Cisco Secure Email Gateway와 보안 인식 통합 구성

목차

소개

이 문서에서는 Cisco CSA(Security Awareness)와 Cisco Secure Email Gateway의 통합을 구성하는 데 필요한 단계를 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Email Gateway 개념 및 컨피그레이션
- CSA 클라우드 서비스

사용되는 구성 요소

이 문서의 정보는 AsyncOS for SEG 14.0 이상을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

CSA 클라우드 서비스에서 피싱 시뮬레이션 생성 및 전송

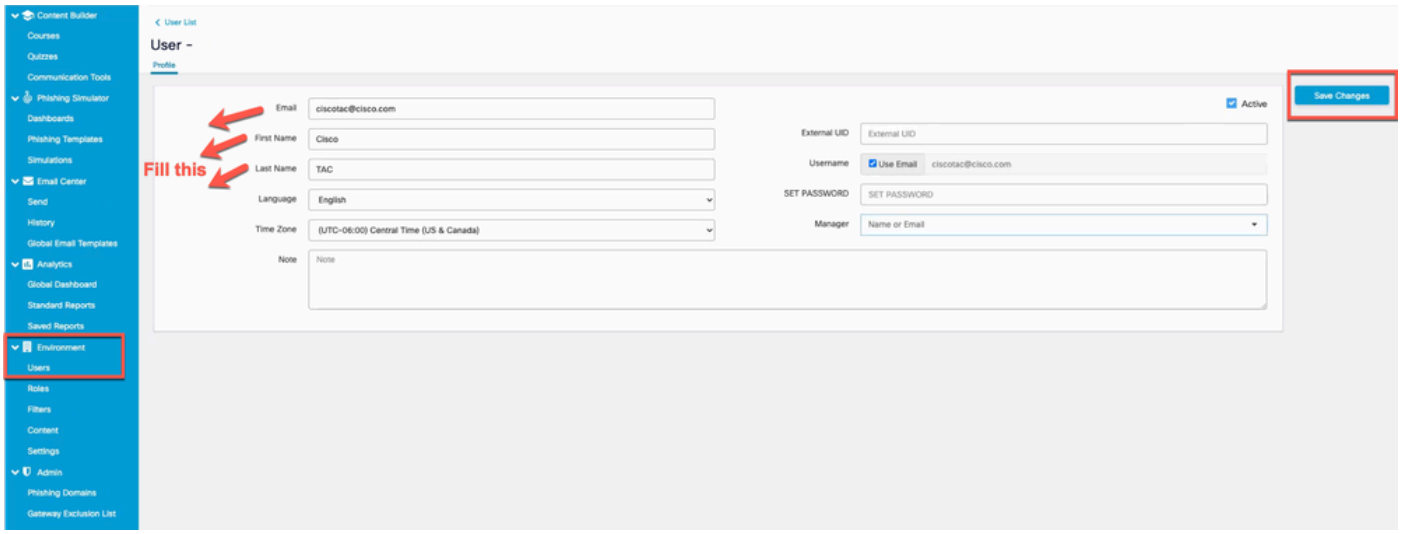
1단계. CSA 클라우드 서비스에 로그인합니다.

참조:
1. https://secat.cisco.com/(미주 지역)

2 . 유럽 지역의 경우 https://secat-eu.cisco.com/

2단계. 피싱 이메일 수신자 생성

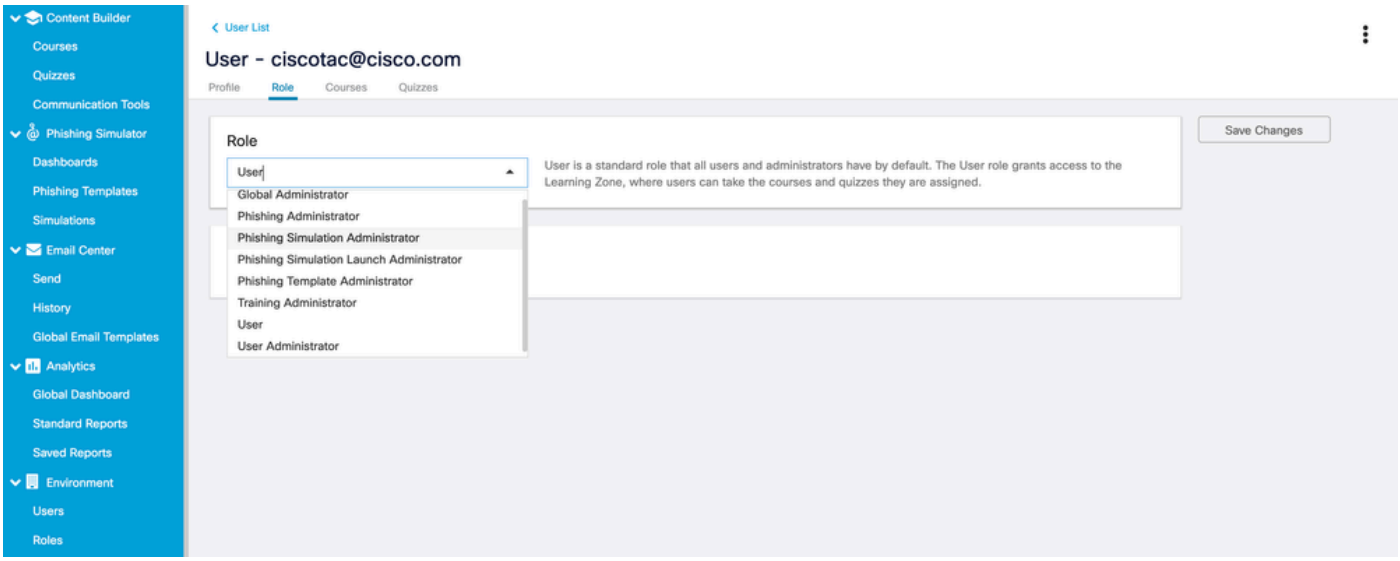
Email(이메일), First Name(이름), Last Name(성) 및 Language(언어) 필드로 **Environment** > **Users** > **Add New User** 이동하여 입력한 다음 이미지**Save Changes**와 같이 클릭합니다.



새 사용자를 추가하기 위한 사용자 인터페이스 페이지의 스크린샷

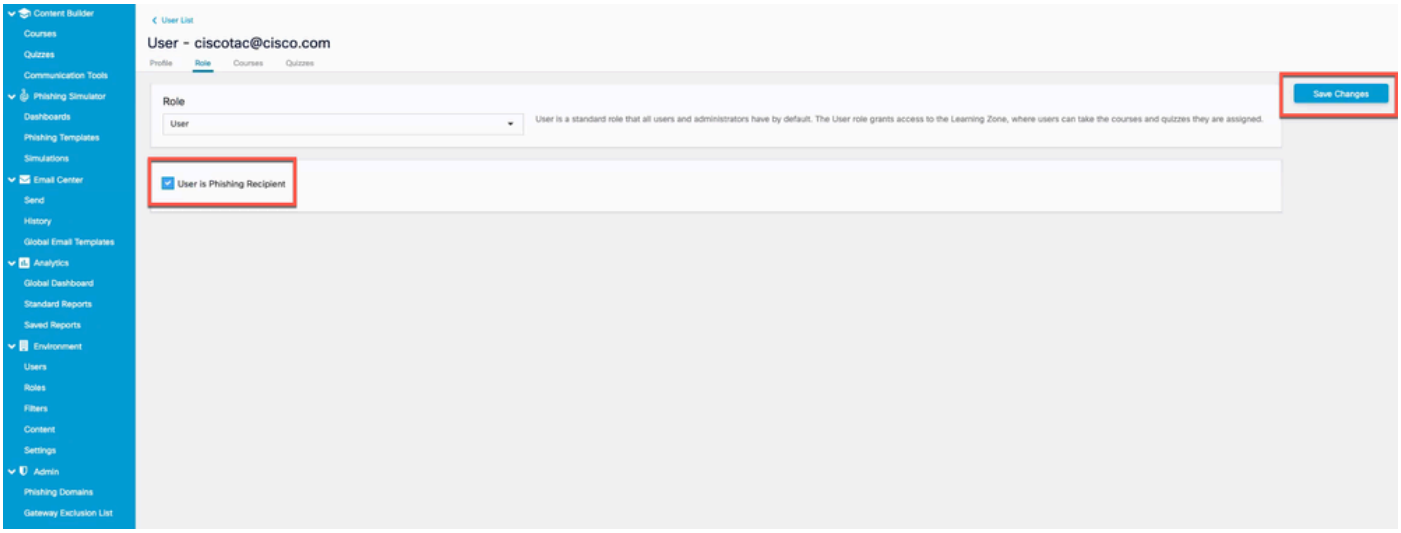
참고: 시뮬레이션을 생성하고 실행할 권한이 있는 CSA 관리자 사용자에 대해서만 비밀번호를 설정해야 합니다.

사용자가 생성되면 사용자의 역할을 선택할 수 있습니다. 이 이미지에 표시된 대로 드롭다운에서 역할을 선택할 수 있습니다.



