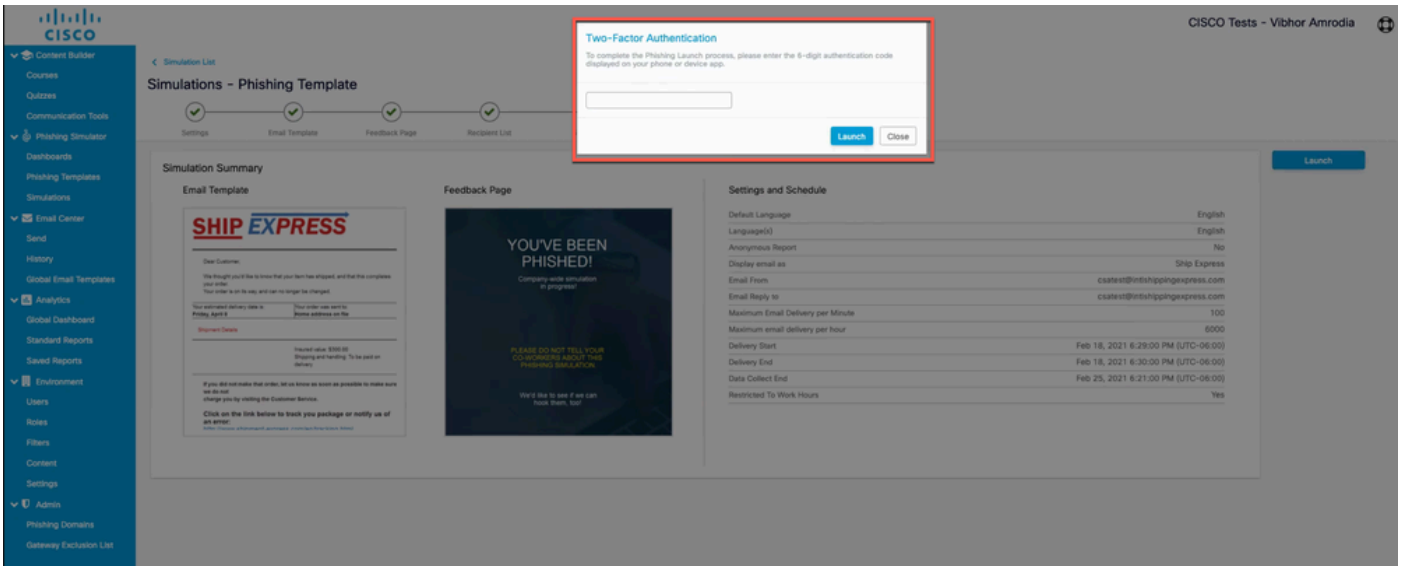
Screenshot des Feldes Datenerfassungsende, das angibt, wann die Simulation beendet werden soll

e. Klicken Sie auf, Launch um die Kampagne wie im Bild dargestellt zu starten.



Screenshot der letzten Registerkarte des Assistenten zum Erstellen von Simulationen, auf der die Kampagne gestartet werden kann

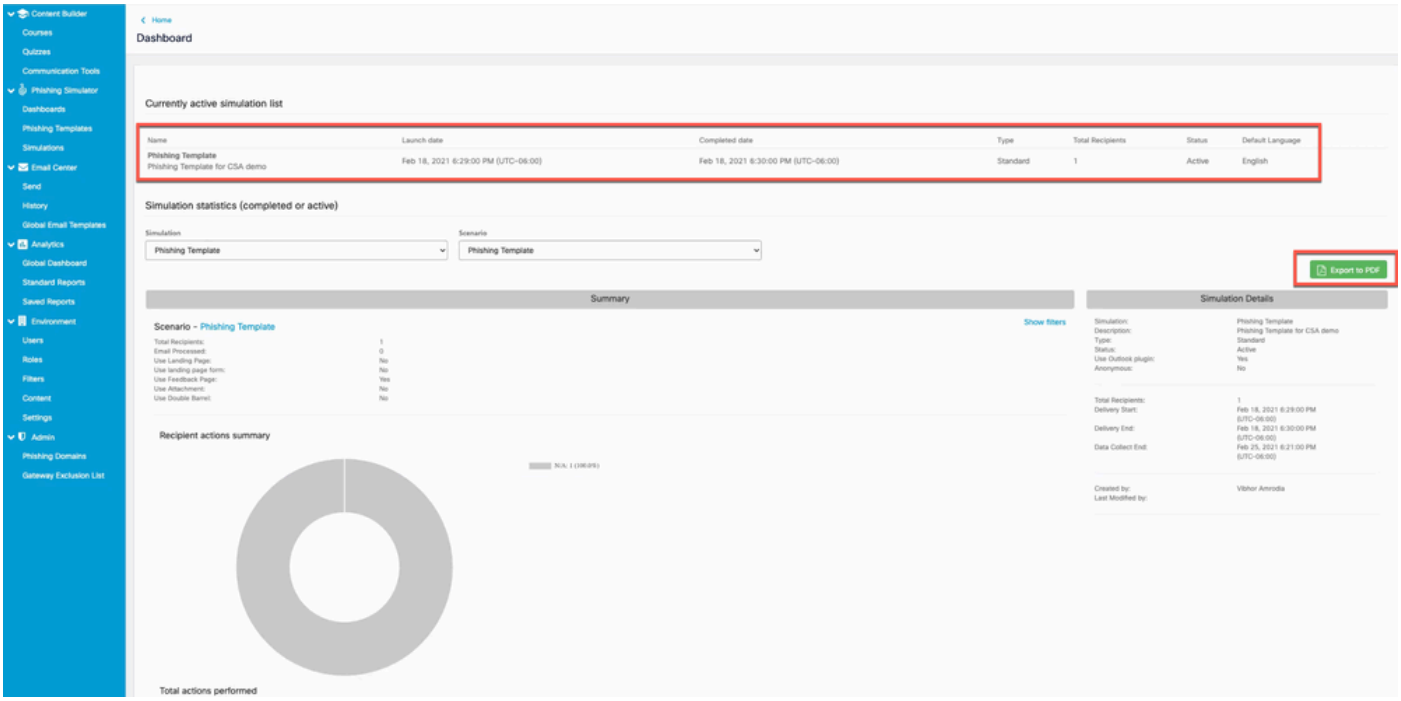
Nach dem Klicken auf die Schaltfläche zum Starten kann ein Zwei-Faktor-Authentifizierungscode angefordert werden. Geben Sie den Code ein, und klicken Sie auf, Launchwie im Bild dargestellt.



