User Guide for Cisco Advanced Phishing Protection

June 22, 2018

Cisco Systems, Inc.
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.
## CONTENTS

### Installing Cisco Advanced Phishing Protection Sensors  1-1

- **Introduction**  1-1
- **Support**  1-1
- **Installing a Cisco Advanced Phishing Protection Sensor**  1-1
  - Questions to Determine Installation Type  1-2
    - Hosted Environment Questions  1-2
    - Dual-Delivery vs. In-Line Installations  1-3
    - Placing Cisco Advanced Phishing Protection Sensors in your Infrastructure  1-4
- **Dual-Delivery Sensor Architecture and Data Flows**  1-5
- **In-line Sensor Architecture and Data Flow**  1-6
- **Prerequisites**  1-7
  - Virtual Machine Hardware Requirements  1-8
  - Firewall Requirements  1-8
    - Firewall Rules: Cisco-Required HTTPS Access  1-9
  - Packages  1-9

### Cisco Advanced Phishing Protection Sensor Installation Script  2-1

- **Running the Script**  2-1
  - Send a Test Email Directly to the Cisco Advanced Phishing Protection Sensor  2-5
    - Troubleshooting Test Email  2-6
    - Install additional Sensors  2-7
    - Planning for Dual Delivery  2-7
    - Interrupting Dual Delivery  2-7
  - Configure Downstream Host to Receive Email
    (In-line only)  2-8
    - Configuring Delivery to the Advanced Phishing Protection Sensor  2-8
  - Configuring Dual Delivery  2-9
    - Specific Dual Delivery Instructions  2-9

### Dual Delivery: Cisco Email Security Gateway  3-1

- **Important Consideration Regarding the “Authentication-Results” Header**  3-1
- **Step 1: Create a Bcc: Filter to Divert Messages**  3-2
- **Step 2: Configure Bounce Handling to the Advanced Phishing Protection Sensor**  3-6
  - System Alerts  3-8
  - Consider Other Whitelisted Email Streams  3-8
Step 3: Whitelist the Alerts Server  3-9
Step 4: Configure Cisco Email Security Gateway to Add an X-Agari-Authentication-Results Header  3-12
Wrapping Up  3-15

User Tasks: Getting Started  4-1
Gaining Access to the Web Application  4-1
Creating/Editing Users  4-2
  User Roles  4-2
Analyzing Incoming Email Traffic  4-3
  Trust Score  4-3
  Attack Classifications  4-6
    Attack Taxonomy  4-7
    Domain Spoof  4-7
    Look-alike Domains  4-8
    Display Name Impostor  4-9
    Compromised Account (Account Take Over)  4-9
  Low Trust Domains  4-10
  Malicious Attachment  4-10
  Legacy Attack Classes  4-11
  Message Details  4-11
The Workflow  4-12
IPs and Domains  4-13
  Domain Details  4-13
  Tagging Domains  4-14
IP Details  4-15
Messages  4-16
Search Messages  4-18
Managing Suspicious Messages  4-18

User Tasks: Policies  5-1
Managing Incoming Mail Via Policies  5-1
  Creating a Policy  5-1
  Actions  5-3
Getting Started with Policies  5-4
  Enable or Disable a Policy  5-5
Creating your own Test Policy  5-5
How Are My Policies Working?  5-7
  Event Log  5-7
  Policy Report  5-7
On-demand Policies  5-8
Contents

On-Demand Policies Index page  5-13
Final Notes  5-14

Administering Cisco Advanced Phishing Protection  6-1
  Administering Cisco Advanced Phishing Protection  6-1
  Advanced Phishing Protection Sensors  6-1
    System Notifications  6-3
    Users  6-3
    Organizations  6-3
  Cisco Advanced Phishing protection Sensor Settings  6-4
  Sender Management and Rapid DMARC  6-5
    Using the Senders Page to Manage Your Senders  6-6
    Column Meanings and Usage  6-6
    Relating Sender Management to Rapid DMARC  6-7
  Attachment Analysis  6-8
    Enabling Attachment Analysis  6-8
      Basic Attachment Information Collection  6-9
      Scanning of Attachments  6-9
    Using Attachment Analysis  6-10
      Using Attachment Analysis Results in Search and Policy  6-10
      Attachment Scan Results  6-11
      Details of the Attachment Scan  6-11
  Azure AD sync with Address Groups  6-12
    Setting up Address Group Sync  6-12
    Creating a Sync’d Address Group  6-14
    Unlinking a Sync’d Address Group  6-15
    Notifications of Azure AD Group Sync Failures  6-17

Single Sign-On (SSO)  7-1
  Logging In  7-3
Installing Cisco Advanced Phishing Protection Sensors

Introduction

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

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

Cisco Advanced Phishing Protection Sensor complements traditional Cisco Email Security Gateway solutions by catching the spear phishing, targeted, low volume, and zero day attacks that typically are the weaknesses of traditional, reactive Cisco Email Security “layers.”

Using the policy engine within Cisco Email Security Gateway, 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.

Support

For support and or questions/updates to this guide, visit http://www.cisco.com/support

For support installing or using Cisco Advanced Phishing Protection Sensor, you can contact the Cisco support team directly at: support@cisco.com.

Installing a Cisco Advanced Phishing Protection Sensor

Cisco Advanced Phishing Protection relies on a Advanced Phishing Protection Sensor to receive a copy of all messages in sent inbound into your organization.
The purpose of the Advanced Phishing Protection Sensor is to collect per-message metadata from your enterprise’s inbound email stream and to relay the metadata to the Cisco Email Security Gateway cloud for analysis. The Advanced Phishing Protection Sensor is intended to be minimally invasive, secure, lightweight (requiring minimal resources), and highly performant.

Questions to Determine 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:
  - Cisco Email Security Gateway - a secure email gateway.
  - 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 Questions

Additionally, if your environment is hosted in G Suite or Office365, these questions will help determine your Advanced Phishing Protection 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 Cisco Advanced Phishing Protection features as soon as possible.
– Minimizing change requests and associated risk with transitioning your installation.

**Dual-Delivery vs. In-Line Installations**

There are two possibilities for Advanced Phishing Protection Sensor deployment: **Dual-Delivery** and **In-line**.

- **Journal / API**
  
  Dual-delivery is the preferred method if installing, because it allows On-Demand enforcement (for Office365 and G Suite customers), and it lowers the risk from client change management.

- **In-line**
  
  In-line sensor installations are primarily used when the client mailboxes have not been migrated to either Office 365 or Google G Suite

**Dual-Delivery**

The Cisco Advanced Phishing Protection 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 Advanced Phishing Protection Sensor. Dual-delivery is typically used for hosted email architectures like Office365 and G Suite.

**Figure 1-1  Dual-delivery installations using Journaling / API mail flow**

Inbound mail sent to the first Email Platform Hop (Cisco Email Security Gateway may or may not be in front):

1. Office 365 or G Suite sends a Journaled copy or bcc: copy of messages to the Advanced Phishing Protection Sensor and continues original delivery.
3. Office 365 or G Suite delivers original messages to mailbox.
4. Sensor will Enforce policy using an API to access individual mailboxes.
5. The Policy Enforcement action occurs at the mailbox based on policy result.
In-Line

In an in-line configuration, the Cisco Advanced Phishing Protection Sensor acts as an MTA: it takes responsibility for accepting the message and delivering it to the next hop (usually another internal MTA). Customers utilizing in-line configurations can use the next-hop MTA to take action on incoming messages based on headers added by the Cisco Advanced Phishing Protection Sensor.

Figure 1-2 Inline Installations Mail Flow

1. Inbound mail sent to MX at Cisco Email Security Gateway.
2. Cisco Email Security Gateway sends to next hop at Cisco Advanced Phishing Protection Sensor for Ingest, scoring, and policy evaluation.
3. Advanced Phishing Protection Sensor Tags message headers with policy result.
4. Advanced Phishing Protection Sensor sends to 1st Email Platform Hop.
5. Exchange Transport Rules Enforce policy action based on tags in message headers.
6. Messages passing through enforcement is Delivered to mailbox.

Note

The Cisco Advanced Phishing Protection Sensor may be referred to by its previous name, the “Collector” in some of the screenshots in this guide.