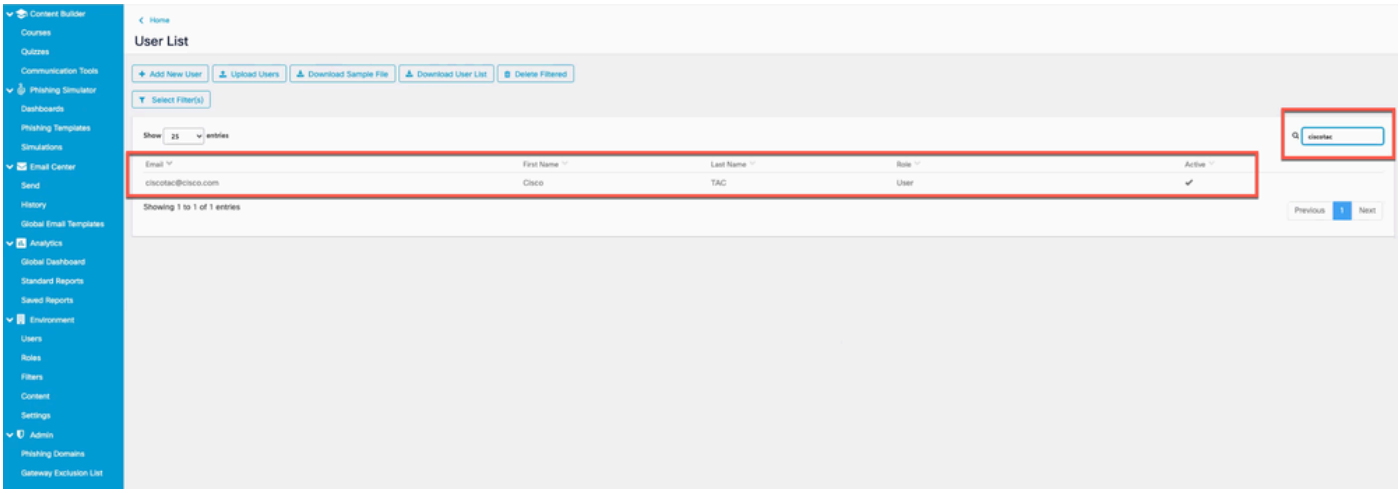
사용자 역할 보기 드롭다운 옵션

이미지에 표시된User is Phishing Recipient > Save Changes확인란을 선택합니다.



"사용자가 피싱 수신자임" 확인란이 활성화된 스크린샷

사용자가 성공적으로 추가되었고 이미지에 표시된 것처럼 Filter(필터)의 이메일 주소를 기준으로 검색하면 나열되는지 확인합니다.

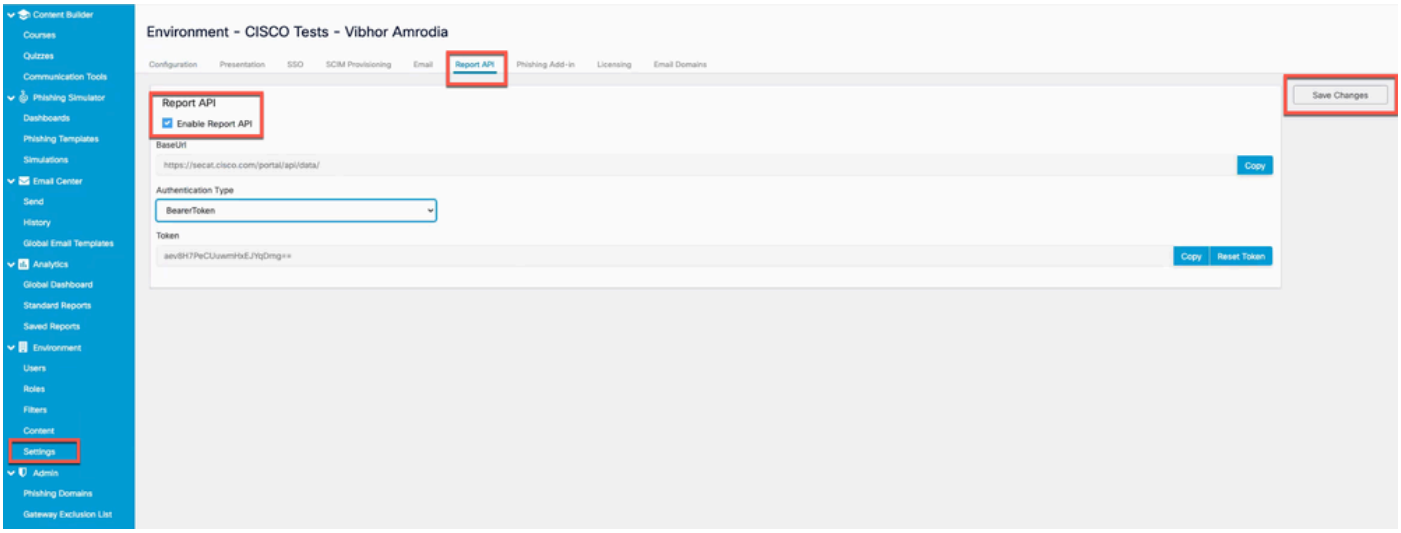


사용자 목록에 있는 새 사용자의 스크린샷

3단계. 보고서 API 활성화

탭으로Environments > Settings > Report API 이동하여 선택합니다Enable Report API > Save Changes .

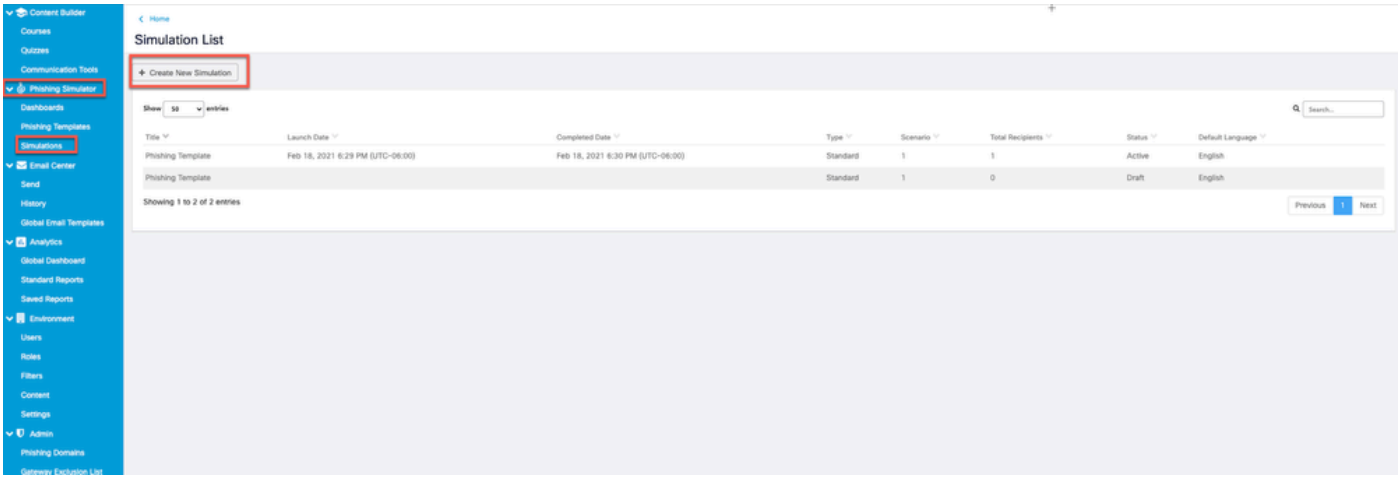
참고: Bearer Token을 기록해 두십시오. CSA와 SEG를 통합하려면 이 기능이 필요합니다.



"Enable Report API(보고서 API 활성화)" 확인란이 활성화된 스크린샷

4단계. 피싱 시뮬레이션 생성

a. 그림과 같이 사용 가능한Phishing Simulator > Simulations > Create New Simulation 목록에서Template원하는 항목을 찾아 선택합니다.

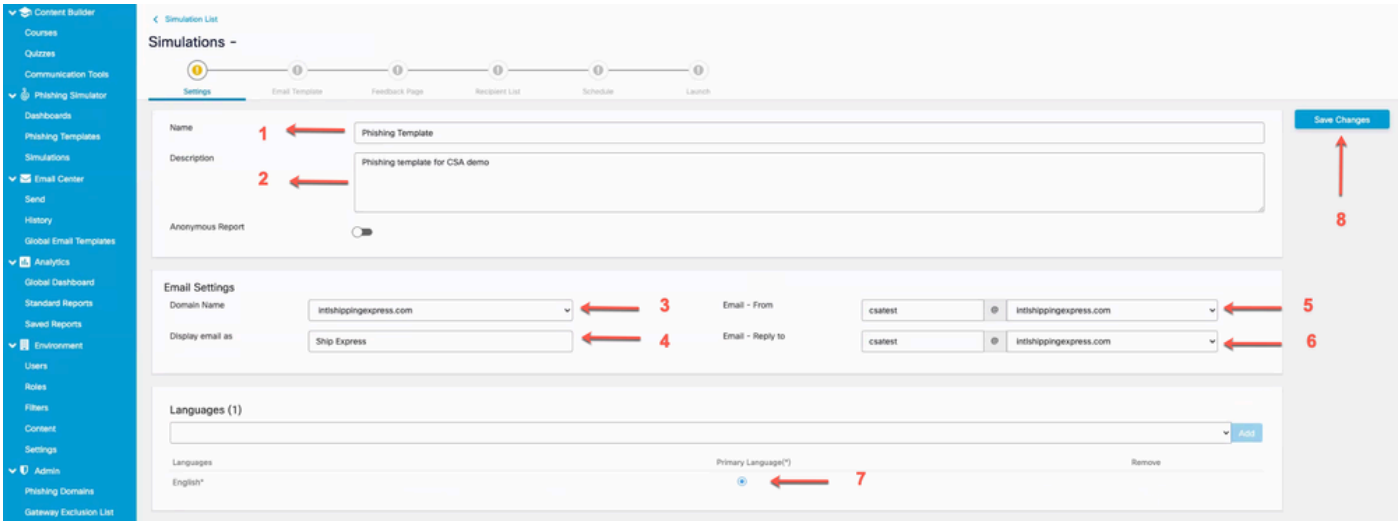


"Create New Simulation(새 시뮬레이션 생성)" 버튼을 강조하는 스크린샷

b. 다음 정보를 입력합니다.

