OpenDNS

cisco OpenDNS is now part of Cisco.

OpenDNS Solution Guide for Meraki Cloud-Managed Networks

Introduction to this Guide

As the administrator of a Meraki device, you are able to connect to the free and fast OpenDNS recursive DNS service which will offer you visibility into all Internet traffic originating from your Meraki device, and result in a faster Internet experience for your users. If you then want to add an additional layer of DNS security to your Meraki device, the easy-to-establish connection to OpenDNS enables you to access our free trial – which you can setup (by yourself) in less than five minutes.

Using OpenDNS

OpenDNS is a leading provider of network security and DNS services, enabling the world to connect to the Internet with confidence on any device, anywhere, anytime. The Umbrella cloud-delivered network security service blocks command & control callbacks, malware, and phishing from compromising systems and exfiltrating data over any port, protocol, or app. We apply statistical models to real-time and historical DNS data to predict domains that are likely malicious and could be used in future attacks. OpenDNS protects all devices globally without hardware to install or software to maintain. OpenDNS has data centers across all regions of the world to ensure that the first hop to the service is as fast as possible.

Traditionally there are several places where a network administrator might change public recursive DNS settings to use OpenDNS, but exactly where the change is made depends on the network configuration.

Note: If you're not certain whether you have a DNS forwarder configured, the best way to determine what needs to be changed is to see what device is being used as the DNS server for client workstations that are receiving DHCP from the network. This information is typically in the DNS section of the network adapter settings on the client workstation.

This document covers how to configure your Meraki network to use the OpenDNS IP addresses of 208.67.222.222 and 208.67.220.220. Additionally, if you are using a DNS forwarder as the primary DNS server for your network, this document covers how to update Windows 2003 Server, Windows 2008 Server, Windows 2012 Server or BIND Server to use OpenDNS.

Once you've configured your Meraki infrastructure to point to OpenDNS, then you can sign up for either a free premium DNS account or a free 14-day trial of OpenDNS Umbrella.

Free Premium DNS:

We offer a free, fast recursive DNS service which gives you visibility into all of your Internet traffic originating from your Meraki device.

https://store.opendns.com/premiumdns/?utm_source=meraki&utm_medium=cisco-partner&utm_campaign=meraki-guide-free-trial-home

Free OpenDNS Umbrella 14-Day Trial at:

If you want to add an additional layer of DNS security to your Meraki device, try our free trial – which you can set up by yourself in less than five minutes.

https://signup.opendns.com/freetrial/?utm_source=meraki&utm_medium=cisco-partner&utm_campaign=meraki-guide-free-trial#company

Setting up OpenDNS for a Meraki network

There are two ways in which you can configure your Meraki networks to use OpenDNS. The first is to use DHCP to distribute the OpenDNS server IP information directly to clients. This is available on all Meraki platforms. The second method, available only on MX Security Appliances and Z1 Teleworker Gateways, is to configure the MX itself to use the OpenDNS servers and to proxy client DNS requests to those same servers.

How to configure OpenDNS for clients

For MX Security Appliances: From your cloud dashboard, select **Security Appliance > Configure > DHCP**. Under the DHCP scope you wish to configure, select **Use OpenDNS** from the **DNS nameservers** drop-down. DHCP must be enabled for the desired subnet for this option to appear.

For MS Switches: From your cloud dashboard, select **Switch > Configure > Routing and DHCP.** Select the route you wish to modify the DHCP service for, and select **Use OpenDNS** from the **DNS nameservers** drop-down under **DHCP Settings**. DHCP must be enabled for the desired subnet for this option to appear.

For more information on how to configure the DHCP server for MX Security Appliances and MS Switches, please see:

http://documentation.meraki.com/MS/Layer_3_Switching/Configuring_DHCP_Services_on_the_MX_and_MS

For MR Access Points (NAT Mode SSIDs only): From your cloud dashboard, select **Wireless > Configure > Access Control.** Select the SSID you wish to configure, and select **Custom DNS** from the **Content filtering** drop-down under **Addressing and Traffic.** Enter in the OpenDNS server IP addresses: **208.67.222.222** and **208.67.220.220**.

How to configure your Meraki network to proxy DNS to OpenDNS (MX Security Appliance and Z1 Teleworker Gateway only)

Note: Static IP configuration for the MX and Z1 devices must performed locally and cannot be done via the cloud dashboard. Once logged into the local status page, browse to the Uplink Configuration page and configure the DNS settings to use 208.67.222.222 and 208.67.220.220 under IP Assignment. This method can only be used with Static IP addressing.

For more information on how to access the local configuration, please see:
https://docs.meraki.com/display/MX/MX+Local+Status+and+Configuration

From your cloud dashboard, select **Security Appliance > Configure > DHCP.** Under **DNS nameservers** select **Proxy to upstream DNS.**

Configuring your DNS forwarder for OpenDNS

Even with a Cisco or Meraki device in place at the gateway or egress, DNS for networks is often handled by DNS forwarders installed on DNS servers within the network environment. A DNS forwarder is a DNS server on a network that forwards DNS queries for external domain names to the OpenDNS servers. A DNS server on a network is designated as a forwarder when the other DNS servers in the network are configured to forward the queries that they cannot resolve locally to that DNS server.