Screenshot des Popup-Fensters mit der Aufforderung, den Code für die Zwei-Faktor-Authentifizierung einzugeben

Schritt 5: Überprüfung aktiver Simulationen

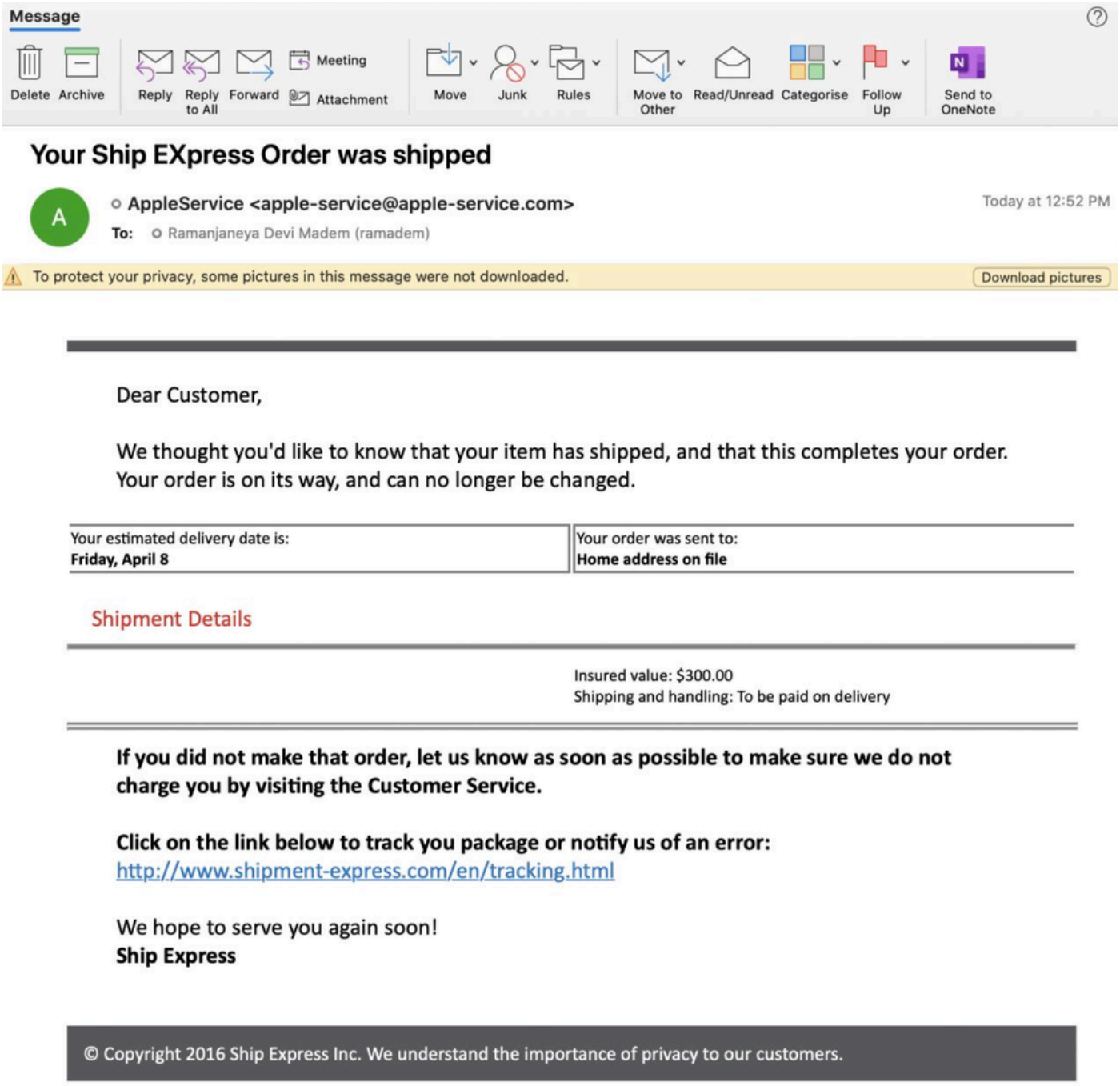
Navigieren Sie zu .Phishing Simulator > Dashboards Die aktive Simulationsliste liefert die aktiven Simulationen. Sie können auch auf Export as PDF klicken und erhalten den gleichen Bericht wie im Bild angezeigt.