Placing Cisco Advanced Phishing Protection Sensors in your Infrastructure

Typically, Cisco Advanced Phishing Protection customers provision host systems in their own environments for running Advanced Phishing Protection Sensors. (If preferred, Cisco can host Advanced Phishing Protection Sensors on your behalf in an administratively separate cloud. Contact your Cisco sales engineer if you prefer this method.)

You should install a Advanced Phishing Protection Sensor 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 Advanced Phishing Protection Sensor for IronPort should only “see” messages that have pass through these filters are deemed worthy of delivery.

If you have a hosted infrastructure (like Google Apps or Microsoft Office 365), the same theory applies: you will direct a copy of your mailstream to the Cisco Advanced Phishing Protection Sensor after all other filtering and scanning has taken place.
1. Messages arrive at the Cisco Email Security Gateway or hosted mailstore and are accepted for spam and virus filtering.

2. After first level spam and virus filtering, the Cisco Email Security Gateway delivers a copy of message (via a dual delivery rule or journaling capability) to the Cisco Advanced Phishing Protection Sensor over an SMTP connection, typically on port 25 (although this can be configured to a different port when the Cisco Advanced Phishing Protection 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.
In-line Sensor Architecture and Data Flow

1. Messages arrive at the Cisco Email Security Gateway and are accepted for spam and virus filtering.

Note
It is common in email infrastructures to have a connection blocking step ahead of the Cisco Email Security Gateway which blocks connections from black listed IP addresses. This step is not depicted in this diagram.

2. After first level spam and virus filtering, the Cisco Email Security Gateway delivers messages to the Cisco Advanced Phishing Protection Sensor over an SMTP connection, typically on port 25 although this can be configured to a different port when the Cisco Advanced Phishing Protection 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.

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

b. After messages have been scored and policies evaluated in the Cisco pipeline, the results of the evaluations are communicated back to the Cisco Advanced Phishing Protection Sensor on the enforcement queue. The Cisco Advanced Phishing Protection Sensor will write those results in new message headers. The new message headers will look like:

   new message headers. The new message headers will look like: nsor
There may be more than one X-Agari-Policy-Matched header present in a message.

The value of the X-Agari-Trust-Score header will be one of the following:

- Numeric value between 0.0 - 10 representing the Trust Score (0 is low, 10 is high).
- “None” - indicating scoring of the message was intentionally skipped per a configuration.
- “Unscored” - indicating that the scoring of the message timed out and the message was delivered without being scored.

The messages will then be queued for outbound delivery from the Cisco Advanced Phishing Protection Sensor.

3. Messages are delivered to the configured downstream MTA over SMTP for continued processing and delivery. The downstream MTA can be the same system that delivered the message to the Cisco Advanced Phishing Protection Sensor or a new downstream MTA.

   It is recommended that when the messages are received by the configured downstream MTA that content filters are set up to read the new X-Agari headers and take specific actions based on the policies and/or scores communicated in those headers.

4. Based on the disposition of the message after the final content filtering, messages can be delivered to a final mail store, delivered to quarantine, delivered back into the mail stream at a point desired for further processing, or not delivered at all (i.e. blocked).

Prerequisites

In on-premises deployments, Advanced Phishing Protection Sensors can be installed on bare-metal installs or a hosted virtual machine (VM) of your choice.

The Cisco Advanced Phishing Protection Sensor is distributed by Cisco via an installation script which 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). A container wraps the Sensor application in a complete filesystem containing everything needed to run the application: code, runtime, system tools, and system libraries.

You should obtain the script to install your first Advanced Phishing Protection 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.
Virtual Machine Hardware Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Specification</th>
</tr>
</thead>
</table>
| Operating System  | Modern, 64-bit Linux:  
                  | - Red Hat Enterprise Linux 7.2 or later  
                  | - CentOS 7.2 or later  
                  | - Ubuntu 14.04 or later |
| CPU               | Intel or AMD x86_64  
                  | 2 cores minimum  
                  | 4 cores recommended |
| Memory            | 16GB minimum  
                  | 32GB recommended |
| Disk              | 50GB minimum  
                  | 100GB+ if anticipated email volume is high, allocated to /var or /var/opt/agari |

Firewall Requirements

When a Advanced Phishing Protection 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 Advanced Phishing Protection Sensor:

<table>
<thead>
<tr>
<th>Type</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound: 25 (SMTP)</td>
<td>For receiving stream of inbound, duplicated messages from your Gateway.</td>
</tr>
<tr>
<td>Outbound: 443 (HTTP/S)</td>
<td>HTTP/S requests to the Cisco cloud and other cloud services (details below)</td>
</tr>
<tr>
<td></td>
<td>Note: The Sensor can be configured to use a proxy for outbound HTTP/S connections.</td>
</tr>
<tr>
<td>Outbound: 53 (DNS)</td>
<td>DNS for hostname/IP address resolution.</td>
</tr>
<tr>
<td></td>
<td>Note: if the host system is using <code>ip</code> or <code>nslookup</code> for the DNS resolution, Docker will not replicate that in the container's <code>/etc/resolv.conf</code> file. Instead it will set the DNS to <code>set the and be</code>, and if you have these addresses are not available through the firewall, DNS will fail.</td>
</tr>
<tr>
<td></td>
<td>You may need to set the host's DNS servers to the actual address of the internal DNS servers used in your enterprise.</td>
</tr>
<tr>
<td>Outbound: 123 (NTP)</td>
<td>NTP for time synchronization services</td>
</tr>
<tr>
<td></td>
<td>Note: On RedHat systems, you can verify that NTP is working correctly by issuing these commands:</td>
</tr>
</tbody>
</table>
|                    | `ntpdate`  
|                    | `ntpd`  
|                    | You want the output of the last command to be a `Y` if the NTP server is being accessed. See the RedHat documentation for more information on checking the status of NTP. |
Firewall Rules: Cisco-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.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

Packages

You may need to install some packages manually.

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 – namely RHEL version 7.1 – 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 Cisco’s own customized version of a postfix server for receiving messages.)

  Disable and remove the Postfix server by running this command:

  Disable and remove the Po

- APT

  APT (Advanced Package Tool) is a set of tools for managing packages. APT resolves dependency problems and retrieves requested packages from designated package repositories.

  wget

  Wget is utility for non-interactive download of files from the Web. You may need to use wget to get the EPEL package.

- EPEL (Extra Packages for Enterprise Linux)

  EPEL is a repository of high-quality add-on packages that complement the Fedora-based Red Hat Enterprise Linux (RHEL) and its compatible spinoffs, such as CentOS and Scientific Linux.

  You can obtain EPEL by typing:

  You can obtain EPEL by typing:

  You can obtain EPEL by typing:

  You can obtain EPEL by typing:

  --

  In order to install this package, you will need access through the firewall to:

  - http://dl.fedoraproject.org
  - Docker and RedHat version 6.x.
Docker may not be distributed by default on RHEL version 6.7. If you are running a distribution of RHEL version without Docker, this version can be installed from: https://docs.docker.com/v1.7/installation/rhel/#red-hat-enterprise-linux-6.5-installation

- Docker and CentOS 7.1 and 7.2
  You may have to explicitly define the Docker repository for systems running CentOS 7.1 and 7.2. The following command creates a file in the /etc/yum.repos.d directory with a file that explicitly defines the base URL for Docker:
  ```
defines the base URL for Docker: file in th
defines the base URL f
defines the base URL for Docker: file in the /etc/yum.rep
defines t
defines th
defines the base URL for Docker: file in
def
After creating the file, you can install Docker, and then start the Docker service:
Docker service:install Dock
```

- Python YAML and Python PIP
  Earlier distributions may not have the Python YAML (yet another markup language) and Python PIP (Python Installer Package) packages installed. The Sensor installation script requires these packages. You can install them by issuing these commands:
  ```
  You can install them by i
  You can install them by
  ```

- Python and Python Argparse
  The Sensor installation script also requires the python and python-argparse packages.
  ```
The Sensor installat
The Sensor installation scrip
```
Cisco Advanced Phishing Protection Sensor Installation Script

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

```
engineering reprogrnameorgdatedate
```

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 Advanced Phishing Protection 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:

```
to set the permissions so that the script can be e
```

In addition to the prerequisites mentioned in Installing Cisco Advanced Phishing Protection Sensors, page 1-1, 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 Advanced Phishing Protection 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:

- Print the version of the script.
- Create the directories
- Stops any existing Cisco Advanced Phishing Protection Sensor services, if necessary.
• Extract installation files into a temporary directory.
• Install Docker.
• Install PyYAML (if necessary).
• Install AWS tools (AWS, AWS SSL).
• Prompt for additional UNIX group permissions for the logs and configuration files (optional; the root group will be used by default).
• Prompt for HTTPS proxy configuration (optional).
• Test for access to the correct S3 buckets for uploading data.
• Prompt for TLS certificates and TLS configuration for connections to the Advanced Phishing Protection Sensor (the default is OFF - TLS connection required).
• Prompt for debugging-level log output (OFF by default).
• Move files to appropriate directories; deletes temporary files.
• Upgrade the version of the Advanced Phishing Protection Sensor (if necessary).

