

DEPLOYMENT GUIDE

DoT and DoH Implementation Guide

Threat Defense

Table of Contents

Introduction.....	2
Why make changes to DNS protocol?.....	2
Introducing DoH and DoT.....	2
DNS over TLS (DoT).....	2
DNS over HTTPS (DoH).....	2
DoT and DoH Enterprise Challenges.....	3
Recommended Best Practices.....	3
Instructions.....	4
Configuring NIOS to download the DoH feed.....	4
NIOS Configuration.....	7
License and Configuration Requirements.....	7
Configuration steps.....	8
Troubleshooting.....	10
Generating & Reviewing Hits.....	11
Configuring BloxOne DDI to forward all queries to BloxOne ThreatDefense.....	11
Configuring DNS over HTTPS and DNS over TLS.....	11
Licensing and Certificate Requirements.....	11
System Requirements.....	12
CLI Commands.....	13
Modifying ADP rules.....	16
Generating Certificate Signing Requests.....	19

Introduction

The sudden rollout of encrypted DNS services in applications and operating systems has left Infoblox customers with unexpected security gaps in their network architecture. The purpose of this guide is to help our customers address these gaps by using Infoblox Encrypted DNS, Advanced DNS Protection, and BloxOne® Threat Defense features in combination with their traditional security solutions.

Why make changes to DNS protocol?

The concept of openness has been a fundamental feature of the Internet since its inception. Although users transmit sensitive information such as credit card numbers, email and passwords between their web browsers and websites using the secure HTTPS protocol, initial requests for Internet addresses and subsequent responses for website locations are transmitted in plain text. As a result, DNS has traditionally suffered from what we describe as a “last mile” security problem. Communications between a DNS client and its local DNS server are almost always unencrypted, and therefore subject to spoofing, interception, hijacking, and more problems. Improvements have been made to incorporate greater end-to-end security. DNS Security Extensions added authentication and data integrity checking to DNS, but the last leg of communication to the web browser was still open to spoofing.

Introducing DoH and DoT

Industry groups within the Internet Engineering Task Force (IETF) have approved two standards to address these issues. They work by encrypting the DNS communication between your operating system’s stub resolver and your recursive DNS resolver. One is known as DNS over TLS (Transport Layer Security) or “DoT,” and the other is DNS over HTTPS or “DoH.” Both technologies ensure data privacy and authentication by encrypting communications between DNS clients and servers. However, in doing so, each point to external DNS resolvers, thereby allowing client devices to access DNS services outside of your control and exposing the enterprise to potential security risk.

DNS over TLS (DoT)

DoT is an IETF standard that uses the common Transmission Control Protocol (TCP) as a connection protocol to layer over TLS encryption and authentication between a DNS client and a DNS server. Functioning at the operating system level, it communicates over TCP port 853. This is a well-known port used for all encrypted DNS traffic, and network administrators are very familiar with it. DoT traffic is encrypted, but its use of a well-understood port makes it easier for network administrators to monitor and control encrypted DNS when it appears. DoT is also a mature standard backed by traditional players in the DNS industry.

DNS over HTTPS (DoH)

Backed by the Mozilla Foundation and Chromium Projects, DoH is the other IETF security protocol that addresses DNS client and DNS server communication security. It leverages the security protocol extension HTTPS to provide encryption and authentication between a DNS client and server. A potential problem with DoH is that it uses the same TCP port (443) that all HTTPS traffic uses. As a result, it might prove challenging to troubleshoot DoH-related DNS issues because of the inability to distinguish DoH-based DNS

requests from regular HTTPS requests. For example, if a network administrator is employing DNS monitoring to block DNS requests to known malicious domains, he or she would not see those particular requests in HTTPS. Hence, that malicious traffic would go undetected. In addition, DoH operates at the application layer rather than the operating system, which introduces the potential for browser traffic to bypass enterprise DNS controls. The circumvention of DNS controls could hamper the support team's ability to maintain the levels of network performance, security, scale, and reliability that enterprises demand from DNS.