Screenshot des Dashboards mit Phishing-Simulationen

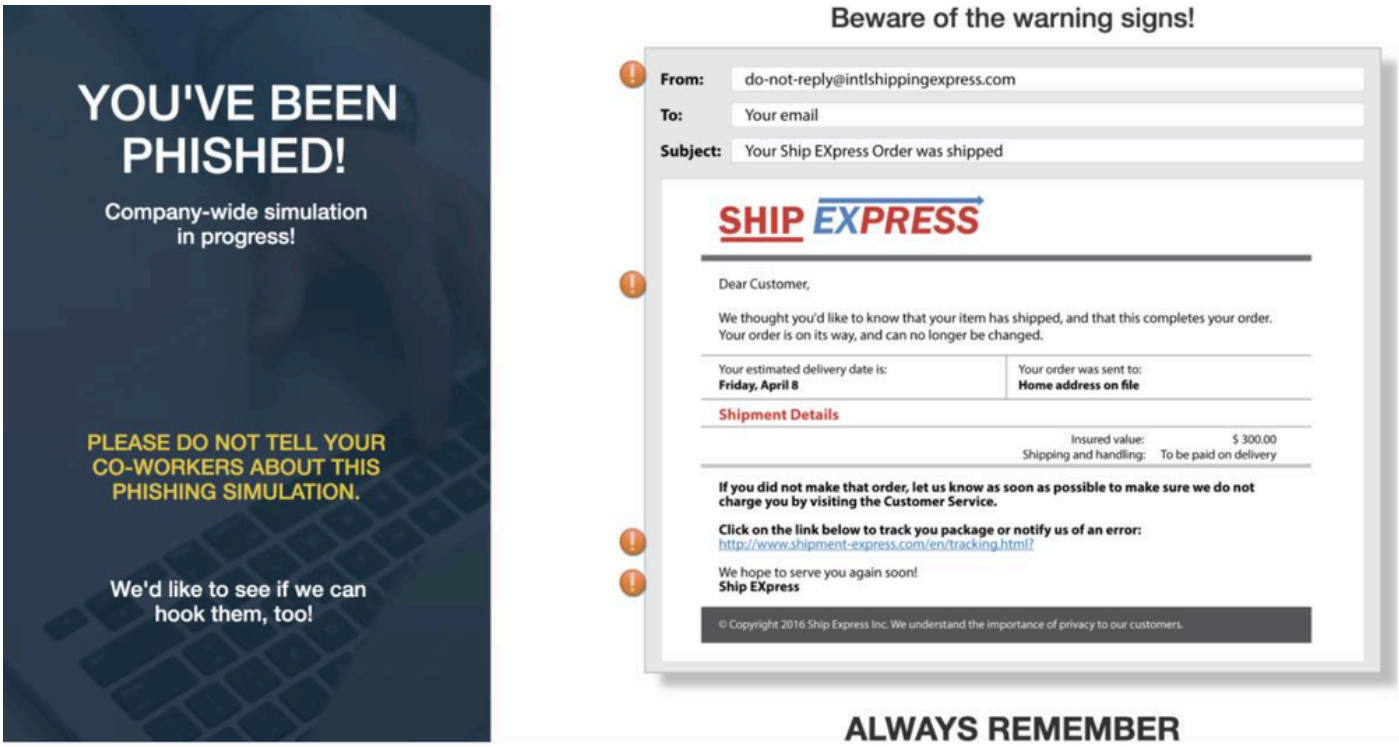
Was sieht man auf der Seite des Empfängers?

Beispiel einer Phishing-Simulations-E-Mail im Empfängereingang.



