Proofpoint Threat Response 5.4.0 – Release Notes

December 2020

Overview

PTR/TRAP 5.4.0 introduces a new integration with **Proofpoint Browser Isolation** to simplify the task of triaging message-related URLs, reported by employees, to the Abuse Mailbox. Analysts now can inspect URLs safely, in a sandbox experience, with a single click, directly from the **PTR/TRAP alerts page**.

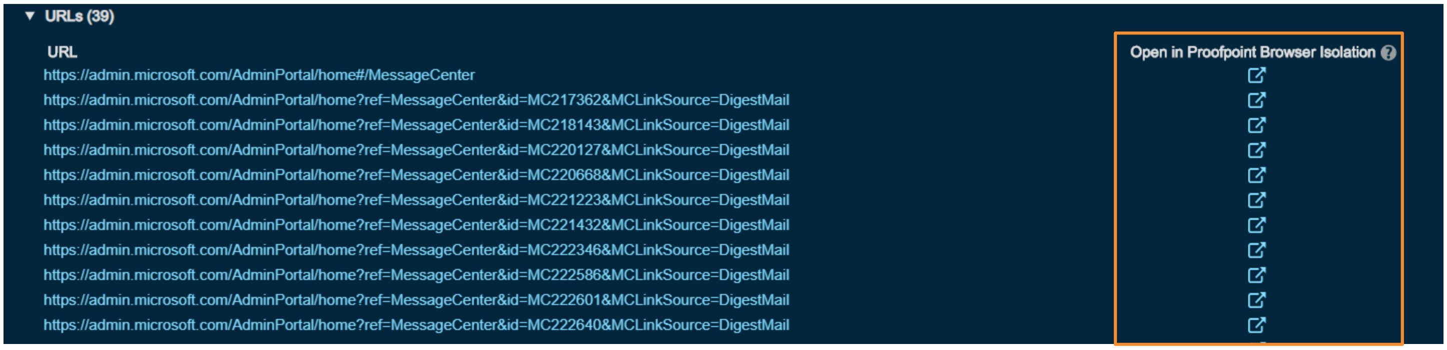
In addition, this release simplifies the incident response workflow for abuse mailbox incidents with **quick links** to the **Alerts and Activity pages** directly from the **incident list page**. Also, it offers enrichment from **Proofpoint Targeted Attack Protection (TAP)** by highlighting **Very Attacked People (VAP)** who are targeted in an incident, thus providing visibility into threat types represented by TAP alerts.

Lastly, customers who use TAP will also benefit from the direct visibility of TRAP quarantine activity on the TAP Dashboard. PTR/TRAP version 5.3.0 added the capability to communicate information about successful quarantines back to the TAP Dashboard. The presentation of this information is now available with the launch of PTR/TRAP 5.4.0.

Closed Loop Email Analysis & Response

Using Proofpoint Browser Isolation to Triage URLs

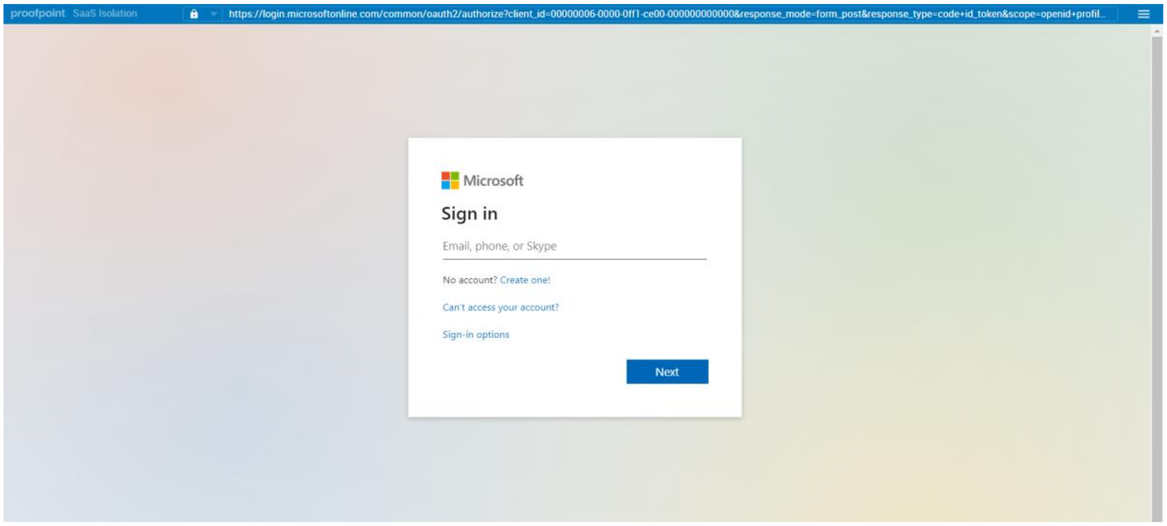
This release enables security teams to triage URLs in messages submitted by employees to the Abuse Mailbox by using the **Closed Loop Email Analysis & Response (CLEAR)** solution with a single click from the **TRAP user interface**. The **URLs section of the Alerts page** has a new column entitled **"Open in Proofpoint Browser Isolation."**



