Configure Cisco Security Awareness Integration with Cisco Secure Email Gateway

Contents

Introduction

This document describes the steps needed to configure Cisco Security Awareness (CSA) integration with the Cisco Secure Email Gateway.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Email Gateway concepts and configuration
- CSA Cloud Service

Components Used

The information in this document is based on AsyncOS for SEG 14.0 and later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Create and Send Phishing Simulations from CSA Cloud Service

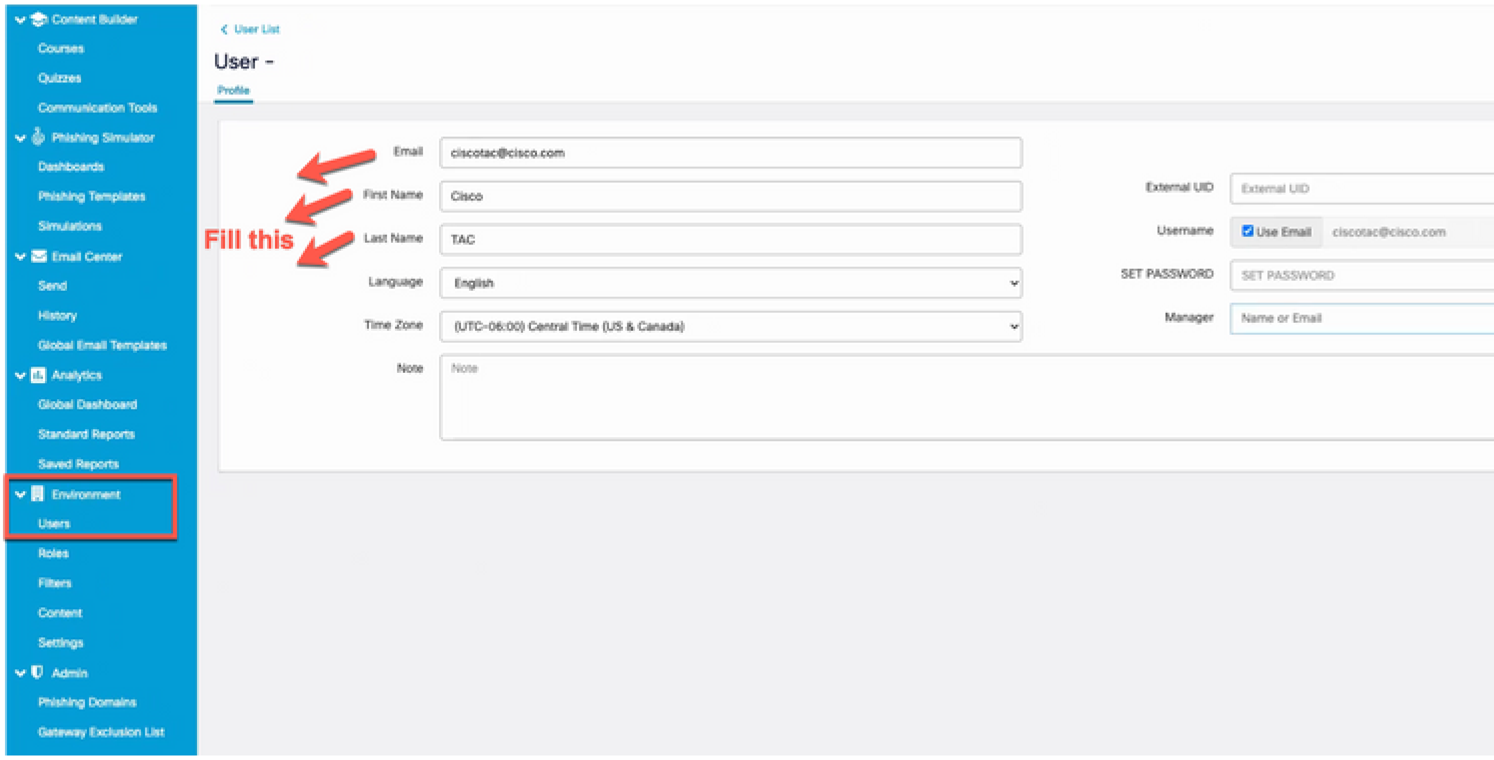
Step 1. Log into CSA Cloud Service

Refer to:
1. https://secat.cisco.com/ for AMERICAS region

2. https://secat-eu.cisco.com/ for EUROPE region

Step 2. Create a Phishing Email Recipient

Navigate to **Environment > Users > Add New User** and fill in the Email, First Name, Last Name and Language fields and then click **Save Changes**as shown in the image.