Beispiel einer simulierten Phishing-E-Mail in einer Benutzer-Mailbox

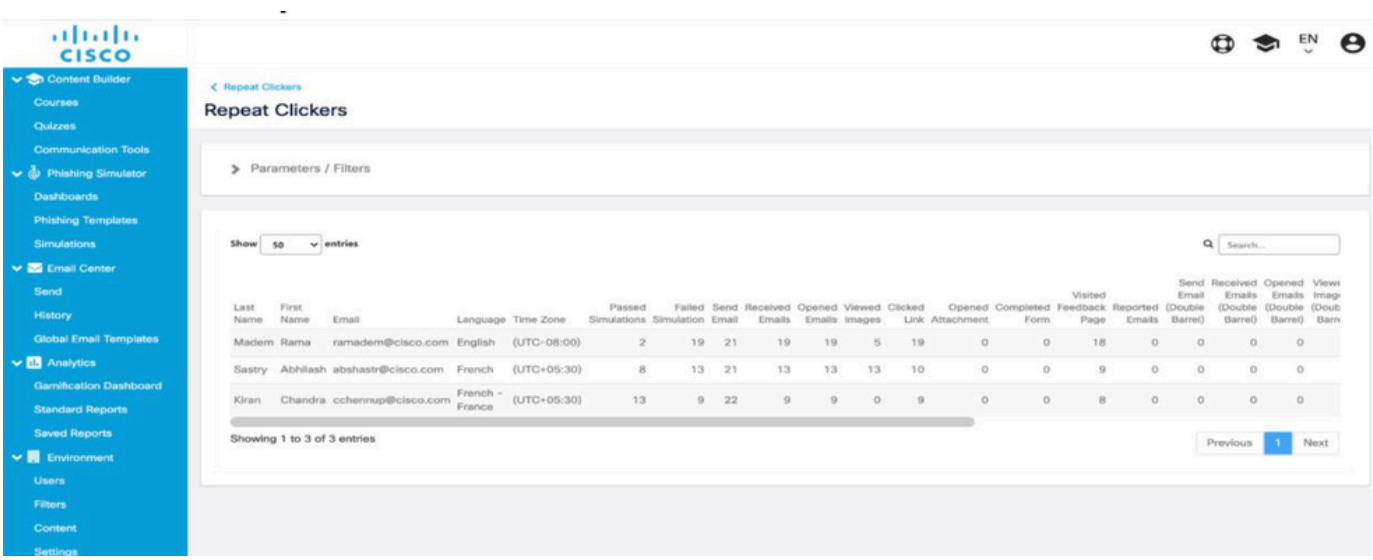
Wenn der Empfänger auf die URL klickt, wird dem Benutzer diese Feedback-Seite angezeigt, und dieser Benutzer wird als Teil der Liste "Repeat Clickers" (Clicker wiederholen, die frei auf die Phishing-URL geklickt haben) in CSA angezeigt.



Beispiel für die Feedbackseite, die der Benutzer nach dem Klicken auf die URL in der Phishing-E-Mail sieht.

Überprüfung auf CSA

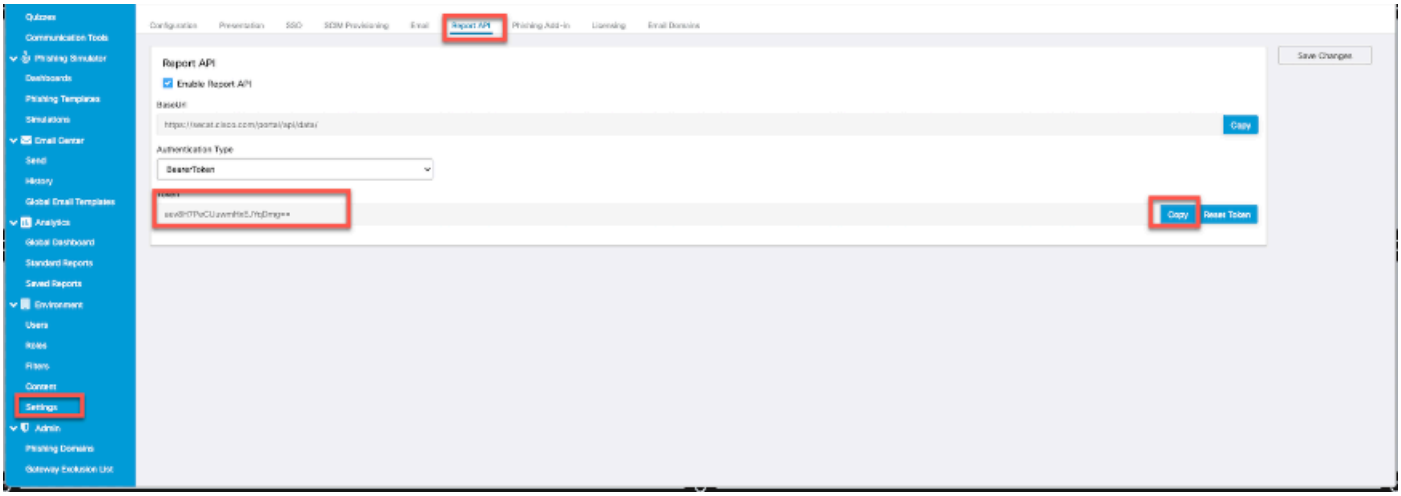
Die Liste Repeat Clickers wird angezeigt unterAnalytics > Standard Reports > Phishing Simulations > Repeat Clickersas shown in the image.