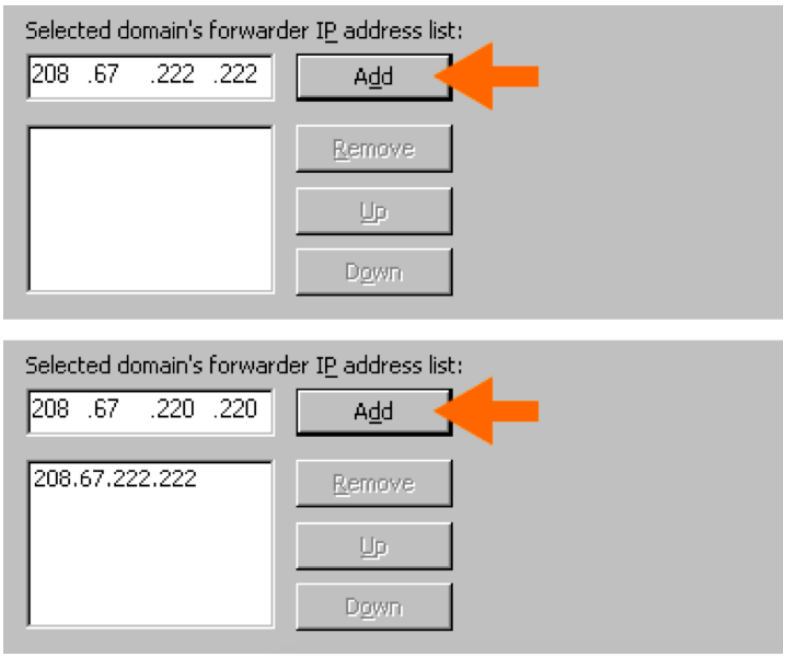
The following instructions cover how to configure your DNS forwarder to use the OpenDNS public DNS servers for BIND and Windows Server 2003, 2008 and 2012.

Windows Server 2003 and 2003 R2

1. From the Start menu, navigate to **Administrative Tools > DNS.**
2. Choose the DNS server you want to edit.
3. Select **Forwarders.**
4. Select **All Other DNS domains** in the DNS domains list.
5. Add OpenDNS addresses to the selected server's forwarder IP address list.

   Please write down your current DNS settings before switching to OpenDNS, in case you want to return to your old settings for any reason.

   OpenDNS' addresses are 208.67.222.222 and 208.67.220.220.



6. Click OK to confirm the changes.

   We recommend that you flush the DNS resolver cache of the server and the DNS caches of the clients/users using the DNS server to ensure that your new DNS configuration settings take immediate effect.

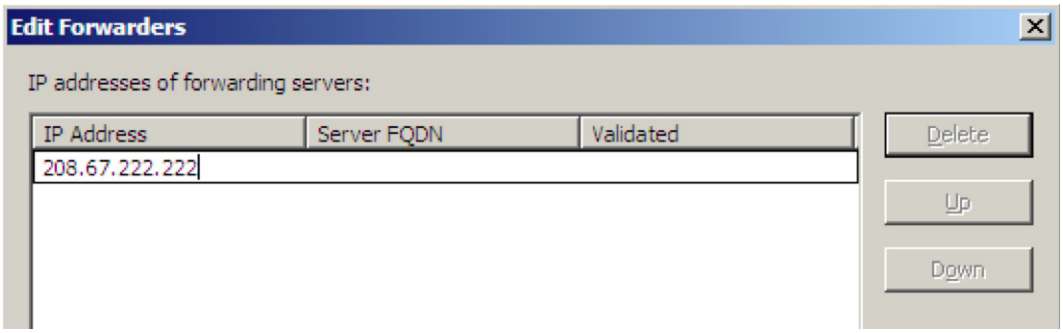
   For more information, see: https://support.opendns.com/entries/26336865

Windows Server 2008 and 2008 R2

1. From the Start menu, navigate to **Administrative Tools > DNS.**
2. Choose the DNS server you want to edit.
3. Select **Forwarders.**
4. Click **Edit.**
5. Add OpenDNS addresses in the selected server's forwarder IP address list.

   Please write down your current DNS settings before switching to OpenDNS, in case you want to return to your old settings for any reason.

   OpenDNS' addresses are 208.67.222.222 and 208.67.220.220.



6. Click **OK.**
7. Click **OK** again to confirm the changes.

   We recommend that you flush the DNS resolver cache of the server and the DNS caches of the clients/users using the DNS server to ensure that your new DNS configuration settings take immediate effect.

