Barracuda Endpoint Shield - Administrator's Guide - Page

Overview

Barracuda Content Shield (BCS) is a service for MSPs managing multiple small and midsize businesses (SMBs) which provides advanced threat protection to users on and off network, with an agent that is deployed to each client.

Traditional signature-based anti-virus solutions are no longer sufficient to defend against new breed of malware attacks. This has resulted in the emergence of heuristic-based anti-virus solutions and advanced threat protection solutions with sandboxing capabilities.

Key Features:

- High level summary of statistics for all accounts showing daily threat activity, scanned files and users affected.
- A dashboard view for each account shows threat activity specific to usernames, endpoints and time frames.
- Reports provide multiple views of threat activity by time, date, user and endpoint.
- Customizable content filtering by categories, with ability to create exceptions by domain.

Dashboard for Managing Accounts - DNS Filtering Subscription

View the Dashboard for Any Account

From the **Accounts** page, you can view the Dashboard for each account you've created. In the **Accounts** table, click **Manage** in the **Action** colu mn. For each account, the Dashboard page is divided into the following panes, displaying data for the last 24 hours:

- **Malware Prevention**: Displays traffic blocked in the *Malware* category.
- **Phishing Prevention**: Displays traffic blocked in the *Phishing & Fraud* categories.
- **Web-Based Threats**: Displays traffic blocked in the *Spyware* category.
- **Blocked Requests**: Displays the total number of blocked requests.

Use this Page to Revise Your Filtering Policies

The right pane of the page displays the **Blocked Supercategories** and the **Top Blocked Categories** tabs. Click on either tab to view the **Count** and **Trend** of number of requests blocked by category or supercategory. The statistics displayed on this page indicate what kind of activity is being blocked for your clients. Tune your policies as needed on the **DNS Filtering** page, as described in How to Configure DNS Filtering Policies.

Adjust the time frame for the **Blocked Supercategories** and the **Top Blocked Categories** tabs at the bottom of the right pane. Select **Last 24 hours**, **Last 7 days**, or **Last 14 days**.

Click **View Report** to go to the Reports page, to create and schedule reports. See Reports for details.

Navigation from the Dashboard

The following screens are available from the Dashboard page left navigation pane:

- **DNS Filtering** – Create, review or delete preset or customized filtering policies by categories of domains. See How to Configure DNS Filtering Policies for details.
- **Web Filtering Logs** – View the allowed and blocked traffic logs. See Web Filtering Logs for details.
- **Reports** – Create or schedule reports on Blocked Categories or Blocked Supercategories. See Reports for details.
- **Alerts** – Create notifications to specific recipients based on a selected event (Notification Type). See Alerts for details.

Reports

The **Reports** page provides administrative reports, based on the type and time frame you select.

Viewing and Downloading a Report Immediately

Viewing a Report

To view a report:

1. Select a **Time Frame**: **Last 24 Hours**, **Last 7 Days**, or **Last 30 days**.
2. Select a **Report Type**:
   - **Blocked Supercategories** – Bar graph and table showing number of blocked requests by supercategory for the selected time frame.
   - **Blocked Categories** – Bar graph and table showing number of blocked requests by category for the selected time frame.
3. Click **View** to see the report in a new browser tab.

Downloading and Saving a Report

Click **PDF Report** or **CSV Report** to download and save the report data. Saving as a PDF maintains the graphic element of the report.

Scheduling a Report to Run Automatically

Scheduling a Report

To schedule a report to run automatically, on a set schedule:

1. Click **Schedule**.
2. Select a **Report Type**:
   - **Blocked Supercategories** – Bar graph and table showing number of blocked requests by supercategory for the selected time frame.
   - **Blocked Categories** – Bar graph and table showing number of blocked requests by category for the selected time frame.
3. Select a **Time Frame**: **Last 24 Hours**, **Last 7 Days**, or **Last 30 days**.
4. Select the **Frequency** for running the report, along with any additional specification needed:
   - **Hourly** – (No further specification needed.)
   - **Daily** – Specify the hour.
   - **Weekly** – Specify the day of the week and the hour.
   - **Bi-Weekly** – Specify the day of the week and the hour.
   - **Monthly** – Specify the day of the month and the hour.
5. Specify the **Email Recipients** who will receive these automatic reports. For multiple email recipients, enter each email on a separate line.

Taking Action with a Scheduled Report

To generate a scheduled report immediately, select the report in the **Scheduled Reports** section, then click **Run Now**.

To edit or delete a scheduled report, in the **Scheduled Reports** section, click the More Options icon (⋮) and select the appropriate action.

Alerts

Use the **ALERTS** page to create notifications to specific recipients based on a selected event (Notification Type). Alert notifications are generated for *blocked* categories only.

1. On the **Alerts** page, click **Add Alert**.
2. In the popup, select **Notification Type**.
   - **Blocked Category** – An alert is sent to recipients when the **Category** you select in the next dropdown is blocked (for the number of times specified in the **Alert Condition** below).
   - **Command and Control Communications** – An alert is sent to recipients when any type of Command and Control communication occurs (for the number of times specified in the **Alert Condition** below). For example, an alert is sent when communication is sent to a known Command and Control domain, like Malicious Sites or Suspicious Sites.
3. Set the **Alert Condition** level for the number of times the event selected above must occur within a 24 hour period to trigger an alert. For example, if a domain in the blocked category *Personals & Dating* is requested more than 2 times in 24 hours, you want the service to send an alert notification to the email recipient(s) you specify below. Select **Any Category** to be alerted to blocks regardless of their category.
4. Enter one or more **Email Recipients**, with each email address on a separate line in the text box.
5. Click **ADD**.

After you have added an alert, you can click the More Options icon (⋮) in the table to take one of the following actions:

- **Edit** – Modify the **Notification Type**, **Category**, **Alert Condition**, or **Email Recipients** for the alert.
- **Suspend** – Temporarily disable the alert. You can **Resume** the alert in the future without having to add it again.
- **Delete** – Delete the alert from the system.

Audit Log

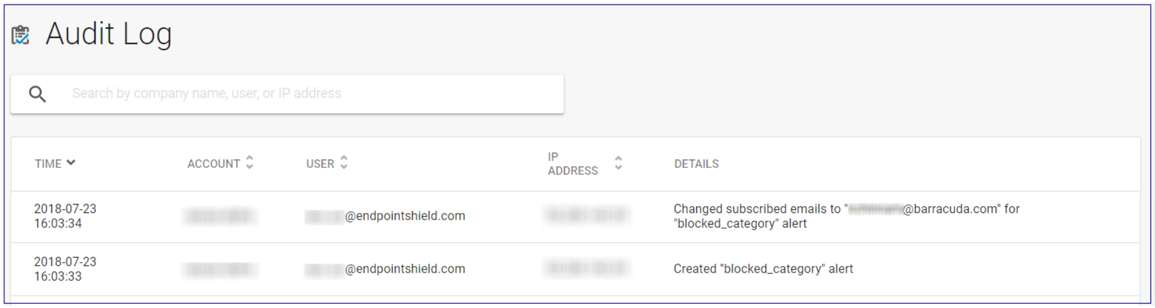
The **Audit Log** is a record of every change the administrator makes in an account.

