



# **User Guide for Cisco Advanced Phishing Protection**

**First Published:** 03-03-2020

---

**Cisco Systems, Inc.**

[www.cisco.com](http://www.cisco.com)

Cisco has more than 200 offices worldwide.

Addresses, phone numbers, and fax numbers are listed on the Cisco website at

[www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco, Inc.

170 West Tasman Dr.

San Jose, CA, 95134, USA

[www.cisco.com](http://www.cisco.com)

Updated: Tuesday, March 3, 2020

Copyright 2020, Cisco, Inc.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

ALL DATA IS PROVIDED "AS IS" AND CISCO, INC MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF ACCURACY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR ARISING FROM COURSE OF PERFORMANCE, DEALING, USAGE OR TRADE, AND CISCO, INC WILL HAVE NO LIABILITY FOR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS, LOST PROFITS, DATA OR BUSINESS, OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Domain Protection™ is a trademark of Cisco, Inc.

All trademarks mentioned in this document or website are the property of their respective owners.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



# Table of Contents

About Advanced Phishing Protection .....	10
Terms of Service .....	10
Before You Begin .....	10
Identify Key Project Team Members .....	11
Review Important Materials .....	11
Gather Initial Data .....	12
What's New in Advanced Phishing Protection .....	13
Sensors .....	16
Placing Sensors In Your Infrastructure .....	16
Sensor Planning .....	17
Mail Infrastructure .....	17
Where is MX delivery? .....	18
What is the first inbound email platform hop? .....	18
Where is mailbox delivery for all user mailboxes? .....	18
Hosted Environment .....	18
Is this a hybrid environment with both Office 365 and Exchange on-premises? .....	18
If so, what is the current state of user mailbox migration to Office 365? .....	18
Sensor Deployment .....	19
Dual-Delivery .....	19
Dual-Delivery Sensor Architecture and Data Flows .....	20
Step 1 .....	20
Step 2 .....	20
Sensor Prerequisites .....	21
Hardware and Software Requirements .....	21
Firewall requirements .....	22
Firewall Rules: Required HTTPS Access .....	22

	Docker Installs .....	23
	Packages .....	23
Postfix .....		23
	Sensor Installation .....	23
	Install additional Sensors .....	24
	Install a Sensor Via Script .....	24
Running the Script .....		24
	Install a Sensor Via OVA .....	29
About OVA files .....		29
Notes before you begin .....		30
Default sensor configuration .....		32
	Sensor Configuration and Operation .....	33
Admin account commands .....		37
	Test a Sensor .....	38
	Troubleshooting Test Email .....	39
	View Sensor Status .....	39
	Download Sensor Diagnostic Information .....	41
Configuring Delivery to the Sensor .....		42
	Configuring Dual Delivery .....	42
	Interrupting Dual Delivery .....	42
	Specific Dual Delivery Instructions .....	43
	Configure Dual Delivery: G Suite .....	43
Wrapping Up .....		47
	Configure Dual Delivery: Office 365 .....	48
	Configure Dual Delivery: Microsoft Exchange .....	53
Configure Dual Delivery: Exchange 2010 .....		54
Configure Dual Delivery: Exchange 2013/2016 .....		57
Test Exchange Dual Delivery .....		60
	Configure Dual Delivery: Cisco ESA .....	60
Important Consideration Regarding the " Authentication-Results" Header .....		61
Configure Cisco ESA to Add an X-Agari-Authentication-Results Header .....		72
	Wrapping Up .....	74



Enforcement .....	75
Configure Enforcement: G Suite .....	75
Wrapping Up .....	82
Configure Enforcement: Office 365 .....	82
Testing the API Enforcement Action with Policies .....	84
Managing Enforcement using Microsoft Office 365 Auditing Tools .....	86
Enabling Auditing .....	86
Performing an Audit .....	87
Enforcement Action Log Example - PowerShell .....	88
Enforcement Action Log Example - WebUI .....	89
Wrapping Up .....	91
Configure Enforcement: Microsoft Exchange .....	92
Enforcement Sensor Status .....	94
Reporting on API Enforcement .....	95
Why are some messages not moved? .....	97
Using Advanced Phishing Protection .....	98
The Workflow .....	98
Manage Suspicious Messages .....	98
Analyze Incoming Email Traffic .....	99
Trust Score .....	99
Zooming In .....	101
Quick Domain Search .....	101
Attack Classifications .....	102
Attack Taxonomy .....	102
Domain Spoof .....	102
Look-alike Domains .....	103
Display Name Impostor .....	103
Compromised Account (Account Take Over) .....	104
Low Trust Domains .....	104
Malicious Attachment .....	105
Likely Malicious URI .....	105

Spam or Graymail .....	105
Messages .....	106
View Messages .....	106
View Message Details .....	107
Send Message to Phishing Response .....	109
Send Message Feedback .....	109
Message Search .....	110
Search Messages .....	113
Download Message Search Results .....	113
Domains and IP Addresses .....	114
View Domain Details .....	115
Domain Tags .....	116
Add a Tag to a Domain .....	117
Delete a Tag from a Domain .....	117
View IP Address Details .....	117
Notifications .....	118
Add a Notification Recipient .....	119
Delete a Notification Recipient .....	119
Policies .....	119
Default Policies .....	120
Create a Policy .....	121
Edit a Policy .....	122
Enable or Disable a Policy .....	122
Delete a Policy .....	122
Customize Policy Notifications .....	122
Policy Notification Content Settings .....	123
Policy Notification Content Variables .....	123
Policy Settings .....	123
Create a Test Policy .....	127
Specifying Actions .....	128
View Policy Results .....	128
Policy Log .....	128

Policy Report .....	129
Reporting on Enforcement .....	129
Search Messages .....	129
On-demand Policies .....	130
On-demand Policies Index Page .....	130
Final Notes .....	130
Performance Note .....	131
Create an On-Demand Policy .....	131
Reports .....	134
Reports Page .....	134
Threat Trends and Executive Summary Reports .....	135
Threat Trends Tab .....	135
Executive Summary Tab .....	136
Threat Trends Reports .....	136
Messages Report .....	137
Attacks Report .....	138
Top Policies Report .....	138
Executive Summary Reports .....	138
How Many Attacks Were Found Report .....	139
How Much Have I Saved by Deploying Advanced Phishing Protection Report .....	140
Configure the How Much Have I Saved By Deploying Advanced Phishing Protection Report .....	141
Values for the How Much Have I Saved By Deploying Advanced Phishing Protection Report .....	142
Currency .....	142
Breach Cost Savings .....	142
BEC Cost Savings .....	142
How Attacked/Protected Am I Relative To My Peers Report .....	143
Compare to an Additional Peer Group .....	145
Download a Threat Trends or Executive Summary Report .....	146
Attachment and URL Analysis .....	147
Using Attachment Analysis .....	147
Using Attachment Analysis Results in Search and Policy .....	147

Attachment Scan Results .....	149
Details of the Attachment Scan .....	149
Using URL Analysis .....	149
Enable Attachment and URL Analysis .....	150
Basic Attachment Information Collection .....	150
Attachment Scanning .....	150
URL Scanning .....	151
Sender Management and Rapid DMARC .....	151
Manage Senders .....	151
Column Meanings and Usage .....	152
Sender Management With Rapid DMARC .....	153
Address Groups .....	154
Address Group Exceptions .....	155
Address Group Examples .....	155
Address Group In the From Field of a Policy .....	156
Address Group In the To Field of a Policy .....	156
Create an Address Group .....	156
Add an Email Address to an Address Group .....	157
Delete an Email Address from an Address Group .....	157
Edit an Address Group .....	157
Delete an Address Group .....	159
Azure Active Directory Synchronization With Address Groups .....	160
Notifications of Azure AD group sync failures .....	160
Skipped Addresses .....	160
Authorize Address Group Synchronization .....	161
<b>Administration .....</b>	<b>163</b>
<b>Organization Settings .....</b>	<b>163</b>
Administrative Tab .....	163
Processing Exceptions Tab .....	167
<b>Audit Trail .....</b>	<b>169</b>
View Organization Activity .....	169

User Accounts .....	170
Create a User Account .....	170
Edit a User Account .....	171
Delete a User Account .....	171
Sign In to Advanced Phishing Protection .....	171
View User Activity .....	171
Configure Global User Account Settings .....	172
User Account Settings .....	172
User Information .....	172
User Roles .....	173
Role Examples .....	174
Single Sign-On (SSO) .....	175
Logging In With SSO .....	175
Enable Single Sign-On for Your Organization .....	175
Application Programming Interface .....	177
Generate API Secret .....	177
View API Documentation .....	177



## CHAPTER 1

# About Advanced Phishing Protection

Cisco Advanced Phishing Protection provides unprecedented insight into the email coming in to your organization, flowing out of your organization, and within your organization. Powered by Cisco Identity Intelligence – Cisco's unique machine learning techniques based on historical email traffic to your organization – Advanced Phishing Protection models the unique behavior of all legitimate email senders and allows you to quickly distinguish good messages from potentially bad messages. Coupled with Identity Intelligence, Cisco's platform of data – built from analyzing billions of email messages worldwide – provides you a risk overview of all messages in your organization and senders who send email into your organization.

Risky messages – such as phishing attempts or "business email compromise" (BEC) messages which may contain no malicious payload or questionable links – are delineated from known good messages.

Advanced Phishing Protection complements traditional secure email gateway (SEG) solutions by catching the spear phishing, targeted, low volume, and zero day attacks that typically are the weaknesses of traditional, reactive SEG security "layers."

Using the policy engine within Advanced Phishing Protection, you can configure alerts to be sent to your end users about bad messages in near-real-time, and you can even move potentially dangerous messages out of your end-users' inboxes altogether.

## Terms of Service

A Cisco Terms of Service (TOS) must be reviewed and accepted before anyone at your organization can use Advanced Phishing Protection. The TOS is presented in one of two ways:

- For most organizations, the first person to log in to Advanced Phishing Protection will be presented the TOS on first login. The TOS must be accepted during that first login.
- For organizations with a master sales agreement, the TOS is managed and accepted outside of the Advanced Phishing Protection application by the Cisco sales team.

## Before You Begin

When you are getting ready to implement Advanced Phishing Protection in your organization, there are several steps you should take before you begin so the implementation will proceed smoothly. This section details what you should do to prepare, and includes:

- Identifying key project team members
- Reviewing important materials
- Gathering initial data

## Identify Key Project Team Members

Having the right people filling the right roles will be important for Advanced Phishing Protection implementation.

Some people may fill multiple roles, while some roles may be filled by multiple people.

The roles in your organization you will want to have filled are:

- **Executive sponsor** - To act as point of escalation for critical issues and project roadblocks.
- **Project owner** - Responsible for the overall success of this project.
- **Project manager** - The primary point of contact, serving as the interface to your organization and responsible for
  - ensuring the project moves forward on the agreed-upon schedule
  - working with other internal groups and departments
- **Deployment engineer** - The expert in your deployment and the primary technical contact for the project.
- **Subject matter experts** - Technical leaders that provide input into the design and integration; they ensure decisions are in line with the organization's business strategy.
- **Messaging architect**
- **Security architect**

## Review Important Materials

Understanding the concepts that underlie Advanced Phishing Protection and the way Advanced Phishing Protection works and interacts with your email infrastructure will help you make good decisions when you are implementing Advanced Phishing Protection. The information you should review in advance includes:

- The User Guide for Cisco Advanced Phishing Protection
- Training videos, including:
  - Creating New Users: <https://cl.ly/qrPd>
  - Benefit of Domain Tagging: <https://cl.ly/2A1m2w391L1Z>
  - Inbox Policies and Whitelisting: <https://cl.ly/1V2w1u463k3e>
  - Reconfiguring the Messages That Recipients Receive Due To a Triggered Policy: <https://cl.ly/1v381o3F0K0A>

## Gather Initial Data

You will want essential details about your email infrastructure in one place for quick reference.

- What is your email architecture? Create a diagram showing the end to end mail flow for determining optimal Sensor placement in your environment. The Sensor essentially acts as an SMTP “message sink;” it accepts copies of email messages over SMTP and extracts metadata in a streaming fashion. Message bodies and attachments are discarded. No SMTP messages leave the Sensor.
- Determine if the sensor be hosted (preferred) or on-premises by your organization.
- Are DKIM and SPF checks currently being performed? If not we recommend enabling DKIM and SPF. (Cisco Domain Protection can help you with this.)

Note that data modeling will be slower to adjust and less complete without these authentication results.

- Review requirements for Sensor installation.
- Capture key users or critical groups to be protected.
- Make note of your questions and provide the best times to schedule a call with support upon completing this prework guide.





## CHAPTER 2

# What's New in Advanced Phishing Protection

Cisco is always working to improve the Advanced Phishing Protection product, from fixing issues to improving existing features to adding new features. This section highlights the feature changes made in Advanced Phishing Protection, as well as documentation updates not necessarily related to product features.

Release	Date	Update Details
2020.02	February 2020	<ul style="list-style-type: none"> <li>Email addresses in the journaling topic had the incorrect domain for Advanced Phishing Protection. This has been corrected.</li> <li>Processing exceptions can now be defined so messages will not be evaluated. See "Processing Exceptions" on page 167 for details.</li> </ul>
2020.01	January 2020	<ul style="list-style-type: none"> <li>Clarified that on-demand policies created from search results can only apply to inbound messages. This is relevant when insider impersonation is enabled and inbound, outbound, and internal messages are being ingested by the Sensor. See "Create an On-Demand Policy" on page 131 for details.</li> </ul>
2019.12	December 2019	<ul style="list-style-type: none"> <li>Clarified mail routing configuration for G Suite. See "Configure Dual Delivery: G Suite" on page 43.</li> <li>Added section on Skipped Addresses for Azure Active Directory address group synchronization. See "Azure Active Directory Synchronization With Address Groups" on page 160.</li> <li>Added information about the Allowed Forwarding IPs setting in the Sensor Settings section of organization settings. See "Organization Settings" on page 163.</li> </ul>
2019.11	November 2019	<ul style="list-style-type: none"> <li>Updated the Sensor requirements. On-premises Sensors now require Python 2.7 or newer.</li> <li>Corrected the naming for Sensor configuration.</li> </ul>
2019.10	October 2019	<ul style="list-style-type: none"> <li>The guide used "global administrator" in a couple of places that were causing confusion, leading users to believe that the role was required for Advanced Phishing Protection to access their systems. In reality, certain access permissions are required just to configure those systems to allow access by Advanced Phishing Protection. The content was changed in those places to more accurately reflect this.</li> <li>Google changed its terminology, no longer referring to "Google Developers Console." The topic for configuring enforcement in G Suite was updated to reflect Google's new nomenclature.</li> </ul>

Release	Date	Update Details
		<ul style="list-style-type: none"> <li>• New reference topic for notification settings. See Notification Settings.</li> <li>• Clarified that Cisco employees cannot make changes to Advanced Phishing Protection user accounts. See "User Accounts" on page 170.</li> <li>• Plain text search fields in Advanced Phishing Protection are now limited to 100 characters.</li> </ul>
2019.09	September 2019	<p>Advanced Phishing Protection has added insider impersonation protection (IIP), giving you 360-degree monitoring of your mail stream: incoming messages, outgoing messages, and internal messages.</p> <p>IIP requires Microsoft 365 or Exchange as your email provider and you must:</p> <ul style="list-style-type: none"> <li>• Explicitly enable this feature in your organization settings. See "Messages Settings" on page 164 for more information.</li> <li>• Insure the proper directionality headers are added to all messages. See "Configure Dual Delivery: Office 365" on page 48 and "Configure Dual Delivery: Microsoft Exchange" on page 53 for more information.</li> </ul> <p>Message directionality is also available in search and policy criteria. See "Message Search" on page 110 and "Policy Settings" on page 123 for more information.</p>
2019.08	August 2019	<ul style="list-style-type: none"> <li>• In message searches and policy settings, for parameters that are numeric and have upper and lower bounds, the upper and lower bound values are now inclusive.</li> </ul>
2019.07	July 2019	<ul style="list-style-type: none"> <li>• The attack vs. peer enforcement graph has been enhanced to clarify its values. See "How Attacked/Protected Am I Relative To My Peers Report" on page 143.</li> <li>• Information about how to prepare for using Advanced Phishing Protection (see "Before You Begin" on page 10) and how to access the Advanced Phishing Protection API documentation (see "Application Programming Interface" on page 177) has been added to this guide.</li> <li>• Additional detail about default policies has been added to this guide. See "Default Policies" on page 120.</li> </ul>
2019.06	June 2019	<ul style="list-style-type: none"> <li>• Advanced Phishing Protection no longer officially supports Sensors in an inline architecture, so that information has been removed from this guide.</li> <li>• Reference content for message search has been added. See "Message Search" on page 110 for details.</li> <li>• Message search results can now be downloaded. See "Download Message Search Results" on page 113 for details.</li> </ul>
2019.05	May 2019	<p>Most of the changes in this version of the guide are correction, clarifications, updates because other systems changed, and bug fixes.</p>

Release	Date	Update Details
2019.04	April 2019	<ul style="list-style-type: none"> <li>The guide clarifies who can change report values. See "Configure the How Much Have I Saved By Deploying Advanced Phishing Protection Report" on page 141 for details.</li> <li>Additional information about how the internal and partner tags are used and best practices for applying them to domains was added to the Domain Tags topic. See "Domain Tags" on page 116 for details.</li> </ul>
2019.03	March 2019	<ul style="list-style-type: none"> <li>You can now set custom date ranges for the Threat Trends and Executive Summary reports.</li> <li>Clarifications were added for Sensor port requirements and for supported Sensor architecture.</li> <li>Additional organization settings are available for how an organization is classified. These classifications, including region, industry, and organization size, are used for one of the executive summary reports. See "How Much Have I Saved by Deploying Advanced Phishing Protection Report" on page 140.</li> </ul>
2019.01	Winter 2019	<ul style="list-style-type: none"> <li>Reporting improvements                     <p>A new set of reports are available in Threat Trends and Executive Summary tabs on the home page, reports that provide at-a-glance views of the benefits of using Advanced Phishing Protection. These reports show a daily updated view of the value that Advanced Phishing Protection provides, and you can download a snapshot of either page as an Adobe Acrobat (PDF) file. Additional organization settings allow customization of the message data in the reports. Find out more in "Threat Trends Reports" on page 136 and "Executive Summary Reports" on page 138.</p> </li> <li>Message feedback improvements                     <p>Advanced Phishing Protection now allows you to provide more details when sending feedback about an individual message. See "Send Message Feedback" on page 109 for details.</p> </li> </ul>



## CHAPTER 3

# Sensors

Cisco Advanced Phishing Protection relies on a Sensor to receive a copy of all messages sent inbound into your organization. Installing a Sensor is the first critical step toward realizing the value of Advanced Phishing Protection.

The purpose of the Sensor is to collect per-message information from your organization's inbound email stream and to relay that information to the Advanced Phishing Protection cloud for analysis. That information includes:

- Message metadata
- Attachments (when enabled)
- URLs (when enabled)

The Sensor is secure, lightweight (requiring minimal resources), and optimized for high performance. It plays a key role in enforcing malicious messages.

Sensors can accept messages that are up to 100 MB in size. If you have attachment scanning enabled (see "Attachment and URL Analysis" on page 147), the total size of a message and its attachments, including any overhead required for encoding, must not be more than 100 MB for the Sensor to accept the message.

## Placing Sensors In Your Infrastructure

You have two basic choices about where to place Sensors:

- You can provision host systems in your own environment for running Sensors, a configuration generally recommended only when you're also running your own Exchange server because you typically want the Sensor close to your mail store for better efficiency. But it also requires that you explicitly update your Sensor instances when updates are available and add Sensors manually when your mail load increases.
- You can have Cisco host Sensors on your behalf in an administratively separate, secure cloud, which is the recommended configuration when you're using any cloud service, such as Office 365 and Gsuite. Hosted Sensors are not only updated as necessary by Cisco, hosted Sensor capacity is also scaled by Cisco as necessary. (Contact your Cisco sales engineer for more information on Cisco-hosted Sensors.)

If you provision your own Sensor, you should connect and integrate it in a place in your infrastructure where it can receive copies of messages that get delivered internally – after other scanning (anti-spam, anti-virus, anti-malware) has taken place on messages. The Sensor for Advanced Phishing Protection should only “see” messages that have passed through these filters and that are deemed worthy of delivery.

If you have a hosted email infrastructure (such as Google Apps or Microsoft Office 365), the same theory applies: you will direct a copy of your mail stream to the Advanced Phishing Protection Sensor after all other filtering and scanning has taken place.

Cisco supports Sensors configured as dual-delivery, deployed as Cisco-hosted or on-premises, as follows:

<b>Dual-Delivery Sensors</b>	
Cisco-Hosted (preferred)	Provides the highest-performance option of dual-delivery with the robustness of Cisco-managed scaling and updating of Sensors. This combination is the preferred option.
On-Premises	Provides the highest-performance option of dual-delivery, but Sensor and Sensor host updates are performed by customer. Typically used when security rules preclude email traffic from being sent outside the email infrastructure.

For on-premises Sensors, you can configure and use a bare-metal machine or run the Sensor software in a virtual machine. For the latter, you can configure the virtual machine manually or download a pre-configured virtual machine package.

If you run your on-premises Sensors on bare metal or your own virtual machine, all Sensor operation is performed through a command line, which requires you to access the machine from a secure shell (ssh). If you use the pre-configured virtual machine package, a character-based front end provides easy access to Sensor information and to its control commands.

Initial Sensor configuration, including its IP address, NTP, DNS, and password, is performed by a VMWare admin via the VMWare console before you can access the Sensor via ssh.

## Sensor Planning

A number of considerations determine how your Sensor will be installed and configured, including

- Mail infrastructure
- Hosted environment
- Deployment

## Mail Infrastructure

Your mail infrastructure can help determine the Sensor installation type. A few fundamental questions can help you determine your installation type.

## Where is MX delivery?

The MX record for your organization is the publicly-facing mail exchange record for your domain (s). The MX record may be pointing to:

- SEG - a Secure Email Gateway, such as a Cisco ESA
- Office 365 - a hosted solution from Microsoft
- Google - a hosted solution from Google

## What is the first inbound email platform hop?

Some customers have a “tiered” environment, where an internal “hop” routes email from the address of the MX record environment to a second gateway. For example, this “next hop” may be:

- Google (G Suite)
- Office 365 (O365)
- Exchange on-premises (on-prem)
- Conditionally at one of multiple sites, each with Exchange on-prem

## Where is mailbox delivery for all user mailboxes?

If mailbox delivery (where end-user mailboxes are store) may entail yet another “hop.” For example, the answer to this question may be:

- The same environment as the first email platform hop (question 2 above)
- Across a hybrid environment (either Office 365 or Exchange on-prem)
- It depends on which mailbox (hybrid with partial mailbox migration)

Some customers have hybrid environments where some mailboxes are being transitioned from on-premises environments to hosted environments.

## Hosted Environment

Additionally, if your environment is hosted in G Suite or Office 365, these questions will help determine your sensor installation strategy:

## Is this a hybrid environment with both Office 365 and Exchange on-premises?

Hybrid environments allow migration of user mailboxes from Exchange on-premises to Office 365

## If so, what is the current state of user mailbox migration to Office 365?

The mailbox migration may have 3 phases and associated timelines

- Pre-migration - all mailboxes are still on Exchange on-prem
- Partial-migration - some mailboxes moved to O365, some still on Exchange on-prem

- Post-migration - all of the mailboxes are on O365

Knowing when the client will have all user mailboxes on Office 365 is key to:

- Maximizing your ability to use all Advanced Phishing Protection features as soon as possible.
- Minimizing change requests and associated risk with transitioning your installation.

## Sensor Deployment

Sensor deployment is dual delivery because it allows on-demand enforcement (for Office 365 and G Suite customers), and it lowers the risk from client change management.

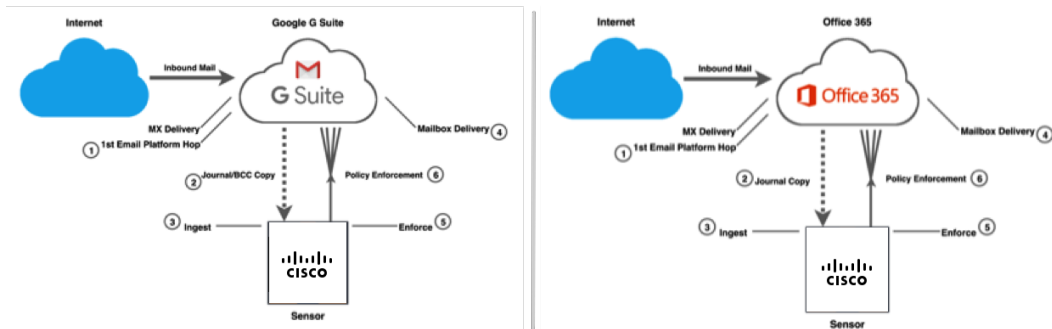
## Dual-Delivery

The Sensor essentially acts as an SMTP “message sink.” It accepts copies of email messages over SMTP and extracts in a streaming fashion the parts of messages necessary for threat analysis:

- Message metadata
- Attachments (when enabled)
- URLs (when enabled)

Message bodies are discarded. No SMTP messages leave the Sensor.

Dual-delivery is typically used for hosted email architectures such as Office365 and G Suite.

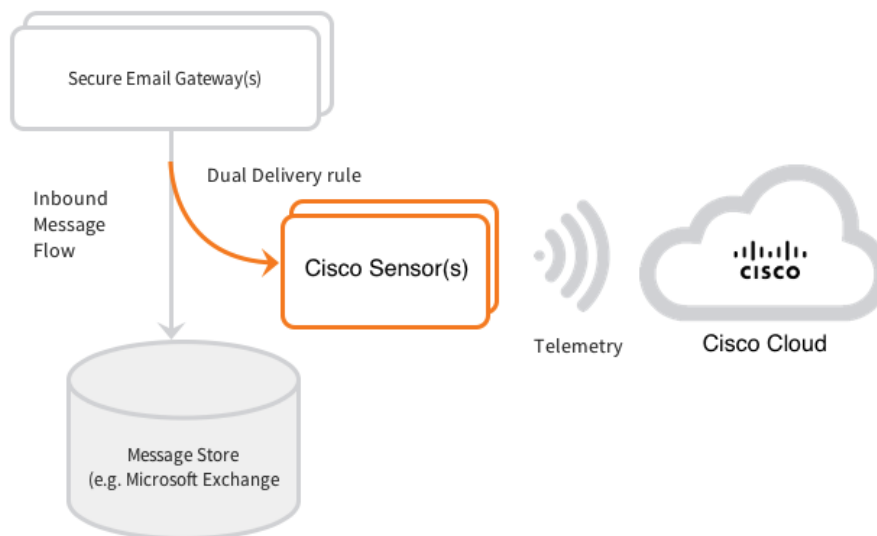


Dual-delivery installations using journaling/API mail flow

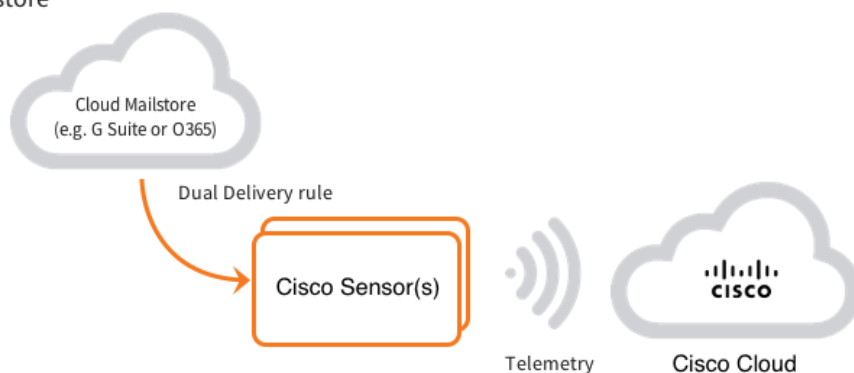
1. Inbound mail sent to the first email platform hop (SEG may or may not be in front), which filters out spam, viruses, and other unwanted messages.
2. Office 365 or G Suite sends a Journalled copy or bcc: copy of messages to the Sensor and continues original delivery.
3. Sensor ingests journal copy for scoring and policy evaluation.
4. Office 365 or G Suite delivers original messages to mailbox.
5. Sensor will enforce policy using an API to access individual mailboxes.
6. The policy enforcement action occurs at the mailbox based on policy result.

## Dual-Delivery Sensor Architecture and Data Flows

### On-premises Gateways



### Hosted Mailstore



### Dual-delivery Sensor architecture

#### Step 1

Messages arrive at the customer secure email gateway (SEG) or hosted mailstore and are accepted for spam and virus filtering.

#### Step 2

After first level spam and virus filtering, the customer SEG delivers a copy of message (via a dual delivery rule or journaling capability) to the Cisco Sensor over an SMTP connection, typically on port 25 (although this can be configured to a different port when the Cisco Sensor is installed). Inbound messages are queued while the Cisco filter process parses the message data to be transmitted to the Cisco pipeline for scoring and policy evaluation.

The parsed email message data is sent to the Cisco pipeline over an HTTPS connection using port 443.



## Sensor Prerequisites

In on-premises deployments, Sensors can be installed on bare-metal installs or a hosted virtual machine (VM). If you use a virtual machine, you can configure your own by following the instructions in this guide or you can download a pre-packaged, pre-configured virtual machine disk image.

For a bare-metal install or your own virtual machine, the Advanced Phishing Protection Sensor is distributed by Cisco via an installation script that is uniquely keyed to your organization. The installation script installs the Sensor application, which is distributed via a Docker container (see <https://www.docker.com/what-docker>). The container wraps the Sensor application in a complete file system containing everything needed to run the application: code, runtime, system tools, and system libraries.

For the pre-packaged, pre-configured virtual machine disk image, you download an OVA file from within Advanced Phishing Protection, which you can import into any supported virtualization software.

You should obtain the script to install your first Sensor from your Cisco Sales representative. After you gain access to the web application, you can obtain a script to install additional Sensors from the Manage > Sensors page. This script is uniquely keyed for your organization.

## Hardware and Software Requirements

If you are installing on bare metal or your own virtual machine, the machine or machine instance must meet the following minimum requirements. If you are using the virtual machine disk image, it is already pre-configured to these requirements, and you should be running the virtualization software on hardware that meets these requirements.

System	Requirement
CPU	Intel or AMD x86_64, 8 cores
Memory	32GB
Disk	The following minimum allocations: <ul style="list-style-type: none"> <li>• /var/opt/agari/: 100GB</li> <li>• /opt/agari/: 20GB</li> <li>• /var/lib/docker: 20GB</li> </ul>
Operating System	Modern, 64-bit Linux: <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux 7.4 or later</li> <li>• CentOS 7.4 or later</li> <li>• Ubuntu 16 or later</li> </ul>
Docker	17.06 or later
Packages	Python 2.7, and added to the \$PATH system variable
Network	1 Gbit/sec recommended
Hypervisor	VMWare ESXi

## Firewall requirements

When a Sensor is installed in your infrastructure, it will need to be able to communicate with the Cisco cloud. Below is a list of firewall requirements for the Sensor:

Port Requirement	Definition
Inbound: 25 (SMTP)	For receiving stream of inbound, duplicated messages from your gateway.  This port is required to be opened for any configuration where the Sensors reside on a different network from the Exchange server that is separated by a firewall.
Outbound: 443 (HTTP/S)	HTTP/S requests to the Cisco cloud and other cloud services (details below).  The Sensor can be configured to use a proxy for outbound HTTP/S connections
Outbound: 53 (DNS)	DNS for hostname/IP address resolution.  If the host system is using 127.0.* or localhost for the DNS resolution, Docker will not replicate that in the container's /etc/resolv.conf file. Instead it will set the DNS to 8.8.8.8 and 8.8.4.4, and if you do not have these addresses available through the firewall, DNS will fail.  You may need to set the host's DNS servers to the actual address of the internal DNS servers used in your enterprise.
Outbound: 123 (NTP)	NTP for time synchronization services Note: On RedHat systems, you can verify that NTP is working correctly by issuing these commands:  ntpstat echo \$?  You want the output of the last command to be a 0 if the NTP server is being accessed. See the RedHat documentation for more information on checking the status of NTP.  <a href="https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/s1-Checking_the_Status_of_NTP.html">https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/s1-Checking_the_Status_of_NTP.html</a>

## Firewall Rules: Required HTTPS Access

The system on which the installation script will be run requires access to the following endpoints in order for the script to successfully execute:

- <https://agari-ep-collector-config-prod.s3.amazonaws.com>
- <https://agari-ep-collector-config.s3.amazonaws.com>
- <https://agari-ep-collector-ingest-avro.s3.amazonaws.com>
- <https://agari-ep-collector-milter-prod.s3.amazonaws.com>
- <https://agari-ep-collector-milter.s3.amazonaws.com>
- <https://aws.amazon.com>

- <https://kinesis.us-west-2.amazonaws.com>
- <https://s3-us-west-2.amazonaws.com>
- <https://sns.us-west-2.amazonaws.com>
- <https://sqs.us-west-2.amazonaws.com/>
- <https://us-west-2.queue.amazonaws.com/>
- <https://registry.ep.agari.com>
- <https://registry-cdn.ep.agari.com>
- <https://sensor-provisioner.ep.prod.agari.com>

## Docker Installs

The Docker documentation has instructions for installing Docker with the Linux versions Cisco supports to run the sensor:

- Red Hat: <https://docs.docker.com/install/linux/docker-ee/rhel/> (Docker EE)
- CentOS: <https://docs.docker.com/install/linux/docker-ee/centos/> (Docker EE) or <https://docs.docker.com/install/linux/docker-ce/centos/> (Docker CE)
- Ubuntu: <https://docs.docker.com/install/linux/docker-ee/ubuntu/> (Docker EE) or <https://docs.docker.com/install/linux/docker-ce/ubuntu/> (Docker CE)

## Packages

If you modify your Linux distribution, you may need to be aware of the packages that the installation script and the Sensor require or are incompatible with.

## Postfix

Some Linux distributions enable a Postfix server by default. If a default Postfix server is running, it must be disabled before running the Sensor installation script. (The Sensor will install its own customized version of a Postfix server for receiving messages.)

Disable and remove the Postfix server by running this command:

```
# sudo yum remove postfix
```

## Sensor Installation

When you install a Sensor, you have a choice to:

- Install a Sensor on bare metal or your own virtual machine via a script you obtain from Cisco. See "Install a Sensor Via Script" on the facing page.
- Install a Sensor via a downloadable pre-packaged, pre-configured virtual machine disk image (OVA). See "Install a Sensor Via OVA" on page 29.

## Install additional Sensors

Because they are evaluating only individual message metadata, plus extracted attachments and URLs if enabled, and discarding the message body, Cisco's Sensors are highly efficient. Based on the number of inbound messages you plan to duplicate from your mail store/email gateways, you may want to configure additional Sensors for either redundancy or increased throughput. To install an additional Sensor, simply run the installation script on a new instance.

A single Sensor has a capacity to sustain throughput of 3Mb/sec (megabits per second). A load balanced, dual Sensor configuration is strongly recommended in a production environment for redundancy.

## Install a Sensor Via Script

You will obtain the first Sensor installation script from your Cisco sales engineering representative. The script will be named something like:

```
sensor-install-<orgname>-<date>.sh
```

You should run the script promptly after receiving it. Attempting to install older, outdated versions of the Sensor installation script may result in errors. When in doubt, be sure that you have received the very latest version of the Sensor installation script.

You can rename the file.

Move the file to the host system (via SCP, for example). If necessary, after moving the file you may need to set the permissions so that the script can be executable. For example:

```
# chmod +x sensor-install-examplecom-2018-02-01.sh
```

In addition to the prerequisites mentioned in "Sensor Prerequisites" on page 21, ensure that you have the following items in order prior to running the installation script for the Sensor:

Do you have root access to the provisioned Linux machine?

Is the firewall configured to allow DNS, NTP, SMTP (inbound), and HTTP/S access to the Cisco Cloud and installation repositories?

Proxy: If using a proxy for HTTP traffic, do you have the proxy type (HTTP or NTLMO), hostname, port, username, and password available?

TLS traffic: During the installation, you can configure that inbound traffic to the Sensor be delivered via TLS. If you plan to use SMTP over TLS delivery to the Sensor, do you have a private key (.key file), a signed TLS certificate (.pem file), and a certificate chain (.pem file)?

## Running the Script

With all of prerequisites and dependencies in consideration, you can execute the installation script.

The script is comprised of the following stages:

1. Print the version of the script
2. Create the directories /opt/agari and /var/opt/agari/etc
3. Stops any existing Cisco Sensor services, if necessary

4. Extract installation files into a temporary directory
5. Install Docker
6. Install PyYAML (if necessary)
7. Install AWS tools (AWS, AWS SSL)
8. Prompt for additional UNIX group permissions for the logs and configuration files (optional; the root group will be used by default)
9. Prompt for HTTPS proxy configuration (optional)
10. Test for access to the correct S3 buckets for uploading data
11. Prompt for TLS certificates and TLS configuration for connections to the Sensor (the default is OFF - TLS connection required)
12. Prompt for debugging-level log output (OFF by default)
13. Move files to appropriate directories; deletes temporary files
14. Upgrade the version of the Sensor (if necessary)

An example of the script being run on an Linux Ubuntu image is below. In the following example, please note:

- Your installation script output will not be identical. The text below is provided as an example.
- Your organization ID is unique.
- The Access key ID is for access to AWS.
- Docker and AWS tools are installed if they are not found on the host system.
- You can specify a UNIX group permission for access to the logs and configuration data.
- You have the option to specify an HTTPS proxy.
- You can specify TLS certificates to use for SMTP connections to the Sensor.
- You can specify DEBUG-level logging.

Example of the running Sensor script:

Version number of the script	\$ sudo ./sensor-install-examplecom-2017-09-27.sh
Create Cisco directories	Cisco Advanced Phishing Protection Sensor Installation ... Wed Sep 27 21:49:03 UTC 2017 VERSION: 17.09.27035106  + mkdir -p /opt/agari /var/opt/agari/etc

	<pre> Extracting install files into /var/- opt/agari/tmp/agari.df8jXF  Running extracted install  Running Install/Upgrade steps...  • agari-collector.service - LSB: start and stop agari-col- lector-milter    Loaded: loaded (/etc/init.d/agari-collector; bad; vendor preset: enabled)    Active: inactive (dead) since Wed 2017-09- 27 14:46:21 PDT; 2min 42s ago    Docs: man:systemd-sysv-generator(8)    Process: 4664 ExecStop=/etc/init.d/agari-collector stop (code=exited, status=0/SUCCESS)    Process: 4284 ExecStart=/etc/init.d/agari-collector start (code=exited, status=0/SUCCESS)  Sep 27 13:38:33 ubuntu systemd[1]: Starting LSB: start and stop agari-collector-milter...  Sep 27 13:38:33 ubuntu agari-collector[4284]: net.ipv4.ip_forward = 1  Sep 27 13:38:33 ubuntu agari-collector[4284]: Waiting for agari-collectord to start...  Sep 27 13:38:34 ubuntu agari-collector[4284]: Started agari-collectord: PID 4299.  Sep 27 13:38:34 ubuntu systemd[1]: Started LSB: start and stop agari-collector-milter.  Sep 27 14:46:21 ubuntu systemd[1]: Stopping LSB: start and stop agari-collector-milter...  Sep 27 14:46:21 ubuntu agari-collector[4664]: agari- collectord is not running.  Sep 27 14:46:21 ubuntu systemd[1]: Stopped LSB: start and stop agari-collector-milter.  Sep 27 14:48:36 ubuntu systemd[1]: Stopped LSB: start and stop agari-collector-milter.  Warning: agari-collector.service changed on disk. Run 'systemctl daemon-reload' to reload units. </pre>
--	--

	<p>Writing sensor configuration to file: /var/-opt/agari/tmp/agari.df8jXF/etc/collector.yml</p>
<p>You can specify UNIX group permissions for access to the logs and configuration data</p> <p>You can specify an HTTPS proxy</p> <p>You can specify TLS certificated to use for SMTP connections to the Sensor</p> <p>You can specify DEBUG -level logging</p>	<p>Do you want to verify the AWS SSL server certificates used for communications from this sensor to AWS? [y/N](no)&gt;no</p> <p>You may optionally specify a Unix group that will be given read access to logs as well as write access to the collector's configuration and data.</p> <p>Group name (root):</p> <p>Will this sensor use an HTTPS proxy to send data to the Agari cloud? [y/N](no)&gt;</p> <p>Testing access to download S3 bucket...</p> <p>OK.</p> <p>Testing access to configuration S3 bucket...</p> <p>OK.</p> <p>Testing access to data ingest S3 bucket...</p> <p>OK.</p> <p>Testing access to statistical ping SNS topic...</p> <p>OK.</p> <p>Testing access to data ingest Kinesis stream...</p>

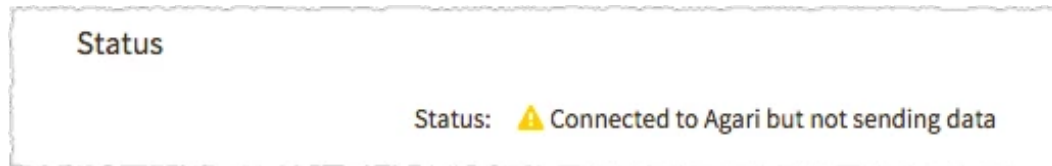
	<p>OK.</p> <p>Do you want to configure TLS Certificates for incoming SMTP traffic to this sensor? [y/N](no)&gt; n</p> <p>Require that all SMTP sessions use TLS? [y/N](no)?&gt; n</p> <p>Which port should this sensor listen on for incoming SMTP connections? [25]&gt;</p> <p>Enable DEBUG-level logging? [y/N](no)&gt; n</p> <p>+ : Creating directories ...</p> <p>+ mkdir -p /var/opt/agari/etc /var/opt/agari/run /var/- opt/agari/spool /var/opt/agari/shared /var/opt/agari/log</p> <p>+ mkdir -p /opt/agari/bin /opt/agari/lib</p> <p>+ ln -Tsf /var/opt/agari/etc/ /opt/agari/etc</p> <p>+ ln -Tsf /var/opt/agari/etc/ /etc/agari</p> <p>+ ln -Tsf /var/opt/agari/log/ /var/log/agari</p>
	<p>Running Install/Upgrade steps...</p> <p>Moving new files to /opt/agari</p> <p>Downloading docker image from S3...</p> <p>Deleting old docker containers...</p> <p>Deleting old docker images...</p> <p>Loading new docker image...</p> <p>Updated version to 17.09.27035106</p> <p>Running post-installation</p> <p>Running post-installation</p> <p>Running post-install steps...</p>



	<p>Removing temporary install files in /var/opt/agari/tmp/agari.df8jXF</p> <p>Installation Complete</p>
--	---

At this point, the Sensor has been successfully installed.

If you have access to Advanced Phishing Protection, you should be able to navigate to the Manage > Sensors pages and see that the Sensor has connected.



Sensor status

The Sensor should phone home after about 2 minutes.

## Install a Sensor Via OVA

If an organization is hosting a Sensor on its own hardware, a virtual machine package (OVA file) that contains a Sensor configured for that organization can be used as a streamlined alternative to the manual command-line installation and configuration. This involves:

- Downloading the virtual machine package from that organization
- Changing the virtual machine password
- Initializing the Sensor
- Configuring the Sensor

The Sensor runs in the virtual machine that contains a preconfigured operating system and software. The virtual machine itself is configured to meet the requirements as described in "Sensor Prerequisites" on page 21.

## About OVA files

An OVA file is a tar archive file that contains an OVF package. OVF stands for open virtualization format, an open standard for packaging and distributing software to be run in virtual machines. An OVF package contains a description of all the files in the package, one or more disk images of virtual machines, and sometimes certificate and other supporting files. OVF is supported by more than a dozen virtualization providers, including VirtualBox, Red Hat Enterprise Virtualization, and VMware.

The OVA file that you can download is a package that contains a virtual machine disk image configured to install, run, and manage a Sensor.

Download the virtual machine package (OVA file) for an organization

Prerequisites

You will need a blank text file, into which you will paste information generated by this procedure that you will need later. This information includes:

- A URL that is unique for your organization.
- A provisioning key, which is a random sequence of 6 words that you will use to initialize the Sensor after you install it. (This is not a license file. It validates the link between the Sensor and your organization in Advanced Phishing Protection.)

1. Go to Manage > Sensors.
2. Click the Installer tab.
3. Click Download Sensor Installer > OVA Image.
4. Copy both the URL to the download and the provisioning key and **save them to a text file**.

The URL is the location from which you will download the OVA file, and the provisioning key is a random sequence of 6 words that you will need later to complete the Sensor install. The download link expires at the date and time stated in the download dialog box. The provisioning key expires 7 days after it was generated.

5. If your browser changed the file extension to .ovf, change the file extension to .ova. (You must have your operating system configured to view file extensions.)
6. Click OK.
7. In a new browser window/tab, paste the URL in the address bar and go to the address. The OVA file will be downloaded automatically to your computer.

