

How to Configure Barracuda DNS Nameservers for Barracuda Content Shield

<https://campus.barracuda.com/doc/78152405/>

In order to use the Barracuda DNS Filtering Service with Barracuda Content Shield, you must direct your router, firewall, or your computer(s) (laptop / desktop) to the assigned Barracuda Domain Name Server (DNS). The IP address for the Barracuda DNS nameserver is shown on the **Configure DNS** step (3) of the **Add Location** popup, which you access on the **DNS FILTERING** page.

Important: If you do not configure the primary DNS nameserver as described in this article, then forwarding user web traffic will stop internet traffic from flowing. Make sure to configure user Locations on the **DNS Filtering** page so that when you forward the traffic, it will function properly.

Ensure DNS Traffic Is Routed from Clients to the Barracuda DNS Nameserver

Use one (or more) of the methods below. It is easier to configure the primary DNS nameserver at the network level rather than to configure on every client machine. You can also create a policy that only allows DNS requests to the Barracuda DNS nameservers as a means of preventing users from circumventing the service. You can also use a GPO or similar RMM tool to lock the DNS nameserver settings from being modified by end users.

- Using a Barracuda Firewall or other firewall solution: Configure your Barracuda NG Firewall or Barracuda CloudGen firewall solution to determine which DNS requests are for internal domains and process those, but restrict external DNS requests from clients to Barracuda DNS nameservers. For the Barracuda CloudGen Firewall, see the article on [DNS](#) which describes using the Barracuda CloudGen Firewall as a DNS server. Also see [How to Configure DNS settings](#) for the Barracuda CloudGen Firewall configuration.
- Configure your router: It is easier to configure the primary DNS nameserver on the router for the network than to configure on all client machines, and this prevents users from circumventing DNS settings. Follow general instructions [for routers](#).
- Configure local DNS server: If using a local DNS server, configure it to forward DNS requests from clients to the Barracuda DNS Nameserver. See [How to Configure a Local DNS Server to Forward to Barracuda DNS Nameservers](#).
- Configure each client machine: See general instructions for your operating system below. You must also secure the settings on your clients so that users cannot change their local DNS server IP addresses.
 - [How to Configure Barracuda DNS Nameservers on Windows 10](#)
 - [How to Configure Barracuda DNS Nameservers on Windows 8](#)
 - [How to Configure Barracuda DNS Nameservers on Mac OS X](#)

Using DHCP and Proxying DNS Requests to Barracuda

If you are using DHCP, configure the DHCP server to provide the Barracuda DNS nameserver IP address to clients with their dynamic IP address.

- For information on setting DHCP DNS addresses for clients on the Barracuda CloudGen Firewall, see [How to Configure the DHCP Service](#).
- For the Barracuda NextGen X Firewall, see [How to Configure the DHCP Server](#).

© 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.