On the **Audit Log** page, search by Account, User, or IP Address. It can be sorted by:

- Time
- Account
- User
- IP Address of the endpoint

Example

An administrator creates a Blocked Category alert, then changes the email associated with that alert. In the Audit Log, you can see the actions taken by the administrator:



Audit Log

Search by company name, user, or IP address

TIME	ACCOUNT	USER	IP ADDRESS	DETAILS
2018-07-23 16:03:34	[redacted]	[redacted]@endpointshield.com	[redacted]	Changed subscribed emails to "[redacted]@barracuda.com" for "blocked_category" alert
2018-07-23 16:03:33	[redacted]	[redacted]@endpointshield.com	[redacted]	Created "blocked_category" alert

How to Configure DNS Filtering Policies

Configure DNS Filtering by outbound IP address (network) with Barracuda Content Shield by selecting either a pre-configured filtering level, as described below, or a custom set of categories of domains. Based on what you select, you can set block/allow policies by content category for web traffic by network IP address. Traffic affected by the DNS filtering policies is logged in the Web Filtering Logs.

> **Best Practice**
> Barracuda recommends testing your initial selection of block/allow policies using various domains that you know you want blocked, and/or that you know your organization needs to access, and then make updates to your policies as needed, as described in this article.

View Configured Filtering Policies

If you have already configured DNS Filtering for a network, the following displays in a table on the **DNS FILTERING** page:

- Name – The name you (optionally) gave to the network when it was added to the system
- Type – Dynamic IP or Static IP
- Outbound IP Address – Identifies the network
- Activity Last Seen – Timestamp of the last traffic seen
- Category Policy – Click to see which content categories are blocked, and to change the selection of categories if needed
- Exception Policy – Click to see block or allow exceptions you created for the list of categories, and to add or delete exceptions

Edit or Delete a Set of Filtering Policies

At the right of a table row, click More Options (⋮) to edit the entry for a network or delete the entry for a network and associated DNS Filtering policies, or to download the Barracuda Dynamic IP Updater to install on a client machine (see step 2b below for details).

Configure New Filtering Policies for a Network

1. Go to the **DNS FILTERING** page.
2. To begin using the wizard, click **Add Location**.
    a. *Optional*: Enter a name you want to use to identify the network.

   b. Select one of two methods of how to specify an outbound IP address for clients. Barracuda Content Shield policies that you configure are applied according to the outbound IP address associated with each client.
      - If the outbound IP address for each client is dynamic (changes periodically), choose **Automatically update the outbound IP addresses**. This will lead you to the Barracuda Dynamic IP Updater installation at the end of the wizard. The Dynamic IP Updater is a tool that installs on a client and runs periodically to sync clients and their current IP address with the Barracuda DNS Filtering service. Click **Start** and skip to **Step 3.**
        – OR –
      - If the outbound IP address for each client is static (remains the same, as opposed to dynamic), choose **Manually configure outbound IP addresses** and continue with step **c**.

   c. If you selected **Manually configure outbound IP addresses**, after clicking **Start**, the **Outbound IP Address** page of the wizard displays. Enter the IP address of the network for outbound web traffic you want to filter with the policies you will create in this wizard. The **Outbound IP Address** (also known as a "public IP address") can commonly be found on the *status* screen or similar screen of most routers.

   d. Enter the **Prefix**.The prefix length shows the number of bits set in the subnet mask; for instance, if the subnet mask is 255.255.255.0, then there are 24 bits in the binary version of the subnet mask, so the prefix length is 24 bits.

   e. Click **Add Outbound IP Address**. Click **Next**.
      Note: To edit Outbound IP Address, Network Name or Prefix after you have added them, click on the 3 dots at the far right of the entry for that outbound IP address in the table and click **Edit.**

3. In the **Category Policy** window, select a filtering strategy, or Category Policy, depending on your organization's requirements:
   a. Begin by selecting one of the pre-configured *Low*, *Moderate*, or *High* levels from the **Category Policy** dropdown, or select *Custom* to start from scratch. You can modify any level by selecting or de-selecting any category. Or, you can click by a Supercategory to include all categories in that supercategory.
      - Low – includes domains categorized under Security, Illegal Activity, Violence, Pornography, and Adult Content
      - Moderate – includes domains categorized under Security, Illegal Activity, Violence, Media Sharing, and Pornography
      - High – includes domains categorized under Security, Illegal Activity, Violence, Gaming, Media Sharing, and Pornography
      - Custom – includes domains categorized under whichever categories you select on the page

   b. Review the set of content categories. All domains in the categories that are checked will be blocked for this network. Add or remove categories per your organization's requirements. You can also create exceptions to these policies by domain.

   c. Click **Next**.

4. In the **Exceptions** window, you have the option to create exceptions for specific domains from the policies you just created.
   a. To *Allow* traffic from a domain that belongs to a category you configured to block as a general policy, enter the domain name in the search box, select either *Allow* or *Block* in the dropdown, and then click **Add Domain**. That domain is then listed in Exceptions table.

   b. To remove a domain exception, click the Remove icon (🗑) in the row of the table for that domain.

   c. When you are finished creating exceptions, click **Next**.

5. On the **Configure DNS** page of the wizard, note the IP addresses of Barracuda DNS nameservers. You must specify these IP address as the Primary and Alternate (or Secondary) DNS Nameservers on any of the following:
   a. Your network router

   b. Your client machines

   c. Your Barracuda Firewall (or other firewall solution)
      Click **Add** on the wizard to add the network. That network location is then listed in Networks table.
      For more information on configuring the Barracuda DNS namservers for your clients, see How to Configure Barracuda DNS Nameservers for Barracuda Content Shield. If you selected **Manual** for **Outbound IP Address** in step 2b, this concludes the wizard.

6. If you selected **Automatic** for **Outbound IP Address** in step 2b, click **Add**. The Dynamic IP Updater page displays.
   On an endpoint machine, run the Windows Dynamic IP Updater installer, which you can download from the wizard page by clicking on **Download Installer**. Click **Download Key** on the page to get the installer key, which you will use when installing the tool on the endpoint machine. The Windows Dynamic IP Updater only needs to be installed on ONE client machine in the network, and will run periodically to sync clients and their current IP addresses with the Barracuda DNS Filtering service.

Copy Policy from Existing Network

When you create a new network, you can copy the policy and exception configurations you specified when defining earlier networks.

To copy policy from a network you previously defined, follow the instructions in "Configure New Filtering Policies for a Network" above, with the following modifications:

- Step 3: In the **Category Policy** window, under **Custom Policies**, select the name of the network from which you want to copy policies.
- Step 4: In the **Exceptions** window, under **Custom Policies**, select the name of the network from which you want to copy policies.