DoT and DoH Enterprise Challenges

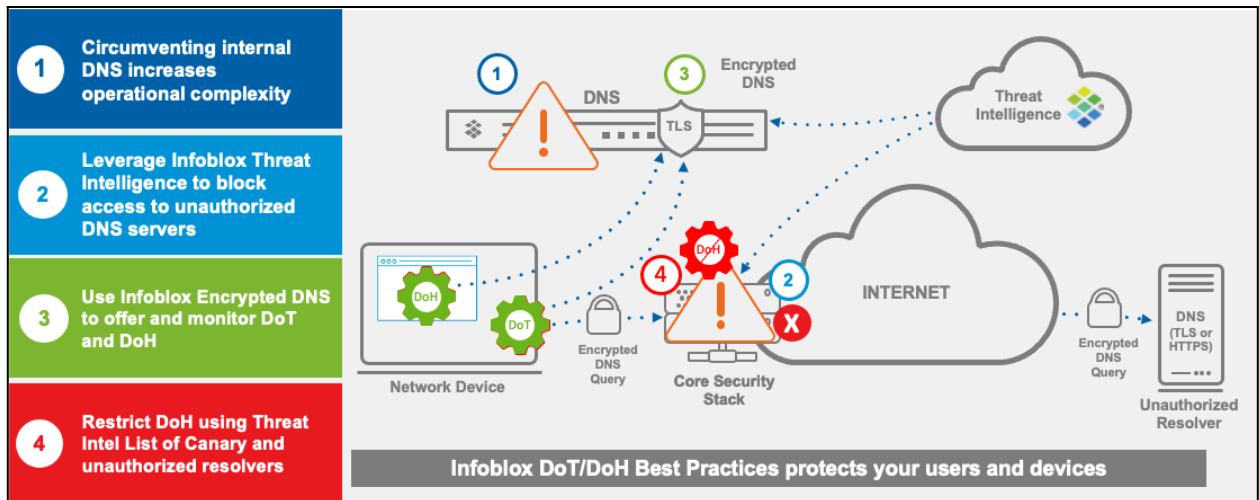
Please refer to this Solution Note: [Solving Unintended Challenges with DoT and DoH](#)

And this Blog Post for more information: [Keeping up with DoT, DoH and HTTP/3 Changes to Your Network](#)

Recommended Best Practices

We recommend a multi-stage approach to mitigate the threat from unauthorized DNS services.

- Block access to unauthorized DNS servers using Infoblox threat intelligence and ADP
- Use Infoblox Encrypted DNS to offer and secure DoT and DoH traffic to your users.




Instructions

Configuring NIOS to download the DoH feed


Navigate to **Policies>On-Prem DNS Firewall** to configure the On-Prem DNS Firewall service. Complete the four-step process to configure your On-Prem DNS Firewall settings. Please note, downloading the Infoblox Threat Intelligence Feed Deployment Guide is Step 1 of the process. Once you have reviewed the guide, please proceed to Step 2 to begin the configuration process.

1. Click **Download Deployment Guide**. Read through the guide thoroughly before proceeding to the next step where you will configure your NIOS feeds.


Complete the 4 steps below to configure the On Prem DNS Firewall settings.

 **Step 1**
Download and read the Deployment Guide.


[Download Deployment Guide](#)

 **Step 2**
Configure feed values in NIOS with these feed addresses.

[Feed Configuration Values](#)

 **Step 3**
Configure distribution server details.

[Distribution Server Configuration Values](#)

 **Step 4**
Configure list of DNS Server to receive notifications on feeds update.

[Configure Members](#)

2. Feed Configuration

Click **Feed Configuration Values** to configure the NIOS feed values with the provided feed addresses based on your subscription. Copy these values to a text editor as you require them later for NIOS configuration. Please note, the record count associated with a feed is published along with the feed's description. Once completed, click **Close** and proceed to Step 3.



3. Distribution Server Configuration Values

Click **Distribution Server Configuration Values** to configure your distribution servers. Both IPv4 and IPv6 IP addresses may be used to serve your feeds, depending on your specific requirements. TSIG Key encryption algorithms supported include HMAC MD5 512-bit and HMAC 256 256-bit. Please be aware; it may take up to one hour before your newly created TSIG keys become active.

- To set up how your feeds are distributed, complete the following steps:
- On the Distribution Server Details screen, for **BLOXONE HITS RPZ FEED**, toggle the switch to Enable to add the option of a custom RPZ feed to the feed distribution. When enabling the custom RPZ feed, specify the maximum number of feed indicators the custom RPZ feed will return along with and an expiration date for the indicators.
- Select either the **IPv4** or **IPv6** IP options for both the US West Distribution and the East Distribution Servers.
- **Copy** and **save** your selected IP addresses. You will need them later when configuring NIOS.
- Select a **TSIG Key algorithm** from among the drop-down menu choices. Algorithm choices include HMAC MD5 512-bit and HMAC 256 256-bit. Once you have made your selection, click **Generate** to generate a new TSIG key.
- **Copy** and **save** the **Key Name** and **TSIG Key**.

- Select the new row by selecting the box next to it.
- In the **NAME** field, add a name for the member you are adding.
- In the **IP ADDRESS** field, add the IP address you want to use for the new member.
- Once you have finished adding members, you can remove any members you will not be using.

To remove a threat retrieval member, complete the following steps:

- Select the configured member you want to remove by selecting the box next to it.
- Click **Remove**.

Once you have configured your threat retrieval members, click Save & Close.

The screenshot shows a web interface titled "Configure Members". At the top left, there are two buttons: "Add Server" and "Remove Server". Below these is a table with two columns: "NAME" and "IP ADDRESS". The first row of the table is highlighted in blue and contains the text "Add to Threat Retrieval" in the NAME column and "192.168.1.104" in the IP ADDRESS column. There are checkboxes to the left of each row. Below the table, there are two buttons: "Cancel" on the left and "Save & Close" on the right.

