



ForeScout

Core Extensions Module: DNS Query Extension Plugin

Configuration Guide

Version 1.3



Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

<https://www.forescout.com/support/>

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Resources page on the Forescout website for additional technical documentation: <https://www.forescout.com/company/resources/>
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

© 2019 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2019-03-07 11:46

Table of Contents

- About the DNS Query Extension 4**
- Configure the Extension 4**
 - Verify That the Plugin Is Running4
- Test the Extension..... 4**
 - Sample Test5
- Detecting Endpoints – DNS Query Properties 6**
 - Is a DNS Server6
 - DNS Event.....7
- Core Extensions Module Information 8**
- Additional Forescout Documentation..... 9**
 - Documentation Downloads9
 - Documentation Portal 10
 - Forescout Help Tools..... 10

About the DNS Query Extension

The DNS Query Extension Plugin is a component of the Forescout® Core Extensions Module. See [Core Extensions Module Information](#) for details about the module.

The DNS Query Extension Plugin is an internal component of the Forescout platform that provides a service for various features in the product. In addition, it provides stand-alone features that:

- Determine whether a given endpoint in the network is a DNS server.
- Check DNS lookups of specific domain names by endpoints in the network. For example, it can detect that an endpoint browsed to a specific website, and then trigger an action to block that endpoint.

The DNS Query Extension sees traffic via the SPAN port. It detects and parses DNS messages in the network that reference specific host names. It does not report other DNS interactions.

This extension provides host properties in the Device Information folder. See [Detecting Endpoints – DNS Query Properties](#).

Configure the Extension

No configuration is required to work with the extension.

Verify That the Plugin Is Running

After installation, verify that the plugin is running.

To verify:

1. Select **Tools>Options** and then select **Modules**.
2. Navigate to the plugin and select **Start** if the plugin is not running.

Test the Extension

Run a test to:

- Verify that the Appliance can see traffic via the SPAN port.
- See the DNS traffic witnessed in the test time-frame (or within a packet count limit).
- Develop and verify regular expressions to use as policy conditions for the DNS Event Property.

Running a test does not let you:

- See the *Is a DNS Server* and *DNS Event* property values.

Use the following procedure to test the extension's ability to parse DNS messaging.

To test the extension:

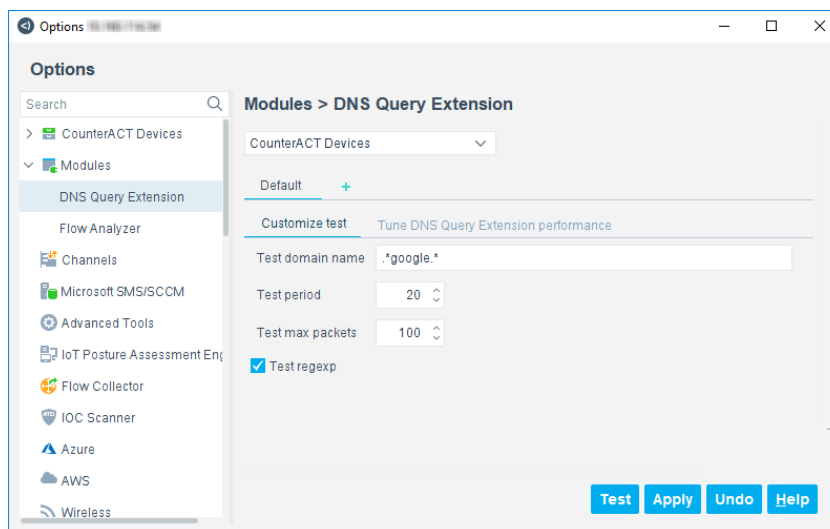
1. In the Forescout Console, select **Options** from the **Tools** menu. The Options dialog box opens.
2. Navigate to and select the **Modules** folder.
3. Select **DNS Query Extension**.
4. Configure the following fields to test the CounterACT device's connection to the DNS servers it detects.

Test domain name	Indicates a domain name used in test queries sent to DNS servers.
Test period	Indicates the maximum time period of the test, in seconds.
Text max packets	Indicates the maximum number of packets that are processed during the test.
Test regexp	Indicates whether the text in the Test domain name field should be evaluated as a regular expression.

