Overview

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

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

If you have purchased Barracuda Total Email Protection, in addition to this Barracuda Forensics & Incident Response documentation space, see the following Campus content:

- Barracuda Essentials
- Barracuda PhishLine
- Barracuda Sentinel

Barracuda Forensics & Incident Response enables your IT team to identify, track, and resolve email attacks from outside or inside your organization, for example, a phishing or ransomware attack. You can search for any allowed email (by subject and/or sender) that your users may report to you as malicious and perform remediation action on the same. Remediation options include the ability to delete a message in a user's inbox, and the ability to send an incident summary to the user. If users click on a fraudulent link in an email, Barracuda Forensics & Incident Response allows you to identify these users for potential security concerns on their workstations, and determine if additional security actions are necessary.

Minimum Requirements

To use Barracuda Forensics & Incident Response, you must have:

- Microsoft Office 365

Optional Products: Accounts for the following products add the functionality listed below, but are not required for Barracuda Forensics & Incident Response.

Barracuda Email Security Service

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

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

Barracuda Content Shield

- Adding block exception policies for linked domains.

Barracuda Sentinel

- Remediating incidents found in Barracuda Sentinel.

Getting Started

To access Barracuda Forensics & Incident Response:

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

- **Bootstrapping/Initial Information Loading** – The first time you log in, Barracuda Forensics & Incident Response must connect to your Office 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 Barracuda Forensics & 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** – If you purchased Barracuda Forensics & Incident Response (standalone or as part of a bundle), you will receive an email from Barracuda 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 Barracuda Forensics & Incident Response as a free trial, you will not receive this email.