Forescout

Core Extensions Module: DNS Enforce Plugin

Configuration Guide

Version 1.4.1

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

Legal Notice

2020-08-02 14:49

Table of Contents

About the DNS Enforce Plugin

The DNS Enforce Plugin is a component of the Forescout® Core Extensions Module. See Core Extensions Module Information for details about the module.

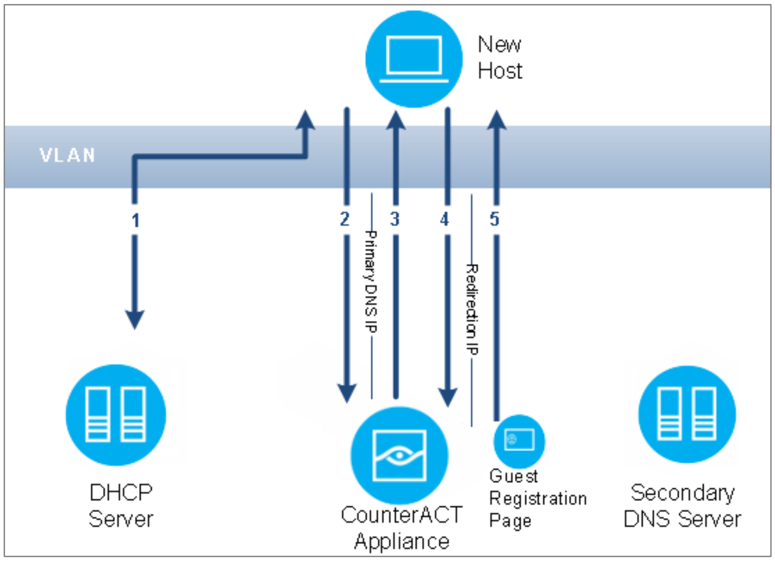
The DNS Enforce Plugin lets the Forescout platform implement HTTP-based policy actions such as *HTTP Notification* and *HTTP Redirection to URL* in cases where stateful traffic inspection is not possible. This is relevant, for example, with a remote site or an unmanaged network segment.

The plugin redirects a guest machine connecting to your corporate network to a predefined location if and only if there is an active HTTP-based policy action associated with that guest machine. If a guest machine is redirected, an application, such as a web browser, interacts with name servers through a domain name resolver. A resolver is an application program that resides on the user workstation and sends requests for DNS information when necessary.

The DNS Enforce Plugin requires that you define a Target IP address (not the CounterACT management IP) and explicitly configure it as the primary DNS server in order to implement HTTP-based actions. The plugin uses the specified Target IP to intercept DNS requests and respond when necessary with the address specified in the HTTP-based action. If these conditions are not met, the response of the Forescout platform forces the guest machine to resolve the address using one of the secondary DNS servers.

When the plugin is running, HTTP redirection interactions proceed as follows:

1. An endpoint connects to the network and submits a DHCP request. The DHCP server response points to the Target IP address as the primary DNS server.
2. The endpoint submits a DNS resolution request (for example *www.example.com*) to its primary DNS server - the plugin-provided network interface using the custom-defined Target IP address.



3. The Forescout platform examines the DNS request. If a policy determines HTTP redirection for this endpoint, the Forescout platform responds with a redirection IP address (for example, guest registration using the *HTTP Login* action will redirect the resolving endpoint to the Forescout platform’s captive portal address).

   The plugin will not always redirect endpoints browsing via an HTTP proxy. Specifically, if the proxy is specified as an IP address.

4. The endpoint sends its HTTP/HTTPS request to the target IP it received – the redirection IP address. The plugin receives the request and redirects it according to the specific HTTP action.
5. As in standard HTTP redirection, the Forescout Appliance examines the endpoint information in the request, and serves the page required by the applicable policy.

Overlapping IP Address Support

The DNS Enforce Plugin supports working with networks that use overlapping IP addresses. For details about enabling and configuring the Forescout platform’s support of overlapping IP address use in an enterprise’s network, refer to the *Forescout Working with Overlapping IP Addresses How-to Guide*. See Additional Forescout Documentation for information on how to access this document.