For both of these steps, you can accept the policies and exceptions that are copied or use them as a starting point and make changes from there.

Adjust Filtering Policies for a Network

After you have created and tested DNS filtering policies, you may need to adjust settings according to the needs of your organization based on the following (or other) reasons:

- Changes in browsing or business policies of your organization
- Need for access to some domains that are included in a category that you need to block, in general

1. Go to the **DNS FILTERING** page.
2. For the network in the **OUTBOUND IP ADDRESS** column for which you want to update policies, click on **CATEGORIES**.
3. (Optional) If you have already defined a network and want to copy its policies: Under **Category Policy**, select the name of the network from which you want to copy policies. Those policies are copied to the network you are currently configuring.
4. Check or uncheck categories for which you want to change your block/allow policies. All domains in the categories you check will be blocked for this network.
5. Click **Save** to save the changes you made.

Web Filtering Logs

The **Web Filtering Logs** show activities related to the DNS filtering policies you configured. For configuration information, refer to How to Configure DNS Filtering Policies.

To access **Web Filtering Logs**, while managing an account, select **Web Filtering Logs** from the left panel.

The **Web Filtering Logs** page displays the date of the activity, whether the attempt was Blocked or Allowed, and information about the domain the user attempted to reach (Categories, Supercategories, and Location Name).

By default, the logs are sorted by date, with recent entries at the top.

Use the **Search** box to filter for **Action**, **Destination Domain**, **Supercategories**, **Categories**, or **Location Name**. You can also specify the time frame for the results: the Last **24 hours**, **7 days**, or **30 days**.

Click **Refresh Logs** to view the latest traffic information. Note that clicking **Refresh Logs** maintains your time frame selection (Last **24 hours**, **7 days**, or **30 days**), whereas performing a browser refresh (pressing F5) reverts to the default **Last 30 days** setting.

To save the data and analyze it, click **Download CSV**.

Dynamic IP Address Updater Tool

DNS filtering policies you create in Barracuda Content Shield are associated with the outbound IP address for all clients on a network. You can either enter the static outbound IP address, if it does not change for clients, in the **Add Location** wizard where you create policies, or you can use the **Dynamic IP Updater** tool provided with the service.

> ⓘ Note that the Dynamic IP Updater:
>
> - Is available only for Windows.
> - Only needs to be installed on ONE client machine in the network, and runs periodically to sync clients and their current IP addresses with the Barracuda DNS Filtering service. That way, your filtering policies are correctly applied to all of the clients on your specified network.

On the DNS Filtering page:

If your client IP addresses are dynamic, for example if you use DHCP or if your ISP assigns dynamic IP addresses to clients, in the **Add Location** wizard, select **Automatically update the outbound IP addresses** for the **Outbound IP Address**. After you create your filtering policies, the **Dynamic IP Updater** page displays. From that page:

1. Click **Download Installer** and save the installer on your local machine or network. Click **Download Key** on the page to get the installer key, which you will use when installing the tool on the endpoint machine.
2. On an endpoint machine, run the Dynamic IP Updater installer.

You can also download the Dynamic IP updater in the network table on the **DNS Filtering** page, under More Options (⋮).

How to Create Exception Policies for DNS Filtering

You can create block or allow exceptions to policies you configured, by domain, as described in How to Configure DNS Filtering Policies. For example, you might want to block the category *Finance and Investment* for your organization, but allow specific bank and brokerage domains so your finance department can do company business.

1. Navigate to the **DNS FILTERING** page.
2. In the **OUTBOUND IP ADDRESS** column, locate the network for which you want to update policies, then click **EXCEPTIONS**.
3. (Optional) If you have already defined a network and want to copy its exceptions: Under **Exception Policy**, select the name of the network from which you want to copy exceptions. Those exceptions are copied to the network you are currently configuring.
4. Select *Allow Traffic* or *Block Traffic*, and then enter the domain name. Click **ADD DOMAIN**.
5. Click **Save** to save the changes you made.

To sort your list of exceptions, select either *All Exception, Block Traffic,* or *Allow Traffic* from the dropdown.

To remove an exception, click the Remove icon (🗑) in the table.

How to Configure Barracuda DNS Nameservers for Barracuda Content Shield

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 nameservers are shown on the **Configure DNS** page of the **Add Location** popup, which you access on the **DNS FILTERING** page.

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. For the Barracuda NextGen Firewall X Series, see How to Add Domains and DNS Records.
- **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.

How to Configure a Local DNS Server to Forward to Barracuda DNS Nameservers

This article provides instruction to configure a local DNS server, running Microsoft Windows server 2016, to forward DNS requests to Barracuda DNS nameservers for Barracuda Content Shield clients. You can also set up conditional forwarders for local domains.

Configure the DNS Server to Forward Requests to Barracuda

1. Log in to your domain controller and open the DNS manager.
2. Right click on the DNS server and click **Properties**.
3. Go to the **Forwarders** tab and click **Edit**.
4. Type in the Barracuda DNS nameserver IP address – **52.0.44.187** – and move it to the top of the table. Click OK.
5. Click **Apply settings**.

Setting Up Conditional Forwarders for Local Domains

If there is more than one DNS server, and/or you want to resolve some domains using another DNS server, do the following. Assume, in this example, that the local DNS server IP address we are configuring/editing is **10.5.7.75**.

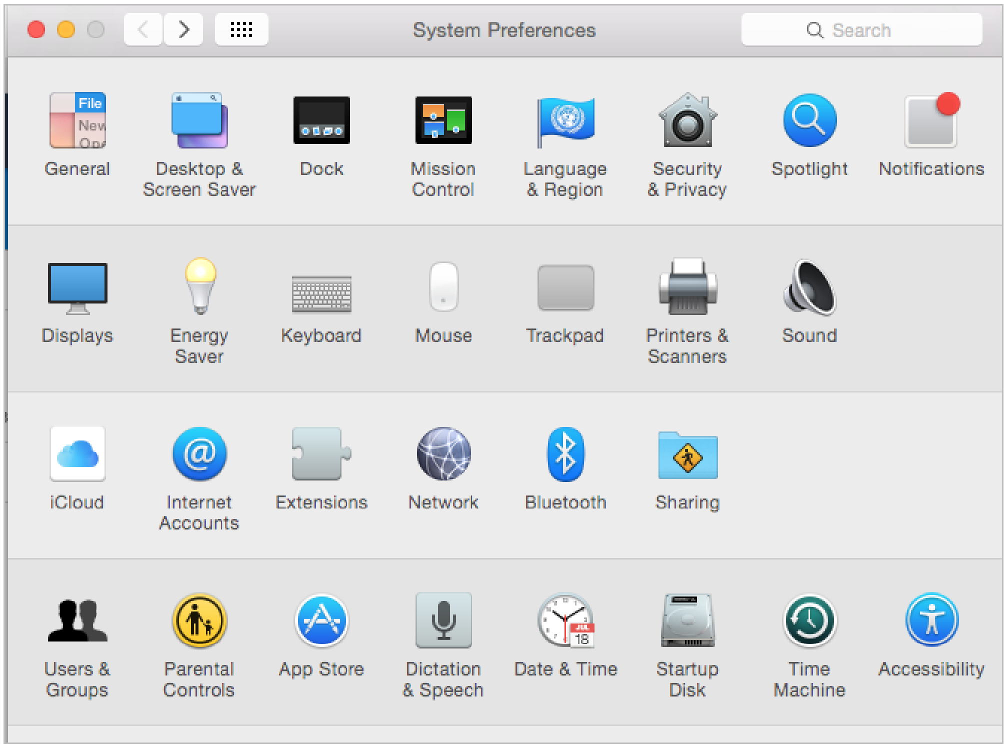
1. Right click on **Conditional Forwarders** and select **New Conditional Forwarder**.
2. Enter a local domain name in the DNS Domain field, and, in the **IP addresses of the master servers** table, enter other local DNS IP addresses where domains are resolved and click **Ok**.