An example of the script being run on a 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 Advanced Phishing Protection sensor script:
## Running the Script

### Version number of the script

<table>
<thead>
<tr>
<th>directories</th>
<th>riptshing Protection Sensor Installation Script</th>
</tr>
</thead>
<tbody>
<tr>
<td>directories</td>
<td>riptshing Protection Sensor Installation Scr</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Prot</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Protection Sensor</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Protection Sensor Installation Script</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing P</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Protecti</td>
</tr>
<tr>
<td>• directories</td>
<td>riptshing Protection Sensor Installation Scriptript:e</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Protection Sensor Installation Scriptript:e</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Protection Sensor Installation Scriptript:e Sen</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Protection Sensor</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Protection Sensor Inst</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Protection Senso</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Protection Sensor Installation</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Pro</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Protection Sensor Installation Scriptri</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Protection Sensor Installation Scriptrip</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing P</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Protection Sensor Installation Scriptri</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing r</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Protection Sensor Installation Scriptri</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Protection Sensor Installation Scriptri</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Protection Sensor Installation Scriptri</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Protection Sensor Installation Scriptri</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Protection Sensor Inst</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Protect</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Protection Sen</td>
</tr>
<tr>
<td>directories</td>
<td>riptshing Protection Sensor Install</td>
</tr>
</tbody>
</table>
You can specify UNIX group permissions for access to the logs and configuration data.

You can specify an HTTPS proxy.
At this point, the Advanced Phishing Protection Sensor has been successfully installed. If you have access to the Cisco Advanced Phishing Protection portal, you should be able to navigate to the Manage > Sensors pages and see that the Sensor has connected.

**Figure 2-1 Sensor status**

Status

![Connected to Cisco but not receiving messages]

The Advanced Phishing Protection sensor should phone home after about 2 minutes.

**Next Steps**

After the first Advanced Phishing Protection Sensor has been installed and can connect to Cisco, you can **Send a Test Email Directly to the Cisco Advanced Phishing Protection Sensor, page 2-5**.

**Send a Test Email Directly to the Cisco Advanced Phishing Protection Sensor**

Since 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:

```
create a test message: llation
```
Running the Scriptsh
Running the Scriptshing P
Running the Scriptshing P
Running the Scriptshing Protection
Running the Script
Running the Scriptsh
Running the Scriptshing Protec
Running the
Running the Scriptshing Prote
Runn
Running the Scriptshing Protection

Running the Scriptshing Protection Sensor
Running the Scriptshing Protection Sens
Runnin^Running th^ Running the Scriptsh
Runn^Running * Running the Script
Running the Scriptshing Protection Sensor Installatio
Running the Scriptshing Protection Se
Running the Scriptshing Prote

Running the
Running the Scriptshing Protection Sensor Installation Sc

Running the
Running the Script
R
Running the Scriptshing Protection
Runn

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 If you get line:

...it is likely the Advanced Phishing Protection Sensor is not up and running yet. Try to:

• Look at the Look at the y the Advanced P on the host to see if you can find a line similar to:
  on the host to see if you can find a line similar to:
  If not, the filter 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 Advanced Phishing Protection sensor? If not, wait the full five minutes and then restart the container if the filter has still not started:
• If after restarting the container there is still an issue, consider restarting the entire collector:

If after restarting the container there

Install additional Sensors

Because they are evaluating individual message metadata and discarding the message body, Cisco Advanced Phishing Protection Sensors are highly efficient. Based on the number of inbound messages you plan to duplicate from your gateways, you may want to configure additional Advanced Phishing Protection Sensors for either redundancy or increased throughput. To install an additional Advanced Phishing Protection Sensor, simply run the installation script on a new instance.

A single Advanced Phishing Protection Sensor can process at least 500,000 messages per day with peak throughput of up to 50 msgs/sec. A load balanced, dual sensor configuration is strongly recommended in a production environment for redundancy.

Planning for Dual Delivery

Once a Advanced Phishing Protection Sensor has been installed, you should now configure your Cisco Email Security Gateway(s) to direct a stream of messages to it (dual delivery).

The steps to configure dual delivery differ depending on your type of Cisco Email Security Gateway. See the dual delivery configuration guide for your Cisco Email Security 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 Cisco Email Security 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 replacement; rather. It is designed to look for inauthentic messages that have passed through this filtering.

Interrupting Dual Delivery

There are two points at which messages from the Cisco Advanced Phishing Protection Sensor to Cisco can be interrupted.

• The Cisco Advanced Phishing Protection 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 the Cisco Advanced Phishing Protection web application. The “Ingest Mode” toggle is a safeguard Cisco uses to protect against sudden spikes in traffic from new organizations sending data into the system.
Configure Downstream Host to Receive Email (In-line only)

After the Advanced Phishing Protection Sensor has been installed and connects to Cisco, you must configure the downstream host and port to receive email from the sensor. This configuration is done in Cisco Advanced Phishing Protection portal on the Manage > Sensors page. At the bottom of the page, a section labeled allow you to enter an IP address or hostname and a port number where it says “Deliver scored messages to:”

![Figure 2-2 Configuring a Downstream Host (In-Line Only)]

**Note**

This configuration is made on a per sensor basis and must be saved for each Advanced Phishing Protection sensor you install.

You should wait about 5 minutes after saving these configuration changes for the sensor to receive the changes and update.

After that, you can send a test message directly to the sensor (see “Send a Test Email Directly to the Cisco Advanced Phishing Protection Sensor” on page 5).

### Configuring Delivery to the Advanced Phishing Protection Sensor

Once a Advanced Phishing Protection Sensor has been installed, you should now configure your Cisco Email Security Gateway(s) to direct a stream of messages to it.

The steps to configure delivery differ depending on your type of Cisco Email Security Gateway. See the delivery configuration guide for your Cisco Email Security Gateway.

Delivery should be configured to take place after initial 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 replacement; rather it is designed to look for inauthentic messages that have passed through this filtering.
Configuring Dual Delivery

Once a Advanced Phishing Protection Sensor has been installed, you can now configure your Cisco Email Security Gateway(s) to direct a stream of messages to it.

The steps to configure dual delivery differ depending on your type of 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 Cisco Email Security 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 replacement; rather, it is designed to look for inauthentic messages that have passed through this filtering.

Specific Dual Delivery Instructions

The Dual Delivery: Cisco Email Security Gateway, page 3-1 section of guide explain how to configure dual-delivery for the Cisco Email Security Gateway.
Dual Delivery: Cisco Email Security Gateway

This document describes how to configure dual delivery from Cisco Email Security Gateway environments to the Cisco Advanced Phishing Protection Sensor.

The general procedure is as follows:

**Step 1** Create a Content Filter which uses the `create` action that will copy messages to the Advanced Phishing Protection Sensor.

**Step 2** Configure bounce handling to properly manage unexpected delivery failures.

**Step 3** Confirm that any desired system alerts are in place to inform administrators of any problems.

**Step 4** Consider other whitelisted email streams.

**Step 5** Whitelist the alerts server to ensure that you and your users receive alerts.

**Important Consideration Regarding the “Authentication-Results” Header**

The Advanced Phishing Protection 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 (i.e. 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, Advanced Phishing Protection 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 in this guide.
Step 1: Create a Bcc: Filter to Divert Messages

Step 1 Log into the Cisco Email Security Gateway as an Administrator user.
Step 2 Navigate to Mail Policies > Incoming Content Filters.

Note If your Cisco Email Security Gateway 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 Cisco Email Security Gateway instances.