	NAME	IP ADDRESS
<input checked="" type="checkbox"/>	Add to Threat Retrieval	192.168.1.104
<input type="checkbox"/>	Specialized feed management	192.168.1.104
<input type="checkbox"/>	Phishing	192.168.1.104
<input type="checkbox"/>	Malware	192.168.1.104
<input type="checkbox"/>	Adware	192.168.1.104
<input type="checkbox"/>	Botnet	192.168.1.104
<input type="checkbox"/>	Domain	192.168.1.104
<input type="checkbox"/>	Reverse lookup	192.168.1.104
<input type="checkbox"/>	Reverse IP lookup	192.168.1.104
<input type="checkbox"/>	Reverse DNS lookup	192.168.1.104
<input type="checkbox"/>	Reverse WHOIS lookup	192.168.1.104

This completes the Cloud Services Portal, On-Prem DNS Firewall portion for the setup and configuration of Infoblox Threat Intelligence feeds. Please proceed to the next page to configure NIOS.

NIOS Configuration

License and Configuration Requirements

To deploy remote RPZ feeds, you will need a Grid member with at least a DNS and RPZ license.

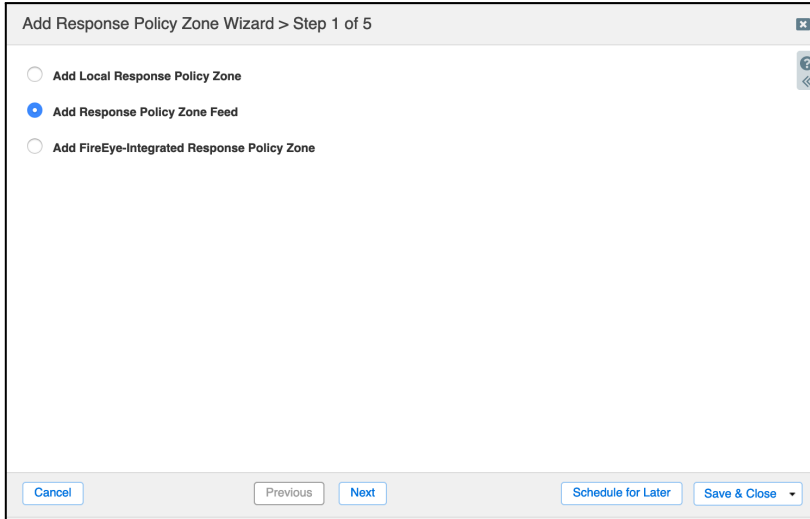
To obtain the feeds, your member will need access to our Threat Intelligence Feed servers on port 53 (UDP and TCP) as the feed data is transferred through a DNS zone transfer. Your server will also need to be able to perform recursion to obtain a response from the Internet.

To review log hits, you need to enable on the member or grid level the RPZ logging category (grid settings, toggle advanced, logging, check RPZ)

Configuration steps

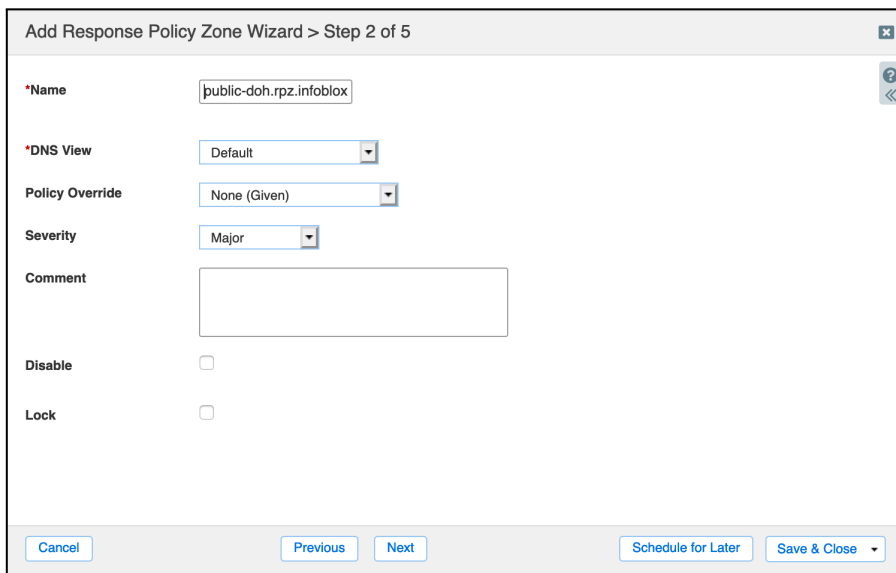
In NIOS navigate to: “Data Management” -> DNS -> “Response Policy Zones” Press the + button or use “Add” in the sidebar.