The OVA file, about 1.2 GB, contains the most current version of all Sensor software.

If you download the OVA file again, a new provisioning key will be generated and the previous key will be invalidated. Note that this will not disable currently provisioned Sensors.

## Notes before you begin

If you're using a standalone box for the sensor, the virtualization software (VirtualBox, VMware, etc.) must be installed on the computer you intend to run the Sensor on, and the OVA file that you downloaded must be copied to that machine. If you're using a hypervisor (only VMWare ESXi is supported), the OVA file that you downloaded is then uploaded to a new virtual machine instance on the hypervisor.

The first boot of an OVA (the first step of the next task) is slow while it finalizes the software pre-load of the Sensor application. If your boot seems to hang at Loading application bundle, please allow at least 3 minutes to complete.

Change the admin password

1. Start the virtual machine and import the OVA file. This creates a virtual machine instance in the virtualization software.
2. From the Sensor management menu, enter 4 (Change Password).
3. When asked if you want to change the password, enter y.
4. Enter a new password, and then press Enter. The password must meet the following requirements

- Minimum length: 6 characters
  - Must not be similar to username
  - Must not be similar to hostname
  - Must not be similar to old password
  - Requires at least 1 upper case, 1 lower case, 1 digit, and 1 special character
5. Enter the password again, and then press Enter.

#### Configure the virtual machine

1. In the network(ing) section of the virtual machine settings, ensure it can connect to your desired DNS and NTP servers, and must have HTTP/HTTPS access to AWS. (In some virtualization software, the firewall rules to allow these connections are already enabled.)
2. Open port 22. The sensor is made available on port 22. (In some virtualization software, port 22 is opened by default.)
3. Ensure the rest of the virtual machine's configuration meets the minimum requirements described in "Sensor Prerequisites" on page 21. (The virtual machine should come pre-configured to meet these requirements; this is just a validation step.)
4. Save the virtual machine settings.

#### Initialize the Sensor

Initializing the Sensor involves running the first-time sensor setup, which you do by a remote command-line login, not the Sensor management menu in the virtual machine.

#### Prerequisites

- The 6-word provisioning key you generated and saved when you downloaded the OVA file
  - If you are using a proxy for HTTP traffic, the hostname, port, username, and password for the proxy
  - If you plan to use SMTP over TLS delivery to the sensor, a private key (.key file), a signed TLS certificate (.pem file), and a certificate chain (.pem file)
1. Open a command prompt.
  2. If you use SMTP over TLS, use scp to upload your private key and certificate files to /data/tls-certs/  
For example, enter the command  
scp private\_key.pem admin@sensor:/data/tls-certs/
  3. SSH into the virtual machine as admin and enter the admin password.
  4. Enter the command first-time-setup and press Enter.
  5. Paste the 6-word provisioning key at the prompt and press Enter.

The Sensor initialization will ask several questions to configure itself correctly for your organization:

Question	Options
Do you want to verify the AWS SSL server certificates used for communications from this sensor to AWS?	Amazon Web Services (AWS) hosts the Advanced Phishing Protection application, and the SSL server certificates authenticate the connection from the Sensor to Advanced Phishing Protection.

Question	Options
	<ul style="list-style-type: none"> <li>• yes (default)</li> <li>• no</li> </ul>
You may optionally specify a Unix group that will be given read access to logs as well as write access to the Sensor's configuration and data.	root is the default group and should be fine for most instances.
Will this Sensor use an HTTPS proxy to send data to the Agari cloud?	<p>If you select yes, you will be prompted to enter the hostname, port, username, and password.</p> <ul style="list-style-type: none"> <li>• yes</li> <li>• no (default)</li> </ul>
Do you want to configure TLS Certificates for incoming SMTP traffic to this Sensor?	<p>This is necessary if you require traffic to be encrypted from the mail server to the Sensor.</p> <ul style="list-style-type: none"> <li>• yes</li> <li>• no (default)</li> </ul>
Require that all SMTP sessions use TLS?	<ul style="list-style-type: none"> <li>• yes</li> <li>• no (default)</li> </ul>
Which port should this Sensor listen on for incoming SMTP connections?	25 is the default, and is the traditional well-known port for SMTP. Depending on your infrastructure, you may need to change this. 587 is often used as an alternative to 25 and is useful for unencrypted or TLS connections, and SSL connections often use 465.
Enable DEBUG-level logging?	<p>DEBUG-level logging sends a lot more data, which can be used if there is an issue with the Sensor. The additional data can slow down data processing, so unless there is a known issue with the Sensor, leave this setting at the default value of no.</p> <ul style="list-style-type: none"> <li>• yes: Generates and sends additional data about the processing of each message.</li> <li>• no (default): Generates and sends only Sensor data.</li> </ul>

Once the initialization is complete, the Sensor is started automatically. After a short wait, you can refresh the Sensors page in the organization and you should see the new Sensor there.

## Default sensor configuration

When a Sensor is initialized, it is configured to the following default settings:

Setting	Value
Status	Started
Autostart	Enabled
DHCP/Static IP address	<p>DHCP</p> <p>While the Sensor can be configured to use DHCP, it requires a static IP address because that IP address is used when configuring other parts of your email infra-</p>

Setting	Value
	structure to communicate with the Sensor. If you do not set a static IP address for the Sensor (see "Set a static IP address" on page 35), you must reserve an IP address lease for the Sensor in your DHCP server.
IP address	Depends on the virtual machine software being used. Most usually have a default value or range of values.
Hostname	sensor
NTP Server	us.pool.ntp.org

## Sensor Configuration and Operation

This section refers only to sensors installed via OVA.

The sensor in the OVA is preconfigured with basic settings that allow it to boot and become available on the network without additional configuration. This includes being assigned an IP address upon startup via DHCP. Sensor configuration is performed with a character-based menu. You can:

- Start, auto-start, reboot, and stop the sensor
- Set a static IP address or enable DHCP
- Set a proxy

Sensor configuration is performed from the sensor management menu on the virtual machine:

```

Networking:
-----
IP Address: 10.0.2.15           Netmask: 255.255.255.0
Gateway: 10.0.2.2             DNS: 10.128.128.128 10.128.128.128
Hostname: sensor              Interface: eth0
NTP Server: us.pool.ntp.org

OS Version: 18.08.04232730   Disk Space: 3.0G of 235G used (2%)
                               Memory: 338M of 3952M used (9%)
                               CPU Load: 0.23, 0.16, 0.14 (4 cores)

Sensor Status: started       Sensor Autostart: enabled

Settings menu:
-----
[1] Static IP Address
*[2] DHCP
[3] Proxy Settings
[4] Change password
[5] Sensor Management
[6] Reboot
[7] Power Off

```

All sensor management assumes that you're starting from here.

Start the Sensor

You can start a Sensor only when it is stopped.

1. Press 5 (Sensor Management).
2. Press 1 (Start Sensor).
3. Press y.

4. Press 3 (Main Menu). (The Sensor management app will return to the main menu automatically after several seconds if you do nothing and will not save your action.)

You can also start the Sensor from the command line when you ssh into the virtual machine. See the Admin account commands section for details.

#### Stop the Sensor

You can stop a Sensor only while it is running.

1. Press 5 (Sensor Management).
2. Press 1 (Stop Sensor).
3. Press y.
4. Press 3 (Main Menu). (The Sensor management app will return to the main menu automatically after several seconds if you do nothing and will not save your action.)

You can also stop the Sensor from the command line when you ssh into the virtual machine. See the Admin account commands section for details.

#### Reboot the virtual machine

1. Press 6 (Reboot).
2. Press y.

#### Boot into safe mode

When booting the virtual machine, for troubleshooting purposes, you can boot directly into safe mode or have a boot menu displayed from which you can choose from normal or safe mode.

1. On boot, before the boot screen appears:
  - Hold down the S key to boot into safe mode. (Safe mode does not restore custom settings on boot.)
  - Hold down any key other than D or S to display a boot menu.

#### Power down the virtual machine

1. Press 7 (Power Off).
2. Press y.

The Sensor is stopped and the virtual machine closes down.

#### Enable Sensor auto-start

Enabling Sensor auto-start means that the Sensor starts up automatically when the virtual machine starts, and enabled is the default setting for a Sensor when it is initialized. You can enable Sensor auto-start only when it is disabled.

1. Press 5 (Sensor Management).
2. Press 2 (Enable Autostart on Reboot).
3. Press y.
4. Press 3 (Main Menu). (The Sensor management app will return to the main menu automatically after several seconds if you do nothing and will not save your action.)

You can also enable auto-start of the Sensor from the command line when you ssh into the virtual machine. See the Admin account commands section for details.

#### Disable Sensor auto-start

Disabling Sensor auto-start means that the Sensor does not start up automatically when the virtual machine starts. You can disable Sensor auto-start only when it is enabled.

1. Press 5 (Sensor Management).
2. Press 2 (Disable Autostart on Reboot).
3. Press y.
4. Press 3 (Main Menu). (The Sensor management app will return to the main menu automatically after several seconds if you do nothing and will not save your action.)

You can also disable auto-start of the Sensor from the command line when you ssh into the virtual machine. See the Admin account commands section for details.

#### Enable DHCP

You should enable DHCP only if you have configured a DNCP reservation to permanently lease a static IP address for the Sensor in your DHCP server.

Enabling DHCP means that the IP address and other network configuration parameters are set dynamically. When you enable DHCP, you will set the hostname and NTP server.

1. Press 2 (DHCP).
2. Enter a value for hostname and press Enter (just press Enter to keep the current value).
3. Enter a value for NTP server and press Enter (just press Enter to keep the current value).

Your screen should look something like this:

```

Networking:
-----
IP Address: 10.0.2.15           Netmask: 255.255.255.0
Gateway: 10.0.2.2             DNS: 10.128.128.128 10.128.128.128
Hostname: sensor              Interface: eth0
NTP Server: us.pool.ntp.org

OS Version: 18.08.04232730   Disk Space: 3.0G of 235G used (2%)
                               Memory: 338M of 3952M used (9%)
                               CPU Load: 0.10, 0.14, 0.13 (4 cores)

Sensor Status: started       Sensor Autostart: enabled

Enter DHCP network settings:
-----
Hostname (sensor):
NTP Server (us.pool.ntp.org):

Do you want to SAVE and APPLY these settings? (y/N) [default: N] █

```

4. Press y.

#### Set a static IP address

Setting a static IP address means that you also define the other network parameters necessary for the Sensor to connect. Typically, you will want to set a static IP address and define the network parameters to that they work within your own network infrastructure.

If you installed the Sensor in an environment without DHCP, no default values were assigned. In that case, there are no “current values” and you will have to enter specific and valid values for each parameter.

1. Press 1 (Static IP Address)
2. Enter a value for hostname and press Enter (just press Enter to keep the current value).
3. Enter a value for NTP server and press Enter (just press Enter to keep the current value).
4. Enter a valid IP address and press Enter (just press Enter to keep the current value).
5. Enter a valid netmask value and press Enter (just press Enter to keep the current value).
6. Enter a valid gateway value and press Enter (just press Enter to keep the current value).
7. Enter a valid DNS value (DNS 1 will typically be your internal DNS server, if any) and press Enter (just press Enter to keep the current value).
8. Enter a second valid DNS value (DNS 2 will often be an external, fallback DNS server to be used when DNS 1 is unavailable) and press Enter (just press Enter to keep the current value).

Your screen should look something like this:

```

Networking:
-----
IP Address: 10.0.2.15           Netmask: 255.255.255.0
Gateway: 10.0.2.2             DNS: 10.128.128.128 10.128.128.128
Hostname: sensor              Interface: eth0
NTP Server: us.pool.ntp.org

OS Version: 18.08.04232730   Disk Space: 3.0G of 235G used (2%)
                               Memory: 338M of 3952M used (9%)
                               CPU Load: 0.18, 0.14, 0.13 (4 cores)

Sensor Status: started       Sensor Autostart: enabled

Enter STATIC network settings:
-----
Hostname (sensor): sensor
NTP Server (us.pool.ntp.org): us.pool.ntp.org
IP Address (10.0.2.15): 10.0.2.15
Netmask (255.255.255.0):
Gateway (10.0.2.2):
DNS 1 (10.128.128.128):
DNS 2 (10.128.128.128):

Do you want to SAVE and APPLY these settings? (y/N) [default: N] █

```

9. Press y.

Set a proxy

If your organization uses a proxy server to connect to the internet, you can configure the Sensor to use that proxy.

1. Press 3 (Proxy Settings).
2. Press y if the proxy server uses NTLM authentication or n (default) if it does not.
3. Enter the connection string for your proxy server and press Enter. The connection string includes protocol, server, port, and optionally (if the server does not require authentication) username and password. The protocol can be either http or https (recommended). For example:



- https://username:password@server:port
- http://server:port

Your screen should look something like this:

```

Enter proxy settings:
-----
Examples:
 1) http://yourproxy:3128
 2) https://username:password@yourproxy:3128

Proxy address (): http://user:pass@proxyserver:port
Do you want to SAVE and APPLY these settings? (y/N) [default: N]
Saving Proxy settings
Do you want to reboot the sensor immediately? (Y/n) [default: Y]

```

4. Press y to save your settings.
5. Press y to reboot the virtual machine.

Disable a proxy

This option is available only when a proxy has been set.

1. Press 3 (Proxy Settings).
2. When asked if you want to disable the proxy, press y.

## Admin account commands

If you ssh into the virtual machine instead of using the Sensor management menu, you can use the following commands for Sensor management:

- first-time-setup - run Sensor setup
- sensor-start - start the Sensor, once set up
- sensor-stop - stop the Sensor, once set up and started
- sensor-service-enable - enable auto-start of Sensor on boot
- sensor-service-disable - disable auto-start of Sensor on boot

Enable a second network interface

1. Connect to the virtual machine as admin.
2. In the home directory, edit the eth1.conf file as follows:
  - DHCP: Uncomment interface in ipv4 or ipv6 as needed
  - Static IP: Uncomment interface, ip, and subnet as needed
3. Reboot the virtual machine.

## Test a Sensor

After the first Sensor has been installed and can connect to Cisco, you can send a test email directly to the Sensor.

Because the Sensor is listening for SMTP conversations on the port you specified in the installation script, it is possible to inject a test message directly to the Sensor. If you can telnet to the SMTP port you configured in the installation script and you are comfortable issue SMTP commands directly, you can create a test message:

```
$ telnet sensor_name:sensor_port
```

```
Trying IP_address...
```

```
Connected to sensor_name
```

```
Escape character is '^'].
```

```
220 collector-milter ESMTP Postfix
```

```
HELO example.com
```

```
250 collector-milter
```

```
MAIL FROM: <test@example.com>
```

```
250 2.1.0 Ok
```

```
RCPT TO: user@yourcompany.com
```

```
DATA
```

```
354 End data with <CR><LF>.<CR><LF>
```

```
Received: from 1.2.3.4 by test.example.com
```

```
Received: from 192.168.3.3. by internal
```

```
From: " John Smith" <jsmith@example.com>
```

```
To: " Jane Doe" <jdoe@example.net>
```

```
Subject: test message sent from manual telnet session
```

```
Date: Wed, 11 May 2011 16:19:57 -0400
```

```
Message-Id: <testing-testing>
```

```
Hello World,
```

```
This is a test message sent from a manual telnet session.
```

```
Yours truly,
```

```
SMTP administrator
```

.

```
250 2.0.0 Ok: queued as message_ID
```

```
quit
```

Be sure that the message DATA contains a Received: header. Entering a "." character on its own line will end the data command. The "250 2.0.0. Ok: queued as..." command means that your test message was accepted successfully, and the Sensor is ready to accept messages routed from your dual delivery configuration.

## Troubleshooting Test Email

If you get an error message similar to this after entering the MAIL FROM: line:

```
>451 4.7.1 Service unavailable - try again later
```

...it is likely the Sensor is not up and running yet. Try:

- Look at the `/var/log/agari/container.log` on the host to see if you can find a line similar to:

```
Feb 01 2017 05:07:59 INFO collector-milter is ready.
```

If not, the milter process has not started up yet. Wait a few more minutes and try again.

- Has it been more than five minutes since you've started the Sensor?

If not, wait the full five minutes and then restart the container if the milter has still not started:

```
$ /opt/agari/bin/agari-ep restart
```

- If after restarting the container there is still an issue, consider restarting the entire Sensor:

```
$ sudo service agari-collector restart
```

## View Sensor Status

View the status of your Sensors and manage them via the [Manage > Sensors](#) page.

## Sensors

Manage the sensors in your infrastructure.

2

✓
86fd5c02-bac1-11e8-8bd4-0242ac110002

✓
872fc0dc-bac1-11e8-bd1c-0242ac110002

1
Installation

Status

3

Status: ✓ Receiving Messages and sending data to Cisco

✓ Enforcement enabled

4

Version: 18.09.04144617

5

Hostname (IP): ██████████

Ubuntu 16.04.5 LTS

Docker version 18.06.1-ce, build e68fc7a

6

Last connected at: 13-Nov-2018 15:09:23 PST ⊙

Started at: 18-Sep-2018 10:00:56 PDT ⊙

Messages received in last hour: 2,529

Messages enforced / attempted in the last hour: 0 / 0

Last hour | 12 hours | 24 hours

Messages processed 1-hour total / 24-hour average

2529 / 3452

▶ Additional Performance Measures

Configuration

Name:

You can rename your sensor at any time without affecting message processing.

Receiving mode: Do Not Upload Data  Upload Data

The "Do Not Upload Data" receiving mode prevents the sensor from uploading files to Cisco. Use this mode when you want to verify messages are being sent from your gateway to the sensor without uploading files to Cisco for analysis.

Attachment Scanning: Do Not Scan Attachments  Scan Attachments

Filenames, file extensions, file types, and hashes of all attachments are analyzed.

URI Scanning: Do Not Scan URIs  Scan URIs

URIs within message bodies and attachments are analyzed. URIs from URL shortening services are resolved.

### The Sensors page

1	You can download a Sensor installation script or a virtual machine package keyed specifically to your organization from the Sensors page. Use this to install additional Sensors to handle increased traffic. See "Install a Sensor Via Script" on page 24 and "Install a Sensor Via OVA" on page 29 for more information.
2	If you have multiple Sensors, select a Sensor from the list of tabs. You can view the current status of the Sensor and make configuration changes from this page. The overall status of a Sensor is indicated by the icon (green/yellow/red) on the tab.
3	If you have enforcement enabled, you can see separate status icons for Send/Receive and Enforcement inside the tab. The Enforcement icon is green when more than 80% of messages that should be enforced, are enforced. It's yellow when below that threshold. See the Why are some messages not moved? link on the Policy Report page for any policy with the Enforcement action (click the Number of Matching Messages bar to the right of the policy name on the Manage > Reports page).
4	Update the Sensor. Select from the list of available versions and click Update.
5	Hostname and IP address of the virtual machine on which the Sensor is deployed.
6	Last Connected is the time the Sensor last checked in with Cisco. This should be within the last two minutes (if the Sensor is active).

For Office 365 customers only, there may be a "Download Credentials File" button, for credentials used by the Sensor to perform enforcement activities.

Click Save Configuration to save any changes you have made for the Sensor. The changes are propagated to the Sensor and can take up to 5 minutes to take effect.


## Download Sensor Diagnostic Information

This functionality requires that a user account has the Organization Administrator role. See "User Roles" on page 173 for more information about user roles.

Sensors and their performance are constantly monitored. Information about each Sensor and its performance is compiled into a set of diagnostic files that is updated and stored on Cisco's secure servers every 24 hours. An on-demand set of files can be requested from Cisco's technical support.

That on-demand set of diagnostic files can also be downloaded directly from the Sensors page in Advanced Phishing Protection.

When you request or download an on-demand set of Sensor diagnostic files, the 24-hour clock for when the next set of diagnostic files will be updated and stored on Cisco's secure servers is reset.

1. Go to Manage > Sensors.
2. Click the tab of the Sensor for which you want to download a set of diagnostic files.
3. Click Get link to download diagnostic information.
4. Copy the link and paste it into a browser's address bar, then go to that address. (You can click the  icon to copy the URL to your clipboard.)

The file will be downloaded automatically to the default locations for your browser's downloads. The file has a name of diagnostics-YYYYMMDD-HHMMSS.tar.gz. This file type is commonly known as a tarball, and is a doubly compressed file. When you uncompress it, you will get a set of folders that will typically include /shared, /container, /host, and /log. (The actual contents of the file set may change over time because the amount of diagnostic information generated and saved over time may change.) If you are performing diagnostics, you will likely want to look at the files in the /log folder, which contains several log files with records of Sensor actions.



## CHAPTER 4

# Configuring Delivery to the Sensor

Once a sensor is installed, you configure your email gateway(s) to direct a stream of messages to the sensor.

The steps to configure delivery differ depending on your type of email gateway. See the delivery configuration guide for your email gateway.

Delivery should be configured to take place after initial anti-spam, anti-virus, anti-malware, or any other filtering or sandboxing has occurred. Advanced Phishing Protection is not a first line of defense anti-spam, anti-malware replacement. Its purpose is to look for inauthentic messages that have cleared this filtering.

## Configuring Dual Delivery

Once a sensor has been installed, you should now configure your email gateway(s) to direct a stream of messages to it (dual delivery).

The steps to configure dual delivery differ depending on your type of email gateway. See the dual delivery configuration guide for your email gateway.

Regardless of the gateway type:

- Dual delivery should be configured to be from the "last hop" into your enterprise. Some enterprises have more than one gateway "tier" or layer of MTA (mail transfer agents) or SEG (secure email gateways); be sure that the dual delivery is configured to be from the final routing point, typically where you would send messages to your internal message store (like Microsoft Exchange).
- Dual delivery should be configured to take place after all anti-spam, anti-virus, anti-malware, or any other filtering or sandboxing has occurred. Cisco Advanced Phishing Protection is not a first line of defense anti-spam, anti-malware replacement. Its purpose is to look for inauthentic messages that have cleared this filtering.

## Interrupting Dual Delivery

There are two points at which messages from the sensor to Cisco can be interrupted.

- The sensor itself contains a "Receiving Mode" setting, which, by default is set to "Upload Data."  
If you need to test delivery to the sensor without uploading the data to Cisco for processing, you can set the Receiving Mode to "Do Not Upload Data."

- Your organization has an “Ingest Mode” toggle which must be configured by your Cisco sales engineer before messages will appear in Advanced Phishing Protection.

The “Ingest Mode” toggle is a safeguard Cisco uses to protect against sudden spikes in traffic from new organizations sending data into the system.

## Specific Dual Delivery Instructions

This guide has information about how to configure dual-delivery for the following environments:

- "Configure Dual Delivery: Cisco ESA" on page 60

## Configure Dual Delivery: G Suite

This section describes how to configure dual delivery for directly from within the Google Apps Gmail administrative user interface. To access the administrative interface, log into the Google Apps admin control panel at <https://admin.google.com/AdminHome> with appropriate administrator credentials.

It is recommended you use the Google Chrome browser to configure Google Apps. Cisco has encountered UI bugs that prevent other browsers (specifically Safari) from completing the dual delivery configuration.

The general procedure is as follows:

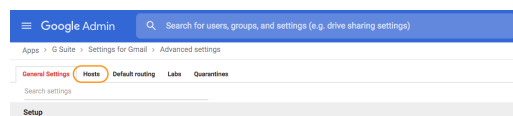
Step 1: Create a new route: a host or host combination as an additional “route” for the Cisco Sensors to which you want to send copies of email.

Step 2: Add a “Default routing” rule to copy the messages to the Sensors via the new route.

Step 3: Whitelist Cisco’s alerts server to ensure that you and your users receive alerts.

Step 1: Create a New Route

1. In the Google Apps admin control panel, go to Apps > G Suite > Gmail > Advanced settings.
2. Click the Hosts tab.



3. Click ADD ROUTE.
4. Enter the details for the mail route:
  - Enter a useful, recognizable name, for example, “Cisco Sensor.”
  - Enter one or more values for email servers, which are hostnames (recommended) or IP addresses and port numbers that correspond to the network location of the Sensors.
    - If Cisco is hosting your Sensors, select Single host and enter the hostname (your sales or support representative will provide you with the information to enter here, which will be in the form of " *symbolicname*.hosted.appc.cisco.com" where *symbolicname* is the symbolic name used for your organization) and port number (25)

for your Sensors. (Technically, the hostname is for a load balancer "in front" of all of the Sensors you use.)

- If you are hosting your Sensors, then select Single host if you are using one Sensor and Multiple hosts if you are using more than one Sensor. For the latter, click Add and enter the IP address, port number, and load percentage for each Sensor you use. You can define hosts as primary and secondary (the latter for fallback purposes), but the total percentage for each category must total 100%. For example, you could have 3 Sensors you define as primary hosts with load percentages of 34, 33, and 33, and 2 Sensors you define as secondary hosts with load percentages of 50 each.
- TLS certificates are already configured on your Sensors, so you can enable Require secure transport (TLS) and optionally also Require CA signed certificate (if appropriate; work with your sales or support representative to determine the proper settings).

**Add mail route** ×

Agari Sensor Help

1. Specify email server

Single host

52.26.66.12 : 25 ⓘ

2. Options

Perform MX lookup on host

Require secure transport (TLS)

Require CA signed certificate

CANCEL SAVE

5. Click SAVE.

### Step 2: Add a "Default routing" Rule to Copy Messages to the Sensor

To divert a copy of messages to the Sensor, you will create a routing rule under the Default routing. You will reference the route you created in the section above in this new routing rule setting.

1. In the Google Apps admin control panel, go to Apps > G Suite > Gmail > Advanced settings.
2. Click the Default routing tab.
3. Click ADD SETTING.
4. Enter the details for the route settings:
  1. For Specify envelope recipients to match, select All recipients.
  2. Select the Add more recipients check box.
  3. Click ADD.
  4. Switch from Basic to Advanced view.
  5. Select the Change route check box, and the select the sensor mail route you created in " Step 1: Create a New Route" on the previous page.
  6. In the Spam and delivery options section, select the Do not deliver spam to this recipient and Suppress bounces from this recipient check boxes.



7. In the Headers section, select the Add X-Gm-Original-To header and Add X-Gm-Spam and X-Gm-Phishy headers check boxes.
  8. Click SAVE.
  9. In the Options section, select Perform this action on non-recognized and recognized addresses.
5. Click SAVE.

Mail will begin to be delivered to the sensors.

You may have other “Default routing” options configured. If so, you will need to carefully consider where to place this new setting among other routes that may be configured. Cisco recommends adding this route as the first setting (Order = “1”) to ensure that all deliverable mail is also delivered to the sensors. However, you may need to consider routing policies that may be unique to your organization and its policies.

### Step 3: Whitelist Cisco’s Notifications Server

When Cisco deems an email suspicious, Advanced Phishing Protection can optionally send an email alert to administrators and/or the original recipient of the suspicious message.

Besides identifying the threatening message, the alert email can contain additional information about the type or severity of the threat. In case of operational problems, the Cisco notification server may also send out alerts regarding your sensor and the overall health of the Advanced Phishing Protection service. Given the importance and utility of these alerts, Cisco recommends that you whitelist the Cisco notifications server to ensure that your system does not block or quarantine these messages.

For example, the messages that the Cisco notifications server sends may sometimes contain portions of the content of the original messages. Because the original messages may contain spam, or otherwise be perceived as suspicious by email filtering software, it is possible that the Cisco alerts may themselves accidentally be perceived as threats.

For this reason, it is important to whitelist the Cisco notification server to prevent triggering of false positives in the filtering software. If there are intermediate filtering steps (for example, other intermediate MTAs, or other anti-phishing solutions which filter email) they should also be configured to whitelist the Cisco notifications server. Cisco’s Sales Engineering and Customer Success teams can assist with configuring the whitelist, if necessary.

Gmail provides two basic methods for whitelisting an upstream MTA:

- Email whitelist (preferred)
- Inbound gateway

#### Whitelist an Upstream MTA via Email Whitelist

In the “Email whitelist” method, there is a small risk that a specified IP address may still be blocked or delayed based on the spam and reputation scanning that Gmail uses. The Cisco alerts server has a good reputation and sends a relatively small volume of mail, so the risk of alerts being blocked or throttled is very small. If you are concerned about any Cisco alerts being blocked or throttled, you can whitelist the Cisco alerts server using the “Inbound Gateway” below.

1. In the Google Apps admin control panel, go to Apps > G Suite > Gmail > Advanced settings.
2. Click the General Settings tab. Scroll down the list of options to the Spam, phishing, and malware section.

3. In the Email whitelist setting, enter 198.2.132.180 in the Enter the IP addresses for your email whitelist field.
4. Click SAVE.

The IP address of the Cisco alerts server is 198.2.132.180. Cisco also maintains a DNS entry for this address at the domain "outbound.cisco.com." In general, it is recommended to use the explicit IP address for this whitelisting rule.

### Whitelist an Upstream MTA via Inbound gateway

Perform these steps only if you cannot whitelist the Cisco alerts server using the method described above.

The preferred method for whitelisting the Cisco alerts server is the "Email whitelist" method outlined in the section above, but if using it is not be practical for you, you can use the "Inbound Gateway" method. This method ensures that absolutely any message sent from the Cisco alerts server will be delivered; however, the steps to are slightly more complicated.

Even if you have no inbound gateway configured already, you can use this method. If you do already have at least one inbound gateway configured, then consider the fact that using this method will disable spam checking for all of your other inbound gateways. If those gateways do their own spam checking, that may be acceptable, but if they do not, you should consider the "Email whitelist" method.

1. In the Google Apps admin control panel, go to Apps > G Suite > Gmail > Advanced settings.
2. In the Spam, phishing, and malware section, for the Inbound gateway setting, click Configure (if you do not already have an inbound gateway) or Edit (for your existing inbound gateway).
3. Enter a text description of the gateway settings, for example: "Whitelist the Cisco Alerts server."
4. Click "ADD" in the IP addresses/ranges box.
5. Enter the IP address 198.2.132.180.
6. Click SAVE.

Do not select the Automatically detect external IP (recommended) option, which relates to the "last-hop" IP address of messages. Because the Cisco notifications server does not relay external messages, this option is not needed. Do not select the Reject all mail not from gateway IPs option unless you are certain that you have the correct configuration; otherwise, you may interrupt your mail service.

7. Select the Require TLS for connections from the email gateways listed above check box unless you have other gateways that require this option to be off.
8. Select the Message is considered spam if the following header regexp matches check box.

In this section, you will create a regular expression ("regexp") that never matches any message. This may seem counterintuitive, but it ensures that Gmail will not blocking any incoming messages from the IP address 198.2.132.180. (Using the alternative "Email whitelist" method does not guarantee that the IP address will be truly whitelisted, just that the messages passed via that IP won't be screened for spam.)

9. In the Regexp field, enter the following text exactly: x^ (that is, a lower-case x and a caret).

This is an expression intentionally crafted to not match any message. (It means: “match the character x, when it occurs before the beginning of the string”, which is impossible.)

10. Leave the Message is spam if regexp matches check box selected.
11. Select the Disable Gmail spam evaluation on mail from this gateway; only use header value check box.

Again, these options apply to all configured Inbound Gateway IPs, so they may or may not be appropriate for your organization. Consider the implications before using this method.

Once configured, the window will look like the following:

12. Click ADD SETTING.

The Inbound gateway will be listed in your overall settings, looking similar to the following:

<b>Inbound gateway</b>	Whitelist the Agari Alerts server
Locally applied	
	Gateway IP(s): 198.2.132.180
	Require Inbound Gateway IP: No
	Require Secure (TLS) Connections: Yes
	Spam Header Tag: x*
	Disable Gmail Spam Filtering: Yes

Inbound Gateway method summary settings

## Wrapping Up

When the above steps are completed, the Cisco sensors will start receiving copies of email messages sent into your organization. There may be a small delay of a few minutes before Google’s systems com-

mit the changes and they take full effect. You can confirm the traffic flow by logging into Advanced Phishing Protection at <https://appc.cisco.com> and navigating to Manage > Sensors to see the status of your installed sensors.

## Configure Dual Delivery: Office 365

This section describes how to configure dual delivery for Microsoft Office 365 environments using a Journaling rule.

The general procedure is as follows:

Step 1: Create a connector that routes journaled messages to your sensor.

Step 2: Create a journal rule in Office 365 that copies messages to your sensor.

Step 3: Whitelist the IP addresses of the alerts server to ensure that you and your users receive alerts.

Advanced Phishing Protection requires that the X-MS-Exchange-Organization-AuthAs: header with the correct value for message directionality be added to all messages. See the Microsoft Exchange documentation for instructions about how to configure this. The following header and values are required for Advanced Phishing Protection to function correctly:

- Internal messages: X-MS-Exchange-Organization-AuthAs: Internal
- Inbound/outbound messages: X-MS-Exchange-Organization-AuthAs: Anonymous

Inbound and outbound messages that add the Internal value for this header will be treated by Advanced Phishing Protection as internal messages and will be scored differently, which can make Advanced Phishing Protection less effective against external attacks. See <https://docs.microsoft.com/en-us/exchange/mail-flow/connectors/allow-anonymous-relay?view=exchserver-2019> and <https://docs.microsoft.com/en-us/powershell/module/exchange/mail-flow/set-inboundconnector?view=exchange-ps> for additional information.

Step 1: Create a Connector that Routes Journaled Messages to Your Sensor

To route journaled messages to the sensor, you will create a placeholder domain to which messages will be routed.

You may have a more complex configuration in place. The goal is to configure this connector such that message coming from the journaling feature will receive special routing.

1. Log in to your Office 365 dashboard at <https://portal.office.com> with an account that has appropriate administrative permissions to create the rule required.
2. Go to Admin centers > Exchange.
3. Click mail flow.
4. Click the connectors tab.
5. Click + to create a new connector.

6. On the Select your mail flow scenario page:
  - In the From drop-down list, select Office 365.
  - In the To drop-down list, select Partner organization.
7. Click Next.
8. On the New connector page:
  - Enter a connector Name and an optional Description. Make the name something useful and recognizable, such as "Cisco sensor."
  - Leave the Turn it on check box selected. (There is a known bug at Microsoft where the validation process (accessed later in this wizard) fails for connectors when this check box is not selected. Refer to: <https://support.microsoft.com/en-us/help/3179588/the-domain-of-the-recipient-is-not-configured-as-part-of-connector-err>.)
9. Click Next.
10. Select the Only when email messages are sent to these domains radio button.
11. Click + to add a new domain.
12. Enter the domain that will redirect messages to use this connector. Your sales or support representative will provide you with the information to enter here, which will be in the form of "symbolicname.hosted.appc.cisco.com" where symbolicname is the symbolic name used for your organization.
13. Click Next.
14. Select the Route email through these smart hosts radio button.
15. Click + to add a smart host.
16. Enter the fully-qualified domain name of your sensor.
  - For Agari-hosted Sensors, this will be the address from step 12.
  - For Sensors you host, you will get the Sensor domain name from your Sensor virtual machine interface.
17. Click Next.
18. Configure the TLS settings for the connections made to the sensor. It is recommended that you:
  - Select the Always use Transport Layer Security check box.
  - Select the Any digital certificate, including self-signed certificates radio button. (If you have installed verified TLS certificates on your sensor, you may want to select the Issued by a trusted certificate authority (CA) radio button.)
19. Click Next, and then on the conformation screen, click Next again.
20. Confirm that the sensor is reachable.
21. Click +.
22. Enter an email address that uses the same placeholder domain you specified earlier (in the above example, "symbolicname.hosted.appc.cisco.com"). The local part of the address to the left of the "@" sign is irrelevant; you can use any address.
23. Click Validate.
24. After a short delay, you will see a confirmation window.

If validation fails, please contact your sales or support representative to troubleshoot. Validation may fail if you have another transport rule which takes precedence or intercepts the validation message. Validation may also fail if there is latency in the Microsoft administrative portal. (In these cases, wait a few moments and attempt to validate again.)

25. Click Close.

You can click the pencil icon for any failed results to view the log from that test and address any issues in the configuration.

26. If you see "Succeeded" for both tasks, click Save.

You will now see the newly-created Connector in your list of Connectors.

#### Step 2: Create a Journal Rule to Copy Messages to the Sensor

Before creating your first journal rule, you will need to either specify an existing or create a new email account that will be used to receive Non-Delivery Reports (sometimes called "NDRs" or "bounce" messages). You should monitor messages sent to this address periodically to ensure that there are no connectivity issues between Office 365 and the machine hosting the sensor.

#### Create a New Account for Journaling

1. Click Select Address.
2. Click recipients
3. Click the shared tab.
4. Click + to create a new shared mailbox.
5. Enter the mailbox information. Enter a descriptive display name and email address. For example, you can specify "JournalReportNDR" for the display name and "journal@yourdomain.onmicrosoft.com" for the email address. Optionally, you can grant access to a specific user or users to monitor this shared mailbox. You can also optionally choose "More options..." to define an alias for this shared mailbox.
6. Click Save.

#### Create the Journaling Rule

1. Log in to your Office 365 dashboard at <https://portal.office.com> with an account that has appropriate administrative permissions to create the rule required.
2. Go to Admin centers > Exchange.
3. Click compliance management.
4. Click the journal rules tab.
5. If there is an email address as the value of Send undeliverable journal reports to, continue with the next step. If the value is Select Address, click Select Address and add as new address, as described in "Create a New Account for Journaling" above, and then continue.
6. Click +.
7. Enter the journaling rule details:
  - In the Send journal reports to field, enter an address that uses the domain you specified in "Step 1: Create a Connector that Routes Journaled Messages to Your Sensor" on page 48. For example, "journal@symbolicname.hosted.appc.cisco.com."

- In the Name field, enter " CiscoSensor"
  - In the If the message is sent to or received from drop-down list, select:
    - Apply to all messages if you want all messages to be sent for analysis.  
If you select External Messages, the Office 365 journaling functionality may miss external messages spoofed as from internal domains.
    - A specific user or group, and select a group if you would like only messages to a subset of your user base to be evaluated, such as for testing purposes. The group you select here must be created via the " recipients > groups" section of the Exchange admin center. You can specify a Distribution Group, a Security Group, or, if you want to avoid changing the group as new members join or leave your organization, you can use a Dynamic Distribution Group.
8. In the Journal the following messages drop-down list, select All messages.
  9. Click Save.
  10. Click Yes in the confirmation message.

Messages will begin flowing to the sensor immediately.

### Step 3: Whitelist the Alerts Server

When an email is deemed suspicious, Advanced Phishing Protection can optionally send an email alert to administrators and/or the original recipient of the suspicious message.

Besides identifying the threatening message, the alert email can contain additional information about the type or severity of the threat. In case of operational problems, the notification server may also send out alerts regarding your sensor and the overall health of the Advanced Phishing Protection service. Given the importance and utility of these alerts, it is recommended that you whitelist the notifications server to ensure that your system does not block or quarantine these messages.

For example, the messages that the notifications server sends may sometimes contain portions of the content of the original messages. Because the original messages may contain spam, or otherwise be perceived as suspicious by email filtering software, it is possible that the alerts may themselves accidentally be perceived as threats.

So it is important to whitelist the notification server to prevent triggering of false positives in the filtering software. If there are intermediate filtering steps (for example, other intermediate MTAs, or other anti-phishing solutions which filter email) they should also be configured to whitelist the notifications server. The Sales Engineering and Customer Success teams can assist with configuring the whitelist, if necessary.

If you are using Office 365 only, you will add a server to your whitelist. If you are also using Exchange Online Protection, you will also add a mail flow rule to prevent spam filtering of the alerts.

These instructions cover:

(O365 only) Adding a server to your " connection filter" whitelist, and

(O365 and EOP) Adding a " mail flow rule" to prevent spam filtering of the alerts

Add the Alerts Server to Your Whilelist

The goal of this task is to configure the "IP Allow list" of the applicable connection filter; typically this will be the "Default" connection filter.

1. Log in to your Office 365 dashboard at <https://portal.office.com> with an account that has appropriate administrative permissions to create the rule required.
2. Go to Admin centers > Exchange.
3. Click protection.
4. Click the connection filter tab.
5. Select the Default connection filter.
6. Click the pencil icon.
7. Click connection filtering.
8. Click +.
9. Enter the IP address of the alerts server: 198.2.132.180, and make sure it is not a blocked IP address.
10. Click OK.
11. Click Save.

Confirm that the Default connection filter shows "IP Allow list: Configured" on the right side of the screen.

(The IP address of the Cisco alerts server is 198.2.132.180. Cisco also maintains a DNS entry for this address at the domain "outbound.cisco.com." In general, it is recommended to use the explicit IP address for this whitelisting rule.)

#### Add a Mail Flow Rule to Prevent Spam Filtering of Alerts

You should do this if you are using Exchange Online Protection with Office 365.

Repeat this procedure for each sensor.

1. Log in to your Office 365 dashboard at <https://portal.office.com> with an account that has appropriate administrative permissions to create the rule required.
2. Go to Admin centers > Exchange.
3. Click mail flow.
4. Click the rules tab.
5. Click +, then select Bypass spam filtering.
6. Enter the filtering rule details:
  - Enter a descriptive name, such as "Whitelist alerts server" or "Whitelist sensor."
  - In the Apply this rule if drop-down list, select IP address is in any of these ranges or exactly matches.
    1. Enter the IP address of the alerts server (in our example, 198.2.132.180).
    2. Click + to add the IP address.
    3. Click OK.



- Make sure that the Stop processing more rules check box is not selected; you will need the subsequent rules to be processed in order for your mail to be processed correctly.

7. Click Save.

Consider the ordering of any other rules that you have in the list: ideally, the whitelist rules could come first in the list to ensure that no other rules interfere with delivery. The alerts server whitelist rule should come before other routing rules that may impact the delivery of alerts to your organization.

As seen above, the IP address of the alerts server is 198.2.132.180. A DNS entry for the address of the alerts server domain is also maintained, but in general, it is recommended to use the explicit IP address for this whitelisting rule.

## Configure Dual Delivery: Microsoft Exchange

This section describes how to configure dual delivery for Microsoft Exchange environments using a Journaling rule.

The steps for configuring Exchange dual delivery are similar for all versions (2010, 2013, and 2016) of Exchange, but the Exchange administration user interface changed from the 2010 version to the 2016 version.

You will configure a send connector that will be used for journaling. In Microsoft Exchange, a journal recipient can be a mailbox or a contact. When you use a contact, you can define it using a placeholder domain. By doing so, you can use that contact as the destination for the send connector. This allows messages to be sent to dev/null if the Sensor is for some reason not reachable, instead of letting the transport queue back up.

For most environments, you will want Premium Journaling, which requires [Exchange Enterprise licensing from Microsoft](#) and may include server licenses or [client access licenses](#) (CALs). Premium Journaling licensing allows you to use journal rules to define both recipients and scope. Microsoft also offers Standard Journaling, which is all-or-nothing journaling on mailbox databases on all Exchange servers. If you have only a Standard Journaling license and you are already using journaling for another purpose, you may be able to set up separate journaling to the CiscoSensor.

"Configure Dual Delivery: Exchange 2010" on the facing page

"Configure Dual Delivery: Exchange 2013/2016" on page 57

"Test Exchange Dual Delivery" on page 60

Each configuration comprises 3 parts:

- Create a placeholder domain
- Create a contact using that placeholder domain
- Create a send connector

Advanced Phishing Protection requires that the X-MS-Exchange-Organization-AuthAs: header with the correct value for message directionality be added to all messages. See the Microsoft Exchange documentation for instructions about how to configure this. The following header and values are required for Advanced Phishing Protection to function correctly:

- Internal messages: X-MS-Exchange-Organization-AuthAs: Internal
- Inbound/outbound messages: X-MS-Exchange-Organization-AuthAs: Anonymous

Inbound and outbound messages that add the Internal value for this header will be treated by Advanced Phishing Protection as internal messages and will be scored differently, which can make Advanced Phishing Protection less effective against external attacks. See <https://docs.microsoft.com/en-us/exchange/mail-flow/connectors/allow-anonymous-relay?view=exchserver-2019> and <https://docs.microsoft.com/en-us/powershell/module/exchange/mail-flow/set-inboundconnector?view=exchange-ps> for additional information.

## Configure Dual Delivery: Exchange 2010

Create a placeholder domain: Exchange 2010

1. In the Exchange Management Console, go to Organization Configuration > Hub Transport.
2. Click the Remote Domains tab.
3. Click New Remote Domain.
4. Enter cisco.sensor.
5. Click Next.
6. Click Finish.
7. Click Apply.
8. Click OK.