Step 3 Click Add Filter and name the filter Cisco_collector.
Step 4 In the Description field, provide a reasonable description so that future administrators will understand what the filter is for and whom 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 joeadmin@example.com”
Step 5 Order the filter so that it enables the Advanced Phishing Protection Sensor to receive all messages that are going to be delivered to the end user – that is: after all spam and virus scanning has occurred, and after any other message filtering policy which would drop messages. If you have other advanced filtering uses where a filter triggers immediate delivery and circumvents subsequent filters, you should consider these and place the Advanced Phishing Protection sensor filter appropriately for the desired result: collection of all messages delivered to the user.

The content filter may not need any Conditions. 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. Again, the goal of the content filter is to only work on messages which are going to be delivered directly to the end user: add conditions to this filter as necessary.

Step 6 Click Add Action to associate an action with this filter. In the Add Action window, select Add/Edit Header.
Step 7 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: $enveloperecipients

If (and only if) your Cisco Email Security Gateway is a perimeter Gateway MTA, then also add this header:
- header name: X-Agari-Authentication-Results header data: $Header[‘Authentication-Results’]

Double check all the header names for typos.
Step 8  Before clicking “Submit,” create the primary action for this filter: to BCC the entire message into the Sensor.

- The Email Address for the BCC action can be a route-able address that will reach the Advanced Phishing Protection Sensor, or you can specify the Advanced Phishing Protection Sensor directly (see below).

- 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 Advanced Phishing Protection 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 Advanced Phishing Protection 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 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 Email Security Gateway “SMTP routes” feature. In other words, you can use this field to directly specify the host or IP address of the Advanced Phishing Protection 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.
Step 9

Click OK.

This example shows the above content filter definition (prior to clicking Submit):
Step 1: Create a Bcc: Filter to Divert Messages

**Figure 3-3** Content filter Summary

![Content Filter Summary](image)

**Note**

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

**Step 10** Click **Submit** to save the new filter.

**Step 11** Associate the filter with an appropriate Incoming Mail Policy. Navigate to Mail Policies -> Incoming Mail Policies and 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.

**Step 12** The modified Policy row may look like this:
Step 2: Configure Bounce Handling to the Advanced Phishing Protection Sensor

In order to use minimal Cisco Email Security Gateway system resources, you should configure the system to fail bounce messages rapidly if the Advanced Phishing Protection Sensor delivery fails. In order to accomplish this safely, follow these steps:

Step 1  Provide an email address to which the Bcc: is delivered that is within a unique domain or subdomain which is accepted by the destination host. The “Alternate Mail Host” delivery action should take care of the message being directed to that server; there is no need to create a specific DNS entry for the email address's domain. For the purposes of this example we will continue to use “collector.host” for the domain.

Step 2  Create a Bounce Profile to rapidly fail bounce messages. Navigate to Network > Bounce Profiles and click Add Bounce Profile to create a new entry. Use values as shown here:

To commit the change, click the Commit Changes >> button. 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

Next, create a specific Destination Control for the unique Advanced Phishing Protection Sensor domain described above (“collector.host”, in this example) that references the aggressive Bounce Profile created in the previous step (named “Impatient” in this example). Navigate to Mail Policies > Destination Controls and create an entry with values shown in the following figure:
If your Advanced Phishing Protection 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 Email Security Gateway will now connect securely to the remote Sensor (over port 25 via “STARTTLS”).

**Step 4** Once properly configured and submitted, click **Commit Changes >>**.

---

**System Alerts**

Navigate 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.

**Consider Other Whitelisted Email Streams**

You may have firewall rules in place that whitelist upstream MTAs sending mail to your Cisco Email Security Gateway. 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 Advanced
Phishing Protection 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 3: Whitelist the Alerts Server

When an email is deemed suspicious, Cisco 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 Advanced Phishing Protection Sensor and the overall health of the Cisco Email Security Gateway 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.

These instructions describe adding the alerts server to your whitelist.

Step 1  On the Cisco Email Security Gateway, navigate to Mail Policies > HAT Overview page.

**Figure 3-7  Host Access Table Overview menu item**

This will open the **Host Access Table** configuration which allows you to add the alerts server to the list of trusted senders.
Step 3: Whitelist the Alerts Server

The configuration pane will look something like this:

**Figure 3-8 Host Access Table**

![Host Access Table Diagram]

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.

**Step 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.

**Step 3** On the window that appears, click **Add Sender** in the **Sender List: Display All Items in List** section. In the window that appears, in the **Sender**: field, enter the IP address of the alerts server: 198.2.132.180. In the **Comment**: field, add a comment such as **Whitelist alerts server**.
Step 3: Whitelist the Alerts Server

Figure 3-9  Whitelisting a Sender

Add Sender to WHITELIST - smtp-in 192.168.109.2:25

Sender Details
Sender: 1
198.2.132.180
(IPv4 or IPv6)
Comment: Whitelist Cisco alerts server

Cancel  Submit

Step 4  Click Submit On the Sender Group pane, confirm the IP address is present in the Sender List section:

Figure 3-10  Sender List Section

Step 5  Click Commit Changes >> for the configuration change to take effect.

As seen above, the IP address of the alerts server is 198.2.132.180. A DNS entry for this address at the domain “outbound.cisco.com” is also maintained. In general, it is recommended to use the explicit IP address for this whitelisting rule.
Step 4: Configure Cisco Email Security Gateway to Add an X-Agari-Authentication-Results Header

This section is intended only for the cases where the Cisco Email Security Gateway system you are configuring is a perimeter Gateway and is not being used for dual delivery. If you are using your Cisco Email Security Gateway 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.

If your Cisco Email Security Gateway system is a perimeter Gateway and you want to add the X-Agari-Authentication-Results header, perform the following steps:

- **Step 1** Log into the Cisco Email Security Gateway as an Administrator.
- **Step 2** Navigate 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 Cisco Email Security Gateway instances). Do not add perform these steps at the machine level.
- **Step 3** Click Add Filter.
- **Step 4** Name the filter Agari_auth_header.
- **Step 5** Add a reasonable description for the filter, for example: Add the X-Agari-Authentication-Results header to all incoming email.
- **Step 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. 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.
- **Step 7** Click Add Action to associate an action with this filter. In the Add Action window, select Add/Edit Header.
- **Step 8** 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: $enveloperecipients

- **Step 9** 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']
Figure 3-11 X-Authentication-Results Header

**Step 10** Ensure the header name are correct and click **OK**. The completed incoming content filter will look something like this:
Step 11 Click **Submit** to save the new filter.

Step 12 To associate the filter with an appropriate Incoming Mail Policy, navigate to **Mail Policies > Incoming Mail Policies** and 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:

![Figure 3-13 Policies page Referencing Content Filter](image-url)
Step 13  
Click **Commit Changes >>** to save the configuration.

**Note**  
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 Advanced Phishing Protection 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 the Cisco Advanced Phishing Protection Portal at [https://appc.cisco.com](https://appc.cisco.com) and navigating to **Manage > Sensors** to see the status of your installed Advanced Phishing Protection Sensors.
User Tasks: Getting Started

This chapter describes the following tasks:

- Gaining Access to the Web Application
- Creating/Editing Users
- Analyzing Incoming Email Traffic

Gaining Access to the Web Application

Cisco Advanced Phishing Protection provides unprecedented insight into your organization's inbound email traffic.

Your sales representative must enable the very first administrator account for accessing the web application. Typically, the very first account has 'administrator' privileges so that you can create additional user accounts for your organization.

Once your sales representative has created the first user account, you should receive an invitation email with a link to activate the user account:

**Figure 4-1  A Sample Invitation Email**

Follow the link sent in the invitation email to activate your user account. Choose a secure password. You'll access the portal at https://appc.cisco.com the next time you log in.
Creating/Editing Users

- User Roles, page 4-2

User Roles

Read-only User
A read only user can search and view data in the application, but cannot make changes or edits anywhere in the application.
- View and search data on all pages under the Analyze menu (Overview, Messages, Domains, IP Addresses, and Search Messages).
- View policy configurations on the Manage > Policies page. Cannot create new policies, on-demand policies, or edit policies.
- View Reports on Manage > Reports.
- View Senders on Manage > Senders. Cannot Approve, Deny, or Undo senders or IPs.
- View metrics and configurations on Manage > Sensors. Cannot modify sensor configurations.
- View own user settings and enable API credentials on Manage > Users. Cannot change own user role.
- View address group configurations on Manage > Address Groups. Cannot create or edit address groups.