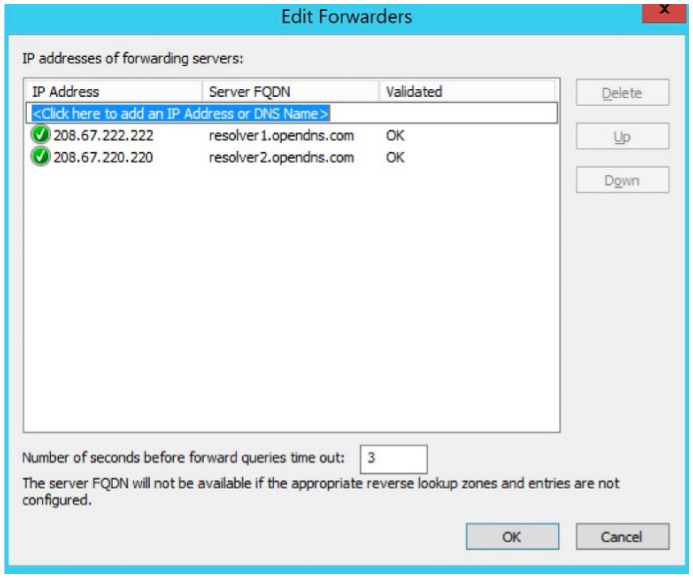
   For more information, see: https://support.opendns.com/entries/26336865.

Windows Server 2012 and 2012 R2

1. In the Start menu, type **DNS** into Search.
2. Select **DNS** from the search results.
3. Choose the DNS server you want to edit.
4. Select **Forwarders**.
5. Click **Edit**.
6. Add OpenDNS addresses to the selected server's forwarder IP address list.

   Please write down your current DNS settings before switching to OpenDNS, in case you want to return to your old settings for any reason.

   OpenDNS' addresses are 208.67.222.222 and 208.67.220.220.



7. Click **OK.**
8. Click **OK** again to confirm the changes.

BIND based DNS server: Configure BIND to use Open DNS via the shell and Webmin

To point your BIND-based DNS server to use OpenDNS resolvers for external resolution you need to modify the file **named.conf.options** and add the OpenDNS resolvers as forwarders.

This can be done in one of two ways:

- Via the command line, Shell\SSH
- Via a GUI if you have Webmin installed on your BIND server

Shell\SSH Instructions

1. Connect directly to your server or SSH to it.
2. Go into **/etc/bind.**

   Note: this is the default location, so you may need to change this based on your configuration.
3. Edit **named.conf.options** in your favorite text editor.
4. Click **Edit.**
5. In **named.conf.options**, look for a line that starts with forwarders {

   If the forwarders are already configured then just change the current resolver IPs to OpenDNS' IP addresses, which are 208.67.222.222 and 208.67.220.220.

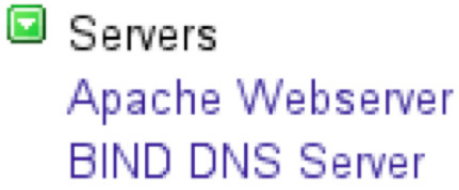
   If the line starting with forwarders { **isn't there, you can add it right above the last** };

   forwarders {
   208.67.222.222;
   208.67.220.220;
   };
6. Save the file to confirm your changes.

Webmin Instructions

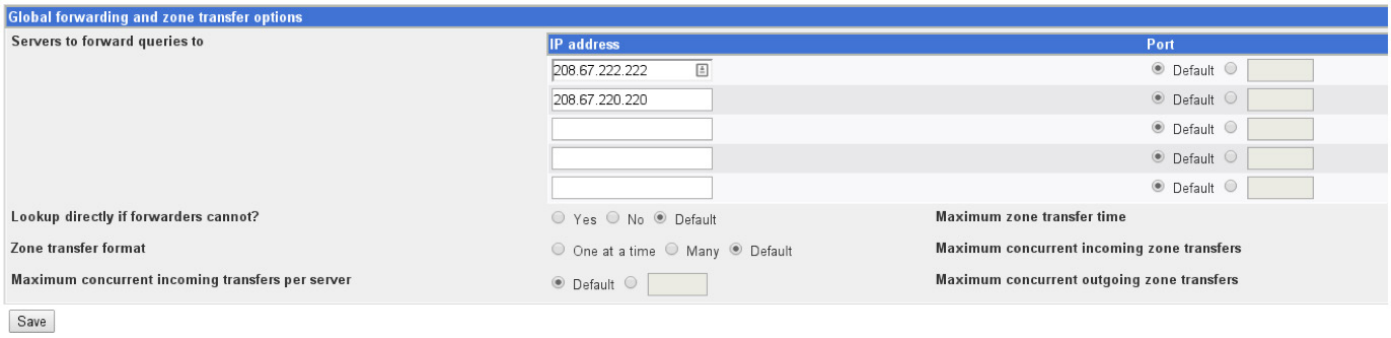
These steps produce a result that is the exact same as the above, except that the Webmin GUI will modify the file **named.conf.options** for you.

1. Log into Webmin.
2. Navigate to **Servers > BIND DNS Server.**



3. Choose **Forwarding and Transfers.**

4. Add OpenDNS' IP addresses, which are 208.67.222.222 and 208.67.220.220, under the **Servers to forward queries to** section:



5. Click **Save** to confirm the changes.

Open DNS Service and Support

OpenDNS customers should continue to use the existing process for configuration and support on OpenDNS technology. Cisco will notify you in advance of any change to the support process.

OpenDNS support: https://www.opendns.com/support/

Legal Information

Cisco Trademark

Cisco Copyright