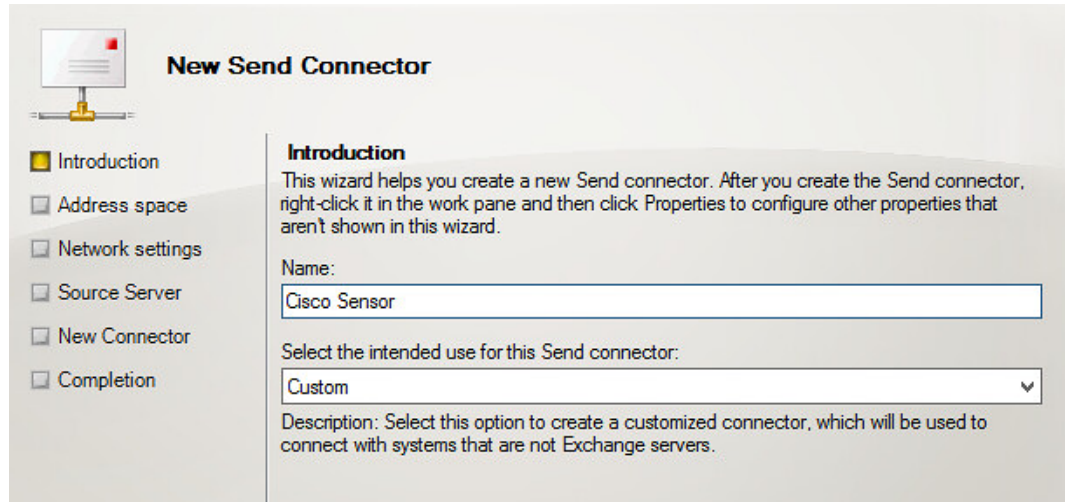
Create a contact using the placeholder domain: Exchange 2010

1. Go to Create Contact.
2. Enter the following values:
  - FirstName: Cisco
  - LastName: Sensor
  - Alias: CiscoSensor
  - External Email Address: journal@cisco.sensor
3. Save the contact.

Create a send connector: Exchange 2010

1. Sign in to Exchange Management Console (2010).
2. Create a new Send Connector.

3. Enter/Select the send connector details:
  - Name: Cisco Sensor
  - Select the intended use for this Send connector: Custom



**New Send Connector**

Introduction  
 Address space  
 Network settings  
 Source Server  
 New Connector  
 Completion

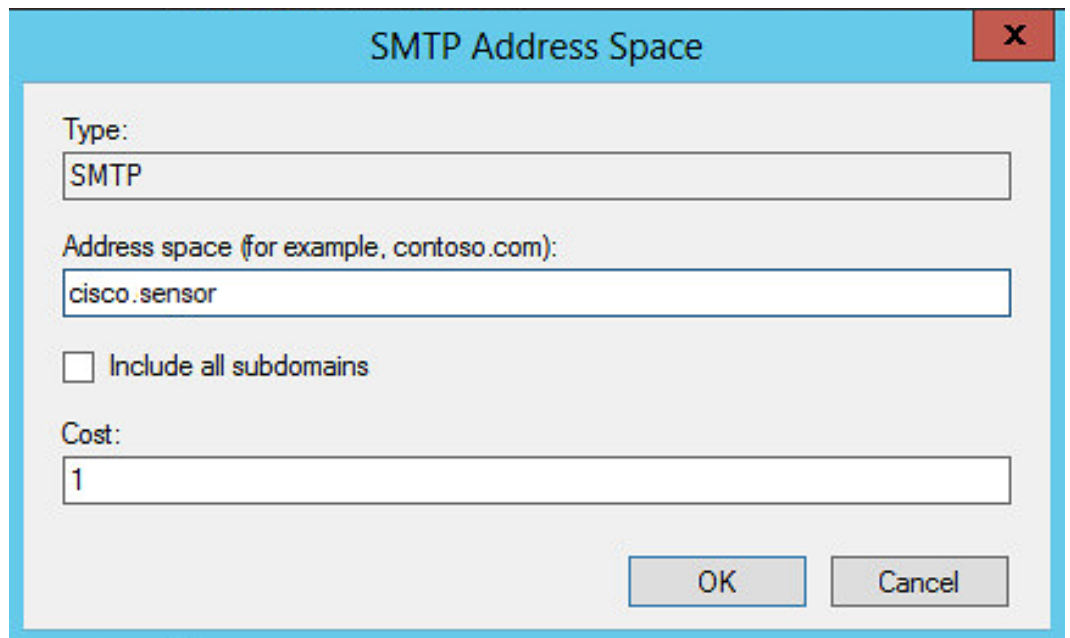
**Introduction**  
This wizard helps you create a new Send connector. After you create the Send connector, right-click it in the work pane and then click Properties to configure other properties that aren't shown in this wizard.

Name:  
Cisco Sensor

Select the intended use for this Send connector:  
Custom

Description: Select this option to create a customized connector, which will be used to connect with systems that are not Exchange servers.

4. Click Add.
5. Enter the information about the SMTP Address Space:
  - Type: SMTP (This is the default and it cannot be changed here.)
  - Address Space: cisco.sensor
  - Cost: 1



**SMTP Address Space**

Type:  
SMTP

Address space (for example, contoso.com):  
cisco.sensor

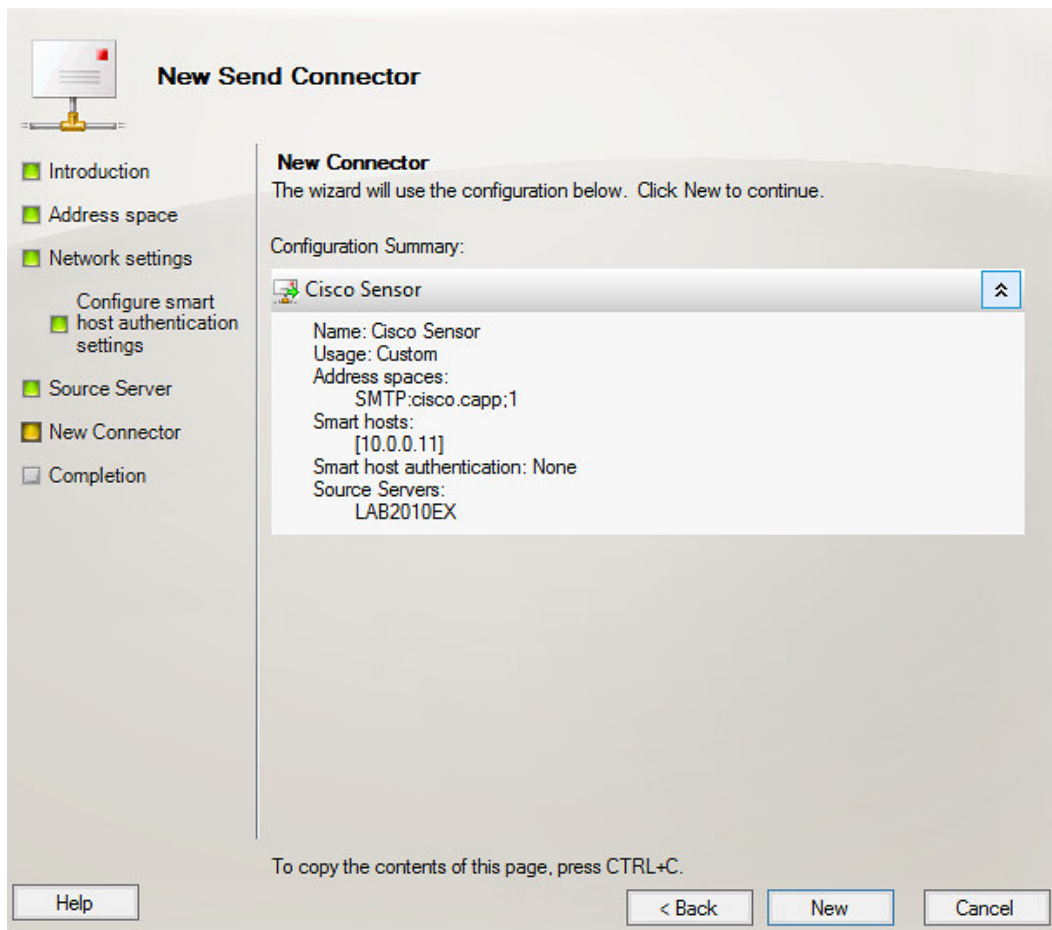
Include all subdomains

Cost:  
1

OK Cancel

6. Click OK.
7. Click Next.
8. For Network settings, select Route mail through the following smart hosts.

9. Click Add.
10. Enter the IP address of the sensor.
11. Click OK.
12. For Configure smart host authentication settings, select None.
13. Click Next.
14. For Source server, make sure you have the correct email gateway server selected.
15. Click Next.
16. Review the settings to make sure they are correct.



17. Click New.
18. Create a new Journal Rule.
19. Enter the journal rule settings:
  - Make sure the domain matches the Send Connector in the previous step.
  - Rule name: Cisco Sensor
  - Send Journal reports to email address: journal@cisco.sensor
  - Scope: Global - all messages

If you select External - messages with an external sender or recipient Messages, the Exchange journaling functionality may miss external messages spoofed as being from internal domains.

- Select the Enable Rule check box.

20. Click New.
21. Review the settings to make sure they are correct.
22. Click Finish.

## Configure Dual Delivery: Exchange 2013/2016

Create a placeholder domain: Exchange 2013/2016

The ability to create placeholder domains was removed from the Exchange Management Console in the 2013/2016 versions, so this must be done at the command line.

1. Open the Exchange Management PowerShell.
2. Enter the following commands:
  - a. Create the placeholder domain:  
New-RemoteDomain -DomainName cisco.sensor -Name "Cisco APP"
  - b. Set up auto-forward:  
Get-RemoteDomain | Where {\$\_.DomainName -eq "cisco.sensor"}  
| Set-RemoteDomain -TNEFEnabled \$false -AutoForwardEnabled \$true

- c. Verify:
- ```
Get-RemoteDomain | Where {$_.DomainName -eq "cisco.sensor"}
|Format-table Name, DomainName, TNEFEnabled, AutoForwardEnabled
```

Create a contact using the placeholder domain: Exchange 2013/2016

1. Go to Create Contact.
2. Enter the following values:
  - FirstName: Cisco
  - LastName: Sensor
  - Alias: CiscoSensor
  - External Email Address: journal@cisco.sensor
3. Save the contact.

Create a send connector: Exchange 2013/2016

1. Sign in to Exchange Admin Center (2013/2016).
2. Create a new Send Connector.
3. Enter/Select the send connector details:
  - Name: Cisco Sensor
  - Type: Custom

### new send connector

[Help](#)

This wizard will create a send connector.

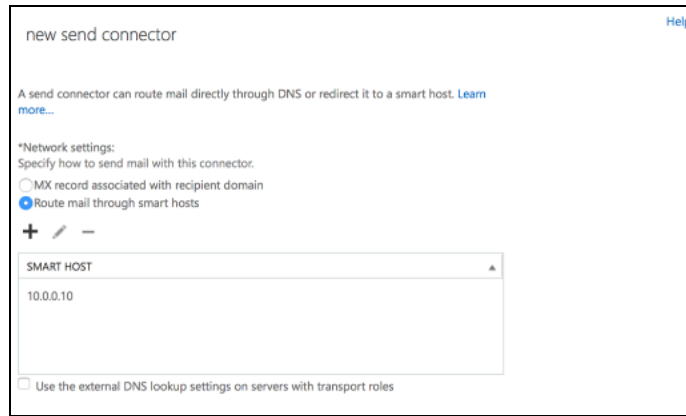
There are four types of send connectors. Each connector has different permissions and network settings. [Learn more...](#)

\*Name:

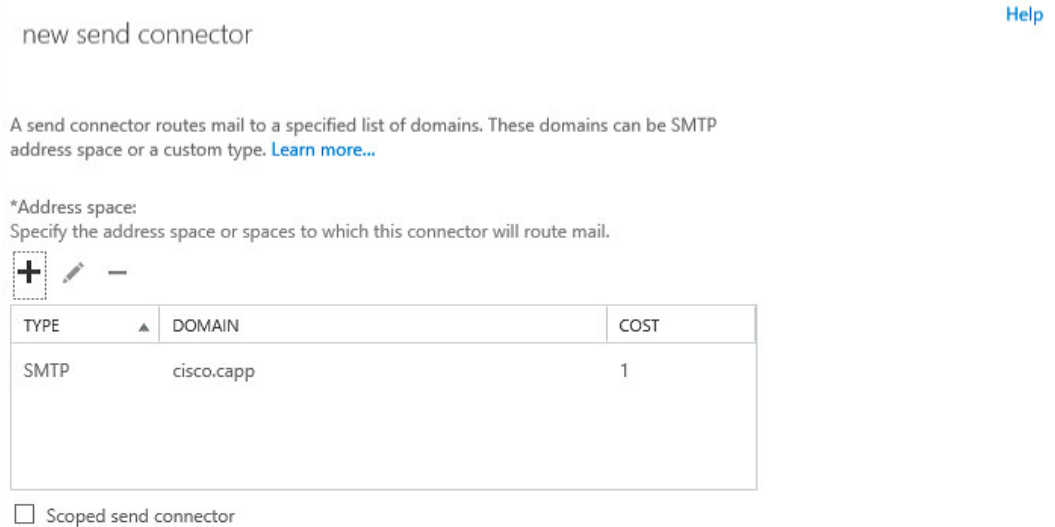
Type:

- Custom (For example, to send to other non-Exchange servers)
- Internal (For example, to send intranet mail)
- Internet (For example, to send internet mail)
- Partner (For example, route mail to trusted 3rd party servers)

4. Click Next.
5. For Network settings, select Route mail through the following smart hosts, and add the IP address of the sensor.



6. Click Next.
7. For Configure smart host authentication settings, select None.
8. Click Next.
9. For Address space, enter cisco.sensor and SMTP.



10. Click Next.
11. For Source server, make sure you have the correct email gateway server selected.
12. Click OK.
13. Create a new Journal Rule.
14. Enter the journal rule settings:
  - Send Journal reports to: journal@cisco.capp
  - Name: CiscoJournaling
  - If the message is sent to or received from: Apply to all messages

- Journal the following: All messages  
If you select External Messages, the Exchange journaling functionality may miss external messages spoofed as being from internal domains.

new journal rule

Apply this rule...

Name:

\*If the message is sent to or received from...

\*Journal the following messages...

\*Send journal reports to:

 To use premium journaling, you must have an Enterprise Client Access License (CAL). [Learn more](#)

15. Click Save.

## Test Exchange Dual Delivery

1. Send a test message from outside your organization/network to one of your users.
2. Review in Advanced Phishing Protection that the message was ingested.

## Configure Dual Delivery: Cisco ESA

This section describes how to configure dual delivery from Cisco Email Security Appliance (formerly known as IronPort) environments to the Cisco Advanced Phishing Protection Sensor.

The general procedure is as follows:

Step 1: Enable SPF/DKIM/DMARC checking in the Cisco ESA.

Step 2: Create a content filter that uses the Bcc: action to copy messages to the sensor.

Step 3: Configure the appropriate mail policies to reference that filter so that only delivered mail (and not spam or PVO (policy, virus, and outbreak) quarantined mail) is copied to the sensor.

Step 4: Configure bounce handling to properly manage unexpected delivery failures.

Step 5: Confirm that any desired system alerts are in place to inform administrators of any problems.

Step 6: Consider other whitelisted email streams.

Step 7: Whitelist the alerts server to ensure that you and your users receive alerts.



## Important Consideration Regarding the "Authentication-Results" Header

The Sensor depends on the presence of an accurate, uncorrupted Authentication-Results header to help evaluate a sending identity. Typically, the "perimeter" MTA for your enterprise (meaning, the first point of entry into your enterprise from the sending MTAs on the internet) will evaluate the incoming messages and add an Authentication-Results header, and any downstream MTAs in your institution will be carefully configured to preserve the integrity of this header (that is, they must not overwrite it with their own header unless they are able to do so with accurate information, and they must not strip the header from the message).

However, mail routing environments can be complex, and it's not always practical to ensure integrity of the header for every downstream MTA. To simplify the situation, sensors will first look for a duplicate of the header called X-Agari-Authentication-Results. If they find none, they will fall back to the Authentication-Results header.

This allows you to configure your perimeter MTA to create (or duplicate) the Authentication-Results header under an alternate name: it will stand a greater chance of making it through your various downstream MTAs without being corrupted. Instructions for how to do this for various MTA products are included in this guide.

### Step 1: Enable SPF/DKIM/DMARC checking in the Cisco ESA

1. Go to Mail Policies > Mail Flow Policies.
2. Click Default Policy Parameters.
3. Ensure that DKIM Verification, SPF/SIDF Verification, and DMARC Verification are all set to On. Leave the related settings as shown below.

| Security Features               |                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Spam Detection:                 | <input checked="" type="radio"/> On <input type="radio"/> Off                                                                                                                                    |
| Virus Protection:               | <input checked="" type="radio"/> On <input type="radio"/> Off                                                                                                                                    |
| Encryption and Authentication:  | TLS: <input type="radio"/> Off <input checked="" type="radio"/> Preferred <input type="radio"/> Required<br><input type="checkbox"/> Verify Client Certificate                                   |
|                                 | SMTP Authentication: <input checked="" type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required                                                                         |
|                                 | If Both TLS and SMTP Authentication are enabled: <input type="checkbox"/> Require TLS To Offer SMTP Authentication                                                                               |
|                                 | Domain Key/DKIM Signing: <input type="radio"/> On <input checked="" type="radio"/> Off                                                                                                           |
| DKIM Verification:              | <input checked="" type="radio"/> On <input type="radio"/> Off                                                                                                                                    |
|                                 | Use DKIM Verification Profile: <input type="text" value="DEFAULT"/>                                                                                                                              |
| S/MIME Decryption/Verification: | <input type="radio"/> On <input checked="" type="radio"/> Off                                                                                                                                    |
| S/MIME Public Key Harvesting:   | Signature After Processing: <input checked="" type="radio"/> Preserve <input type="radio"/> Remove                                                                                               |
|                                 | S/MIME Public Key Harvesting: <input checked="" type="radio"/> Disable <input type="radio"/> Enable                                                                                              |
|                                 | Harvest Certificates on Verification Failure: <input checked="" type="radio"/> Disable <input type="radio"/> Enable                                                                              |
|                                 | Store Updated Certificate: <input type="radio"/> Disable <input checked="" type="radio"/> Enable                                                                                                 |
| SPF/SIDF Verification:          | <input checked="" type="radio"/> On <input type="radio"/> Off                                                                                                                                    |
|                                 | Conformance Level: <input type="text" value="SIDF Compatible"/>                                                                                                                                  |
|                                 | Downgrade PRA verification result if 'Resent-Sender:' or 'Resent-From:' were used: <input type="radio"/> No <input checked="" type="radio"/> Yes                                                 |
|                                 | HELO Test: <input checked="" type="radio"/> Off <input type="radio"/> On                                                                                                                         |
| DMARC Verification:             | <input checked="" type="radio"/> On <input type="radio"/> Off                                                                                                                                    |
|                                 | Use DMARC Verification Profile: <input type="text" value="DEFAULT"/>                                                                                                                             |
|                                 | DMARC Feedback Reports: <input type="text" value="Send aggregate feedback reports"/>                                                                                                             |
|                                 | <small>* DMARC reporting message must be DMARC compliant.<br/>* Recommended: Enable TLS encryption for domains that will receive reports. Go to Mail Policies &gt; Destination Controls.</small> |
| Bounce Verification:            | Consider Untagged Bounces to be Valid: <input type="radio"/> Yes <input checked="" type="radio"/> No                                                                                             |
|                                 | <small>(Applies only if bounce verification address tagging is in use. See Mail Policies &gt; Bounce Verification.)</small>                                                                      |

The DKIM Verification, SPF/SIDF Verification, and DMARC Verification settings all configured correctly in the CISCO ESA.

### Step 2: Create a Bcc: Filter to Divert Messages

1. Log into the Cisco ESA (Email Security Appliance) as an Administrator user.
2. Go to Mail Policies -> Incoming Content Filters.
 

If your Cisco ESA environment is configured for cluster management: the following steps should be completed at either the top Cluster level or at a subgroup level if the action is intended to only affect a certain set of Email Security Appliance (ESA) instances.
3. Click Add Filter and give the filter a recognizable name, such as " Cisco\_sensor."
4. In the Description field, enter a description so that future administrators will understand what the filter is for and who to contact. For example: " This is a filter to send a BCC stream of messages to a Sensor, where certain aspects of the message headers and authentication data are saved and communicated. Questions? Contact Joe Administrator at joe-admin@example.com"
5. Order the filter so that it enables the Sensor to receive all messages that are going to be delivered to the end user after all spam and virus scanning has occurred, and after any other message filtering policy that would drop messages. If you have other advanced filtering uses where a filter triggers immediate delivery and circumvents subsequent filters in the "master list" of content filters, you should consider these and place the Sensor filter appropriately for the desired result: collection of all messages delivered to the user.
6. Optionally add a condition to the content filter. Depending on your environment, the filter can be associated with a specific Incoming Mail Policy (see later in these instructions) for certain recipients or domains. If there is filtering logic such that messages found to be anti-spam positive or anti-virus positive are not dropped (and are not delivered on to the user), then you will need to include conditions in the filter so that the Sensor filter will not match. Otherwise, you can skip adding a condition to the content filter and it will evaluate to "True" for any message. Again, the goal of the content filter is to only work on messages that are going to be delivered directly to the end user.
7. Add actions to add headers to the message. You will add an X-Agari-Original-From and an X-Agari-Original-To to messages, and if your Cisco ESA is a perimeter gateway, you will also add an X-Agari-Authentication-Results header. You add one header per action, so repeat the following sub-steps for each action.
  - a. Click Add Action.
  - b. In the Add Action dialog box, select Add/Edit Header.
  - c. Enter a Header Name value per the table below.
  - d. Select Specify Value for New Header and enter a value per the table below.
  - e. Double check the names for typos.
  - f. Click OK.

| Header Name Value              | Specify Value for New Header Value                                                                       |
|--------------------------------|----------------------------------------------------------------------------------------------------------|
| X-Agari-Original-From          | \$EnvelopeFrom                                                                                           |
| X-Agari-Original-To            | \$enveloperecipients                                                                                     |
| X-Agari-Authentication-Results | \$Header['Authentication-Results']<br>Add this header only if your CISCO ESA is a perimeter gateway MTA. |

**Edit Action**

Quarantine  
 Encrypt on Delivery  
 Strip Attachment by Content  
 Strip Attachment by File Info  
 URL Category  
 URL Reputation  
 Add Disclaimer Text  
 Bypass Outbreak Filter Scanning  
 Bypass DKIM Signing  
 Send Copy (Bcc:)  
 Notify  
 Change Recipient to  
 Send to Alternate Destination Host  
 Deliver from IP Interface  
 Strip Header  
**Add/Edit Header**  
 Add Message Tag  
 Add Log Entry  
 S/MIME Sign/Encrypt on Delivery  
 Encrypt and Deliver Now (Final Action)  
 S/MIME Sign/Encrypt (Final Action)  
 Bounce (Final Action)  
 Skip Remaining Content Filters (Final Action)  
 Drop (Final Action)

**Add/Edit Header** Help

Inserts a header and value pair into the message or modifies value of an existing header before delivering.

Header Name:   
*New Header Name or Existing Header*

Specify Value for New Header (optional):

Prepend to the Value of Existing Header:

Append to the Value of Existing Header:

Search & Replace from the Value of Existing Header:  
 Search for:  \*  
 Replace with:   
*Leave blank to remove searched text from value.*

(\*) accepts regular expression

Example Content Filter Action for the X-Agari-Original-To header.

8. Create the primary action for this filter: to BCC the entire message into the sensor.
  - The Email Address for the BCC action should be:
    - [username]@[symbolic\_name].hosted.agari.com (for Cisco-hosted Sensors)
    - [username]@[sensor\_IP\_address] (when Sensors are in your own infrastructure)
  - The Subject of the Bcc: message should be the same as original, so leave the Subject field as "\$Subject"
  - The Return Path entry should initially be set to an appropriate address where bounces are either entirely ignored, or monitored for failure to deliver into the Sensor. Do not leave the Return Path field blank. Doing so could expose the original message sender to bounce-backs in case of problems delivering to the Sensor. Once you are certain that your configured delivery is operating correctly, you can later change the Return Path entry to be "<>", which causes any explicit delivery failures to be immediately deleted from the delivery queue.
  - If the domain specified in the Bcc email address will not result in the message being delivered to the appropriate desired destination, you can use an "Alternate Mail Host"

entry. The result of this setting will be such that the delivery attempt will be made directly to the specified host rather than to whatever is specified by the MX record of the Email Address or the Cisco ESA's "SMTP routes" feature. In other words, you can use this field to directly specify the host or IP address of the Sensor (IP addresses should be enclosed in square brackets, e.g. [123.123.45.67]). Note that the domain used in the Email Address specified above is still relevant to Bounce handling, as described below.

The screenshot shows the 'Edit Action' dialog box with a list of actions on the left and the configuration for 'Send Copy (Bcc:)' on the right. The 'Send Copy (Bcc:)' action is selected and highlighted. The configuration fields are as follows:

- Send Copy (Bcc:)** (Help)
- Copies this message anonymously to specified recipient(s).
- Email Addresses: collector\_user@collector.host
- The following settings are optional.
- Subject: \$Subject
- Return Path: blackhole@tomki.com
- Alternate Mail Host: [123.123.45.67]

Buttons: Cancel, OK

Bcc: action

9. Click OK.

This example shows the above content filter definition (prior to clicking Submit):

### Content filter summary

The above image shows the X-Agari-Authentication-Results header being added: you should only add this header if your Cisco ESA MTA is a perimeter gateway MTA. If your Cisco ESA MTA is downstream from the perimeter gateway(s), then you should not add this header.

10. Click **Submit** to save the new filter.
11. Associate the filter with all appropriate Incoming Mail policies.
  - a. Go to Mail Policies -> Incoming Mail Policies.
  - b. In the Content Filters column for the appropriate row, edit the assigned Content filters to reference (enable) the newly created filter. You may need to Enable Content Filters entirely for that Policy in the process.

The modified Policy row may look like this:

| Order | Policy Name | Anti-Spam                                                                                             | Anti-Virus                                                            | Advanced Malware Protection | Content Filters | Outbreak Filters | Delete |
|-------|-------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|-----------------------------|-----------------|------------------|--------|
| 7     |             | IronPort Anti-Spam<br>Cloudmark Service Pr...<br>Positive: Quarantine<br>Suspected: Quarantine<br>... | Sophos<br>McAfee<br>Encrypted: Deliver<br>Unscannable: Deliver<br>... | (use default)               | Agari_collector | (use default)    |        |

### Policy row containing Content Filter.

Remember that any policy that delivers mail to end users (and doesn't put messages in a quarantine folder or delete the messages) should reference the content filters used to BCC messages to the sensor. The sensor should get a BCC copy of all delivered messages, but not any spam or virus mail that is dropped or quarantined.

12. Click Commit Changes.

Note that after committing changes, mail will begin to route to the Sensor. If there is any issue with messages bouncing, your system may be burdened. Alternatively, you may wait to Commit Changes until completing the Bounce handling steps in the next section.

Step 3: Exclude quarantined messages from being copied to the sensor

Spam, virus, graymail, and similar messages that your policies quarantine should not be sent to the Cisco sensor. To exclude these quarantined messages from being impacted by the BCC content filter created above, you can add an action to the Incoming Mail Policies to insert specific headers for the different types of quarantined messages, and then use the existence of any of those headers as a condition to exclude the messages from being triggered by the content filter and copied to the sensor.

If your policies do not add custom headers to your messages to identify them as spam, you may also want to modify the policies to which this filter will be attached to that the filter condition can properly identify the messages to exclude.

#### Modify the Policies That Will Use This Filter

This will add one or more custom headers to a policy. The goal here is to perform this action on any policies you have defined that are used to identify spam and quarantine messages.

1. Go to Mail Policies > Incoming Mail Policies.
2. Click the anti-spam, (for spam), anti-virus, advanced malware protection, or graymail (for quarantined messages) settings in the row of the policy you want to edit.
3. Click Advanced. (Depending on which setting you're modifying, it could be in the Suspected Spam Settings, Virus Infected Messages, or Action on Bulk Email sections.)

| Suspected Spam Settings                   |                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Suspected Spam Scanning:           | <input type="radio"/> No <input checked="" type="radio"/> Yes                                                                                                                                                                                                                                                                        |
| Apply This Action to Message:             | Spam Quarantine <input type="button" value="v"/><br><small>Note: If local and external quarantines are defined, mail will be sent to local quarantine.</small>                                                                                                                                                                       |
| Add Text to Subject:                      | Prepend <input type="button" value="v"/> [SUSPECTED SPAM]                                                                                                                                                                                                                                                                            |
| <input type="button" value="v"/> Advanced | <div style="border: 1px solid orange; padding: 5px;">           Add Custom Header (optional):<br/>           Header: <input type="text"/><br/>           Value: <input type="text"/> </div> Send to an Alternate Envelope Recipient (optional):<br>Email Address: <input type="text"/><br><small>(e.g. employee@company.com)</small> |
| Archive Message:                          | <input checked="" type="radio"/> No <input type="radio"/> Yes                                                                                                                                                                                                                                                                        |

4. In the Add Custom Header section, enter values for Header and Value. The header should be both unique and self explanatory. For example, for spam, it could be *MyCompany\_suspected\_spam*. The value should be something that makes sense for the vocabulary you use, such as *positive* or *true*.
5. Make note of the Header value so you can use it in the next section, "Add a Condition to the Filter" below.
6. Click Submit.

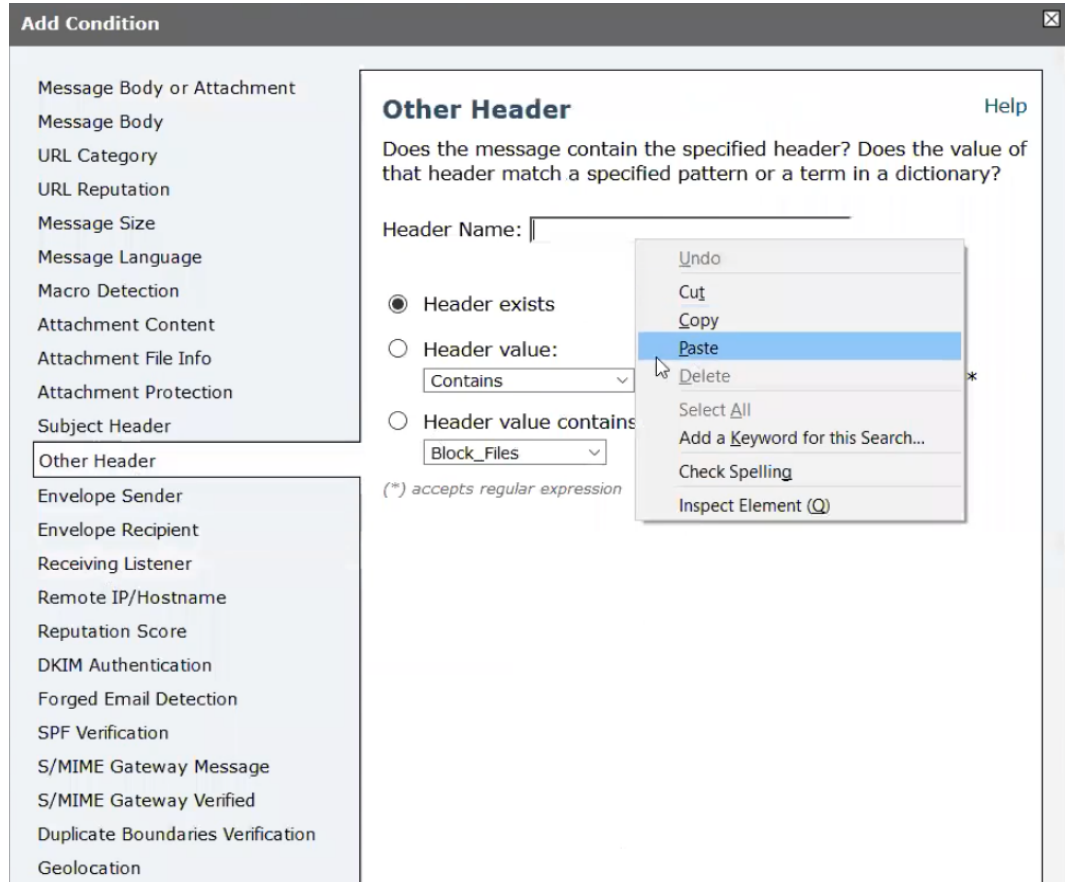
Repeat for all of the spam, anti-virus, and graymail policies that quarantine messages.

Your policy may also modify message subjects when identifying spam. For example, some companies will configure a spam rule to prepend [SUSPECTED SPAM] to identified spam messages. While you can configure a policy condition to match message modifications in the subject, doing so is more complicated and can take longer. Matching header values is both faster and more reliable.

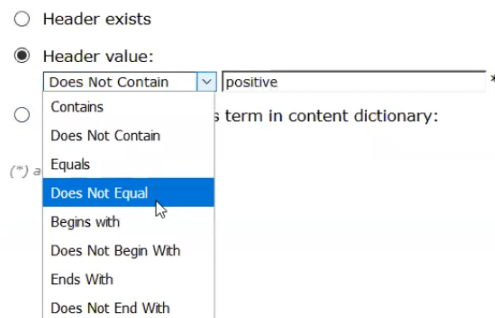
#### Add a Condition to the Filter

1. Go to Mail Policies > Incoming Mail Filters.
2. Click the name of the filter you created in step 1.
3. Click Add Condition.

4. Click Other Header.
5. In the Header Name field, enter the name of a custom header you created in "Modify the Policies That Will Use This Filter" on the previous page.



6. In the Header Value drop-down list, select Does Not Equal, and then enter the value of the custom header you created above.



7. Click OK.
8. Repeat steps 3 through 7 for all the headers you added in "Modify the Policies That Will Use This Filter" on the previous page.
9. In the Apply Rule drop-down list, select Only if all conditions match.

| Conditions       |              |                                          |        |
|------------------|--------------|------------------------------------------|--------|
| Add Condition... |              | Apply rule: Only if all conditions match |        |
| Order            | Condition    | Rule                                     | Delete |
| 1                | Other Header | header("X-Spam") != "True\$"             |        |
| 2                | Other Header | header("X-Virus") != "True\$"            |        |

10. Click Submit.

If you remember, in step 1, this content filter was configured to send a copy via bcc: to the Cisco sensor. This condition now modifies this directive to send a copy via bcc: to the Cisco sensor except if there is a custom header in the message that exists because the message was identified as spam.

| Content Filter Settings     |                                                          |
|-----------------------------|----------------------------------------------------------|
| Name:                       | <input type="text" value="Spam_Scanner"/>                |
| Currently Used by Policies: | Temp Whitelist, Test URL content filters, Default Policy |

The policies that use this content filter.

Note that this content filter must be referenced in and enabled on any policies where you want this filter to be used. Make sure that the policies where you added custom headers to be used by content filters have those content filters included and active in the policies.

#### Step 4: Configure Bounce Handling to the Sensor

To use minimal ESA system resources, you should configure the system to fail bounce messages rapidly if delivery to the Sensor fails.

1. Provide an email address that the Bcc: is delivered to that is within a unique domain or sub-domain and that is accepted by the destination host. The "Alternate Mail Host" delivery action should take care of the message being directed to that server, so there is no need to create a specific DNS entry for the email address's domain. For the purposes of this example we will use "symbolic\_name.hosted.appc.cisco.com" for the domain.
2. Create a Bounce Profile to rapidly fail bounce messages.
  1. Go to Network > Bounce Profiles.
  2. Click Add Bounce Profile to create a new entry.
  3. Enter values as shown in the following figure:



### Edit Bounce Profile

Mode — Cluster: Cluster-o-rama Change Mode...

Centralized Management Options

---

#### Edit Bounce Profile

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| Profile Name:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Impatient                                              |
| Maximum Number of Retries:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 1<br><small>(between 0 and 10000)</small>              |
| Maximum Time in Queue:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 3600 seconds<br><small>(between 0 and 3000000)</small> |
| Initial Time to Wait per Message:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 60 seconds<br><small>(between 60 and 86400)</small>    |
| Maximum Time to Wait per Message:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 3600 seconds<br><small>(between 60 and 86400)</small>  |
| <b>Hard Bounce and Delay Warning Messages:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                        |
| Send Hard Bounce Messages:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                        |
| <input checked="" type="radio"/> Use Default (Yes) <input type="radio"/> Yes <input type="radio"/> No<br>Use DSN format for bounce messages:<br><input checked="" type="radio"/> Use Default (Yes) <input type="radio"/> Yes <input type="radio"/> No<br>Message Composition<br>Message Subject: Delivery Status Notification (Failure)<br>Parse DSN "Status" field from bounce responses: <input checked="" type="radio"/> Use Default (No) <input type="radio"/> Yes <input type="radio"/> No<br>Notification Template: System Generated <a href="#">Preview Message</a> |                                                        |
| Send Delay Warning Messages:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                        |
| <input checked="" type="radio"/> Use Default (No) <input type="radio"/> Yes <input type="radio"/> No<br>Message Composition<br>Message Subject: Delivery Status Notification (Delay)<br>Notification Template: System Generated <a href="#">Preview Message</a><br>Minimum Interval Between Messages: 14400 seconds<br>Maximum Number of Messages to Send: 1                                                                                                                                                                                                               |                                                        |
| Recipient for Bounce and Warning Messages:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                        |
| <input checked="" type="radio"/> Message sender<br><input type="radio"/> Alternate:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                        |
| Use Domain Key Signing for Bounce and Delay Messages:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                        |
| <input checked="" type="radio"/> Use Default (Yes) <input type="radio"/> Yes <input type="radio"/> No<br><small>There is no signing profile matching bounce from address MAILER-DAEMON@___NOTSET___. Bounce messages will not be signed until you create appropriate signing profile.</small>                                                                                                                                                                                                                                                                              |                                                        |

Cancel Submit

3. Create a specific Destination Control for the unique Sensor domain described above ("symbolic\_name.hosted.appc.cisco.com", in this example) that references the aggressive Bounce Profile created in the previous step (named "Impatient" in this example):
  1. Go to Mail Policies -> Destination Controls.
  2. Enter values as shown in the following figure:

**Edit Destination Controls**

Destination: collector.host

IP Address Preference: Default (IPv6 Preferred)

**Limits:**

- Concurrent Connections:
  - Use Default (500)
  - Maximum of  (between 1 and 1,000)
- Maximum Messages Per Connection:
  - Use Default (50)
  - Maximum of  (between 1 and 1,000)
- Recipients:
  - Use Default (No Limit)
  - Maximum of  per  minutes  
Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60
- Apply limits: Per ESA hostname:
  - System Wide
  - Each Virtual Gateway  
(recommended if Virtual Gateways are in use)

**TLS Support:** None

A security certificate/key has not yet been configured. Enabling TLS will automatically enable the "Demo" certificate/key. (To configure a different certificate/key, start the CLI and use the certconfig command.)

**Bounce Verification:**

Perform address tagging:
 

- Default (No)
- No
- Yes

Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.

**Bounce Profile:** Impatient

Bounce Profile can be configured at Network > Bounce Profiles.

Cancel Submit

- If your Sensor is not inside your protected network and you would like to encrypt the stream of mail going to it, you can change the TLS Support option to Required. The Cisco ESA will now connect securely to the remote Sensor (over port 25 via "STARTTLS").
- Click Commit Changes.

#### Step 5: Confirm System Alerts

Go to System Administration > Alerts and confirm that System and Hardware alerts will be sent to an address that is monitored in case there are any issues with the dual delivery setup and configuration.

#### Step 6: Consider Other Whitelisted Email Streams

You may have firewall rules in place that whitelist upstream MTAs sending mail to your Cisco ESA system. This is usually accomplished with the Host Access Table (HAT), which delivers the message and skips any subsequent content filters. Assuming you have configured dual delivery as described in this document, such messages will fail to be copied to the sensor because the dual delivery mechanism is part of a content filter and is evaluated later in the email pipeline.

Addressing this issue will depend on the specifics of your inbound email flow, but one possible method is to use a content filter rather than the Host Access Table to whitelist inbound traffic. You can instead create a content filter rule that matches on the sender's IP address, sends a copy to the sensor (using the same configuration described in this document), and then triggers the message to be delivered without further filtering (using the Skip Remaining Content Filters action). You could then deactivate the corresponding HAT entry for that sending IP.

#### Step 7: Whitelist the Alerts Server

When an email is deemed suspicious, Advanced Phishing Protection can optionally send an email alert to administrators and/or the original recipient of the suspicious message.

Besides identifying the threatening message, the alert email can contain additional information about the type or severity of the threat. In case of operational problems, the notification server may also send out alerts regarding your Sensor and the overall health of the Advanced Phishing Protection service. Given the importance and utility of these alerts, it is recommended that you whitelist the notifications server to ensure that your system does not block or quarantine these messages.

For example, the messages that the notifications server sends may sometimes contain portions of the content of the original messages. Since the original messages may contain spam, or otherwise be perceived as suspicious by email filtering software, it is possible that the alerts may themselves accidentally be perceived as threats.

So it is important to whitelist the notification server to prevent triggering of false positives in the filtering software. If there are intermediate filtering steps (for example, other intermediate MTAs, or other anti-phishing solutions which filter email) they should also be configured to whitelist the notifications server. The Sales Engineering and Customer Success teams can assist with configuring the whitelist, if necessary.

1. Go to Mail Policies > HAT Overview. This will open the "Host Access Table" configuration which allows you to add the alerts server to the list of trusted senders. The configuration pane will look something like this:

**HAT Overview**

Find Senders

Find Senders that Contain this Text:

Sender Groups (Listener: smtp-in 192.168.109.2:25 )

| Order | Sender Group | SenderBase™ Reputation Score <sup>?</sup> |    |    |    |    |   |   |   |   |   |     | Mail Flow Policy | Delete                                |
|-------|--------------|-------------------------------------------|----|----|----|----|---|---|---|---|---|-----|------------------|---------------------------------------|
|       |              | -10                                       | -8 | -6 | -4 | -2 | 0 | 2 | 4 | 6 | 8 | +10 |                  |                                       |
| 1     | WHITELIST    |                                           |    |    |    |    |   |   |   |   |   |     | TRUSTED          | <input type="button" value="Delete"/> |
| 2     | BLACKLIST    |                                           |    |    |    |    |   |   |   |   |   |     | BLOCKED          | <input type="button" value="Delete"/> |
| 3     | SUSPECTLIST  |                                           |    |    |    |    |   |   |   |   |   |     | THROTTLED        | <input type="button" value="Delete"/> |
| 4     | UNKNOWNLIST  |                                           |    |    |    |    |   |   |   |   |   |     | ACCEPTED         | <input type="button" value="Delete"/> |
|       | ALL          |                                           |    |    |    |    |   |   |   |   |   |     | ACCEPTED         |                                       |

Key:

Your configuration may differ in various ways, and you may need to adjust these instructions to suit your particular environment. For example, you will need to repeat this configuration for each inbound listener, so that the alerts server is whitelisted for all configured inbound listeners.

2. Assuming you have the default Sender Groups in place, click the WHITELIST link. If you have alternate Sender Groups, use the one that maps to a "TRUSTED" Mail Flow Policy or its equivalent.
3. In the Sender List: Display All Items in List section, click Add Sender.
4. In the Sender field, enter the IP address of the alerts server: 198.2.132.180.
5. In the Comment field, add a comment, such as "Whitelist alerts server."
6. Click Submit.

- On the Sender Group pane, confirm the IP address is present in the Sender List section:

**Sender Group: WHITELIST - smtp-in 192.168.109.2:25**

Success — Sender "198.2.132.180" was added.

| Sender Group Settings             |                                                                |
|-----------------------------------|----------------------------------------------------------------|
| Name:                             | WHITELIST                                                      |
| Order:                            | 1                                                              |
| Comment:                          | My trusted senders have no anti-spam scanning or rate limiting |
| Policy:                           | TRUSTED                                                        |
| SBRS (Optional):                  | Not in use                                                     |
| DNS Lists (Optional):             | None                                                           |
| Connecting Host DNS Verification: | None Included                                                  |

[<< Back to HAT Overview](#) [Edit Settings...](#)

---

**Find Senders**

Find Senders that Contain this Text:  [Find](#)

---

**Sender List: Display All Items in List** Items per page 20

[Add Sender...](#)

| Sender        | Comment                       | All<br><input type="checkbox"/><br>Delete |
|---------------|-------------------------------|-------------------------------------------|
| 198.2.132.180 | Whitelist Agari alerts server | <input type="checkbox"/><br>Delete        |

[<< Back to HAT Overview](#) [Delete](#)

- Click Commit Changes.

As seen above, the IP address of the alerts server is 198.2.132.180. A DNS entry for this address is also maintained, but in general, it is recommended to use the explicit IP address for this whitelisting rule.

## Configure Cisco ESA to Add an X-Agari-Authentication-Results Header

This section is intended only for the cases where the Cisco ESA system you are configuring is a perimeter gateway and is not being used for dual delivery. If you are using your Cisco ESA system to generate the dual delivery stream, then do not use this section; instead follow the above instructions which include the proper way to add the X-Agari-Authentication-Results header.

- Log into the Cisco ESA as an Administrator.
- Go to Mail Policies > Incoming Content Filters.

If your environment is Clustered, execute the remaining steps at either the top level or at the group level (if the action is intended to only affect a certain set of ESA instances). Do not add perform these steps at the machine level.

- Click Add Filter.
- Name the filter "Agari\_auth\_header."
- Add a reasonable description for the filter, for example: "Add the X-Agari-Authentication-Results header to all incoming email."

