Integrating Email Gateway with Cisco Secure Awareness Cloud Service

This chapter contains the following sections:

Overview

The Cisco Secure Awareness cloud service allows you to effectively deploy phishing simulations, awareness training, or both to measure and report results. It empowers the security operations team to focus on real-time threats and not end-user mitigation.

The Cisco Secure Awareness cloud service provides reports of repeat clickers - users who repeatedly click on any URL or attachment in messages. These users are identified via a phishing simulation campaign defined by the Cisco Secure Awareness cloud service.

For more information on the Cisco Secure Awareness cloud service, see https://secat.cisco.com.

You can integrate your email gateway with the Cisco Secure Awareness cloud service to:

- Improve end-user awareness towards real-world phishing attacks.
- Allow email administrators to configure stringent policies for users identified as repeat clickers.

How to Integrate Email Gateway with Cisco Secure Awareness Cloud Service

Perform these steps in order:

Steps	Do This	More Information
Step 1	[On Cisco Secure Awareness] Create a Cisco Security Awareness cloud service account for your organization based on your region.	Creating Cisco Secure Awareness Cloud Service Account, on page 3
Step 2	Configure firewall settings to allow your email gateway to access the Cisco Secure Awareness cloud service.	Configuring Firewall Settings to Access Cisco Secure Awareness Cloud Service, on page 3
Step 3	Create a new sender group to allow simulated phishing messages from the Cisco Secure Awareness cloud service in your email gateway.	Creating Sender Group to Allow Simulated Phishing Messages in Email Gateway, on page 4
Step 4	[On Cisco Secure Awareness] Create a new user in the Cisco Secure Awareness cloud service to identify repeat clickers. :	See the CSA Administrator Guide at: • https://secat.cisco.com/portal/Support [applicable for Americas users] • https://secat-eu.cisco.com/portal/Support [applicable for European Union (EU) users]
Step 5	[On Cisco Secure Awareness] Create simulated phishing messages in the Cisco Secure Awareness cloud service and send them to the end users in your organization. This process is used to track the end users who repeatedly click on any attachment or URL in messages.	See the CSA Administrator Guide at: • https://secat.cisco.com/portal/Support [applicable for Americas users] • https://secat-eu.cisco.com/portal/Support [applicable for European Union (EU) users]
Step 6	Obtain the authentication token from the Cisco Secure Awareness cloud service.	Obtaining Authentication Token from Cisco Secure Awareness Cloud Service, on page 5
Step 7	Enable the Cisco Secure Awareness cloud service on your email gateway.	Enabling Cisco Secure Awareness Cloud Service on Email Gateway, on page 6

Steps	Do This	More Information
Step 8	Create a custom incoming mail policy to configure aggressive mail policies for end users categorized as repeat clickers.	Create Custom Incoming Mail Policy for End Users Categorized as Repeat Clickers, on page 7

Creating Cisco Secure Awareness Cloud Service Account

Depending on your region, create a Cisco Secure Awareness cloud service account with admin acess rights for your organization using one of the following URLs:

- https://secat.cisco.com [applicable for Americas users]
- https://secat-eu.cisco.com [applicable for European Union (EU) users]

What to do Next

Configure firewall settings to connect your email gateway to the Cisco Secure Awareness cloud service. For more information, see Configuring Firewall Settings to Access Cisco Secure Awareness Cloud Service, on page 3

Configuring Firewall Settings to Access Cisco Secure Awareness Cloud Service

You must open HTTPS (Out) 443 port on the firewall for the following hostnames or IP addresses (refer to the table below) to connect your email gateway to the Cisco Secure Awareness cloud service.

Service	Americas		European Union	
	Hostname	IP Address	Hostname	IP Address
Cisco Secure Awareness cloud service	secat.cisco.com	52.242.31.199	secat-eu.cisco.com	40.127.163.97
Course Notification (Outbound)	-	167.89.98.161	-	40.127.163.97
Landing and Feedback Pages (Outbound)	-	52.242.31.199	-	
Email Attachment (Outbound)	-		-	

Note The IP addresses listed in the above table may change. For the latest list of IP addresses, see the 'IP Allowlist Guide' on the Cisco Secure Awareness cloud service at https://secat.cisco.com/portal/Support/IpWhitelistingGuide

What to do Next

Create a new sender group to allow simulated phishing messsages from the Cisco Secure Awareness cloud service in your email gateway. For more information, see Creating Sender Group to Allow Simulated Phishing Messages in Email Gateway, on page 4

Creating Sender Group to Allow Simulated Phishing Messages in Email Gateway

You must create a new sender group to allow simulated phishing messages from the Cisco Secure Awareness cloud service in your email gateway.