Screenshot der Seite "Repeat Clickers"

Konfigurieren des sicheren E-Mail-Gateways

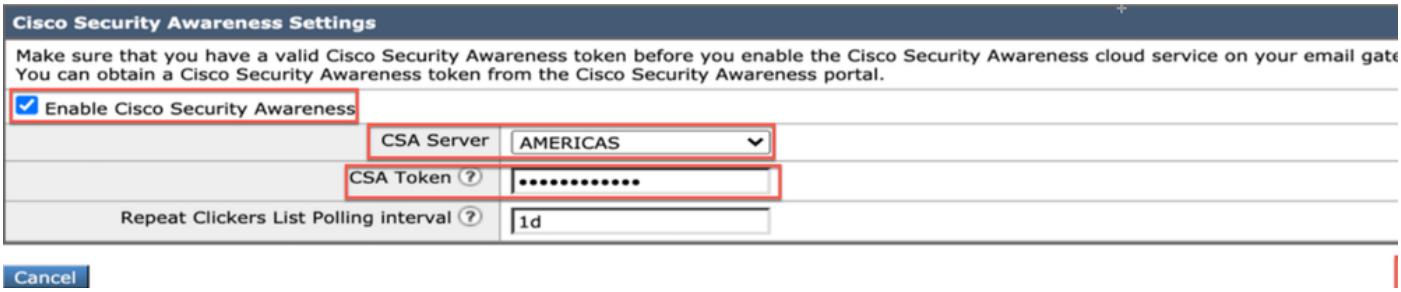
Anmerkung: Im Abschnitt Create and Send Phishing Simulations von CSA Cloud Service Schritt 3. haben Sie bei Aktivierung Report API das Trägertoken notiert. Halten Sie das bereit!



Screenshot der Seite unter Report API, auf der der Administrator das Trägertoken finden kann

Schritt 1: Aktivieren der Cisco Security Awareness-Funktion im sicheren E-Mail-Gateway

Navigieren Sie auf der Benutzeroberfläche des sicheren E-Mail-Gateways zu Security Services > Cisco Security Awareness > Enable . Enter the Region and the CSA Token (Bearer Token, erhalten vom CSA Cloud Service, wie in der zuvor erwähnten Anmerkung gezeigt), und senden Sie die Änderungen ein, und bestätigen Sie sie.



Screenshot der Seite mit den Cisco Security Awareness-Einstellungen auf dem Cisco Secure Email Gateway

CLI-Konfiguration

Geben Sie csaconfig ein, um CSA über die CLI zu konfigurieren.

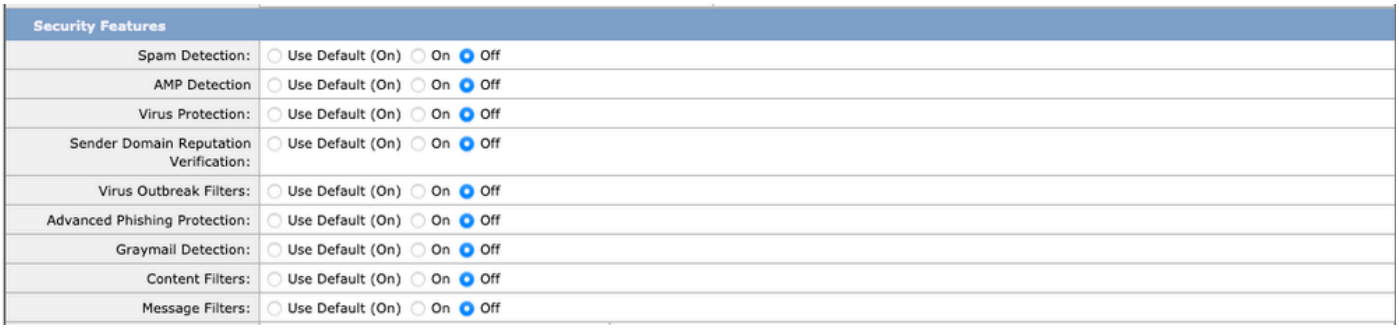
```
ESA (SERVICE)> csaconfig


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]>
```

Schritt 2: Simulierte Phishing-E-Mails vom CSA Cloud Service zulassen

---

Anmerkung: Die CYBERSEC_AWARENESS_ALLOWED Mailflow-Richtlinie wird standardmäßig erstellt, wobei alle Scan-Engines wie hier dargestellt deaktiviert sind.