After configuring these above steps, configure the primary DNS IP address as **10.5.7.75** on the client machine. All local requests should be resolved by the conditional forwarder DNS and other requests should be sent to the Barracuda DNS nameserver.

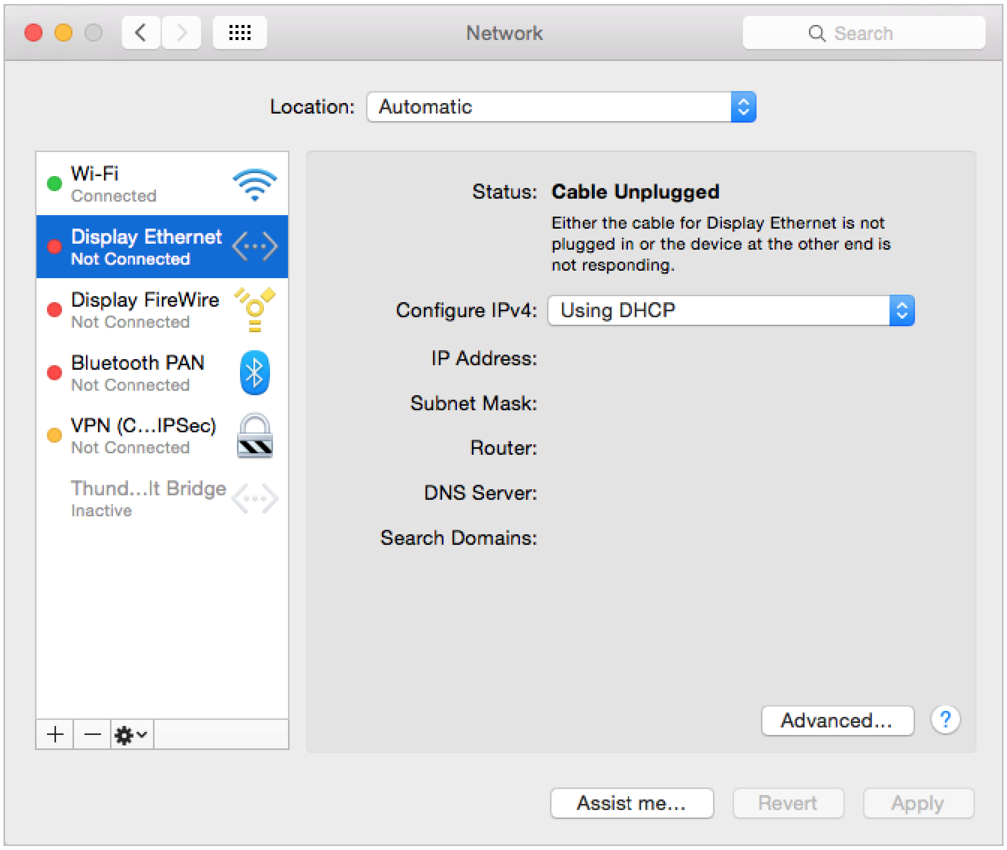
How to Configure Barracuda DNS Nameservers on Mac OS X

In order to use the Barracuda Web Filtering Service, you must direct your Mac(s) to the assigned Barracuda Domain Nameservers (DNS). The IP address for the Barracuda DNS nameservers are shown on the **Configure DNS** page of the **Add Location** popup, which you access on the **DNS FILTERING** page.

1. Go to System Preferences and click on **Network**.



2. Select the first connection in your list and click **Advanced**.



Location: Automatic

Status: **Cable Unplugged**

Either the cable for Display Ethernet is not plugged in or the device at the other end is not responding.

Configure IPv4: Using DHCP

IP Address:

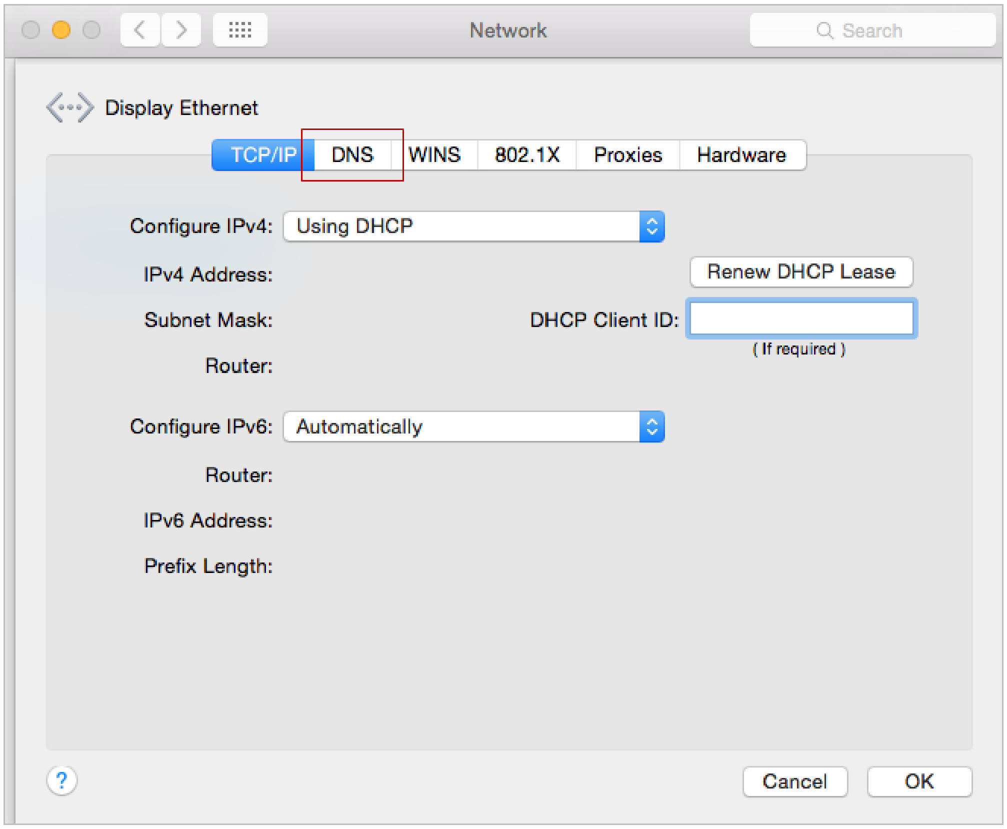
Subnet Mask:

Router:

DNS Server:

Search Domains:

3. Select the **DNS** tab.



Display Ethernet

Configure IPv4: Using DHCP

IPv4 Address:

Subnet Mask:

DHCP Client ID:

(If required)

Router:

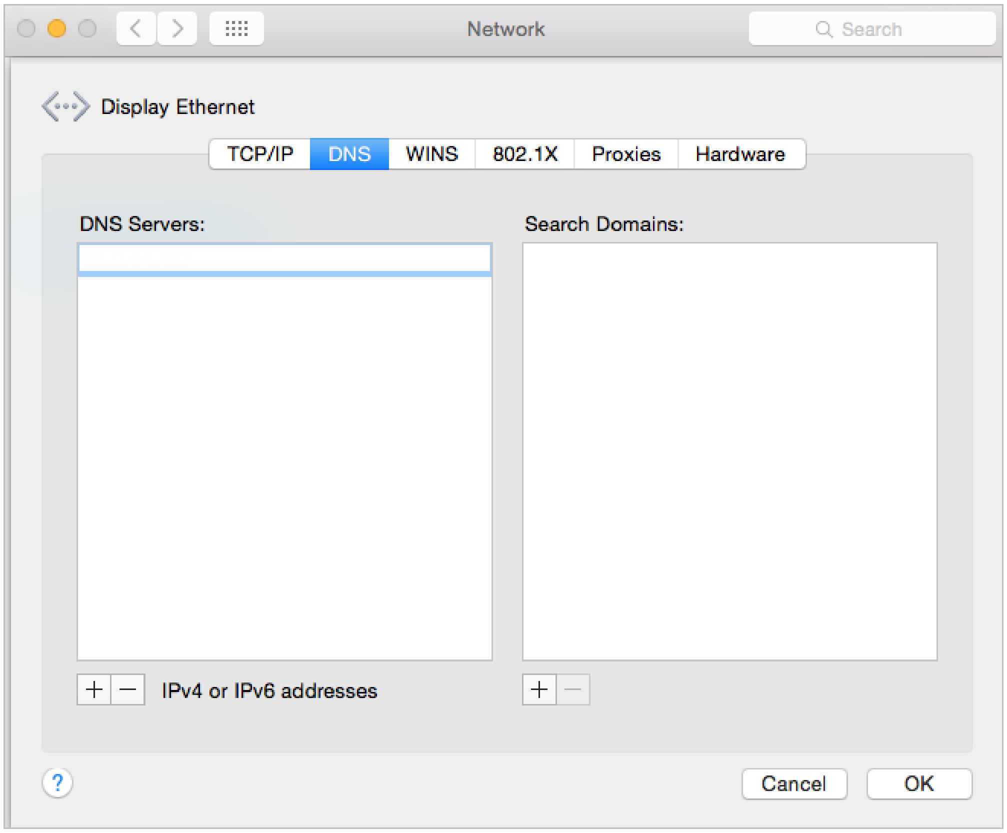
Configure IPv6: Automatically

Router:

IPv6 Address:

Prefix Length:

4. Add the Barracuda DNS nameserver IP addresses to the list of DNS servers. Click **OK** then click **Apply**.

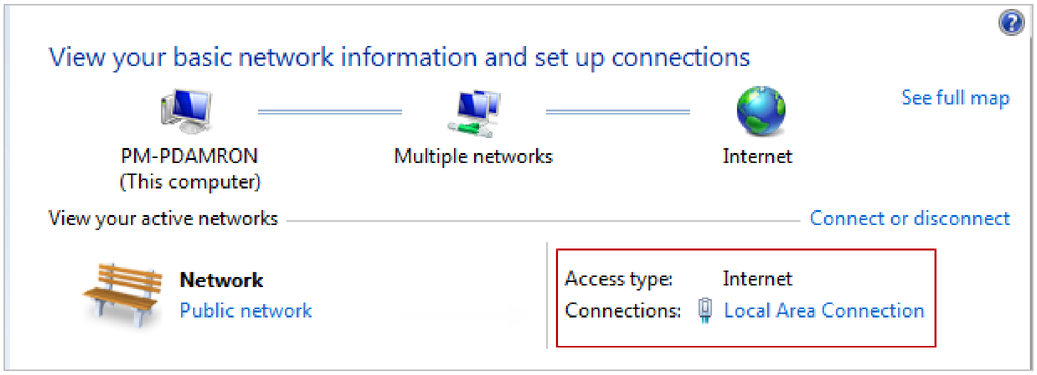


5. Clear your browser and DNS cache. This ensures that your new DNS configuration settings take effect immediately.

How to Configure Barracuda DNS Nameservers on Windows 8

In order to use the Barracuda DNS Filtering Service, you must direct your computer(s) (laptop / desktop) to the assigned Barracuda Domain Name Server (DNS). The IP address for the Barracuda DNS nameservers are shown on the **Configure DNS** page of the **Add Location** popup, which you access on the **DNS FILTERING** page.

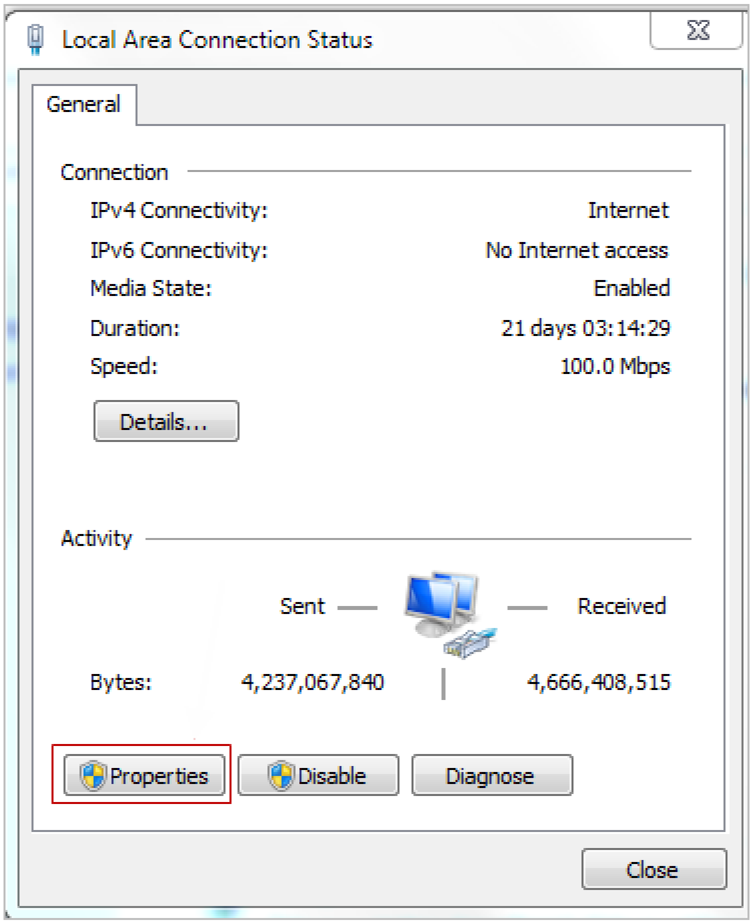
1. From the Windows 8 Desktop, right click the **Networks** icon and select **Open Network and Sharing Center.**
2. Click on your primary connection or **Local Area Connection** under **Active Networks**.
3. While in the **Open Network and Sharing Center,** click the current active connection or the connection that you want to configure the Barracuda nameserver on.