6. Adjust the order of the filter so such that it adds the header to all incoming email. The filter, then, should be placed at or near the top of the list: consider this filter's placement with respect to your existing filter.
7. The filter does not need any Conditions; a filter with no conditions defaults to matching all messages. Depending on the environment, you can associate the filter to a specific Incoming Mail Policy (as described below) for certain recipients or domains.
8. Click Add Action to associate an action with this filter.
9. In the Add Action window, select Add/Edit Header.
10. Using the interface, specify the filter to add two new headers to the message to indicate both the original recipients and original sender (which are not always correctly reflected in the visible message headers):
  - Header name: X-Agari-Original-From Header data: \$EnvelopeFrom
  - Header name: X-Agari-Original-To Header data: \$envelope recipients
11. Using the interface, direct the filter to duplicate the Authentication-Results header:
  - Header Name: X-Agari-Authentication-Results "Specify Value for New Header" : \$Header ['Authentication-Results']

The screenshot shows the 'Add Action' dialog box with the 'Add/Edit Header' action selected. The configuration is as follows:

- Header Name:** X-Agari-Authentication-Results
- Specify Value for New Header (optional):** \$Header['Authentication-Results']
- Prepend to the Value of Existing Header:** (empty)
- Append to the Value of Existing Header:** (empty)
- Search & Replace from the Value of Existing Header:** (unchecked)
- Search for:** (empty)
- Replace with:** (empty)

Additional text in the dialog includes: "Inserts a header and value pair into the message or modifies value of an existing header before delivering." and a note: "(\*) accepts regular expression".

12. Click OK. The completed incoming content filter will look something like this:

**Add Incoming Content Filter**

**Content Filter Settings**

Name:

Currently Used by Policies: *No policies currently use this rule.*

Description:

Order:  (of 2)

**Conditions**

*There are no conditions, so actions will always apply.*

**Actions**

| Order | Action          | Rule                                                                                  | Delete                                |
|-------|-----------------|---------------------------------------------------------------------------------------|---------------------------------------|
| 1     | Add/Edit Header | insert-header("X-Agari-Authentication-Results", "\${Header[Authentication-Results]}") | <input type="button" value="Delete"/> |

13. Click Submit.
14. Associate the filter with an appropriate Incoming Mail Policy:
1. Go to Mail Policies > Incoming Mail Policies.
  2. In the Content Filters column for the appropriate row, edit the assigned Content filters to reference the newly-created filter. You may need to enable Content Filters for that Policy in the process. The modified Policy row will look similar to the following:

| Order | Policy Name | Anti-Spam                                                                                             | Anti-Virus                                                            | Advanced Malware Protection | Content Filters   | Outbreak Filters | Delete                                |
|-------|-------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|-----------------------------|-------------------|------------------|---------------------------------------|
| 7     | tomki.com   | IronPort Anti-Spam<br>Cloudmark Service Pr...<br>Positive: Quarantine<br>Suspected: Quarantine<br>... | Sophos<br>McAfee<br>Encrypted: Deliver<br>Unscannable: Deliver<br>... | (use default)               | Agari_auth_header | (use default)    | <input type="button" value="Delete"/> |

15. Click Commit Changes.

You should also confirm that evaluation of SPF, DKIM, and any other authentication mechanisms (Sender ID, DMARC, etc.) is enabled on the ESA, so that the "X-Agari-Authentication-Results" header will be populated with the correct data.

## Wrapping Up

When the above steps are completed, the sensors will start receiving copies of email messages sent into your organization. There may be a small delay of a few minutes before the changes take full effect. You can confirm the traffic flow by logging into Advanced Phishing Protection at <https://appc.cisco.com> and navigating to Manage > Sensors to see the status of your installed sensors.



## CHAPTER 5

# Enforcement

*Enforcement* is the term used where you configure Cisco Advanced Phishing Protection to move identified messages from your users' inboxes to a special folder. It is sometimes referred to as *API enforcement* because messages are moved by using an API (application programming interface) that communicates programmatically between Advanced Phishing Protection and your users' mailboxes.

The enforcement action is an enhancement to policies. In addition to logging and alerting, you can configure the system so that matching messages are moved to a folder you designate.

API Enforcement is available for Office 365, Exchange (2010, 2013, and 2016), and G Suite environments only.

## Configure Enforcement: G Suite

Enforcement for G Suite users is available only for organizations with hosted Sensors. See "Sensors" on page 16 for more information.

This topic describes how to configure enforcement for Google G Suite.

The general procedure is as follows:

Step 1: Configure a service account for G Suite.

Step 2: Enable enforcement on your sensors

Step 3: Enable enforcement in the web application.

Step 4: Enable the system notification for enforcement problems.

Step 5: Test the enforcement policy action.

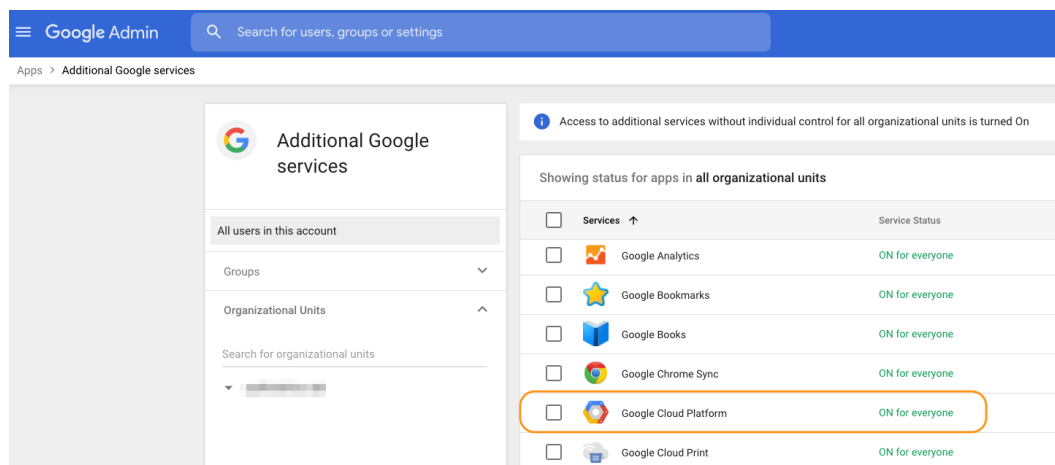
Step 1: Configure a Service Account

This section explains how to configure a service account for G Suite. This involves creating the service account and granting scope to the service account.

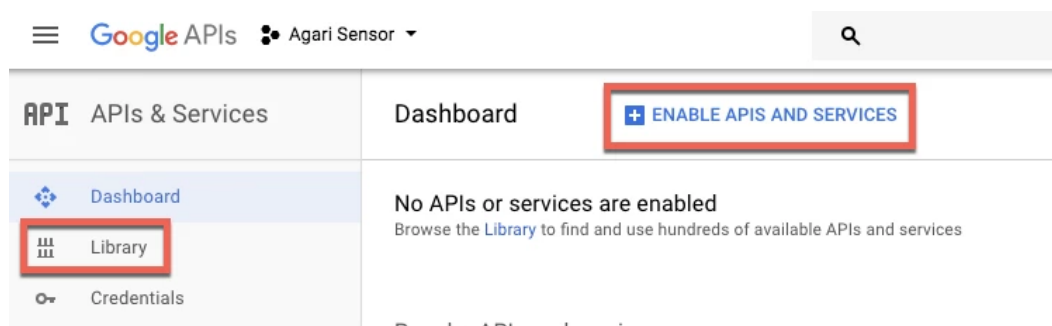
Create the Service Account

1. Ensure that your G Suite account has been enabled in the Google Cloud Platform:
  1. Go to <http://admin.google.com> and log in as a user with administrator privileges.
  2. Click Apps: Manage apps and their settings.
  3. Click Additional Google Services.

- From the list of additional services, scroll to find Google Cloud Platform (there are multiple pages, so it may be easier to type *cloud platform* in the search bar).

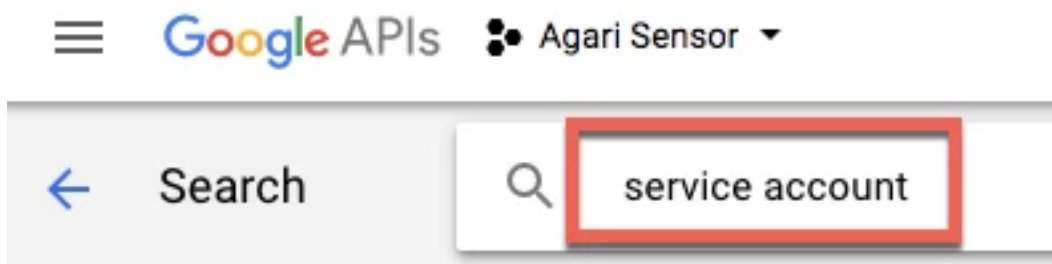


- Select the Google Cloud Platform check box so that it will be On for everyone.
- Go to the Developers Console at <https://console.developers.google.com/>. You will create a project and generate a credentials file for Advanced Phishing Protection to access your Gmail application.
- API Credentials are associated with "projects." To create a new project, click the Select a project drop-down list, and then in the new window, click New Project.
- Enter Cisco Sensor for the Project Name.
- Click Create. It is not necessary to set any advanced options. You may need to wait up to 2 minutes for the project to be created completely..
- Once the project is created, select it from the list (if it doesn't automatically open):
- Enable APIs - if the API library doesn't automatically open, you can access by clicking "ENABLE APIS AND SERVICES" or "Library" - you will be presented with a list of available APIs.



- Search for Service Account.





9. Click Identity and Access Management (IAM) API.
10. Click Enable.
11. Click Credentials.
12. Click Create credentials > Service account key.
13. In the Service account drop-down list, select New service account.
14. Enter or select the following settings:
  - Service Account Name: Cisco Sensor
  - Select a Role: Service Accounts > Service Account Token Creator and Service Account User
  - Service Account ID: will be automatically populated
  - Key Type: JSON
15. Click Create.
16. Save the .json file.
 

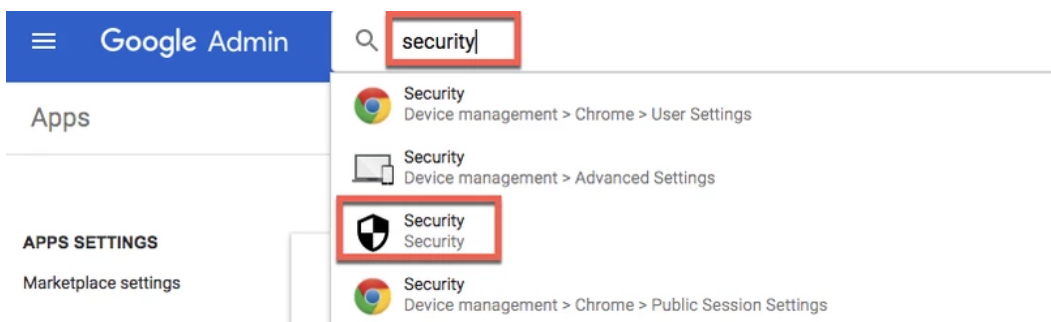
Save this file to a secure location, and do not lose this file. The credentials contained in this file grant limited access to all of the inboxes in your organization. You will use these credentials in the next section to grant access to the sensor(s).
17. Click Close.
18. Click Manage service accounts.
19. Click Edit.
20. Select the Enable G Suite Domain-wide Delegation check box.
21. In the Product name for consent screen field, enter Cisco Sensor
22. Click Save.
23. The project associated with the credentials must be activated to use the Gmail API. Click the Google APIs link in the top menu.
24. Click Library.
25. Search for Gmail and select Gmail API.
26. Click Enable.
27. Click Library.
28. Search for Admin SDK and select Admin SDK.
29. Click Enable.

The service account is now configured to be used with the Gmail API and Admin SDK API.

## Grant Scopes to the Service Account

Now you must grant access scopes (specific for Gmail) to the service account you created in "Create the Service Account" on page 75.

1. Go to the Administrator console at <http://admin.google.com> and, if necessary, log in as a user with administrator privileges.
2. Go to Apps.
3. Search for security and select the Security app shown here:



4. Click API reference.
5. Select the Enable API Access check box.
6. Click Advanced settings.
7. Click Manage API client access.
8. In the Client Name field, enter the Client ID of the service account created in "Create the Service Account" on page 75. You can find this ID in two places:
  - In the .json file that you downloaded, it will appear on a line by itself. In this example, the client\_id is on line 7:

```

1 | {
2 |   "type": "service_account",
3 |   "project_id": "cisco-sensor-202903",
4 |   "private_key_id": "-----",
5 |   "private_key": "-----",
6 |   "client_email": "ag-----",
7 |   "client_id": "109-----",
8 |   "auth_uri": "https://accounts.google.com/o/oauth2/auth",
9 |   "token_uri": "https://accounts.google.com/o/oauth2/token",
10 |  "auth_provider": "google.com",
11 |  "client_x509_certs": [
12 |    {
13 |      "cert": "-----"
    }
  ]
}

```

- In the developers console (<https://console.developers.google.com>), click Credentials. The Client ID is listed there:

| OAuth 2.0 client IDs     |                       |               |                        |
|--------------------------|-----------------------|---------------|------------------------|
| <input type="checkbox"/> | Name                  | Creation date | Type                   |
| <input type="checkbox"/> | Client for cisco-demo | May 2, 2018   | Service account client |

The Client ID field in the table above is highlighted with a red box, showing the value: 109-----

Copy the Client ID (not including the quotations) and paste it into the Client Name field

9. In the One or More API Scopes field, enter the following strings exactly as below, with no changes or extra information in the field. You can simply copy and paste the entire string in the field - it will appear wrapped across multiple lines in this document, but will paste as a single line:

<https://mail.google.com/>, <https://www.googleapis.com/auth/gmail.labels>, <https://www.googleapis.com/auth/gmail.modify>, <https://www.googleapis.com/auth/gmail.readonly>, <https://www.googleapis.com/auth/admin.directory.user.readonly>

Make sure that if you copy the entire string of URLs and you paste the string of URLs into the field, that no spaces are added within the URLs themselves.

10. Click Authorize.

A row will appear indicating that permissions have now been granted to the supplied Client ID

### Step 2: Enable Enforcement on Your Sensor(s)

Using the JSON credentials you downloaded in "Create the Service Account" on page 75, you can now enable enforcement on each of your sensors. You can accomplish this within Advanced Phishing Protection or using the command-line interface for each sensor.

#### Enable Enforcement on a Sensor in Advanced Phishing Protection

Prerequisite: The JSON file you downloaded in "Create the Service Account" on page 75.

1. Go to Manage > Sensors.
2. If you have more than one sensor, select the appropriate tab for the sensor.
3. Click Enable API Enforcement.
4. Copy the entire contents of the JSON service credentials file and paste those contents into the Service account credentials field.
5. Enter a Test administrator email address. You must provide a test email address that is an actual known good inbox in your G Suite environment; this test address is used to test that Advanced Phishing Protection can successfully authenticate and use the API to see and access the mailboxes in your environment.
6. Click Test and Enable API Enforcement.

No test email is sent during this enablement step.

A success message appears informing you that the permissions were granted successfully from the G Suite service account:

This process only provides the ability for Advanced Phishing Protection to be able to enforce messages via the API. Enforcement will not yet be enabled. You will still need to enable enforcement at the organizational level within Advanced Phishing Protection and then configure policies to use an enforcement action before any messages are to be moved from users' inboxes.

### Step 3: Enable Enforcement for Your Organization

Once you have enabled enforcement on at least one sensor, you will be able to configure enforcement for your organization in the web application.

1. Go to Manage > Organizations.
2. Click the name of the organization.
3. In the Enforcement Settings section, set the Enforcement switch to Enable.
4. Enter an Enforcement Label. The enforcement label is the "tag" or "folder name" that will be added to messages that are enforced; effectively the message will be moved to this folder

name, and it will be the name of the folder users see in their email client.

5. Click Save.

#### Step 4: Enable the Enforcement-related System Notification

When enforcement is enabled for your organization, an additional system notification is available to alert you to when the credentials the sensor uses for enforcement are broken.

1. Go to Manage > Policies.
2. Click the System Notifications tab.
3. Select the The credentials supplied for... check box.
4. Click Save.

#### Step 5: Test the Enforcement Actions with Policies

When enforcement has been enabled on each sensor and globally for the organization, you can begin to create policies with an enforcement action.

To test the enforcement action, begin by creating a policy with a very narrow set of conditions that you are confident will match.

For example, you could create a policy with a From: address of your exact personal (public) email address with a very specific Subject line:

### Create Policy

Based on conditions in emails coming into your organization, trigger an event.

Policy Name:

**Content**  
All conditions must apply (logical AND)

From:

Reply-To:   
 Reply-To: address does not match From: address

To:   
 To: address is equal to the From: address

Subject:

The From, Reply-To, To, and Subject fields are case-insensitive, partial matching

Creating a policy: conditions

In the Actions section of the policy creation page, specify an Enforcement action:

**Actions**  
 Enforce and Notify actions are optional; all messages matching conditions of a saved policy are logged in the Event Log.

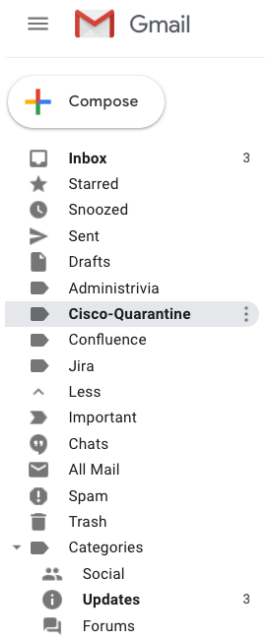
Enforce:  Move matching messages to folder: Cisco-Quarantine

Defining an enforcement action in a policy

Save your policy, and then send a test message that will match the conditions in the policy.

You should see that the message (if it not filtered by any other upstream process in your mail stream) will be moved to the folder specified in the Enforcement action.

For example, folders appears in Gmail clients like this:



The Cisco-Quarantine folder in Gmail

Additionally, note that the Policies page contains a column indicating which policies have an enforcement action:

Policies

System Notifications | Event Log

Configure Policies based on message content.

Create Policy | Configure Policy Text for Original Recipients

Displaying 1 - 22 of 22 Policies

| Name                 | Conditions                                   | Move? | Notify Recipients? | Last Triggered           | Number of Times Triggered (in last 30d) |
|----------------------|----------------------------------------------|-------|--------------------|--------------------------|-----------------------------------------|
| Untrusted + enforced | • Message Trust Score is between 0.0 and 1.1 | Y     | N                  | 16-Nov-2016 20:05:53 UTC | 1,838                                   |

The Move column on the Policies page

## Wrapping Up

Among the actions you can take at this point are to view a report on enforcement (see "Reporting on API Enforcement" on page 95) and making sure enforcement is working on a Sensor (see "Enforcement Sensor Status" on page 94).

As you create policies with an enforcement action, you can expand the conditions to include a wider range of matching emails.

You can also expand who is notified (additional recipients and the original recipients).

## Configure Enforcement: Office 365

Enforcement for Office 365 users is available only for organizations with hosted Sensors. See "Sensors" on page 16 for more information.

This section describes how to configure enforcement for Office 365.

Before you begin, Have your sales representative register your organization for API Enforcement. (This is done outside of Advanced Phishing Protection.)

Registering for API Enforcement will register the Sensor as an application in the Cisco Secure Email Cloud environment.

The general procedure is as follows:

Step 1: Enable enforcement on your sensors, which will request API access to your Office 365 environment.

Step 2: Enable enforcement in Advanced Phishing Protection.

Step 3: Optionally enable the enforcement-related system notification.

Step 1: Enable Enforcement on Your Sensors

1. Go to Manage > Sensors.
2. If you have more than one sensor, select the appropriate tab for the sensor.
3. Click Enable API Enforcement.

A dialog window appears informing you that, after supplying a test email address, you will be directed to the Office 365 login screen.

An account that has appropriate administrative permissions must log in and approve (via an OAuth Admin Consent) the permissions requested by the Advanced Phishing Protection application.

The consent screen will be presented immediately after a Global Administrator logs in, and the consent only needs to be granted once per sensor by a Global Administrator to enable enforcement capability for all inboxes in your Office 365 environment.

You must provide a test email address which is an actual known good inbox in your Office 365 environment; this test address is used to test that the Advanced Phishing Protection application can successfully authenticate and use the API to see and access the mailboxes in your environment.

No test email is sent during this enablement step.

4. Enter a test email address.
5. Click Test and Enable API Enforcement.
6. In the Office 365 login page, log in as a Global Administrator for your Office 365 environment.

After logging in, the consent screen is presented.

The screen requests permissions for the sensor application to access the inboxes of users in your Office 365 organization in order to move messages.

Important note: Clicking "Accept" only provides the ability for the Advanced Phishing Protection application to be able to enforce messages via the API.

Enforcement will not yet be enabled by clicking accept; you will still need to enable enforcement at the organizational level within Advanced Phishing Protection and then configure policies to use an enforcement action before any messages are to be moved from users' inboxes.

For more information on monitoring enforcement actions performed by the API, see "Managing Enforcement using Microsoft Office 365 Auditing Tools" below. Note that You have the ability to disable AND revoke permissions granted in this step at any time.

7. Click Accept to grant permissions and return the Advanced Phishing Protection application.

A success message appears informing you that the permissions were granted successfully from the Microsoft API.

### Step 2: Enable API Enforcement for Your Organization

If your sales representative has enabled the API Enforcement feature for your organization and you have enabled API Enforcement on at least one sensor, you will see in Advanced Phishing Protection that enforcement can now be enabled at the organization-wide level.

1. Go to Manage > Organizations.
2. Click the name of the organization.
3. In the Enforcement Settings section, set the Enforcement switch to Enable.
4. Enter an Enforcement Label. The enforcement label is the "tag" or "folder name" that will be added to messages that are enforced; effectively the message will be moved to this folder name, and it will be the name of the folder users see in their email client. If that folder already exists exactly in a user's email client, that folder will be used for API-enforced messages. If it does not exist in a user's email client, it will not be created in the client until a message is first received that is then enforced.

You can also specify the "Junk Email" folder to enforce messages directly to Office 365's trash email folder; note that messages in this folder are subject to the automatic deletion rules in Office 365.

5. Click Save.

Microsoft has changed the default name of the junk email folder in its email client software over the years, names that have included Junk, Junk E-Mail, and Junk Email, and other email clients may also use their own naming conventions for junk email folders. You may want to enter multiple folder names for junk message enforcement if in your email environment you're using clients with different folder names for junk email.

### Step 3: Enable the Enforcement-related System Notification

When enforcement is enabled for your organization, an additional system notification is available to alert you to when the credentials the Sensor uses for enforcement are broken.

1. Go to Manage > Policies.
2. Click the System Notifications tab.
3. Select the The credentials supplied for... check box.
4. Click Save.

## Testing the API Enforcement Action with Policies

When enforcement has been enabled on each sensor and globally for the organization, you can begin to create policies with an enforcement action. You can either create an explicitly defined policy, as described in this section, or you can create an on-demand policy. See "On-demand Policies" on page 130 for instructions on how to do the latter.

To test the enforcement action, begin by creating a policy with a very narrow set of conditions that you are confident will match.

For example, you could create a policy with a From: address of your exact personal (public) email address with a very specific Subject line:



### Create Policy

Based on conditions in emails coming into your organization, trigger an event.

Policy Name:

**Content**  
All conditions must apply (logical AND)

From:

Reply-To:   
 Reply-To: address does not match From: address

To:   
 To: address is equal to the From: address

Subject:

The From, Reply-To, To, and Subject fields are case-insensitive, partial matching

#### Creating a policy: conditions

In the Actions section of the policy creation page, specify an Enforcement action:

**Actions**  
Enforce and Notify actions are optional; all messages matching conditions of a saved policy are logged in the Event Log.

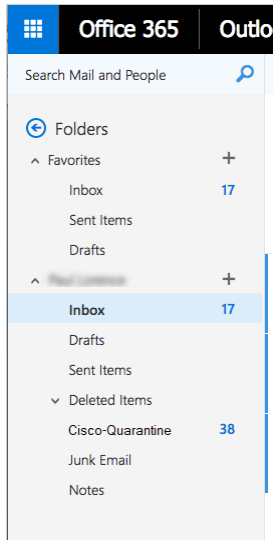
Enforce:  Move matching messages to folder: Cisco-Quarantine

#### Defining an enforcement action in a policy

Save your policy, and then send a test message that will match the conditions in the policy.

You should see that the message (if it not filtered by any other upstream process in your mail stream) will be moved to the folder specified in the Enforcement action.

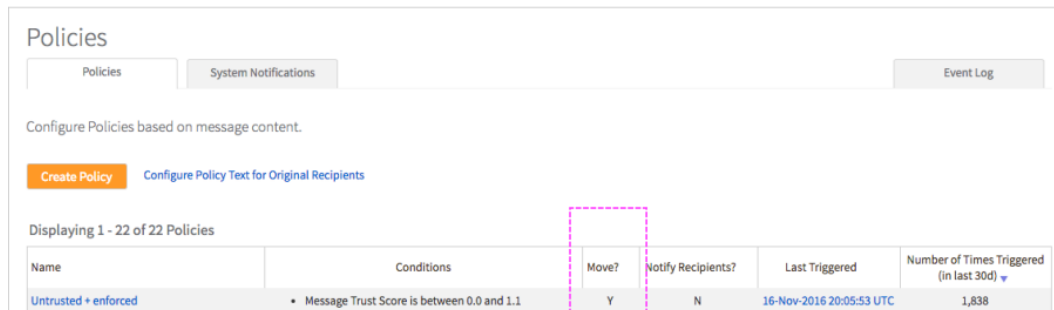
For example, folders appears in O365 clients like this:



Quarantine folder in the Office 365 client

Your users may need to refresh their browser in order to see the "Cisco-Quarantine" folder immediately after the folder is created.

Additionally, note that the Policies page contains a column indicating which policies have an enforcement action:



Move action column

## Managing Enforcement using Microsoft Office 365 Auditing Tools

### Enabling Auditing

Office 365 provides extensive auditing of mailboxes and user and administrator actions; however it is not enabled by default.

Read this article to enable it:

[https://technet.microsoft.com/en-us/library/jj150552\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/jj150552(v=exchg.150).aspx)

The key PowerShell command to enable auditing is:

```
Set-Mailbox <Identity> -AuditEnabled $true
```

The enforcement action is logged as an "Owner" logon type; a PowerShell command to enable auditing of certain events might look like:

```
Set-Mailbox <Identity> -AuditOwner Mail-
boxLogin,HardDelete,SoftDelete,Move,MovetoDeletedItems $true
```

If you have O365 access via PowerShell, you can check the audit actions for a specific mailbox by issuing the command:

```
Get-mailbox " mailbox_name" | Select-Object -ExpandProperty AuditAdmin
```

```
Get-mailbox " mailbox_name" | Select-Object -ExpandProperty AuditDelegate
```

```
Get-mailbox " mailbox_name" | Select-Object -ExpandProperty AuditOwner
```

For example:

```
PS C:\Windows\system32> Get-mailbox plorenc | Select-Object -ExpandProperty AuditOwner
```

Creating a new session for implicit remoting of "Get-Mailbox" command...

WARNING: Commands available in the newly opened remote session are different than when the im

created. Consider recreating the module using Export-PSSession cmdlet.

Update

Move (<--)

MoveToDeletedItems

SoftDelete

HardDelete

MailboxLogin

## Performing an Audit

If individual mailbox auditing has been enabled, you can use Microsoft's PowerShell commands to audit a user's inbox to see if Advanced Phishing Protection enforced the message.

For example, the Get-MessageTrace command can specifically requests unique MessageTraceID:

```
PS C:\Windows\system32> Get-MessageTrace -SenderAddress " plorenc@gmail.com" -
StartDate 06/04/2017 -EndDate 06/06/2017 |
```

```
Select-Object Received, SenderAddress, RecipientAddress, Subject, Status, ToIP, FromIP, Size,
MessageID, MessageTraceID
```

```
Received : 6/5/2017 5:16:09 PM
```

```
SenderAddress : plorenc@gmail.com
```

```
RecipientAddress : plorenc@saintmetrics.com
```

```
Subject : move this message automatically enforce me
```

```
Status : Delivered
```

```
ToIP :
```

```
FromIP : 209.85.161.180
```

```
Size : 11049
```

MessageId : <CAEKxqn+Qabt8aHg=Pp=pPW2tYyHuO9TO8dJgs09=bp4uv-ndnw@mail.gmail.com>

MessageTraceId : 8d02ca26-1f78-4185-aa07-08d4ac368ef1

Using the MessageTraceId, you can issue a request for trace details:

```
PS C:\Windows\system32> Get-MessageTraceDetail -MessageTraceId 8d02ca26-1f78-4185-aa07-08d4ac368ef1 -RecipientAddress "p
```

```
lorenc@saintmetrics.com" -StartDate 06/04/2017 -EndDate 06/06/2017
```

Date Event Detail

-----

6/5/2017 5:16:10 PM Receive Message received by: MWHPR16MB1375

6/5/2017 5:16:12 PM Journal Message was journaled. Journal report was sent to test\_stage@stage.en-for...

6/5/2017 5:16:12 PM Journal Message was journaled. Journal report was sent to test\_stage@stage.en-for...

6/5/2017 5:16:12 PM Deliver The message was successfully delivered.

6/5/2017 5:16:12 PM Spam Diagnostics

Note how the Trace shows that the message was delivered, but not moved by the Advanced Phishing Protection API.

However, this command will set up a job to email the search results as an XML attachment to users you specify.

New-MailboxAuditLogSearch - [https://technet.microsoft.com/en-us/library/ff522362\(v=exch.160\).aspx](https://technet.microsoft.com/en-us/library/ff522362(v=exch.160).aspx)

## Enforcement Action Log Example - PowerShell

You can search the audit log to show the move (enforcement) action Advanced Phishing Protection took with the API:

```
PS C:\Windows\system32> Search-MailboxAuditLog -Identity "plarence" -LogonTypes Owner -ShowDetails |select Operation,Fol
```

```
derPathName,DestFolder-
```

```
PathName,LogonType,ClientInfoString,LogonUserDisplayName,SourceltemSubjectsList,LastAccessed
```

```
Operation : Move
```

```
FolderPathName : \Inbox
```

```
DestFolderPathName : \Agari-Quarantine
```

```
LogonType : Owner
```

```
ClientInfoString : Client=REST;Client=RESTSystem;;
```

```
LogonUserDisplayName : Paul Lorence
```

```
SourceltemSubjectsList : Thursday enforce me
```

```
LastAccessed : 6/8/2017 9:11:10 AM
```

Note how the " Move " operation is requested; the DestinationFolderPathname is " Agari-Quar-antine " (the default), and how the LogonType audit action is " Owner. " (Messages which are moved by the API are not considered " Delegate " owner logon actions nor " External Access " audit actions.)

## Enforcement Action Log Example - WebUI

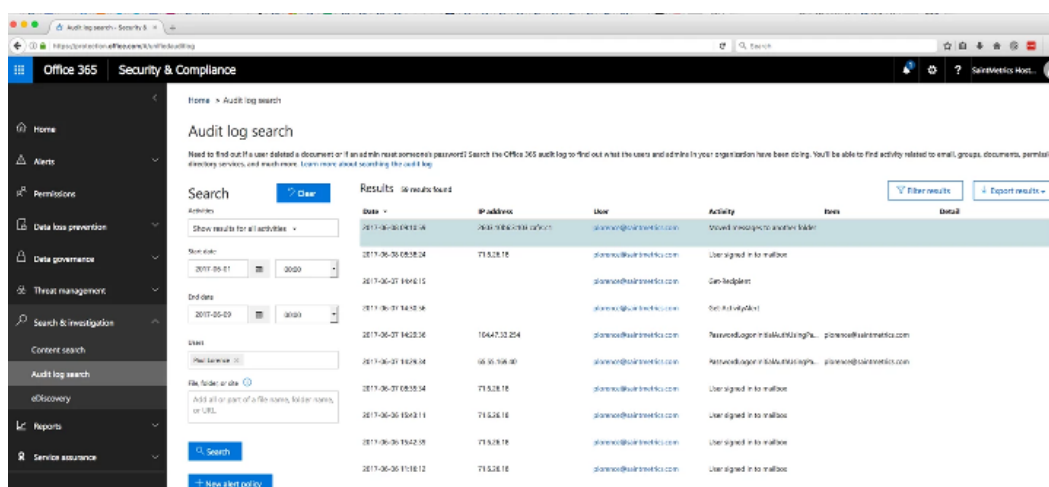
This same information auditing information is shown in the " Security and Compliance " WebUI for Exchange Online Protection (EOP) customers.

If auditing is enabled for your Office 365 organization:

1. Go to https://protection.office.com and authenticate as an Office 365 administrator.
2. Select the Security & Compliance admin center.
3. Choose Search & investigation > Audit log search.
4. Enter the search parameters.
5. View details.

For example, here is the same message viewed in the search results.

Note: " Moved message to another folder " activity:



Audit Log Search message results

Drilling in on the details:

Note the Logon Type value is " 0 " for " Mailbox Owner " :

Details
✕

|                                                       |                                                   |
|-------------------------------------------------------|---------------------------------------------------|
| <b>Date:</b>                                          | 2017-06-08 09:10:59                               |
| <b>IP address:</b>                                    | 2603:10b6:3:103:cafe::c1                          |
| <b>User:</b>                                          | plorence@saintmetrics.com                         |
| <b>Activity:</b>                                      | Moved messages to another folder                  |
| <b>Item:</b>                                          |                                                   |
| <b>Detail:</b>                                        |                                                   |
| <b>Id:</b>                                            | 1b903b61-2b94-4c63-b25d-08d4ae88f37f              |
| <b>Logon Type:</b>                                    | 0                                                 |
| <b>Mailbox Guid:</b>                                  | a7a93b57-6f8b-4f68-9198-099a5b02c0d6              |
| <b>Mailbox Owner UPN:</b>                             | plorence@saintmetrics.com                         |
| <b>Mailbox Owner Sid:</b>                             | S-1-5-21-1927014365-4043437681-3430716724-8054944 |
| <b>Logon User Sid:</b>                                | S-1-5-21-1927014365-4043437681-3430716724-8054944 |
| <b>Record Type:</b>                                   | 3                                                 |
| <b>External Access:</b>                               | false                                             |
| <b>Client Info String:</b>                            | Client=REST;Client=RESTSystem;;                   |
| More information <span style="float: right;">▼</span> |                                                   |

Close

### Audit log details

Click More Information for additional details. Note the ClientInfoString and the DestFolder values:

More information ^

**AffectedItems:**

```
{
  "Id": "RgAAAAA1FAByEUmaTYQkbPnJZf0nBwCHMBEb3yDTT6SNFC1A4Yc",
  "ParentFolder": {
    "Id": "LgAAAAA1FAByEUmaTYQkbPnJZf0nAQCHMBEb3yDTT6SNFC1A4Yk",
    "Path": "\\Inbox"
  },
  "Subject": "Thursday enforce me"
}
```

**ClientIPAddress:** 2603:10b6:3:103:cafe:c1

**ClientInfoString:** Client=REST;Client=RESTSystem;

**CreationTime:** 2017-06-08T16:10:59

**CrossMailboxOperation:** false

**DestFolder:**

```
{
  "Id": "LgAAAAA1FAByEUmaTYQkbPnJZf0nAQCHMBEb3yDTT6SNFC1A4Yk",
  "Path": "\\Agar-i-QuarantLine"
}
```

**ExternalAccess:** false

**Folder:**

```
{
  "Id": "LgAAAAA1FAByEUmaTYQkbPnJZf0nAQCHMBEb3yDTT6SNFC1A4Yk",
  "Path": "\\Inbox"
}
```

**Id:** 1b903b61-2b94-4c63-b25d-08d4ae88f37f

**InternalLogonType:** 0

**LogonType:** 0

**LogonUserSid:** S-1-5-21-1927014365-4043437681-3430716724-8054944

**MailboxGuid:** a7a93b57-6f8b-4f68-9198-099a5b02c0d6

**MailboxOwnerSid:** S-1-5-21-1927014365-4043437681-3430716724-8054944

**MailboxOwnerUPN:** plorenc@saintmetrics.com

**Operation:** Move

**OrganizationId:** d5ed11db-58a1-4ca8-84f6-2af550d9862e

**OrganizationName:** saintmetrics.com.onmicrosoft.com

**OriginatingServer:** DM5PR16MB1372 (15.01.1157.000)

**RecordType:** 3

**ResultStatus:** Succeeded

**UserId:** plorenc@saintmetrics.com

**UserKey:** 10037FF9880A17D

**UserType:** 0

**Version:** 1

**Workload:** Exchange

Close

Audit log details: more details

Here are some good references for auditing Office 365 inboxes using PowerShell commands:

<http://techgenix.com/using-powershell-simplify-mailbox-auditing-part1/>

<http://techgenix.com/using-powershell-simplify-mailbox-auditing-part2/>

<http://techgenix.com/using-powershell-simplify-mailbox-auditing-part3/>

## Wrapping Up

Among the actions you can take at this point are to view a report on enforcement (see " Reporting on API Enforcement" on page 95) and making sure enforcement is working on a Sensor (see " Enforcement Sensor Status" on page 94).

As you create policies with an enforce action, you can expand the conditions to include a wider range of matching emails.

You can also expand who is notified (additional recipients and/or the original recipients).

# Configure Enforcement: Microsoft Exchange

This topic describes how to configure enforcement for Microsoft Exchange versions 2010, 2013, and 2016.

The general procedure is as follows:

Step 1: Upgrade your sensor to the latest version.

Step 2: Configure Exchange enforcement.

Step 3: Enable enforcement in Advanced Phishing Protection

Step 1: Upgrade Your Sensor

Your sensor must be upgraded to the latest version in order to perform enforcement.

You can upgrade your sensor in Advanced Phishing Protection or at the command line.

Upgrade the Sensor in Advanced Phishing Protection

1. Go to Manage > Sensors.

Any active sensor that is not running the most recent version will display an upgrade link.

2. Click Upgrade Now.
3. Select the version with the most recent date. Versions are configured as YYYY.MM.DDHHMMSS, where YYYY is the year, MM is the month, DD is the day, and HHMMSSS is the time of the released version.

Upgrade the Sensor From the Command Line

1. ssh into the sensor machine.
2. Enter the command:

```
sudo /opt/agari/bin/agari-ep update
```

Step 2: Configure Exchange Enforcement

1. Sign in to Active Directory.
2. Create a new user.
3. Enter/select the user details:
  - Full name: ciscoEWS
  - User logon name: ciscoews



- Select the Password never expires check box and note the password that you enter.

The screenshot shows a web-based form titled "New Object - User". At the top, it says "Create in: [redacted]/Users". Below this are several input fields: "First name:" (empty), "Initials:" (empty), "Last name:" (empty), "Full name:" (CiscoEWS), "User logon name:" (ciscoews), and "User logon name (pre-Windows 2000):" (ciscoews). There are also buttons for "< Back", "Next >", and "Cancel".

This screenshot shows the password configuration section of the "New Object - User" form. It includes two password input fields, both filled with dots. Below the fields are four checkboxes: "User must change password at next logon" (unchecked), "User cannot change password" (unchecked), "Password never expires" (checked), and "Account is disabled" (unchecked). Navigation buttons "< Back", "Next >", and "Cancel" are at the bottom.

4. Grant Exchange impersonation rights:
5. In the Exchange Management Shell (Powershell), run the command  

```
New-ManagementRoleAssignment -Name " Cisco Sensor EWS" -Role " ApplicationImpersonation" -User " ciscoews"
```

(This command is all one line. If you copy and paste, make sure no extraneous characters are added accidentally.)

6. Configure the Exchange Web Services virtual directory Basic Authentication:
  - Exchange 2010
    1. Open IIS 7.
    2. Expand Sites > Default Web Site.
    3. Select Exchange Web Services.
    4. Click Authentication.
    5. Make sure Basic Authentication is Enabled.
  - Exchange 2013/2016
    1. Go to Servers > Virtual Directories.
    2. Edit Exchange Web Services (Default Web Site).
    3. Click the Authentication tab.
    4. Make sure Basic Authentication is Enabled.
7. Ensure the DNS value is correct for autodiscover. It should be: Autodiscover.domain.tld
8. SSH into the sensor.
9. Run the command

```
sudo /opt/agari/bin/configure-ews-enforcement
```
10. Enter the password established when the sensor was first installed and booted.
11. Use the service account you created at the beginning of the procedure. The username must be in the format domain\user (netbios\serviceAccount).
12. Test enforcement.
  - Run the command

```
sudo /opt/agari/bin/agari-ep test-api-creds user@email.address
```

    - user@email.address should be a valid user, not the service account above.
    - It may take up to 10 minutes for this test to complete successfully.

### Step 3: Enable Enforcement in Advanced Phishing Protection

1. In Advanced Phishing Protection, go to Manage > Organization.
2. Click the organization name.
3. In the Enforcement Settings section, move the Enforcement switch to Enable.
4. Click Save.

## Enforcement Sensor Status

When enforcement has been enabled for a sensor, the enforcement status is listed on the Manage > Sensors page for that sensor:

Status: ✔ Receiving Messages and sending data to Cisco  
✔ Enforcement enabled

### Successful enforcement status for the sensor

The combination of these 2 states are reflected in the tab for the sensor.

Advanced Phishing Protection may report the status " Errors with enforcement actions:"

Status: ✔ Receiving Messages and sending data to Cisco  
● Errors with Enforcement actions

### Enforcement status errors

The " Errors with Enforcement actions" state is defined as:

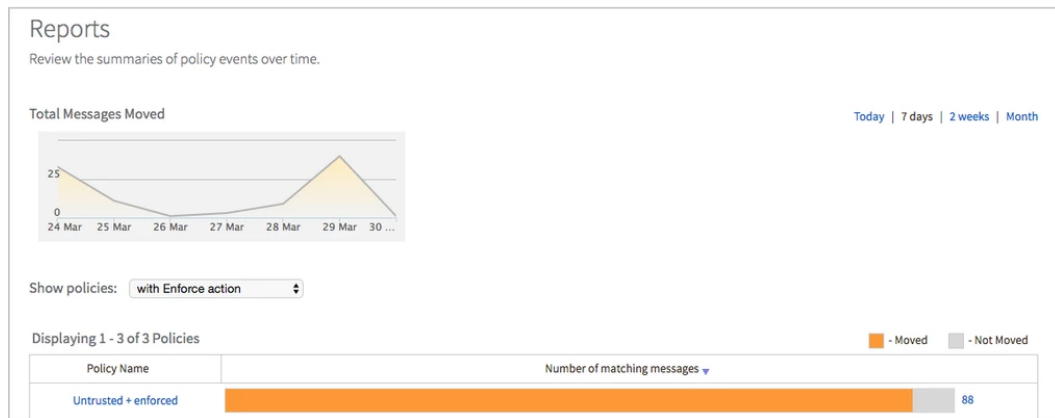
Fewer than 80 out of the last 100 messages could be enforced

This state may be shown in the very beginning stages as you are testing enforcement.

## Reporting on API Enforcement

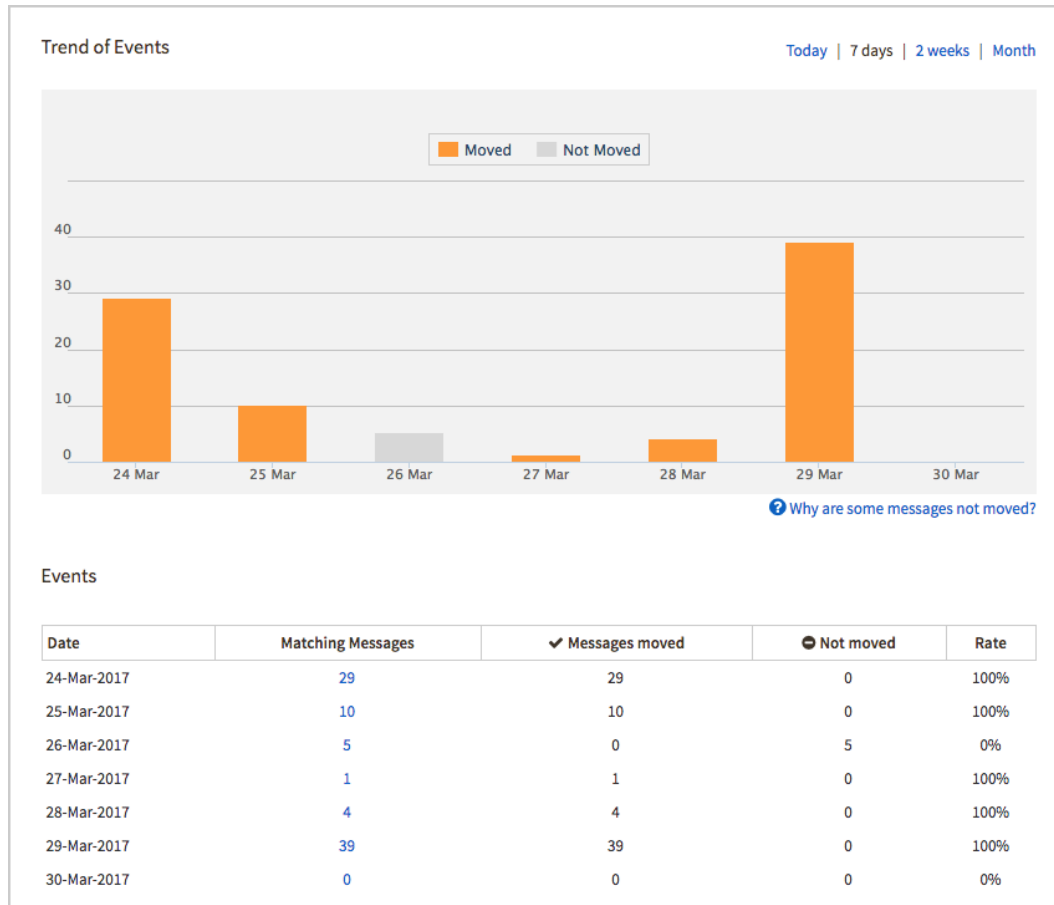
Go to the Reports page (Manage > Reports) and select with Enforce action from the Show policies list to view a summary of the moved and not moved messages for all policies with the Enforce action.

