Release Notes for Cisco Advanced Phishing Protection

First Published: July 8, 2019
Last Updated: July 10, 2020

Contents

• What’s New In Cisco Advanced Phishing Protection, page 1
• Related Documentation, page 2
• Service and Support, page 2

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.

• June 2020 Release Updates, page 2
• April 2020 Release Updates, page 2
• March 2020 Release Updates, page 2
• February 2020 Release Updates, page 2
June 2020 Release Updates

- Significant changes to the search language that you can use to create continuous detection and response (CDR) rules have been made. See "Domain Specific Language Reference" on page 131 for details.
- The ability to create custom, local continuous detection and response (CDR) rules has been added. See "Continuous Detection and Response Rules" on page 130.

April 2020 Release Updates

- (CDR) rules added. See "Continuous Detection and Response Rules" on page 130.

March 2020 Release Updates

- Message details now provide additional insight into how a message score and attack classification was determined. "Attack Classifications" on page 105 shows details for the different attack types.

February 2020 Release Updates

- Email addresses in the journaling topic had the incorrect domain for Advanced Phishing Protection. This has been corrected.
- Processing exceptions can now be defined so messages will not be evaluated. See “Processing Exceptions” on page 189 for details.

Related Documentation

<table>
<thead>
<tr>
<th>Documentation For Cisco Email Security Products</th>
<th>Location</th>
</tr>
</thead>
</table>

Service and Support

Note

To get support for virtual appliances, have your Virtual License Number (VLN) number ready when you call Cisco TAC.
For non-critical issues, you can also access customer support from the appliance. For instructions, see the User Guide or online help.