User -

Fill this

Email: ciscotac@cisco.com

First Name: Cisco

Last Name: TAC

Language: English

Time Zone: (UTC-06:00) Central Time (US & Canada)

Note: Note

External UID: External UID

Username: ☑ Use Email ciscotac@cisco.com

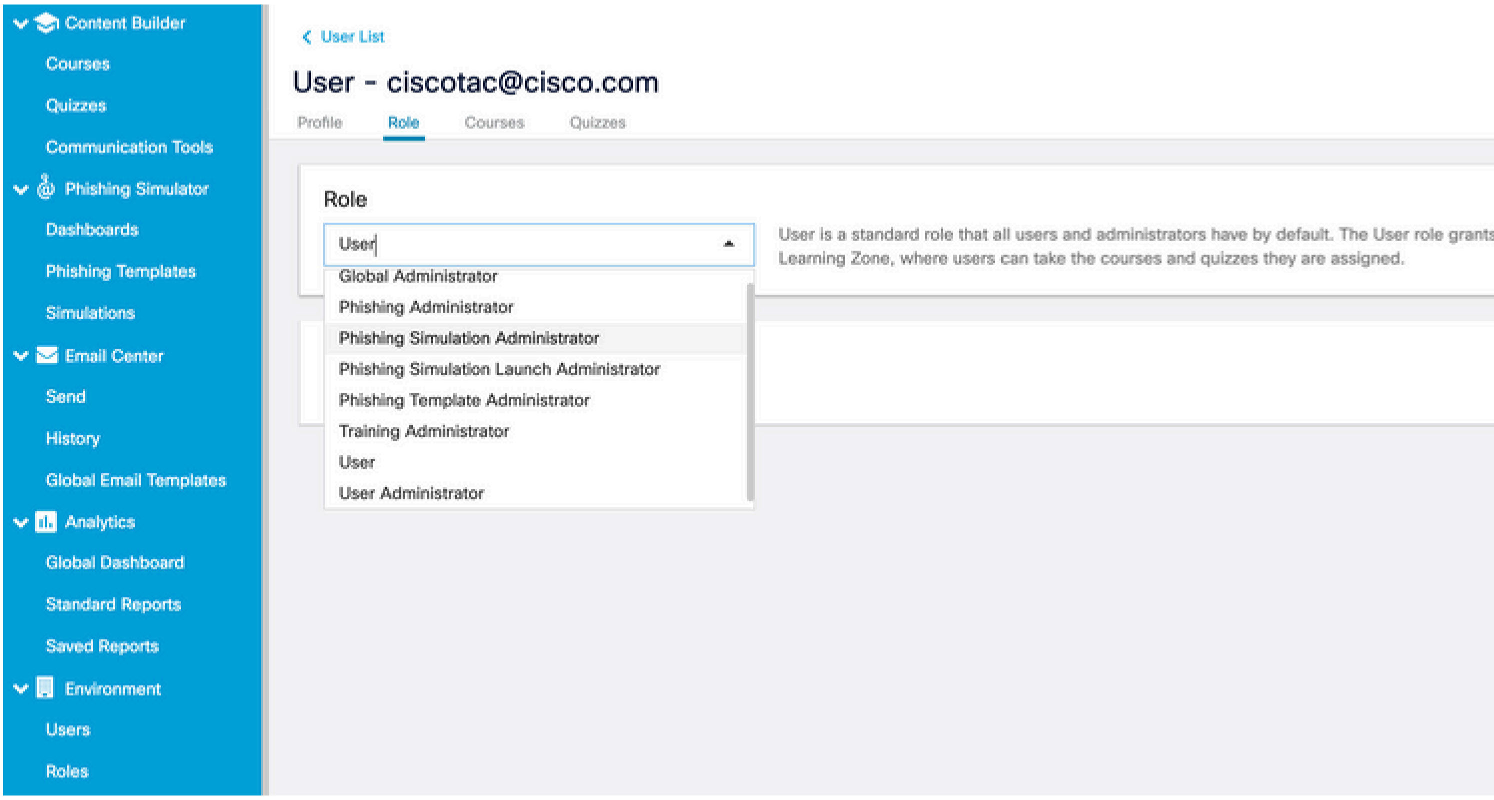
SET PASSWORD: SET PASSWORD

Manager: Name or Email

Screenshot of user interface page to add new user

> **Note**: A password needs to be set only for a CSA admin user who is authorised to create and launch simulations.