Auditing User
An auditing user will by default have all permissions of a read only user, unless the read only role is specifically unchecked. In addition an auditing user can view users audit logs.
- View and search user audit logs at Manage > Users.

User Administrator
A user administrator will by default have all permissions of a read-only user and auditing user unless those roles are specifically unchecked. In addition and auditing user can create and edit other users in the organization.
- Create and edit users at Manage > Users.

Organization Administrator
An organization Administrator will by default have all permissions of a read-only, auditing, and user administrator unless those roles are specifically unchecked. In addition the organization administrator can make changes to organization settings, policies, and Address Groups.
- View and edit organization settings at Manage > Organization.
- View, create, and edit policy configurations at Manage > Policies.
- Create On-demand Policies at Search Messages (if applicable to customer configuration).
- View, approve, deny, or undo Senders and IPs at Manage > Senders.
- View metrics and update configurations at Manage > Sensors.
- View, create, and edit address groups at Manage > Address Groups.
Analyzing Incoming Email Traffic

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

The overview page is a unique visualization of Risk Overview of your organization’s inbound email traffic. Every message received by the Cisco 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?

  and

- **Domain Reputation** – is this a domain reputable, i.e. someone with whom I have a credible business relationship?

Trust Score

A Trust Score is calculated for every 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. It is important to note that the content of the message is not a factor in the Trust Score.

- 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 Analyze > Overview page represents a sending domain and the circles are sized based on the relative amount of traffic they send. 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.
You can winnow the results, limiting them to just one or all three of the basic three attack types by clicking on the boxes in the Show Attacks section on the left of the page. Use this feature to quickly identify potential problem messages and senders.

To return to the original traffic view, click the Top Sending Domains 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:

**Figure 4-4 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 which looks like this:
This says that IronPort has analyzed 5,195 legitimate messages from the *gmail.com* domain in the past day; hovering over the smaller circle shows that 41 messages may warrant further investigation because they have a lower authenticity score. Clear the search box to return to the original view.

**Attack Classifications**

- Attack Taxonomy, page 4-7
- Domain Spoof, page 4-7
- Look-alike Domains, page 4-8
- Display Name Impostor, page 4-9
- Compromised Account (Account Take Over), page 4-9
- Low Trust Domains, page 4-10
Messages that are Untrusted, per the Message Trust Score, will be classified into one or more of the attack taxonomy classes seen in the figure above. The attack classifications will be seen in the Message Details view.

**Note**

The taxonomy attack classifications are not currently available for search and policy, they are only informational notes in the Message Details.

Below are descriptions and examples of the taxonomy attack classifications.

### Domain Spoof

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

Figure 4-9  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 IronPort finds indicators of account take over we will classify it as a message from a Compromised Account.

Figure 4-10  Compromised Account Example
Low Trust Domains

In addition to the previously mentioned Sender classifications, Cisco 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.

Figure 4-11  Low Trust Domain Example

Malicious Attachment

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

Figure 4-12  Malicious Attachment Example
Legacy Attack Classes

The three attack classes below remain available in the Cisco Advanced Phishing Protection web application. In a future release they will be absorbed into the newer taxonomy attack classes. You can use these classifications to take further actions, such as alerting based on the attack classification. There are several places in the Cisco Advanced Phishing Protection web application where you can filter messages by these legacy classes - including the Risk Overview, the Messages dashboard when you filter by common attributes, and the Search Messages page. Here is a brief description of each attack classification.

Impostor
Impostor attacks include Look-alike domains and some Display Name Impostors (primarily major brands used in display names). To ensure your internal or partner domains are used to identify impostors and not classified as impostors themselves, tag the domains in the Cisco Advanced Phishing Protection web UI on the Analyze > Domains page.

Spoof
Spoof attacks are Domain Spoofs in the new taxonomy class. Messages that use a high reputation sender domain, but come from an inauthentic source. These attacks are “spoofing” the trusted identity of a known sender. To understand more about how the authenticity of the message source is determined see the section on the Authenticity Score.

Zero Day
Zero Day attacks are a subset of the Low Trust Domain class in the new taxonomy. Zero day attacks are those where a new domain appears and suddenly sends messages to a significant number of recipients in your organization (a.k.a pop-up domains). These domains typically start out with a low sender domain reputation with no or minimal sending history in data. You will often find general junk email and “business spam” caught in this classification.

Message Details

Now that you've identified a few untrustworthy senders, click on 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. Click on a message to view the Message Details. Remember that Cisco Advanced Phishing Protection does not track the body of the message.
Analyzing Incoming Email Traffic

Chapter 4      User Tasks: Getting Started

Analyzing Incoming Email Traffic

Figure 4-13 Message Details Pane

The Message Details page shows the headers and scoring information for the message, including the reason for the score the message was given. In the upper right side of the message details view, you can click the bell icon ( ) to quickly create a policy with conditions that match this message. See Managing Incoming Mail Via Policies for more on creating Policies.

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?

The Workflow

Use the Overview page to find problem senders and messages. Clicking on the various attack classifications on the right 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.
- Review the score.
- 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.
IPs and Domains

From the Analyze menu you can view lists of sending IPs and Domains (Analyze > Domains and Analyze > IP Addresses). The pages function very 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. Similarly, clicking a domain in the list on the Analyze > Domains page shows you the Details page 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.

Domain Details

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

Figure 4-14 The Domain Details Page
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>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.</td>
</tr>
<tr>
<td>2</td>
<td>The domain reputation (as scored by IronPort) 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.</td>
</tr>
</tbody>
</table>
| 3       | 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.   
- Authentic messages are those that adhere to the authentication standards as published by the domain itself: SPF, DMARC, or DKIM.  
- Inauthentic messages are messages which fail authentication and are deemed not to be within sender model for that domain.  
- Likely authentic messages are messages which do not pass authentication but are deemed to be "likely authentic" from the sending domain.  
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). 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. |
| 4       | 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." |
| 5       | The "Messages by IP Address" catalogs each IP address which has sent for the domain during the time period.   
- 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.   
- 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. |

### Tagging Domains

On the Analyze > Domains page or on the Domain Details page you can specify tags for Domains in the right-hand column. You may need to apply tags to some internal and partner domains as necessary. Tagging Domains can help with analytics and Policy creation. The “internal” and “partner” tags are used in the scoring processes. Other custom tags are not used in scoring but can be useful in Policies and can help with the visualization on the Analyze > Overview page and with Search results.
**IP 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)
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 Cisco.

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 "In this example, the sending IP has sent 42 messages into the organization: 42 messages for the domain "domain nt 42 messa" and one message for " and one message for ".

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.

Messages

Whereas the Overview page provides an interactive visualization of Spoofs, Zero-Day domains, and good messages, the Analyze > Message page provides more of an Operational view to help you explore your data.
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

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?
- **Zero-Day Domains** – Which of these Untrusted messages are sent from Zero-Day domains?
- **Impostor Domains** – Of all the messages scored as Suspicious, which have been sent from Importer domains?
- **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?
- **Campaigns** – How many of these Untrusted messages are from one sender with the same Subject?
- **From / To / Subject / Date** – Who are my riskiest Senders? Who are my riskiest Receivers? Was I attacked on a particular day?
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.

Click the Message Feedback link on the Search results page to send comments regarding the sending domain.

When you click on a message in the search listing (or in the Analyze > Messages page) the Message Details page is displayed:

![Figure 4-19 The Message Details Pane](image)

The Message Details page shows information about the message including headers and scoring (and the reasons for the scores received); which policies, if any, the message matched; and (if you have enforcement enabled) whether the message was enforced.

Using the icons in the upper right of the Message Details page you can:

- Link to view of the message details in the main window (with a URL which will link directly to this view).
- Mail the message details view to a colleague
- Create a Policy related to this message's conditions
- Provide feedback about a message's scoring

Managing Suspicious Messages

Now that 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 Managing Incoming Mail Via Policies, page 5-1.
User Tasks: Policies

This chapter describes the following tasks:

- Managing Incoming Mail via Policies
- On-demand Policies

Managing Incoming Mail Via 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 customers only), or even deleting a message entirely (Enforcement customers only).


