Configure Cisco Security Awareness Integration with Cisco Secure Email Gateway

Contents

Introduction **Prerequisites Requirements Components Used** Create and Send Phishing Simulations from CSA Cloud Service Step 1. Log into CSA Cloud Service Step 2. Create a Phishing Email Recipient Step 3. Enable Report API Step 4. Create Phishing Simulations Step 5. Verification of Active Simulations What is seen on the side of the recipient? Verify on CSA Configure the Secure Email Gateway Step 1. Enable the Cisco Security Awareness Feature in the Secure Email Gateway Step 2. Allow Simulated Phishing Emails from CSA Cloud Service Step 3. Take Action on Repeat Clicker from SEG **Troubleshoot Guide Related Information**

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. <u>https://secat.cisco.com/</u> for AMERICAS region

2. <u>https://secat-eu.cisco.com/</u> 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 Changesas shown in the image.

Communication Tools ◆ Plakking Simulators Dashboards Pasaking Templates Simulations Cisco Send History Global Estellist Global Estellist Note	✓ ♣ Content Builder Courses Quizzes	< User List User - Profile			
Passbarg templates Print Name Clico Simulations Username Use Email ciscotac@clicico.com Send Last Name TAC SET PASSWORD Send Language English SET PASSWORD Ristory Time Zone (UTC-06:00) Central Time (US & Canada) Manager Qiobal Email Templates Note	🗸 🁌 Phishing Simulator		ciscotac@cisco.com		
Send Language English SET PASSWORD SET PASSWORD History Time Zone (UTC-06:00) Central Time (US & Canada) Manager Name or Email Global Email Templates Note Imager Imager Imager					
Clobal Email Templates (UTC-06:00) Central Time (US & Canada) Clobal Email Templates Note Clobal Dashboard Note		-			
Global Dashboard		Time Zone		Manager	Name or Email
	Global Dashboard	Note	Note		
Saved Reports	Saved Reports				
Users Roles	Users				
Filters Content					
Settings V D Admin					
Phishing Domains Gateway Exclusion List					

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:

✓ ⇒ Content Builder	✓ User List	
Courses	User - ciscotac@cisco.com	
Quizzes	Profile Role Courses Quizzes	
Communication Tools		
🗸 💩 Phishing Simulator	Role	
Dashboards	User	User is a standard role that all users and administrators have by default. The User role grant
Phishing Templates	Global Administrator	Learning Zone, where users can take the courses and quizzes they are assigned.
Simulations	Phishing Administrator	
🗸 🖂 Email Center	Phishing Simulation Administrator Phishing Simulation Launch Administrator	
Send	Phishing Template Administrator	
History	Training Administrator	
Global Email Templates	User User Administrator	
✓ II. Analytics		
Global Dashboard		
Standard Reports		
Saved Reports		
🗸 📃 Environment		
Users		
Roles		



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

🗸 📚 Content Builder	< User List
Courses	

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 Settin	igs		
Make sure that you have a valid Cisco Security Awareness token before you enable the Cisco Security Awar You can obtain a Cisco Security Awareness token from the Cisco Security Awareness portal.			
Enable Cisco Security Awarenes	s		
	CSA Server	AMERICAS 🗸	
	CSA Token 🥐	•••••	
Repeat Clickers List Poll	ng interval 🧿	1d	

Cancel

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 O 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.

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

<u>Technical Support & Documentation - Cisco Systems</u>