1. Select ‘Add a Response Policy Zone Feed’ then press Next.



2. Add the feed you want to use. In the case of DoH feeds, choose **Public_DOH** and **Public_DOH_IP**.

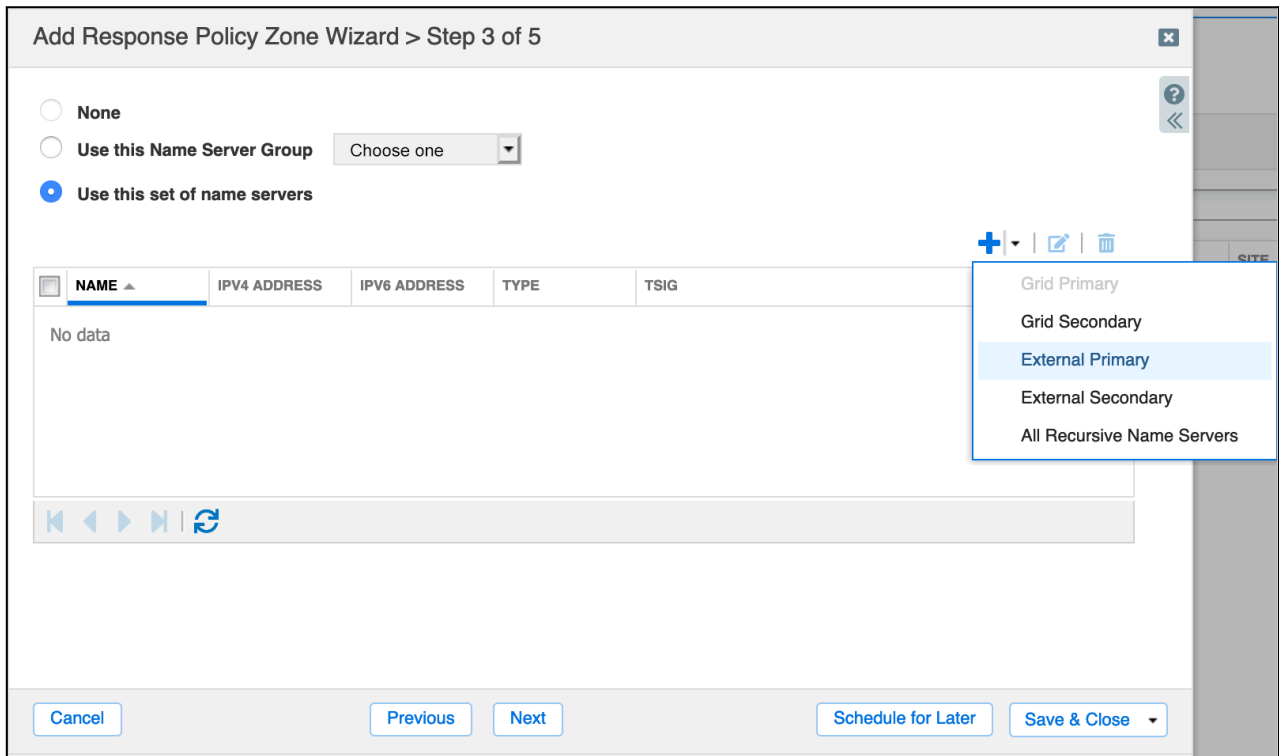
Note that each feed is a subset of the data, and deploying multiple feeds is required to cover all bases. You will have to repeat these steps for each RPZ.



- Leave Policy override on “None (Given)” for now. For the other policy override settings, please refer to the Admin Guide.
- Modify logging Severity if needed
- Press **next**

3. Add the External Primary

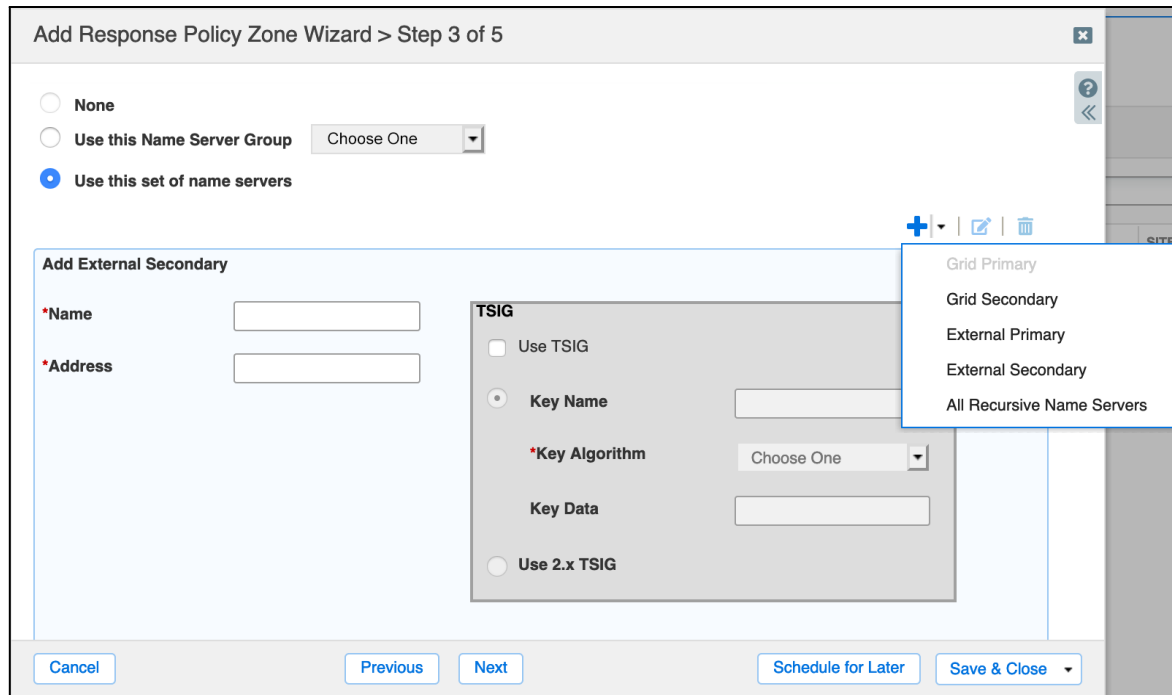
Use the drop-down next to the “+” sign to select External Primary



