



Getting Started with OpenDNS Enterprise

Configuring OpenDNS Security and Filtering Settings

Introduction

Now that you're sending DNS queries to OpenDNS, it's time to configure your security and filtering settings in your OpenDNS dashboard. This guide will walk you through the necessary steps to add your network to your OpenDNS account and configure your security and filtering settings.

OpenDNS Settings

OpenDNS Enterprise requires an active subscription license. For more information, please visit <http://www.opendns.com/business-solutions/>.

1. Open a web browser and navigate to www.OpenDNS.com. Click "Sign in".



2. Sign in with your OpenDNS registered email address and password.

A screenshot of the OpenDNS sign-in form. The OpenDNS logo is on the left. The form fields are: 'Email (or username):' with the value 'arubasetup@opendns.com', and 'Password:' with a masked password '.....'. There is a checkbox for 'Keep me signed in until I sign out' and a 'SIGN IN' button. At the bottom, there are links for 'Forgot your password?' and 'Don't have an account? Get started!'.

3. Click on the “Settings” tab to create or manage your network(s).
 - To create your network(s) in the OpenDNS Dashboard, you will need to enter the external IP address, select the appropriate CIDR prefix size and identify the appropriate organization.
 - Once you’ve populated the correct information, click “Add this network.”

The screenshot shows the OpenDNS dashboard with the 'SETTINGS' tab selected. The 'Add a network' form is displayed, featuring a dropdown for 'Settings for:' with the text '— Select an organization —'. Below this, there are sections for 'Dynamic IP addresses' and 'Network verification'. The 'Add a network' form includes input fields for 'IP:' (67, 215, 89, 23) and 'Organization:' (OpenDNS). A list of CIDR prefix sizes is shown on the right, ranging from 32 (1 IP Address) to 19 (8,192 IP Addresses). A button labeled 'ADD THIS NETWORK' is visible. Below the form, a message states 'No networks have been assigned to OpenDNS. Add a n'.




4. You will be prompted to add a label to the network and if it is a /32, indicate whether your IP address is static or dynamic. We recommend creating easy to remember network names, such as “Corporate Headquarters,” “Branch Office West” or “Guest Wi-Fi.”

If your mail server has a unique external IP address, please add your mail server’s public IP address as its own network and configure the outbound SMTP service to use OpenDNS directly. Be sure to avoid applying filtering settings to your mail network as this may result in mail being undelivered.

Note: Dynamic IP networks require running a lightweight IP updater client on a computer on the network.

The screenshot shows a confirmation message: "You've successfully added a network! Just a few more steps and you're home free." Below this, there are two numbered steps: 1. Give it a friendly name: Office Network. Something simple like "Office" or "Home" will do. 2. Is this a dynamic IP address? What is a dynamic IP address?. There is a checkbox labeled "Yes, it is dynamic" which is currently unchecked.

5. Click on the network's IP address to modify settings.

OpenDNS »			
LABEL	IP	USERS	STATS
Office Network	67.215.89.23		 
DELETE			

6. Configure content filtering settings by choosing from pre-defined filtering levels or you may choose "Custom" to build a custom bundle from 57 categories. If you have multiple networks registered with OpenDNS you will have the option to apply this change to all of your networks.

Settings for: Office Network (67.215.88.202) [Add/manage networks](#)

Web Content Filtering
[Security](#)
[Bypass Blocked Pages](#)
[Customization](#)
[Stats and Logs](#)
[Advanced Settings](#)

Web Content Filtering
Choose your filtering level

☐ **Whitelist Only** Enabling this feature will **block all websites** except those listed below under your "Never block" individual domains.
☐ **High** Protects against all adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters. [26 categories in this group - View - Customize](#)
☐ **Moderate** Protects against all adult-related sites and illegal activity. [13 categories in this group - View - Customize](#)
☐ **Low** Protects against pornography. [4 categories in this group - View - Customize](#)
☐ **None** Nothing blocked.
☒ **Custom** Choose the categories you want to block.