Note the horizontal bar chart will show orange for messages that have been moved because of API Enforcement.



The Reports index page

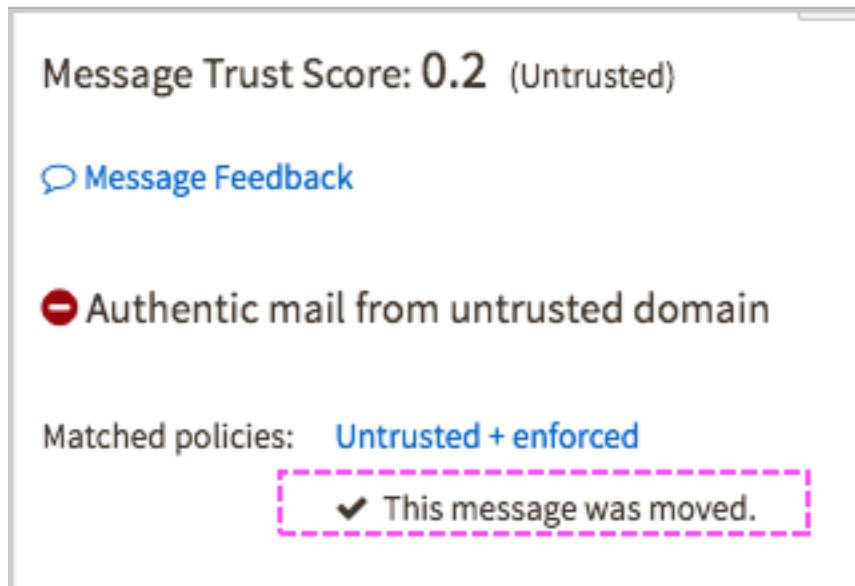
Clicking the horizontal bar chart will show a trend of that policy (with an enforce action) over time:



Reports details page

You can click links in the matching messages column to see search results of messages which matched the policy and were successfully moved.

A messages moved status is also shown on the message details view:



Message moved status on message details

## Why are some messages not moved?

Messages can be shown as "not moved" for 2 reasons:

- A policy has no enforcement action defined.
- The message could not be moved by the API. This can happen if a user has deleted the message from the Inbox before the API call is made or the user account has been deleted or locked.

For each sensor, enforcement actions are logged to the `/var/log/agari/enforcer.log*` files.



## CHAPTER 6

# Using Advanced Phishing Protection

Once you get Advanced Phishing Protection fully configured, you'll use it to monitor your email traffic and identify any issues with that traffic.

## The Workflow

Use the Overview page to find problem senders and messages. Clicking on the various attack classifications on the left side helps with your investigation.

Investigate senders via the IP Addresses and Domains pages, switching between them to identify suspicious senders and the messages they've sent. You may need to apply tags to some internal and partner domains as necessary (see Tagging Domains below). You'll notice that all of the Analyze pages eventually lead to Search Message results though there are multiple paths to get there.

Search for and/or view suspicious messages and:

- Review the scoring
- Use the link from the Message Details page to create a policy
- Send feedback for specific messages
- View the message in the main window and link directly to it

## Manage Suspicious Messages

Once you have identified some suspicious senders and messages, you'll want to create Policies (Manage > Policies) to actually act on the messages.

Tip: When viewing a message in the Message Details page you can use the bell icon to create a Policy; when viewing the message search results, you can click the "Create a Policy" link to do the same.

You can use policies to send notifications when a suspicious message arrives or even move the message to a different mailbox/folder (when enforcement is enabled).

For more information about creating policies, see "Policies" on page 119.

## Analyze Incoming Email Traffic

Cisco Advanced Phishing Protection provides insight into your organization's incoming email traffic, insight that includes where email messages are coming from (IP, Domain) and the risk associated with those messages and their senders.

The overview page is a unique visualization of Risk Overview of your organization's inbound email traffic. Every inbound message received by the Advanced Phishing Protection Sensor receives a Trust Score and is plotted in terms of:

- **Message Authenticity** – is the message really from who it claims to be from?
- **Domain Reputation** – is this domain reputable, that is, someone with whom I have a credible business relationship?
- **Sender Legitimacy** – is the sender IP address, evaluated by SenderBase Reputation Score (SBRS), legitimate?

## Trust Score

A Trust Score is calculated for every inbound message delivered to an organization's users. It answers the basic question: How much should I trust this message? The Trust Score is used to separate the email into three groups: Untrusted, Suspicious, and Trusted. Messages are scored on a scale from 0 – 10, where 0 is the lowest trust and 10 is the highest.

The Trust Score takes into account the Domain Reputation score, the Authenticity score of the message, and per-message features.

The body of the message is not a factor in the Trust Score. The exception to this is if you have URI analysis enabled (see "Enable Attachment and URL Analysis" on page 150), in which case URIs extracted from message bodies are scored for potential maliciousness.

- High Authenticity score from a sender with a low Domain Reputation score = suspicious
- High Authenticity score from a sender with a high Domain Reputation score = trusted
- Low Authenticity score from a sender with a high Domain Reputation score = suspicious, especially if a domain does Authentication correctly and frequently
- Low Authenticity score from a sender with a low Domain Reputation score = usually bulk email, zero-day domains, or cousin (look-alike) domains

Each circle in the Overview page represents a sending domain and the circles are sized based on the relative amount of traffic they sent within the selected time period. Reputable, high-volume, good messages are represented by green circles in the upper right. You should see the names of familiar senders in this quadrant. The top 200 domains are shown in each quadrant. Hover over a circle to see the number of messages from that sending domain.

Less trustworthy senders are lower and to the left.

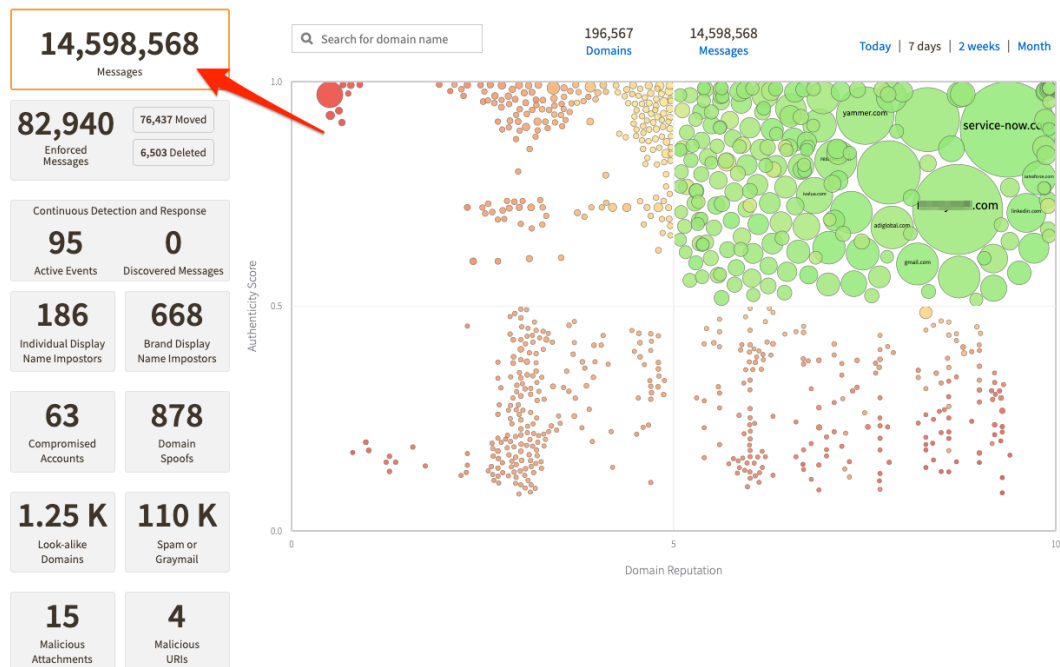
## Using Advanced Phishing Protection



### Quadrants on the overview page

You can filter the results, limiting them to just one of the basic attack types by clicking on any of the smaller boxes to the left of the quadrants display. Use this feature to quickly identify potential problem messages and senders.

To return to the original traffic view, click the Messages filter.

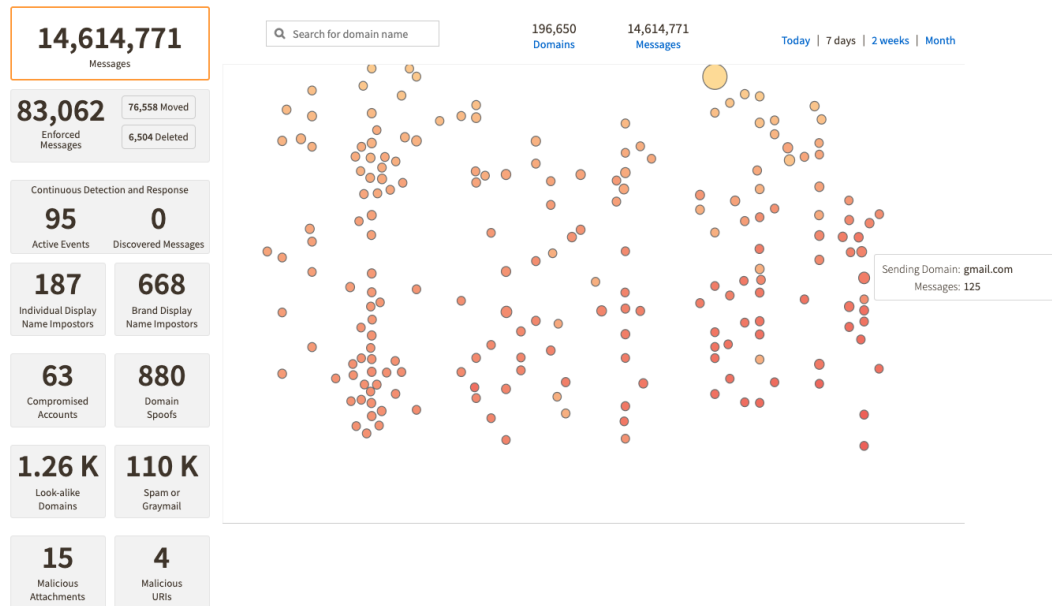


### The Messages filter



## Zooming In

Click on the empty space inside one of the quadrants to zoom in on that quadrant. It should be easier to see the bad senders. Hover over a circle to see the sending domain. For example:



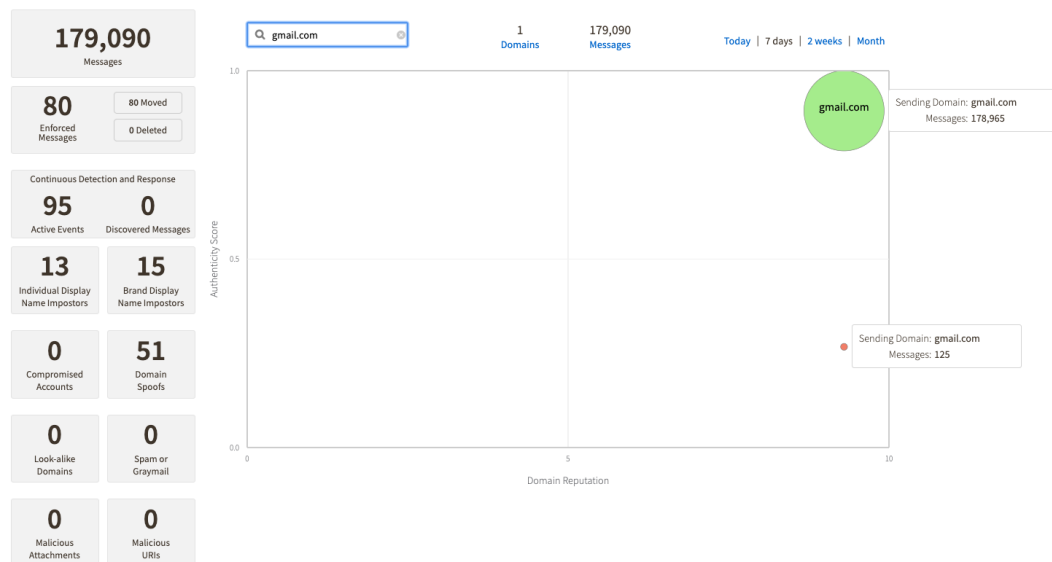
A zoomed-in quadrant

Click on the empty space again to zoom back out.

## Quick Domain Search

You can also use the search box on the main visualization page to quickly classify the authenticity of the mail you receive from a specific domain.

For example, type "gmail.com" into the search box. You may see a pattern that looks like this:



Searching for mail from the domain gmail.com

This says that Advanced Phishing Protection has analyzed 161,016 legitimate messages from the gmail.com domain in the past 7 days; hovering over the smaller circle shows that 818 messages may warrant further investigation because they have a lower authenticity score.

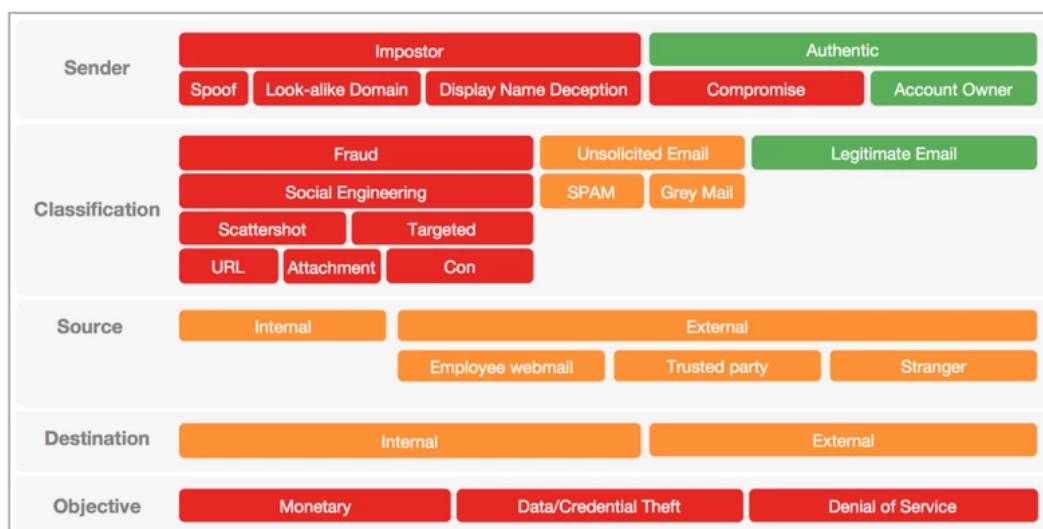
Clear the search box to return to the original view.

## Attack Classifications

This topic describes the different types of email attacks.

## Attack Taxonomy

Messages that are untrusted, per the Message Trust Score, are classified by Advanced Phishing Protection into one or more of the attack taxonomy classes seen in the figure below.



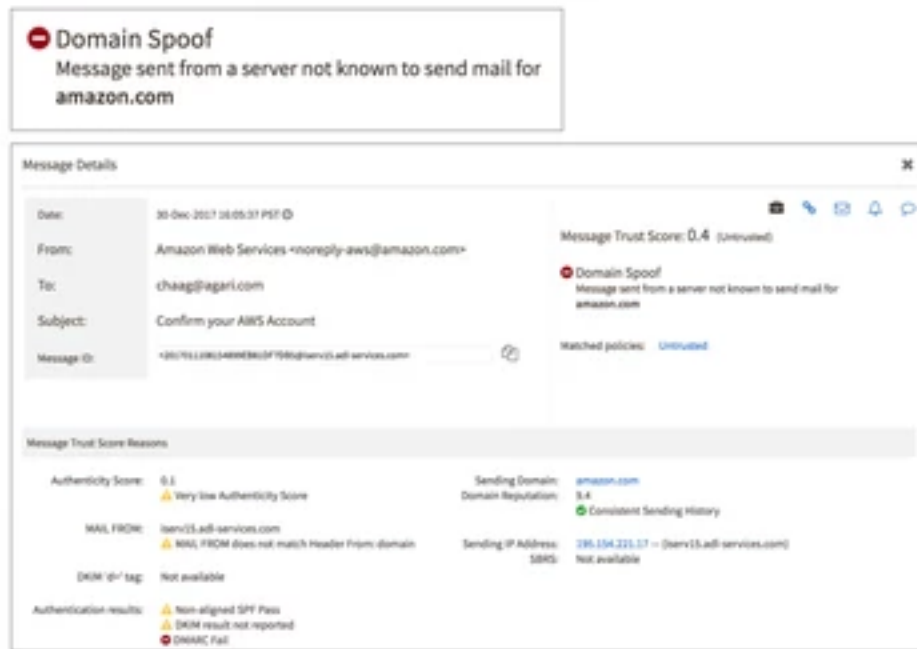
The Attack classification taxonomy

The attack classifications will be seen in the Message Details view and can be used for search and policy.

The taxonomy attack classifications are described in more detail below.

## Domain Spoof

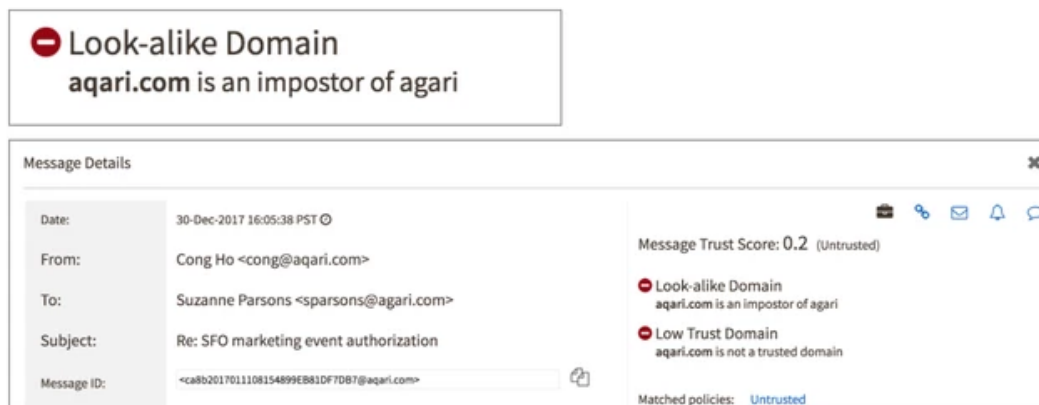
A Domain Spoof is a message that purports to be sent by a high reputation domain, but Advanced Phishing Protection has detected it is not coming from an authentic sending source for that domain.



Domain Spoof example

## Look-alike Domains

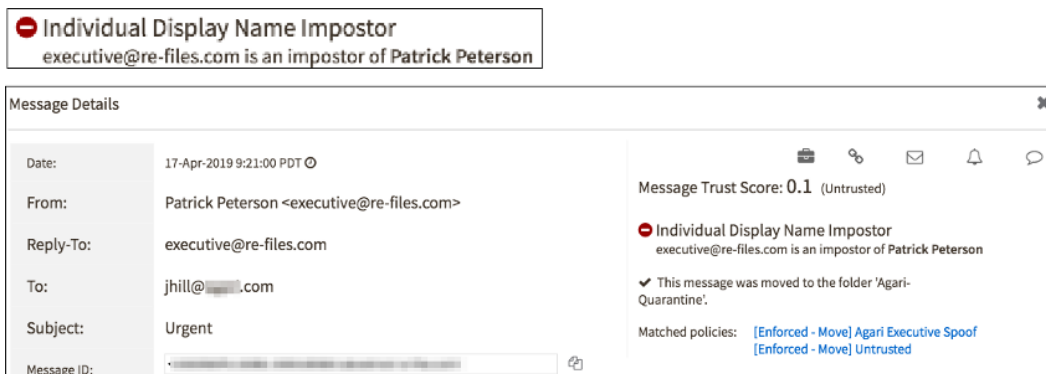
A Look-alike Domain attack is when a domain attempts to look like a highly trusted and well known domain, like one of your internal or partner domains.



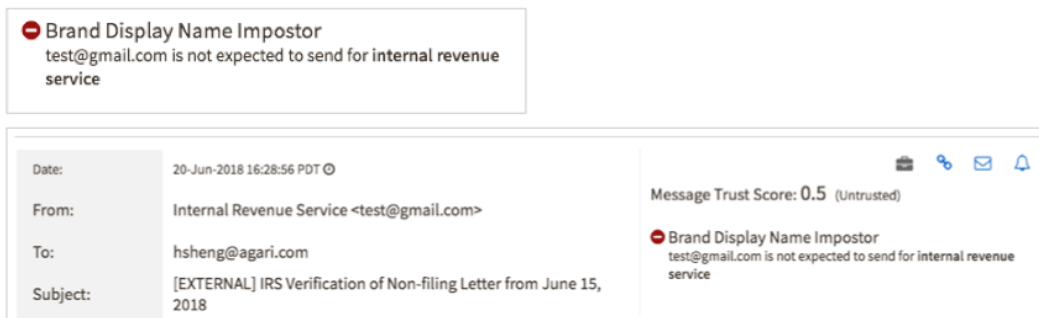
Look-alike domain example

## Display Name Impostor

A Display Name Impostor is when the display name portion of the From field is changed to look like a well known brand or a different individual. Display name deception is frequently used along with other attack types like Look-alike Domains or Compromised Accounts. In Advanced Phishing Protection, Display Name Impostors are split two classes: Individual Display Name Impostors and Brand Display Name Impostors.



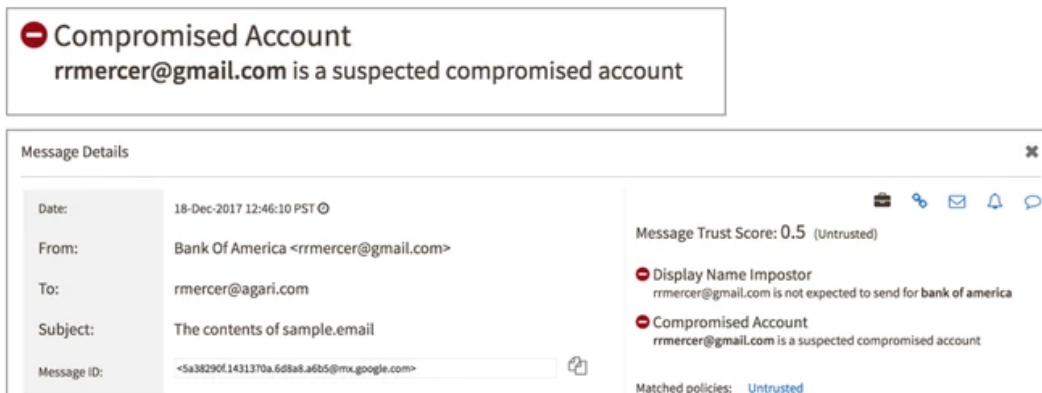
Individual Display Name impostor example



Brand Display Name impostor example

## Compromised Account (Account Take Over)

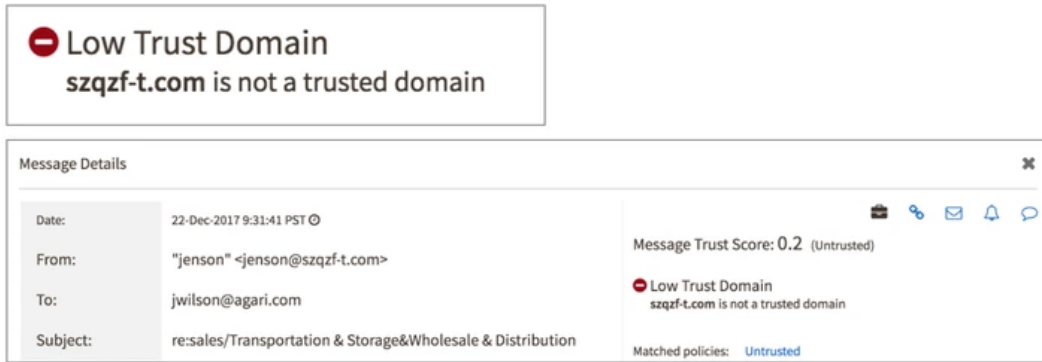
A Compromised Account is an account that belongs to a real person/user but has been taken over by a bad actor and used for malicious purposes. When Advanced Phishing Protection finds indicators of account take over we will classify it as a message from a Compromised Account.



Compromised account example

## Low Trust Domains

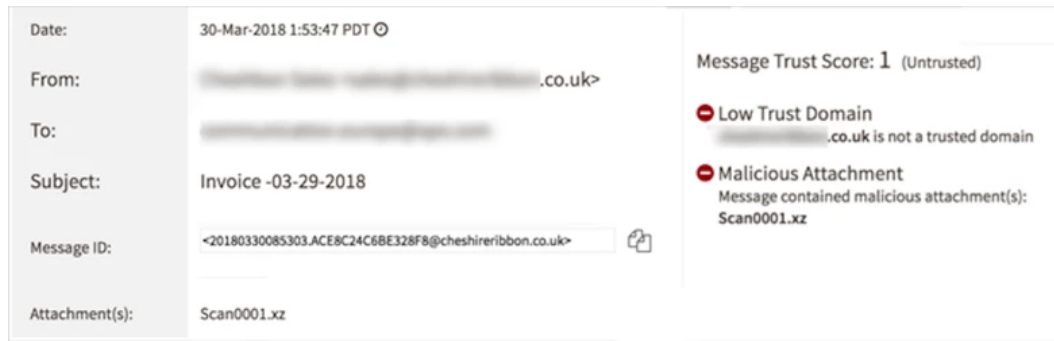
In addition to the previously mentioned sender classifications, Advanced Phishing Protection will also classify messages that simply come from a Low Trust Domain. Many messages that fit the taxonomy classifications of Fraud and Unsolicited Email (Spam and Greymail) come from domains that should not be trusted, regardless of the sender classifications.



Low trust domain example

## Malicious Attachment

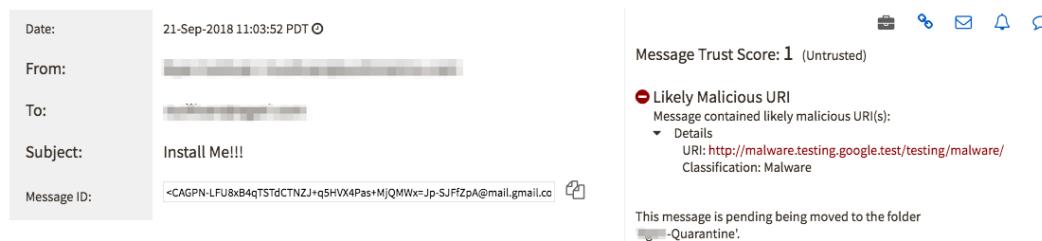
If attachment scanning is enabled, Advanced Phishing Protection will tell you when an attachment is likely to be malicious.



Malicious attachment example

## Likely Malicious URI

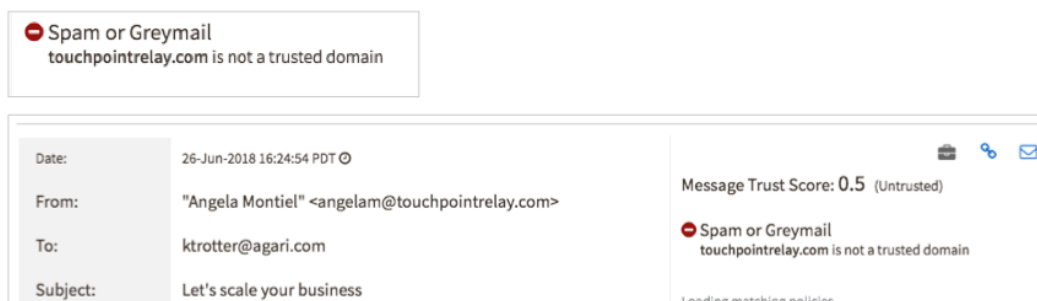
If URI scanning is enabled, Advanced Phishing Protection will tell you when a URI is found in the body of a message that is likely to be malicious.



Malicious URI example

## Spam or Graymail

In addition to the sender classifications that identify malicious messages, Advanced Phishing Protection also classifies messages that are not necessarily malicious, but represent unwanted or unsolicited email. Messages that fit the Spam or Graymail class should not be trusted, regardless of the other sender classifications.



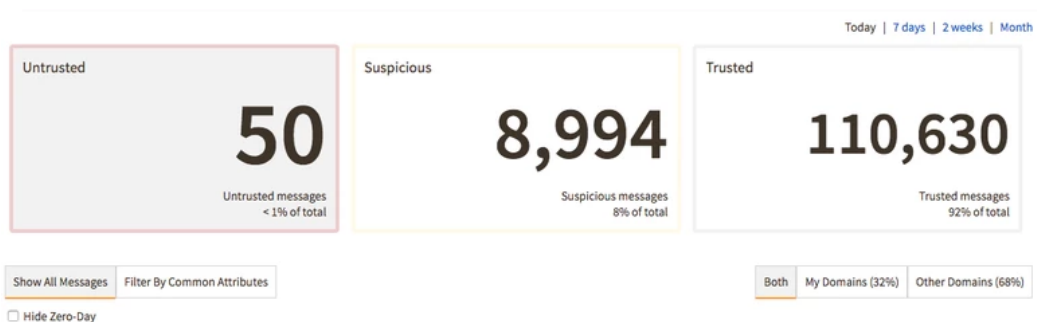
Spam or Greymail example

## Messages

The messages analyzed by Cisco Advanced Phishing Protection and the data and threat analysis about those messages can be viewed in several ways. In addition to the real-time dashboard view (Analyze > Dashboard, Real time tab), two other useful view are the messages list (Analyze > Messages) and the message search (Analyze > Search Messages).

## View Messages

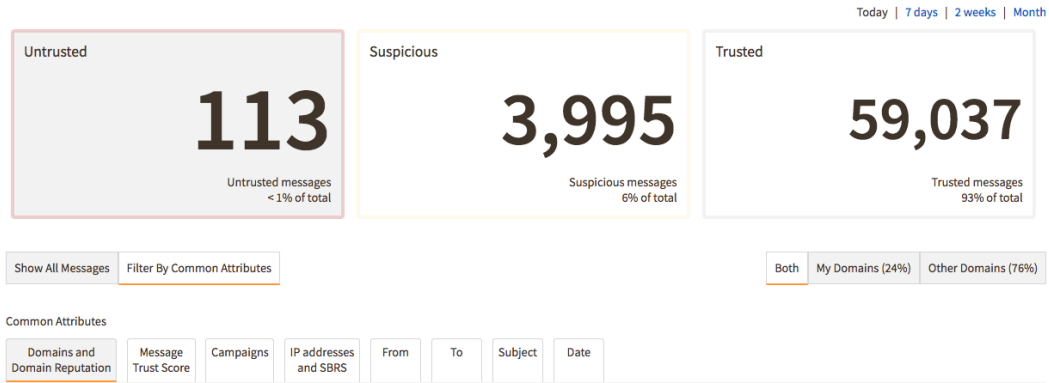
Whereas the Overview page provides an interactive visualization of spoofs, name imposters, look-alike domains, and good messages, the Analyze > Messages page provides more of an operational view to help you explore your data.



The messages page summary counts

Messages are split into three categories: Untrusted, Suspicious, and Trusted. You can click on a box to select that category.

To drill down further, click Filter by Common Attributes:



**Domains and Domain Reputation Score**  
Domains identified in this category and their domain reputation.

### Filtering by common attribute

The default view sorts the Untrusted messages by Domain. You can also click other tabs to sort to visualize:

- **Message Trust Score** – What is the distribution of these Untrusted messages by Trust Score?
- **Campaigns** – How many of these Untrusted messages are from one sender with the same Subject?
- **IP Address/SBRS** – Of all the messages scored as Untrusted, which are the top sending IP addresses for those messages, and what are the reputation scores of those IPs?
- **From / To / Subject / Date** – Who are my riskiest Senders? Who are my riskiest Receivers? Was I attacked on a particular day?

## View Message Details

You will often want to view the details of messages sent by untrustworthy senders, which are represented by the red circles.

1. Click one of the red circles to view a list of the messages sent by that sender. The messages from that sender are displayed in the search messages results. You can filter to further limit the list.
2. Click a message to view the Message Details.

Message Details

Date: 13-Feb-2020 18:02:49 PST

From: Wells Fargo <superian.jenkins@yahoo.com>

To: [redacted]@cisco.com

Subject: Account Problem

Message ID: <2017011108154899e[redacted]@iserv15.adl-services.com>

Message Trust Score: 0.5 (Untrusted)

Domain Spoof  
Message sent from a server not known to send mail for yahoo.com

Brand Display Name Impostor  
superian.jenkins@yahoo.com is not expected to send for wells fargo

Matched policies: [\[QUAR\] Untrusted Messages](#)  
[Brand Display Name Impostors](#)

Message Trust Score Reasons

|                                                                                         |                                                                                                                  |
|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Authenticity Score: 0.1<br>⚠ Very low Authenticity Score                                | Sending Domain: <a href="#">yahoo.com</a><br>Domain Reputation: 8.9<br>✔ Frequent, High Volume Sender            |
| MAIL FROM: iserv15.adl-services.com<br>⚠ MAIL FROM does not match Header From: domain   | Sending IP Address: <a href="#">195.154.221.17</a> — (195-154-221-17.rev.poneytelecom.eu)<br>SBRS: Not available |
| DKIM 'd=' tag: Not available                                                            |                                                                                                                  |
| Authentication results: ⚠ Non-aligned SPF Pass<br>⚠ DKIM result not reported<br>Unknown |                                                                                                                  |

[Search for similar messages](#)

OK

### Message Details pane

The Message Details page shows information about the message including:

- Headers and scoring (and the reasons for the scores received)
- Directionality of the message (Inbound, Outbound, or Internal) if All messages is selected for the Evaluate Messages setting in your organization, see "Evaluate Messages" on page 164)
- Which policies, if any, the message matched (each policy is a link to the specific policy event)
- Whether the message was enforced (if you have enforcement enabled)

Internal and outbound messages do not show the Message Trust Score Reasons section.

Remember that Advanced Phishing Protection does not track the body of the message.

However, it is often more useful to follow the cross links for Sending Domain and Sending IP Address.

- The Sending Domain link will answer the question: How often is this domain sending email into my organization, and from how many IP addresses? Are most of the messages legitimate?
- The Sending IP Address link will answer the question: For what other domains does this IP address send email to my organization? Is the IP reputable? Does it send for a few domains or many?

In the upper right of the Message Details page, you can click the:

- Message Details link icon (🔍) to view of the message details in the main window (with a URL that will link directly to this view).
- Headers icon (📄) to view all of the headers in the message.
- Mail icon (✉) so send the message details view to a colleague.



- Bell icon (🔔) to create a policy with conditions that match this message. See "Create a Policy" on page 121 for more on creating policies.
- Message Feedback icon (👍) to provide feedback about a message's scoring. See "Send Message Feedback" below for details.

## Send Message to Phishing Response

If you also have a subscription to Phishing Response, you can send a message that you're viewing in Advanced Phishing Protection to Phishing Response so that it can be investigated further by Phishing Response and by your security team. When you have Phishing Response and when you view message details (see "View Message Details" on page 107), you will get an additional icon in the upper left of the message:



The Send to Cisco Phishing Response button in the top-right of a message details page.

1. View an individual message. See "View Message Details" on page 107 for information.
2. Click the Send to Cisco Phishing Response button (⚠️) in the upper right corner.
3. Click Send.

One of two things will happen:

- If this message is determined to be related to a current open investigation in Phishing Response, this message will be added to that investigation and that investigation's analysis and triage.
- If this message is determined to not be related to an existing open investigation in Phishing Response, a new investigation will be opened that will include this message, and automatic analysis and triage in Phishing Response will be initiated on the investigation.

## Send Message Feedback

A great way to improve how well Advanced Phishing Protection identifies your email correctly is to provide feedback on individual messages. This is not entirely unlike telling your email provider or client software "This is spam" for a message in your Inbox, but in the Advanced Phishing Protection case, you can provide much more specific detail about message threats.

1. View the details of a message by clicking on the message in any view with a list of messages, including on the analyze messages page (Analyze > Messages, on the Show All Messages tab) or the Search Messages page (Analyze > Search Messages).
2. In the upper-right corner of the Message Details dialog box, click the Message Feedback icon (👍).  
In the Provide Feedback dialog box, based on the Message Trust Score, the message will already be categorized as Legitimate or an Attack.





Similarly, if you go to the Analyze > Messages page, click on Suspicious messages, click a common attribute, such as From, and then click a number in the list, you'll go to the message search results page you'll see a list of all messages from that address, between the time period specified, and in the Trust Score range for suspicious messages.

These shortcuts come in very handy, but so does the ability to find tune search results, either when you start from scratch or from any of the many shortcuts.

When a search has been run, fields that were used for the search are outlined in orange.

This topic explains all of the fields on the Search Messages page.

| Search Field                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| From, To, Reply-To, Subject | <p>These are all collected from the respective fields in message headers when messages are ingested by Advanced Phishing Protection. Enter all or part of any email address or subject line. The search for these fields is partial matching, case insensitive. For example, if you enter "pens" in the Subject field, messages with subjects such as "Shop My Etsy Pens Store," "That's too expensive for me," and "Please buy some pens from Amazon" will all be found.</p> <p><input type="checkbox"/> Limited to 100 characters.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Attachment                  | <p>This field is available only when attachment scanning is enabled in organization settings (see "Organization Settings" on page 163), and has 5 options:</p> <ul style="list-style-type: none"> <li>• has any attachment - Finds any messages with any attachment.</li> <li>• has a likely malicious attachment - Finds any messages with at least one attachment that Advanced Phishing Protection has determined to be likely malicious.</li> <li>• has attachment name - Finds messages with attachment file names that contain all or part of what is entered in this field. Like with other text search fields, this is partial matching, case insensitive.</li> <li>• has attachment filename extension - Finds messages with attachment file names that have any of the entered extensions. File name extensions are the part of a file name that follows the rightmost period. Enter one or more extensions, separated by commas. Like with other text search fields, this is partial matching, case insensitive. For example, if you enter PROP, it will find a file named system.properties.</li> <li>• has an attachment hash of - Finds messages that match the entered hash. A hash is produced by a cryptographic algorithm to uniquely identify the contents of a file. If any changes are made to a file, the hash produced for that file changes, usually significantly, so it is easy to determine if a file has changed if you compare the original and current hashes. This is a full, case-sensitive match.</li> </ul> <p><input type="checkbox"/> Limited to 100 characters.</p> |
| Received between            | This defines the start and end dates, inclusive, of the search.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Search Field             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          | <ul style="list-style-type: none"> <li>The start date can be no earlier than 60 days prior to the current date. (Advanced Phishing Protection purges message data older than 60 days.)</li> <li>The end date can be no later than the current date.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Trust Score Range        | This defines the upper and lower bounds of the Trust Score of messages that will be found in a search, including the values you select. Drag the lower and upper bound sliders to change the range.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Authenticity Score Range | This defines the upper and lower bounds of the Authenticity Score of messages that will be found in a search, including the values you select. Drag the lower and upper bound sliders to change the range.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Matched Policy           | This defines a single policy that a message must have been enforced on to be found in a search. The list of policies that you can choose from includes all policies in Advanced Phishing Protection: enabled (and active), disabled, and on-demand policies (see "On-demand Policies" on page 130).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Enforcement              | <p>This defines whether a message has been enforced by any policy, and how. Select one option from:</p> <ul style="list-style-type: none"> <li>All Messages (default) - Messages that were enforced in any way.</li> <li>Pending - Messages that match a policy where enforcement is defined but the enforcement has not happened yet.</li> <li>Enforced - Messages that have been enforced by policy. Sub-categories of enforcement can also be selected: <ul style="list-style-type: none"> <li>Moved (to any folder)</li> <li>Moved to Inbox</li> <li>Deleted</li> </ul> </li> <li>Not Enforced - Messages that matched a policy with an enforcement action but were not enforced by the policy. (This option is useful for determining what messages match a policy to see if the policy catches what it is supposed to before enabling any sort of enforcement that would more or delete messages or for discovering when policy enforcement is failing.)</li> </ul> |
| Message ID               | <p>Enter a single message ID in this field to search for a specific message in Advanced Phishing Protection that matches the message ID.</p> <div style="border: 1px solid black; padding: 2px;"> <input type="checkbox"/> Limited to 100 characters. </div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Direction                | <p>This defines the directionality of a message. Click in the field to select one or more directions, from:</p> <ul style="list-style-type: none"> <li>Inbound - Messages that were sent into your organization from somewhere outside your organization. In the Direction column, inbound message are indicated with a  icon.</li> <li>Outbound - Messages that were sent from within your organization to somewhere outside your organization. In the Direction column, inbound message are indicated with a  icon.</li> </ul>                                                                                                                                                                                                                                                                |

| Search Field            | Description                                                                                                                                                                                                                      |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                         | <ul style="list-style-type: none"> <li>Internal - Messages that started and ended within your organization. In the Direction column, inbound message are indicated with a "i" icon.</li> </ul>                                   |
| Attack Type             | Click in the field to select one or more attack types. Messages that match any of the selected attack types will be found in a search.                                                                                           |
| Domain Reputation Range | This defines the upper and lower bounds of the Domain Reputation range of messages that will be found in a search, including the values you select. Drag the lower and upper bound sliders to change the range.                  |
| Sending Domain          | Enter one or more sender domains, separated by commas. Messages that match any of the domains will be found in a search.<br><input type="checkbox"/> Limited to 100 characters.                                                  |
| Domain Tags             | Click in the field to select one or more domain tags. Messages that match any of the selected domain tags will be found in a search.                                                                                             |
| Hostname                | Enter a single PTR hostname to an IP address. Messages that contain the hostname will be found in a search.<br><input type="checkbox"/> Limited to 100 characters.                                                               |
| SBRS Range              | This defines the upper and lower bounds of the SenderBase Reputation Score (SBRS) range of messages that will be found in a search, including the values you select. Drag the lower and upper bound sliders to change the range. |
| IP Address              | Enter a single IP addresses or CDR. Messages that contain the IP address will be found in a search.<br><input type="checkbox"/> Limited to 100 characters.                                                                       |

## Search Messages

Use the Search Messages page to search and filter your incoming mail. You can go directly to the Analyze > Search Messages page via the menu or by clicking on the number of messages in the Domains detail or IP Address details pages.

1. Go to Analyze > Search Messages.
2. Enter the search criteria. See "Message Search" on page 110 for details on each search field.
3. Click Search.

## Download Message Search Results

Whenever you are on the Search Results page, you can download information about the list of messages that match the current search filters.

The downloaded file will contain information about up to 10,000 messages. If more than 10,000 messages are in the search results, the downloaded file will contain the first 10,000, determined by the display order, which you can change by clicking the top of any column in the search results table.

1. Go to Analyze > Search Messages. (You can also get to the message Search Results page in many other ways. For example, if you're on the dashboard, click a threat type, and then click Show messages, you'll be taken to the Search Message page with the threat type already defined as a filter.)
2. Define the filters for the messages you want to see in the list.
3. Click Search.
4. Click Download Results.
5. Click Download CSV.

A file named message export.csv is downloaded automatically to the default location that you have set in your browser for downloaded files. The file will contain the following information from/about each message, if available:

- Date
- From
- Reply-to/Forwarded From
- To
- Subject
- Message-ID
- Message Trust Score\*
- Sending Domain
- Domain Reputation\*
- Sending IP Address
- PTR Name
- SBRS (SenderBase Reputation Score)

\* Calculated by Advanced Phishing Protection.