The role of the user can be selected once the user is created. You can select the role from the dropdown as indicated in this image:



User - ciscotac@cisco.com

Role

User

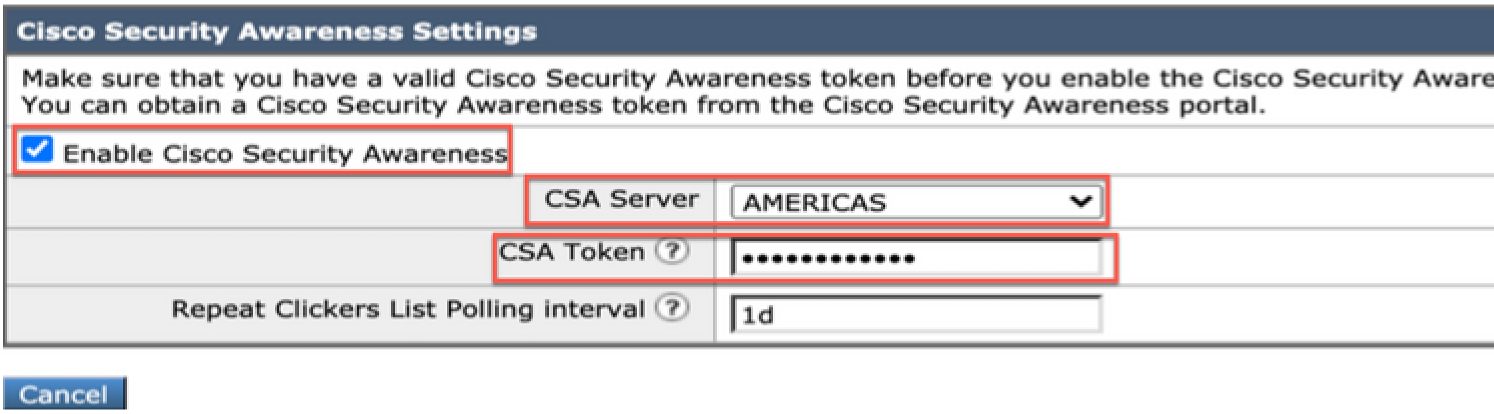
- Global Administrator
- Phishing Administrator
- Phishing Simulation Administrator
- Phishing Simulation Launch Administrator
- Phishing Template Administrator
- Training Administrator
- User
- User Administrator

User is a standard role that all users and administrators have by default. The User role grants
Learning Zone, where users can take the courses and quizzes they are assigned.

View of the user role drop down options

Select the checkboxUser is Phishing Recipient > Save Changesas shown in the image.

Enter the Region and the CSA Token (Bearer Token obtained from CSA Cloud Service as shown in the previously mentioned Note) and submit and commit the changes.



Cisco Security Awareness Settings

Make sure that you have a valid Cisco Security Awareness token before you enable the Cisco Security Aware
You can obtain a Cisco Security Awareness token from the Cisco Security Awareness portal.

☑ Enable Cisco Security Awareness

CSA Server	AMERICAS
CSA Token ?	•••••••••••••
Repeat Clickers List Polling interval ?	1d

Screenshot of the Cisco Security Awareness settings page on the Cisco Secure Email Gateway

