

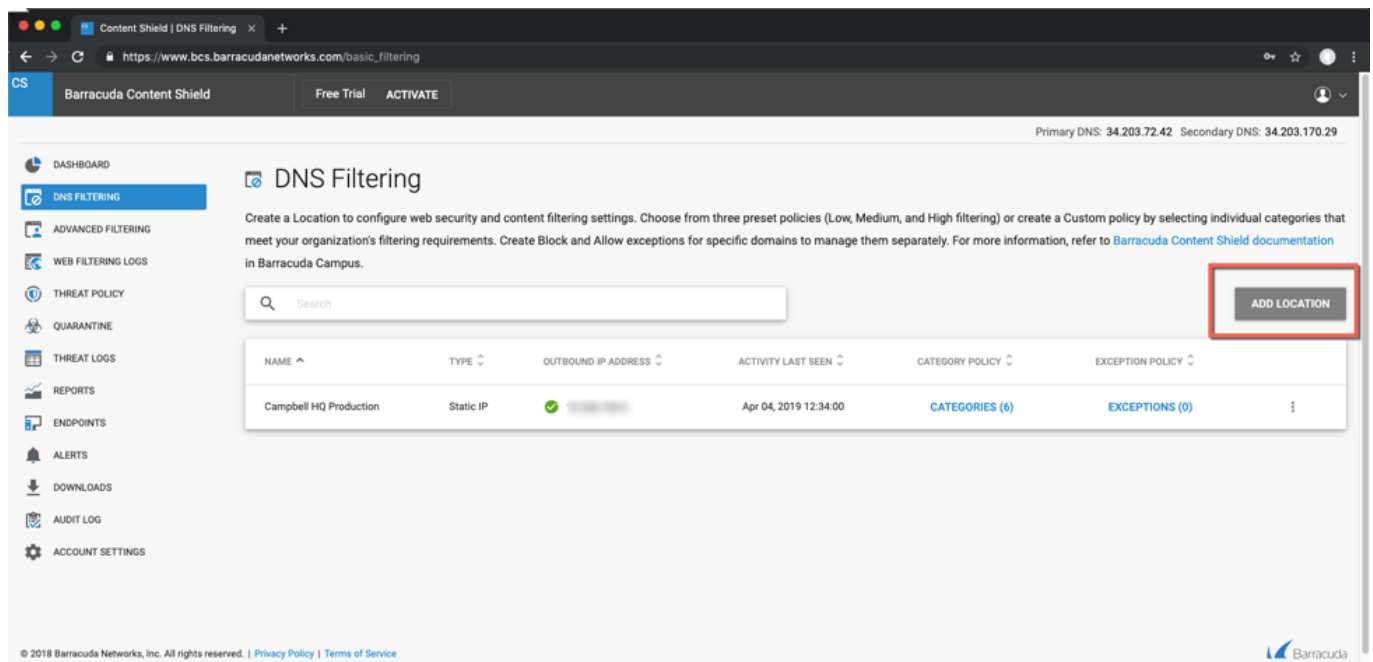
Barracuda Content Shield Evaluation Guide with Incident Response

<https://campus.barracuda.com/doc/91980505/>

If you are using Incident Response and want to evaluate how it integrates with Barracuda Content Shield (BCS), follow this guide for basic configuration. For more about options to configure in BCS, see [Barracuda Content Shield Overview](#). If you have a BCS free trial and want to convert it to a licensed subscription, see [Converting Your Trial Subscription to a Valid License](#).

Step 1. Configure BCS DNS Based Filtering

The first step is to register your egress IP address with BCS. If you are unsure of your egress IP address, you can use a site like **whatismyip.com** to determine what it is. Navigate to the **DNS filtering** page using the left navigation menu and select **ADD LOCATION**. Follow steps in the wizard to complete adding the location.



The screenshot shows the Barracuda Content Shield web interface. The top navigation bar includes 'Barracuda Content Shield', 'Free Trial', and 'ACTIVATE'. The left sidebar lists various menu items, with 'DNS FILTERING' selected. The main content area is titled 'DNS Filtering' and contains instructions on how to create a location. Below the instructions is a search bar and a table of existing locations. The 'ADD LOCATION' button is highlighted with a red box.

