Using Extension Mechanisms for DNS (EDNS0)

The NIOS appliance supports EDNS0 (Extension Mechanisms for DNS), which allows DNS clients to expand and advertise up to 4096 bytes of UDP packets for certain DNS parameters. EDNS0 facilitates the transfer of UDP packets beyond the original restricted packet size of 512 bytes. As defined in RFC 6891, EDNS0 provides extended UDP packet size that supports additional DNS functionality, such as DNSSEC. When EDNS0 is supported, the DNS client adds information to the additional data section of a DNS request in the form of an OPT pseudo-RR (resource record). An OPT RR does not contain actual DNS data and its contents pertain to the UDP transport layer message only. An OPT RR is not cached, forwarded, or stored. For more information about EDNS0, refer to RFC 6891: Extension Mechanisms for DNS (EDNS0).

EDNS0 is enabled on the NIOS appliance by default, which means all outgoing recursive queries are set to have a maximum UDP packet size of 4096 bytes. Typically, when the appliance receives a DNS request that contains an OPT RR, it assumes the DNS client supports EDNS0 and thus scales its response accordingly. When the appliance is used as a forwarder or a resolver for recursive queries and communicates with a client that does not support EDNS0, the appliance sends three queries starting with one that contains EDNS0 and DNSSEC support messages and is set to a maximum UDP packet size of 4096 bytes. When the first query fails, the appliance sends another query that contains only the EDNS0 support message. If the second attempt fails too, the appliance sends a third query that indicates a standard 512-byte query. Note that when EDNS0 is not used, DNS packets may be sent over TCP. For DNS service to function properly at this stage, ensure that you configure your firewall accordingly.

The following information demonstrates how the appliance responds when EDNS0 is enabled by default and the end server does not support EDNS0:

Packet 0954: 08:19:38.925 - query for www.google.com from Infoblox to forwarder (with EDNS0 support by setting the Extended Label Type to '01' and DNSSEC OK bit to '1')
Packet 1138: 08:19:47.927 - query for www.google.com from Infoblox to forwarder (with EDNS0 support by setting the Extended Label Type to '01' and DNSSEC OK bit to '0')
Packet 1504: 08:19:58.929 - query for www.google.com from Infoblox to forwarder (without EDNS0 and DNSSEC support by sending a standard 512-byte query)
Packet 1505: 08:19:30:960 - query response for www.google.com from forwarder to Infoblox

To ensure that end servers that do not support EDNS0 can respond to recursive queries from the NIOS appliance and to improve DNS performance, you can disable EDNS0 for the Grid and override the Grid settings for individual members. Note that you cannot configure the maximum UDP packet size, which is set for 4096 bytes by default. When you disable EDNS0, the appliance does not include OPT RRs for all outgoing recursive DNS queries. Thus remote end servers that do not support EDNS0 can still respond to the queries. This feature is useful when your NIOS appliance is used as a forwarder or a resolver for recursive queries, and the end servers in the configuration do not support EDNS0.

**WARNING:** When you disable EDNS0, all outgoing DNSSEC queries to zones within trusted anchors will fail even if DNSSEC validation is enabled. This is due to the restriction of the UDP packet length when you disable EDNS0. For information about DNSSEC, see About DNSSEC.

To disable EDNS0:

1. **Grid:** From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
   **Member:** From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.
2. In the Grid DNS Properties or Member DNS Properties editor, click the General tab -> Advanced tab, and complete the following:
   - **Disable EDNS0:** This check box is deselected and EDNS0 is enabled by default. To override the value inherited from the Grid, click Override. To retain the same value as the Grid, click Inherit. Select this check box to disable EDNS0. When you disable EDNS0, the appliance does not include OPT RRs for all outgoing recursive DNS queries and all outgoing DNSSEC queries to zones within trusted anchors will fail even if DNSSEC validation is enabled.
3. Save the configuration and click Restart if it appears at the top of the screen.