Release Notes

https://campus.barracuda.com/doc/90446521/

What's New in the September 29, 2022 Release

Enhancement

- Automated Workflows can now send notifications to Microsoft Teams. See Automated Workflows Settings for configuration information.
- Incident Response can create and Send a User List to Barracuda Security Awareness Training. It is a convenient way to:
  - Train users identified through Incident Response to recognize malicious emails,
  - Provide follow up testing, and
  - Analyze results with advanced metrics and reporting.

What's New in the August 4, 2022 Release

Enhancement

- Sender policies created in Barracuda Email Gateway Defense can now trigger Automated Workflows.

What's New in the July 28, 2022 Release

Enhancement

- You are now able to search in the body of the message using keywords of up to 200 characters and search for a URL within the body of the message. The View Incidents details page has been updated to show the additional search fields when creating an incident.

What's New in the April 4, 2022 Release

Enhancement

- You can now create an incident to investigate the impact of the incident without deleting emails or any remediation action. Once you have reviewed and have completed the investigation, you can click on the button “Delete emails” to delete the emails impacted in the Reviewing

Incidents page.

What's New in the March 1, 2022 Release

Enhancement

- You can now use templates to easily create automated workflows. For details, refer to Automated Workflows.

What's New in the January 13, 2022 Release

Automated Workflows can now be triggered for Potential Incidents. For details, refer to Automated Workflows.

What's New in the December 6, 2021 Release

As part of the Barracuda Email Protection, the features described here are now known as Automatic Remediation and Incident Response.

What's New in the October 20, 2021 Release

Enhancement

You can now see which users potentially clicked on links in emails associated with an incident. For details, refer to Reviewing Incidents .

What's New in the September 28, 2021 Release

Enhancement

Automated Workflows improvements and enhancements, based on feedback from the Beta testers, including:

- For Incidents created by Automated Workflows, you can now decide if you want to move emails

from users' mailboxes to the junk folders or delete the emails entirely.
For details, refer to the Automated Workflows Settings section of Automated Workflows .

What's New in the September 9, 2021 Release

Enhancement

- You can now create an automated workflow by defining a trigger, determining conditions, and assigning the desired actions through a streamlined user interface. When a workflow is triggered, you can choose to receive a notification via Slack, email, or both, and can review details of the actions carried out. Workflows can easily be paused or modified at any time. For details, refer to Automated Workflows.
  Note: For this inaugural release, there is one trigger available – when an end user reports an email through the Barracuda Outlook email reporting add-in. Additional triggers will be added over time.
  Prerequisites for this trigger:
  - Your organization must be using the Barracuda Outlook add-in for reporting questionable emails.
  - An end user in your organization must report an email by using the Barracuda Outlook add-in.

What's New in the May 9, 2021 Release

Enhancement

- Public API for Barracuda Forensics & Incident Response is now available. Refer to Public API Overview.

What's New in the March 31, 2021 Release

Enhancements

- When you create an incident by searching by email attachment name, words related to your search terms are also automatically searched. For more information, refer to Searching for Messages and Creating an Incident.
- You can add custom tags to incidents to help you identify them more easily later. You come up with the tags that are helpful to you and use them like nicknames for your incidents. For details, refer to the **Tags** section of Reviewing Incidents.

What's New in the February 2, 2021 Release

Enhancement

- During the startup process, Barracuda Forensics & Incident Response sends an email to your administrator to inform them of when the initial scan of the system is complete.

What's New in the January 5, 2021 Release

Enhancement

- You can now dismiss user-reported emails that appear to be innocuous. Refer to the **Viewing and Creating an Incident from User-Reported Emails** section of User-Reported Emails for more information.

What's New in the December 3, 2020 Release

Enhancement

- The User-Reported Emails page has a new chart, displaying the five users in your organization who have reported the most emails as suspicious. At a glance, you can review how accurate these reporters are – whether the emails they are reporting actually require remediation. For details, refer to User-Reported Emails.

What's New in the November 16, 2020 Release

Enhancement

- An administrator who is reviewing user-reported emails can now dismiss any user-reported emails that appear to be innocuous. These dismissed reports can be viewed by clicking **Show Dismissed** above the **User-Reported Emails** table. For additional information, refer to User-Reported Emails.

Fix

- When exporting data to a CSV file from the **View Incident** page, data from the **Opened Emails** column is now included.

What's New in the October 12, 2020 Release (Version 2.0)

Enhancements

- New visualizations at the top of the Incidents page enable you to see your data at a glance. Charts include Incidents Created, Threats Remediated, and Top 5 Attacked Users. For details, see Reviewing Incidents.
- Updated look and feel will enable quicker feature creation and deployment for future releases.