What to Do

You must perform the following to work with this plugin:

- Verify that requirements are met. See DNS Enforce Plugin Requirements for details.
- Configure a redirection target and other plugin behavior for the Forescout Appliance. See Configure the Plugin for details.
- For every network segment requiring DNS redirection, ensure that the DHCP server configuration uses the Target IP as the primary DNS server.

DNS Enforce Plugin Requirements

The plugin requires the following:

- Forescout interim release 8.2.1.
- Endpoint Module version 1.2.1 with the HPS Inspection Engine running.
- The plugin-specified Target IP address must be defined in the DHCP server as the primary DNS server.

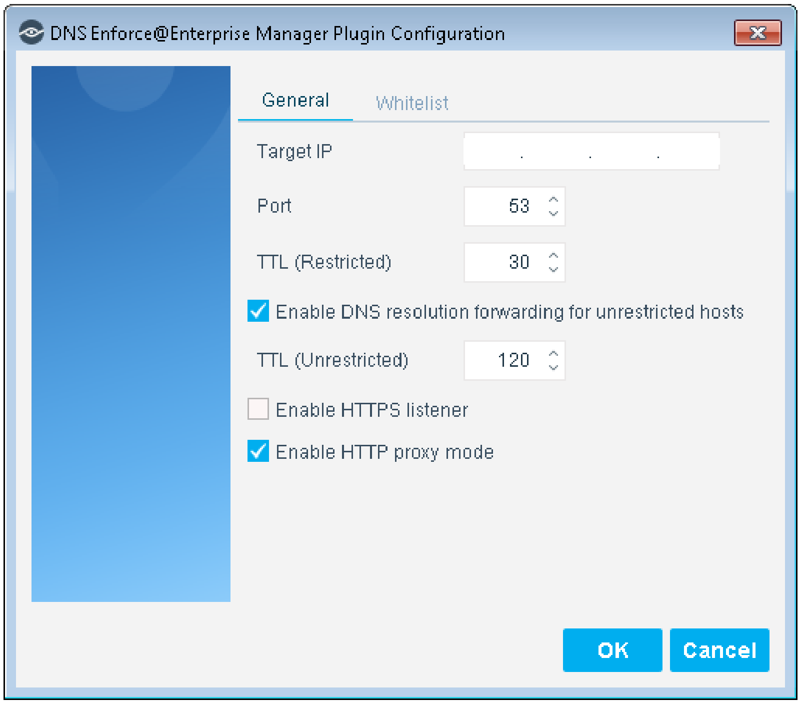
Configure the Plugin

This section describes how to configure the plugin.

To configure the plugin:

1. In the Forescout Console, select **Options** from the *Tools* menu. The *Options* pane opens.
2. Open the **Modules** pane and select **Core Extensions > DNS Enforce**.
3. Select **Configure**. If this is an Enterprise Manager, select the Forescout device on which you want to implement the redirect behavior and select **OK**.

   The *Plugin Configuration* dialog box opens.



Target IP . . .

