

Barracuda Forensics & Incident Response and DNS Filtering With Barracuda Content Shield

<https://campus.barracuda.com/doc/84312558/>

This article explains how Barracuda Content Shield (BCS) DNS Filtering can integrate with Barracuda Forensics & Incident Response to better protect your users from receiving malicious or suspicious emails.

If you do not yet have a BCS account, visit <https://www.bcs.barracudanetworks.com/trial> to start your free trial. For more information about Barracuda Forensics & Incident Response, see [Overview of Barracuda Forensics & Incident Response](#).

After you have set up your BCS account, you can configure Barracuda Forensics & Incident Response to work together with BCS on incident remediation. To do so, in your Barracuda Forensics & Incident Response account, enable the **Block all user web traffic for domains contained in links** feature (see [Creating an Incident](#)). This action creates new exceptions that block web traffic from the domains contained in incident email for every **DNS Location** you have configured in BCS (see the [DNS Filtering](#) page). These new BCS exceptions will be labeled as having been created by Barracuda Forensics & Incident Response.

If you have already created a policy or policies on the **DNS Filtering** page, edit the existing policy for each DNS Location by clicking **Categories** in the table.

1. In the **Categories** screen of the **Add Location** wizard, select the following categories from the **Security** section, which Barracuda recommends for the default policy to integrate with your Barracuda Forensics & Incident Response service.
 - Malicious Sites
 - Phishing & Fraud
 - Spam
 - Spyware
 - Suspicious Sites
2. Click **Next**.
3. Continue with the wizard, creating exceptions as needed. See [How to Configure DNS Filtering Policies](#) for more detail

If you are creating a new DNS Location, following instructions in the **Configure a New Filtering Policy For a Network** section of [How to Configure DNS Filtering Policies](#) and incorporate the steps below.

1. In the **Categories** screen of the **Add Location** wizard, in the **Category Policy** drop-down, select *Custom*. This clears all categories.
2. Next, select the following categories from the **Security** section, which Barracuda recommends for the default policy to integrate with your Barracuda Forensics & Incident Response service. Then click **Next**.

- Malicious Sites
 - Phishing & Fraud
 - Spam
 - Spyware
 - Suspicious Sites
3. Continue with the wizard, creating exceptions as needed. See [How to Configure DNS Filtering Policies](#) for more detail.

TIP: When you create a *Custom* policy, it is saved in the list of category policies which can be used later if you add additional locations. This allows you to easily duplicate the same policy across your locations in the future, and there is no limit on the number of locations you can add in one BCS account.

© Barracuda Networks Inc., 2021 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.