Creating 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 which 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:
  - Inbox
  - Delete
  - Default folder move
  - Additional folder moves in order set in organization enforcement settings (see Administering Cisco Advanced Phishing Protection, page 6-1).
• You can create a policy with no notification or enforcement actions; all messages which match policies are logged in the Event Log and Reports.

**Conditions**
Enter criteria to match messages based on email header information, specifically: the Enter, , t, and , and cri headers, the message Subject, and/or the sending domain.

You can also specify Domain Tags to match here. Domain Tags are assigned on the Analyze > Domains page and discussed in Analyzing Incoming Email Traffic.

Additional criteria are available in the advanced dialog (below).

**Using Address Groups in Policies**
You may want to specify a group of email addresses on which to match Policies. For example, you may want to create a policy that looks for email sent to any one of a group of executives. Rather than entering the names individually into multiple Policies, you can create an Address Group containing the list of names and then reference that Address Group in a single Policy.

One or more address groups can be referenced by a policy. Address groups can be used in the From, To, and Reply-To conditions of the policy.

You can create and manage Address Groups via the Manage > Address Groups page.

**In the From: field**
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. 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.

The condition will also take into account the authenticity of the message, if the From address matches the entered address.

For example, consider an address group containing the following address:

"For example, consider an address group containing the following address:

*For example, consider an address group containing the following address:*

• If a message is received From: “John Doe” <jdoe@not-example.com>, 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.).

• If an inauthentic message is received From: “John Doe” <jdoe@example.com>, 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.

• If no Friendly From portion exists, the local part of the address is evaluated, so an address of <jdoe@example3.com> would match based on the local part of the email address in the From header matching.

**In the To: field**
Address groups will simply look for messages where the To field exactly matches an entry in the address group, ignoring the Display portion. A policy matching an address group in the 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,” and Message Trust Score is 0 - 4.9.
Populating an Address Group

Populate your address group by entering a first name, last name, and email address for each user in the group. You can enter a user multiple times if, for example, the user has multiple internal email addresses. Address group matching uses the first name and last name fields you enter when evaluating the “Friendly-From” portion of the email address. (In the example above “John Doe” is the “Friendly-From” portion; it is often this portion of the “To:” header which is visible on some Mail User Agents (MUAs) like Office365, Gmail, or the Mail app on iOS.)

Address Group Exceptions

Addresses in the exception list are for specifying “known good” or personal email addresses of the people in the address group 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 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 is inauthentic, and they are only considered when the address group is referenced by the From: and Reply-To: conditions.

- You can add addresses like messenger@webex.com or reply@chatter.salesforce.com so that when a user in your Address Group is spoofed legitimately, like “John Doe <messenger@webex.com>” or “John Doe <reply@chatter.salesforce.com>” the condition will not match.
- You can also add personal addresses like “johndoe@gmail.com” which may share the Friendly From of addresses above.

Scoring

You can set a score threshold and whether to match Domains that are either Zero-Day or Impostor (or neither).

Advanced

Advanced criteria provide more granular scoring matches (authenticity, domain reputation, or SBRS ranges) as well as the option to match a specific IP Address.

Note

A policy needs only a single condition to be a valid policy. 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”). 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”). Use caution when configuring policies so that you do not create policies which are too noisy.

Actions

Specify what Cisco Advanced Phishing Protection should do when messages match this Policy.

Notify

You can specify who to notify and how to notify them (digest/etc.). Notify original recipients will send an individual notification to all recipients of message which matches the criteria. (Note that this could cause bounce messages, for example, if the Cisco Advanced Phishing Protection Sensor parses a message and attempts to send a notification to a non-existent mailbox.)
Notify administrators will send either a single notification message for every matching message, or a single digest notification when the number of message matching a given policy exceeds a threshold you define.

You can customize the global notification users receive via the Configure Policy Text for Original Recipients link on the Manage > Policies page.

**Note**

This notification template is shared by all Policies.

**Enforce**

If you use O365 or G Suite as your mail store and have enabled Enforcement, 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. Note that 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 IronPort moved a message based on a policy condition match.

- 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 “Administering Cisco Advanced Phishing Protection” on page 181).

**Getting Started with Policies**

**Out of the Box Policies**

You will start out with 6 default policies to match the most common conditions that Cisco customers will catch with Cisco Advanced Phishing Protection. These policies need to be enabled to start matching messages and notify and/or enforce actions need to be set up for the policies. It is recommended that you enable the policies with no actions first and after logging policy matches and monitoring results, then choose your notify and enforce actions.

Here are the default policies:

<table>
<thead>
<tr>
<th>Name</th>
<th>Conditions</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>C-Level Impostors</td>
<td>From: matches a Display Name in the address group C-Level Executives</td>
<td>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.</td>
</tr>
<tr>
<td>Executive Impostors</td>
<td>From: matches a Display Name in the address group Executives</td>
<td>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.</td>
</tr>
</tbody>
</table>
Chapter 5  User Tasks: Policies

Managing Incoming Mail Via Policies

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Conditions</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rapid DMARC</td>
<td>Domain tag is “internal”</td>
<td>Catch spoofs of your own domains being sent to your employees. This policy mimics a DMARC reject policy without the need to go through a long process of authenticating all sources. Cisco’s trust models learn the authenticity of inbound sources.</td>
</tr>
<tr>
<td></td>
<td>Authenticity score is &lt; 0.4</td>
<td></td>
</tr>
<tr>
<td>Spoof of Partner Domains</td>
<td>Domain tag is 'partner'</td>
<td>Catch spoofs of your partners' domains</td>
</tr>
<tr>
<td></td>
<td>Authenticity score is &lt; 0.4</td>
<td></td>
</tr>
<tr>
<td>General Impostors</td>
<td>Domains/Brands are Impostor</td>
<td>Catch impostor domains with intentionally similar names, things like cisco.com or paypa1.com. Also catch brand impostors where common brands are spoofed in the display name.</td>
</tr>
<tr>
<td></td>
<td>Message Trust Score is &lt; 5.0</td>
<td></td>
</tr>
<tr>
<td>Low Message Trust and Low Sender Reputation</td>
<td>Message Trust Score is &lt; 2.5 SBRS score is &lt; -2.0</td>
<td>Catch general spam and greymail that slips past your Cisco Email Security Gateway.</td>
</tr>
</tbody>
</table>

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.

Enable or Disable a Policy

To enable a policy, click the policy name on the index page (Manage > Policies) to get to the Edit Policy page. At the top of this page you will see the slider to enable the policy directly below the policy name.

Figure 5-1  Enabling a Policy

Don’t forget to save your enabled policy with the Save button at the bottom of the page.

Creating your own Test Policy

Let's get started creating that test Policy. It's simple: you only need to enter three pieces of information.
Managing Incoming Mail Via Policies

**Step 1** On the Manage > Policies page, click Create Policy. Name the Policy and then enter your personal email address in the email field and your company email address of your own inbox in the field.

**Figure 5-2 Creating a Policy**

![Create Policy](image)

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.

**Step 2** Click Create.

**Step 3** Send a message from your personal account to your company address.

**Step 4** 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.

**Figure 5-3 Policy Event Log for a Policy Event**

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Policy Name/System Notification</th>
<th>Event</th>
</tr>
</thead>
</table>
| 13-Feb-2017 10:45:27 PST | MyTest                         | Event with 1 message
No Recipients notified. |

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. 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).

How Are My Policies Working?

Once you have created some Policies you probably want some insight into the results. Are the Policies working as you expected? How many messages are matching? Is the number of matching trending upwards? etc. There are three places you can check for this kind of information. Policy Log is a running log of Policy matches, the Manage > Reports page is a view of aggregate Policy matches over time, and on the Search Messages page you can search for Matched Policies.

Event Log

Click the Policy Log tab on the Manage > Policies page to view the 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). From the Policy Log you can view the matched Policy by clicking the name of the Policy and you can view the message details for the message(s) matching the Policy by clicking the line in the Event column. You can also filter the Policy Log to show the matched messages for a specific policy. You can also choose whether to show System Notifications in this view.

To see matches by Policy (all messages matching a Policy over a specific time period) use the Policy report via Manage > Reports.