4. Define the External Primary’s settings

Refer to the portal for the values from your account. Select the nearest name server and use the values you copied from CSP during feed configuration. Note that the name field is only for reference purposes and you can use any name you choose to.

5. Add a Grid Secondary



- Use **“Select”** to select which member(s) you want to add or use **“All recursive servers”** if you want to add all recursive nodes with an RPZ license.
- Note that you can configure a single secondary to be **“Lead secondary.”** If you set this up, that member will be the only one to reach out to the external primary. You will then redistribute the feed internally between your members through zone transfers.
- Press **Add**
- Press **Save** and **Close**, restart services as required (use the banner at the top)
- Give services 5 minutes to fetch the zone. If you refresh the GUI, you will see the last updated value for when the last transfer was successful.

Troubleshooting

In case you are not getting a feed from our servers, verify if:

- You used the correct feed name
- Your time is set correctly (ntp should be used)
- You use the right key name, TSIG key, and algorithm

For further troubleshooting, check the syslog of your (lead) secondary for a message that includes **“transfer.”**

Generating & Reviewing Hits

1. Navigate to the **Data Management** → **DNS** → **Response Policy Zones**.
2. Find the Public_DOH or Public_DOH_IP feed.
3. Click on one of the feeds to export to a **.csv** file.
4. Pick an entry from the **.csv** file.
5. Run **nslookup** or **dig** against the member with the IP address or name.
6. Check the syslog for security hits. You should see a CEF entry with the domain(s) you are testing. You can also refer to the security dashboard for graphed out results based on the last 30 minutes of traffic.



Configuring BloxOne DDI to forward all queries to BloxOne ThreatDefense

1. Please follow the instructions in the following link: [Configuring DNS Forwarding Proxy and BloxOne DDI DNS](#)

Configuring DNS over HTTPS and DNS over TLS

As of NIOS 8.5.2, there is support for DNS over HTTPS and DNS over TLS.

Note: DNS over HTTPS and DNS over TLS are not supported on Grid Master or Grid Master Candidate. Please view the link below in the System Requirements link for supported appliance platforms.

Licensing and Certificate Requirements

DNS over TLS and DNS over HTTPS require the vDCA (virtual DNS Cache Acceleration) or vADP (virtual Advanced DNS Protection) service to be licensed and enabled. If the vDCA and/or the vADP services are not enabled, the DNS over TLS and DNS over HTTPS features will not work even if they are enabled.

The DNS over TLS or the DNS over HTTPS service uses the same self-signed certificate that NIOS generates for HTTPS communication when it first starts.

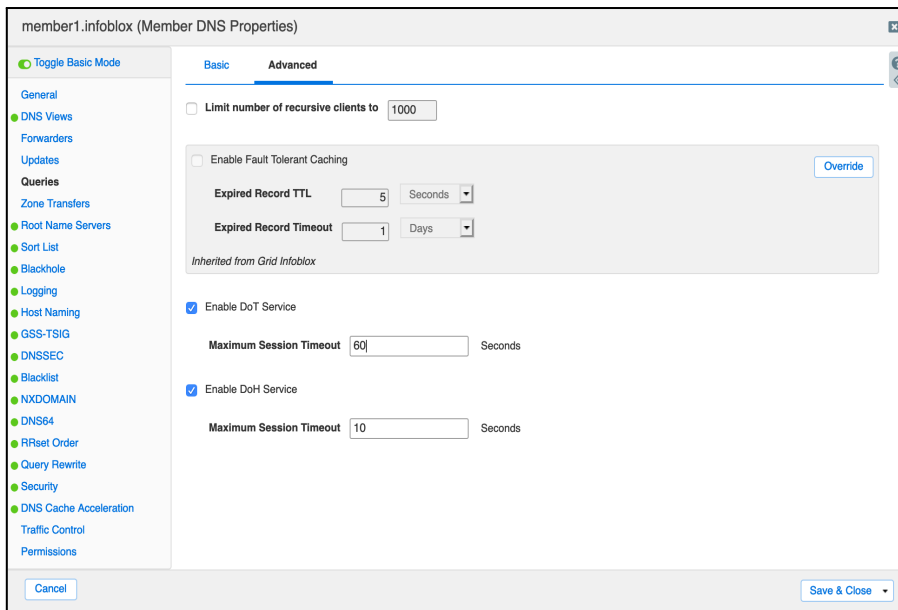
Infoblox recommends that you generate a certificate signing request (CSR) and use it to obtain a signed certificate from your own trusted certificate authority (CA).