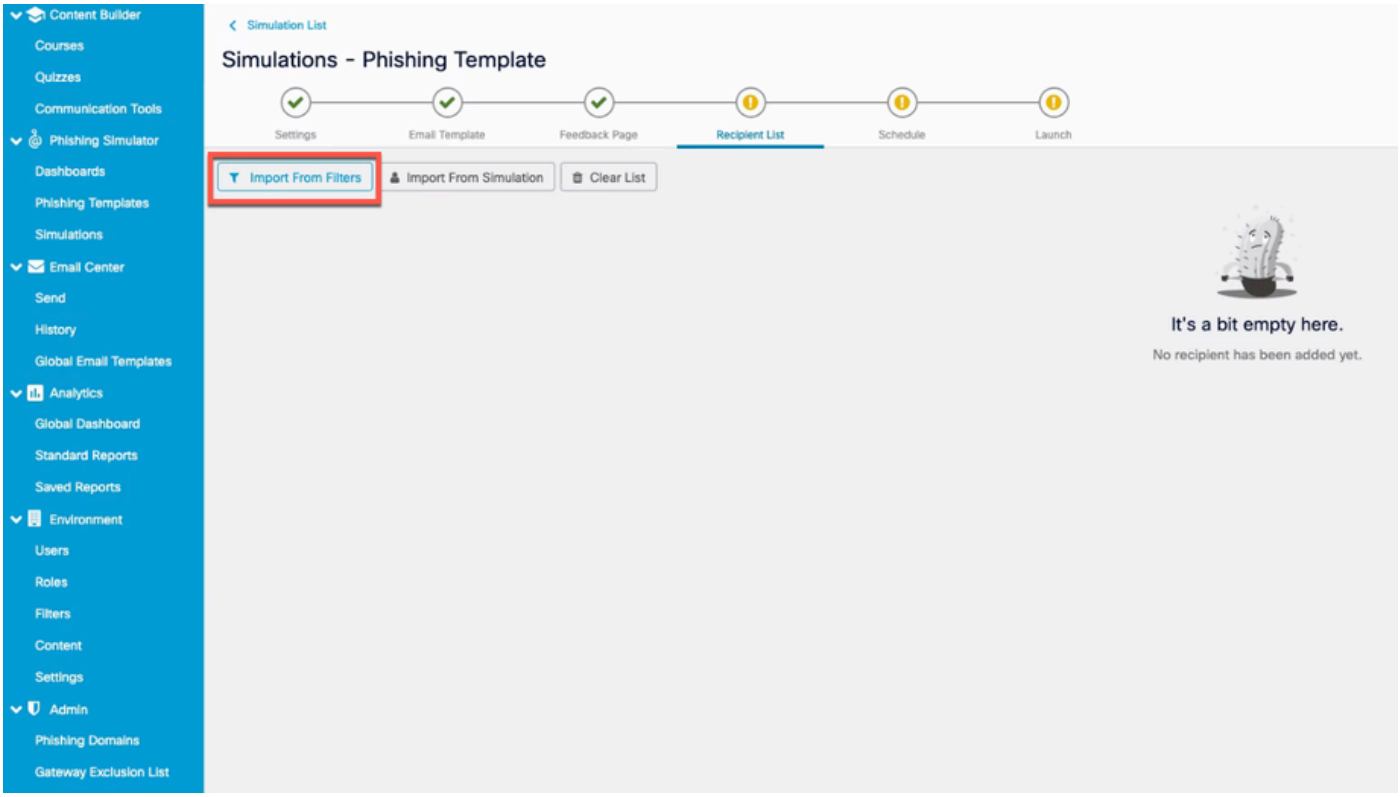
1. 템플릿의 이름을 선택합니다.
2. 템플릿에 대해 설명합니다.

3. 피싱 이메일이 전송되는 도메인 이름입니다.
4. 피싱 이메일의 표시 이름입니다.
5. 이메일 발신 주소(드롭다운에서 선택)
6. 회신 주소(드롭다운에서 선택)
7. 언어를 선택합니다.
8. 변경 사항을 저장합니다.



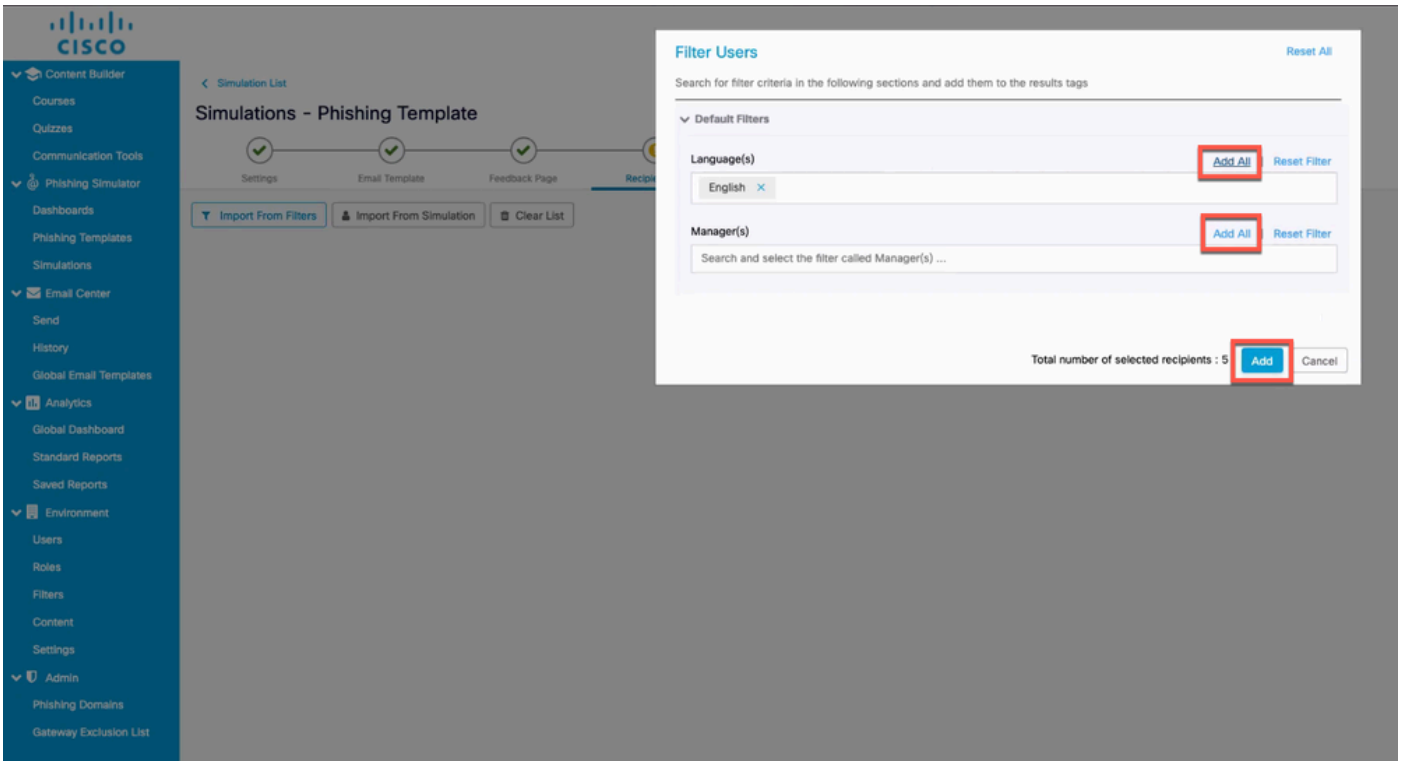
새 시뮬레이션 구성을 위해 채워야 하는 필드를 강조 표시하는 스크린샷

c. 를 클릭하고 이미지Import from Filters 에 표시된Recipient List대로 피싱 이메일 수신자를에 추가합니다.



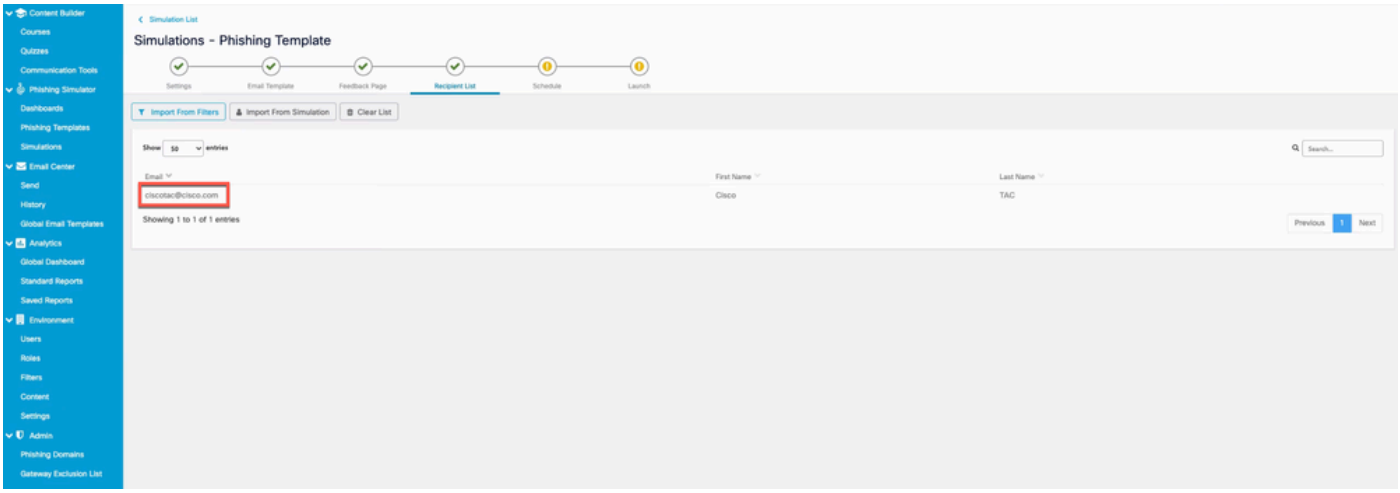
"Import from Filters(필터에서 가져오기)" 버튼을 강조 표시한 스크린샷

사용자를 언어 또는 관리자로 필터링할 수 있습니다. 이미지에Add 표시된 대로 를 클릭합니다.



