ForeScout CounterACT®

Core Extensions Module: DNS Query Extension Plugin

Configuration Guide

Version 1.2

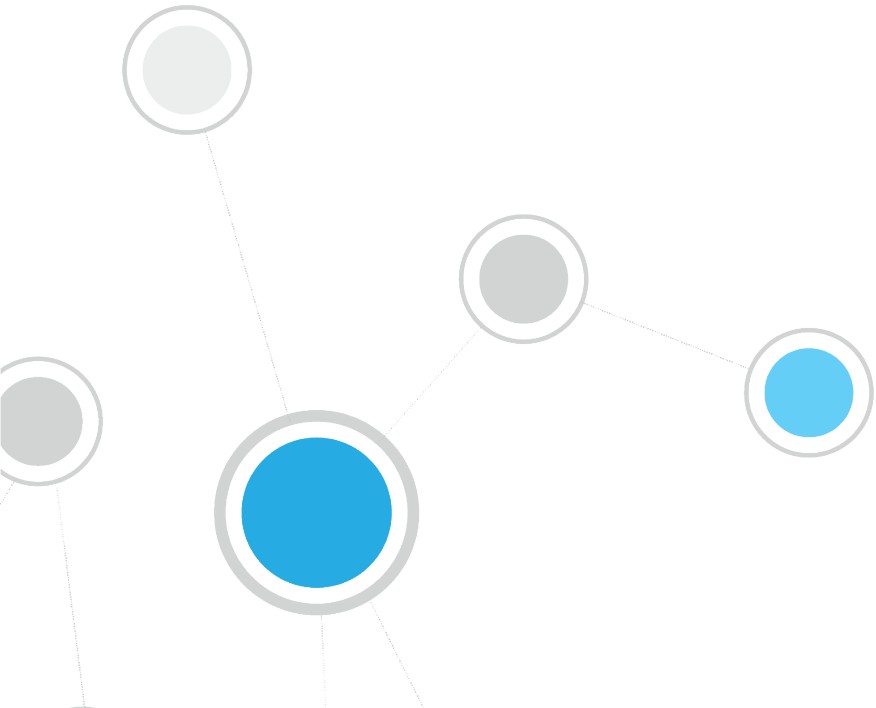


Table of Contents

About the DNS Query Extension

The DNS Query Extension Plugin is a component of the ForeScout CounterACT® Core Extensions Module. See Core Extensions Module Information for details about the module.

The DNS Query Extension is an internal component of CounterACT 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:

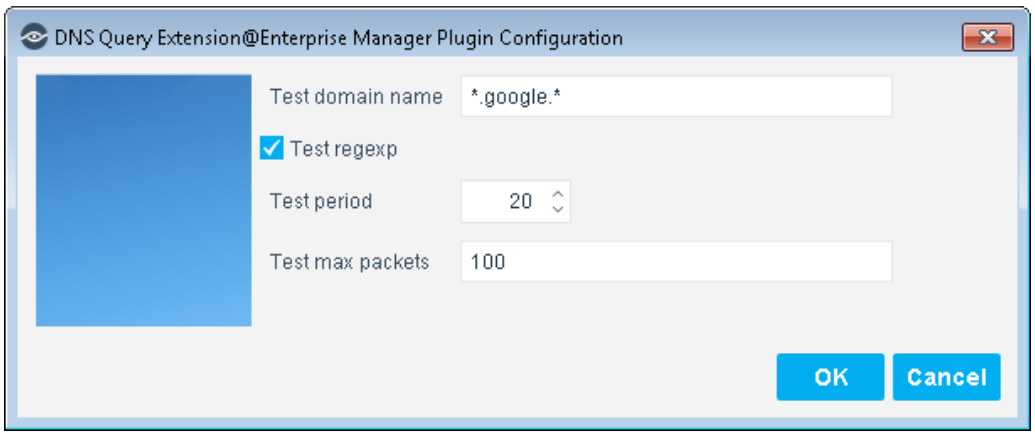
1. In the CounterACT Console, select **Options** from the **Tools** menu. The Options dialog box opens.
2. Navigate to and select the **Plugins** folder.
3. In the **Plugins** pane, select **DNS Query Extension**, and select **Configure**. The Select Appliances dialog box opens.
4. Select the Appliance or Enterprise Manager on which to text the extension, and select **OK**. The DNS Query Extension Configuration dialog box opens.
5. 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 regexp	Indicates whether the text in the **Test domain name** field should be evaluated as a regular expression.
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.