System Requirements

See the NIOS Administrator's guide at the following link: [Configuring DNS over TLS and DNS over HTTPS Services - Infoblox NIOS 8.5](#)

To configure the DNS over HTTPS feature, complete the following steps:

1. **Grid member:** On the **Data Management** tab, click the **DNS** tab -> **Members** tab, select the member check box, and then click the **Edit** icon. **Standalone system:** On the Data Management tab, click the **DNS** tab, expand the **Toolbar**, and then click **System DNS Properties**.
2. In the **Member DNS Properties** editor/**System DNS Properties** editor, click **Toggle Advanced Mode** if the editor is in basic mode.
3. On the **Queries** tab, select the **Enable DoH Service** check box to enable the DNS over HTTPS feature.
4. In the **Maximum Session Duration** field, specify the maximum time in seconds a session can remain idle before it times out and closes. The default value is 10 seconds.
5. **Save** the configuration
6. As prompted, manually restart the member to enable the DNS over HTTPS feature.



To configure the DNS over TLS feature, complete the following steps:

1. **Grid member:** On the **Data Management** tab, click the **DNS** tab -> **Members** tab, select the member check box, and then click the **Edit** icon. **Standalone system:** On the **Data Management** tab, click the **DNS** tab, expand the **Toolbar**, and then click **System DNS Properties**. In the **Member DNS Properties** editor/**System DNS Properties** editor, click **Toggle Advanced Mode** if the editor is in basic mode.
2. On the **Queries** tab, select the **Enable DoT Service** check box to enable the DNS over TLS feature.

The screenshot shows the 'member1.infoblox (Member DNS Properties)' configuration window. The 'Advanced' tab is active. In the 'Queries' section, the following settings are visible:

- Limit number of recursive clients to 1000
- Enable Fault Tolerant Caching (with an 'Override' button)
- Expired Record TTL: 5 Seconds
- Expired Record Timeout: 1 Days
- Inherited from Grid Infoblox*
- Enable DoT Service
 - Maximum Session Timeout: 60 Seconds
- Enable DoH Service
 - Maximum Session Timeout: 10 Seconds

Buttons for 'Cancel' and 'Save & Close' are located at the bottom of the window.

3. In the **Maximum Session Duration** field, specify the maximum time in seconds a session can remain idle before it times out and closes. The default value is 60 seconds.
4. **Save** the configuration.
5. As prompted, manually **restart** the member to enable the DNS over TLS feature.

CLI Commands

From an SSH session or console connection, you can view the status of the DNS over HTTPS or DNS over TLS service, configuration, and details of active sessions using the following commands:

show doh-status

```
Infoblox > show doh-status
```

```
DoH is enabled
DoH trace is off
DoH key logging is off
Max server sockets: 128
curr server sockets: 2
Max client sockets: 200128
curr client sockets: 0
```

show doh-config

```
Infoblox > show doh-config
DoH listen on v4 addresses:
10.39.51.58
DoH listen on v6 addresses:
2620:10a:6000:2745::1011
DoH listen on port: 443
```

show doh-stats

```
Infoblox > show doh-stats
IP 10.39.51.58
rx_queries: 0
tx_queries: 0
dropped_packets: 0
max_qry_overflow_sess_drop: 0
opened_sessions: 11
closed_sessions: 11
curr_sessions: 0
IP 2620:010a:6000:2745::1011
```

```
rx_queries: 0
tx_queries: 0
dropped_packets: 0
max_qry_overflow_sess_drop: 0
opened_sessions: 0
closed_sessions: 0
curr_sessions: 0
```

show dns-over-tls-status

```
Infoblox > show dns-over-tls-status

DoT is enabled

DoT trace is off

DoT key logging is off
```

show dns-over-tls-config

```
Infoblox > show dns-over-tls-config

DoT listen on v4 addresses:

10.39.51.58

DoT listen on v6 addresses:

2620:10a:6000:2745::1011

DoT listen on port: 853
```

show dns-over-tls-stats

```
Infoblox > show dns-over-tls-stats

IP 10.39.51.58 (TLS):

rx_packets: 0

tx_packets: 0

dropped_packets: 0
```