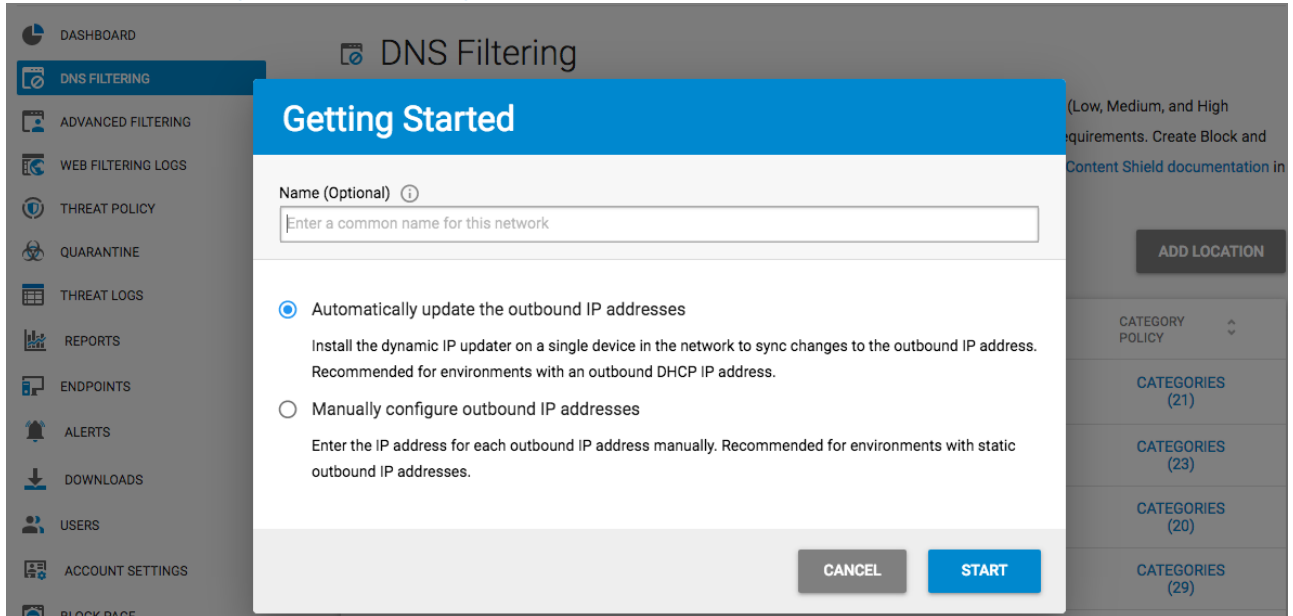
NAME	TYPE	OUTBOUND IP ADDRESS	ACTIVITY LAST SEEN	CATEGORY POLICY	EXCEPTION POLICY
Campbell HQ Production	Static IP	✓	Apr 04, 2019 12:34:00	CATEGORIES (6)	EXCEPTIONS (0)

Configure the IP address, either automatically or manually, in the **Getting Started** screen as shown below:

- Use the *Manual* setting if your ISP provides a static IP address that does not change. Click **Start**, and follow the prompts in the wizard.
- Use the *Automatic* setting if your ISP provides a dynamic IP address. Click **Start**, and follow the prompts in the wizard. In this case, you must install the [Dynamic IP updater](#) on a single machine

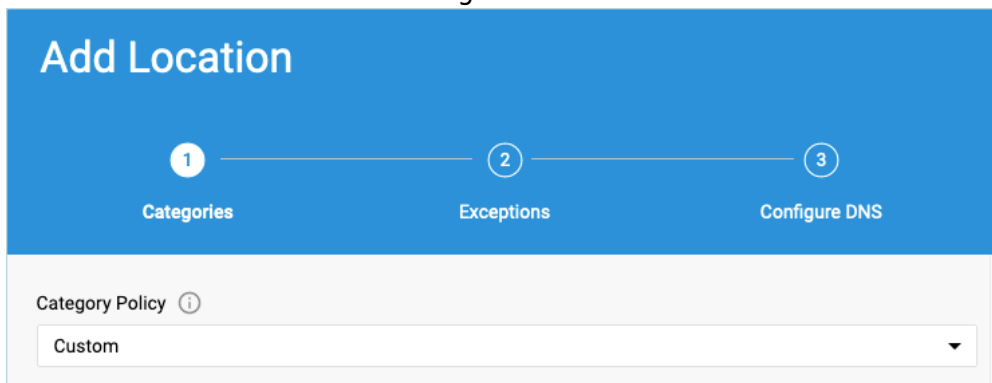
that permanently resides within the environment. This allows the BCS service to be updated automatically when your IP address changes. The final step of the wizard provides links to download the Dynamic IP updater and installer key.

See [How to Configure DNS Filtering and Policies](#) for details.



Step 2. Create Filtering Policies to Work With Incident Response

1. In the **Add Location** screen of the wizard as shown below, in the **Category Policy** drop-down, select *Custom*. This clears all categories.