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

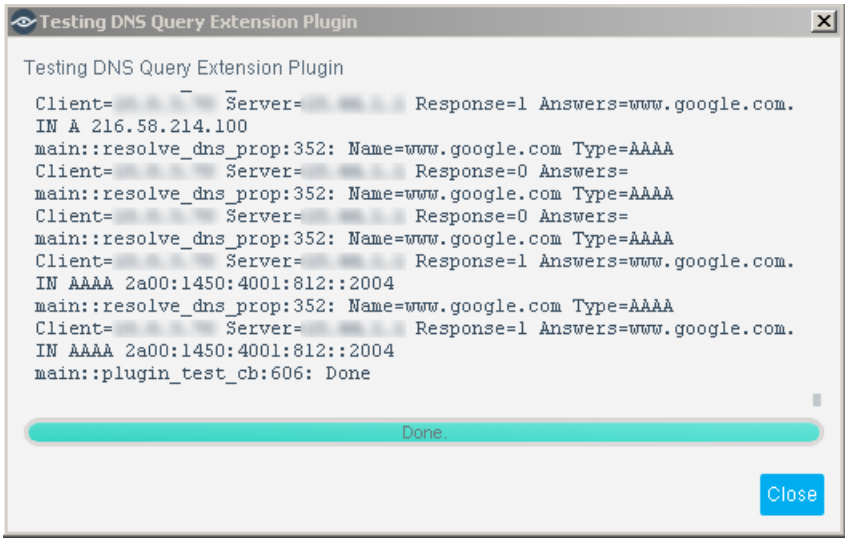
Sample Test

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



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 “regexp” was selected, in which case it prints all those that constitute a regular expression.



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 CounterACT monitored network.

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 *CounterACT Administration Guide* for more information on custom policies.