▼ URLs (39)

URL	Open in Proofpoint Browser Isolation ?
https://admin.microsoft.com/AdminPortal/home#/MessageCenter	↗
https://admin.microsoft.com/AdminPortal/home?ref=MessageCenter&id=MC217362&MCLinkSource=DigestMail	↗
https://admin.microsoft.com/AdminPortal/home?ref=MessageCenter&id=MC218143&MCLinkSource=DigestMail	↗
https://admin.microsoft.com/AdminPortal/home?ref=MessageCenter&id=MC220127&MCLinkSource=DigestMail	↗
https://admin.microsoft.com/AdminPortal/home?ref=MessageCenter&id=MC220668&MCLinkSource=DigestMail	↗
https://admin.microsoft.com/AdminPortal/home?ref=MessageCenter&id=MC221223&MCLinkSource=DigestMail	↗
https://admin.microsoft.com/AdminPortal/home?ref=MessageCenter&id=MC221432&MCLinkSource=DigestMail	↗
https://admin.microsoft.com/AdminPortal/home?ref=MessageCenter&id=MC222346&MCLinkSource=DigestMail	↗
https://admin.microsoft.com/AdminPortal/home?ref=MessageCenter&id=MC222586&MCLinkSource=DigestMail	↗
https://admin.microsoft.com/AdminPortal/home?ref=MessageCenter&id=MC222601&MCLinkSource=DigestMail	↗
https://admin.microsoft.com/AdminPortal/home?ref=MessageCenter&id=MC222640&MCLinkSource=DigestMail	↗

Clicking on a link in **"Open in Proofpoint Browser Isolation"** opens the webpage in a safe web browsing environment (sandbox) entitled **"Proofpoint SaaS Isolation.**"


proofpoint SaaS Isolation

https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000006-0000-0ff1-ce00-000000000000&response_mode=form_post&response_type=code+id_token&scope=openid+profil...

Microsoft

Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?

Sign-in options

Next

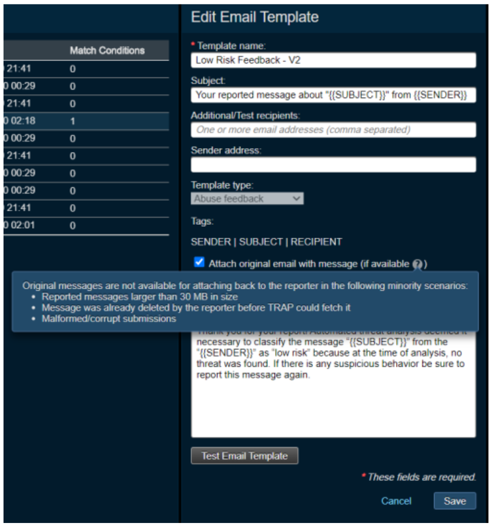
Browsing by means of Proofpoint Browser Isolation enables an analyst to click on a URL in the same way that an end user would behave. The analyst can click on links on the webpage and submit forms, thereby identifying potential phishing/spam threats without the fear of infection from malware as the browsing experience does not allow uploads/downloads of files to the system.

Customers don't need to own a license for Proofpoint Browser Isolation to use this feature. Further information about the Proofpoint Browser Isolation product can be obtained by clicking on this link.

Note: The use of Proofpoint Browser Isolation requires that an analyst's machine be connected to the internet. Further, use of a proxy is supported on condition that there is internet connectivity.