☐ [Academic Fraud](#)
☐ [Alcohol](#)
☐ [Blogs](#)
☐ [Classifieds](#)
☐ [Ecommerce/Shopping](#)
☐ [Financial institutions](#)
☐ [Games](#)
☐ [Hate/Discrimination](#)
☐ [Instant messaging](#)
☐ [Movies](#)
☐ [Non-profits](#)
☐ [Parked Domains](#)
☐ [Politics](#)
☐ [Proxy/Anonymizer](#)
☐ [Research/Reference](#)
☐ [Social networking](#)
☐ [Tasteless](#)
☐ [Travel](#)
☐ [Weapons](#)

☐ [Adult Themes](#)
☐ [Auctions](#)
☐ [Business Services](#)
☐ [Dating](#)
☐ [Educational Institutions](#)
☐ [Forums/Message boards](#)
☐ [German Youth](#)
☐ [Health](#)
☐ [Jobs/Employment](#)
☐ [Music](#)
☐ [Nudity](#)
☐ [Photo sharing](#)
☐ [Pornography](#)
☐ [Radio](#)
☐ [Search engines](#)
☐ [Software/Technology](#)
☐ [Television](#)
☐ [Video sharing](#)
☐ [Webmail](#)

☐ [Adware](#)
☐ [Automotive](#)
☐ [Chat](#)
☐ [Drugs](#)
☐ [File storage](#)
☐ [Gambling](#)
☐ [Government](#)
☐ [Humor](#)
☐ [Lingerie/Bikini](#)
☐ [News/Media](#)
☐ [P2P/File sharing](#)
☐ [Podcasts](#)
☐ [Portals](#)
☐ [Religious](#)
☐ [Sexuality](#)
☐ [Sports](#)
☐ [Tobacco](#)
☐ [Visual search engines](#)

Looking for [security categories?](#)

[APPLY](#)

Users can contact you
Your users can contact you directly from the block page if they have questions. It'll show up as an email in your inbox.

Note about DNS forwarding
If you are forwarding requests to OpenDNS, domain blocking may not work properly if the domain's address is in your forwarder's cache.

Check a domain
[Find out](#) whether it would be blocked, and why.

Support Articles

7. You may also manage individual domains using the “Never block” or “Always block” interface.

Manage individual domains

If there are domains you want to make sure are always blocked (or always allowed) regardless of the categories blocked above, you can add them below.

Always block

ADD DOMAIN

8. To Configure Malware, Botnet and Phishing protection, you will need to select “Security” in the left navigation panel. Once you are on the Security configuration page, you will have the option to enable different types of security protection.

Settings for: Office Network (67.215.89.23) [Add/Manage Networks](#)

Web Content Filtering
Security
[Bypass Blocked Pages](#)
[Customization](#)
[Stats and Logs](#)
[Advanced Settings](#)

Security

Botnet Protection ☒ **Enable botnet protection**
Enabling this option will stop known command and control hosts and websites from resolving on your network. We're continuously updating our database of known malicious hosts to keep you better protected online.

Malware Protection ☒ **Enable malware protection**
Enabling this option will prevent known malware drop sites (sources of infection) from resolving on your network. We're constantly updating this list of websites in coordination with a number of other security organizations.

Internet-Scale Malware/Botnet Protection ☒ **Enable basic malware/botnet protection**
Enabling this feature will protect your network from certain types of Internet-scale botnets and wide-reaching malware, such as the Conficker virus and the Internet Explorer Zero Day Exploit. This is different from the Enterprise-class Malware and Botnet protection above. We recommend you enable it for added security.

Phishing Protection ☒ **Enable phishing protection**
By enabling phishing protection, you'll protect everyone on your network from known phishing sites using the best data available.

Suspicious Responses ☒ **Block internal IP addresses**
When enabled, DNS responses containing IP addresses listed in [RFC1918](#) will be filtered out. This helps to prevent [DNS Redirection attacks](#). For example, if `badstuff.attacker.com` points to `192.168.1.1`, this option would filter out that response.

The three blocks of IP addresses filtered in responses are:

10.0.0.0	-	10.255.255.255	(10/8)
172.16.0.0	-	172.31.255.255	(172.16/12)
192.168.0.0	-	192.168.255.255	(192.168/16)

APPLY ☒ Apply to all my OpenDNS networks

9. Further settings such as custom logos, custom block messaging, block page bypass codes and stats preferences may be configured using the left navigation panel.

Verifying OpenDNS Filtering Settings

After you've configured your security and filtering settings in your OpenDNS Enterprise account, you'll want to verify that filtering is working appropriately. If you've enabled blocking of the category "Social Networking", when you try to visit <http://facebook.com> you should be redirected to a block page.

Remember, after making any changes to your OpenDNS settings, we recommend that you clear your DNS cache to ensure that the new settings are made effective. To do this, see [Clearing the DNS Cache](#).