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

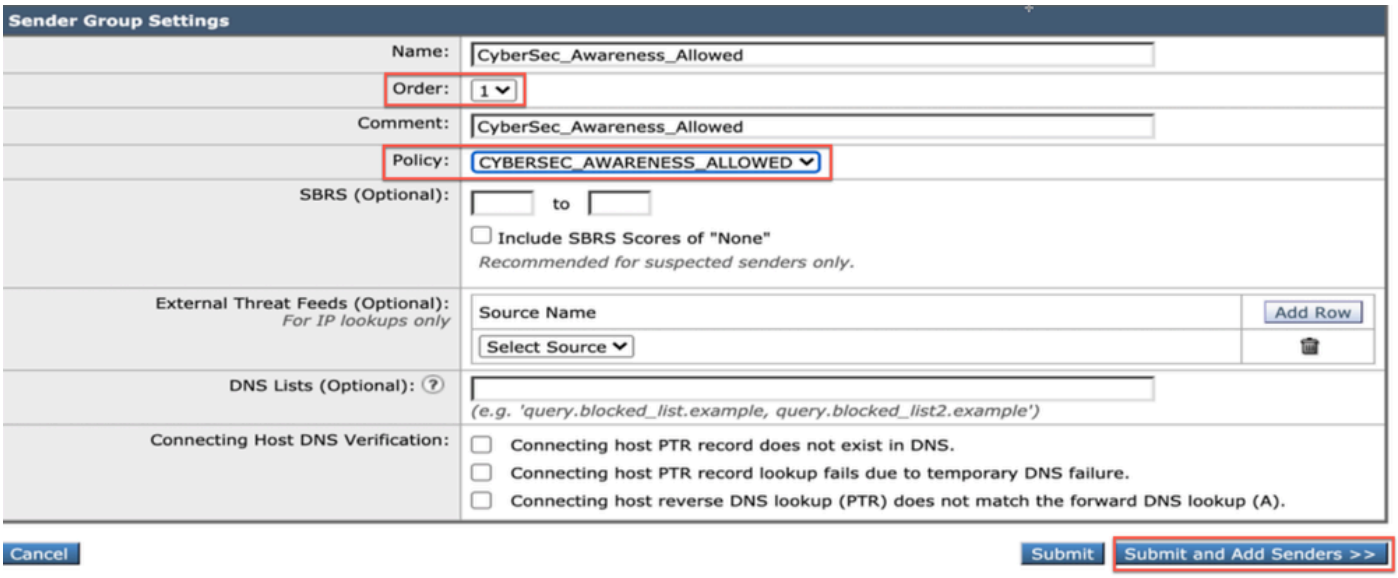
Screenshot der "CYBERSEC_AWARENESS_ALLOWED"-Mail Flow-Richtlinie mit deaktivierten Sicherheitsfunktionen

So lassen Sie simulierte Phishing-Kampagnen-E-Mails vom CSA Cloud Service zu, um alle Scan-Engines auf Secure Email Gateway zu umgehen:

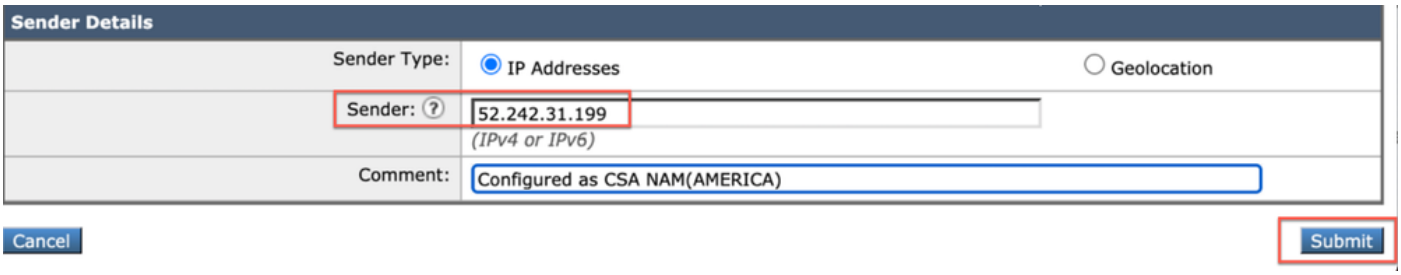
antwort: Erstellen Sie eine neue Absendergruppe, und weisen Sie die CYBERSEC_AWARENESS_ALLOWED Mail Flow-Richtlinie zu. Navigieren Sie zu Mail Policies > HAT Overview > Add Sender Group , wählen Sie die Richtlinie aus, und legen Sie die Reihenfolge auf 1 fest CYBERSEC_AWARENESS_ALLOWED. Submit and Add Senders.

b. Fügen Sie einen Absender IP/domain oderGeo Locationeinen Absender hinzu, von dem aus die Phishing-Kampagnen-E-Mails initiiert werden.

Navigieren Sie zuMail Polices > HAT Overview > Add Sender Group > Submit and Add Senders > Add the sender IP > SubmitundCommitändern Sie die im Bild angezeigten Änderungen.



Screenshot einer Absendergruppe "CyberSec_Awareness_Allowed", bei der die Mail Flow-Richtlinie "CYBERSEC_AWARENESS_ALLOWED" ausgewählt wurde.



Screenshot der Seite mit den Cisco Security Awareness-Einstellungen auf dem Cisco Secure Email Gateway

CLI-Konfiguration:

1. Navigieren Sie zu listenerconfig > Edit > Inbound (PublicInterface) > HOSTACCESS > NEW > New Sender Group .

2. Erstellen Sie eine neue Absendergruppe mitCYBERSEC_AWARENESS_ALLOWEDE-Mail-Richtlinie, und fügen Sie eine Absender-IP/Domäne hinzu, von der aus die E-Mails der Phishing-Kampagne initiiert werden.

