Integrating the Email Gateway with Cisco Advanced Phishing Protection

This chapter contains the following sections:

- Overview of Cisco Advanced Phishing Protection, on page 1
- How to Integrate Email Gateway with the Cisco Advanced Phishing Protection Cloud Service, on page 3
- Advanced Phishing Protection and Clusters, on page 9
- Advanced Phishing Protection Report Page, on page 9
- Monitoring Message Metadata on the Cisco Advanced Phishing Protection Cloud Service, on page 10
- Displaying Messages Submitted to the Cisco Advanced Phishing Protection Cloud Service, on page 10

Overview of Cisco Advanced Phishing Protection

Cisco Advanced Phishing Protection provides Business Email Compromise (BEC) and phishing detection capabilities. It detects identity deception-based threats by performing reputation checks on sender address by using advanced machine learning techniques and added intelligence. This intelligence continuously adapts to drive a real-time understanding of senders and provides enhanced protection.

The Advanced Phishing Protection engine on the email gateway checks the unique behavior of all legitimate senders, based on the historic email traffic to your organization. The cloud service interface of the Cisco Advanced Phishing Protection provides risk analysis to distinguish good messages from potentially malicious messages.

The Cisco Advanced Phishing Protection cloud service relies on the email gateway as a sensor engine to receive a copy of the message metadata sent inbound into your organization. This sensor engine collects metadata such as message headers from the email gateway and relay them to the Cisco Advanced Phishing Protection cloud service for analysis. After the analysis, potentially malicious messages are remediated from the recipient mailbox automatically, based on the pre-configured policies on the Advanced Phishing Protection cloud service.

The ability to use the email gateway as a sensor engine helps an organization to:

- Identify, investigate, and remediate threats observed on the message headers, from the recipient mailbox.
- View the reporting data of the metadata of the message from multiple email gateways in your organization.

No Support for Cisco Secure Email Phishing Défense:

As of December 14, 2022, the Cisco Secure Email Phishing Defense (formerly known as Cisco Advanced Phishing Protection) feature will no longer be supported from Secure Email Cloud Gateway 14.3 onwards. For more details, click here. Contact Cisco Technical Assistance for further assistance.

Note The above statement does not apply to existing users who have a valid license and are actively using the Cisco Secure Email Phishing Défense feature.

Benefits of Cisco Advanced Phishing Protection

The following are the benefits of deploying Cisco Advanced Phishing Protection on the email gateway:

- The Sensor-based solution can be rapidly deployed to ensure that your users are fully protected from damaging breaches.
- Provides another layer of defense to more effectively secure your email environment.
- Gain a real-time understanding of senders, learn, and authenticate email identities and behavioral relationships to protect against BEC attacks.
- Automatically remove malicious emails from the recipient's inbox and calls out identity deception techniques to prevent wire fraud or other advanced attacks.
- Get detailed visibility into email attack activity, including total messages secured and attacks prevented.
- Prevents the following:
  - Attacks that use compromised accounts and social engineering.
  - Phishing, ransomware, zero-day attacks and spoofing.
  - BEC with no malicious payload or URL.

Workflow

1. Activate the license to access the Cisco Advanced Phishing Protection cloud service.
2. Set up the email gateway as a sensor engine on the Cisco Advanced Phishing Protection cloud service. This deploys the email gateway as a lightweight sensor via the cloud or on-premise.
3. Register the sensor engine on the email gateway with the Cisco Advanced Phishing Protection cloud service.
4. The sensor engine on the email gateway forwards the metadata of messages considered clean, to the Cisco Advanced Phishing Protection cloud service.
5. The Cisco Advanced Phishing Protection cloud service determines if the message metadata is malicious.
6. Pre-configured policies on the Cisco Advanced Phishing Protection cloud service, when configured with an 'Enforcement' sensor, blocks or redirects the message for further incident investigation.

