# Verify Your Egress DNS IP Address

## Contents

## Introduction

This document describes how to identify the egress IP address used by the DNS servers on your network. You are able to use this information to ensure that your company's networks are fully secured.

Cisco Umbrella applies security policies based on the IP address from which that network's DNS requests originate. If this IP address is not properly registered or maintained in our database, then your network does not see the full security benefits of Umbrella.

## Verifying your egress DNS IP address

The first thing to confirm is that you have registered the public IP address of your network to the Umbrella Dashboard. Information on how to add your public IP address to the Umbrella Dashboard can be found here: https://docs.umbrella.com/deployment-umbrella/docs/protect-your-network

The second thing to confirm is that the forwarders on your internal DNS servers are configured to use Umbrella. We have a general guide available to you here that outlines the steps:

https://docs.umbrella.com/deployment-umbrella/docs/point-your-dns-to-cisco

Now that you have added your public IP address and pointed your DNS you need to confirm that your IP address is reporting to us correctly and matches with what you have registered to the Dashboard. Your egress (public) IP address is used to identify you and apply your Dashboard settings to your account.

To verify your egress IP address you need to run a debug query.

## Verifying through Windows Command Prompt

1. To open your Command Prompt go to the Windows Start Menu and select 'run' and enter cmd.exe.
2. Your command prompt window opens.
3. Type this command in the window:

```
nslookup -type=txt debug.opendns.com
```

The resulting output looks like this:

```
Results for: nslookup -timeout=10 -type=txt debug.opendns.com.
stdout:
Server: exampledc1.local
Address: 192.168.1.1
debug.opendns.com text =
"server m5.nyc"
debug.opendns.com text =
"flags 20 0 1040 59F9000380000000000"
debug.opendns.com text =
"originid 123456"
debug.opendns.com text =
"orgid 789100"
debug.opendns.com text =
"actype 0"
debug.opendns.com text =
"bundle 543215"
debug.opendns.com text =
"source 146.138.21.85:60965"
```

# Verifying through Mac OSX Terminal

1. To open your Terminal on your Mac, go to the top right of your Mac and select the magnify glass icon.
2. A search field appears. Enter 'terminal' and select the program.
3. Your Terminal window opens.
4. Type this command in the window:

```
/usr/bin/dig +time=10 debug.opendns.com txt
```

The resulting output looks like this:

```
debug.opendns.com. 0 IN TXT "server m5.nyc"
debug.opendns.com. 0 IN TXT "flags 20 0 1040 59F9000380000000000"
debug.opendns.com. 0 IN TXT "originid 1234567"
debug.opendns.com. 0 IN TXT "orgid 789100"
debug.opendns.com. 0 IN TXT "actype 0"
debug.opendns.com. 0 IN TXT "bundle 543215"
debug.opendns.com. 0 IN TXT "source 146.138.21.85:60965"
```

# Interpreting the Debug Query

The debug query provides information for support to identify specific settings that are applied to your network but also provides some relevant information about your connection such as which data center you are sending requests to, the internal address of your DNS server sending the request and the IP address of the network that made the query.

We are interested in what the egress IP shows up as in the results. In these examples, we see the output shows as "source 146.138.21.85:60965". This tells us that the egress IP address for the DNS server that made the request was 146.138.21.85, which must match with the IP address that you have registered on the Umbrella Dashboard. If the address does not match, you need to register the correct IP address to your Dashboard to ensure you get the full security benefits of Umbrella and ensure that your settings are applied.