3. Legen Sie die Reihenfolge der neuen Absendergruppe auf 1 fest, und verwenden Sie dieMoveOption unter listenerconfig > EDIT > Inbound (PublicInterface) > HOSTACCESS > MOVE .

4. Verpflichten.

Anmerkung: Die Absender-IP ist die IP-Adresse des CSA und basiert auf der ausgewählten Region. Die richtige IP-Adresse finden Sie in der Tabelle. Lassen Sie diese IP-Adressen/Hostnamen in der Firewall mit der Portnummer 443 für SEG 14.0.0-xxx zu, um eine Verbindung mit dem CSA-Cloud-Service herzustellen.

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	

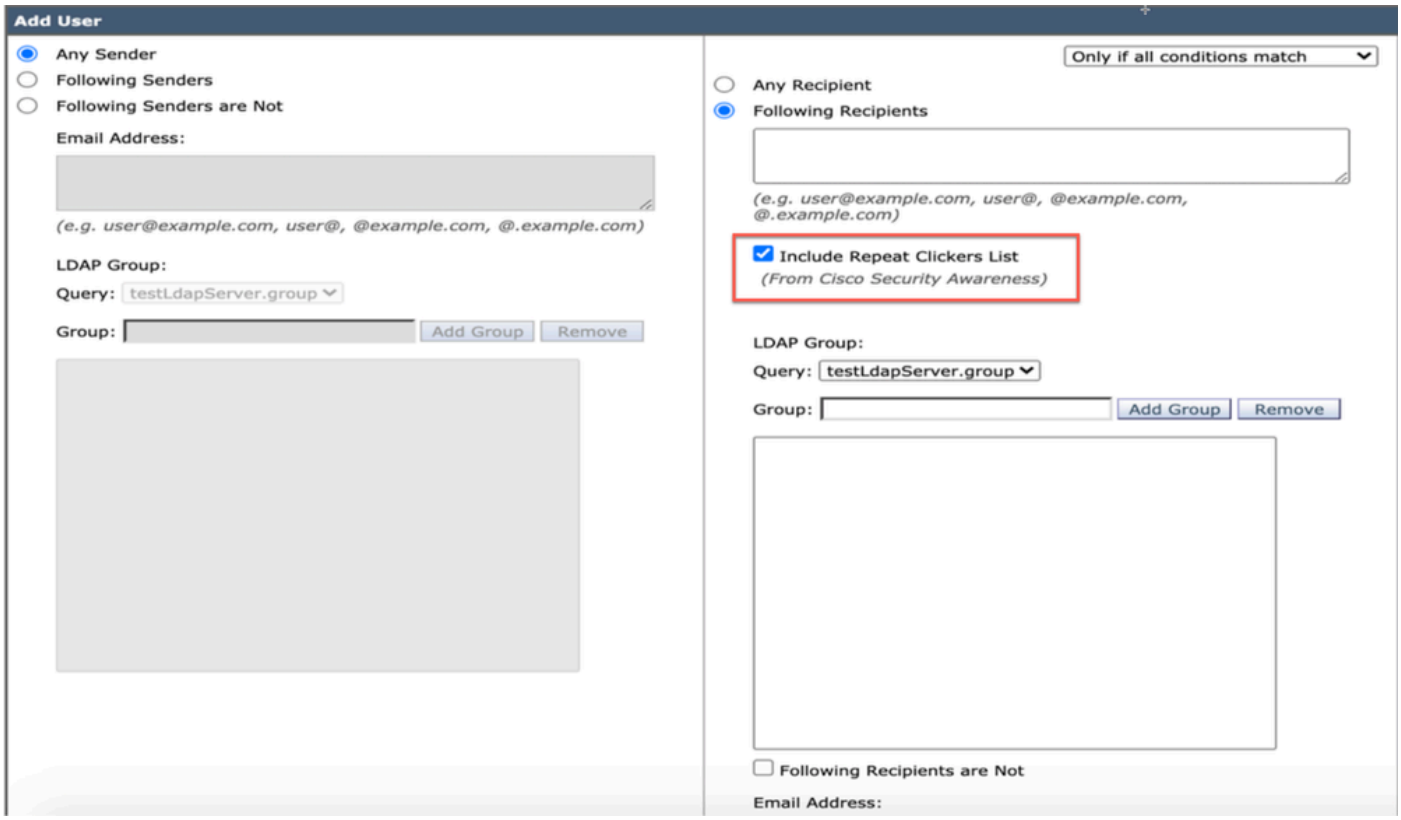
Screenshot der IP-Adressen und Hostnamen der CSA Americas- und EU-Regionen

Schritt 3. Ergreifen Sie Maßnahmen auf Repeat Clicker von SEG

Sobald die Phishing-E-Mails versendet und die Liste der wiederholten Klicker in der SEG ausgefüllt wurde, kann eine aggressive Richtlinie für eingehende E-Mails erstellt werden, um Maßnahmen für E-Mails an diese spezifischen Benutzer zu ergreifen.

Erstellen Sie eine neue aggressive benutzerdefinierte Richtlinie für eingehende E-Mails, und aktivieren Sie Include Repeat Clickers List das Kontrollkästchen im Empfängerbereich.