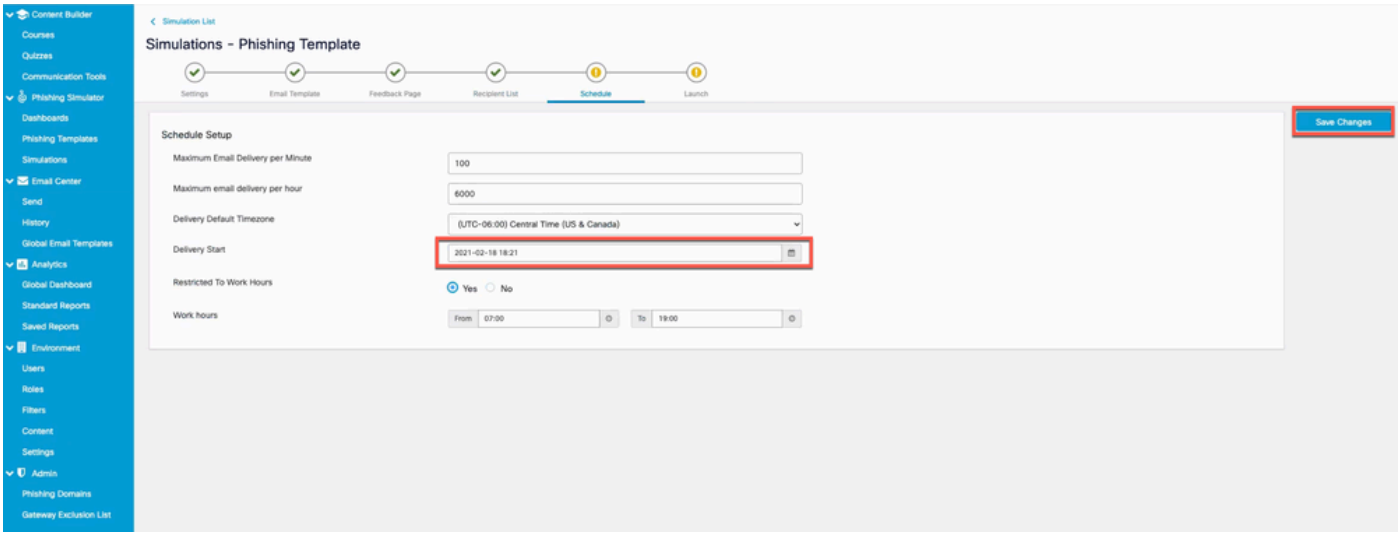
언어 또는 관리자별로 필터링할 수 있는 Filter Users(사용자 필터링) 대화 상자의 스크린샷

다음은 2단계에서 생성한 사용자의 예입니다. 이제 이미지에 표시된 대로 수신자 목록에 추가됩니다.



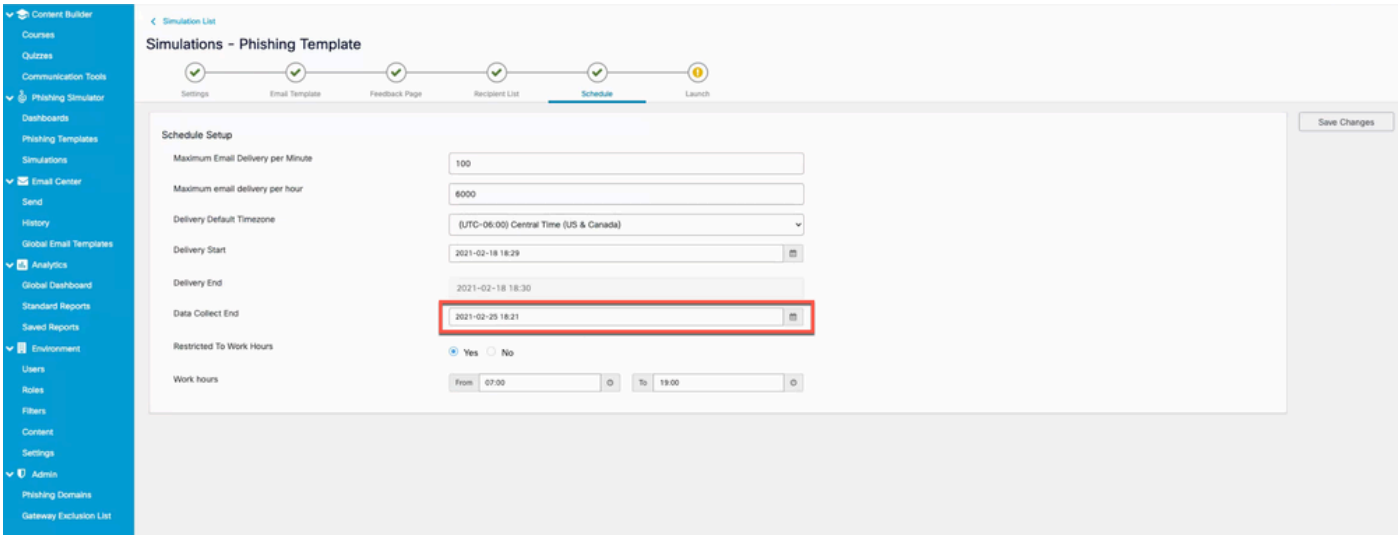
피싱 시뮬레이션의 수신자로 앞서 생성한 사용자의 스크린샷

d. 이미지Delivery Start에 표시된 대로 캠페인 일정을 계획하도록 날짜 및Save 변경 사항을 설정합니다.



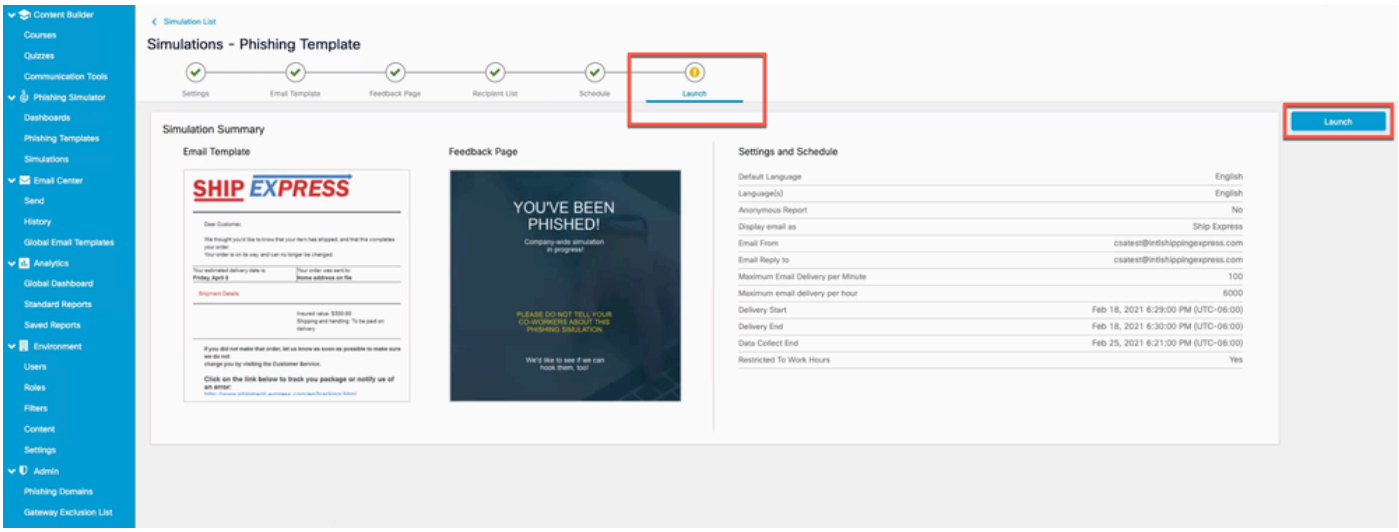
Delivery start(제공 시작) 필드를 강조하는 스크린샷

시작 날짜를 선택하면 이미지에 표시된 것처럼 캠페인end date 에 대한 선택 옵션이 활성화됩니다.