Before you begin

Make sure you have configured the firewall settings to allow your email gateway to access the Cisco Secure Awareness cloud service. For more information, see Configuring Firewall Settings to Access Cisco Secure Awareness Cloud Service, on page 3

Procedure

Step 1 Click **Mail Policies** > **HAT Overview**.

Step 2 Click **Add Sender Group**.

Step 3 Enter a name for the sender group.

Step 4 Select the priority order as **1**.

Step 5 Select the policy as **CYBERSEC_AWARENESS_ALLOWED**.

Step 6 Check the **SBRS to Not in Use** checkbox to disable IP Reputation filtering.

Step 7 Click **Submit and Add Senders**.

Step 8 Add any one of the following Cisco Secure Awareness cloud service IP addresses to configure as the sender IP address based on your region:

- Americas - 207.200.3.14 or 173.244.184.143
- European Union (EU) - 77.32.150.153

Note The Cisco Secure Awareness cloud service IP addresses are used to prevent your email gateway from interpreting simulated phishing messages as actual phish..

Step 9 Submit and commit your changes.

What to do next

1. Create a new user in the Cisco Secure Awareness cloud service to identify repeat clickers.
2. Create simulated phishing messages in the Cisco Secure Awareness cloud service and send them to the end users in your organization.

   For more information on how to complete the above two tasks, see the CSA Administrator Guide at:

   - https://secat.cisco.com/portal/Support [applicable for Americas users]
   - https://secat-eu.cisco.com/portal/Support [applicable for European Union (EU) users]

3. Obtain an authentication token from the Cisco Secure Awareness cloud service to download the Repeat Clickers list from the Cisco Secure Awareness cloud service. For more information, see Obtaining Authentication Token from Cisco Secure Awareness Cloud Service, on page 5

Obtaining Authentication Token from Cisco Secure Awareness Cloud Service

You must obtain an authentication token from the Cisco Secure Awareness cloud service and use it to download the Repeat Clickers list from the Cisco Secure Awareness cloud service.

Before you begin

Make sure that you have an account in the Cisco Secure Awareness cloud service with admin access rights. For more information, see Creating Cisco Secure Awareness Cloud Service Account, on page 3. If you are unable to access the Cisco Secure Awareness cloud service, contact Cisco Support for assistance.

Procedure

Step 1 Log in to the Cisco Secure Awareness cloud service.

Step 2 Go to **Environment > Setttings**

Step 3 Click the **Report API** tab.

Step 4 Check the **Enable Report API** check box .

Step 5 Copy the authentication token.

Use this authentication token to download the Repeat Clickers list from the Cisco Secure Awareness cloud service.

What to do next

Enable the Cisco Secure Awareness cloud service on your email gateway. For more information, see Enabling Cisco Secure Awareness Cloud Service on Email Gateway, on page 6

Enabling Cisco Secure Awareness Cloud Service on Email Gateway

Before you begin

Make sure you have:

- A valid account in the Cisco Secure Awareness cloud service with admin access rights.
- Obtained a valid authentication token from the Cisco Secure Awareness cloud service. For more information, see Obtaining Authentication Token from Cisco Secure Awareness Cloud Service, on page 5,

Procedure

Step 1 Go to **Security Services > Cisco Secure Awareness**.

Step 2 Click **Enable**.

Step 3 Check the **Enable Cisco Secure Awareness** check box .

Step 4 Choose the required server to connect your email gateway to the Cisco Secure Awareness cloud service.

Step 5 Enter the authentication token obtained from the Cisco Secure Awareness cloud service.

Step 6 [Optional] Enter the polling interval to download the Repeat Clickers list from the Cisco Secure Awareness cloud service.

Step 7 Submit and commit your changes.