## Domains and IP Addresses

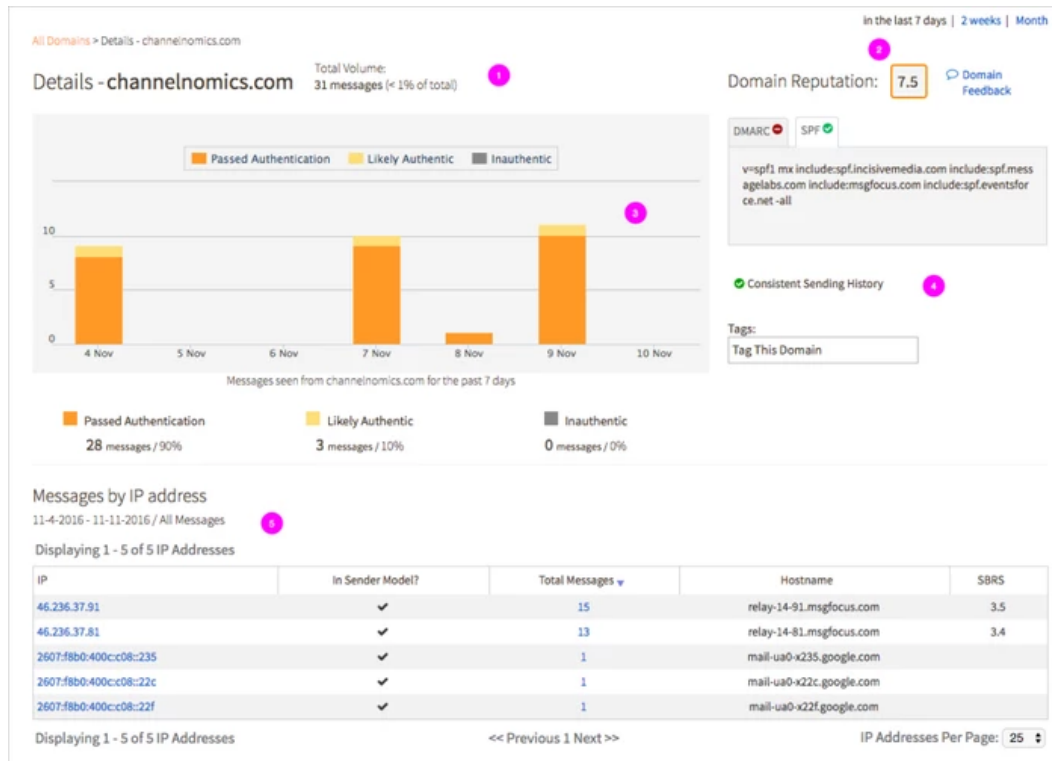
From the Analyze menu you can view lists of sending domains and IP addresses (Analyze > Domains and Analyze > IP Addresses). The pages function similarly and you will switch between them as you investigate incoming traffic. When you click an IP address or domain in the list, you can see the Details page for that item. For IP addresses, the Details page shows information about that IP, including a list of domains sending to your organization from the IP address and a link to the messages sent by each domain. For domains, the Details page shows you the information for that domain including a list of IP addresses sending to your organization from that domain and the messages sent.

Moving between viewing IPs addresses and domains and the associated messages from each is a powerful way to drill down into the details and analyze incoming traffic.

## View Domain Details

The domain-to-IP address relationships are a key component of the sender modeling features of Advanced Phishing Protection, and the Domain Details page displays much of the information about the sender model.

1. Go to Analyze > Domains.
2. Click a domain name.



The Domain Details page

The Domain Details page shows the following information.

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | The domain name, the domain's volume, and the percentage of overall volume of your inbound mail stream from that domain are listed at the top of the page.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 2 | The domain reputation (as scored by Advanced Phishing Protection) is listed in the upper right. The "Domain Feedback" link allows you to send feedback if you feel the domain has been incorrectly scored. Domain reputation is scored from 0.0 to 10.0, with 0.0 representing the lowest reputation and the 10.0 representing the most reputable.                                                                                                                                                                                                                                                                                                           |
| 3 | <p>The graph of message volume from the sending domain is in the middle of the page. Messages are categorized as: Passed Authentication, Inauthentic, or Likely Authentic.</p> <ul style="list-style-type: none"> <li>• Authentic messages are those that adhere to the authentication standards as published by the domain itself: SPF, DMARC, or DKIM.</li> <li>• Inauthentic messages are messages which fail authentication and are deemed not to be within sender model for that domain.</li> <li>• Likely authentic messages are messages which do not pass authentication but are deemed to be "likely authentic" from the sending domain.</li> </ul> |

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | <p>You can toggle the visibility of the Passed Authentic, Inauthentic, and Likely Authentic bars in the bar chart by clicking the key at the top of the chart. Similarly, the time range of the chart is controlled by the time range selector in the upper right of the page (7 days / 2 weeks / 30 days).</p> <p>You can select a specific day by clicking on one of the bars in the bar chart. To clear your selection, select "Clear" in the Messages by IP address table header.</p>                                                |
| 4 | <p>If applicable, the domain's DMARC and SPF records are presented here. Beneath that area, positive and negative factors affecting domain reputation are shown. For example, this screen shows that the domain has a "consistent sending history."</p>                                                                                                                                                                                                                                                                                  |
| 5 | <p>The "Messages by IP Address" catalogs each IP address which has sent for the domain during the time period.</p> <ul style="list-style-type: none"> <li>• Clicking an IP address will effectively pivot the view: instead of viewing all IPs for a given domain, you will instead be viewing all domains for which that single IP has sent messages.</li> <li>• Click the number in the "Total Messages" column of the Detail page to view the list of messages for that sender (IP or domain) in the Search Messages page.</li> </ul> |

## Domain Tags

Domains can be assigned tags. Tags are used to influence scoring, to analyze domain use, and to create policies. You can assign one or more tags from a defined list of tags to any domain tracked by your organization in Advanced Phishing Protection.

Two tags, internal and partner, are used in the message scoring process. In general, you want to give the:

- internal tag to domains you own, can control, and inherently trust the domain reputation
- partner tag to domains of external organizations with whom you exchange email, have established a trusted relationship, and trust their domain's reputation

Adding either the internal or partner tag to a domain increases that domain's reputation for properly authenticated messages.

You should avoid adding both the internal and partner tags to the same domain.

The other tags that are available for you to add to a domain can help with visualization on the Analyze > Overview page, with search results, and with policy creation.



**Domains**  
Domains that have sent mail to you.

Today | 7 days | 2 weeks | Month

Filter Options:

Filter By Tags:  Reputation Range:  0.0  10.0   Search:

Displaying 1 - 25 of 8,428 Receiver Domains

| Domain                             | Legitimate Senders |         | Unauthorized Senders |        | Reputation | SPF Record | DMARC Record | Tags                                         |
|------------------------------------|--------------------|---------|----------------------|--------|------------|------------|--------------|----------------------------------------------|
|                                    | Volume             | Auth %  | Volume               | Auth % |            |            |              |                                              |
| <a href="#">t.illustration.com</a> | 21,013             | 92.21%  | 24                   | 0.00%  | 8.5        | yes        | yes          | <input type="text" value="internal"/>        |
| <a href="#">c.illustration.com</a> | 16,968             | 98.76%  | 5                    | 0.00%  | 8.5        | yes        | yes          | <input type="text" value="internal"/>        |
| <a href="#">l.illustration.com</a> | 5,212              | 85.52%  | 41                   | 0.00%  | 8.1        | yes        | yes          | <input type="text" value="newsletter"/>      |
| <a href="#">i.illustration.com</a> | 4,424              | 98.60%  | 0                    | 0.00%  | 8.5        | yes        | no           | <input type="text" value="partner"/>         |
| <a href="#">f.illustration.com</a> | 3,755              | 100.00% | 0                    | 0.00%  | 8.5        | no         | yes          | <input type="text" value="internal"/>        |
| <a href="#">t.illustration.com</a> | 3,614              | 34.95%  | 4                    | 0.00%  | 8.5        | yes        | yes          | <input type="text" value="internal"/>        |
| <a href="#">t.illustration.com</a> | 2,992              | 81.80%  | 7                    | 0.00%  | 8.5        | yes        | no           | <input type="text" value="internal"/>        |
| <a href="#">i.illustration.com</a> | 2,437              | 100.00% | 0                    | 0.00%  | 8.1        | yes        | yes          | <input type="text" value="social"/>          |
| <a href="#">l.illustration.com</a> | 2,301              | 93.78%  | 0                    | 0.00%  | 8.1        | yes        | yes          | <input type="text" value="newsletter"/>      |
| <a href="#">c.illustration.com</a> | 1,053              | 99.91%  | 0                    | 0.00%  | 8.1        | error      | yes          | <input type="text" value="consumer"/>        |
| <a href="#">e.illustration.com</a> | 897                | 95.90%  | 0                    | 0.00%  | 8.5        | yes        | no           | <input type="text" value="partner"/>         |
| <a href="#">r.illustration.com</a> | 802                | 100.00% | 0                    | 0.00%  | 7.9        | yes        | yes          | <input type="text" value="consumer"/>        |
| <a href="#">t.illustration.com</a> | 801                | 100.00% | 0                    | 0.00%  | 8          | yes        | yes          | <input type="text" value="social"/>          |
| <a href="#">t.illustration.com</a> | 582                | 97.88%  | 4                    | 0.00%  | 8.1        | yes        | yes          | <input type="text" value="Tag This Domain"/> |

The domains index page

## Add a Tag to a Domain

1. Go to Analyze > Domains.
2. Click in the Tags field for any domain.
3. Select an unused tag.

The tag is added automatically.

You can also add a tag to a domain on the Domain Details page (Analyze > Domains, then click a domain name). The Tags field is on the right side.

## Delete a Tag from a Domain

1. Go to Analyze > Domains.
2. In the Tags field for a domain, click the x on the tag you want to delete from the domain.

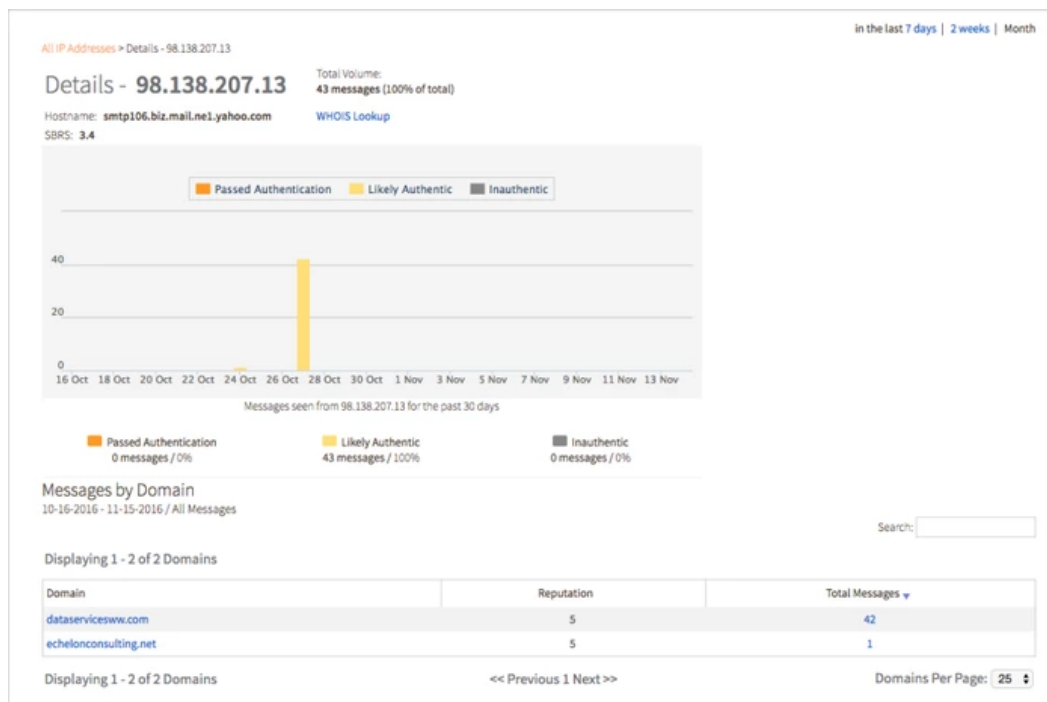
The tag is deleted immediately.

## View IP Address Details

Viewing the details for a given IP address can help confirm if the IP address is:

- Owned completely by the sending domain (sends for very few domains)
- A shared IP address (sends for many domains)

- A mail forwarder (sends for large numbers of domains)



The IP Details page

On the Domain Details page, you can see the hostname for the IP, the total message volume as seen by your organization from that IP for the given time period, and the SBRS (SenderBase Reputation Score) from Advanced Phishing Protection.

The page also contains a link for the WHOIS information for the given IP address.

Like the time series charts on the domain details page, you can change the time range and toggle the display of authentic, inauthentic, and likely authentic message counts.

In this example, the sending IP address 98.138.207.13 – which has the hostname of "smtp106.biz.mail.ne1.yahoo.com" has sent 42 messages into the organization: 42 messages for the domain "dataservicesww.com" and one message for "echelonconsulting.net."

Click the number in the "Total Messages" column of the Detail page to view the list of messages for that sender (IP or domain) in the Search Messages page.

## Notifications

Advanced Phishing Protection provides a notification system that can inform you about the occurrence of system events. These notifications are classified into categories:

- Sensor
- Host system
- Policies

The notifications you can enable depend on your system configuration. For example, if you use Google G Suite, one of the notifications that you can enable is The credentials supplied for G Suite stop authenticating correctly.

Select the check box for any notifications you want sent. Clear the check box for any notification you do not want sent. Click Save when you are finished.

Any notifications that you have selected will be sent to all email addresses in the Email Address list in the Notification section.

## Add a Notification Recipient

1. Go to Manage > Policies.
2. Click the System Notifications tab.
3. In the Notification section, enter an email address in the Additional Recipients field.
4. Click Add.
5. Click Save.

## Delete a Notification Recipient

1. Go to Manage > Policies.
2. Click the System Notifications tab.
3. In the Notification section, click the x next to a name in the Email Address list.
4. Click Save.

## Policies

Use policies to specify what happens when messages meeting certain criteria are received by your organization. For example, you could write a policy that finds all messages from a specific sending domain and notifies the recipient and an administrator. Or you could create a policy that moves suspicious messages to a quarantine folder (Enforcement customers only). The basic idea is to react to certain conditions (which you specify) in your incoming email traffic.

Possible actions include logging incoming messages for searching and reporting in the web UI (the default action), sending notifications (to the original recipients and/or designated admin users), moving the messages to a specific mail folder (Enforcement configuration only), or even deleting a message entirely (Enforcement configuration only).

The Policies page lists the existing policies. From this page you can create policies, subscribe to system notifications, and view the Event Log entries for policies. See "View Policy Results" on page 128 for more information about your policies. See "Default Policies" on the facing page for information about the policies that are predefined for you. See "Create a Test Policy" on page 127 to try policies for yourself.

## Default Policies

When an organization is initially created in Advanced Phishing Protection, a set of default, pre-configured policies is created automatically. These policies match the most common conditions that Cisco customers will catch with Advanced Phishing Protection, and they need to be enabled to start matching messages and to have notify and/or enforce actions defined for the policies. It is recommended that you enable the policies with no actions first. Start by just logging policy matches and monitoring results, then choose your notify and enforce actions.

This section describes the out-of-the-box configuration of the default policies.

This information can be useful if you have changed the configuration of any of these policies and need to return them to their default state.

Any settings not specifically defined in the table below have the following values:

- Direction: Inbound
- Text fields: empty
- Check boxes: unchecked
- Drop-down lists: no value selected
- Sliders with two handles: left handle at left end, right handle at right end (the When message count exceeds control has just one handle, and its default is 10)

| Policy Name                                 | Setting           | Value                              | Description                                                                                                                                                                                                                                                                             |
|---------------------------------------------|-------------------|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Brand Display Name Imposters                | Attack Types      | Brand Display Name Imposter        | Attack types include Brand DNI. To catch brand impostors where common brands are spoofed in the display name.                                                                                                                                                                           |
| C-Level Imposters                           | From              | C-Level Executives (address group) | Matches a Display Name in the address group C-Level Executives. To catch BEC attacks/ impostors of your CEO, CFO, and other top executives. Note that this policy requires you populate the C-Level Executives address group, which is also created for you as a default address group. |
| Executive Imposters                         | From              | Executives (address group)         | Matches a Display Name in the address group Executives. To catch BEC attacks/ impostors of other executives in your organization. Note that this policy requires you populate the Executives address group, which is also created for you as a default address group.                   |
| Look-alike Domains                          | Attack Types      | Look-alike Domain                  | Attack types include Look-alike Domain. Catch imposter domains with intentionally similar names, things like cisco.com or paypa1.com.                                                                                                                                                   |
| Low Message Trust and Low Server Reputation | Trust Score Range | 0.0 to 2.5                         | Message Trust Score is $\leq 2.5$ and SBRS score is $\leq -2.0$ . To catch general spam and graymail that slips past your SEG.                                                                                                                                                          |
|                                             | SBRS Range        | -10.0 to -2.0                      |                                                                                                                                                                                                                                                                                         |
| Rapid DMARC                                 | Domain's Tags     | Internal                           | Domain tag is "internal" and attack types include Domain Spoof. To catch spoofs of your own domains being sent to your employees. This policy mimics a DMARC reject policy                                                                                                              |

| Policy Name                    | Setting           | Value                              | Description                                                                                                                                                                                                        |
|--------------------------------|-------------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                | Attack Types      | Domain Spoof                       | without the need to go through a long process of authenticating all sources. Agari's trust models learn the authenticity of inbound sources.                                                                       |
| Spoof of Partner Domains       | Domain's Tags     | Partner                            | Domain tag is "partner" and attack types include Domain Spoof. To catch spoofs of your partners' domains.                                                                                                          |
|                                | Attack Types      | Domain Spoof                       |                                                                                                                                                                                                                    |
| Suspicious Messages to C-Level | To                | C-Level Executives (address group) | Matches an email address in C-Level Executives with a Message Trust Score between 0 and 3.0, inclusive. To catch messages that are either untrusted or very suspicious and sent to one of your C-Level executives. |
|                                | Trust Score Range | 0.0 to 3.0                         |                                                                                                                                                                                                                    |
| Untrusted Messages             | Trust Score Range | 0.0 to 1.1                         | Message Trust Score is between 0 and 1.0, inclusive.                                                                                                                                                               |

The conditions in these default policies can be edited based on your experience and characteristics of your organization's mail flow. The out-of-the-box conditions are based on what has been effective across the Cisco customer base.

## Create a Policy

Creating a policy is straightforward: specify criteria to match certain kinds of messages, and then set the action to be taken for messages that match those criteria.

A few important things you should know before creating a policy:

- Every policy is evaluated for every message, and a single message can match multiple policies.
- Enforcement actions on a message that matches multiple enforcement policies will occur in the following priority order:
  - a. Inbox
  - b. Delete
  - c. Default folder move
  - d. Additional folder moves in order set in organization enforcement settings (see "Organization Settings" on page 163).

You can create a policy with no notification or enforcement actions; all messages that match policies are logged in the Event Log and Reports.

1. Go to Manage > Policies.
2. Click Create Policy.

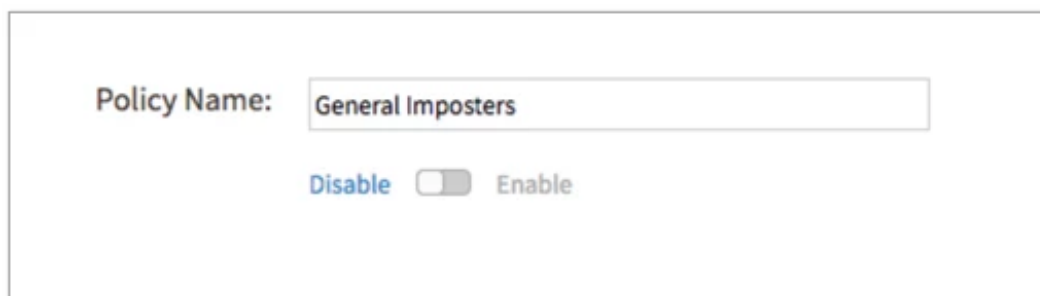
3. Define the policy settings. See " Policy Settings" on the next page for details.
4. Click Create.

## Edit a Policy

1. Go to Manage > Policies.
2. Click a policy name.
3. Make any desired changes to the policy settings. See " Policy Settings" on the next page for details.
4. Click Save.

## Enable or Disable a Policy

1. Go to Manage > Policies.
2. Click a policy name.
3. Click the slider below the policy name to enable or disable the policy.



4. Click Save.

## Delete a Policy

1. Go to Manage > Policies.
2. Click the name of a policy.
3. At the bottom of the page, click the Delete [policy name] link.
4. Click OK.

## Customize Policy Notifications

Policy notifications contain text that you can customize, including using variables placeholders that will include defined message content.

1. Go to Manage > Policies.
2. Click the Configure Policy Text for Original Recipients link.
3. Enter the content you want for your policy notifications. The content defined here will be used for all policy notifications. See the Policy Notification Content Settings and Policy Notification Content Variables sections below for more information.
4. Click OK.

## Policy Notification Content Settings

Policy notifications contain the following sections.

| Section       | Description                                                                                                | Default Content                                               |
|---------------|------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Subject       | This will be the notification subject line.                                                                | [Untrusted Message] \$subject                                 |
| Message Open  | This is optional text that you can use for the beginning of the notification message.                      | WARNING:<br><br>The system has detected an untrusted message: |
| Message Body  | This displays the From and Subject of the message that triggered the notification. This cannot be changed. | From: "\$from"<br>Subject: "\$subject"                        |
| Message Close | This is optional text that you can use for the end of the notification message.                            | Please proceed with caution!                                  |

## Policy Notification Content Variables

These are the variables that you can use in the Subject, Message Open, and Message Close sections of policy notifications. You should avoid using variables that represent large amounts of content in the Subject section.

| Variable  | Definition                                                                                |
|-----------|-------------------------------------------------------------------------------------------|
| \$from    | Represents the contents of the From field of the message that triggered the notification. |
| \$subject | Represents the subject line of the message that triggered the notification.               |

## Policy Settings

This topic describes policy settings. A message must match all of the settings in a policy for the policy to be enforced on the message.

A policy needs only a single condition to be a valid policy, and no action is required. (Policies with no actions defined are sometimes known as "monitor" policies.) The interface for creating policies allows you to create very narrow conditions to match a very specific set of messages (for example, "From: UserA and To: UserB with a sending IP reputation between -6.7 and -6.6, inclusive"). You can also use the interface to set up very broad conditions, which may match a very large number (or nearly all) of

your incoming messages (for example, " Any message whose Trust Score is between 2.2 and 10.0, inclusive" ). Use caution when configuring policies so that you do not create policies that are overly broad.

Policy settings that are ranges, that is, where you set an upper-bound value and a lower-bound value, are always inclusive ranges. That means that the range includes the upper and lower bounds. In technical terms, this means you define " greater than or equal" and " lesser than or equal" boundaries, not strictly " greater than" and " lesser than," which would not include the boundary values.

| Setting                                                                                                                                                                                                                                                                                                                                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Policy Name                                                                                                                                                                                                                                                                                                                                                  | The name should be a good descriptor of what the policy is designed to do.                                                                                                                                                                                                                                                                                                                                                                                                                    |       |
| Enable/Disable                                                                                                                                                                                                                                                                                                                                               | Determines if the policy is applied to your email stream.                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |
| Message Direction                                                                                                                                                                                                                                                                                                                                            | Select the message direction you want to match, from: <ul style="list-style-type: none"> <li>inbound - Messages that were sent into your organization from outside your organization</li> <li>outbound - Messages that were sent from within your organization to outside your organization</li> <li>internal - Messages that started and ended within your organization</li> </ul> Some policy settings are available only for some message directions, as indicated by the following table: |       |
|                                                                                                                                                                                                                                                                                                                                                              | <b>Policy Setting</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |       |
|                                                                                                                                                                                                                                                                                                                                                              | <b>Inbound Outbound Internal</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                              |       |
|                                                                                                                                                                                                                                                                                                                                                              | From/Reply-To/To                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | ✘ ✘ ✘ |
|                                                                                                                                                                                                                                                                                                                                                              | Subject                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | ✘ ✘ ✘ |
|                                                                                                                                                                                                                                                                                                                                                              | Sending Domain                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | ✘     |
|                                                                                                                                                                                                                                                                                                                                                              | Domain's Tags                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | ✘     |
|                                                                                                                                                                                                                                                                                                                                                              | Attachments                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | ✘ ✘ ✘ |
|                                                                                                                                                                                                                                                                                                                                                              | Truse Score Range                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | ✘     |
|                                                                                                                                                                                                                                                                                                                                                              | Attack Types                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | ✘ ✘ ✘ |
|                                                                                                                                                                                                                                                                                                                                                              | Advanced (Authenticity Score Range, Domain Reputation Range, SBRS Range, IP Address)                                                                                                                                                                                                                                                                                                                                                                                                          | ✘     |
|                                                                                                                                                                                                                                                                                                                                                              | Enforce                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | ✘ ✘ ✘ |
| Notify                                                                                                                                                                                                                                                                                                                                                       | ✘ ✘ ✘                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |       |
| <b>Content</b>                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |
| In the From, Reply-To, and To fields, you can either <ul style="list-style-type: none"> <li>Enter an individual email address</li> <li>Click in the field and select an address group</li> </ul> (In general, using address groups makes your policies easier to manage.) The From, Reply-To, To, and Subject fields are case-insensitive, partial matching. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |
| From                                                                                                                                                                                                                                                                                                                                                         | Use an address group in the From field of a policy condition when you want to detect impostors of the users in the address group. The condition will look for the address group members' names in the Display Name (i.e.                                                                                                                                                                                                                                                                      |       |



| Setting           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | <p>Friendly From) of the From header. If a given From header does not use a Display Name, the condition evaluates the local part of the email address in the address group to see if it matches the email address in the From header.</p> <p>The condition will also take into account the authenticity of the message if the From address matches the entered address.</p> <p>For example, consider an address group containing the following address:</p> <p>" John Doe" &lt;jdoe@example.com&gt;</p> <ul style="list-style-type: none"> <li>• If a message is received From: " John Doe" &lt;jdoe@not-example.com&gt;, then the condition would match as an impostor of John Doe in the Friendly From and the action defined for the policy would be taken (alert, enforcement, etc.).</li> <li>• If an inauthentic message is received From: " John Doe" &lt;jdoe@example.com&gt;, then the condition would match as an impostor of John Doe, because even though the real email address is used, it is not authentic. An action would be taken.</li> <li>• If no Friendly From portion exists, the local part of the address is evaluated, so an address of &lt;jdoe@example3.com&gt; would match based on the local part of the email address in the From header matching.</li> </ul> |
| Reply-To          | Address groups will simply look for messages where the Reply-To and To fields exactly matches an entry in the address group, ignoring the Display portion. A policy matching an address group in the Reply-To or To field might commonly be used along with other criteria like a Subject string match and Message Trust Score. For example, your policy conditions might be: To a member of the Finance address group, and Subject contains "Invoice,"                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| To                | and Message Trust Score is 0 - 4.9.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Subject           | Enter what you want matched in a message subject line. The policy will look for the entire value anywhere in a subject. For example, if you enter " goo" , the policy will match subject lines that include " Google Password Confirmation," " Goo-Goo Dolls tickets," and " Check out this gooey brownie recipe." Or if you enter " red fish blue fish" , the policy will match subject lines that include " one fish two fish red fish blue fish" but not subject lines that include " there were fish in the blue sea" .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Sending Domain    | Enter a single domain name. This setting looks for matches of the sending domain value of any DKIM records in the message header.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Domains' Tags     | Click in the field to select one or more domain tags. The condition will evaluate if any domain contains any of the selected tags.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Scoring</b>    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Trust Score Range | Use the sliders to define the Trust Score range that the message must have for the policy to be considered. The values you select are included in the range, that is, the range is inclusive. For example, if you select the Trust Score Range boundaries to be 1.0 at the lower end and 2.0 at the upper end, the policy will match messages with a trust score of exactly 1.0 or 2.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Attack Types      | Click in the field to select one or more attack types that the message must have for the policy to be considered. The policy will be considered if any of                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Setting                                                                                                                                                                                                                                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                               | the attack types apply to the message.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Advanced</b>                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Authenticity Score Range                                                                                                                                                                                                                                                      | Adjust the sliders if you want the policy to match any range other than the default, which is everything in the range. The values you select are included in the range, that is, the range is inclusive. For example, if you select the Domain Reputation Range boundaries to be 1.0 at the lower end and 2.0 at the upper end, the policy will match messages with a domain reputation of exactly 1.0 or 2.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Domain Reputation Range                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SBRS Range                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| IP Address                                                                                                                                                                                                                                                                    | Enter one or more IP addresses, separated by commas. You can also enter IP address ranges. The condition will evaluate if any IP address in the header matches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Actions</b>                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Any settings you define here determine any additional actions that will be taken when a message matches the policy. The default action is that any message that matches a policy is recorded in the Policy Log, but the message itself and its intended route is not altered. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Enforce                                                                                                                                                                                                                                                                       | <p>If you use Office 365 or G Suite as your mail store and have enabled Enforcement (see "Configure Enforcement: Office 365" on page 82 or "Configure Enforcement: G Suite" on page 75), you can choose to have matching messages deleted or moved out of the inbox and into a designated folder. You can also create a "whitelist" policy by choosing to move messages to the inbox when matching a set of policy conditions.</p> <p>An enforce action can be used in combination with a notification to the original recipients so that end users could receive a notification every time a Advanced Phishing Protection moves a message based on a policy condition match.</p> <p>Enforcement actions on a message that matches multiple enforcement policies will occur in the following priority order:</p> <ul style="list-style-type: none"> <li>• Inbox</li> <li>• Delete</li> <li>• Default folder move</li> <li>• Additional folder moves in the order set in organization enforcement settings (see "Organization Settings" on page 163).</li> </ul> |
| Notify                                                                                                                                                                                                                                                                        | <p>You can specify who to notify and how to notify them.</p> <p>Notify original recipients will send an individual notification to all recipients of message when the policy is triggered. (Note that this could cause bounce messages. For example, it could occur if the sensor parses a message and attempts to send a notification to a non-existent mailbox.)</p> <p>Notify administrators will send either a single notification message for every matching message, or a single digest notification when the number of messages matching a given policy exceeds a threshold you define.</p> <p>You can customize the content of notifications users receive. See "Customize Policy Notifications" on page 122 for details.</p>                                                                                                                                                                                                                                                                                                                           |

## Create a Test Policy

Creating a basic policy is simple: you need to enter only three pieces of information.

1. Go to Manage > Policies.
2. Click Create Policy.
3. Enter the following information:
  - Policy Name: MyTest
  - From: Your personal email address
  - To: Your company email address

### Create Policy

Based on conditions in emails coming into your organization, trigger an event.

Policy Name:

Disable  Enable

Message Direction:

Content  
All conditions must apply (logical AND)

From:

Reply-To:

Reply-To: domain address does not match From: address domain

To:

To: address is equal to the From: address

Subject:

The From, Reply-To, To, and Subject fields are case-insensitive, partial matching

At this point, your Policy is finished. Note that we did not specify an action. The default action for all matched policies is to log the message in the Policy Log.

4. Click Create.
5. Send a message from your personal account to your company address.
6. On the Manage > Policies page, click the Policy Log tab. An entry in the log for your policy and the message you just sent should appear.

| Timestamp                | Policy Name / System Notification | Event                                           |
|--------------------------|-----------------------------------|-------------------------------------------------|
| 13-Feb-2017 10:45:27 PST | MyTest                            | Event with 1 message<br>No Recipients notified. |

Policy event log for a policy event

And that's it. You have successfully created a policy to match incoming mail.

Matching incoming messages based on conditions is a basic building block for creating a policy. From here you can add more detail and complexity, matching subjects or specific domains or IP addresses. You can create address groups for matching groups of senders or recipients. (See "Address Groups" on page 154 for more information.) You can specify a range of scoring options.

Next, you will want to specify actions to take on matched messages.

## Specifying Actions

Now that you are comfortable creating policies to match messages, it's time to specify what will happen when those matches occur. In addition to the default logging, you can also specify two other actions: Notify and Enforce (enforcement customers only). Think of the actions as part of a spectrum: logging is the action with the lowest impact, and followed by a notify action, and then enforcement at the highest end. So while you are coming up to speed on policies, first try logging only, then notify just the Admin, then notify the message recipients, and then consider enforcing.

Enforcement customers: test your policies before enabling enforcement to ensure they are not too broad (overly broad policies can lead to false positives).

## View Policy Results

Once you have created and enabled some policies, you will want some insight into the results, answers to questions such as

- Are the policies working as you expected?
- How many messages are matching?
- Is the number of matches trending upwards?

There are three ways you can check for this kind of information:

- The Policy Log is a running log of policy matches
- On the Manage > Reports page is a view of aggregate policy matches over time,
- On the Search Messages page you can search for Matched Policies.

## Policy Log

On the Manage > Policies page, click the Policy Log tab. This is a log of all policy match and system notification events.

The Policy Log shows each policy match as it happens. This is a list of policy matches by message (one message per match).

View the matched policy by clicking the name of the policy. View the message details for the message(s) matching the policy by clicking the line in the Event column.

You can filter the Policy Log to show the matched messages for a specific policy and choose whether to show system notifications in this view.

## Policy Report

The Manage > Reports page shows the summaries of policy events over time: how many matches for each policy.

Click the policy name to review the policy conditions and actions from within the policy editor.

Click the number of messages (or the horizontal bar) to view a detailed report for that policy.

The Policy Report shows the number of matches for the current day. You can expand the timeline by selecting a longer time period on the right. This view can show trends in matching for that policy. Are more messages matching that policy now? Fewer? Click on the number of messages in the policy report to view the messages in the Search Messages results.

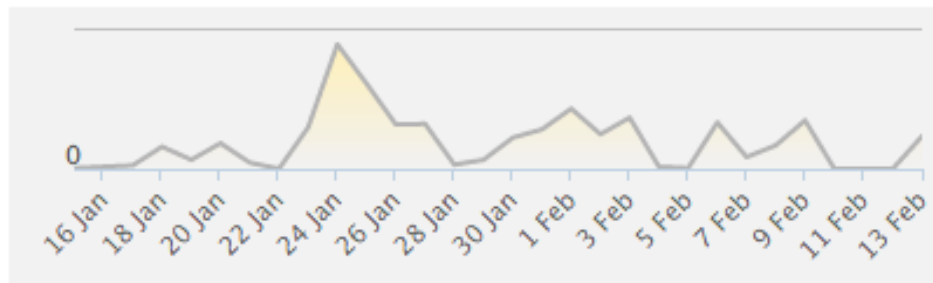
## Reporting on Enforcement

Select with Enforce action from the Show policies drop-down list to view a summary of the moved and not moved messages for all policies with the Enforce action.

### Reports

Review the summaries of policy events over time.

#### Total Messages Moved



Show policies:

Filter policy reports by enforcement actions

## Search Messages

On the Analyze > Search Messages page, you can select a policy in the Matched Policy field to search for messages that triggered the selected policy.

## On-demand Policies

On-demand policies are policies that you can quickly and easily create based on the criteria used for a message search. They are available to Cisco Advanced Phishing Protection customers who have enabled enforcement for their G Suite or Office365 environments.

Using an on-demand policy, you can selectively enforce a policy action on a set of messages. This includes moving messages from your users' inboxes to a specific folder (you may have multiple folders available for moving messages to), deleting a message, or moving a message back to a user's inbox. By enforcing messages after they have been delivered to users' inboxes, Advanced Phishing Protection provides you with another tool to mitigate threats. For example, if certain email messages have evaded the existing lines of defense (like spam and virus filtering), you can use the on-demand policies feature in Advanced Phishing Protection to move those messages out of users' inboxes.

On-demand policies are only available if you have enabled enforcement for your organization.

## On-demand Policies Index Page

All on-demand policies are listed chronologically in the on-demand policies index page. Click the On-Demand Policies tab on the Manage > Policies page to view it.

| Name                                 | Conditions                                                                                                                                                                                                                                                                                                                                           | Initiated On             | Initiated By    | Enforced Rate | Delete |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|-----------------|---------------|--------|
| On-Demand Policy 2017-09-27 17:23:30 | <ul style="list-style-type: none"> <li>From: address:               <ul style="list-style-type: none"> <li>contains <a href="#">datadog alerting</a></li> </ul> </li> <li>To: address:               <ul style="list-style-type: none"> <li>contains <a href="#">plorence</a></li> </ul> </li> <li>Date range: 27-Sep-2017 to 28-Sep-2017</li> </ul> | 27-Sep-2017 17:23:30 UTC | Paul Lorence EP | 3/3 - 100%    |        |
| On-Demand Policy 2017-09-26 19:17:03 | <ul style="list-style-type: none"> <li>From: address:               <ul style="list-style-type: none"> <li>contains <a href="#">datadog</a></li> </ul> </li> <li>To: address:               <ul style="list-style-type: none"> <li>contains <a href="#">plorence</a></li> </ul> </li> <li>Date range: 25-Sep-2017 to 27-Sep-2017</li> </ul>          | 26-Sep-2017 19:17:03 UTC | Paul Lorence EP | 11/11 - 100%  |        |

### On-demand policies index page

From this view, you can rename the on-demand policies and view the conditions, who initiated the policy and when, and the enforcement rate of the policies.

Click the Delete icon to remove the on-demand policy from this listing. Note that clicking delete only removes the on-demand policy from the listing; it does not affect the disposition of messages.

## Final Notes

On-demand policies are searchable from the search page:

On-demand policies are tracked in the audit logs for an organization. To view the audit log, go to Manage > Organizations, and then click the Audit link under the organization name.

## Performance Note

The rate at which messages are moved depends on the speed and latency of the API call into the mailbox provider (G Suite or Office365).

The same queuing system is used for enforcement actions from both on-demand policies and "regular" (on-going) message policies. If you routinely enforce large numbers of messages from message policies, adding additional enforcement actions to the queue from on-demand policies will impact the overall performance of enforcing messages in Advanced Phishing Protection. The queuing system accepts enforcement actions from all sensors simultaneously. You can view the log for enforcement actions on any sensor in the `/var/log/cisco/enforcer.log`.

## Create an On-Demand Policy

On-demand policies are created from the search results page. See "Message Search" on page 110 for details.

Creating an on-demand policy is done with the Enforce Now button on the message search results page, and the Enforce Now button is visible only if enforcement has been enabled for your organization.

You can only enforce 2000 or fewer messages at a time using an on-demand policy so the Create Now button is disabled for search results larger than 2000 messages.

For example, note the button state and the number of results in each of these examples:

The screenshot shows the search results page with the following filters and controls:

- Domain Reputation Range: Slider from 0.0 to 5.0.
- Domain Tags: Filter By Tags.
- Sending Domain: redwoodcompliance.com.
- Domain Type: Zero-Day, Impostor.
- Buttons: Search, Reset, and Enforce Now ...

Below the filters, the text "Displaying 1 - 16 of 16 Messages" is shown above a table of results:

| Trust Score ▲ | Date        | From                                     |      |
|---------------|-------------|------------------------------------------|------|
| 3             | 27-Sep-2017 | Amber Leon <amber@redwoodcompliance.com> | vapp |
| 3             | 27-Sep-2017 | Amber Leon <amber@redwoodcompliance.com> | dsp  |
| 3             | 27-Sep-2017 | Amber Leon <amber@redwoodcompliance.com> | san  |
| 3             | 27-Sep-2017 | Amber Leon <amber@redwoodcompliance.com> | sken |

Enforce Now... button available

Domain Reputation Range:  0.0 5.0

Domain Tags:

Sending Domain:

Domain Type:

Maximum 2,000 messages

Displaying 1 - 25 of 3,905 Messages

| Trust Score ▲ | Date        | From                                     |      |
|---------------|-------------|------------------------------------------|------|
| 3             | 27-Sep-2017 | Amber Leon <amber@redwoodcompliance.com> | vapp |
| 3             | 27-Sep-2017 | Amber Leon <amber@redwoodcompliance.com> | dspe |
| 3             | 27-Sep-2017 | Amber Leon <amber@redwoodcompliance.com> | san  |
| 3             | 27-Sep-2017 | Amber Leon <amber@redwoodcompliance.com> | sken |

Enforce Now... button unavailable

1. View a list of messages by either going to Analyze > Search Messages or clicking a Message link on the Dashboard (Analyze > Dashboard).
2. If necessary, narrow your search criteria so that the results shown are fewer than 2000 messages.

You can narrow your results by adding more condition to the search criteria. For example, you can add specific Message-ID to search criteria like "To:", "From:" and "Subject."

In this example, the search criteria are narrowed to a set of messages from a particular domain to a single user:

Search Messages

Search and filter mail that has been sent to you.

From:

To:

Reply-To:

Subject:

Attachment:

Received between:  and

Trust Score Range:  0.0 10.0

Authenticity Score Range:  0.0 1.0

Matched Policy:

Enforcement:

Message ID:

---

Attack Type:    
 Multiple attack types are logical ORs

Domain Reputation Range:  0.0 10.0

Domain Tags:

SBRS Range:  -10.0 10.0

Sending Domain:

Hostname:

IP Address:

[Message Feedback](#)  
[Create a Policy](#)  
[Download Results](#)

Displaying 1 - 25 of 48 Messages

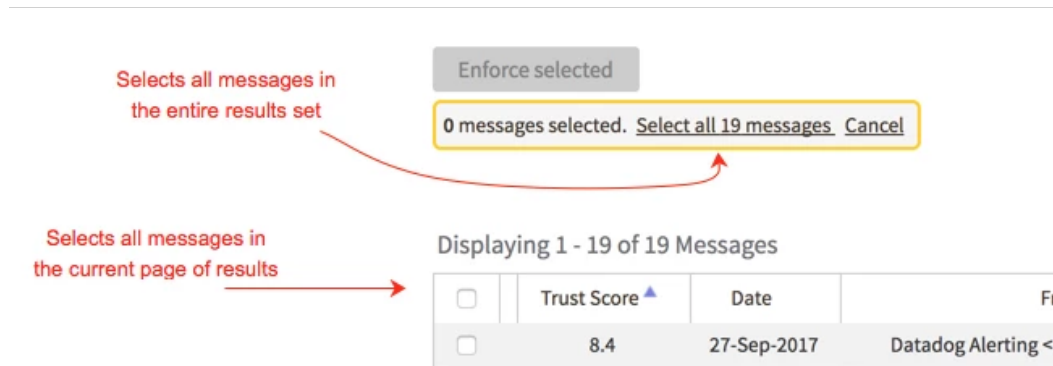
| Enforced? | Trust Score ▲ | Date        | From                                            | To             | Subject                         |
|-----------|---------------|-------------|-------------------------------------------------|----------------|---------------------------------|
|           | 9.4           | 17-May-2019 | Google Alerts <googlealerts-noreply@google.com> | jcreech@...com | Google Alert - Proofpoint       |
|           | 9.4           | 17-May-2019 | Google Alerts <googlealerts-noreply@google.com> | jcreech@...com | Google Alert - "phishing"       |
|           | 9.4           | 17-May-2019 | Google Alerts <googlealerts-noreply@google.com> | jcreech@...com | Google Alert - "spear phishing" |
|           | 9.4           | 17-May-2019 | Google Alerts <googlealerts-noreply@google.com> | jcreech@...com | Google Alert - "phishing"       |
|           | 9.4           | 17-May-2019 | Google Alerts <googlealerts-noreply@google.com> | jcreech@...com | Google Alert - "spear phishing" |

Narrowing search results

3. Click Enforce Now to select individual or all messages within the results set.



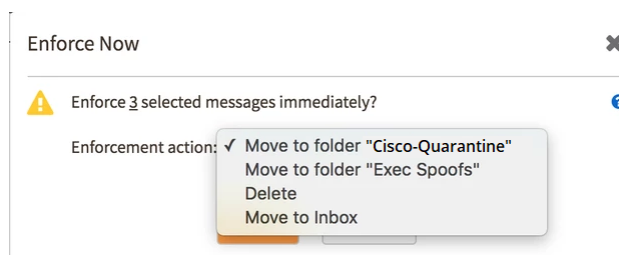
- Select either all of the messages in the search results by clicking on the link or select individual or a page of search results by clicking in the boxes in the left column of search results. Note the differences in selecting all messages in the entire set versus selecting all messages shown on the current page of results:



#### Selecting individual messages versus selecting all messages

If your organization has Insider Impersonation Protection enabled and is evaluating all messages (see the "Evaluate Messages" on page 164 setting in Organization Settings) on-demand policies can apply to only inbound messages. If your selection includes messages that are not inbound, those messages will not be used to create the on-demand policy.

- After selecting at least one message, click Enforce selected.
- In the Enforce Now dialog box, confirm the number of messages to be enforced and choose the enforcement action you would like to take. (The question mark icon provides additional information on why some messages may not be able to be moved.)