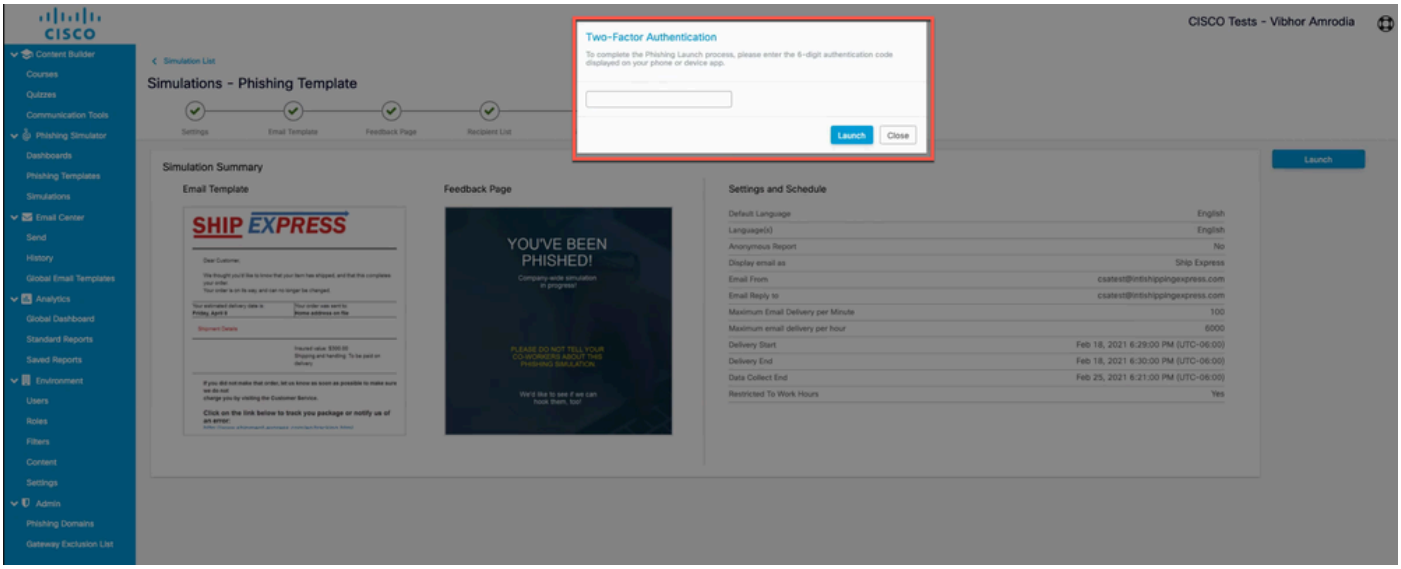
시뮬레이션을 종료해야 하는 시점을 지정하는 Data Collect End(데이터 수집 종료) 필드를 강조 표시하는 스크린 샷

e. 이미지Launch 에 표시된 것처럼 캠페인을 시작하려면 클릭합니다.



캠페인을 시작할 수 있는 시뮬레이션 생성 마법사의 마지막 탭의 스크린샷

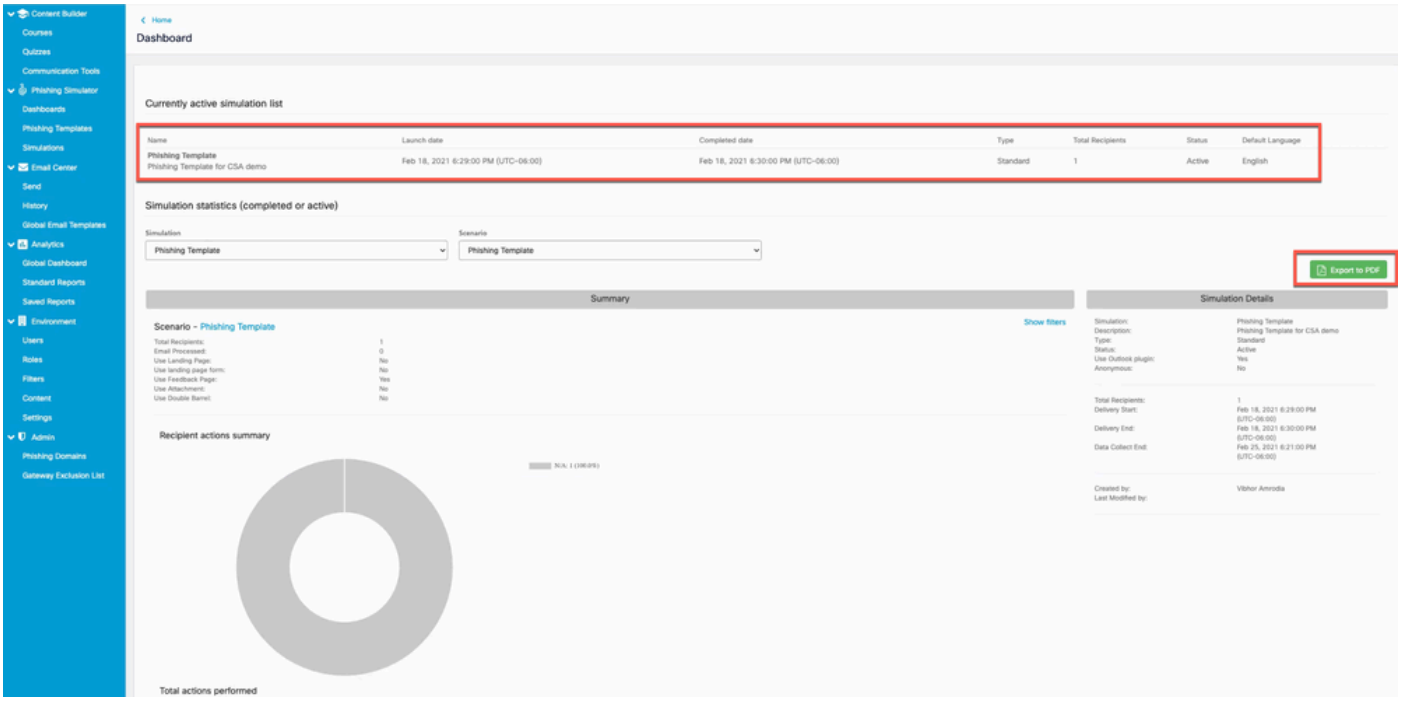
2단계 인증 코드는 시작 버튼을 클릭한 후에 요청할 수 있습니다. 코드를 입력하고 이미지에Launch표시된 대로 클릭합니다.



Two Factor Authentication 코드를 요청하는 팝업의 스크린샷

5단계. 활성 시뮬레이션 확인

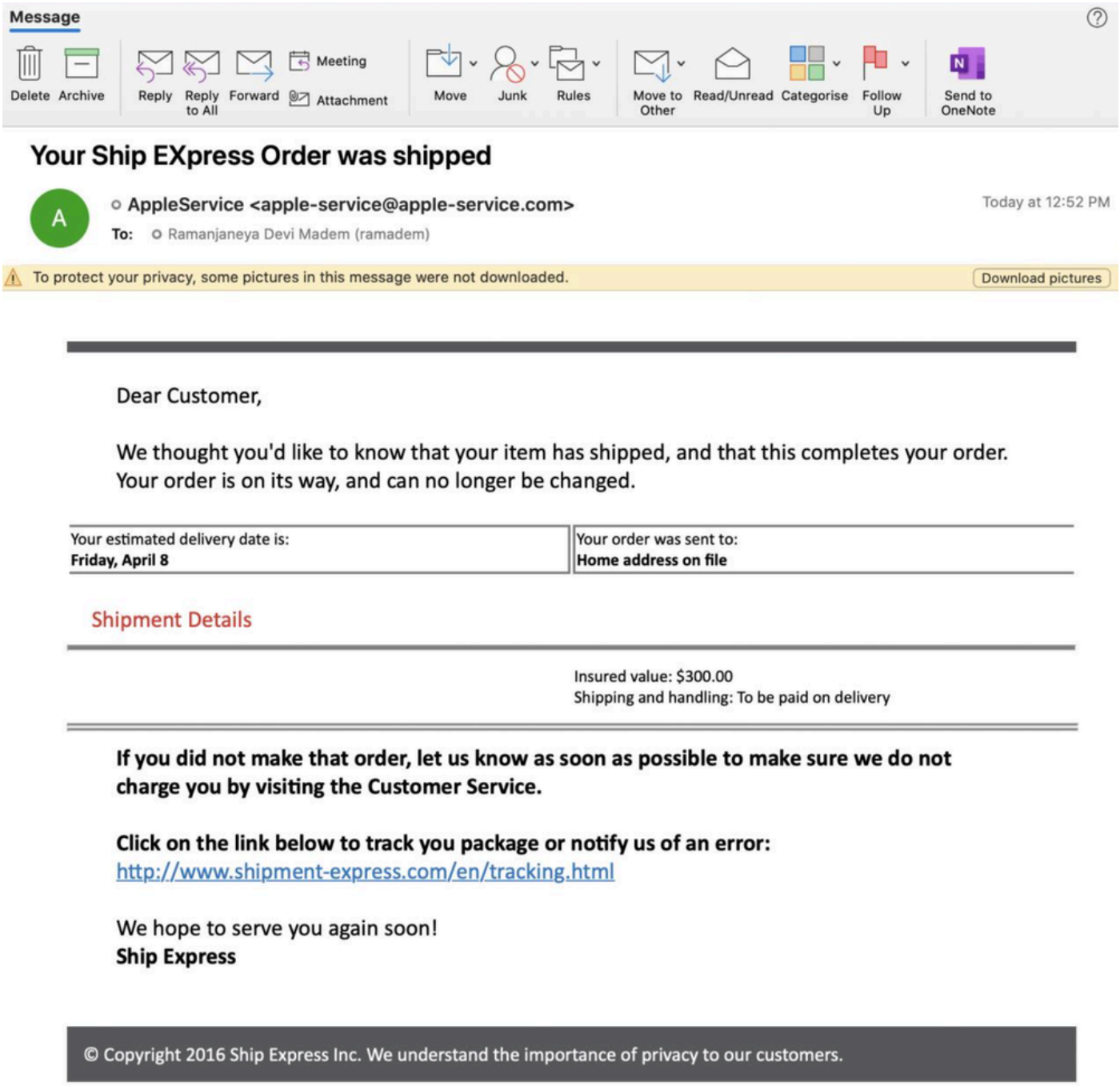
로 이동합니다.Phishing Simulator > Dashboards 현재 활성 시뮬레이션 목록은 활성 시뮬레이션을 제공합니다. 를 클릭하여 Export as PDF이미지에 표시된 것과 동일한 보고서를 가져올 수도 있습니다.



