Congratulations on signing up for our Malicious Domain Blocking and Reporting (MDBR) service! The final step to complete your enrollment for the service is to configure your local forwarder to send DNS queries to Akamai’s primary and secondary recursive DNS servers at 96.7.136.4 and 96.7.137.4.

Typically, you can configure these “forwarders” in the same location where you manage other settings for your DNS. The following are the most common scenarios, but will be dependent on your organization’s specific DNS setup:

**For Windows Servers:**
DNS settings management is available as an Administrative Tool in the Control Panel. Once you access the DNS management tool, edit the Forwarders, which are located in Properties, to include the IP addresses for Akamai’s primary and secondary recursive DNS servers (96.7.136.4 and 96.7.137.4).

**For organizations using BIND:**
Open and modify the named.conf.options file to include the IP addresses for Akamai’s primary and secondary recursive DNS servers (96.7.136.4 and 96.7.137.4) in the Forwarders area.

**For organizations using a Next-Generation Firewall (NGFW) or Secure Web Gateway (SWG) product:**
Navigate to the DNS Proxy or Server settings for your organization’s applicable product, and enter the IP addresses for Akamai’s primary and secondary recursive DNS servers (96.7.136.4 and 96.7.137.4).

**To test your organization’s DNS change:**
After configuring your local forwarder to send DNS inquiries to Akamai’s recursive servers, you can test that your DNS change was successful with the following URLs:

- CnC: akamaietpcncctest.com
- Phishing: akamaietpphishingtest.com
- Malware: akamaietpmalwaretest.com

If the service is operating properly, you will be directed to a pre-configured block page, indicating that access to the website it prohibited. If your organization’s DNS requests are not reaching Akamai’s servers, you will be directed to a demonstration website indicating that Akamai Enterprise Threat Protector (ETP) has not been set up correctly.

For step-by-step guides on how to configure DNS forwarding, please visit Akamai’s Enterprise Threat Protector Help website.

For additional information and troubleshooting, please visit the CIS MDBR FAQ page.

For questions or additional help in setting up DNS forwarding, please contact soc@cisecurity.org.