5. Select **OK** to configure the CounterACT device with the specified test values.
6. Repeat this procedure to configure test values on other CounterACT devices.
7. Select **Test** to test the extension.

Sample Test

- Test domain name: **. *google. ***
- Test period: **20**
- Test max packets: **100**
- Test regexp: **(Checked)**



This example runs a traffic sniffer (pcap) for a maximum of 20 seconds or until the packet count is reached.

While capturing, it displays the packets that match the exact name unless “regex” was selected, in which case it prints all those that constitute a regular expression.

```

main:plugin_test_cb:750: Processing up to 100 DNS packets during 20 seconds...
main:setup_dns_listeners:216: Listening for DNS traffic on [eth0 eth1]
main:resolve_us_dns_server:526: ip=1.5.0.1 is a DNS server
main:resolve_us_dns_server:526: ip=10.44.1.1 is a DNS server
main:resolve_us_dns_server:526: ip=1.0.0.5 is a DNS server
main:resolve_us_dns_server:526: ip=1.5.26.93 is a DNS server
main:resolve_dns_prop:474: Name=docs.google.com Type=AAAA Client=1.5.3.86 Server=1.5.0.1 Response=0 Answers=
main:resolve_dns_prop:474: Name=docs.google.com Type=AAAA Client=1.5.3.86 Server=1.5.0.1 Response=1 Answers=docs.google.com. IN AAAA 2a00:1450:4009:806::200e
main:resolve_dns_prop:474: Name=ih6.googleusercontent.com Type=A Client=1.5.5.39 Server=1.5.0.1 Response=0 Answers=
main:resolve_dns_prop:474: Name=ih6.googleusercontent.com Type=A Client=1.5.5.39 Server=1.5.0.1 Response=1 Answers=ih6.googleusercontent.com. IN CNAME
googlehosted.l.googleusercontent.com.
main:resolve_us_dns_server:526: ip=1.5.0.4 is a DNS server
main:resolve_us_dns_server:526: ip=1.5.0.4 is a DNS server
main:resolve_us_dns_server:526: ip=1.5.0.4 is a DNS server
main:resolve_dns_prop:474: Name=ih6.googleusercontent.com Type=AAAA Client=1.5.5.39 Server=1.5.0.1 Response=0 Answers=
main:resolve_dns_prop:474: Name=ih6.googleusercontent.com Type=AAAA Client=1.5.5.39 Server=1.5.0.1 Response=1 Answers=ih6.googleusercontent.com. IN CNAME
googlehosted.l.googleusercontent.com. IN A 216.58.212.66
main:resolve_us_dns_server:526: ip=1.5.0.4 is a DNS server
main:resolve_us_dns_server:526: ip=1.5.0.4 is a DNS server
main:resolve_us_dns_server:526: ip=1.5.0.4 is a DNS server
main:resolve_dns_prop:474: Name=tools.google.com Type=A Client=1.5.1.3 Server=1.5.34.10 Response=0 Answers=
main:resolve_dns_prop:474: Name=tools.google.com Type=A Client=1.5.1.3 Server=1.5.34.10 Response=1 Answers=tools.google.com. IN CNAME tools.l.google.com.
tools.l.google.com. IN A 216.58.206.14
tools.l.google.com. IN A 216.58.206.14
main:resolve_us_dns_server:526: ip=1.5.48.1 is a DNS server
main:plugin_test_cb:773: Done

```

In order to generate traffic for the sample text, open an internet browser and navigate to ***drive.google.com*** or ***mail.google.com*** on a computer connected to a network monitored by the Forescout platform.

The output appears as follows:

```

Processing up to 100 DNS packets during 20 seconds...
Listening for DNS traffic on [eth0 eth1]
Name=drive.google.com Type=A Client= endpoint-ip Server= dns-server-ip Response=0 Answers=
<...etc...>
Done.

```

Detecting Endpoints – DNS Query Properties

This extension provides the following host properties in the Device Information folder:

- [Is a DNS Server](#)
- [DNS Event](#)

You can use these properties in custom policies. Refer to the *Forescout Administration Guide* for more information on custom policies.