Attaching Reported Email with Feedback Templates and Sending It to End Users

PTR/TRAP 5.4.0 enables security teams to attach an original message, reported by end users, to the **email template responses** sent to them from TRAP. This is helpful when an email is scored as either **Low Risk** or **Bulk**; moreover, it is desirable for end users to be able to retrieve the reported email with ease. This setting can be configured by PTR/TRAP admins when creating/editing an email template here: **Abuse Feedback under Email Templates (in System Settings)**.



	Match Conditions
21:41	0
0 00:29	0
21:41	0
0 02:18	1
0 00:29	0
21:41	0
0 00:29	0
0 00:29	0
21:41	0
0 02:01	0

Edit Email Template

* Template name: Low Risk Feedback - V2

Subject: Your reported message about "{{SUBJECT}}" from {{SENDER}}

Additional/Test recipients: One or more email addresses (comma separated)

Sender address:

Template type: Abuse feedback

Tags:

SENDER | SUBJECT | RECIPIENT

☑ Attach original email with message (if available ?)

Original messages are not available for attaching back to the reporter in the following minority scenarios:

- Reported messages larger than 30 MB in size
- Message was already deleted by the reporter before TRAP could fetch it
- Malformed/corrupt submissions

Thank you for your report. Automated threat analysis deemed it necessary to classify the message "{{SUBJECT}}" from the "{{SENDER}}" as "low risk" because at the time of analysis, no threat was found. If there is any suspicious behavior be sure to report this message again.

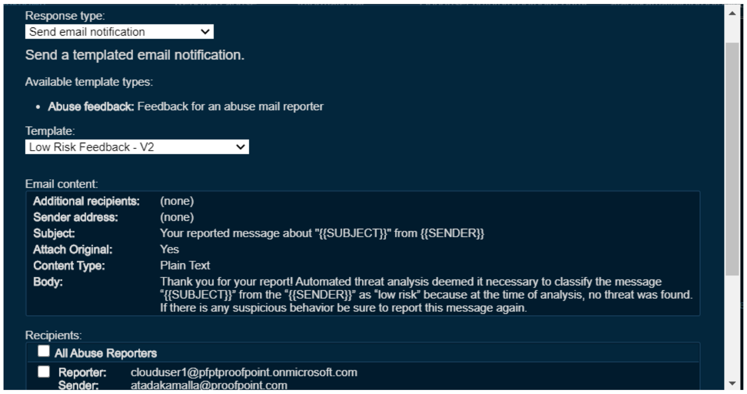
Test Email Template

* *These fields are required.*

Cancel Save

Previewing an Email Template’s Content Prior to Sending a Manual Response

This release enables manual **“Send email notification”** response actions from the **incident/alert page** to provide a preview of the content of an email template prior to sending it to an end user. This helps to verify that the appropriate email feedback template is being sent to the end user to reinforce their security awareness training.



Response type:
Send email notification

Send a templated email notification.

Available template types:

- **Abuse feedback:** Feedback for an abuse mail reporter

Template:
Low Risk Feedback - V2

Email content:

Additional recipients:	(none)
Sender address:	(none)
Subject:	Your reported message about "{{SUBJECT}}" from {{SENDER}}
Attach Original:	Yes
Content Type:	Plain Text
Body:	Thank you for your report! Automated threat analysis deemed it necessary to classify the message “{{SUBJECT}}” from the “{{SENDER}}” as “low risk” because at the time of analysis, no threat was found. If there is any suspicious behavior be sure to report this message again.

Recipients:

☐ **All Abuse Reporters**

☐ **Reporter:** clouduser1@pfptproofpoint.onmicrosoft.com
Sender: atadakamalla@proofpoint.com

Quick Links to the Alerts and Activity Pages from the Incident List

PTR/TRAP 5.4.0 adds **quick links** to the **Alerts and Activity pages**, directly from the **incident list**, to reduce the number of clicks required to reach critical information for resolving incidents.

Abuse Incidents List Is a Supported Default Landing Page

The **Incident List - Abuse Incidents page** is now a supported landing page in the **Account Preferences** section.

TAP Enhancements

Quarantine Reporting on the TAP Dashboard

Importantly**,** while this feature is being announced and will be generally available with the launch of PTR/TRAP 5.4.0, the underlying components have been populating data since the launch of PTR/TRAP 5.3.0.