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 Policy 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 list to view a summary of the moved and not moved messages for all policies with the Enforce action.
On-demand Policies

On-demand Policies 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, Cisco 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 Cisco 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 are initiated from the search results page.

On the search results page, the “Enforce Now” button will be displayed if enforcement has been enabled for your organization.

The button is disabled for results larger than 2000 messages; you can only enforce 2000 or fewer messages at a time using an on-demand policy.

For example, note the button state and the number of results in each of these examples:
Figure 5-5    Enforce Now... Button Available

Domain Reputation Range: 0.0 - 5.0  Domain Tags: Filter By Tags
Sending Domain: redwoodcompliance.com  Domain Type: Zero-Day  Impostor

Search  Reset

Displaying 1 - 16 of 16 Messages

<table>
<thead>
<tr>
<th>Trust Score</th>
<th>Date</th>
<th>From</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>27-Sep-2017</td>
<td>Amber Leon <a href="mailto:amber@redwoodcompliance.com">amber@redwoodcompliance.com</a> vaps</td>
</tr>
<tr>
<td>3</td>
<td>27-Sep-2017</td>
<td>Amber Leon <a href="mailto:amber@redwoodcompliance.com">amber@redwoodcompliance.com</a> dspc</td>
</tr>
<tr>
<td>3</td>
<td>27-Sep-2017</td>
<td>Amber Leon <a href="mailto:amber@redwoodcompliance.com">amber@redwoodcompliance.com</a> san</td>
</tr>
<tr>
<td>3</td>
<td>27-Sep-2017</td>
<td>Amber Leon <a href="mailto:amber@redwoodcompliance.com">amber@redwoodcompliance.com</a> sken</td>
</tr>
</tbody>
</table>

Figure 5-6    Enforce Now... Button Unavailable

Domain Reputation Range: 0.0 - 5.0  Domain Tags: Filter By Tags
Sending Domain: redwoodcompliance.com  Domain Type: Zero-Day  Impostor

Search  Reset

Displaying 1 - 25 of 3,905 Messages

<table>
<thead>
<tr>
<th>Trust Score</th>
<th>Date</th>
<th>From</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>27-Sep-2017</td>
<td>Amber Leon <a href="mailto:amber@redwoodcompliance.com">amber@redwoodcompliance.com</a> vaps</td>
</tr>
<tr>
<td>3</td>
<td>27-Sep-2017</td>
<td>Amber Leon <a href="mailto:amber@redwoodcompliance.com">amber@redwoodcompliance.com</a> dspc</td>
</tr>
<tr>
<td>3</td>
<td>27-Sep-2017</td>
<td>Amber Leon <a href="mailto:amber@redwoodcompliance.com">amber@redwoodcompliance.com</a> san</td>
</tr>
<tr>
<td>3</td>
<td>27-Sep-2017</td>
<td>Amber Leon <a href="mailto:amber@redwoodcompliance.com">amber@redwoodcompliance.com</a> sken</td>
</tr>
</tbody>
</table>
To begin, 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:

**Figure 5-7 Narrowing Search Results**

Click the “Enforce Now...” button to select individual or all messages within the results set. Note the differences in selecting all messages in the entire set versus selecting all messages shown on the current page of results:

**Figure 5-8 Selecting Individual Messages Versus Selecting all Messages**
After selecting at least one message, click “Enforce selected.” A dialog box is displayed, where you can confirm the number of messages to be enforced and choose the enforcement action you would like to take or cancel the process. (The question mark icon provides additional information on why some messages may not be able to be moved.)

**Figure 5-9 Choosing an Enforcement Action**

After choosing the enforcement action click **OK** to enforce the message(s) immediately.

**Figure 5-10 On-Demand Policy Action Confirmation**

After you click okay, the On-demand policy details page is displayed while the Cisco EP system contacts your Cisco Advanced Phishing Protection sensor(s):
On-demand Policy
The parameters and status associated with an On-demand policy.

Details for On-Demand Policy 2017-09-27 17:23:30

Conditions:
- From address: contains <some-email>
- To address: contains <some-email>
- Date range: 27-Sep-2017 to 28-Sep-2017

Action:
On-demand: Move to folder: Agari-Quarantine
User: Paul Lorenz
Initiated on: 27-Sep-2017 16:23:30

The system is contacting your sensor.

After the Cisco Advanced Phishing Protection 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

Conditions:
- To address: contains <some-email>
- Date range: 26-Dec-2017 to 30-Dec-2017

Action:
On-demand: Delete
User: Mike Jones
Initiated on: 3-Jan-2018 16:17:44 PST

Processing messages...
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:

**Figure 5-13    Final Status of an 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.

**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.
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 polices are search-able from the search page:

On-demand policies are tracked in the audit logs for an organization.

To view the audit log, click the “Audit” link from the Manage > Organizations page to see the entries:
**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 Cisco 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 system.
Administering Cisco Advanced Phishing Protection

This chapter describes the following tasks:
- Administering Cisco Advanced Phishing Protection
- Sender Management and Rapid DMARC
- Attachment Analysis
- Azure AD Sync with Cisco Address Groups

Advanced Phishing Protection Sensors

View the status of your Cisco Advanced Phishing Protection Sensors and manage them via the Manage > Sensors page.
1 You can download the Sensor installation script keyed specifically to your Organization from the Cisco Advanced Phishing Protection Sensors page. Use this to install additional Sensors to handle increased traffic.

2 If you have multiple sensors, select a Sensor from the list of tabs. You can view the current status of the Cisco Advanced Phishing Protection 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 VM on which the sensor is deployed.

6 Last Connected is the time the Cisco Advanced Phishing Protection Sensor last checked in with Cisco. This should be within the last two minutes (if the Cisco Advanced Phishing Protection sensor is active).
For Office 365 customers only, there may be a “Download Credentials File” button, for credentials used by the Cisco Advanced Phishing Protection Sensor to perform enforcement activities.

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

### System Notifications

System Notification are system alerts managed via the **Manage > Policies** page. Click on the **System Notifications** tab to configure and to subscribe to the notifications. You can configure notifications based on conditions with Cisco Advanced Phishing Protection Sensors, the Host System itself, or Policies.

### Users

Create and manage Users for Cisco Advanced Phishing Protection. Users can interact with Cisco Advanced Phishing Protection to perform analysis and manage Policies, Users, Organizations, Cisco Advanced Phishing Protection Sensors, etc.

Click the “Audit User” link for a user to view a log of events for that user, including actions like logging in/out and changing configurations. 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.

You can set global access policy for users – password policy, session timeout, etc. – in the User Account Settings section of the Edit Organization page as discussed below.

### Organizations

You can manage your Organization from the Organization page. Click the **Audit** link to see the audit log for your Organization, including information such as user log in/out and configuration changes. 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.

Click the Organization name to access the “Edit Organization” page.

**Enforcement Settings**

You can enable or disable Enforcement for your organization in the Enforcement Settings.
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:

**Cisco Advanced Phishing Protection Sensor Settings**

The Cisco Advanced Phishing Protection 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.

**Internal MTA IP Addresses**

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.

**Note**

Use this only in the case of upstream MTAs.
Figure 6-4  The Sensor Settings Section

User Account Settings
Manage global user account access settings: how users log on, when they are logged off, and password policies.

Figure 6-5  The User Account Settings Section

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 Cisco 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 Cisco Advanced Phishing Protection to reject inauthentic messages from your own domains.
Using the Senders Page to Manage Your Senders

Navigate 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 switch to the Unassigned IP Addresses tab.

**Figure 6-6 The Senders Page**

<table>
<thead>
<tr>
<th>Column Meanings and Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sender</strong></td>
</tr>
<tr>
<td><strong>Inbound - Messages</strong></td>
</tr>
</tbody>
</table>
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 Cisco’s sender modeling for this sender/domain combination.

Note: The Authenticity Score displayed here is an average for all messages from all IPs associated with this sender/domain combination seen across the Cisco 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 Cisco 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 Cisco 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 Cisco Advanced Phishing Protection.
- Deny will explicitly deny a sender for that domain, ensuring that future messages from that sender will be considered inauthentic by Cisco Advanced Phishing Protection.

Relating Sender Management to 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 IronPort 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 EP, 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.