Access type: Internet

Connections: Local Area Connection

4. Choose/open the properties for that connection.



Local Area Connection Status

General

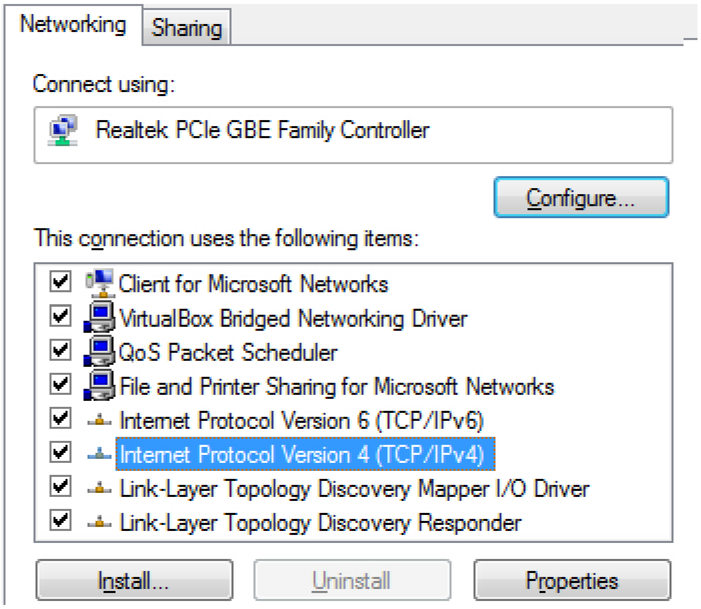
Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	No Internet access
Media State:	Enabled
Duration:	21 days 03:14:29
Speed:	100.0 Mbps

Activity

	Sent	Received
Bytes:	4,237,067,840	4,666,408,515

5. Highlight the Internet Protocol Version 4 (TCP/IPv4) option, then click Properties.



Networking Sharing

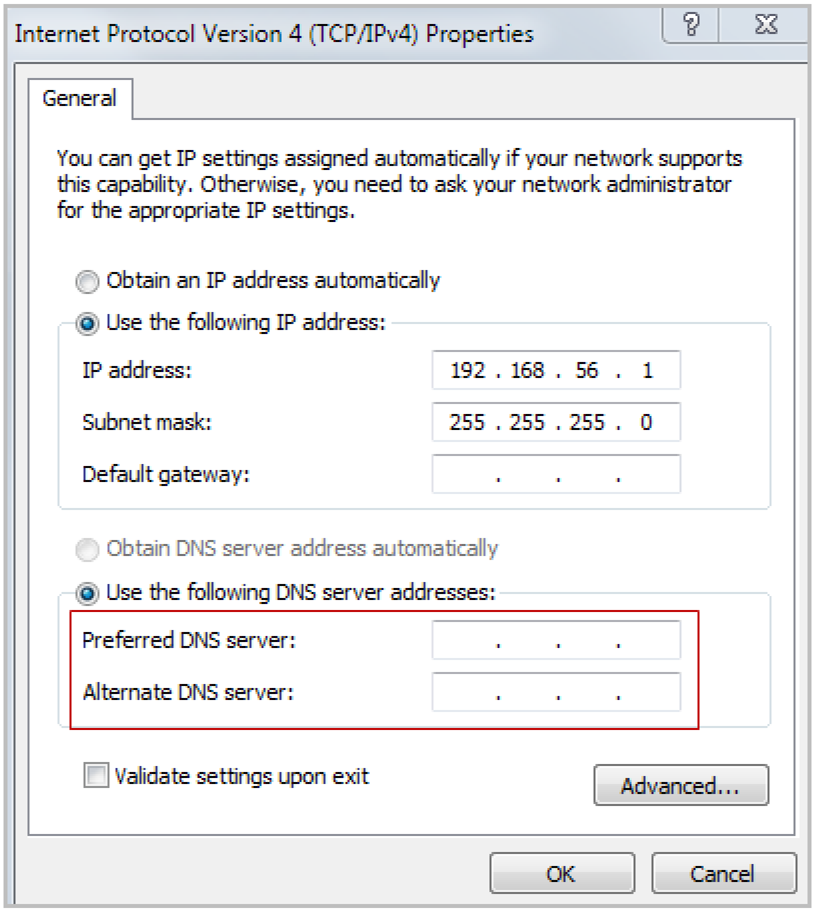
Connect using:

Realtek PCIe GBE Family Controller

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ VirtualBox Bridged Networking Driver
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

6. Select **Use the following DNS server addresses** and fill out the **Preferred DNS server** and **Alternate DNS Server** fields with the Barracuda DNS server IP addresses. Click **OK**.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 56 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

