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.

2019-07-10 11:53
Table of Contents

About the DNS Query Extension ................................................................. 4

Configure the Extension ........................................................................... 4
  Verify That the Plugin Is Running .......................................................... 4

Tune the Performance of the Extension .................................................... 4

Test the Extension .................................................................................... 6
  Sample Test ............................................................................................ 7

Detecting Endpoints – DNS Query Properties .......................................... 8
  Is a DNS Server ..................................................................................... 8
  DNS Event ............................................................................................. 8

Core Extensions Module Information ...................................................... 10

Additional Forescout Documentation ...................................................... 11
  Documentation Downloads ................................................................... 11
  Documentation Portal .......................................................................... 12
  Forescout Help Tools ........................................................................... 12
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 performed by network endpoints. For example, it can detect endpoints that browsed to a specific website, and then it can trigger an action to block those endpoints.

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.

Tune the Performance of the Extension

By default, the DNS Query Extension Plugin reports DNS Event entries for every endpoint that requests or receives DNS addresses of interest. The reporting frequency of DNS Event entries can be high.

Forescout defines DNS addresses of interest as:

- DN patterns raised by policy conditions, or by the Flow Connector or NetFlow Plugin

- DNS names that determine which indicators are CNC IOCs

The plugin provides two rate settings to limit the frequency of DNS Events. You can define a threshold and a period for each setting, where the threshold is the...
maximum number of events to handle per period. You must provide both rate settings to tune the performance of the plugin.

You can set rate limits for:

- DN Pattern/Endpoint limit: Used to avoid flooding an endpoint with entries after the policy condition matched the endpoint. By default: For a distinct combination of DN Pattern and Endpoint address, resolve only one DNS Event property per hour.

- FQDN/Resolved Address limit: Used to avoid flooding additional endpoints with entries, after a suspicious address is reported for the traffic on any endpoint. By default: For distinct combination of FQDN and Resolved Address, resolve only one DNS Event property per hour (regardless of actual arbitrary endpoint).

To tune 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, and select the Tune DNS Query Extension performance tab.
4. Configure the following fields to fine-tune the CounterACT device’s connection to the DNS servers it detects.

<table>
<thead>
<tr>
<th>Ignore whitelisted names:</th>
<th>Enable this option for ignoring any matching whitelisted entries.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore DNS names matching Do not resolve the DNS Event property for names that match an of the entries (regular expressions) in this list. You must separate the entries in the list with commas.</td>
<td></td>
</tr>
<tr>
<td>Limit the rate of DNS events (events are discarded only if all limits are exceeded):</td>
<td>Enable this option for ignoring DNS Events when either of the rate limits is reached. Note: You must apply both rate limits to tune the plugin's performance.</td>
</tr>
<tr>
<td>DN pattern/endpoint period defined below: Do not report the DNS Event property more than the threshold number of times specified in this field, per period.</td>
<td></td>
</tr>
<tr>
<td>DN pattern/endpoint period defined below: Do not report the DNS Event property more than the above-defined threshold number of times, per period defined in this field.</td>
<td></td>
</tr>
<tr>
<td>FQDN/resolved address For any given distinct combination of Endpoint and DN Pattern: Do not report the DNS Event property more than the above-defined threshold number of times, per period defined in this field.</td>
<td></td>
</tr>
<tr>
<td>threshold defined below: Do not report the DNS Event property more than the threshold number of times specified in this field, per period.</td>
<td></td>
</tr>
</tbody>
</table>
### FQDN/resolved address period (seconds): For any given distinct combination of FQDN and Resolved Address: Do not report the DNS Event property more than the above-defined threshold number of times, per period defined in this field.

<table>
<thead>
<tr>
<th>Options</th>
<th>Modules &gt; DNS Query Extension</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Customize test: Tune DNS Query Extension performance</td>
</tr>
<tr>
<td></td>
<td>Ignore whitelisted names</td>
</tr>
<tr>
<td></td>
<td>Limit the rate of DNS events (events are discarded only if exceeded all limits)</td>
</tr>
<tr>
<td></td>
<td>Rate limits</td>
</tr>
<tr>
<td></td>
<td>Ignore DNS names matching</td>
</tr>
<tr>
<td></td>
<td>DN pattern/endpoint threshold (count) 9</td>
</tr>
<tr>
<td></td>
<td>DN pattern/endpoint period (seconds) 2000</td>
</tr>
<tr>
<td></td>
<td>FQDN/resolved address threshold (count) 9</td>
</tr>
<tr>
<td></td>
<td>FQDN/resolved address period (seconds) 9600</td>
</tr>
</tbody>
</table>

5. Select **Apply** to configure the CounterACT device with the specified performance tuning values.

6. Select **Test** to test the performance.

## Test the Extension

Run a test to:

- Verify that the Appliance can see traffic via the SPAN port.
- See the DNS traffic detected 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**, and select the **Customize test** tab.
4. Configure the following fields to test the CounterACT device’s connection to the DNS servers it detects.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Test domain name</strong></td>
<td>Indicates a domain name used in test queries sent to DNS servers.</td>
</tr>
<tr>
<td><strong>Test period</strong></td>
<td>Indicates the maximum time period of the test, in seconds.</td>
</tr>
<tr>
<td><strong>Text max packets</strong></td>
<td>Indicates the maximum number of packets that are processed during the test.</td>
</tr>
<tr>
<td><strong>Test regexp</strong></td>
<td>Indicates whether the text in the Test domain name field should be evaluated as a regular expression.</td>
</tr>
</tbody>
</table>

5. Select **Apply** 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 “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 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.

<table>
<thead>
<tr>
<th><strong>DNS Name</strong></th>
<th>Indicates the hostname that the DNS server is asked to resolve.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DNS Query Type</strong></td>
<td>Indicates the Query Type of the DNS message. This is also known as the Request Type, Record Type, or Lookup Type.</td>
</tr>
<tr>
<td><strong>DNS Query/Response</strong></td>
<td>Indicates whether this message is the initial query or the response of the DNS Server. Valid string values are “query” and “response”.</td>
</tr>
<tr>
<td><strong>DNS Zone</strong></td>
<td>In DNS response messages, contains the response message in zone file format.</td>
</tr>
<tr>
<td><strong>DNS Addresses</strong></td>
<td>In DNS response messages, indicates the IP addresses returned by the DNS server.</td>
</tr>
<tr>
<td>DNS Server Address</td>
<td>Indicates the IP address of the DNS server to which the query is addressed.</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DNS Monitoring Tag</td>
<td>Indicates the reason that the Forescout platform monitors messaging for the specified hostname. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Policy</strong> – Indicates that this hostname is specified in a policy condition using this host property. See DNS Monitoring for Policy Conditions.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>ATD</strong> – Indicates that Advanced Threat Detection mechanisms have identified this hostname for monitoring. See DNS Monitoring for IOCs.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>FLOW</strong> – Indicates that the Flow Analyzer has identified this hostname for monitoring. See DNS Monitoring for the Flow Analyzer.</td>
</tr>
<tr>
<td></td>
<td>All values can be valid simultaneously for a single DNS name.</td>
</tr>
</tbody>
</table>

**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.

---

**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
- CEF Plugin
- DHCP Classifier Plugin
- DNS Client Plugin
- DNS Enforce Plugin
- DNS Query Extension Plugin
- Dashboard Plugin
- Device Classification Engine
- External Classifier Plugin
- Flow Analyzer Plugin
- Flow Collector
- IOC Scanner Plugin
- NBT Scanner Plugin
- Packet Engine
- Reports Plugin
- Syslog Plugin
- Technical Support 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:


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).