Step 1: Click the Rapid DMARC policy name on the Manage > Policies page to get to the Edit Policy page.
Step 2: Under the Policy Name, move the slider to Enable.
Step 3 Scroll down to the **Actions** section to set up your enforcement action for this policy and/or to enable an alert on policy matches.

Step 4 Click **Save** at the bottom of the page.

Customers that were set up in EP before January 2018 did not receive a Rapid DMARC policy. You can create your Rapid DMARC policy with these steps:

---

**Step 1** Click on **Create Policy** on the **Manage > Policies** page.

**Step 2** In Policy Name enter “Rapid DMARC”.

**Step 3** Scroll down to Domain Tags and click in the empty box. Select “internal” from the list of available domain tags.

**Step 4** Scroll down and open the **Advanced** toggle.

**Step 5** Move the top end of the **Authenticity Score Range** to 0.4. It should look like this:

![The Authenticity Score Slider on the Policy Page](image)

**Step 6** Click **Save** at the bottom of the page.

---

### Attachment Analysis

Cisco Advanced Phishing Protection is capable of analyzing message attachments 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 attachment analysis possible in Cisco 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.

### Enabling Attachment Analysis

Attachment analysis in Cisco Advanced Phishing Protection is a multistep process, depending on which level of analysis you want to have performed.
Basic Attachment Information Collection

To collect the attachment name and file extension information only, but not perform full attachment scanning, you must enable an organization level setting to allow Cisco Advanced Phishing Protection to collect this information.

---

**Step 1** Navigate to Manage > Organization

**Step 2** Scroll down to the Cisco Advanced Phishing Protection Sensor Settings section and then the settings for “Message Components:”.

**Step 3** Check the box next to “Upload list of attachment names” to enable this for your organization.

**Step 4** Scroll to the bottom of the page and click **Save**.

*Figure 6-8  The Upload List of Attachment Names Checkbox*

---

Scanning of Attachments

Scanning of attachment content for malicious intent must be enabled on a per sensor basis. If you manage your own Cisco Advanced Phishing Protection sensor environment you may choose to only scan attachments on a subset of your sensor appliances, routing email with attachments to those specific sensors.

---

**Note**

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. Please see **Installing a Cisco Advanced Phishing Protection Sensor, page 1-1** for updates to Cisco Advanced Phishing Protection sensor host system specifications.

---

**Step 1** First you must perform the steps above to set your organization level policy on attachment name collection.

**Step 2** Navigate to **Manage > Sensors** page.
Step 3 Scroll down to the **Configuration** section.

Step 4 Move the “Attachment Scanning:” slider to “Scan Attachments”.

Step 5 Click **Save Configuration** at the bottom of the page.

Step 6 If you have multiple sensors repeat these steps on each tab for which you want the sensor to perform attachment scanning.

Figure 6-9 **Enabling Attachment Scanning**

Using Attachment Analysis

- Using Attachment Analysis Results in Search and Policy, page 6-10
- Attachment Scan Results, page 6-11
- Details of the Attachment Scan, page 6-11
- Notifications of Azure AD Group Sync Failures, page 6-17

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.

Figure 6-10 **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.
If you have enabled attachment scanning then all of the options will be available for search and policy.

### Attachment Scan Results

When attachment scanning is enabled Cisco Advanced Phishing Protection uses the results of the scan in it's 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.

### Details of the Attachment Scan

Cisco 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.
Cisco 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

Azure AD sync with Address Groups

Manage your Address Group based policies more efficiently by syncing IronPort Address Groups with your Azure Active Directory groups. IronPort will automatically pull the members from your Azure AD groups into a sync'd Address Group so that you no longer have to worry about manual updates.

To learn about how Address Groups are used in policies, see Managing Incoming Mail Via Policies, page 5-1.

Setting up Address Group Sync

To set up Address Group sync you must first authorize Cisco to sync with your Azure AD.

**Step 1**
Click Enable Azure AD Sync on the Manage > Address Groups page.

**Step 2**
You will be presented with a dialog to connect with Azure AD and grant permission. You will need to login as a Global Administrator to do so.
Step 3  You will be directed to Microsoft to select the account that you will use to grant consent and asked to login to that account.

Step 4  Upon login you will be presented with the option to approve the Cisco AD Group Reader application.
Figure 6-17  Granting Permissions

Step 5  After approving you will be directed back to the Cisco Advanced Phishing Protection application and will be authorized to sync groups with Azure AD.

Creating a Sync'd Address Group

Step 1  Now that you are sync'd to Azure AD, click on Create Address Group on the Manage > Address Groups page.

Step 2  You can add addresses now have the option via Azure AD.

Figure 6-18  Creating an Address Group from an AD Group

Step 3  Click Azure AD Group box to see a list of available groups.

Step 4  Select the group you want to sync. The names and email addresses in that group will appear.
Figure 6-19 Selecting an AD Group

Step 5 If there are members of the Azure AD group that cannot be sync’d to an Address Group they will appear in a section called **Skipped Addresses**.

Figure 6-20 Skipped Addresses

Step 6 Click **Create** at the bottom of the page to save the Address Group.

**Unlinking a Sync'd Address Group**

You can tell an Address Group is sync’d 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”.

---

**Figure 6-19**

![Selecting an AD Group](image1)

**Figure 6-20**

![Skipped Addresses](image2)
Figure 6-21  The Source Column of the Address Group Index Page

<table>
<thead>
<tr>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linked to Azure AD</td>
</tr>
<tr>
<td>Linked to Azure AD</td>
</tr>
<tr>
<td>Manually unlinked from Azure AD</td>
</tr>
<tr>
<td>Individually added</td>
</tr>
<tr>
<td>Automatically unlinked from Azure AD</td>
</tr>
<tr>
<td>Manually unlinked from Azure AD</td>
</tr>
</tbody>
</table>

Step 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”.

Figure 6-22  Unlinking an Azure AD Group

Step 2  Clicking that will stop the group from further syncing with Azure AD, 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.
Step 3  Click Save at the bottom of the page to save the Address Group.

Notifications of Azure AD Group Sync Failures

After setting up sync’d address groups it is recommended that you sign up for system notifications about failures to of the regular sync jobs.

Step 1  Navigate to Manage > Policies and click on the System Notifications tab.
Step 2  Scroll down to the Policies section and check the box for “Azure AD sync fails to sync an Address Group within a day”.

Figure 6-24  Enabling the System Notification for Azure AD Sync Failures
Single Sign-On (SSO)

Cisco 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 Cisco Advanced Phishing Protection username, which eliminates the need for a separate Cisco Advanced Phishing Protection password.
- Revoke user access centrally. When an employee leaves the company, you can remove access within the SSO provider rather than having to log directly into Cisco Advanced Phishing Protection portal.
- 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 Cisco Advanced Phishing Protection (which effectively bypasses the single sign-on mechanism). You can also allow specific users to authenticate with the credentials stored in IronPort only in the event when the SSO identity service fails (for example, during outages).

To enable Single Sign-On for your organization:

**Step 1** Log in to Cisco Advanced Phishing Protection and navigate to Manage > Organization page.

**Step 2** Navigate to the “User Account Settings” configuration section.

**Step 3** Click Enable to enable Single Sign-on.
The Single Sign-On Enable Button

![Figure 7-1 The Single Sign-On Enable Button]

The Single Sign-On Configuration page is displayed:

![Figure 7-2 Configuring and Testing Single Sign-On]

In the dialog, enter the following information:

- **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)**
  
  Both of these values should be provided to you from your Single Sign-On identity provider.
a. Click **Test Settings** to validate the Endpoint URL and certificate values provided by your identity provider.  

The **Test Settings** button calls the Identity Provider with the public certificate credential at the location you enter.  

If the settings are correct, your browser will be redirected to Cisco Advanced Phishing Protection with a success message displayed.

b. Click **Save Settings** at the bottom of the page to save all settings for your organization and enable Single Sign-On for user accounts.

---

**Note**  
Warning! At this point, Single Sign-On will be enabled and:

- All existing users will receive an email that instructs them how to perform the one-time binding of their username to their SSO account in order to use their Single Sign-On identity provider credentials when accessing Cisco Advanced Phishing Protection.
- Users currently logged into the system will continue their sessions without interruption; however, they will be directed to the Identity Provider on subsequent login attempts.

---

**Logging In**

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 Cisco 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 IronPort 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 Cisco Advanced Phishing Protection Overview page.