OpenDNS

Getting Started with OpenDNS Enterprise

Configuring OpenDNS Security and Filtering Settings

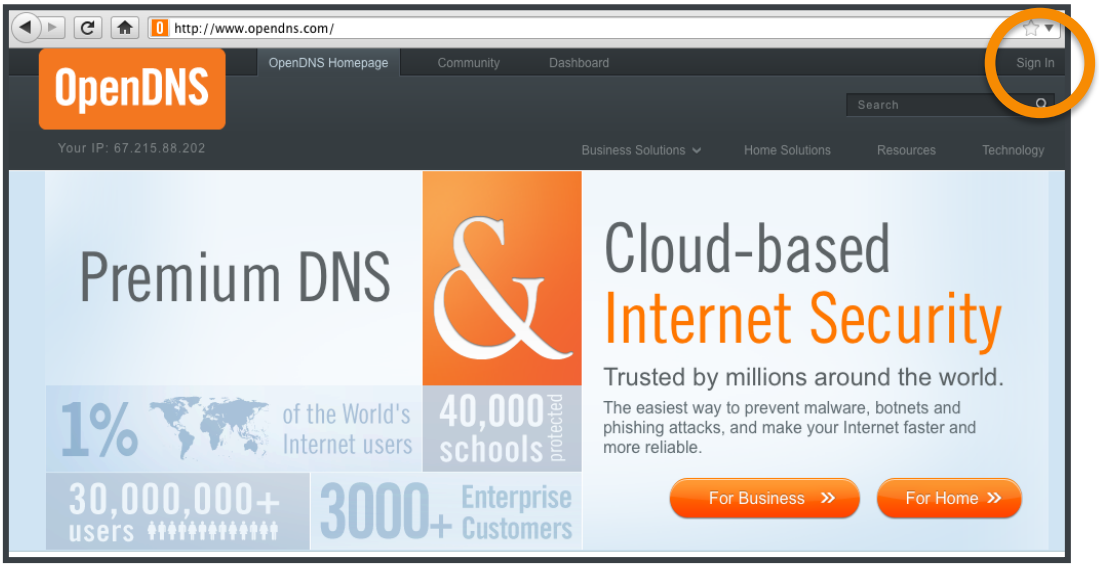
Introduction

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 to steps to add your network to your OpenDNS account and configure your security and filtering settings.