What to do next

- After you enable the Cisco Secure Awareness cloud service, the email gateway automatically downloads the Repeat Clickers list from the Cisco Secure Awareness cloud service. You can view the number of repeat clicker users in the Repeat Clickers list by navigating to **Security Services** > **Cisco Secure Awareness** > **Repeat Clickers List Settings** section in the web interface of your email gateway. For more information about the Repeat Clickers list, log in to the Cisco Secure Awareness cloud service and navigate to Analytics > Standard Reports > Phishing Simulations > Repeat Clickers section.
- Create a custom incoming mail policy to configure aggressive mail policies for end users categorized as repeat clickers. For more information, see Create Custom Incoming Mail Policy for End Users Categorized as Repeat Clickers, on page 7.
- Cisco Secure Email Submission Add-In now supports submission of simulated phishing messages sent through the Cisco Secure Awareness (CSA) cloud service portal. You can now submit the simulated phishing messages using the Secure Email Submission Add-In itself. For more details, see the User Guide for Cisco Secure Email Submission Add-In.

Create Custom Incoming Mail Policy for End Users Categorized as Repeat Clickers

You must create a custom incoming mail policy to configure aggressive mail policies for end users categorized as repeat clickers.

Procedure

Step 1	Go to **Mail Policies** > **Incoming Mail Policies**.
Step 2	Click **Add Policy**.
Step 3	Enter a name for the policy.
Step 4	Check **Add User**.
Step 5	Select **Following Recipients**.
Step 6	Check the **Include Repeat Clicker List** checkbox to include the list of recipients categorized as repeat clickers by the Cisco Secure Awareness cloud service.
Step 7	Click **OK**.
Step 8	Click **Submit**.
Step 9	Configure the required service engines (for example, Anti-Virus, Graymail, and so on) for the mail policy.
Step 10	Commit your changes.

Cisco Secure Awareness Cloud Service and Clusters

If you use centralized management, you can enable the Cisco Secure Awareness cloud service at the cluster, group, and machine level. If you have enabled your email gateway with the Cisco Secure Awareness cloud service in standalone mode, you can choose to join a cluster registered with the Cisco Secure Awareness cloud service.

Note When you disable the Cisco Secure Awareness cloud service at the machine level, it is disabled only for the logged-in email gateway while the other machines in the cluster are still connected to the Cisco Secure Awareness cloud service.

Viewing Logs

The Cisco Secure Awareness cloud service information is posted to the Mail Logs. Most information is at the Info or Debug level.

Examples of Cisco Secure Awareness Log Entries:

- In this example, the log shows that the download of the Repeat Clickers list from the Cisco Secure Awareness cloud service failed because of an invalid token.

```
Tue Oct 13 10:12:59 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Secure Awareness cloud service failed because
of an invalid token.
```

Solution: Make sure you obtain a valid authentication token from the Cisco Secure Awareness cloud service.

- In this example, the log shows that the download of the Repeat Clickers list from the Cisco Secure Awareness cloud service failed because of a connection error.

```
Wed Oct 14 10:59:36 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Secure Awareness cloud service failed because
of a connection error.
```

Solution: Verify the firewall configuration settings used to connect your email gateway to the Cisco Secure Awareness cloud service.

- In this example, the log shows that the download of the Repeat Clickers list from the Cisco Secure Awareness cloud service failed because of an internal server error.

```
Wed Oct 14 10:59:36 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Secure Awareness cloud service failed because
of an internal server error.
```

Solution: Contact Cisco Support for technical assistance.

- In this example, the log shows that the download of the Repeat Clickers list from the Cisco Secure Awareness cloud service failed because the SSL certificate verification failed.

```
Wed Oct 14 11:02:46 2020 Warning: CSA:
 The download of the Repeat Clickers list from
the Cisco Secure Awareness cloud service failed because
the SSL certificate verification failed.
```

Solution: Add the required CA certificate of the proxy server in the custom certificate authority list of your email gateway.

- In this example, the log shows that the download of the Repeat Clickers list from the Cisco Secure Awareness cloud service failed because the proxy authentication failed.

```
Wed Oct 14 11:09:48 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Secure Awareness cloud service failed
because the proxy authentication failed.
```

Solution: Check whether the proxy server is configured with the correct authentication credentials in your email gateway.

- In this example, the log shows that a request to the Cisco Secure Awareness cloud service failed because the Report API was not enabled on the Cisco Secure Awareness cloud service.

```
Mon Aug 17 15:35:42 2020 Warning: CSA:
The download of the Repeat Clickers list failed.
A request to the CSA cloud service failed because
the Report API was not enabled on the CSA cloud service
```

Solution: Check the Enable Report API check box in Environment > Settings > Report API tab of the Cisco Secure Awareness cloud service.