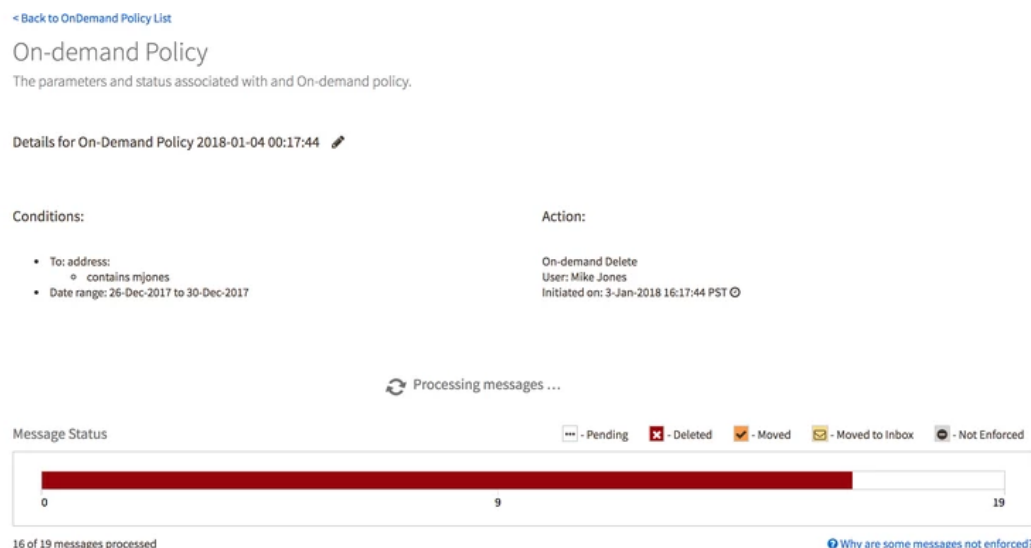


#### Choosing an enforcement action

- Click OK to enforce the message(s) immediately.

After you click OK, the On-demand policy details page is displayed while Advanced Phishing Protection contacts your sensor(s). After the sensor has been contacted, the list of messages to be enforced is displayed in the Message status area.

At first, the status for the entire set of messages is listed as " pending:"



### In-progress status of an on-demand policy

As the system continues to process the set of messages, the page is refreshed as new information is received about the disposition of messages – either " Deleted" , " Moved" , " Moved to Inbox" , or " Not Enforced" .

After all messages have been processed, the page displays the final results of the on-demand policy:

Click the pencil icon to re-name the on-demand policy, if necessary. (For example, " Deleted Spam messages." )

In addition to the status of the enforcement action, you will also be able to see if the recipient of the message had read the message or not at the time the enforcement happened. If the Read? column contains an open envelope, it means the recipient had already read the message.

## Reports

Cisco Advanced Phishing Protection provides two types of reports:

- Information about policies, with or without enforcement action, defined in Advanced Phishing Protection, which are available on the Manage > Reports page.
- Information about key threat metrics, presented in graphical form, which are available on the Executive Summary and Threat Trends tabs on the Advanced Phishing Protection dashboard (Analyze > Dashboard, or click the product logo).

## Reports Page

The Reports page shows the summaries of policy events over time. Specifically, how many messages matched each policy during the selected time period? Click the policy name to view the policy configuration in the Policy editor. Click the number of messages (or the horizontal bar) to view the Policy Report for that Policy.

By default, the Policy Report shows the number of matches for the current day. You can expand the timeline by selecting a longer time period on the right. This view can show the trend over time of messages matching that policy. Are more messages matching that policy now? Fewer? Click on the number of messages in the policy report to view the list of messages in the Search Messages results.

## Threat Trends and Executive Summary Reports

Both the Threat Trends and Executive Summary tabs on the home page (Analyze > Dashboard), summarize recent data accumulated by Advanced Phishing Protection.

In the line and bar graph report displays, you can hover over the representation for any date and view a pop-up that contains the detailed data for that date.

You can select a time period for all reports on the page. Choose from:

- 7 days
- 2 weeks
- 1 month
- Custom (select a start date and an end date)

The aggregate data in the reports does not include data from the current date or from before the date you had data accumulating from your organization. The data displays in the charts as follows:

- For the 7 days and 2 weeks time periods, each data point represents a full day of data. For example, if you select 7 days, you will see the past 7 full days of data, but no data from today.
- For the 1 month time period, the data points each represent a full Monday-through-Sunday week of data, starting with the week that began the Monday of 1 month ago. Depending on the day of the week and the number of days in the current month, this means that the first week or the last week may have less than 7 days of data.
- For custom, if you select a time period from a single day up to 2 weeks, each data point represents a full day of data. If you select a time period of more than 2 weeks, each data point represents a full Monday-through-Sunday week of data. If you set a start date to a date before your organization started accumulating report data, the "Since..." notation at the top of each chart will indicate the earliest date of the data in the chart. Custom date ranges are also "sticky," in that they do not reset when you navigate away from the tab or page, but only when you log out.

You can download the current page in Adobe Acrobat (PDF) format. See "Download a Threat Trends or Executive Summary Report" on page 146 for details.

For more information, see "Threat Trends Reports" on the facing page and "Executive Summary Reports" on page 138 and the individual description section for each report. To change global settings for these reports, see "Report Settings" on page 165 in the "Organization Settings" on page 163 section.

## Threat Trends Tab

The Threat Trends tab contains data views that detail key trends of attacks over time. It shows:

- Messages

This graph shows various key numbers over time, including total messages, spam/graymail, attacks, and messages matched by policy per day.

- Attacks

This graph shows how many attacks were found by Advanced Phishing Protection.

- Top policies

This graph shows the top 5 policies that were triggered.

See "Threat Trends Reports" below.

## Executive Summary Tab

The Executive Summary tab contains data views that detail the cumulative impact and value of protecting your employees with Advanced Phishing Protection. It answers the following questions:

- How many attacks were found?

This graph shows how many attacks were found by Advanced Phishing Protection. (Note that a single message may contain multiple attack vectors.)

- How much have I saved by deploying Cisco Advanced Phishing Protection?

This graph estimates the amount of money your organization saved by Advanced Phishing Protection's protection from phishing and other malicious attacks.

- How attacked am I and how protected am I relative to my peers?

This two-graph panel shows attack numbers and how well Advanced Phishing Protection protects you in comparison to peer organizations.

See "Executive Summary Reports" on page 138.

The reports on the Threat Trends and Executive Summary tabs show aggregated data. The aggregated data is updated once per day, at midnight UTC.

## Threat Trends Reports

Threat trends reports are a set of reports presented in a dashboard format on the Threat Trends tab on the Cisco Advanced Phishing Protection home page (Analyze > Dashboard). The reports summarize key data generated by Advanced Phishing Protection and present that data in easy-to-review charts.

The reports on the Threat Trends include:

- Messages, which shows what threats and attacks my organization has faced. (See "Messages Report" on the next page)
- Attacks, which shows what type of attacks my organization is facing. (The data in this chart is the same as the data in the How many attacks were found? report on the Executive Summary tab, except there is no attacks total number at the top of the chart. See "How Many Attacks Were Found Report" on page 139)

- Top 5 Policies, which shows which of my policies are triggered the most. (See " Top Policies Report" on the facing page)

The report views on this page are designed to give you a look at key trends over time, rather than just cumulative numbers.

You can customize the data set for some of the reports. See the section on each report for details about the data used in the report and instructions on how to how to configure the report.

## Messages Report

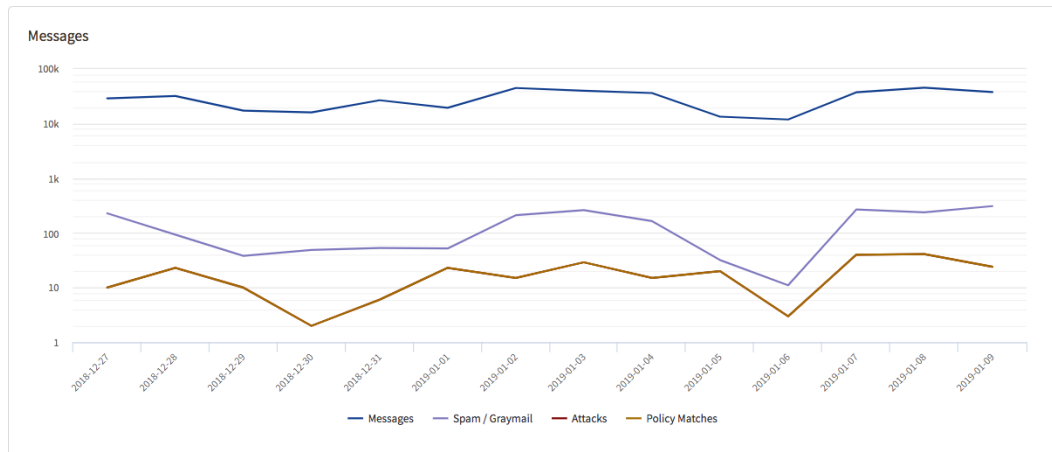
The Messages report shows you:

- How many messages were received by Advanced Phishing Protection
- How many of those messages were
  - Spam or graymail
  - Identified as any type of attacks
  - Attacks matched by any policy

The chart is in a line chart format. Hover over any point on a line, representing a single time period (day or week), to see the data for that time period.

When you view either 7 days or 2 weeks of data, each point represents 1 day. When you review 1 month of data, each point represents 1 week of data.

The items in the legend are also toggles. You can click on an item in the legend to include or exclude it from the report.



A sample report showing 2 weeks of messages.

Unlike other reports, the Y axis in this chart is logarithmic.

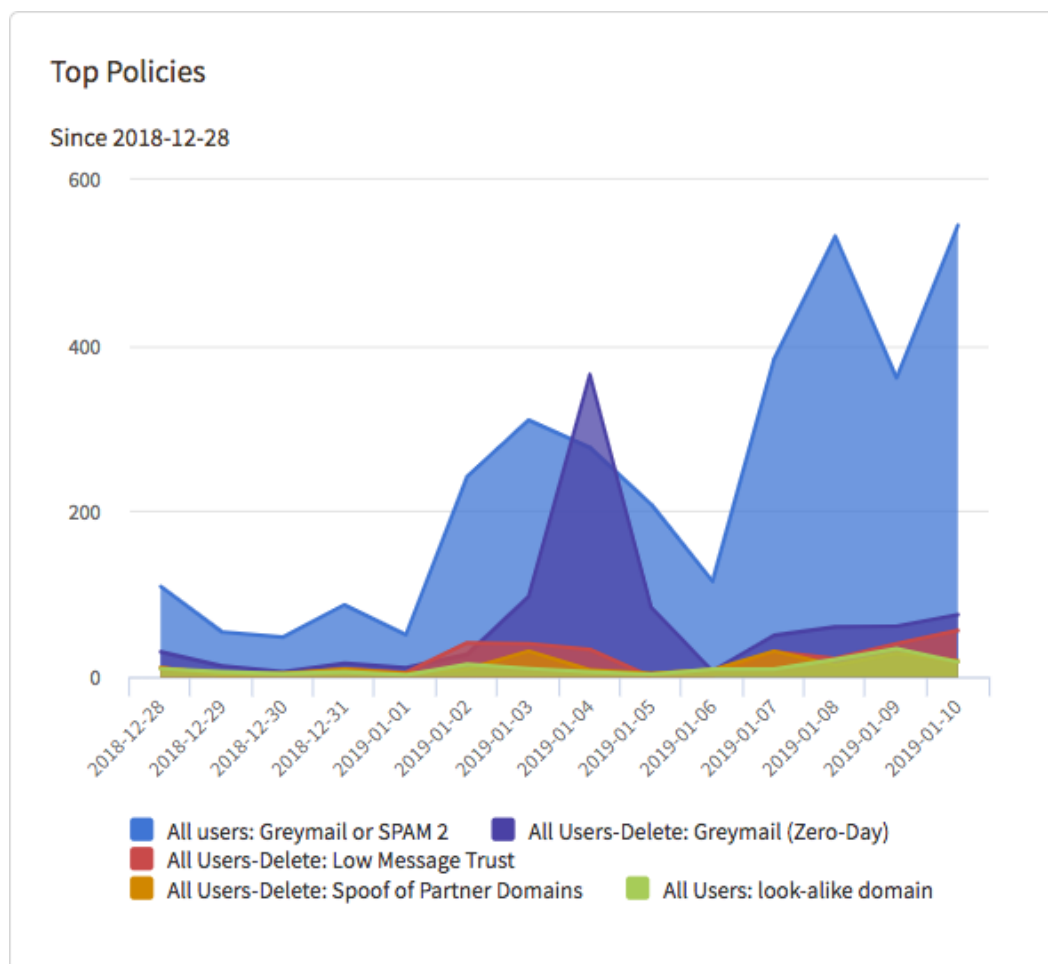
If you're polices are well-tuned to match the attacks you receive (see " Policies" on page 119), the Attacks and Policy Matches lines should be very close or even overlap. (In this example they do overlap, meaning that at least one policy matches every attack received, which is why you see only 3 visible lines.)

## Attacks Report

The Attack Types report contains the same data and interactivity as the How many attacks were found? report on the Executive Summary tab, except there is no total number at the top of the chart. See "How Many Attacks Were Found Report" on the next page for details about what data is in this report and how you can customize what you view in the report.

## Top Policies Report

This report shows the 5 policies that have matched the most messages per time period. Specifically, when you select a time period (7 days, 2 weeks, or Month), Advanced Phishing Protection looks at which 5 policies matched the more messages during that time period, and then creates an incremental plot for each policy, a daily increment for the 7 days and 2 weeks views, a weekly increment for the Month view.



A sample report showing 2 weeks of policy matches.

## Executive Summary Reports

Executive summary reports are a set of reports presented in a dashboard format on the Executive Summary tab on the Cisco Advanced Phishing Protection home page (Analyze > Dashboard). The reports summarize key data generated by Advanced Phishing Protection and presents that data in

easy-to-review charts.

The reports on the Executive Summary page answer the following questions:

- How many attacks were found? (See "How Many Attacks Were Found Report" below)
- How much have I saved by deploying Cisco Advanced Phishing Protection? (See "How Much Have I Saved by Deploying Advanced Phishing Protection Report" on the facing page)
- How attacked am I and how protected am I relative to my peers? (See "How Attacked/Protected Am I Relative To My Peers Report" on page 143)

You can customize the data set for some of the reports. See the section on each report for details about the data used in the report and instructions on how to how to configure the report.

## ***How Many Attacks Were Found Report***

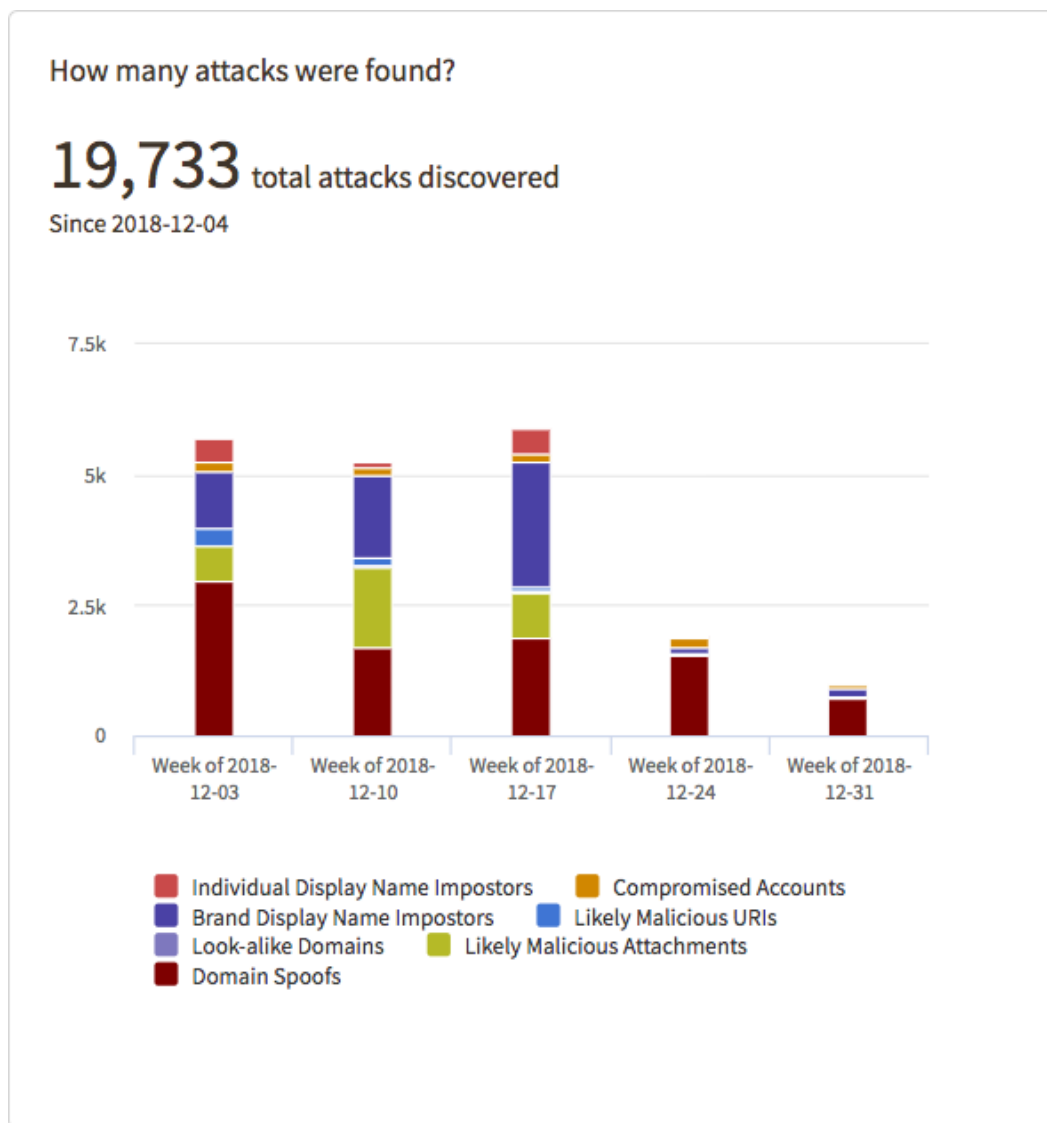
This report shows the number of attacks that Advanced Phishing Protection found, both the total number of attacks and the number of attacks by attack type, in a bar chart format. Hover over any segment, representing a specific attack type, in a bar to see the number of attacks of that type.

The number at the top answers the title's question, the total number of attacks discovered in the time period shown. This is always a cumulative number of all attack types.

When you view either 7 days or 2 weeks of data, each bar represents 1 day. When you review 1 month of data, each bar represents 1 week of data.

The attack type legend is also a toggle. You can click on an attack type to include or exclude it from the bar chart.

Changing the attack types shown in the bar chart does not change the total number of attacks shown at the top.



A sample report showing a month of attacks.

Each bar shows the total number of attacks per time period (per day in the 7 days and 2 weeks view, per week in the month view). Segments in the chart correspond to the number of attacks per attack type. Hover over a segment to view the number of attacks of the type represented by the segment.

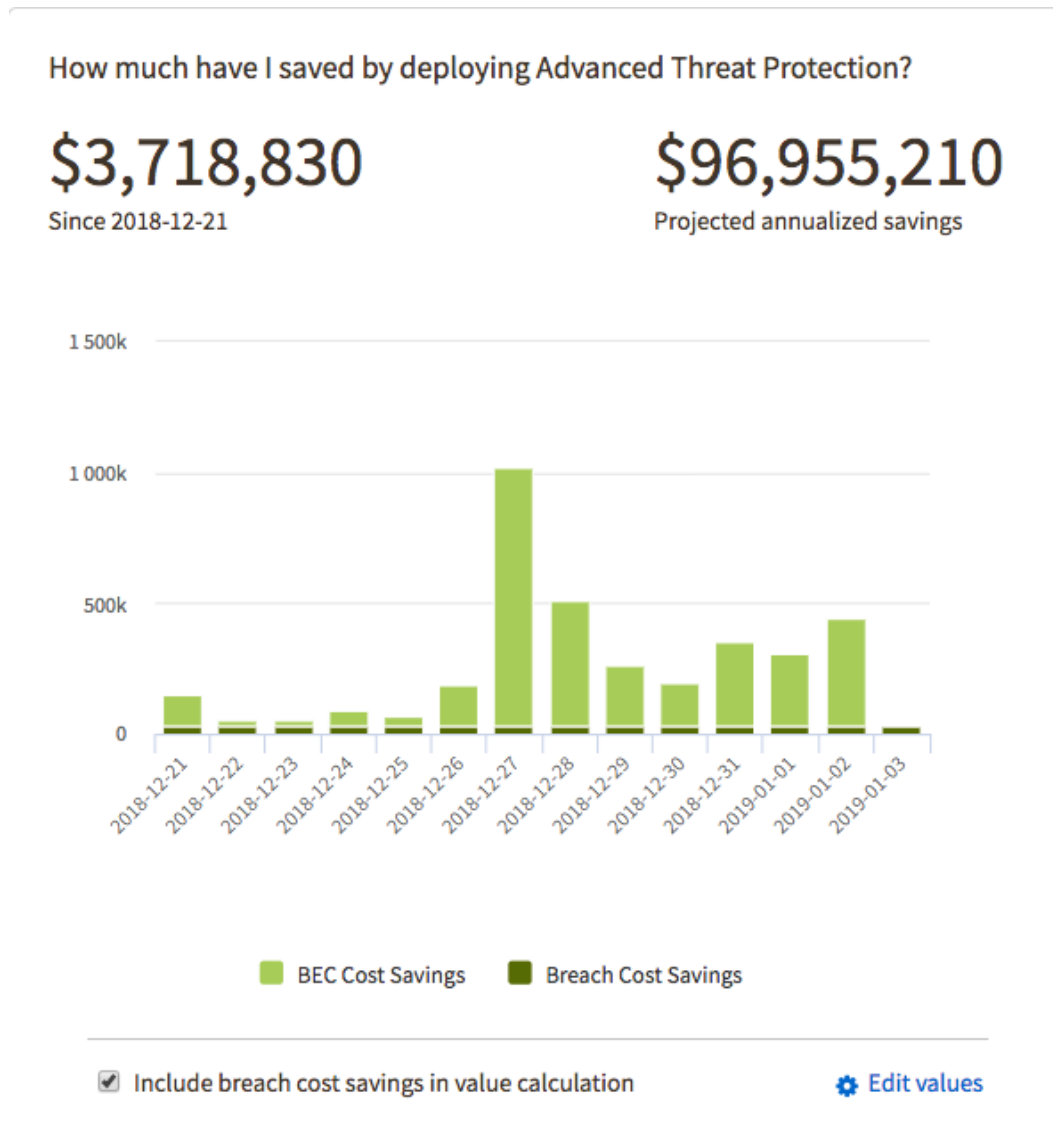
## ***How Much Have I Saved by Deploying Advanced Phishing Protection Report***

This report shows how much money Advanced Phishing Protection has saved you. It tracks how many business email compromise threat messages have been deleted or moved by both your real-time and your on-demand policies, and graphs how much it would have cost your organization if those messages had been allowed into or to remain in your organization's inboxes.

You can optionally also include the money saved by the stopping of email breaches.

See "Configure the How Much Have I Saved By Deploying Advanced Phishing Protection Report" on the next page for details on how to configure the values used in this report.





A sample report showing 2 weeks of savings.

The numbers at the top answer the title's question. The first number is the amount you have saved, based on the values entered, during the time period shown. The second number is an annualized number extrapolated from the first number.

## Configure the *How Much Have I Saved By Deploying Advanced Phishing Protection Report*

The *How much have I saved by deploying Advanced Phishing Protection* report can be configured in two ways. You can

- Include breach cost in the report calculation
- Adjust threat costs

Only users who have the Organization administrator role can configure this report. See "User Roles" on page 173 for more information.

Change the values used in the comparison

The information in this report is calculated similarly to the Cisco Secure Email Cloud ROI Analyzer for Cisco Advanced Phishing Protection at <https://www.agari.com/insights/tools/roi-calculator/#>. The default values used in the report are based on Cisco's extensive threat research data set. If you have data that differs from the Cisco data set, you can enter different values to create a calculation that will be more specific and relevant to your organization.

1. Go to Analyze > Dashboard.
2. Click the Executive Summary tab.
3. At the bottom of the How much have I saved by deploying Advanced Phishing Protection? report, click Edit values.
4. Enter your desired values. See the descriptions below for more information about each report value.
5. Click Save Values.

The report will update with the values you entered.

Click Reset all to default values at the bottom of the dialog box to revert any changes you made and replace them with the Cisco defaults.

Changes are not per user, but apply to all users within the organization viewing these reports.

## Values for the How Much Have I Saved By Deploying Advanced Phishing Protection Report

If you enter values that are below the default, you will see a warning indicator. In general, values below the default values, values that are backed by extensive, world-wide research, may give you a result that does not reflect real-world data.

### Currency

You can select Dollar or Euro.

### Breach Cost Savings

You can define the values that you believe one breach costs your organization specifically.

The default values are the average based on your region and industry, values that are based on extensive research.

- Average cost of a successful breach - Many people do not realize the total cost of an email breach. The default value may seem high, but it is backed by real data.
- Percentage of data breaches initiated through email - The overwhelming majority of data breaches are through some sort of email attack.
- Probability of a new email breach annually - This default reflects the cumulative results of years of data analysis of real-world email-based data breaches.

### BEC Cost Savings

The attack types represented here are the ones that Cisco Advanced Phishing Protection identifies. The values you enter for each attack type, if you know the actual average value for each in your organization, can significantly increase the accuracy of this report. Typically, the average cost of a

successful attack is higher than you might estimate because attacks can have both direct and collateral costs.

For example, your email system might be configured to never allow attachments of any kind. You could set the Threshold value to 0 because you are confident it will never happen in your system.

Note that the success probability is the probability without Advanced Phishing Protection.

For the What percentage of Advanced Email Threats are BEC attacks setting, enter the percentage of your total email attacks that are BEC attacks. Do not include spam or graymail in the total used for this calculation.

## ***How Attacked/Protected Am I Relative To My Peers Report***

This report shows how attacked you are and how well Cisco Advanced Phishing Protection protects your organization, both in comparison to your peer organizations. If there are not enough peer organizations, then the report falls back to a wider data set. The "peer" hierarchy is as follows:

- Region, industry, and mailboxes in your organization
- Industry and mailboxes in your organization
- Mailboxes in your organization
- Average of all organizations in the entire Cisco data set

"Region" is a defined geographic area such as North America or EMEA (Europe, the Middle East, and Africa)

"Industry" is a category such as manufacturing or finance

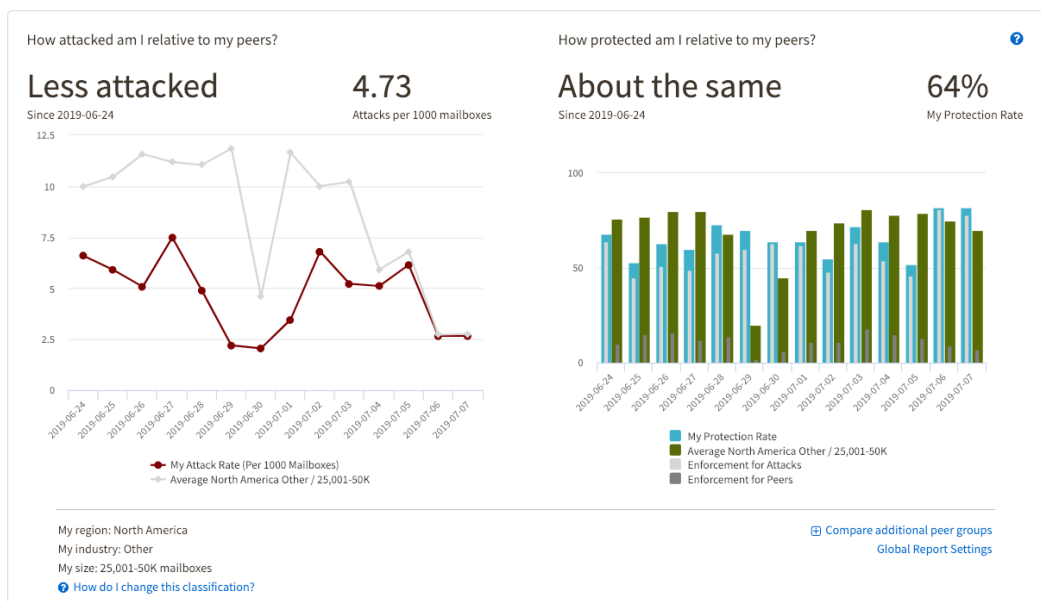
"Mailboxes" is defined by a set of tiers. For example, if you have 10,000 mailboxes in your organization, the comparison would be limited to other organizations in the tier that includes 10,000 mailboxes.

For each level in the hierarchy, if there are not at least 5 organizations in that level that can be used for comparison, the next level down is used. For example, say you're an airplane parts manufacturer in South America and there are just 2 other companies in South America in that same industry. So the first level would not be used. But there are more than 5 world-wide, and if there are enough that are about the same size ("size" being defined as the same amount of mailboxes), then the second level would be used for this report.

At the bottom of the report, you will see the region, industry, and mailbox size that is defined for your organization and that is being used for the current report. Click Compare additional to change the facets to which you compare your organization. See "Compare to an Additional Peer Group" on page 145 for details.

The report itself graphs the daily value of using Advanced Phishing Protection vs. not using Advanced Phishing Protection. As with all the reports on the Executive Dashboard, you can select time periods of the past 7 days (default), the past 2 weeks, or the past month.

See "Compare to an Additional Peer Group" on page 145 for more information on how to configure this report.



A sample report showing 2 weeks of comparative data.

In the How attacked am I relative to my peers line chart, one line represents your attack rate per 1000 mailboxes per time period (per day in the 7 days and 2 weeks view, average per day in the week in the month view). The other line is the average attack rate for your peers (region, industry, number of mailboxes). If you have added an additional peer group for comparison, a third line will show the attack rate for that group.

The summary at the top answers the chart's title question and quantifies your daily average attack rate (per 1000 mailboxes) for the time period shown. The answer can be any of:

- More attacked - more than 10% greater than your peer average rate over the time period shown
- Slightly more attacked - between 2% and 10% greater than your peer average rate over the time period shown
- About the same - between 2% less than and 2% greater than your peer average rate over the timer period shown
- Slightly less attacked - between 10% and 2% less than your peer average rate over the time period shown
- Much less attacked - less than 10% of your peer average rate over the time period shown

In the How protected am I relative to my peers bar chart, one bar shows your protection rate per time period (per day in the 7 days and 2 weeks view, average per day in the week in the month view). The other bar shows the average protection rate for your peers (region, industry, number of mailboxes). If you have added an additional peer group for comparison, a third bar will show the attack rate for that group. If you have policy enforcement enabled, an internal bar will show the rate of enforcement vs. protection.

The calculations for these are as follows:

- For protection rates, it is the number of attack messages matching any policy divided by the total number of attack messages divided by 100.

- For enforcement rates, it is the number of attack messages enforced by any existing policy divided by the total number of attack messages divided by 100.

These can differ because you may have policies configured in Advanced Phishing Protection that match messages but do not enforce messages, meaning that they are not moved or deleted from inboxes.

The summary at the top answers the chart's title question and quantifies your daily average protection rate (per 1000 mailboxes) for the time period shown. The answer can be any of:

- More protected - more than 10% greater than your peer average rate over the time period shown
- Slightly more protected - between 2% and 10% greater than your peer average rate over the time period shown
- About the same - between 2% less than and 2% greater than your peer average rate over the timer period shown
- Slightly less protected - between 10% and 2% less than your peer average rate over the time period shown
- Much less protected - less than 10% of your peer average rate over the time period shown

A higher number means that you have policies that are configured to protect you from the attacks you face.

## Compare to an Additional Peer Group

The companies used for comparison in the How attacked/protected am I relative to my peers report are the ones in your region, in your industry, and similar to your mailbox size. You can also add a comparison to an additional region, industry, or mailbox size.

1. Go to Analyze > Dashboard.
2. Click the Executive Summary tab.
3. At the bottom of the How attacked/protected am i relative to my peers report, click Compare additional peer groups.
4. Select a(n):
  - Region. You can choose from:
    - All Cisco customers
    - North America
    - EMEA (Europe, the Middle East, and Africa)
    - APAC (Asia Pacific)
  - Industry. You can choose from:
    - All Cisco customers
    - Finance
    - Government
    - Healthcare
    - Other

- Retail
- Technology
- (Mailbox) Size. You can choose from:
  - All Cisco customers
  - 0-250
  - 250-1K
  - 1001- 3K
  - 3001-5K
  - 5001-10K
  - 10,001-25K
  - 25,001-50K
  - 50,001-100K
  - 100K+

5. Click Update.

The report will refresh using the new comparison facets. Note that if there are not enough data sources for your selections and the report expands to the next tier (see "How Attacked/Protected Am I Relative To My Peers Report" on page 143 for details), the report may not change. The legend will reflect your choices, but the report will use the first tier that contains enough data for a useful comparison.

When you add a set of peers used for this report, the changes are "sticky." This is, if you navigate away from the page and come back, the data will still show the additional set of peers.

## Download a Threat Trends or Executive Summary Report

You can download the current view of a Threat Trends or an Executive Summary report, which includes all of the graphs, as an Adobe Acrobat (PDF) file.

1. Go to Analyze > Dashboard.
2. Click either the Threat Trends or the Executive Summary tab.
3. Configure the time period for the report. If you're viewing the Executive Summary report, you can also configure the data in the How much have I save by deploying Advanced Phishing Protection? and How attacked/protected am I relative to my peers? graphs. See "Configure the How Much Have I Saved By Deploying Advanced Phishing Protection Report" on page 141 and "Compare to an Additional Peer Group" on the previous page for details.
4. Click Download PDF.

A PDF of the current view is created and downloaded automatically to the default download location for your browser.

# Attachment and URL Analysis

Cisco Advanced Phishing Protection is capable of analyzing attachments to messages and URLs in message bodies, and using the results of that analysis, in addition to identity intelligence, to determine the overall trust of a message.

There are two levels of malicious content analysis possible in Advanced Phishing Protection:

- Basic collection of attachment information, such as name and file extension, which can be used in Search and Policy.
- Scanning of attachments for indicators of malicious intent, to enhance scoring and message classification.

URL analysis will:

- Extract URLs from:
  - The text/HTML MIME parts of messages, including base URLs from head sections
  - Microsoft Office and Adobe Acrobat documents attached to messages
- Parse both http and https schemes
- Will display URLs in message details views, but those URLs will not be clickable
- Identify URLs that use common URL shorteners and identify websites behind those URL shorteners

## Using Attachment Analysis

Once attachment analysis is enabled, you can use the results of attachment analysis in different ways.

## Using Attachment Analysis Results in Search and Policy

You will notice a new option on your Analyze > Search Messages page. The same field will also appear in Manage > Policies when you want to create or edit a policy.

# Search Messages


Search and filter mail that has been sent to you.

From:

To:

Reply-To:

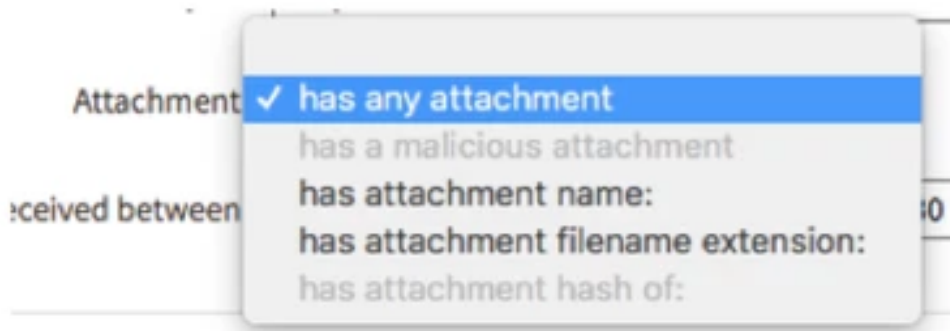
Subject:

Attachment: **has any attachment** 

Received between:  and

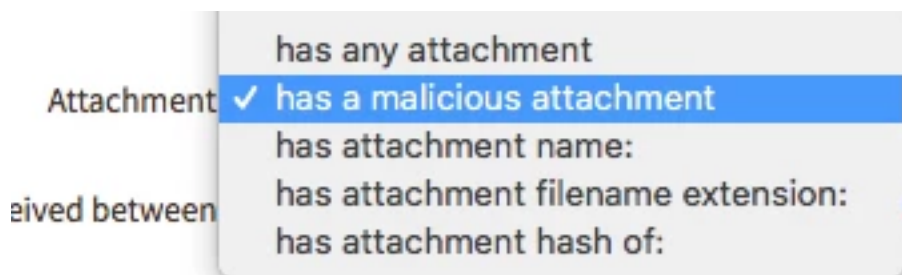
Searching for messages with an attachment

If you are only collecting attachment name information the following options will be available for you to search and set policy on.



Searching for attachments: limited selection

If you have enabled attachment scanning then all of the options will be available for search and policy.



Searching for attachments: with attachment scanning enabled



## Attachment Scan Results

When attachment scanning is enabled, Advanced Phishing Protection uses the results of the scan in its scoring models and message classification models. For example you will see the "Malicious Attachment" message classification like below in the Message Details. (NOTE: Coming soon you will also be able to expand the malicious attachment classification to see details on the malicious components that were detected.)



Attachment scanning results in the message details pane

## Details of the Attachment Scan

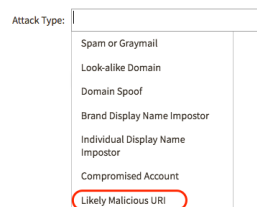
Advanced Phishing Protection attachment scanning is focused on identifying potentially malicious behaviors in document based attachments. It is not a sandbox and does not try to force malicious code to execute.

Advanced Phishing Protection will unpack, de-obfuscate, and perform static analysis of the following types of files:

- Archive file formats (zip/rar/tar/{gz/gzip/tgz}/{bz2/bzip2/tbz2/tbz}/cab)
- Office files, PDF, MHTML, email files, image files, flat data files, RTF
- Flash, video formats, Javascript, VBA

## Using URL Analysis

URL analysis is available in both message search and policy creation. In both cases, you can select Likely Malicious URI from the Attack Type drop-down list to be included in the search or policy filter.



Select this to include messages with likely malicious URLs in searches or policies.

## Enable Attachment and URL Analysis

Attachment and URL analysis in Advanced Phishing Protection is a multistep process, depending on which level of analysis you want to have performed.

The process described here to enable attachment and URL analysis applies to all customers with an Cisco-hosted sensor and for customers with an on-premise sensor that was installed on or after the 18.05.21222056 release (May 2018), meeting the host system specifications for that release.

Customers hosting their own on-premise sensor prior to the 18.05.21222056 release, will likely need host upgrades and to contact Cisco support to request that the Attachment Scanning and URI Scanning switches be enabled. Once this is done you can continue with the processes below to enable attachment and URL analysis.

## Basic Attachment Information Collection

To allow attachment and URL scanning, you must enable an organization level setting to allow Advanced Phishing Protection to collect this information. This setting is enabled by default.

1. Go to Manage > Organization.
2. Scroll down to the Sensor Settings section, and in the Message Components setting, select the Process message contents check box to enable this for your organization.
3. Click Save.

Once the organization allows attachment and URI scanning, the functionality is enabled on a sensor level, and on a per-sensor basis.

If you do enable this setting, but do not enable attachment scanning for any sensor, Advanced Phishing Protection will still perform basic collection of attachment information, such as name and file extension, which can be used in Search and Policy.

## Attachment Scanning

Scanning of attachment content for malicious intent must be enabled on a per-sensor basis. If you manage your own sensor environment you may choose to only scan attachments on a subset of your sensors, routing email with attachments to those specific sensors. If your sensors are hosted by Cisco (which is the recommended configuration), you should enable scanning on all sensors.

Attachment scanning may require upgrades to your sensor host system VM or machine. You will also need to open a new firewall hole for these sensors. See "Sensor Prerequisites" on page 21 for information about sensor host system specifications.

First you must perform the steps above to set your organization level policy on attachment name collection.

1. Go to Manage > Sensors.
2. Scroll down to the Configuration section.
3. Move the Attachment Scanning slider to Scan Attachments.
4. Click Save Configuration.

The first time you enable attachment scanning on a sensor you manage in your own environment (not Cisco-hosted) will involve downloading the scan engine container in the background, after which your sensor will restart. This process can take more than 30 minutes. We recommend you perform this action one sensor at a time.

If you have multiple sensors, repeat these steps on each tab for which you want the sensor to perform attachment scanning.

## URL Scanning

Scanning of URLs for malicious intent must be enabled on a per sensor basis. If you manage your own sensor environment you may choose to only scan URLs on a subset of your sensor appliances, routing email with attachments to those specific sensors. If your sensors are hosted by Cisco (which is the recommended configuration), you should enable scanning on all sensors.

Advanced Phishing Protection can also scan URLs in Microsoft Office and Adobe Acrobat documents that are attached to messages, but attachment scanning must also be enabled for this to occur.

URL scanning may require upgrades to your sensor host system VM or machine. You will also need to open a new firewall hole for these sensors. See "Sensor Prerequisites" on page 21 for information about sensor host system specifications.

First you must perform the steps above to set your organization level policy on URL collection.

1. Go to Manage > Sensors.
2. Scroll down to the Configuration section.
3. Move the URI Scanning slider to Scan URIs.
4. Click Save Configuration.

If you have multiple sensors, repeat these steps on each tab for which you want the sensor to perform URL scanning.

## Sender Management and Rapid DMARC

The Senders page in Cisco Advanced Phishing Protection gives you a view of the well known senders that are seen sending messages into your organization using your internal domains. You can quickly see how Advanced Phishing Protection has modeled the traffic from senders for your internal domains and you can also explicitly approve or deny a given sender with a single click. With this understanding of your sender models and ability to make manual adjustments, you can safely implement a Rapid DMARC policy in Advanced Phishing Protection to reject inauthentic messages from your own domains.

### Manage Senders

Go to Manage >Senders to get a view of the Well Known Senders for your domains. The page will be filtered to your highest volume internal domain and show you today's data by default.

To change the domain you are viewing you can click on the up/down arrow next to the domain name.

Any domain you have tagged as "internal" on the Analyze > Domains page will appear in the domain list here.









The page will also be set to view Senders by default, as seen in the image below. To view IP addresses that are not assigned to a well known sender, click the Unassigned IP Addresses tab.

Senders  
Review senders to internal domains  
Show senders for internal domain:

Today | 7 days | 2 weeks | Month

Senders Unassigned IP Addresses

Displaying 1 - 19 of 19 IP Addresses

| Sender                                                                              | Inbound  |              | Authenticity |        | Action                                    |
|-------------------------------------------------------------------------------------|----------|--------------|--------------|--------|-------------------------------------------|
|                                                                                     | Messages | IP addresses | Score        | Reason |                                           |
|    | 237      | 2            | 0.9          | Manual | <span>✓ Approved</span> <span>Undo</span> |
|    | 2        | 2            | 0.1          | Manual | <span>✗ Denied</span> <span>Undo</span>   |
|    | 5665     | 1            | 1.0          | Model  | <span>+ Approve</span> <span>Deny</span>  |
|    | 101      | 5            | 0.9          | Model  | <span>+ Approve</span> <span>Deny</span>  |
|    | 1        | 1            | 0.9          | Model  | <span>+ Approve</span> <span>Deny</span>  |
|    | 646      | 5            | 0.8          | Model  | <span>+ Approve</span> <span>Deny</span>  |
|  | 524      | 18           | 0.8          | Model  | <span>+ Approve</span> <span>Deny</span>  |
|  | 6        | 2            | 0.3          | Model  | <span>+ Approve</span> <span>Deny</span>  |

Displaying 1 - 19 of 19 IP Addresses << Previous 1 Next >> IP Addresses Per Page: 25

he Senders page

## Column Meanings and Usage

**Sender:** The name/logo of the Well Known Sender. Clicking on the sender will drill down a level and show you message counts from individual IPs.

**Inbound - Messages:** The number of messages seen from this domain/sender combination in the time period specified.

**Inbound- IP addresses:** The number of IP Addresses seen sending those messages from this domain/sender combination in the time period specified.

**Authenticity - Score:** This is the average global authenticity score from Agari's sender modeling for this sender/domain combination.

The Authenticity Score displayed here is an average for all messages from all IPs associated with this sender/domain combination seen across the Agari platform for the entire time period. Therefore, as you drill down into any specific message it is normal and expected that there are variations in the authenticity score on a single message.

**Authenticity - Reason:** How we determine the authenticity score.

Manual means the sender was manually approved or denied. The average authenticity will not immediately change upon approval or denial of a Sender or IP address, but new messages from that sender/domain or IP/domain combination will begin receiving either a 1.0 authenticity if approved or a 0 authenticity score if denied within minutes of the change.

Model means that the scored was calculated based on Advanced Phishing Protection's sender modeling.

Authenticated means the most of the messages seen from that sender/domain combination are passing the authentications standards with full DMARC alignment.

Action: These are the actions you can take to Approve or Deny a sender or to Undo a previous approval or denial.

Undo will revert a sender to a state where it is modeled by Advanced Phishing Protection's sender modeling. You may undo an approval or denial at any point in time.

Approve will explicitly approve a sender for that domain, ensuring that future messages from that sender will be considered authentic by Advanced Phishing Protection.

Deny will explicitly deny a sender for that domain, ensuring that future messages from that sender will be considered inauthentic by Advanced Phishing Protection.

## Sender Management With Rapid DMARC

As with public DMARC policies, in Rapid DMARC you must have your senders properly authenticated in order to safely enforce a policy to delete or quarantine inauthentic messages from your domains.