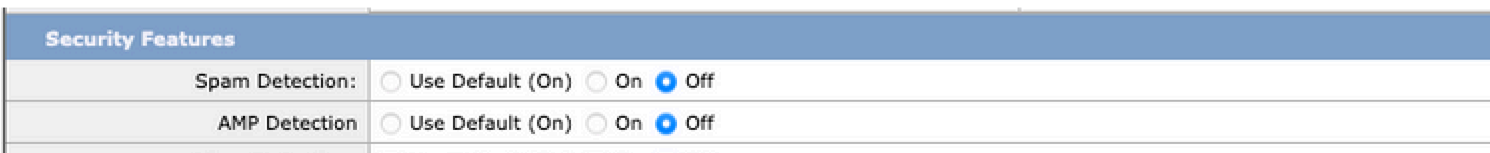
CLI Configuration

Type `csaconfig` to configure CSA via the 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]>
```

Step 2. Allow Simulated Phishing Emails from CSA Cloud Service

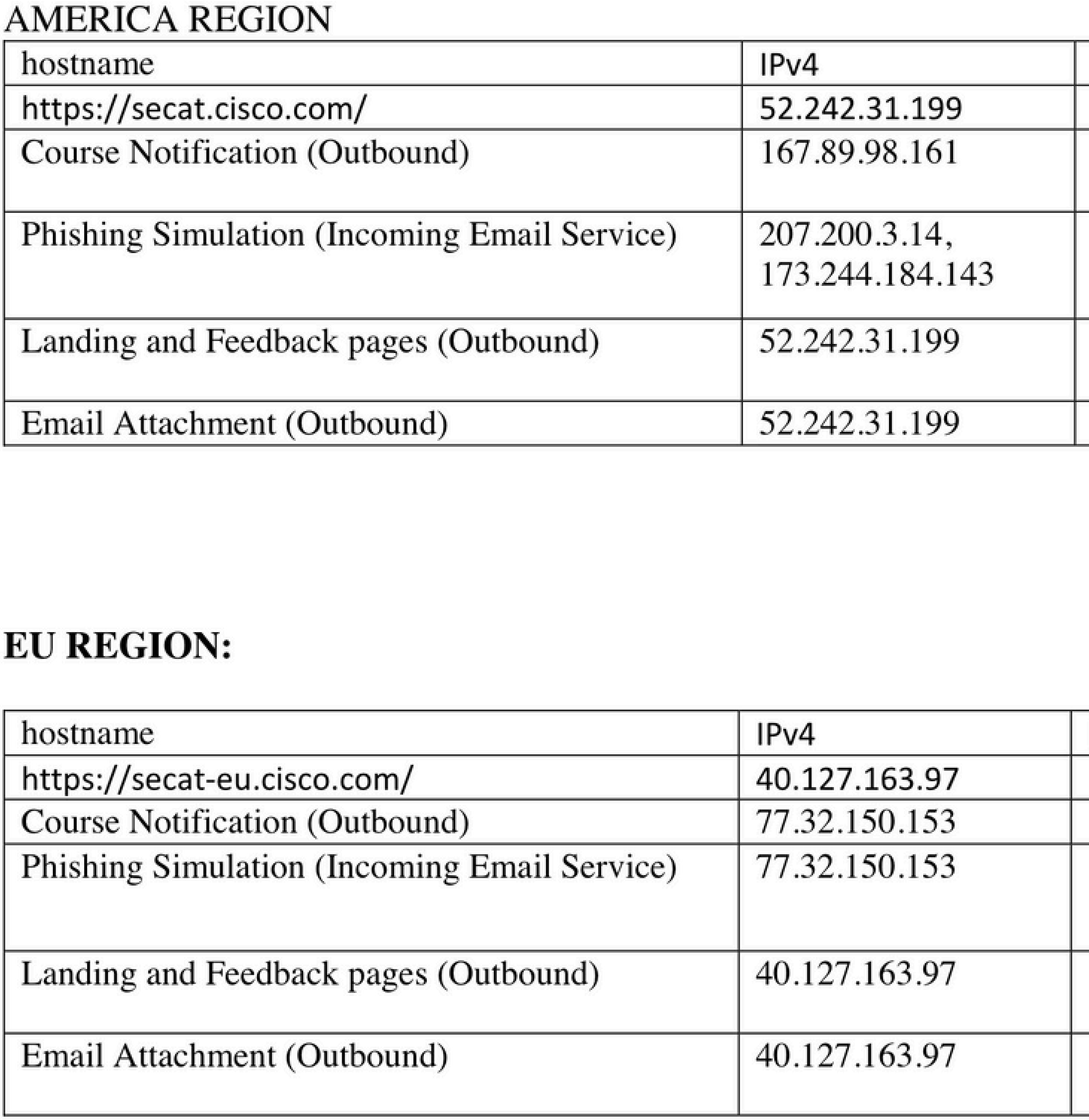
> **Note**: The CYBERSEC_AWARENESS_ALLOWED Mailflow policy is created by default with all the scanning engines set to Off as shown here.



Security Features

Spam Detection:	○ Use Default (On) ○ On ● Off
AMP Detection	○ Use Default (On) ○ On ● Off

: The sender IP is the IP address of the CSA and is based on the region you selected. Refer to the table for the correct IP address to be used. Allow these IP addresses/hostnames in the firewall with port number 443 for SEG 14.0.0-xxx to connect to the CSA cloud service.



AMERICA REGION

hostname	IPv4
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
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 of the CSA Americas and EU regions IP addresses and hostnames

Step 3. Take Action on Repeat Clicker from SEG

Once the phishing emails have been sent and the repeat clickers list populated in the SEG, an aggressive incoming mail policy can be created to take action on mail to those specific users.

Create a new aggressive Incoming Custom Mail Policy and enable Include Repeat Clickers List check box in the recipient section.

From GUI, navigate to Mail Policies > Incoming Mail Policies > Add Policy > Add User > Include Repeat Clickers List > Submit and Commit the changes.

- **Technical Support & Documentation - Cisco Systems**