피싱 시뮬레이션 대시보드 스크린샷

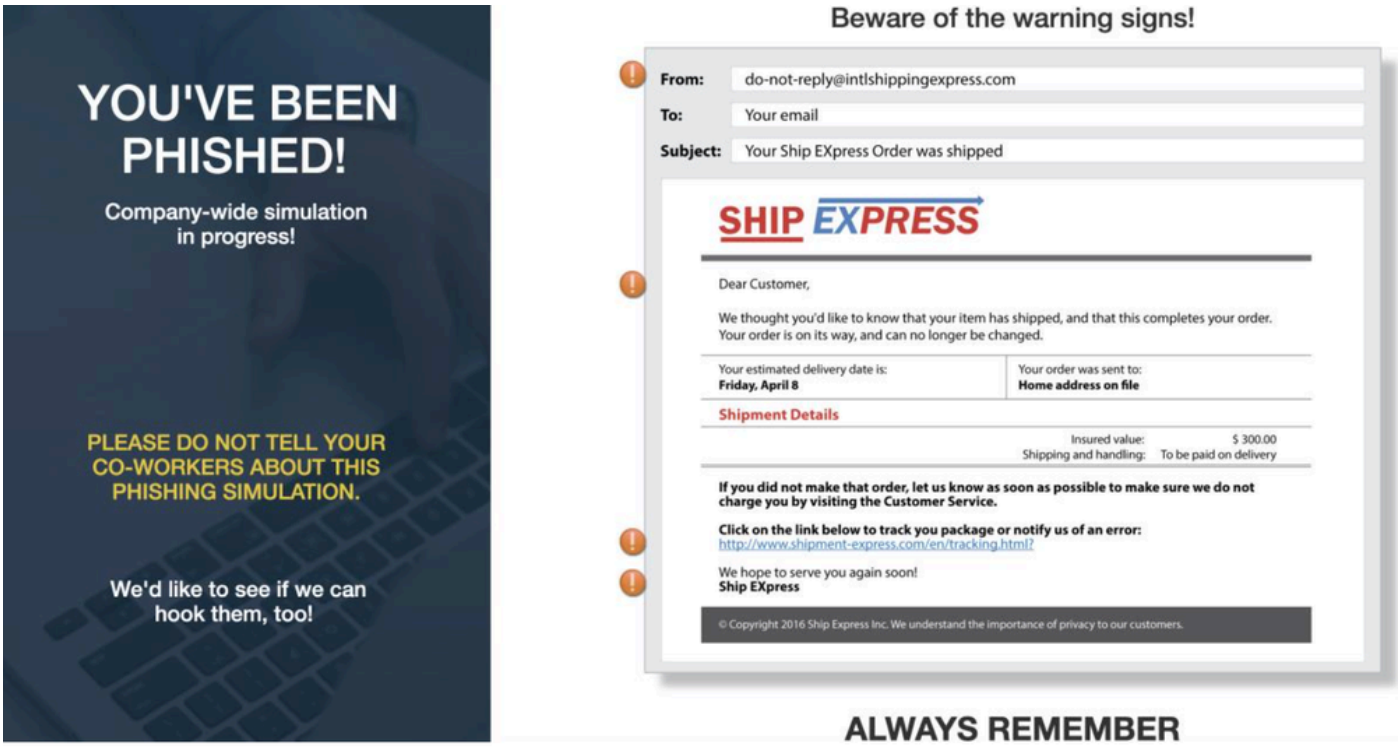
받는 사람 옆에는 무엇이 보이는가?

받는 사람 받은 편지함에 있는 피싱 시뮬레이션 이메일의 예.



사용자 사서함에 시뮬레이션된 피싱 이메일의 예

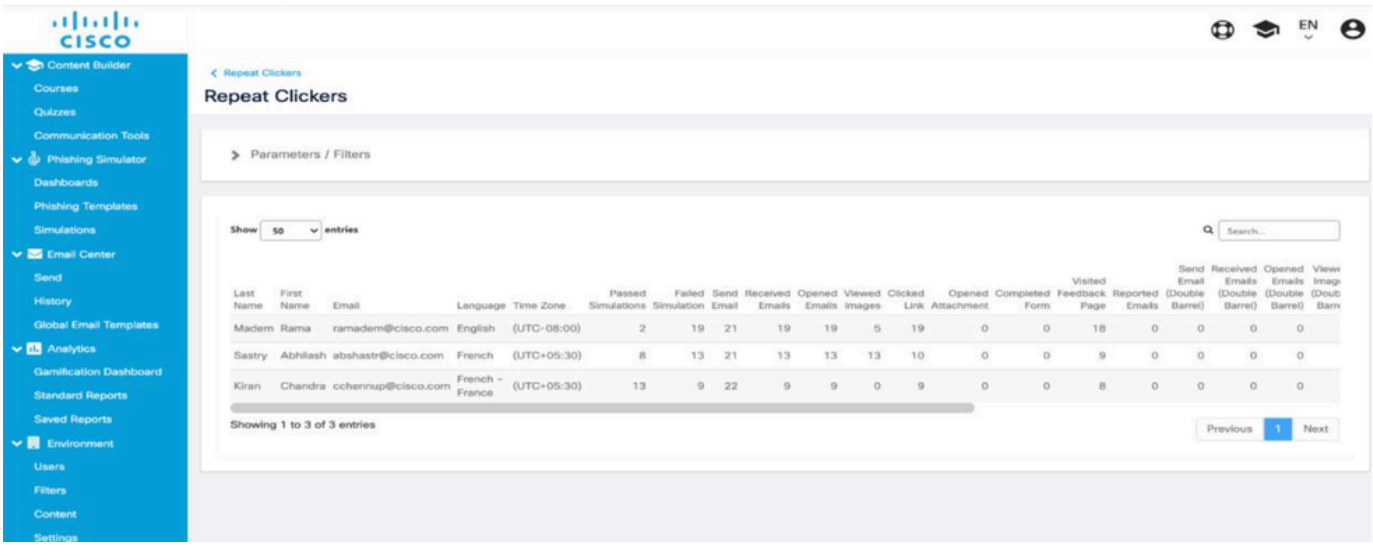
수신자가 URL을 클릭하면 이 피드백 페이지가 사용자에게 표시되고 이 사용자는 CSA의 반복 클릭커 목록(피싱 URL을 자유롭게 클릭한 사람)에 속합니다.



피싱 이메일에서 URL을 클릭하면 사용자에게 표시되는 피드백 페이지의 예

CSA에서 확인

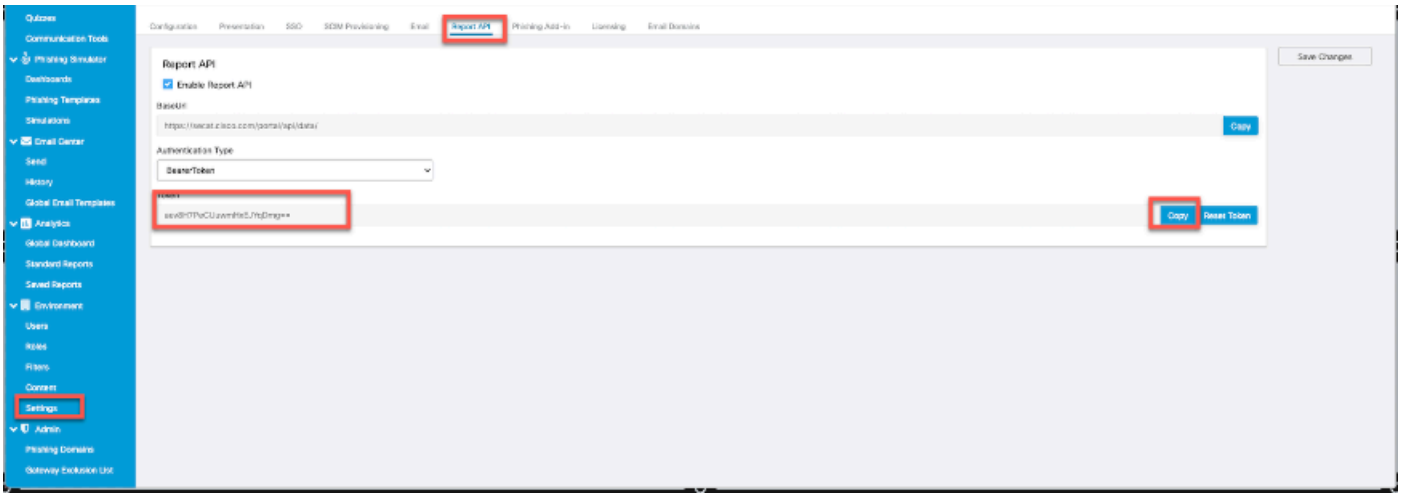
Repeat Clicker(반복 클릭커) 목록이 아래에 표시됩니다.Analytics > Standard Reports > Phishing Simulations > Repeat Clickersas shown in the image.