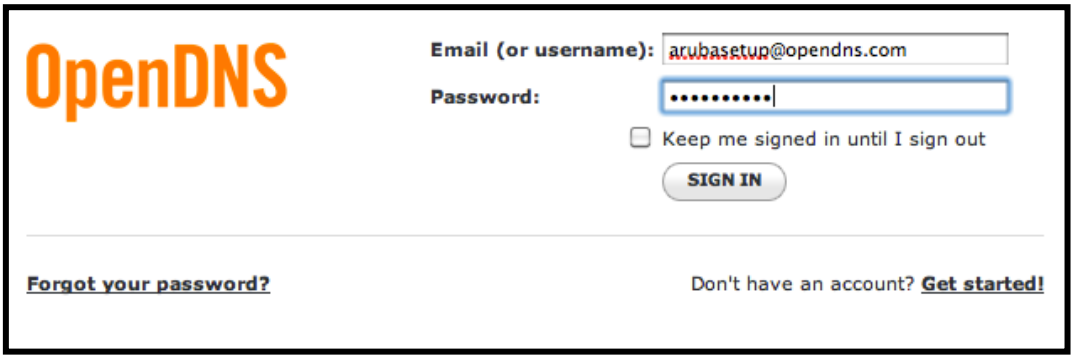
OpenDNS Settings

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

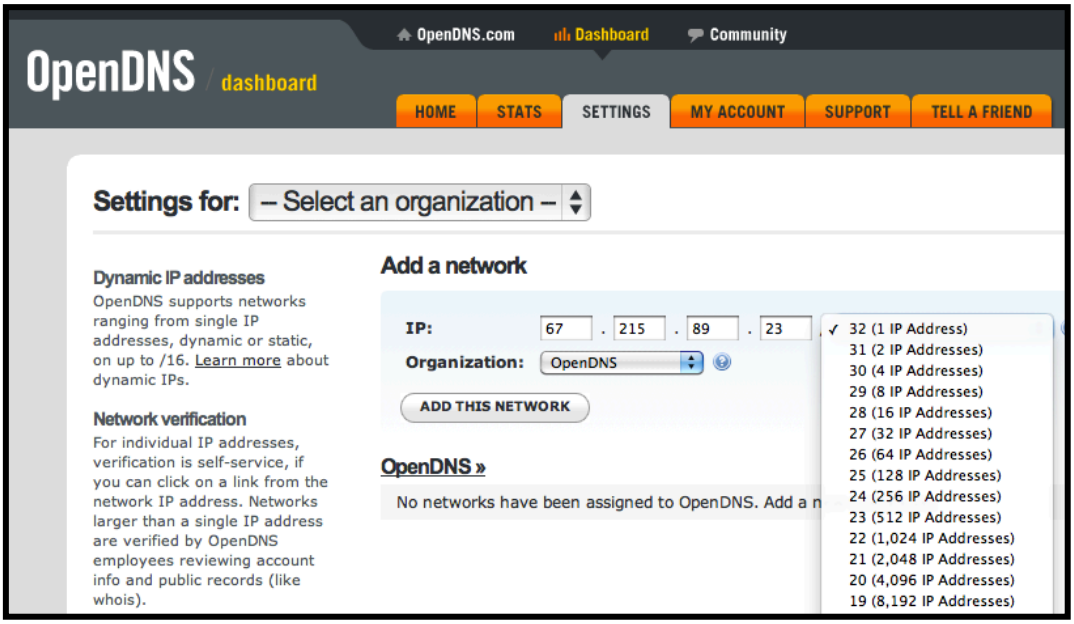
1. Open a web browser and navigate to www.OpenDNS.com. Click "Sign in".



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



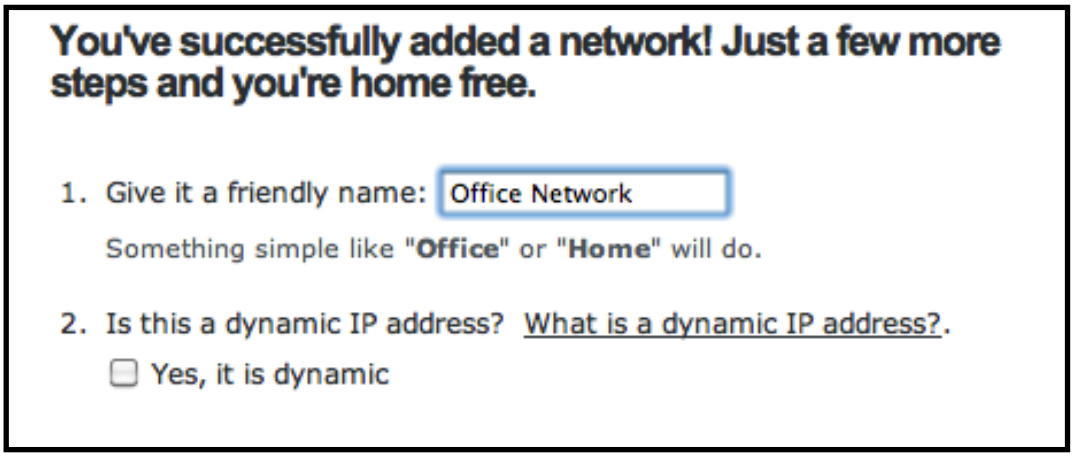
3. Click on the "Settings" tab to create or manage your network(s).
    - To create your network(s) in the OpenDNS Dashboard, you will need to enter the external IP address, select the appropriate CIDR prefix size and identify the appropriate organization.
    - Once you've populated the correct information,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