PTR/TRAP can now communicate with the TAP Dashboard to provide customers with visibility into **successful and skipped quarantines** directly on the **TAP Dashboard**. Quarantine information is correlated with delivered messages and is presented clearly in order to help security teams capture the value delivered by TRAP, namely the mitigation of delivered threats and reduced exposure to risk.

Customers must be running PTR/TRAP 5.3.0 or above and need to turn on **Feedback Reporting (in System Settings)** to benefit from this feature.

TAP Threat Type Is Available on the Alerts View

In addition, PTR/TRAP 5.4.0 contributes to the enrichment of TAP alerts by providing **details of the type of threat** represented by the alert on the **Alerts page**. The threat type maps to one of the following values:

- Permitted Clicks
- Delivered Attachment Threats
- Unprotected URL Threats
- Delivered URL Threats
- Delivered Impostor Threats

Very Attacked People Enrichment, Badges, and Match Conditions

This release supplements alerts and incidents with information as it relates to VAPs from TAP. VAP recipients who are targeted and identified in incidents are marked with a **"badge"** on the i**ncidents and alerts pages**.

Dedicated match conditions can also be configured for VAP recipients to enforce greater security controls as they represent a potentially higher risk to your organization by virtue of being attacked more.

General Improvements and Notable Tech Upgrades

Expand_Events Query Parameter Extended to the Incident API

PTR/TRAP 5.4.0 extends support for the **expand_events query parameter** in the Get Incident Details **API**. Setting this parameter to a **value of false** can **speed up API calls** significantly. This can be used in scenarios where individual alert details are not required in the API response.

Hostname Support for the License Proxy Server

The proxy server field under **Licensing** on the **Appliance Management Console** now supports hostnames besides IP addresses.

Improved PTR/TRAP Error-handling

PTR/TRAP 5.4.0 **removes points of failure** around **licensing-related restarts** and **EWS request failures** thereby improving product robustness.

Download Instructions

PTR/TRAP 5.4.0 requires a minimum of VMware ESXi 6.0. Please use the Proofpoint CTS credentials to access the downloaded images.

- 5.4.0 OVA File (Fresh Installations and Upgrades From 3.x, 4.x) – Download OVA and SHA-256.
- 5.4.0 IMG File (Upgrades From 5.x) – Download IMG and SHA-256.
- 5.4.1 VHDX File (AWS AMI Installations) – Download VHDX and SHA-256.

The API documentation for PTR/TRAP 5.4.0 can be found here.

Installation Instructions

Please refer to the PTR Installation Guide or TRAP Installation Guide for instructions concerning the installation of 5.4.0. There are a few changes in the following sections in both guides.

- The virtual machine requirements include a slightly bigger HDD for the base system.
- The required ports for network communication include new entries for clustered deployments.
- The initial configuration wizard consists of a different set of steps as compared to older versions.

Please refer to the PTR AWS Installation Guide for instructions concerning the installation of 5.4.0 on AWS.

Upgrade Instructions: 3.x to 4.x

The upgrade process from a 3.x or a 4.x version requires a new virtual machine to be set up using the 5.4.0 OVA file. Data must be migrated from the older version of PTR/TRAP to 5.4.0. Refer to the Upgrade Guide for detailed instructions about upgrading an older version of PTR/TRAP to 5.4.0. The FAQ (Frequently Asked Questions) section contains answers to several common queries about the upgrade process.

Upgrade Instructions From 5.x

Upgrading from PTR/TRAP 5.x to 5.4.0 can be completed “in place” (on the appliance) using the IMG file. Refer to the Console Guide for instructions.

Note: An issue in PTR/TRAP 5.0.0 prevents rolling back to 5.0.0 after the appliance has been upgraded and running 5.4.0. Before upgrading the appliance from 5.0.0 to 5.4.0, it is advisable to take a VM snapshot first.

AWS Deployments – Upgrade Instructions

The upgrade process for AWS deployments requires a new EC2 instance to be set up using the 5.4.0 VHDX file. Data must be migrated from the older version of PTR/TRAP to 5.4.0. Refer to the AMI Installation Guide for detailed instructions on deploying PTR/TRAP 5.4.0 on AWS.