Repeat Clicker 페이지의 스크린샷

보안 이메일 게이트웨이 구성

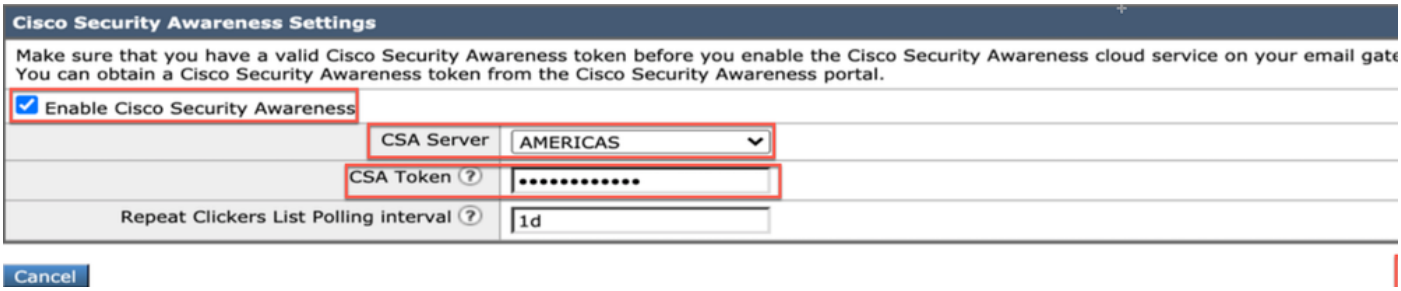
참고: CSA Cloud Service Step 3.의 섹션Create and Send Phishing Simulations아래에서Report APIBearer 토큰을 활성화하면 표시됩니다. 이 물건을 보관하세요.



관리자가 전달자 토큰을 찾을 수 있는 Report API(보고서 API) 아래의 페이지 스크린샷

1단계. Secure Email Gateway에서 Cisco Security Awareness Feature 활성화

Secure Email Gateway GUI에서 Enter the Region and the CSA Token(Bearer Token)(지역 및 CSA 토큰 입력(앞서 설명한 참고에서Security Services > Cisco Security Awareness > Enable . CSA Cloud Service에서 가져온 베어러 토큰)으로 이동하여 변경 사항을 제출하고 커밋합니다.



Cisco Secure Email Gateway의 Cisco Security Awareness 설정 페이지 스크린샷

CLI 구성

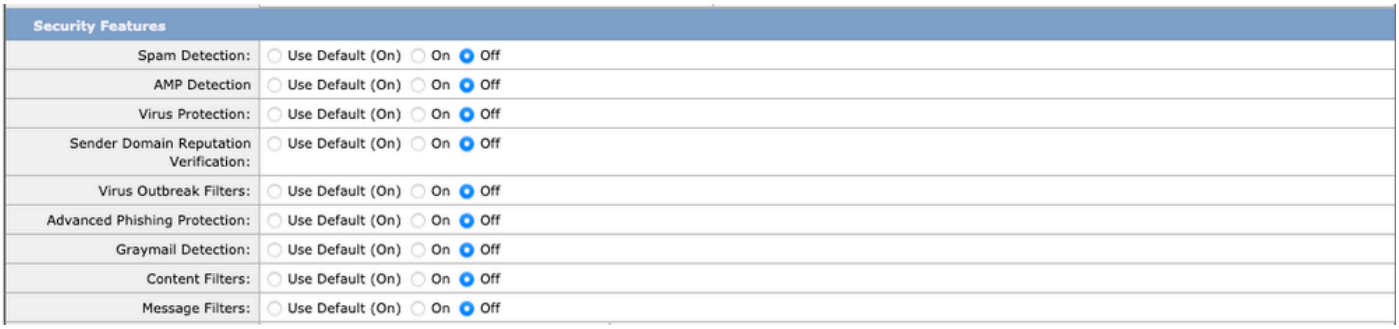
CLIcsaconfig 를 통해 CSA를 구성하려면 을 입력합니다.

```
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]>
```

2단계. CSA Cloud Service에서 시뮬레이션된 피싱 이메일 허용

참고: MailflowCYBERSEC_AWARENESS_ALLOWED정책은 기본적으로 모든 검사 엔진이 Off로 설정되어 여기에 표시된 대로 생성됩니다.



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

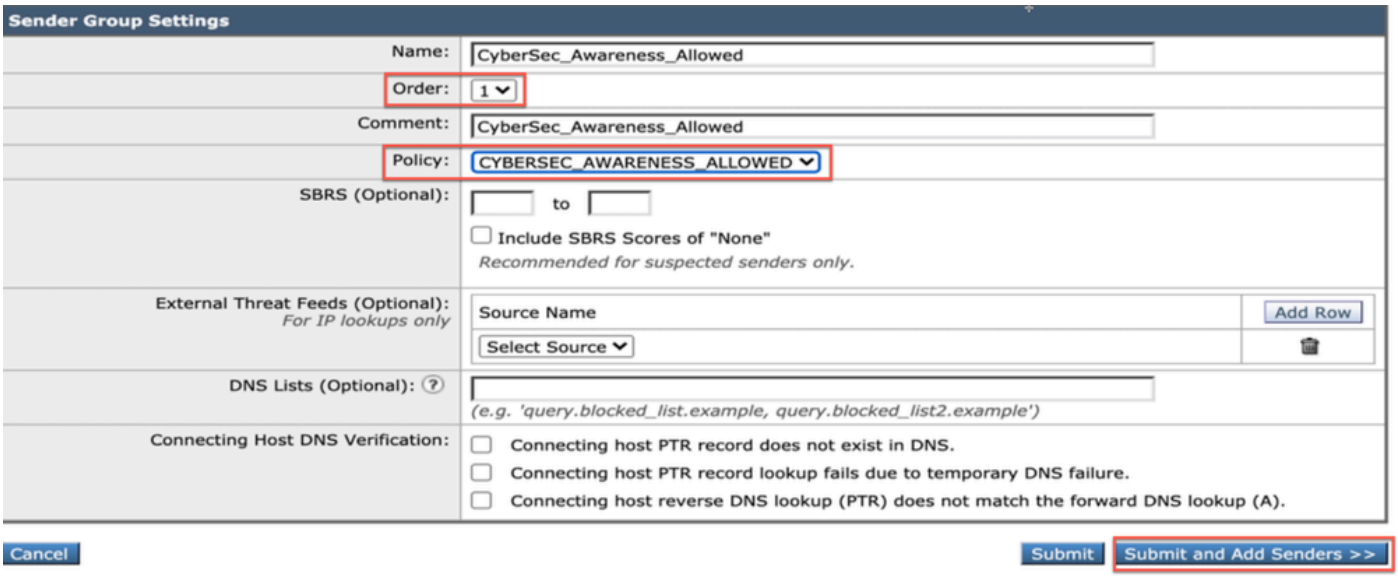
보안 기능이 비활성화된 "CYBERSEC_AWARENESS_ALLOWED" 메일 플로우 정책의 스크린샷

CSA Cloud Service에서 시뮬레이션된 피싱 캠페인 이메일이 Secure Email Gateway의 모든 스캐닝 엔진을 우회하도록 허용하려면 다음을 수행합니다.

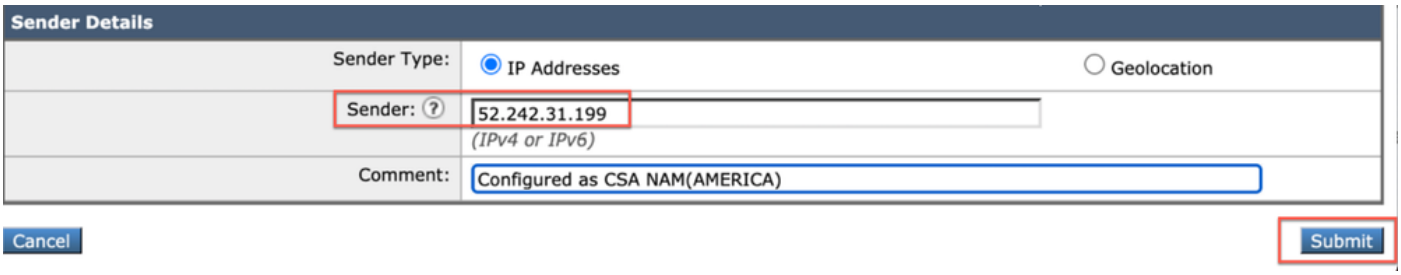
a. 새 Sender Group을 생성하고 메일 플로우 정책을CYBERSEC_AWARENESS_ALLOWED할당합니다. 정책으로Mail Policies > HAT Overview > Add Sender Group이동하여 정책을 선택하고CYBERSEC_AWARENESS_ALLOWED순서를 1로 설정한 다음 Submit and Add Senders.

b. IP/domain피싱 캠페인 이메일이Geo Location시작된 위치에서 발신자 또는 발신자를 추가합니다.

이미지에Mail Polices > HAT Overview > Add Sender Group > Submit and Add Senders > Add the sender IP > Submit표시된 대로 이동하여Commit변경합니다.



"CYBERSEC_AWARENESS_ALLOWED 메일 플로우 정책이 선택된 CyberSec_Awareness_Allowed 발신자 그룹의 스크린샷입니다.



Cisco Secure Email Gateway의 Cisco Security Awareness 설정 페이지 스크린샷

CLI 구성:

1. 다음으로 이동 listenerconfig > Edit > Inbound (PublicInterface) > HOSTACCESS > NEW > New Sender Group .

2.CYBERSEC_AWARENESS_ALLOWED메일 정책으로 새 발신자 그룹을 만들고 피싱 캠페인 이메일이 시작되는 발신자 IP/도메인을 추가합니다.