The difference is that Rapid DMARC sender management is fast and easy. You simply look at the senders and IPs for your internal domains and see how Advanced Phishing Protection has modeled them. If you agree with the models, there is no need for further action, although you may choose to explicitly approve your large senders. If you have senders that are difficult to align identities for with public DMARC, you don't have to worry about that for Rapid DMARC. There is no need to contact the sender and implement DNS changes; just click "Approve" on your Senders page and you're done.

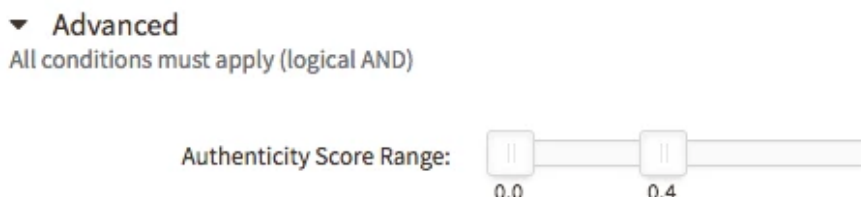
Once you are comfortable with your senders in Advanced Phishing Protection, you can move the Manage > Policies page and set up your Rapid DMARC policy for enforcement.

Customers on-boarded starting in January of 2018 have a default Rapid DMARC policy that is already created for you.

1. Go to Manage > Policies.
2. Click the Rapid DMARC policy name.
3. Under the policy name, move the slider to Enable.
4. Scroll down to the Actions section to set up your enforcement action for this policy and to enable an alert on policy matches.
5. Click Save.

Customers that were set up in Advanced Phishing Protection before January 2018 did not receive a Rapid DMARC policy. You can create your Rapid DMARC policy with these steps:

1. Go to Manage > Policies.
2. Click Create Policy.
3. In Policy Name enter " Rapid DMARC" .
4. Scroll down to Domain Tags and click in the empty box. Select internal from the list of available domain tags.
5. Scroll down and open the Advanced toggle.
6. Move the top end of the Authenticity Score Range to 0.4. It should look like this:



7. Click Save.

## Address Groups

Address groups are simply named groups of one or more, up to 1000, email addresses. Address groups are used often in policies, and can be used for the following reasons:

- To identify spoofs of a set of your users. When you specify an address group in the From field of a policy, the policy will match on display name spoofs of members of that group. By default, the Trust Score of messages identified as display name spoofs will be lowered. To do policy matching with an address group but not affect the Trust Score, clear the Use this group to affect message scoring policy setting. A detailed example of address group matching in the From field is below.
- To filter a policy based on a group of message recipients. When you specify an address group in the To field of a policy, then the policy will only match if the message recipient is in the address group. Using an address group in the To field never affects message scoring.
- To filter a policy based a group of Reply-To addresses. When you specify an address group in the Reply-To field of a policy, then the policy will only match if the Reply-To address is in that address group. Using an address group in the Reply-To field never affects message scoring.

When you create a new organization, three address groups are pre-created for you:

- Executives (automatically associated with the *Executive Imposters* policy, see " Default Policies" on page 120 for details)
- C-Level Executives (automatically associated with the *C-Level Imposters* and *Suspicious Messages to C-Level* policies, see " Default Policies" on page 120 for details)
- Top Partners and Vendors (automatically populated with up to 1000 email addresses from domains tagged Partner or Vendor, see " Domain Tags" on page 116 for details)

One of the first tasks you should do when setting up a new organization is to populate these address groups with your executive and C-level executive email addresses, and then configure the associated policies.

The Top Partners and Vendors address group is updated automatically on a weekly basis. Advanced Phishing Protection detects individuals at partners and vendors (from domains tagged as Partner or Vendor, see "Domain Tags" on page 116 for details) who regularly communicate with employees at your organization and populates the Top Partners and Vendors address group with up to 1000 of these individuals.

## Address Group Exceptions

Addresses in the exception list are for specifying "known good" email addresses of the people in the address group, such as or personal email addresses, to avoid false positives.

For example, suppose that legitimate messages using your company's executives' names are sent from the address <yourco\_announce@example.com>. You can add that email address to the exceptions list for the Executives address group. Now when an authentic message from <yourco\_announce@example.com> is detected, it will not fire an alert based on this address group.

Addresses in the exceptions list are never tagged as impostors unless the message itself is inauthentic, and they are only considered when the address group is referenced by the From and Reply-To conditions in a policy.

You can add addresses such as messenger@webex.com or reply@chatter.salesforce.com so that when a user in your Address Group is spoofed legitimately, such as "John Doe <messenger@webex.com>" or "John Doe <reply@chatter.salesforce.com>" the condition will not match.

You can also add personal addresses such as "johndoe@gmail.com," which may share the Friendly From of addresses above.

Some email services make use of "+" addressing, per the sieve filtering standard. In these cases the local part of an email address will vary with a random text string after the "+" in the address, which can cause problems for setting an exception in an address group. For example "John Doe <notifications+2hef98h2uibf8h@yammer.com>." In these cases, the address group matching will automatically ignore the '+' and all characters between the "+" and the "@." So you could add just "notifications@yammer.com" to the exceptions list to ignore this so it will not match on the John Doe display name.

Some messages are automatically excepted from address group display name matching by Cisco. For example, messages that pass authentication and come from a domain tagged as "internal," "partner," or "service" will not be called an address group match.

## Address Group Examples

The section shows how address groups and policies work together.

## Address Group In the From Field of a Policy

When an address group is referenced in the From field of a policy, the First Name and Last Name of users in the group will be used to identify Imposters of group members in incoming email.

For example, your Genius address group contains Albert Einstein <aeinstein@genius.com> and the group is used in the policy titled Genius Spoofs. Because aeinstein@genius.com is his legitimate business address, anytime authentic email from 'Albert Einstein <aeinstein@genius.com>' is seen in incoming email, Advanced Phishing Protection will NOT trigger the policy because that is a known good source of email for Albert Einstein.

But if email from Albert Einstein <genius\_spoof@not-a-genius.com> is seen coming into your organization, Advanced Phishing Protection will trigger a policy match for the Genius Spoofs policy.

So what if Mr. Einstein sometimes uses his personal AOL address, <IQ160@aol.com>, to send email into your organization? That is the purpose of the exceptions list. If you add IQ160@aol.com to the exceptions list, then authentic email from 'Albert Einstein <IQ160@aol.com>' also will not trigger a policy match for the Genius Spoofs policy.

## Address Group In the To Field of a Policy

When an address group is referenced in the To field of a policy, it is simply a recipient filter for the policy. The policy will apply only when the recipient address is in the address group.

For example, your Genius address group now contains Albert Einstein <aeinstein@genius.com> and Stephen Hawking <shawking@genius.com>. If you now create a policy called Untrusted messages sent to geniuses and put the Genius address group in the To field of the policy, that policy will only match on messages that meet the trust criteria and have aeinstein@genius.com or shawking@genius.com as the recipient. Exceptions do not apply to the use of address groups in the To field.

## Create an Address Group

An address group can be composed of individual email addresses that you add one at a time, or, if you are connected to Azure Active Directory, an address group can be composed of an existing Active Directory group.

### Create an Address Group from Individual Email Addresses

1. Go to Manage > Address Groups.
2. Click Create Address Group.
3. Enter a name. The name should reflect the email addresses you plan to put in the group.
4. Add one or more addresses:
  1. Make sure the Individual tab is selected.
  2. Enter a First Name, a Last Name, and a valid Email Address.
  3. Click Add.
5. If you want to add exception email addresses, enter each valid email address one at a time



and click Add after entering each one.

6. Click Create.


#### Create an Address Group from an Azure Active Directory Group

1. Go to Manage > Address Groups.
2. Click Create Address Group.
3. Enter a name. The name should reflect the email addresses you plan to put in the group.
4. Click the via Azure AD tab.
5. Click in the Azure AD group field.
6. Select an Active Directory group. The names and email addresses from the Active Directory group that contain both first and last names are added to the address group list.
7. If you want to add exception email addresses, enter each valid email address one at a time and click Add after entering each one.
8. Click Create.

## Add an Email Address to an Address Group

1. Go to Manage > Address Groups.
2. Click the name of an address group.
3. In the Add Addresses section, enter a First name, Last name, and Email address.
4. Click Add.
5. Click Save.

## Delete an Email Address from an Address Group



1. Go to Manage > Address Groups.
2. Click the name of an address group.
3. In the Add Addresses list, click the  next to an email address.
4. Click Save.

## Edit an Address Group


If an address group is composed of individual addresses, you can add, edit, or delete any of the address group entries. If the address group is linked to Azure Active Directory, you can only switch the Active Directory group used in the address group.

#### Edit an Address Group Composed of Individual Email Addresses

1. Go to Manage > Address Groups.
2. Click the name of an address group that has a Source of Individually added.

3. Make any desired changes. You can:
  - Change the address group name.
  - Enter a First Name, Last Name, and valid Email Address and click Add to add a member to the address group.
  - Click  next to a name in the address list to delete a member from the address group.
  - Enter a valid email address and click Add to add an exception.
  - Click  next to a name in the exceptions list to delete an exception.
4. Click Save.

#### Edit an Address Group Linked to Azure Active Directory

1. Go to Manage > Address Groups.
2. Click the name of an address group that has a Source of Linked to Azure AD.
3. Make any desired changes. You can:
  - Change the address group name.
  - Click in the Azure AD group field and select an Active Directory group.
  - Unlink a synchronized address group.
  - Enter a valid email address and click Add to add an exception.
  - Click  next to a name in the exceptions list to delete an exception.
4. Click Save.

#### Unlink an Address Group Linked to Azure Active Directory

You can tell an Address Group is synchronized with Azure Active Directory by looking at the Source column on the Manage > Address Groups page. You will see Linked to Azure AD. Other statuses include Individually Added, Manually Unlinked from Azure AD, and Automatically unlinked from Azure AD.

| Source                               |
|--------------------------------------|
| Linked to Azure AD                   |
| Linked to Azure AD                   |
| Manually unlinked from Azure AD      |
| Individually added                   |
| Automatically unlinked from Azure AD |
| Manually unlinked from Azure AD      |

The Source column of the Address Group index page

1. Click the name of a linked group to get to the Edit Address Group page. Below the box of names on the right side you will see a link to Unlink Azure AD Group.

Add Addresses: Azure AD group:

You cannot sync to AD groups with more than 1000 users.

| First Name | Last Name | Email Address <sup>▲</sup> |
|------------|-----------|----------------------------|
| Nathan     | it        | nt@metrics.com             |

Group last updated: 30-Mar-2018 18:03:45 PDT ⓘ

[Refresh now](#) 1 total address

[Unlink Azure AD Group](#)

2. Click the Unlink Azure AD Group link. This will stop the group from further synchronizing with Azure Active Directory, but it will maintain the current group membership. At this point you can manually modify the group and your modifications will not be overwritten by the next sync.
3. Click Save.

## Delete an Address Group

You cannot delete an address group that is being used in a policy.

1. Go to Manage > Address Groups.
2. Click the name of an address group.
3. At the bottom of the page, click the Delete [address group name] link.
4. Click OK.

## Azure Active Directory Synchronization With Address Groups

Manage your address group-based policies more efficiently by syncing Advanced Phishing Protection Address Groups with your Azure Active Directory groups. Advanced Phishing Protection will automatically pull the members from your Azure AD groups into a synchronized Advanced Phishing Protection address group so that you no longer have to worry about manual updates.

To learn about how address groups are used in policies, see "Policies" on page 119.

### Notifications of Azure AD group sync failures

After setting up synchronized address groups it is recommended that you sign up for system notifications about failures to of the regular sync jobs.

1. Go to Manage > Policies.
2. Click on the System Notifications tab.
3. Scroll down to the Policies section and select the Azure AD sync fails to sync an Address Group within a day check box.
4. Click Save.

See "Notifications" on page 118 for more information.

## Skipped Addresses

When Advanced Phishing Protection synchronizes with an Azure Active Directory address group that contains any entry with a missing first name, last name, or email address, those entries will not be included in the address group. Instead, Advanced Phishing Protection will add a Skipped Addresses section to the address group and list those entries in that section.

Group Name:

Use this group to affect message scoring

Add Addresses: Azure AD group:

You cannot sync to AD groups with more than 1000 users.

| First Name | Last Name     | Email Address            |
|------------|---------------|--------------------------|
| [REDACTED] | ORLOMMO       | [REDACTED]@[REDACTED].cl |
| [REDACTED] | [REDACTED]    | [REDACTED]@[REDACTED].mx |
| [REDACTED] | [REDACTED]    | [REDACTED].com.co        |
| [REDACTED] | Quelido Costa | [REDACTED].com.br        |
| [REDACTED] | [REDACTED]    | [REDACTED].mx            |

Group last updated: 16-May-2019 15:39:16 EDT

[Refresh now](#)

157 total addresses

[Unlink Azure AD Group](#)

Skipped Addresses

Addresses are skipped if they do not provide a first name and last name. (For example, external addresses.)

A Skipped Addresses section in an address group.

## Authorize Address Group Synchronization

To set up Address Group synchronization, you must first authorize Cisco to sync with your Azure Active Directory.

1. Go to Manage > Address Groups.
2. Click Enable Azure AD Sync.

### Address Groups

Create, view, and manage groups of email addresses.

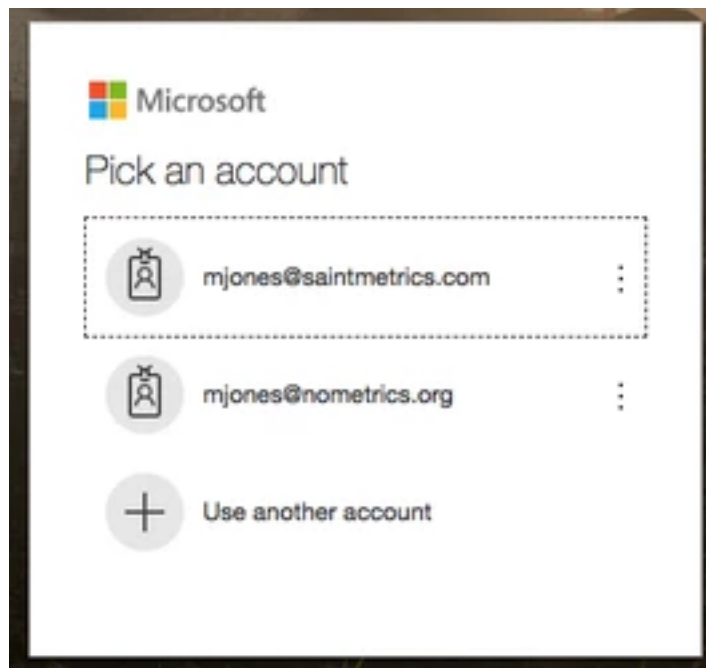
[Create Address Group](#) [Enable Azure AD Sync](#)

Displaying 1 - 2 of 2 Address Groups

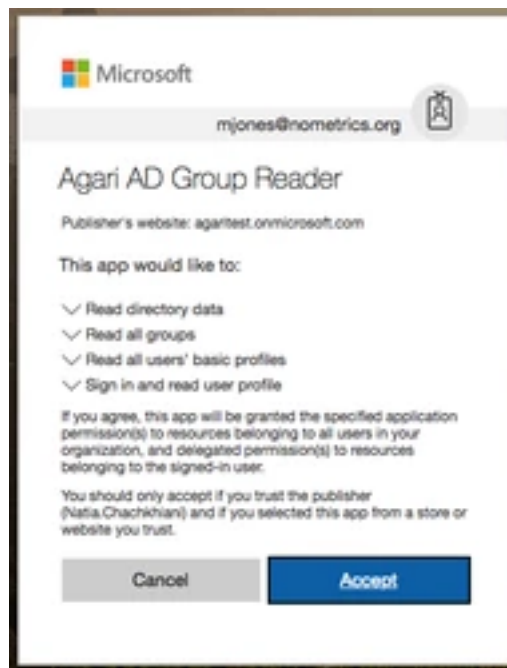
| Name                        | Email Addresses | Referenced By Policy(s)   | Used in Scoring |
|-----------------------------|-----------------|---------------------------|-----------------|
| Executives - Previous Execs |                 | Executive Imposter - Live | Y               |
| Executives                  |                 | Executive Imposter - Live | Y               |

Displaying 1 - 2 of 2 Address Groups Address Groups Per Page: 25

3. You will be presented with a dialog to connect with Azure AD and grant permission. Login as an account that has appropriate administrative permissions.
4. You will be directed to Microsoft to select the account that you will use to grant consent and asked to login to that account.



5. Upon login you will be presented with the option to approve the Agari AD Group Reader application. Click Accept.



After approving you will be directed back to the Advanced Phishing Protection application and will be authorized to sync groups with Azure Active Directory.



## CHAPTER 7

# Administration

Advanced Phishing Protection administration includes defining an organization's settings, reviewing the activity in an organization, and managing Advanced Phishing Protection users in an organization.

You can make changes to the organization settings, view the audit trail, and manage users only if you have the Organization Administrator role.

## Organization Settings

Organization settings determine how Advanced Phishing Protection works in your organization. You manage your organization on the Edit Organization page. The Edit Organization page contains tabs on which settings are collected, and each tab contains sections of related settings. Here, you configure the following categories of settings:


- Administrative
- Organization
- Report
- Sensor
- Enforcement
- User Account
- Processing Exceptions

To view organization settings, go to Manage > Organizations, and then click the organization name.

You can make changes to the organization settings only if you have the Organization Administrator role. (Certain settings require higher-level roles that are available only to Cisco administrators. If you do not see a setting in your view or you cannot change a setting, this is likely the reason.)

## Administrative Tab

| Setting           | Description                                                                                                                                                                                     |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | <b>Administrative</b>                                                                                                                                                                           |
| Organization Name | The name of your organization. This is what you see wherever there is information displayed about or relating to your organization, such as audit trails. You can change the organization name. |

| Setting                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Symbolic Name                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | A unique string created from the initial organization name to uniquely define the organization. This identifier is used by the system and is viewable only here. It cannot be changed.                                                                                                                                                                                                                                                                                                           |
| Subdomain                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | The part of the application URL that is unique to your organization. It is a subdomain of appc.cisco.com.                                                                                                                                                                                                                                                                                                                                                                                        |
| Creation Date                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Shows the date and time that the organization was created.<br>Click  to toggle between local time and UTC ( <a href="#">Coordinated Universal Time</a> ).                                                                                                                                                                                                                                                       |
| <b>Organization Settings</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Primary Administrative Contact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | The organization user selected here will be the person who will receive all administrative contact from Cisco.                                                                                                                                                                                                                                                                                                                                                                                   |
| Organization Type                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Defines if the organization is: <ul style="list-style-type: none"> <li>• Eval: Reviewing Advanced Phishing Protection</li> <li>• Subscriber: Has paid for Advanced Phishing Protection</li> </ul>                                                                                                                                                                                                                                                                                                |
| Expiration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Defines when an organization's subscription expires and is up for renewal.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Classification Settings</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| An organization's classification settings are used for reporting, especially for comparing an organization's aggregate data to industry peer aggregate data. See "Reports" on page 134 for more information.                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Region                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | This is used to determine geographic peers.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Industry                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | This is used to determine industry peers. If your organization isn't categorized by one of the defined choices, select Other.                                                                                                                                                                                                                                                                                                                                                                    |
| Mailboxes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | This is used to determine peers based on mailbox size range as a proxy for organization size.                                                                                                                                                                                                                                                                                                                                                                                                    |
| Exact mailbox count                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Enter the actual number of mailboxes in your organization.<br>This should be a number in the range you selected above.                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Messages Settings</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| An organization's message settings determine what messages Advanced Phishing Protection will ingest. These settings are only available if the Messaging Platform setting in the Sensor Settings section is <i>Microsoft Office 365 or Exchange Online (journaled)</i> or <i>Microsoft Exchange Server (journaled)</i> . You will also need to have journaling configured correctly, as explained in "Configure Dual Delivery: Office 365" on page 48 and "Configure Dual Delivery: Microsoft Exchange" on page 53. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Evaluate Messages                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Defines what messages are ingested. Select from: <ul style="list-style-type: none"> <li>• Inbound messages - Only messages sent into your organization are ingested and evaluated by the Sensor.</li> <li>• All messages (Inbound, Internal, Outbound) - All messages sent into your organization, out of your organization, and within your organization are ingested and evaluated by the Sensor. This selection requires that messages are journaled and that you identify domains</li> </ul> |




| Setting                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | for which you accept email.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Accepted Domains                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <p>Defines the domains for which you accept messages. Required if you select <i>All messages</i> in Evaluate Messages.</p> <p>This should be a list of your domains, including subdomains, that receive your email messages. For example, mycompany.com is your domain, but you have mail.- mycompany.com as your email server. These, (and possibly others) should be in this list. Advanced Phishing Protection uses this list to help determine message directionality.</p> <p>Any domains that you have tagged as internal (see " Domain Tags" on page 116) are automatically added to this list.</p> |
| <b>Report Settings</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <p>The Report Settings section is where you define the threshold you want in all the reports for each attack type. For each attack type, you can select:</p> <ul style="list-style-type: none"> <li>• Untrusted - Message Trust Score between 0.0 and 1.0</li> <li>• Untrusted and Suspicious - Message Trust Score between 0.0 and 5.0</li> </ul> <p>Messages with a Trust Score of between 0.0 and 1.0 (on a scale of 0.0 to 10.0) are considered untrusted. Messages with a Trust Score greater than 1.0 and up to 5.0 are considered suspicious. This setting allows you to define whether you want reports for each attack type to contain only untrusted messages or both untrusted and suspicious messages.</p> <p>The default for all attack types except Domain Spoof is <i>Untrusted and Suspicious</i>.</p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Sensor Settings</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <p>The Sensor Settings section refers to global sensor settings for the organization. Choose which components of messages are uploaded for analysis by Cisco. Cisco recommends that you enable all message components.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Operational Mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Defines how the sensor is placed in the email infrastructure. See " Configuring Delivery to the Sensor" on page 42 for more information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Messaging Platform                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <p>Defines the messaging platform. Select:</p> <ul style="list-style-type: none"> <li>• G Suite (formerly Google Apps for Work)</li> <li>• Microsoft Office 365 or Exchange Online (journaled)</li> <li>• Microsoft Exchange Server (journaled)</li> <li>• Other</li> </ul>                                                                                                                                                                                                                                                                                                                               |
| Original-To Header Name                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <p>Used only for Sensor processing overrides. Leave as-is unless instructed otherwise by Cisco.</p> <p>When a value is entered in this field, the value replaces the Original-To Header when the message is processed by the Sensor. This can help you identify Sensor-processed messages when you are creating policies.</p>                                                                                                                                                                                                                                                                             |
| Original-Mail-From Header Name                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Used only for Sensor processing overrides. Leave as-is unless instructed otherwise by Cisco.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Setting                                                                                                                                                                                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Internal MTA IPs                                                                                                                                                                                                       | <p>List IP addresses for any upstream MTA sending traffic that you want to capture. The form accepts CIDR notation for specifying ranges of IP addresses.</p> <p>Use this only in the case of upstream MTAs.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Allowed Forwarding IPs                                                                                                                                                                                                 | <p>Determines the IP addresses from which Sensors will accept forwarded messages. One or more IP addresses entered in this field will prevent mail forwarding from any IP address not listed.</p> <p>This is generally used for heightened security measures, and is typically left blank</p> <p>This also affects the testing of SMTP connections.</p> <p>To add an IP address to the list, enter an IP address into the <i>IP Address</i> field, and then click Add. The IP addresses in this list should be only the IP addresses of the servers in your email infrastructure that forward messages to Sensors.</p>                                                                                                                                                                                                                                                                                                     |
| Message Components                                                                                                                                                                                                     | <p>Determines which components of messages to upload to the sensor for analysis. Cisco recommends analyzing all available message components. All components are selected by default.</p> <p>The "Include" options (subject header and full from, reply to, and recipient) allow the sensor to better analyze the message metadata, resulting in more accurate scoring.</p> <p>The Process message content option allows the sensor to extract only any attachments and URIs from the body of the message and analyze only those components for maliciousness. Non-attachment and non-URL content is not analyzed and is discarded immediately after attachment and URL extraction.</p>                                                                                                                                                                                                                                    |
| <b>Enforcement Settings</b>                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <p>Enforcement allows you to create policies that move messages to a designated folder in the end-user's inbox. Enforcement is available for Gmail, Office 365, and Exchange Web Services (EWS) environments only.</p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Enforcement                                                                                                                                                                                                            | <p>When set to Enable, allows policies to enforce rules on messages based on policy settings.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Enforcement Label(s)                                                                                                                                                                                                   | <p>The default enforcement folder can be changed and additional folders set in the Enforcement Settings. These folders are displayed in the Enforce Actions for all Policies and are the names of the folders or labels that end users will see in their mail client:</p> <div data-bbox="852 1753 1144 1837" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Actions<br/>Enforce and notify actions are optional; all messages matching conditions of a saved policy are tagged in the Policy Log.</p> <p>Enforce: <input checked="" type="checkbox"/> Enforce action</p> <p>Notify: <input type="checkbox"/> Notify action</p> <p>Move to folder: "Cisco-Quarantine" (different enforcement actions, 1 in Enforcement Settings)</p> <p>Move to folder: "Cisco-Spam" (different enforcement actions, 1 in Enforcement Settings)</p> <p>Move to Inbox</p> </div> <p>Enforcement actions in a policy</p> |
| <b>User Account Settings</b>                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Setting                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Single Sign-On                | Determines whether your users need to enter a password in addition to their user name to access Advanced Phishing Protection or whether they can use your existing authentication. See "Single Sign-On (SSO)" on page 175 and "Enable Single Sign-On for Your Organization" on page 175 for more information.                                                                                                                                                                                                                                                                                                                                    |
| Session Inactivity Logoff     | Determines how long users can stay signed in to Advanced Phishing Protection before they get signed out automatically. The default is 4 hours.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Session Absolute Logoff       | <p>Determines how automatic log off happens. Select from:</p> <ul style="list-style-type: none"> <li>• Relative (default): Automatic log off happens if no activity in Advanced Phishing Protection happens within the time period set in the Session Inactivity Logoff setting.</li> <li>• Absolute: Automatic log off happens when the time period set in the Session Inactivity Logoff setting expires after log in. In other words, the Session Inactivity Logoff clock starts at log in and does not reset for any user activity. This setting may result in users being logged off while they are in the middle of an activity.</li> </ul> |
| Password expiration           | Determines the time period before users have to select a new password. The default is Never.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Maximum failed login attempts | Determines how many times a user can attempt logins without success before being locked out and requiring a new activation link to be sent. Select Disabled if you do not want to limit login attempts.                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Password policy               | <p>When you require a password for login (non-SSO), determines the minimum complexity of the password. The default is</p> <ul style="list-style-type: none"> <li>• Minimum length: 10 characters</li> <li>• Minimum upper case characters: 1</li> <li>• Minimum lower case characters: 1</li> <li>• Minimum symbols (non-alpha-numeric characters): 1</li> <li>• Minimum numbers: 1</li> <li>• Prevent password reuse for N past passwords: 0</li> </ul> <p>Select Custom to modify any of these password characteristics for your users.</p>                                                                                                    |

## Processing Exceptions Tab

| Setting                      | Description |
|------------------------------|-------------|
| <b>Processing Exceptions</b> |             |

| Setting                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                 | <p>Processing exception settings are rules that tell Advanced Phishing Protection which messages it should not evaluate process. Messages that meet any of these rules will not be evaluated by the Sensor, scored for any threats, or managed by any policies. Messages that are not processed by Advanced Phishing Protection cannot be searched for, nor will they appear, individually or cumulatively, in any reports.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Office 365 Spam Processing      | <p>For Office 365 organizations only.</p> <p>When a message is sent through Office 365 spam filtering, it is assigned a spam score, which is mapped to a spam confidence level (SCL) rating. Spam scores of 5 and above are considered spam by Office 365 and are moved by default to users' Junk folders. (Source: <a href="#">Spam confidence levels.</a>)</p> <p>Some organizations have configured a different spam score on Office 365 for which messages are sent to users' Junk folder. Because you generally do not want Advanced Phishing Protection to process messages that Office 365 has already determined to be spam, the optimal value for this setting is the same as the organization's Office 365 value.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Message Scoring Exception Rules | <p>Defines message rules, rules that tell Advanced Phishing Protection for which messages to skip any processing. These rules act similarly to message-handling rules in email clients. You select the rule type and enter a value for that type.</p> <p>Available rules are for headers found in messages, headers that include:</p> <ul style="list-style-type: none"> <li>• IP address or CDR</li> <li>• MAIL FROM domain</li> <li>• From:</li> <li>• To:</li> <li>• Subject:</li> <li>• X-Header</li> </ul> <p>To add an exception rule, select a rule type, enter a single value, click Add Exception, and then click Save.</p> <p>The value field accepts only one value (or in the case of X-Header, an X-Header itself and optionally an X-Header value), and does not support wild cards or regular expressions. It is a strict exact text match only (except for Subject, where any subject must contain the entered value anywhere in the message subject to match), and validates for correct values before you can add the exception rule.</p> <p>To delete an exception rule, click the  next to a rule, then click Save.</p> |

## Audit Trail

Advanced Phishing Protection creates a thorough and detailed audit trail to document and authenticate all activity in an organization. All activity is listed in reverse chronological order on the Audit the activity log pages for both your organization (see "View Organization Activity" below) and each user (see "View User Activity" on page 171) in your organization. The list uses icons to categorize the type of activity.

On the Audit log page, click the "Help" icon (question mark) at the top of the page for more information about searching and using the log.

| Icon | Activity Category                                                                                                                                     |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | Indicates that the user signed in, either of Advanced Phishing Protection itself or an organization in Advanced Phishing Protection.                  |
|      | Indicates that the user signed out, either of Advanced Phishing Protection itself or an organization in Advanced Phishing Protection.                 |
|      | Indicates that the user created, edited, or deleted a user account, policy, or address group.                                                         |
|      | Indicates that the user created, edited, deleted, or performed other actions on a domain.                                                             |
| ◆    | Indicates that the user created, edited, deleted, or performed other actions on a sender.                                                             |
|      | Indicates that the user created a report request.                                                                                                     |
| ⚙    | Indicates that the user created, edited, deleted, or performed other actions on a domain group.                                                       |
| 🕒    | Indicates that a user performed an organization-level activity, such as accepting the Cisco Terms of Service (TOS) or changing organization settings. |

## View Organization Activity

Advanced Phishing Protection creates a thorough and detailed audit trail to document and authenticate all activity in an organization

You must have the Organization Administrator role to view organization activity.

1. Go to Manage > Organizations.
2. Click the Audit link under an organization name.

All of the activity in the Advanced Phishing Protection organization is listed in reverse chronological order. The list uses icons to categorize the type of activity. See "Audit Trail" above for descriptions of each icon.

## User Accounts

User accounts define the credentials and access capabilities of Advanced Phishing Protection users. Advanced Phishing Protection uses Role-Based Access Control (RBAC), which allows you to assign each user one or more roles for access to Advanced Phishing Protection functionality.

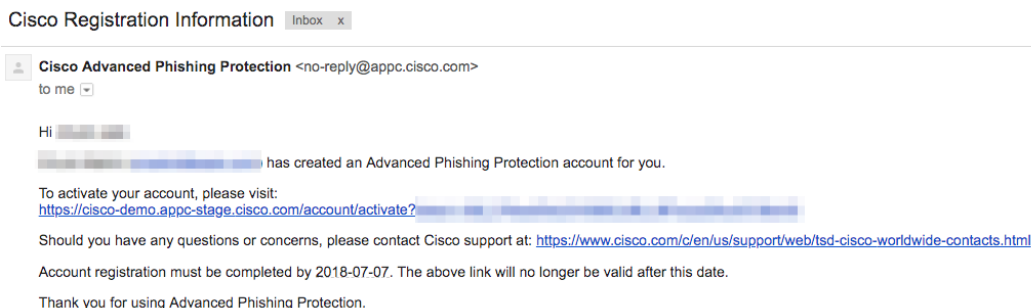
Cisco support personnel do not have access rights to create, enable, edit, or delete user accounts in your Domain Protection organization.

## Create a User Account

Only users with the Organization Administrator role can create user accounts.

1. Go to Manage > Users.
2. Click Create User.
3. Enter a Full Name and an Email address.

You must enter a valid email address. The email address is where the invitation email message is sent. The invitation email message contains a unique link that the new user must click to validate the new account.



A sample invitation email message.

4. Select if you want this user account to be allowed to use secondary authentication (local authentication in the form of a password) in addition to or instead of single sign-on (see "Single Sign-On (SSO)" on page 175 for details). If you select this option, then also choose:
  - Only when Single Sign-On Fails - To allow this user account to enter a password when single sign-on does not work.
  - Exclusively (Do Not Authenticate via Single Sign-On) - To limit this user account to local authorization only, that is, the user will always have to enter both a username and password and cannot use SSO.
5. Select the roles that you want the user account to have. See "User Roles" on page 173 for more information.
6. Click Invite New User.

An email will be sent to the email address you entered with a link to validate the user and for the user to set an account password.

Your sales representative must enable the very first administrator account for accessing Advanced Phishing Protection. Typically, the very first account is assigned multiple administrator roles, including the Organization Administrator role so that you can create additional user accounts for your organization.

## Edit a User Account

1. Go to Admin > Users.
2. Click the name of a user.
3. Make any desired changes to the user information and settings. See "User Account Settings" on the next page for details.
4. Click Update.

## Delete a User Account

1. Go to Admin > Users.
2. Click the name of a user.
3. In the lower right, click the Delete [username] entirely from... link.
4. Click OK.

## Sign In to Advanced Phishing Protection

Before you can sign in to Advanced Phishing Protection, you must have an account created for you (see "Create a User Account" on the previous page), and then you must have clicked on the link in the welcome email to verify your email address.

1. In a supported browser, go to the Advanced Phishing Protection URL: <https://ap-pc.cisco.com>.
2. Enter your email address.
3. Optionality, if your organization has not enabled single-sign-on (SSO), enter your password.
4. Click Next.

## View User Activity

Advanced Phishing Protection creates a thorough and detailed audit trail to document and authenticate all user activity. You must have the Auditing User role to view user activity.

1. Go to Admin > Users.
2. Click the Audit link under a user name.

All of the user's activity in the Advanced Phishing Protection organization is listed in reverse chronological order. The list uses icons to categorize the type of activity. See "Audit Trail" on page 169 for descriptions of each icon.

You can also click Download CSV to download a comma-separated values text file with all the records of a user's activity.

## Configure Global User Account Settings

Global user account settings include how users log on, when they are logged off, and password policies.

User Account Settings

Single Sign-On:  Enable

If Single Sign-On is enabled for the users in an organization, some of the following settings may be overridden by the Identity Provider used for authentication. Refer to the documentation for the Identity Provider for specific settings regarding failed login attempts and password policy.

Session Inactivity Logoff:

Session Absolute Logoff:  Relative  Absolute

Password expiration:

Maximum failed login attempts:

Password policy:  Default  Custom

Ingest:  Disabled  Enabled

Parsing:  Invalid  Valid

### The User Account Settings section

1. Go to Manage > Organizations.
2. Click on the Organization name.
3. Make any desired changes in the User Account Settings. See the User Account Settings section in "Organization Settings" on page 163 for details.
4. Click Save.

## User Account Settings

This topic describes the settings for Advanced Phishing Protection user accounts.

### User Information

| Setting                  | Description                                                                                                                                                                                                                                                                                                                                            |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Full Name                | The user's full name for display, as shown in the list of users, at the top of each page while the user is logged in, and in the audit logs of activity.                                                                                                                                                                                               |
| Email                    | The user's email address, which is used for the user's login credentials as well as the destination address for reports and alerts. Note that this email address used for the invitation email with the initial activation token.                                                                                                                      |
| Secondary Authentication | If your organization uses single-sign on (SSO), this option determines whether secondary authentication (username and password) is optional or required. If you do not select this option, SSO is always used, and if the SSO provider is unavailable at the moment of sign in, application access is not possible. If you select this option, you are |



| Setting | Description                                                                                                                                                                                                                                                                                                 |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | <p>then given two additional options:</p> <ul style="list-style-type: none"> <li>• Only when SSO fails: The user is prompted with a password field if the SSO provider fails</li> <li>• Exclusively (do not authenticate with SSO): The user is always prompted for a password (SSO is not used)</li> </ul> |

In addition, users are assigned one or more roles. See "User Roles" below for information about Advanced Phishing Protection user roles.

## User Roles

This topic describes the user roles that you can assign user accounts in Advanced Phishing Protection. Roles in Advanced Phishing Protection are divided into two categories:

- User roles, which are read-only roles that allow users to only view specific areas in Advanced Phishing Protection, the "R" in the common "CRUD" (create, read, update, delete) paradigm.
- Administrator roles, which allow users to make changes in various areas of Advanced Phishing Protection, the "C," "U" , and "D" in "CRUD."

Roles are by default hierarchical. That is, what you assign a user account a role, that account is also assigned all roles "below" the selected role automatically. Roles below the selected role can be unassigned manually.

The following table lists the available roles in order of that hierarchy.

| Role                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Administrator Roles</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Organization Administrator | <p>An Organization Administrator will by default have all permissions of a read-only, auditing, and user administrator unless those roles are specifically unselected. In addition the organization administrator can make changes to organization settings, policies, and address groups:</p> <ul style="list-style-type: none"> <li>• View and edit organization settings at Manage &gt; Organization.</li> <li>• View, create, and edit policy configurations at Manage &gt; Policies.</li> <li>• Create on-demand policies at Search Messages (if applicable to customer configuration).</li> <li>• View, approve, deny, or undo senders and IPs at Manage &gt; Senders.</li> <li>• View metrics and update configurations at Manage &gt; Sensors.</li> <li>• View, create, and edit address groups at Manage &gt; Address Groups.</li> </ul> |
| User Administrator         | <p>A user administrator will by default have all permissions of a read-only user and auditing user unless those roles are specifically unselected. In addition and auditing user can:</p> <ul style="list-style-type: none"> <li>• Create and edit users at Manage &gt; Users.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Role              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>User Roles</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Auditing User     | <p>An auditing user will by default have all permissions of a read only user, unless the read only role is specifically unselected. In addition an auditing user can:</p> <ul style="list-style-type: none"> <li>• View and search user audit logs at Manage &gt; Users.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Read-only User    | <p>A read only user can search and view data in Advanced Phishing Protection, but cannot make changes or edits anywhere.</p> <ul style="list-style-type: none"> <li>• View and search data on all pages under the Analyze menu (Overview, Messages, Domains, IP Addresses, and Search Messages).</li> <li>• View policy configurations on the Manage &gt; Policies page. Cannot create new policies, on-demand policies, or edit policies.</li> <li>• View reports on Manage &gt; Reports.</li> <li>• View senders on Manage &gt; Senders. Cannot Approve, Deny, or Undo senders or IPs.</li> <li>• View metrics and configurations on Manage &gt; Sensors. Cannot modify sensor configurations.</li> <li>• View own user settings and enable API credentials on Manage &gt; Users. Cannot change own user role.</li> <li>• View address group configurations on Manage &gt; Address Groups. Cannot create or edit address groups.</li> </ul> |

## Role Examples

This topic contains examples of how you would configure roles for some specific use cases.

Create a Read Only user who can receive emailed reports and alerts

When you select the Read Only role for a user, the Report Recipient role will also be selected by default. In order to create a read only user who can also receive emailed reports and alerts, simply accept these defaults. If you choose to de-select the Report Recipient role, your read only user will not show up in the list of available users to send a report to or in the list of users who can be subscribed to alerts.

Create a User Admin with Read Only access and who can create other Read Only users

Select User Admin as the highest access role for the user. Since you want this User Admin to only be able to create and manage users with Read Only access and below, you would de-select the “All privileges” option in the “Manage Users” box directly below the User Admin role. Then select the “Read Only” and “Report Recipient” options. Now this user will be able to create and manage users with Read Only and below permissions.

Create a User Admin who can only create other users

Create a User Admin for the sole purpose of creating or editing other users. This role cannot use the product to view data or receive reports and alerts.

Create a new user, then select the User Admin role for the user you are creating, and then de-select all of the roles that were automatically selected beneath User Admin. The User Admin you create is allowed to create other users with “All Privileges” unless you change the setting in the Manage Users box below the User Admin role.

If you would like this new User Admin to be able to create all roles except for Organization Admin and User Admin, select the ‘x’ remove “All Privileges.” Then, use the “Select Role Types” input to select each of the roles except for Organization Admin and User Admin.

## Single Sign-On (SSO)

Advanced Phishing Protection now includes the ability for you to enable a Single Sign-On (“SSO”) mechanism for authenticating users in your organization via the SAML 2.0 protocol.

With Single Sign-On, you can:

- Create a “one-click” login experience. You can bind your existing corporate login identities (accounts) to the Advanced Phishing Protection username, which eliminates the need for a separate Advanced Phishing Protection password.
- Revoke user access centrally. When an employee leaves the company, you can remove Advanced Phishing Protection access within the SSO provider rather than within Advanced Phishing Protection separately.
- Provide optional secondary authentication. You can allow specific users (for example, contractors not available in your identity provider system) to authenticate exclusively with the credentials stored in Advanced Phishing Protection (which effectively bypasses the single sign-on mechanism). You can also allow specific users to authenticate with the credentials stored in Advanced Phishing Protection only in the event when the SSO identity service fails (for example, during outages).

## Logging In With SSO

Your user’s login process with SSO enabled will depend on how you implement SSO.

- For identity provider-initiated SSO, your users will not need to enter a credential or go to the login page. They will initiate their connection to through your organization’s identity service provider and be logged in.
- For service provider-initiated SSO, your users will come to the Advanced Phishing Protection login page at <https://appc.cisco.com> and enter their email address. They will not be presented with a Password field on the Advanced Phishing Protection login page, unless you enable secondary authentication. (Secondary authentication allows a user to log in via a password if necessary.) Instead, users will be redirected to your identity provider. If users are not already authenticated with the identity provider, they will be prompted to authenticate. (Your identity provider may present authentication in several screens.) Once users have authenticated with the identity provider, they are redirected once again to the Advanced Phishing Protection Overview page.

## Enable Single Sign-On for Your Organization

Before you begin, you must get two pieces of information from your single sign-on provider:

- SAML 2.0 Endpoint (HTTP) URL (This is sometimes referred to as the “destination” or “SAML Recipient” in Identity Provider systems.)
- Public Certificate (X.509)

You must have the Organization Admin role to perform this task.

1. Go to Admin > Organization.
2. Click Edit Organization Details.
3. In the User Account Settings section, select Enable Single Sign-On.
4. In the confirmation message, click OK.
5. Enter the SSO parameters:

| Single Sign-On Parameter          | Description                                                                                                                                                                                                                                                     |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name Identifier Format            | Select from: <ul style="list-style-type: none"> <li>• urn:oasis:names:tc:SAML:1.1nameid-format:unspecified</li> <li>• urn:oasis:names:tc:SAML:1.1nameid-format:emailAddress</li> <li>• urn:oasis:names:tc:SAML:2.0nameid-format:persistent (default)</li> </ul> |
| SAML 2.0 Endpoint (HTTP Redirect) | Enter the SAML 2.0 endpoint URL you obtained from your single sign-on provider.                                                                                                                                                                                 |
| Public Certificate                | Enter the entire text of the certificate you received from your single sign-on provider. (It is probably easiest to copy-and-paste.)                                                                                                                            |

6. Click Test Settings to validate the Endpoint URL and certificate values provided by your identity provider. Advanced Phishing Protection calls the Identity Provider with the public certificate credential at the location you enter.

You may be required to authenticate with your Identity Provider if you are not already logged in there.

7. Click Save Settings.
8. In the confirmation message, click OK.
9. Click Update Information.

At this point, Single Sign-On will be enabled and:

- All existing users will receive an email that instructs them to use their Single Sign-On identity provider credentials when accessing Advanced Phishing Protection.
- Users currently logged into Advanced Phishing Protection will continue their sessions without interruption; however, they will be directed to the Identity Provider on subsequent login attempts.



## Application Programming Interface

Domain Protection includes an application programming interface (API) that allows developers within your organization to programmatically access data within Domain Protection.

The Domain Protection API is built on RESTful principles with JSON data representations. Clients authenticate API requests using the [OAuth 2.0 protocol](#). A user account may be assigned one API credential consisting of an API Client ID and Client Secret. The resources and data made available with those credentials is directly tied to the permissions assigned to that user by an account administrator in the Domain Protection user interface.

### Generate API Secret

An API (application programming interface) credential, also known as an API secret, must be generated for a user before that user can use the Cisco Domain Protection API.

Only users with the User Administrator role can generate API credentials.

1. In Cisco Domain Protection, go to Manage > Users.
2. Click a username.
3. In the API Access UID section, click Generate API Secret.
4. Copy and save the API Access UID and secret in a secure place. You will need to enter it on the API Documentation page when you test an API or when you are using an Cisco integration via API.

### View API Documentation

Before you can view the Domain Protection API (application programming interface) documentation, you must first have an API credential generated for your user account. See "Generate API Secret" above for details.

1. In the upper-right of a Domain Protection page, click your name.
2. Click Domain Protection Documentation.