Navigieren Sie in der GUI zu Mail Policies > Incoming Mail Policies > Add Policy > Add User > Include Repeat Clickers List > Submit , und ändern Sie Commit die Einstellungen.



Screenshot einer benutzerdefinierten Richtlinie für eingehende E-Mails, die so konfiguriert ist, dass sie für wiederholte Klicker bestimmte E-Mails verarbeitet

Leitfaden zur Fehlerbehebung

1. Navigieren Sie zu, csaconfig > SHOW_LISTum die Details der Liste der wiederholten Klicker anzuzeigen.

```
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. Navigieren Sie zu , csaconfig > UPDATE_LIST wenn Sie die Aktualisierung der Liste der wiederholten Klicker erzwingen möchten.

```
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.
```

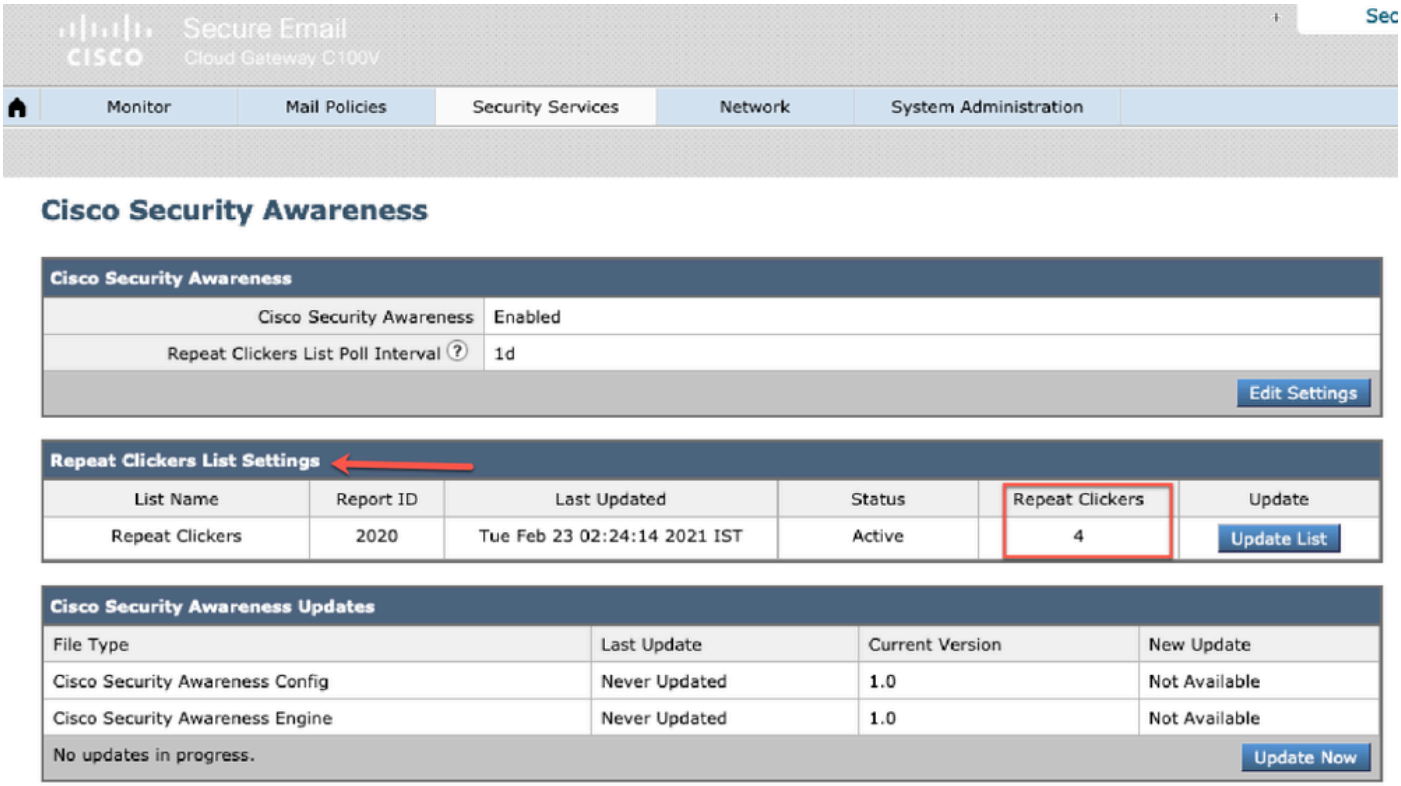
3. Überprüfen Sie in den CSA-Protokollen, ob die Liste der wiederholten Klicker heruntergeladen wurde oder ob ein Fehler vorliegt. Dies ist die working setup:

```
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. Die Anzahl der wiederholten Klicker ist auch in der GUI zu sehen. Navigieren Sie zu, wie im Bild dargestellt.Security Services > Cisco Security Awareness



Screenshot der Seite Security Services > Cisco Security Awareness mit Angabe der Anzahl der wiederholten Klicker

Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.