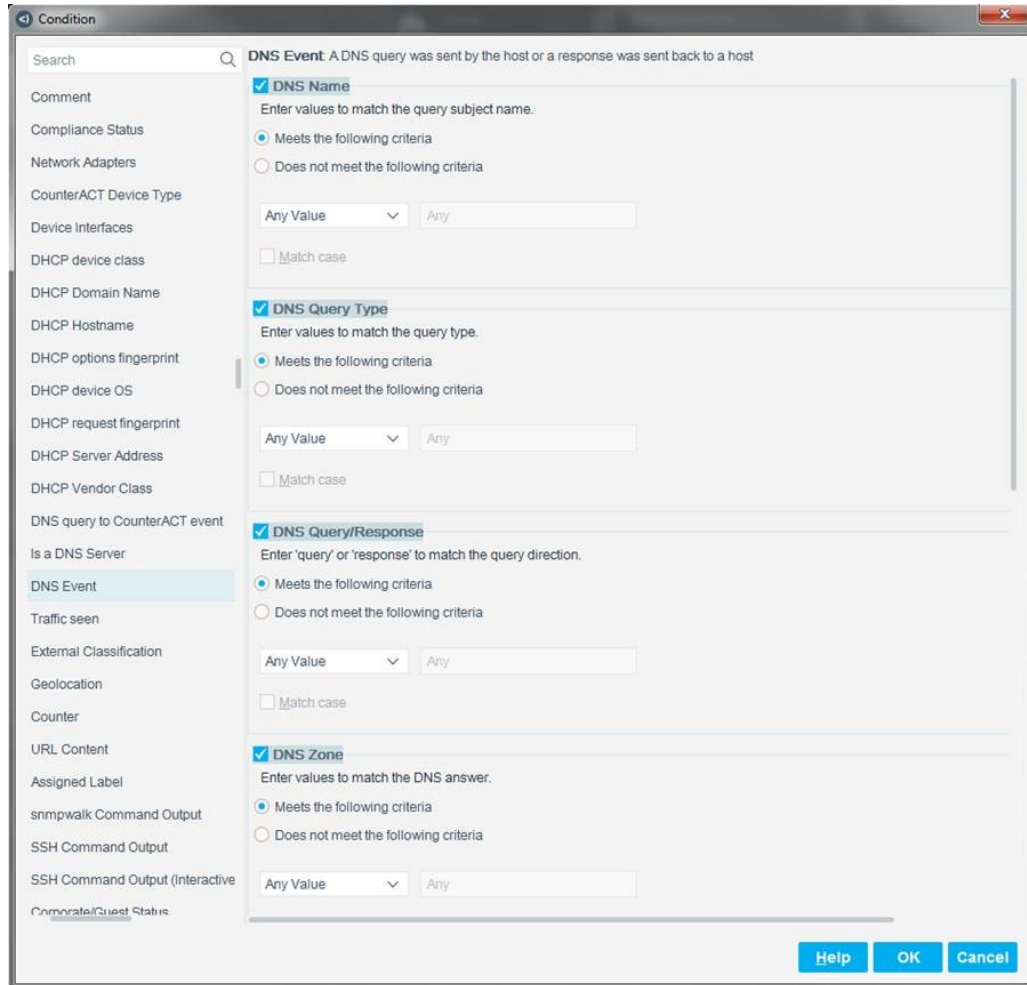
Is a DNS Server

This Boolean property indicates if the DNS Query Extension has observed the host accepting and responding to DNS queries.

DNS Event

This composite property indicates details of DNS messages to and from the host that were parsed by the DNS Query Extension during any of the following:

- [DNS Monitoring for Policy Conditions](#)
- [DNS Monitoring for IOCs](#)



Enter values to filter the condition search.

If the filters are not restrictive enough and the number of searches is high, the condition will not work properly.

The following information is reported for all DNS messages.

DNS Name	Indicates the hostname that the DNS server is asked to resolve.
DNS Query Type	Indicates the Query Type of the DNS message. This is also known as the Request Type, Record Type, or Lookup Type.