3. 새 Sender Group의 순서를 1로 설정하고 아래의 옵션을Move사용합니다. listenerconfig > EDIT > Inbound (PublicInterface) > HOSTACCESS > MOVE .

4. 커밋합니다.

참고: 발신자 IP는 CSA의 IP 주소이며 선택한 지역을 기반으로 합니다. 사용할 올바른 IP 주소는 표를 참조하십시오. SEG 14.0.0-xxx가 CSA 클라우드 서비스에 연결하기 위해 포트 번호가 443인 방화벽에서 이러한 IP 주소/호스트 이름을 허용합니다.

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	

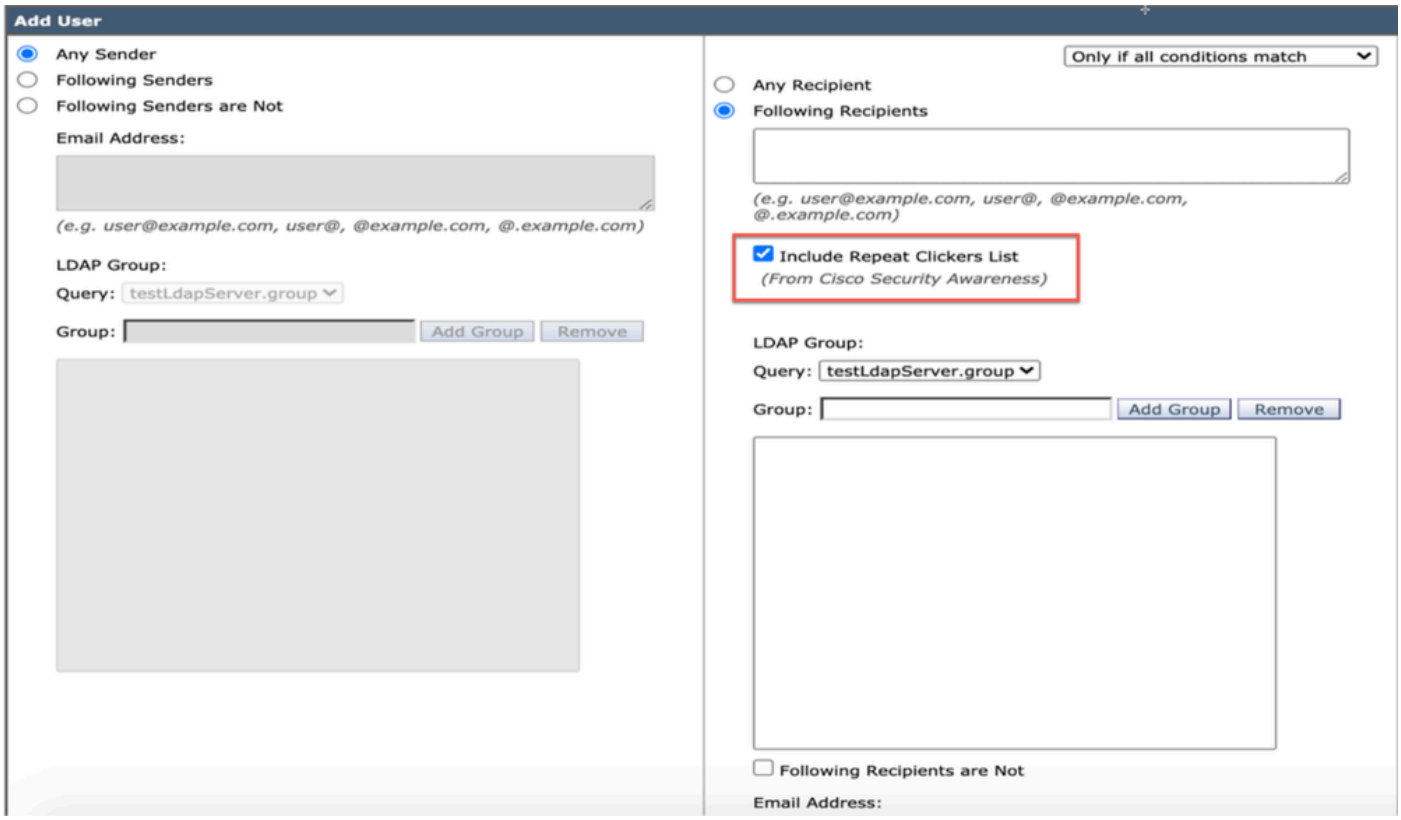
CSA 미주 및 EU 지역 IP 주소 및 호스트 이름 스크린샷

3단계. SEG에서 반복 클릭커에 대한 작업 수행

피싱 이메일이 전송되고 SEG에 반복 클릭커 목록이 채워지면 공격적인 수신 메일 정책을 만들어 특정 사용자에게 메일에 대한 조치를 취할 수 있습니다.

새로운 공격적인 수신 사용자 지정 메일 정책을 생성하고 수신자 섹션에서 enableInclude Repeat Clickers List확인란을 선택합니다.

GUI에서Mail Policies > Incoming Mail Policies > Add Policy > Add User > Include Repeat Clickers List > Submit로 이동하고 변경 사항을Commit확인합니다.



반복 클릭자를 대상으로 메일을 처리하도록 구성된 사용자 지정 수신 메일 정책의 스크린샷

문제 해결 가이드

1. 반복csaconfig > SHOW_LIST클릭커 목록의 상세내역을 보려면 이동합니다.

```
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.csaconfig > UPDATE_LIST 반복 클릭커 목록을 강제로 갱신하려면 다음으로 이동합니다.

```
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.
```

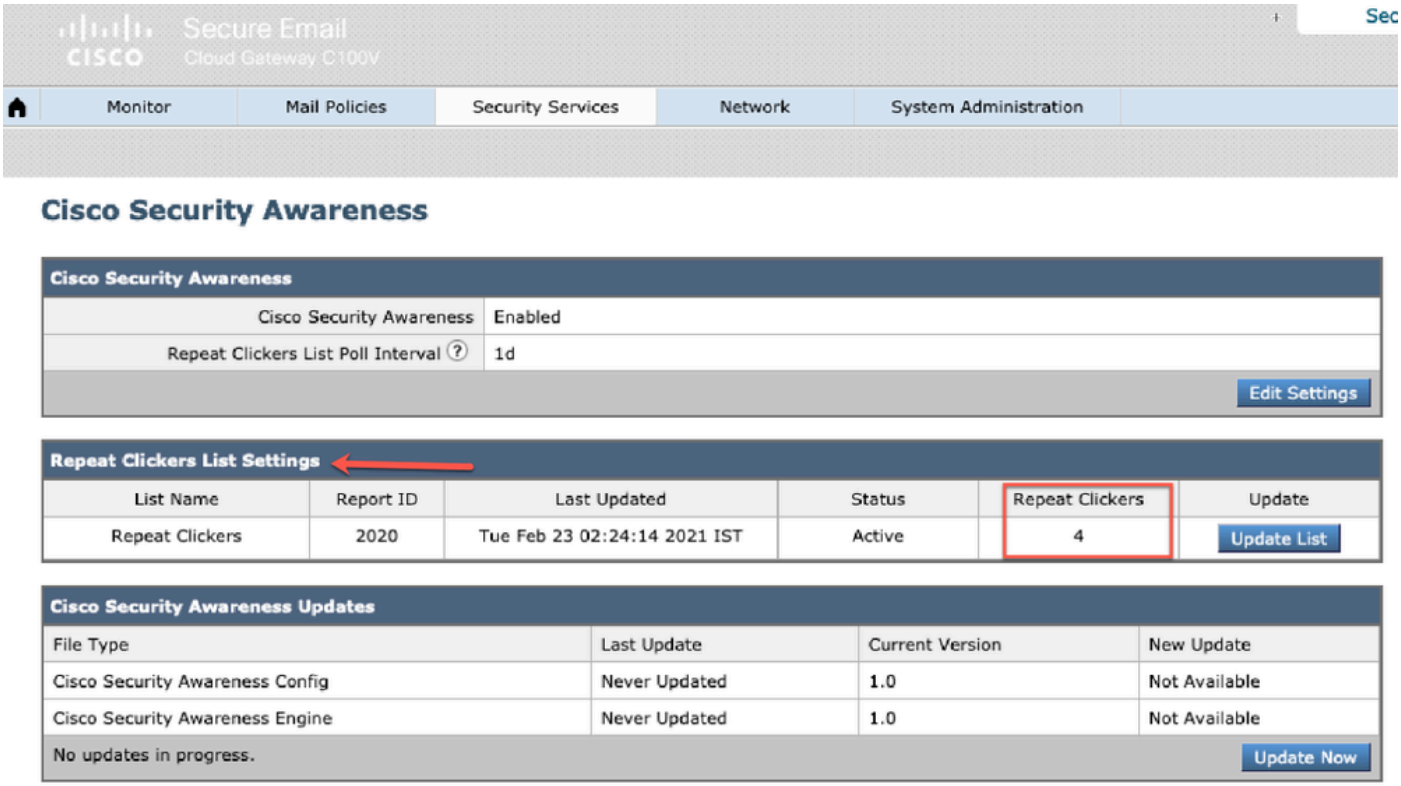
3. csa 로그를 테일링하여 반복 클릭커 목록이 다운로드되었는지 또는 오류가 있는지 확인합니다. 다음은 working setup:

```
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. GUI에서 반복 클릭커 목록을 볼 수도 있습니다. 이미지에Security Services > Cisco Security Awareness표시된 대로 이동합니다.



Security Services(보안 서비스) > Cisco Security Awareness(Cisco 보안 인식) 페이지의 스크린샷에서 반복 클릭커 수를 강조 표시했습니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.