2. Next, select the following categories from the **Security** section as the default policy to integrate with your Incident Response service. Then click **Next**.
 - Malicious Sites
 - Phishing & Fraud
 - Spam
 - Spyware
 - Suspicious Sites

Add Location

1 Categories
2 Exceptions
3 Configure DNS

<input type="checkbox"/> ADULT MATERIAL <input type="checkbox"/> Adult Content <input type="checkbox"/> Incidental Nudity <input type="checkbox"/> Intimate Apparel & Swimwear <input type="checkbox"/> Nudity <input type="checkbox"/> Personals & Dating <input type="checkbox"/> Pornography <input type="checkbox"/> Text/Audio Only <input type="checkbox"/> COMMERCE & SHOPPING <input type="checkbox"/> Advertisements & Popups <input type="checkbox"/> Auctions & Classifieds <input type="checkbox"/> Business <input type="checkbox"/> Finance & Investment	<input type="checkbox"/> ILLEGAL OR IMPROPER <input type="checkbox"/> Academic Cheating <input type="checkbox"/> Alcohol & Tobacco <input type="checkbox"/> Criminal Activity <input type="checkbox"/> Extremely Offensive <input type="checkbox"/> Gambling <input type="checkbox"/> Gambling Related <input type="checkbox"/> Illegal Drugs <input type="checkbox"/> Illegal Software <input type="checkbox"/> Intolerance & Hate <input type="checkbox"/> Profanity <input type="checkbox"/> Tasteless & Offensive <input type="checkbox"/> NEWS & INFORMATION	<input checked="" type="checkbox"/> SECURITY <input type="checkbox"/> Hacking <input type="checkbox"/> Information Security <input checked="" type="checkbox"/> Malicious Sites <input checked="" type="checkbox"/> Phishing & Fraud <input type="checkbox"/> Proxies <input type="checkbox"/> Proxy Utilities <input checked="" type="checkbox"/> Spam <input checked="" type="checkbox"/> Spyware <input checked="" type="checkbox"/> Suspicious Sites <input type="checkbox"/> SOCIETY & LIFESTYLE <input type="checkbox"/> Advocacy & NGO <input type="checkbox"/> Fashion & Beauty
--	---	---

See [How to Configure DNS Filtering and Policies](#) for more information.

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.

3. After you click **Next**, you have the opportunity to create any *block* or *allow* exceptions to your category policy. You can block or allow specific domains (ex: *google.com*) or subdomains (ex: *mail.google.com*). There is no need to specify protocols like HTTP or leading with www. [Exceptions](#) take precedence over category policies and can be set to *block* or *allow*.
4. The final step shows the DNS servers, as shown below, that you will provide to all of the clients on the network being filtered. Barracuda Networks recommends initially setting these DNS servers manually on the systems you are going to test policy with. After you are satisfied with your policy, these DNS servers can be added to your DHCP server, which can then pass out the Barracuda DNS IP address to clients connecting to your network. Or, if you have your own

internal DNS server, you can set that up as a conditional forwarder. This allows your DNS server to resolve any internal resources and forward any requests to the BCS service for external resources and filtering based on your set policy. See [How to Configure Barracuda DNS Nameservers for Barracuda Content Shield](#) for details.

Add Location

✓



✓

3

CategoriesExceptionsConfigure DNS

In order to enforce your policy, send traffic from your network to the Content Shield DNS servers. Open the preferences for your router or device and change your DNS server settings to the Content Shield primary and secondary DNS servers listed below.

Need instructions? [Check our list of specific device instructions](#)

PRIMARY DNS SERVER		COPY TO CLIPBOARD
SECONDARY DNS SERVER		COPY TO CLIPBOARD

NOTE: Before changing both the primary and secondary DNS servers it is recommended that you make note of the original settings.

CANCEL

BACK

ADD

How Incident Response Can Automatically Update your BCS Policies

After you have performed this basic configuration of your BCS account, you can set Incident Response to trigger new DNS filtering exceptions when it detects links in emails that were identified as part of an incident. The Incident Response wizard includes a section where the administrator can choose to block all user web traffic for domains contained in these links as part of incident remediation. For BCS, this means that new exceptions to block web traffic for these domains will be created for every DNS location configured on the [DNS Filtering](#) page.

Step 3. Evaluate Agent-Based Protection at the Endpoint

As stated above, to provide DNS-based filtering for clients that are outside of the network, you must install the Barracuda Content Shield (BCS) agent on endpoint computers. The agent can enable the BCS Plus features on endpoints, including [Advanced Filtering Policies](#). For more information,

see [Barracuda Content Shield Agent for Endpoints](#).

Figures

1. DNS FilteringPage.png
2. ConfigOutboundIPAddress.png
3. SelectCustomPolicy.png
4. SitesToBlock.png
5. DNSServers.png

© Barracuda Networks Inc., 2024 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.