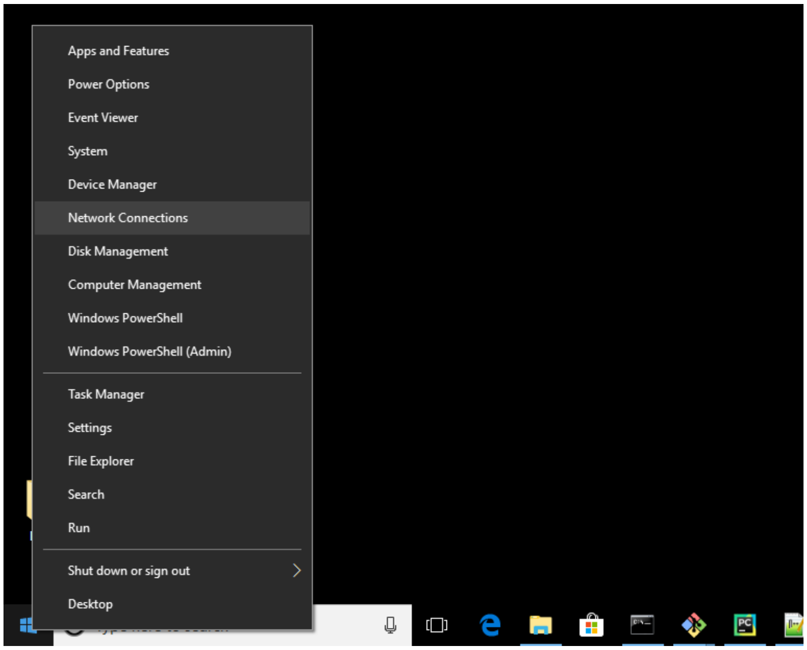
□ Validate settings upon exit

7. Clear your browser and DNS cache. This ensures that your new DNS configuration settings take effect immediately.

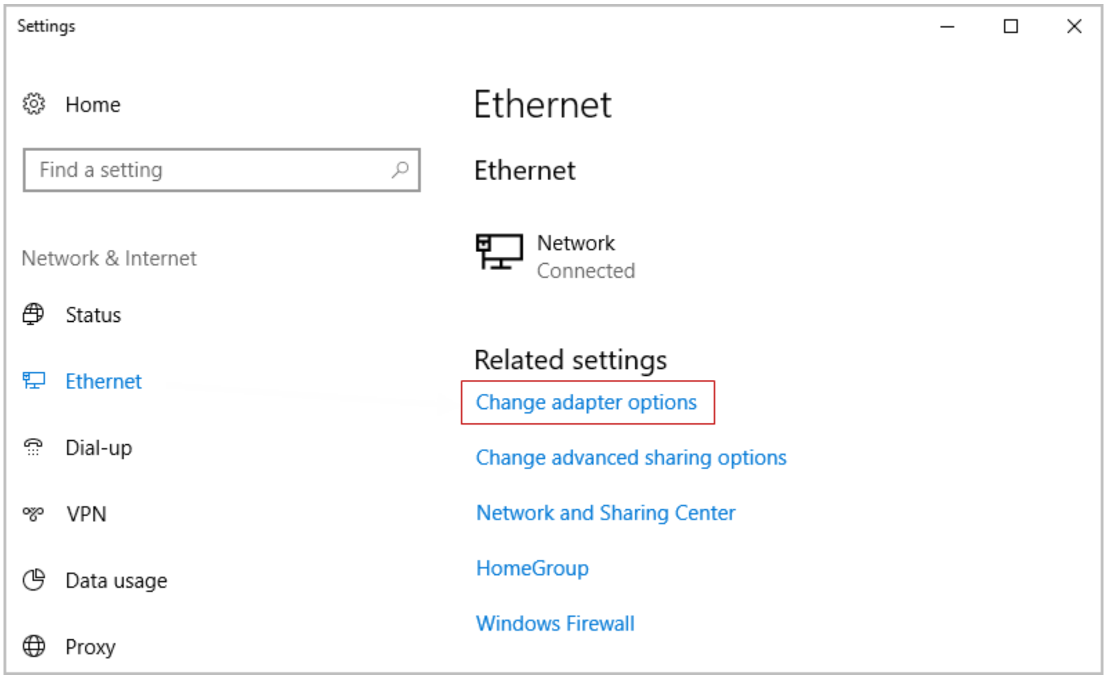
How to Configure Barracuda DNS Nameservers on Windows 10

In order to use the Barracuda DNS Filtering Service, you must direct your computer(s) (laptop / desktop) to the assigned Barracuda Domain Name Server (DNS). The IP address for the Barracuda DNS nameservers are shown on the **Configure DNS** page of the **Add Location** popup, which you access on the **DNS FILTERING** page.

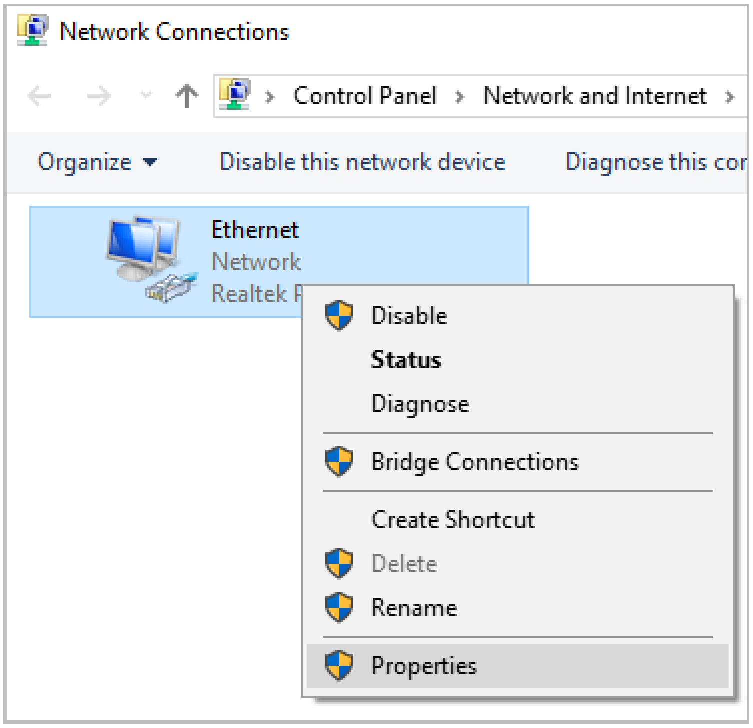
1. Right click the Start menu and select **Network Connections**.



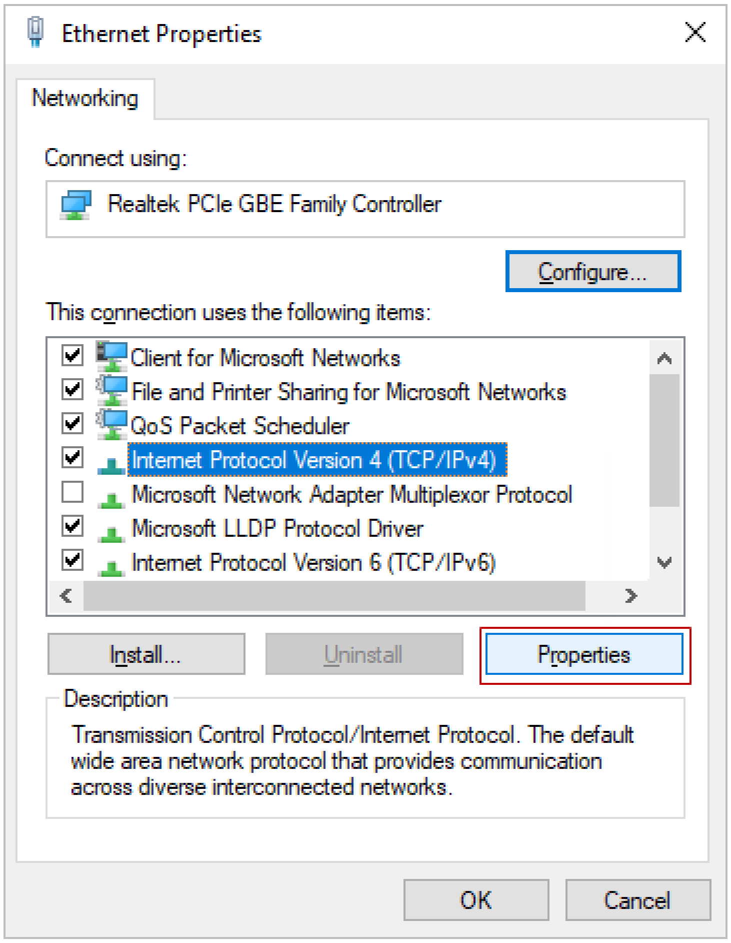
2. Click **Ethernet**, and in **Ethernet** click **Change adapter options**.