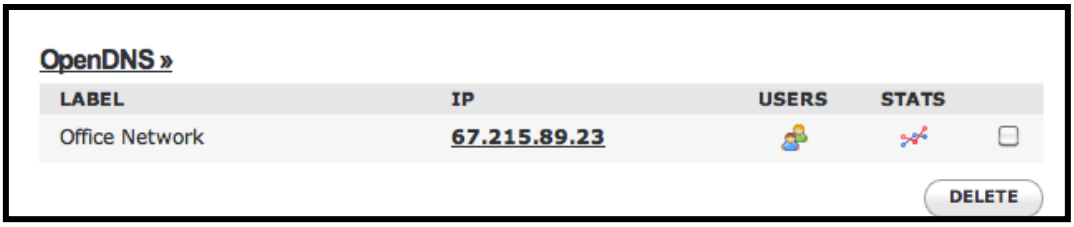
4. You will be prompted to add a label to the network and if it is a /32, indicate whether your IP address is static or dynamic. We recommend creating easy to remember network names, such as "Corporate Headquarters," "Branch Office West" or "Guest Wi-Fi."

    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.

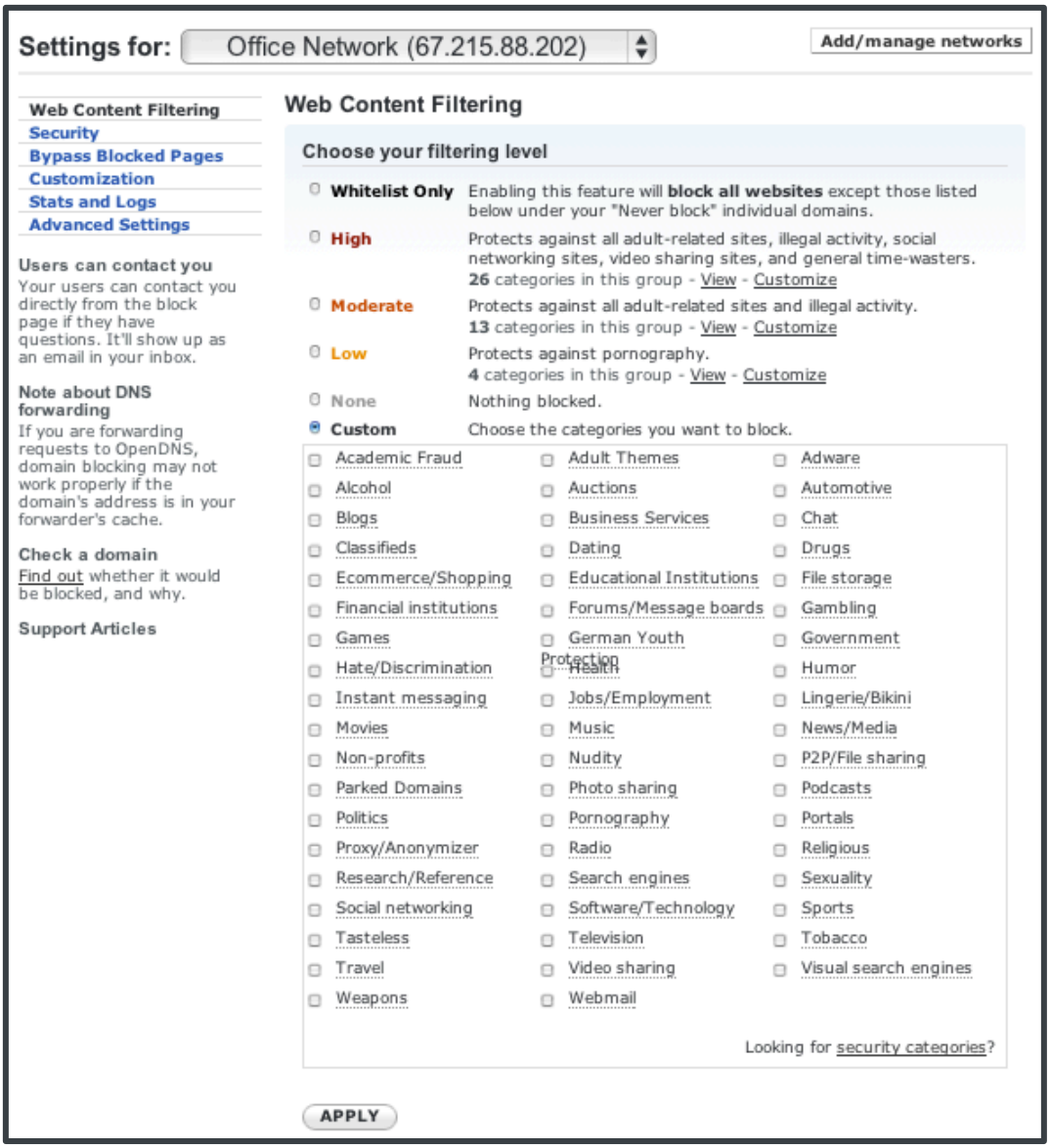
    Note: Dynamic IP networks require running a lightweight IP updater client on a computer on the network.