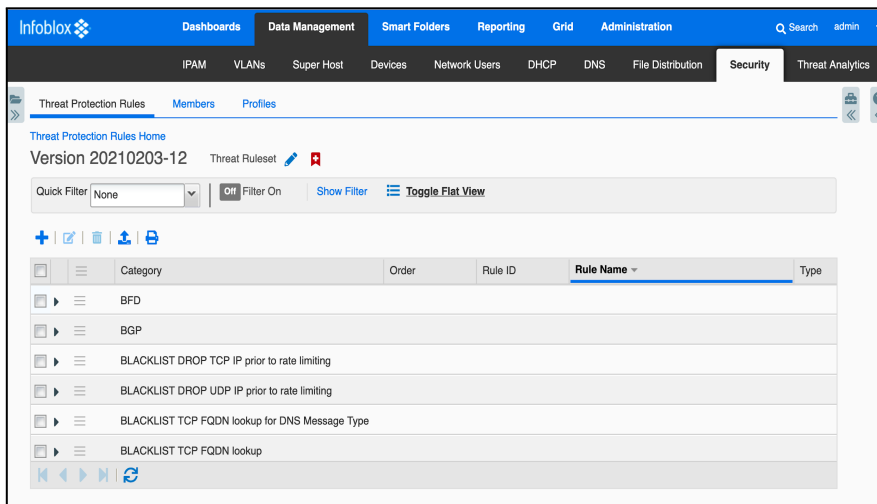


```
max_qry_overflow_sess_drop: 0
opened_sessions: 0
closed_sessions: 0
curr_sessions: 0
IP 2620:010a:6000:2745::1011 (TLS):
rx_packets: 0
tx_packets: 0
dropped_packets: 0
max_qry_overflow_sess_drop: 0
opened_sessions: 0
closed_sessions: 0
curr_sessions: 0
```

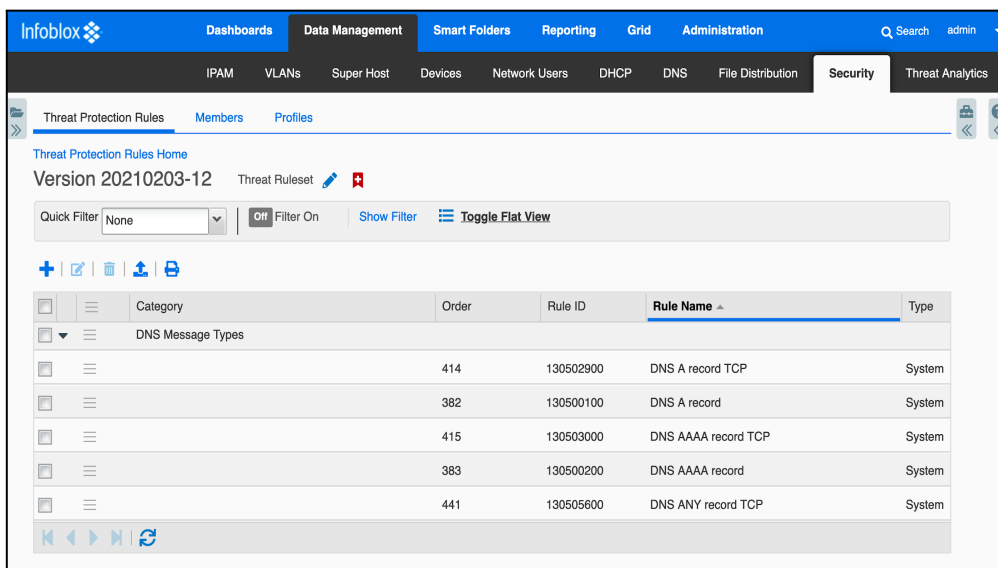
Modifying ADP rules

ADP blocks SVCB and HTTPS DNS records by default. These DNS message types can be used to discover DoH resolvers not operated by your organization. They can also be used to bypass protections from Response Policy Zones (RPZ). For most Enterprise organizations, we recommend you continue to block these rule types until the standards they are based on are completed and additional protections can be implemented. If you decide to pass these messages instead, you will need to modify 4 rules in the Threat Protection Ruleset as described below.

1. Navigate to **Data Management** → **Security** → **Threat Protection Rules**.



2. Scroll down the list to **DNS Message Types** and click on the **arrow** to expand the list. Click on the **'Rule Name'** column to either sort in descending or ascending order.



3. Scroll down the list to view the following filters:

- DNS HTTPS record - Rule ID 130502880
- DNS HTTPS record TCP - Rule ID 130506000
- DNS SVCB record - Rule ID 130502870
- DNS SVCB record TCP - Rule ID 130505900

Note: You may need to toggle the 'Rule Name' column in order to view the rules and perform the steps above.

4. Click on the corresponding hamburger icon and select 'Edit'.

DNS HTTPS record TCP (System Rule)

Basic

General Settings

Rule ID: 130506000

Name: DNS HTTPS record TCP

Category: DNS Message Types

Description: By default, this rule drops all TCP DNS packets that contain HTTPS record requests. You can change the default action to Pass.

Order: 445

Comment:

Disable

Cancel Save & Close

5. Click on the 'Settings' button and then click on the 'Action' drop-down menu and select 'Pass'. Click on 'Save & Close'.

