Release Notes for Cisco Advanced Phishing Protection

Published: July 8, 2019
Revised: January 06, 2020

Contents

What’s New In Cisco Advanced Phishing Protection

Cisco is always working to improve the Cisco Advanced Phishing Protection product, from fixing issues to improving existing features to adding new features.

The following release versions explains the feature changes in Cisco Advanced Phishing Protection, as well as documentation updates not necessarily related to product features.

December 2019 Release Updates

This December 2019 release has the following documentation improvements:

- Updated the mail routing configuration for G Suite. For more information, see section "Configure Dual Delivery: G Suite" of the user guide.

- Added section on **Skipped Addresses for Azure Active Directory** address group syncronization. For more information, see section "Azure Active Directory Synchronization With Address Groups" of the user guide.
- Added information about the Allowed Forwarding IPs setting in the Sensor Settings section of organization settings. For more information, see section "Organization Settings" of the user guide.

November 2019 Release Updates

This November 2019 release has the following documentation improvements:

- Sensor requirements updates. On-premises Sensors now require Python 2.7 or newer.
- Naming for Sensor configuration has been updated.

October 2019 Release Updates

This October 2019 release has the following documentation improvements:

- You do not require the "Global Administrator" user role to access your systems. However certain permissions are required to configure access to the system.
- The **View AIR Investigation** link is visible in Continuous Detection and Response events. For more information, see section "View Continuous Detection and Response Event Details" of the user guide.
- The "Google Developers Console" section to configure enforcement in G Suite was updated to reflect Google's new nomenclature.
- Updates for notification settings. For more information, see section "Notification Settings" of the user guide.
- End-users do not have permisssions to modify user accounts on the Cisco Advanced Phishing Protection cloud service. For more information, see section "User Accounts" of the user guide.
- Plain text search fields in are now limited to 100 characters.
- Updates on Insider Impersonation Protection (IIP), providing you 360-degree monitoring of your incoming messages, outgoing messages, and internal messages. IIP requires Microsoft Office 365 or Exchange as your email provider and you must:
  - Explicitly enable this feature in your organization settings. For more information, see section "Messages Settings" of the user guide.
  - Make sure that message headers for all direction are added to all messages. For more information, see section "Configure Dual Delivery: Office 365 and Configure Dual Delivery: Microsoft Exchange" of the user guide.
- Message direction is now available for search and policy criteria. For more information, see section "Message Search and Policy Settings" of the user guide.
- For parameters consisting numeric values with upper and lower bounds, the upper and lower bound values are now inclusive for Message Search and Policy Settings.
- The attack vs. peer enforcement graph has been enhanced to clarify its values. For more information, see section "How Attacked/Protected Am I Relative To My Peers Report" of the user guide.
- Information about how to prepare for using (see **Before You Begin**) and how to access the API documentation (see **Application Programming Interface**) has been added to the user guide.

- Additional information on default policies has been updated. For more information, see section "Default Policies" of the user guide.
- The support for Sensors in an inline architecture has been removed.
- Reference content for message search has been updated. For more information, see section "Message Search" of the user guide.
- You can now download message search results. For more information, see section "Download Message Search Results" of the user guide.
- You can now download search results as a comma-separated value (CSV) file. For more information, see section "Download Message Search Results" of the user guide.
- Continuous Detection and Response (CDR) is now available on the Cisco Advanced Phishing Protection cloud service. CDR is an Secure Email Cloud (SEC) technology that allows organizations to prevent or mitigate data breaches as new threat intelligence is discovered. CDR is available to users having a subscription. Contact Cisco Customer Support to understand the requirements for obtaining CDR. For more information, see section "Continuous Detection and Response" of the user guide. Secure Email Cloud (SEC) also includes a mobile application that allows you to monitor and take actions on continuous detection and response (CDR) events.
- You can see who can change the report values. For more information, see section "Configure the How Much Have I Saved By Deploying Cisco Advanced Phishing Protection Report" of the user guide.
- The architecture diagram for inline Sensors has been updated. For more information, see section "Sensor Deployment" of the user guide.
- Additional information on how the internal and partner tags are used and best practices for applying them to domains has been updated to the Domain Tags. For more information, see section "Domain Tags" of the user guide.
- You can now set custom date ranges for the Threat Trends and Executive Summary reports.
- Updated sensor port requirements and supported Sensor architecture.
- Additional organization settings are available for how an organization is classified. These classifications, including region, industry, and organization size, are used for one of the executive summary reports. For more information, see "How Much Have I Saved by Deploying Cisco Advanced Phishing Protection Report Report" of the user guide.
- A new set of reports are available in Threat Trends and Executive Summary tab on the home page, reports that provide at-a-glance views of the benefits of using. These reports show a daily updated view of the value that Advanced Threat Protection provides, and you can download a snapshot of either page as an Adobe Acrobat (PDF) file. Additional organization settings allow customization of the message data in the reports. For more information, see "Threat Trends Reports and Executive Summary Reports" of the user guide.
- You can obtain more details when sending feedback about an individual message. For more information, see "Send Message Feedback" of the user guide.

Related Documentation

Documentation For Cisco Email Security Products	Location
Cisco Domain Protection	https://www.cisco.com/c/dam/en/us/td/docs/security/phishing_protection-and-domain_protection/dp_user_guide.pdf
Cisco Advanced Phishing Protection	https://www.cisco.com/c/dam/en/us/td/docs/security/phishing_protection-and-domain_protection/app_user_guide.pdf

Service and Support

Note To get support for virtual appliances, have your Virtual License Number (VLN) number ready when you call Cisco TAC.

Cisco TAC: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Support Site for legacy IronPort: http://www.cisco.com/web/services/acquisitions/ironport.html

For non-critical issues, you can also access customer support from the appliance. For instructions, see the User Guide or online help.

This document is to be used in conjunction with the documents listed in the "Documentation for BETA" section.

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