How to Integrate Email Gateway with the Cisco Advanced Phishing Protection Cloud Service

Perform these steps in the following order:

Procedure

	Command or Action	Purpose
Step 1	Review the prerequsites.	Prerequisites, on page 3
Step 2	Obtain the provisioning key from Cisco Advanced Phishing Protection cloud service.	Obtaining the Provisioning Key from the Cisco Advanced Phishing Protection Cloud Service, on page 4
Step 3	Register your email gateway as a sensor engine with the Cisco Advanced Phishing Protection cloud service.	Registering the Cisco Advanced Phishing Protection Sensor on the Email Gateway, on page 4
Step 4	Enable Advanced Phishing Protection on the email gateway.	Enabling Advanced Phishing Protection on the Email Gateway, on page 6
Step 5	Obtaining API Access Keys from the Cisco Advanced Phishing Protection cloud service.	Obtaining API Access Keys from Cisco Advanced Phishing Protection Cloud Service, on page 6
Step 6	Configure incoming mail policies to enable forwarding of message metadata.	Configuring Incoming Mail Policies to Enable Forwarding of Message Metadata, on page 7
Step 7	Monitor metadata of message forwarded to the Advanced Phishing Protection Cloud Service.	Monitoring Message Metadata on the Cisco Advanced Phishing Protection Cloud Service, on page 9

Prerequisites

- Activating the Account for Cisco Advanced Phishing Protection Cloud Service, on page 3
- Installing Sensors on the Cisco Advanced Phishing Protection Cloud Service, on page 4

Activating the Account for Cisco Advanced Phishing Protection Cloud Service

Make sure that you have:

- Obtained a license to access the Cisco Advanced Phishing Protection cloud service from the following URL - https://www.cisco.com/c/en/us/buy.html.
- Activated your account using the activation link that you receive through an email notification to get provisioned with the Cisco Advanced Phishing Protection cloud service.

Installing Sensors on the Cisco Advanced Phishing Protection Cloud Service

Make sure that you have setup your email gateway as sensor engine as per your organizational requirements. For more information, see *User Guide for Cisco Advanced Phishing Protection*.

Obtaining the Provisioning Key from the Cisco Advanced Phishing Protection Cloud Service

Before you begin

Make sure that you have access to Cisco Advanced Phishing Protection cloud service with admin access rights. For more information, see Prerequisites, on page 3. If you are unable to access the Cisco Advanced Phishing Protection cloud service, contact Cisco TAC for assistance.

Procedure

Step 1 Log in to the Cisco Advanced Phishing Protection cloud service.

Step 2 Choose **Manage** > **Sensors**.

Step 3 Select **Installation** > **Download Sensor Installer**.

Step 4 From the drop-down, select the sensor installation script configured as per your organizational requirements. For example: Cisco SEG.

For more information, see Installing Sensors on the Cisco Advanced Phishing Protection Cloud Service, on page 4.

Step 5 Copy the 6-word provisioning key.

Use this provisioning key to configure the Cisco Email Security Gateway as a sensor.

Note
To register the email gateway as a sensor, you must use the provisioning key within 7 days of generation.

What to do next

Register your email gateway with the Cisco Advanced Phishing Protection cloud service. For more information, see Registering the Cisco Advanced Phishing Protection Sensor on the Email Gateway, on page 4.

Registering the Cisco Advanced Phishing Protection Sensor on the Email Gateway

Before you begin

Make sure that you have:

- A valid provisioning key to register your email gateway with the Advanced Phishing Protection cloud service. For more information, see Obtaining the Provisioning Key from the Cisco Advanced Phishing Protection Cloud Service, on page 4.
- Opened HTTPS (In and Out) 443 port on the firewall for the FQDNs to register your email gateway with the Cisco Advanced Phishing Protection cloud service.

Procedure

Step 1 Log in to the email gateway using the CLI.

Step 2 Run the `eaasconfig` command and follow the instructions as shown in the example below:

```
mail1.example.com> eaasconfig

Choose the operation you want to perform:
- REGISTER - To Register the appliance with APP portal
[]> register

Available list of APP region(s) for the registration
1. AMERICA

Select the EAAS region to connect
[]> 1

Enter passphrase obtained from APP portal: xxxxxx

Registration is in progress. Please wait.
Successfully registered the device with APP portal.

Would you like enable APP [Y]>

mail1.example.com> commit

Please enter some comments describing your changes:
[]>

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Fri Feb 14 07:49:57 2023 GMT
mail1.example.com>
```

The Cisco Advanced Phishing Protection cloud service generates a Universally Unique ID (UUID) after you register your email gateway with the sensor.