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

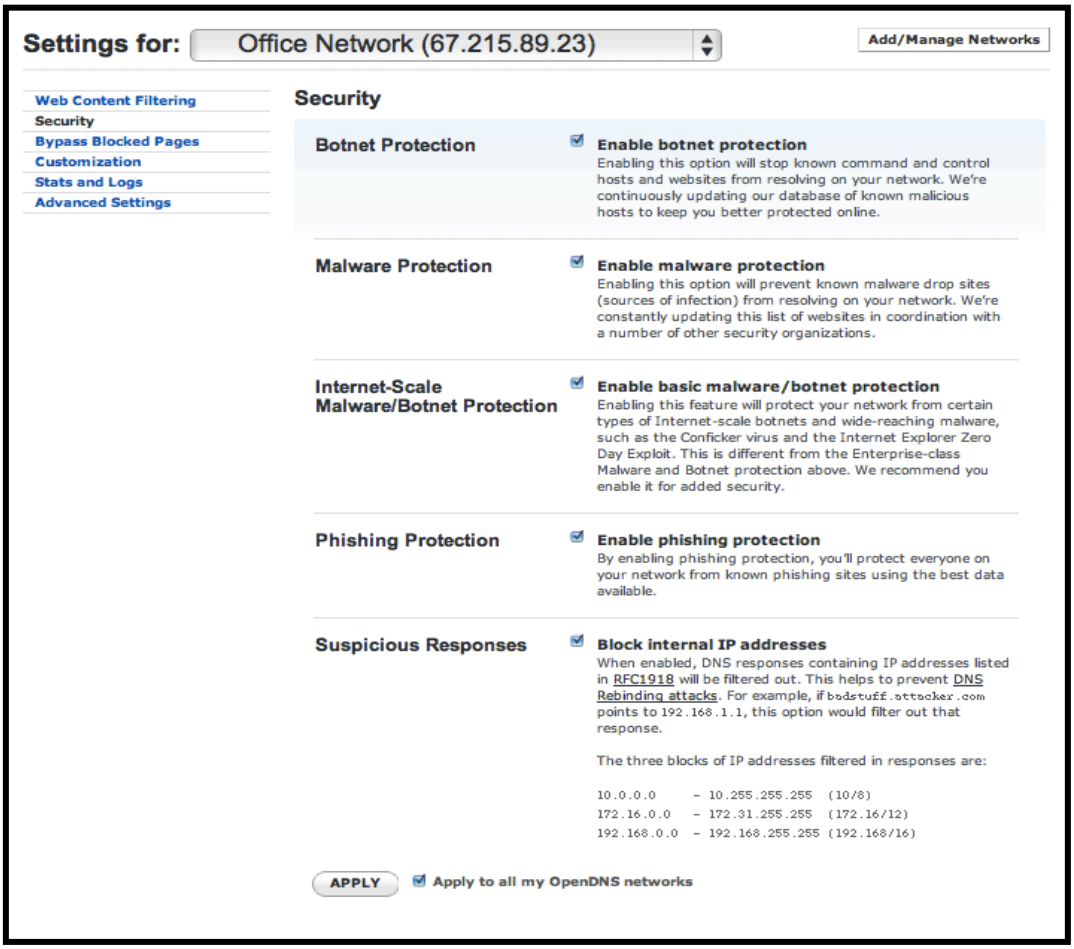


6. Configure content filtering settings by choosing from pre-defined filtering levels or you may choose "Custom" to build a custom bundle from 57 categories. If you have multiple networks registered with OpenDNS you will have the option to apply this change to all of your networks.



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

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.



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.