- In this example, the log shows that the Cisco Secure Awareness feature expires on a particular date.

```
2020-10-15 08:00:11,968 INFO csa The Cisco Secure
Awareness feature expires on 2029-12-28T23:59:59Z. You need to
contact your Cisco Account Manager to renew the license.
```

Solution: Contact your Cisco Account Manager to renew the license.

- In this example, the log shows that the Cisco Secure Awareness feature license has expired, and the feature is disabled on your email gateway.

```
2020-10-27 13:33:21,714 CRITICAL csa The Cisco Secure
Awareness feature license has expired, and the feature is
disabled on your email gateway. Contact your Cisco Account Manager
to renew the license.
```

Solution: Contact your Cisco Account Manager to renew the license.

- In this example, the log shows that the downloaded Repeat Clickers list is empty.

```
Tue Oct 13 10:10:18 2020 Info: CSA: The downloaded
Repeat Clickers list is empty.
```

Solution: Create simulated phishing messages in the Cisco Secure Awareness cloud service and send them to the recipients in your organization.

- In this example, the log shows that the download of the Repeat Clickers list from the Cisco Secure Awareness cloud service failed because you have reached the maximum number of download attempts.

```
Fri Oct 16 05:22:08 2020 Warning: CSA: The download
of the Repeat Clickers list from the Cisco Secure Awareness
cloud service failed because you have reached the maximum
number of attempts.
```

Solution: Contact Cisco Support to increase the number of attempts to download the Repeat Clickers list from the Cisco Secure Awareness cloud service.

Viewing Alerts

The following table lists the system alerts generated for the Cisco Secure Awareness cloud service, including a description of the alert and the alert severity.

Component/Alert Name	Message and Description	Parameters
MAIL.CSA.DOWNLOAD _FAILURE	Alert text: The download of the Repeat Clickers list from the Cisco Secure Awareness cloud service failed. $reason. Alert level: WARNING. Description: Alert is sent when the download of the Repeat Clickers list from the Cisco Secure Awareness cloud service fails.	Parameters: reason reason - Reason for the failure to download repeat clickers list from Cisco Secure Awareness cloud service. For example: ‘invalid token,’ ‘reached the maximum number of attempts,’ and so on.

Component/Alert Name	Message and Description	Parameters
MAIL.CSA.EMPTY_ EMAIL_LIST	Alert text: The downloaded Repeat Clickers list is empty. Alert level: INFO. Description: Alert is sent when the downloaded Repeat Clickers list is empty. This alert indicates that there are no Repeat Clickers listed in the Cisco Secure Awareness cloud service.	N/A.
MAIL.CSA.LICENSE_ EXPIRING	Alert text: The Cisco Secure Awareness feature license expires on $expiry. You must contact your Cisco Account Manager to renew the license. Region: $region Server: $server Alert level: INFO Description: Alert is sent on 7 days prior to expiry, 3 days prior to expiry and 1 day prior to expiry.	Parameters: expiry, region, server expiry – The date on which the Cisco Secure Awareness license is expiring. region – The region of the Cisco Secure Awareness license which is expiring. The region can be AMERICAS, EUROPE, and so on. server – The name of the server URL, for example,https://secat.cisco.com.
MAIL.CSA.LICENSE_ EXPIRED	Alert text: The Cisco Secure Awareness feature license has expired, and the feature is disabled on your email gateway. Contact your Cisco Account Manager to renew the license. Region: $region Server: $server Alert Level: Critical Description: Alert is sent on expiry of the Cisco Secure Awareness license.	Parameters: region, server region – Region of the Cisco Secure Awareness license which has expired. The region can be AMERICAS, EUROPE, and so on. server – Name of the server URL, for example, https://secat.cisco.com.

Component/Alert Name	Message and Description	Parameters
MAIL.CSA.LICENSE_ RETRIVAL_FAILURE	Alert text: The retrieval of the license expiry details from the Cisco Secure Awareness cloud service failed $reason Alert level: WARNING Description: Alert is sent on failure to retrieve license expiry details from Cisco Secure Awareness cloud service for three consecutive times. Every day one attempt is made to retrieve the license expiry details until the license expiry details are retrieved successfully.	Parameters: reason reason – Reason for the failure to retrieve the license expiry details from the Cisco Secure Awareness cloud service. For example: 'invalid token', and 'reached the maximum number of attempts.'