Note
After successful registration, the Cisco Advanced Phishing Protection cloud service identifies the email gateway's hostname in the cloud service.

What to do next

Enable Cisco Advanced Phishing Protection engine on the email gateway. For more information, see Enabling Advanced Phishing Protection on the Email Gateway, on page 6.

Enabling Advanced Phishing Protection on the Email Gateway

Before you begin

Make sure that you have registered your email gateway as a sensor on the Cisco Advanced Phishing Protection cloud service. For more information, see Registering the Cisco Advanced Phishing Protection Sensor on the Email Gateway, on page 4.

Procedure

Step 1 Log in to the email gateway.

Step 2 Go to **Security Services > Advanced Phishing Protection**.

Note
You can view the Advanced Phishing Protection sub menu only if you have registered your email gateway as a sensor on the Cisco Advanced Phishing Protection cloud service using the CLI.

Step 3 Click **Enable**.

Step 4 Commit your changes.

What to do next

Enable forwarding of message metadata to the Cisco Advanced Phishing Protection cloud service. For more information, see Configuring Incoming Mail Policies to Enable Forwarding of Message Metadata, on page 7.

Obtaining API Access Keys from Cisco Advanced Phishing Protection Cloud Service

You can use the API access keys to perform the following tasks in your email gateway:

- Send email notification alerts about APP license expiry details to users.
- View total number of messages that are sent from all email gateways at the organizational level to the Cisco Advanced Phishing Protection cloud service in a dashboard widget. The dashboard widget is available on the Advanced Phishing Protection report page of the new web interface.

Before you begin

Make sure that you have:

- Registered the email gateway as a sensor on the Cisco Advanced Phishing Protection cloud service. For more information, see Registering the Cisco Advanced Phishing Protection Sensor on the Email Gateway, on page 4.
- Enabled Advanced Phishing Protection on the email gateway. For more information, see Enabling Advanced Phishing Protection on the Email Gateway, on page 6.

Procedure

Step 1 Log in to the Cisco Advanced Phishing Protection cloud service.

Step 2 Choose **Manage** > **Users**.

Step 3 Click the required username.

Step 4 Click **Generate API Secret** link to generate the API Access keys.

Step 5 Copy the **API Access UID** and **API Access Secret** keys locally on your system.

Note
In case if you do not copy the API Access keys and close the Cisco Advanced Phishing Protection cloud service, you need to follow steps **1-3** of the procedure and click **Regenerate API Secret** link to obtain new API Access keys.

Step 6 Log in to the legacy web interface of your email gateway.

Step 7 Go to **Security Services**> **Advanced Phishing Protection**.

Step 8 Click **Edit Settings** under 'Advanced Phishing Protection API Access' section.

Step 9 Enter the **API Access UID** key in the 'API Access UID' field.

Step 10 Enter the **API Access Secret** key in the 'API Access key field.

Step 11 Click **Submit**.

What to do next

Enable forwarding of message metadata to the Cisco Advanced Phishing Protection cloud service. For more information, see Configuring Incoming Mail Policies to Enable Forwarding of Message Metadata, on page 7.

Configuring Incoming Mail Policies to Enable Forwarding of Message Metadata

You can configure mail policies to enable forwarding of message metadata to the Cisco Advanced Phishing Protection cloud service.