DNS Query/Response	Indicates whether this message is the initial query or the response of the DNS Server. Valid string values are “query” and “response”.
DNS Zone	In DNS response messages, contains the response message in zone file format.
DNS Addresses	In DNS response messages, indicates the IP addresses returned by the DNS server.
DNS Server Address	Indicates the IP address of the DNS server to which the query is addressed.
DNS Monitoring Tag	<p>Indicates the reason that the Forescout platform monitors messaging for the specified hostname. Valid values are:</p> <ul style="list-style-type: none"> ▪ Policy – Indicates that this hostname is specified in a policy condition using this host property. See DNS Monitoring for Policy Conditions. ▪ ATD – Indicates that Advanced Threat Detection mechanisms have identified this hostname for monitoring. See DNS Monitoring for IOCs. ▪ FLOW – Indicates that the Flow Analyzer has identified this hostname for monitoring. See DNS Monitoring for the Flow Analyzer. <p>All values can be valid simultaneously for a single DNS name.</p>

DNS Monitoring for Policy Conditions


When you create a policy condition using the **DNS Event** property provided by the extension, the Forescout platform monitors DNS traffic that matches the host name you specify. Only messages that reference the specific host names of interest are reported.

DNS Monitoring for IOCs

When a *DNS Query* IOC (indicator of compromise) is reported to the Forescout platform, the IOC Scanner initiates DNS monitoring that detects all DNS interactions that reference the suspect host name mentioned in the IOC. Only messages that reference the specific host names of interest are reported.

DNS Monitoring for the Flow Analyzer

When the Flow Analyzer is configured to collect flow data statistics, the Forescout platform monitors DNS traffic samples.

 *The Flow Analyzer component is not available at the time of this writing.*

Core Extensions Module Information

The DNS Extensions plugin is installed with the Forescout Core Extensions Module.

The Forescout Core Extensions Module provides an extensive range of capabilities that enhance the core Forescout solution. These capabilities enhance detection,

classification, reporting, troubleshooting and more. The following components are installed with the Core Extensions Module:

Advanced Tools Plugin	Dashboard Plugin	NBT Scanner Plugin
CEF Plugin	Device Classification Engine	Packet Engine
DHCP Classifier Plugin	External Classifier Plugin	Reports Plugin
DNS Client Plugin	Flow Analyzer Plugin	Syslog Plugin
DNS Enforce Plugin	Flow Collector	Technical Support Plugin
DNS Query Extension Plugin	IOC Scanner Plugin	Web Client Plugin
	IoT Posture Assessment Engine	

The Core Extensions Module is a Forescout Base Module. Base Modules are delivered with each Forescout release. This module is automatically installed when you upgrade the Forescout version or perform a clean installation.

Additional Forescout Documentation

For information about other Forescout features and modules, refer to the following resources:

- [Documentation Downloads](#)
- [Documentation Portal](#)
- [Forescout Help Tools](#)

Documentation Downloads

Documentation downloads can be accessed from the [Forescout Resources Page](#), or one of two Forescout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** – [Product Updates Portal](#)
- **Flexx Licensing Mode** – [Customer Portal](#)

 *Software downloads are also available from these portals.*

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.

Forescout Resources Page

The Forescout Resources Page provides links to the full range of technical documentation.

To access the Forescout Resources Page:

- Go to <https://www.Forescout.com/company/resources/>, select **Technical Documentation** and search for documents.

Product Updates Portal

The Product Updates Portal provides links to Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

- Go to <https://updates.forescout.com/support/index.php?url=counteract> and select the version you want to discover.

Customer Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Forescout Customer Portal:

- Go to <https://Forescout.force.com/support/> and select **Downloads**.

Documentation Portal

The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

- 📖 *If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.*

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

Forescout Administration Guide

- Select **Forescout Help** from the **Help** menu.

Plugin Help Files

- After the plugin is installed, select **Tools** > **Options** > **Modules**, select the plugin and then select **Help**.

Online Documentation

- Select **Online Documentation** from the **Help** menu to access either the [Forescout Resources Page](#) (Flexx licensing) or the [Documentation Portal](#) (Per-Appliance licensing).