3. Right click the network connection you are using and select **Properties**.



4. Highlight the **Internet Protocol Version 4 (TCP/IPv4)** option, then click **Properties**.



Connect using:

Realtek PCIe GBE Family Controller

This connection uses the following items:

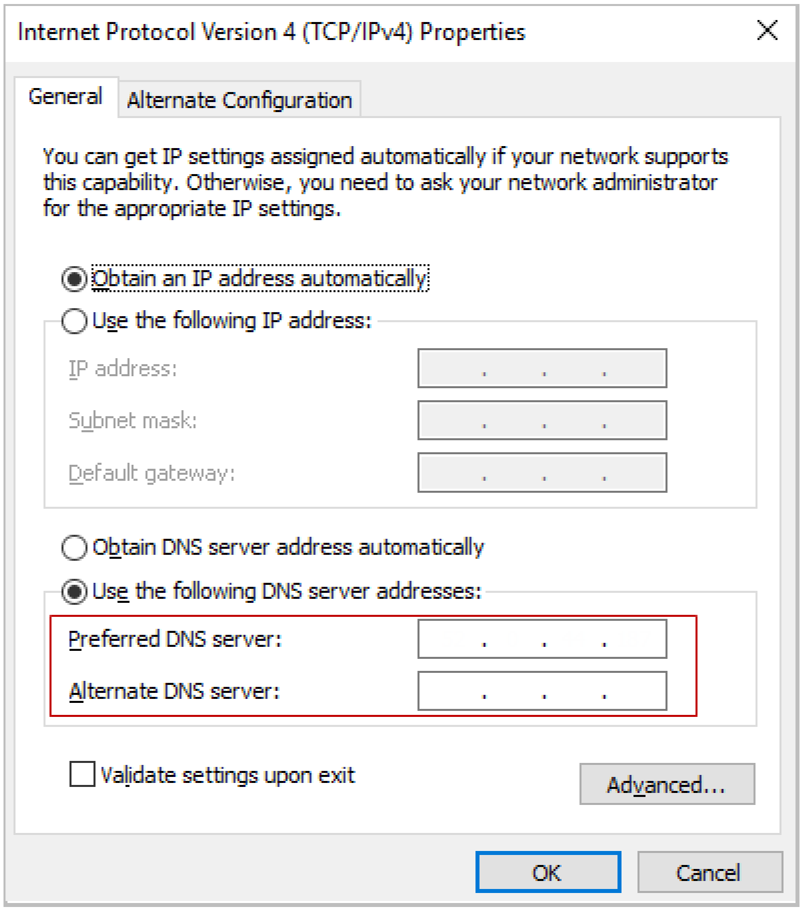
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

5. Select **Use the following DNS server addresses** and fill out the **Preferred DNS server** and **Alternate DNS Sever** fields with the

Barracuda DNS server IP addresses. Click **OK**.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

6. Clear your browser and DNS cache. This ensures that your new DNS configuration settings take effect immediately.

How to Configure the Barracuda DNS Nameserver on Your Router

This article offers general instructions for how to change the DNS server settings on a router. In order to use the Barracuda DNS Filtering Service, you must direct your router to the assigned Barracuda Domain Nameserver (DNS). The IP address for the Barracuda DNS nameservers are shown on the **Configure DNS** page of the **Add Location** popup, which you access on the **DNS FILTERING** page.

Note that there are many routers available on the market, and these basic instructions should apply to most. Please refer to your specific manufacturer documentation for detailed instructions.

1. **Open the preferences for your router.** Often, the preferences are set in your web browser, via a URL with IP addresses (example: http://192.168.0.1 or http://192.168.1.1). You may need a password. Or, preferences may be set via a specific application for your router, which you installed on your computer when you added the router.
2. **Find the DNS server settings.** Scan for the letters DNS next to a field which allows two or three sets of numbers, each broken into four groups of one to three numbers. These are IP addresses, and will look something like this: `108.67.222.100`
3. **Write down your current settings,** just in case. Next, put in the Barracuda nameserver address as shown above, and save the changes.
4. **Flush the DNS resolver cache.** After you have configured your DNS settings and saved them, Barracuda recommends that you flush your DNS resolver cache to ensure that your new DNS configuration settings take immediate effect.

How to Prevent Users from Circumventing Barracuda DNS Servers Using Firewall Rules

This article explains steps administrators can take to prevent users on the network from circumventing of Barracudas DNS nameservers.

Savvy internet users may try to bypass Barracuda DNS nameservers you have configured if your network security configuration allows them to change the local DNS IP server from the Barracuda IP address. This would bypass the security policies you have configured in Barracuda Content Shield and may leave your network vulnerable. However, it is possible to not allow those other DNS services through your network firewall to the Internet, which will prevent these users from circumventing policies.

Most routers and firewalls will allow you to force all DNS traffic over port 53, thus requiring everyone on the network to use the DNS settings defined on the router/firewall (in this case, Barracuda DNS nameserver). The preferred recommendation is to forward all DNS requests to go to the Barracuda IP address listed below. This way, you simply forward users' DNS requests without them knowing, instead of having the possibility of someone manually configuring DNS and having it not work.

Create two firewall rules to only allow DNS (TCP/UDP) to Barracuda DNS nameservers and restrict all other DNS traffic to any other IP addresses. Add this policy to the firewall that is at the furthest edge of your network. The rules would look something like this:

> ***ALLOW*** TCP/UDP IN/OUT to <Barracuda DNS nameserver IP> on Port 53
>
> and
>
> ***BLOCK*** TCP/UDP IN/OUT all IP addresses on Port 53

The first rule takes precedence over the second rule. Put simply, any requests to Barracuda will be allowed and any requests to any other IP address will be blocked.

- Depending on your firewall configuration interface, you may need to set up a separate rule for each of these protocols, or one rule which covers both.
- The rule can be applied on either the firewall or the router, but is normally best placed on the device most at network edge. A similar rule could be applied to software firewalls installed on a workstation as well, such as the built-in firewall on Windows or Mac OS X.

For help with creating firewall rules on a Barracuda CloudGen Firewall, see Firewall Access Rules. For the Barracuda NextGen Firewall, see Firewall Rules. If you are not using a Barracuda firewall solution, note that each firewall or router has a unique configuration interface and these vary greatly. If you are uncertain, you should check your router or firewall documentation or contact the manufacturer to see if this is possible with your device.