When you enable the Cisco Advanced Phishing Protection cloud service on your email gateway, the following message headers are shared with the Cisco Advanced Phishing Protection Cloud service :

- Authentication-Results
- Authentication-Results-original
- DMARC-result
- DKIM-domain
- DKIM-result
- DKIM-selector
- DKIM-signatures
- From-header

- Full-Header-From
- HELO_domain
- Last-Hop-IP-Address
- List-ID
- Mail-From
- Mailing-list
- Message-ID
- Rcpt-To
- Received-Header
- Received-SPF
- Received-Timestamps
- Reply-To
- SPF-result
- Subject-header
- To-header
- Originator-Return-Address
- X-Mailer
- X-Original-Authentication-Results
- X-Original-From
- X-Original-To
- X-Original-Sender
- X-Originating-IP
- X-OriginatorOrg
- X-Received

Before you begin

Make sure that you have:

- Registered the email gateway as a sensor on the Cisco Advanced Phishing Protection cloud service. For more information, see Registering the Cisco Advanced Phishing Protection Sensor on the Email Gateway, on page 4.
- Enabled Advanced Phishing Protection on the email gateway. For more information, see Enabling Advanced Phishing Protection on the Email Gateway, on page 6.

Procedure

Step 1 Log in to the email security gateway.

Step 2 Go to **Mail Policies > Incoming Mail Policies**.

Step 3 Click the link below APP Filter.

Step 4 Select **Enable Advanced Phishing Protection (Customize Settings)** from the drop-down list.

Step 5 Select the check box for **Enable Forwarding**.

Step 6 Click **Submit** and commit your changes.

Monitoring Message Metadata on the Cisco Advanced Phishing Protection Cloud Service

You can monitor metadata of the message that your email security gateway forwards to the Cisco Advanced Phishing Protection cloud service. The Analyze > Messages page of the cloud service provides insights on the source of the message and the risk associated with the message and the senders.

The metadata of the message on the Cisco Advanced Phishing Protection cloud service receives a trust score based on the following:

- Message Authenticity
- Domain Reputation
- Sender Legitimacy

Advanced Phishing Protection and Clusters

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

Note When you disable the Advanced Phishing Protection at the machine level, the same is disabled on the group and cluster levels.

Advanced Phishing Protection Report Page

The **Monitor > Advanced Phishing Protection** report page displays the following:

- Total number of messages successfully forwarded to the Cisco Advanced Phishing Protection cloud service.

- Total number of messages that are not forwarded to the Cisco Advanced Phishing Protection cloud service.

Note If the forwarding of message metadata has failed, you must validate the configurations of the Advanced Phishing Protection feature. For more information, see How to Integrate Email Gateway with the Cisco Advanced Phishing Protection Cloud Service, on page 3.

You can use the Advanced Phishing Protection report page to view:

- Total number of messages attempted to be forwarded to the Cisco Advanced Phishing Protection cloud service, in a graphical format.
- Summary of messages forwarded to the Cisco Advanced Phishing Protection cloud service in a graphical format.

To view the detailed information on the metadata of the message that is forwarded to the Cisco Advanced Phishing Protection cloud service, click on the link and login to the Cisco Advanced Phishing Protection cloud service. For more information, see Monitoring Message Metadata on the Cisco Advanced Phishing Protection Cloud Service, on page 9.

Monitoring Message Metadata on the Cisco Advanced Phishing Protection Cloud Service

You can monitor metadata of the message that your email security gateway forwards to the Cisco Advanced Phishing Protection cloud service. The Analyze > Messages page of the cloud service provides insights on the source of the message and the risk associated with the message and the senders.

The metadata of the message on the Cisco Advanced Phishing Protection cloud service receives a trust score based on the following:

- Message Authenticity
- Domain Reputation
- Sender Legitimacy

Displaying Messages Submitted to the Cisco Advanced Phishing Protection Cloud Service

You can view the metadata of the message that you forward to the Cisco Advanced Phishing Protection cloud service corresponding to the success and failure.

Before you begin

Make sure that you enable the Message Tracking feature on the email gateway. To enable Message Tracking, go to **Security Services > Centralized Services > Message Tracking** page in the web interface.

Procedure

Step 1 Log in to the email security gateway.

Step 2 Go to **Monitor > Message Tracking**.

Step 3 Click **Advanced**.

Step 4 Check **Advanced Phishing Protection Forwarding** under Message Event.

Step 5 (Optional) Select **Select Successful** to view messages that are forwarded successfully to the Cisco Advanced Phishing Protection cloud service.

Step 6 (Optional) Select **Failed** to view messages that are not forwarded to the Cisco Advanced Phishing Protection cloud service.

Step 7 Click **Search**.