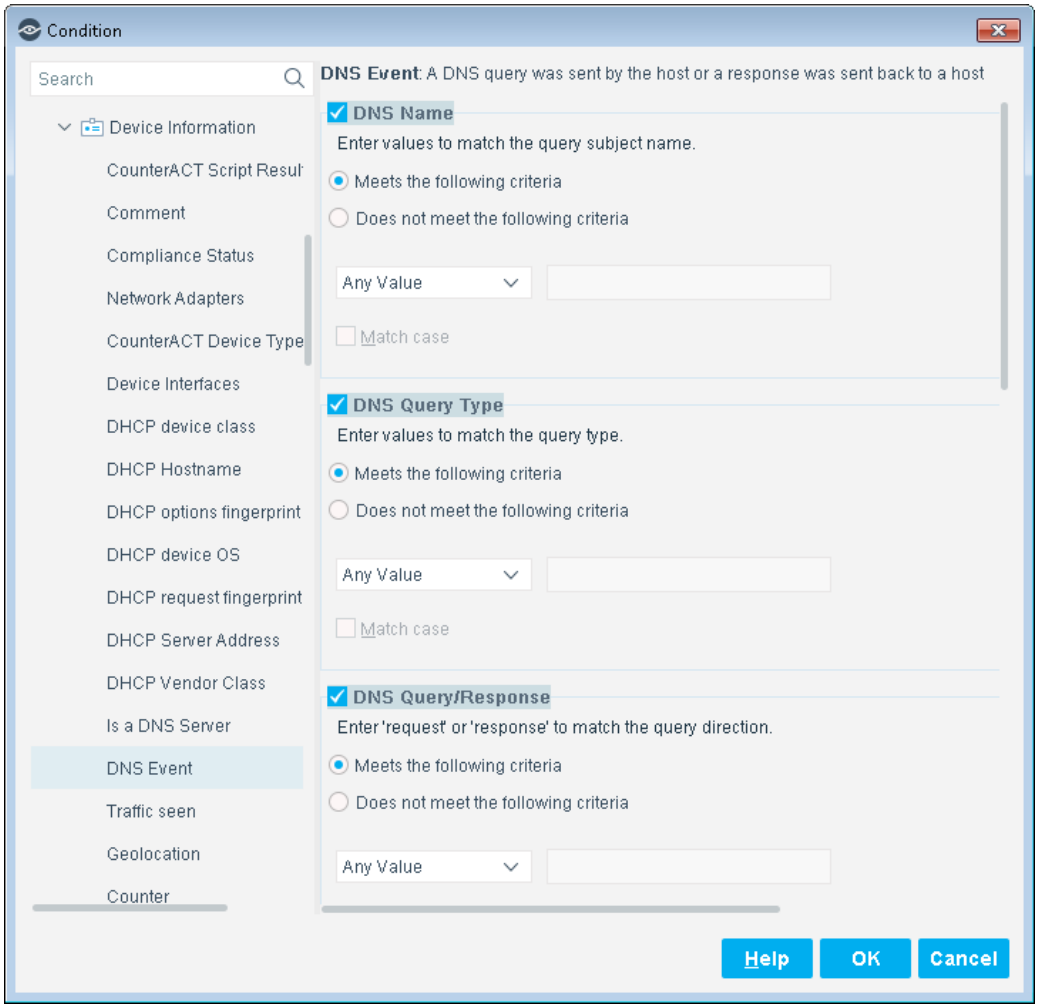
Is a DNS Server

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	Indicates the reason that CounterACT monitors messaging for the specified hostname. Valid values are: ▪ **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. All values can be valid simultaneously for a single DNS name.

DNS Monitoring for Policy Conditions

When you create a policy condition using the **DNS Event** property provided by the extension, CounterACT 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 CounterACT, 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, CounterACT 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 CounterACT Core Extensions Module.

The Core Extensions Module provides an extensive range of capabilities that enhance the core CounterACT solution. These capabilities enhance detection, classification, reporting, troubleshooting and more, and include the following components:

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

The Core Extensions Module is a ForeScout Base Module. Base Modules are delivered with each CounterACT release.

Components listed above are released and rolled back with the Core Extensions Module.

Refer to the *CounterACT Core Extensions Module Guide* for more module information, for example module requirements, upgrade and rollback instructions. See *Additional CounterACT Documentation* for information about how to access the module guide.

Additional CounterACT Documentation

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

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** - Product Updates Portal
- ***Centralized Licensing Mode*** - Customer Portal

Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

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

To access the Product Updates Portal:

1. Go to https://updates.forescout.com/support/index.php?url=counteract.
2. Select the CounterACT version you want to discover.

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, 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. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to https://forescout.force.com/support/.
2. Select **Downloads** or **Documentation**.

Documentation Portal

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

If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

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

CounterACT Administration Guide

Select **CounterACT Help** from the **Help** menu.

Plugin Help Files

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.
2. Select the plugin and then select **Help**.

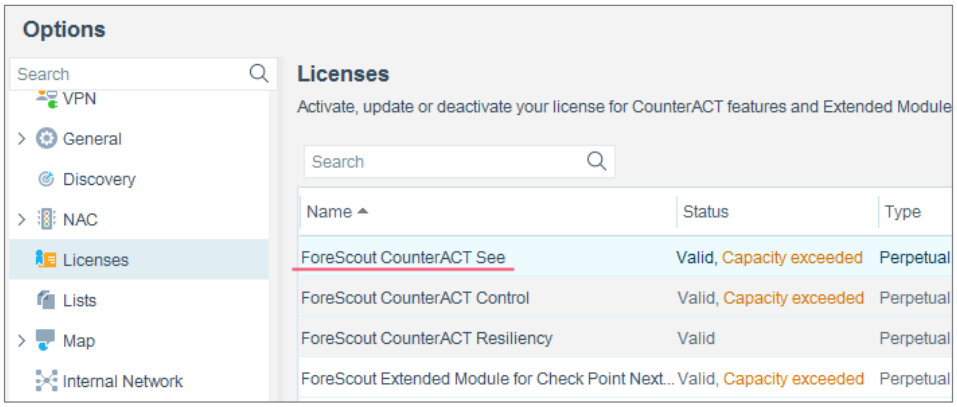
Documentation Portal

Select **Documentation Portal** from the **Help** menu.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

2018-04-10 09:21