

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 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 reported as suspicious through
 - the [Barracuda Essentials Outlook Add-in](#).
 - the [Message Log in Barracuda Email Security Service](#).

The following settings are required if you are using Barracuda Forensics & Incident Response with

Barracuda Email Security Service to take advantage of the functionality described in [Integration with Other Barracuda Products](#).

Shared Account

To fully enable this integration, you must use a common account for both products. When you initially sign up for Barracuda Forensics & Incident Response, be sure to select the same account that you are using for Barracuda Email Security Service. If your user is associated with more than one Barracuda account, these accounts are displayed in a menu where you can choose the correct account.

Verified Domains

Verifying domains is essential for mail to flow through Barracuda Email Security Service and, in turn, for Barracuda Forensics & Incident Response to work with the emails. As described in [Understanding the Domains Page](#), each of the domains where you want to filter email must be verified by the Barracuda Email Security Service for proof of ownership; the Barracuda Email Security Service does not process email for a domain until the verification process is complete. See [Understanding the Domains Page](#) and the [deployment process](#) for your specific platform for more details.

Link Protection Feature

The Link Protection feature in Barracuda Email Security Service (part of Barracuda Essentials) is required for the functionality of the **Users at Risk** feature.

Ensure that the [Link Protection](#) feature is turned ON for the appropriate accounts and domains.

If Link Protection is turned OFF when a suspicious email is received, users that are potentially affected by that incident might not be listed as **Users at Risk** and might not receive the proper remediation and attention.

Link Protection must be turned ON when emails are received to provide complete results for **Users at Risk** for a specific incident. Turning Link Protect ON after a suspicious email has already been received will not change the **Users at Risk** results for an incident involving that email.

[Barracuda Content Shield](#)

- Adding block exception policies for linked domains.

[Barracuda Sentinel](#)

- Remediating incidents found in Barracuda Sentinel.

Logging In

Sign into Barracuda Forensics & Incident Response at <https://forensics.barracudanetworks.com>.

In this Section

© Barracuda Networks Inc., 2020 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.