What's New in the July 27, 2020 Release

Enhancement

- Added ability to export event data to a syslog server or a security information and events management (SIEM) system. For details, see Syslog Options Settings. [BNFIR-951]

What's New in the July 6, 2020 Release

Enhancement

- You can now use Automatic Remediation for malicious attachments. [BNFIR-720]

What's New in the June 22, 2020 Release

Enhancement

- On the **View Incident** page, there is now no limit to the number of records you can download from the **Email/Users** table. [BNFIR-888]

Fixes

- When creating an incident, you must include an email. You are no longer able to create incidents with zero emails.
- The **Potential Incidents** page no longer include emails that:
  - are older than 30 days old
  - were remediated in a way that was not initiated from the **Potential Incidents** page

What's New in the June 17, 2020 Release

Enhancement

- The system can now automatically create incidents for and remediate user-reported emails with malicious attachments, in addition to malicious URLs. [BNFIR-720]
  See the following articles for more information:
  - Automatic Remediation for background information
  - Reviewing Incidents for the new Threats tab associated with Automatic Remediation
  - Setting Default Remediation Options for directions on enabling Automatic Remediation and specifying its default settings

What's New in the May 29, 2020 Release

Enhancement

- You can now customize email alerts to the recipient. You can either save your changes to be used later during Incident creation or restore the default text. For information, refer to Setting Default Remediation Options. [BNFIR-757]

What's New in the May 26, 2020 Release

Enhancement

- On the Incidents page, the Email and Users tables at the bottom of the page are now paginated, eliminating the need for scrolling. [BNFIR-532]

Fix

- On the Incidents page, the Summary box in the top right corner of the page now includes a count of all emails deleted, including those remediated through continuous remediation. Before, the count stopped at 1000. [BNFIR-532]

What's New in the May 11, 2020 Release

Enhancements

- The system can now automatically create incidents for and remediate user-reported emails with

malicious links. See the following articles for more information:
  - Automatic Remediation for background information
  - Reviewing Incidents for the new Threats tab associated with Automatic Remediation
  - Setting Default Remediation Options for directions on enabling Automatic Remediation and specifying its default settings

Known Issue

- When exporting to CSV files, there is currently a 2000 row limit.

What's New in the April 27, 2020 Release

Enhancements

- **Potential Incidents** – Can now send alerts when a potential incident is created. For details, see Potential Incidents.
- **Incident Wizard** – Your search criteria now appear at the top of the second page. When creating an incident from certain locations, the wizard automatically skips the first page and goes straight to the second page. If needed, you can click **Refine Search** and change your search criteria.

What's New in the April 13, 2020 Release

Enhancements

- **User-Reported Emails Page** For details, see User-Reported Emails.
  - Malicious URLs: Display a warning icon when a malicious URL is detected. [BNFIR-647]
  - New columns: **Number of Users Reported** and **Number of Mailboxes Affected** [BNFIR-688]
  - Settings: Can now send alerts when a user reports a suspicious email. [BNFIR-799]
- **Insights Page**
  - Terminology: Changed the value **Unknown** to **Undetected**. For details, see Reviewing Insights. [BNFIR-574]

Known Issue

- In the **User-Reported Emails** page, for a specific email, you might see the same user listed twice when you hover over the **Number of Users Reported** value. This happens in the unlikely case where the same user reports more than one email with similar attributes that would match in a search. For example, if the same user separately reported two emails that both had the word *winner* in the subject line, that user will appear twice when you hover over the **Number of Users Reported** value.

What's New in the March 30, 2020 Release

Enhancements

- **Potential Incidents** – Barracuda Forensics & Incident Response can now locate potential threats looming in your Office 365 account, either based on an incident you already created or based on Barracuda Networks' intelligence on currently circulating threats, threats that might already be present in your inbox. See Potential Incidents for more information.
- **User-Reported Emails** – User-reported emails with the same search criteria are now grouped by the user who created them. [BNFIR-688]

Fixes

What's New in the March 16, 2020 Release

Enhancement

- **Expiration Date Banner** – A banner now appears across the top of your Barracuda Forensics pages, indicating the end date of either your free trial or paid subscription. The banner changes color as the date approaches. You will also receive an email as the expiration date approaches. [BNFIR-690]

What's New in the March 2, 2020 Release

Enhancements

- **What's New feature** added in the upper right corner of Barracuda Forensics pages, enables you to find out about new features, improvements, fixes, and scheduled maintenance. [BNFIR-278]
- **Who created an incident** – On the Incidents page, you can now see which Barracuda Forensics administrator created the incident. [BNFIR-653]

What's New in the February 18, 2020 Release

Enhancement

- **Sent emails** – Barracuda Forensics now remediates sent emails. [BNFIR-564]
- **Opened email** – When viewing an Incident, there is a new column in Users table that indicates

whether a user opened an email. See Reviewing Incidents for more information. [BNFIR-548]
- **Editing your serial number** – You can now input your serial number by yourself. [BNFIR-693]

What's New in the January 21, 2020 Release

Enhancement

- **Incidents Table** – Periodically refresh incidents table to provide most current results. [BNFIR-589]

What's New in the January 7, 2020 Release

Enhancement

- **Improved Searching** – You can now create an incident using phrase searching. For more information, see Searching for Messages and Creating an Incident. [BNFIR-588]

What's New in the December 17, 2019 Release

Enhancement

- **Improved User Experience –** Moved incident creation to end of the wizard. [BNFIR-561]

What's New in the November 22, 2019 Release

Enhancements

- **Incident Creation Wizard** – Minor changes to workflow:
  - Incident creation is later in the process [BNFIR-561].
  - Remediation action shows number of emails, no longer number of users. [BNFIR-522]
- **User's First Time Linking to Forensics** – When a user clicks a link to move from either Barracuda Email Security Service or Barracuda Sentinel to Barracuda Forensics for the first time, an intermediate page displays, informing the user they are moving to a different product and asking if they want to begin a 14-day free trial of Barracuda Forensics. If the user continues, they are brought to the appropriate page in Barracuda Forensics. [BNFIR-543]

What's New in the October 1, 2019 Release

Enhancements

- **Standalone** – Barracuda Forensics & Incident Response is now a standalone product.