Release Notes

https://campus.barracuda.com/doc/14464/

What's New in June 2025

- BarracudaONE account switching support has been added for Incident Response.
- A new message log incorporating logs from Impersonation Protection, Incident Response and Email Gateway Defense is now available.

What's New in April 2025

- Our simplified onboarding wizard for Email Protection customers and trials is now available. This update introduces a streamlined, step-by-step experience for setting up key features, including Email Gateway Defense, Impersonation Protection, and Incident Response.
  Stay tuned for upcoming enhancements, including the ability to easily configure mail flow through Inline Deployment.

What's New in February 2025

- All features and functionality of Barracuda Incident Response are included with any of the currently available Barracuda Email Protection plans. The legacy Email Protection Advanced plan did not include all functionality for Incident Response. Talk to your Barracuda Sales representative to upgrade to a current plan.

What's New in January 2025

- Links from Allowed Senders will no longer be clicked by Barracuda. This allows proper functioning of one-time-use links and training campaigns that use phishing techniques.

What's New in December 2024

- The Allowed Senders list is editable from both Barracuda Incident Response settings and Barracuda Impersonation Protection settings.

What's New in November 2024

- Automatic remediation is now available for verified threats. Malicious emails that are identified and reviewed by Barracuda are visible as threat insights. You can choose to have these automatically remediated across your environment.

What's New in October 2024

- An updated Best Practices guide for configuring Barracuda Impersonation Protection and Barracuda Incident Response is available.

What's New in September 2024

- Improved the Business Email Compromise (BEC) machine learning classifier, doubling the rate of detection of BEC emails.

What's New in August 2024

- Updated User Interface aligns all Email Security capabilities to the same design and navigation experience.

What's New in April 2024

- The time and day can be selected for a report to be generated and delivered via email.

What's New in March 2024

- Incident Response offers a variety of new reports, which can be customized and saved. Reports can be generated and delivered via email on the day and time you select. Up to 10,000 lines can be exported from any report.
- Incident Response can send a list of users involved in an incident to Security Awareness Training. They can then be trained to recognize malicious emails and receive follow up testing.

What's New in June 2023

- The external recipients of incident messages can now be seen under the **Users** tab in the **Incident** details. See Reviewing Incidents for more information.
- Emails that are part of Security Awareness Training campaigns will be marked as such in the **Subject** column.

What's New in May 2023

- Email subject searches include words related to your search terms unless searching for an exact match.

What's New in February 2023

- Incident Response works with Barracuda CloudGen Access to automatically create a policy that blocks all traffic from a domain.

What's New in September 2022

- 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 August 2022

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

What's New in July 2022

- 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 April 2022

- 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 March 2022

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

What's New in January 2022

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

What's New in December 2021

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

What's New in October 2021

- 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 September 2021

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 September 2021

- 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 May 2021

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

What's New in March 2021

- 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 February 2021

- During the startup process, Barracuda 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 January 2021

- 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 December 2020

- 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 November 2020

- 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 October 2020 (Version 2.0)

- 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 July 2020

- 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 July 2020

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

What's New in June 2020

- 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 June 2020

- 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 May 2020

- 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 May 2020

- 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 May 2020

- 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 April 2020

- **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 April 2020

- **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 March 2020

- **Potential Incidents** – Barracuda 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]

What's New in March 2020

- **Expiration Date Banner** – A banner now appears across the top of your Barracuda Incident Response 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 March 2020

- **What's New feature** added in the upper right corner of Barracuda Incident Response 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 Incident Response administrator created the incident. [BNFIR-653]

What's New in February 2020

- **Sent emails** – Barracuda Incident Response 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 January 2020

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

What's New in January 2020

- **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 December 2019

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

What's New in November 2019

- **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 Incident Response** – When a user clicks a link to move from either Barracuda Email Security Service or Barracuda Sentinel to Barracuda Incident Response 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 Incident Response. If the user continues, they are brought to the appropriate page in Barracuda Incident Response. [BNFIR-543]

What's New in October 2019

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