Overview

https://campus.barracuda.com/doc/79463558/

Be sure to read about License Definitions for the Barracuda Email Protection plan.

The functionality described in the following articles is available only with Incident Response, available only with Barracuda Email Protection Premium and Premium Plus plans. These individual articles are also labeled with this information. To upgrade to one of these plans, contact your Barracuda Networks Sales Representative.

- Automated Workflows
- Creating an Incident
- Public API Overview (along with the articles for public APIs: Get Accounts, Get Tenants, Create Incident, Get Incident, Get Incidents, and Get User-Reported Emails)
- Reviewing Insights
- Portions of User-Reported Emails
- Portions of Integration with Other Barracuda Networks Features
- Settings
  - Automated Workflows Settings
  - Manual Remediation Settings

Automatic Remediation – Automatic Remediation can automatically remediate email messages that contain malicious URLs or attachments. All user-reported messages are automatically scanned for malicious content. When a threat is detected all matching emails are moved from users' mailboxes into their junk folders. Security teams will receive an alert notifying them of an incident.

Incident Response (included with Barracuda Email Protection Premium and Premium Plus plans) – Remediate threats quickly and efficiently, by automating investigative workflows and enabling direct removal of malicious emails. Take advantage of fully-automated, post-delivery incident response and threat-hunting capabilities.

Minimum Requirements

To use Automatic Remediation or Incident Response, you must have:

- Microsoft 365

Your first login requires Microsoft 365 global administrator credentials.

Optional Integration

Accounts for the following products add the functionality listed below, but are not required for Incident Response.

These features are included in Barracuda Email Protection plans. DNS Filtering is available in Barracuda Email Protection Premium and Premium Plus plans.

Email Gateway Defense

- Creating a new incident.
- Working with geographical insights.
- Working with emails users reported as suspicious through
  - the Barracuda Outlook Add-in.
  - the Message Log in Email Gateway Defense.

For a description of configuration requirements for integration, refer to Integration with Other Barracuda Networks Features.

DNS Filtering

- Adding block exception policies for linked domains.

Impersonation Protection

- Remediating incidents found in Impersonation Protection.

Getting Started

Before You Begin

Provision Incident Response in Barracuda Cloud Control. For details, refer to Account Administrator Actions in the Barracuda Cloud Control documentation.

Accessing Incident Response

To access Incident Response:

- Log in through Barracuda Cloud Control.
- Open https://forensics.barracudanetworks.com in a browser.

Your First Login

This process requires Microsoft 365 global administrator credentials.

Log into Barracuda Cloud Control – https://login.barracudanetworks.com/account/office365. If you do not already have an account, you can create one here.
To activate Incident Response:

1. In the left navigation panel, select **Incident Response**.
2. Follow on-screen instructions to connect your Microsoft 365 account.
3. Within Incident Response, on the top menu bar, click the blue box to enter your serial number and linking code.

- **Bootstrapping/Initial Information Loading** – The first time you log in, Incident Response must connect to your Microsoft 365 account and load your email information for the last 30 days. This process can take anywhere from an hour to a day or more, depending on the volume of email in your account.
- **Reporting Suspicious Messages** – When you first start using Incident Response, wait about one hour before reporting suspicious messages with the Outlook Add-in. It takes about an hour for the two systems to coordinate. See User-Reported Emails for information on how to report messages.
- **Serial Number and Linking Code** – With your purchase, you received an email from Barracuda Networks that includes your serial number and linking code. Follow the instructions in the email for entering this information and getting started.
  If you are evaluating Incident Response as a free trial, you will not receive this email.