DNS HTTPS record TCP (System Rule)

Basic

General Settings

Action: **Drop**
✓ Pass

Log Severity: Informational

***RULE PARAMETERS**

Description	Value
Events per second	1

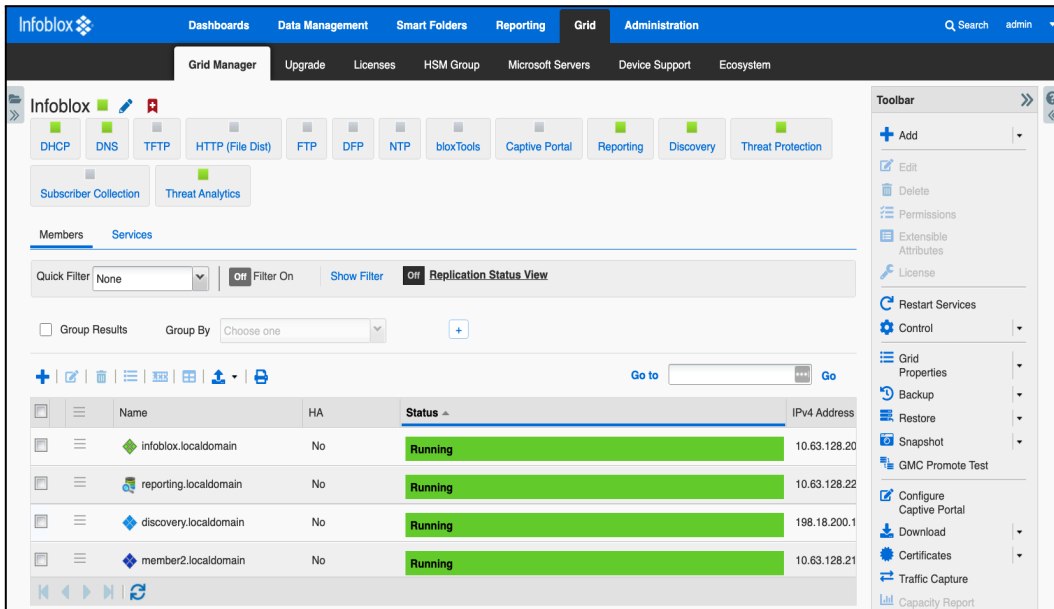
Cancel Save & Close

6. Repeat steps 3-5 above for the remaining records mentioned in step 3.

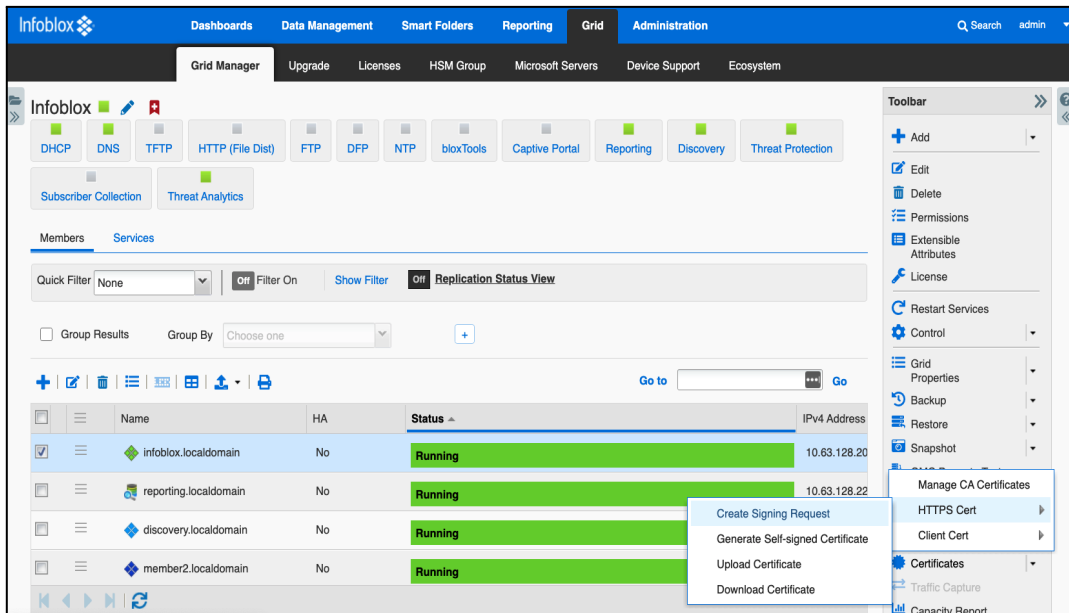
Generating Certificate Signing Requests

The DNS over TLS or the DNS over HTTPS service uses the same self-signed certificate that NIOS generates for HTTPS communication when it first starts. You can also generate a certificate signing request (CSR) and use it to obtain a signed certificate from your own trusted certificate authority (CA).

1. Navigate to **Grid** → **Grid Manager** → **Members**.



2. Click on a member. Navigate to **Toolbar** → **Certificates** → **HTTPS Certificate** → **Create Signing Request**.



3. Fill out the dialog box. Click **OK**.

Create Signing Request

***Secure Hash Algorithm and Key Size**

***Common Name (e.g. FQDN)**

Organization (e.g. Company)

Organizational Unit (e.g. Department)

Locality

State or Province

Country Code (2-letter code)

Admin Email Address

Comment

SUBJECT ALTERNATIVE NAME + | 🗑️

Type	Value
No data	



Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com