Port 53

TTL (Restricted) 30

☑ Enable DNS resolution forwarding for unrestricted hosts

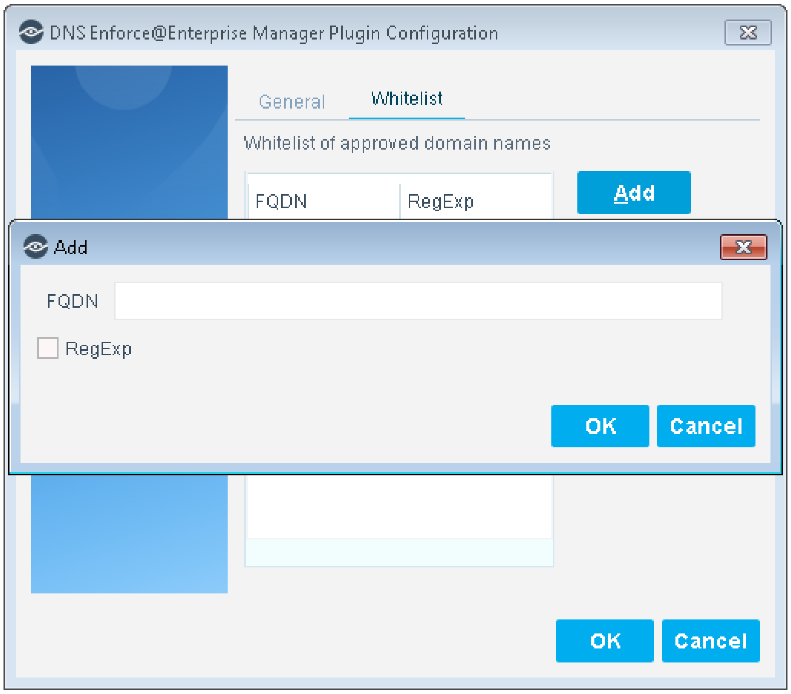
TTL (Unrestricted) 120

□ Enable HTTPS listener

☑ Enable HTTP proxy mode

4. In the *General* tab, specify values for the following parameters:
   - Target IP
   - Port Information
   - Time to Live Interval
   - Forwarding DNS Mode
   - HTTPS Listener
   - HTTP Proxy Mode

5. In the *Whitelist* tab, add any approved domain names. See Whitelist of Excluded Domain Names.


DNS Enforce@Enterprise Manager Plugin Configuration
General
Whitelist
Whitelist of approved domain names
FQDN
RegExp
Add
Add
FQDN
RegExp
OK
Cancel
OK
Cancel

6. Select **OK**.

Target IP

The plugin uses the Target IP to dynamically create a network interface on the appliance, to provide the following service:

- DNS queries received on that interface are examined to determine if redirection is needed (if an HTTP-based action is pending for the endpoint).

The specified Target IP address must be:

- Free/unassigned by any network connected device.
- Different from the management IP address.
- On the same VLAN as the Forescout management interface and reachable from remote devices (routed).

Port Information

DNS generally uses port 53 (default value) to complete requests. In rare cases you may want to modify the port settings to align with the network configuration.

Time to Live Interval

You can configure the time to live (TTL) interval that is included in the DNS resolve response. This value, in seconds, typically helps the resolver know the validity period of the result.

When caching is enabled on the endpoint, endpoints tend to use the cached value rather than retrieve it from the name server again. Typically, TTL intervals are very long (1-3 days) and would prevent the DNS Enforce Plugin from effectively restricting endpoints. If, for example, the TTL is 3 days, the endpoint will repeatedly assume that the address resolved by the Forescout platform is the server address of *www.example.com* long after the user successfully completed the guest login or compliance remediation steps.

Since the length of this interval depends upon whether the endpoint is redirected or not, configure a separate TTL interval for each category of endpoint, as follows:

- ***Restricted endpoints:*** A restricted endpoint is an endpoint having an HTTP-based policy action applied to it. The TTL interval value should be short enough so that endpoints do not continue to use cached values after they are released by user actions (user confirms message, successfully logs in, etc.), but long enough to avoid unneeded repetition that can potentially cause DNS Server overload. The default value is 30 seconds.
- ***Unrestricted endpoints:*** The TTL interval value should be short enough so that endpoints that are not subject to an HTTP action at the time of DNS resolution can be redirected later, if needed. The default is 120 seconds.

🗎 *The **TTL (Unrestricted)** option is only applicable when Forwarding DNS Mode is selected.*

Forwarding DNS Mode

You can configure how to respond to requests coming from endpoints that do not have an HTTP-based policy action applied to them (unrestricted endpoints).

You can configure the plugin to respond in any one of the following ways:

- Forward requests to an upstream DNS server(s), and limit the TTL of responses.
- Respond to such endpoints with a *DNS: Not Implemented* message.

If you select the *Enable forwarding DNS mode for unrestricted hosts* checkbox in the plugin configuration *General* tab, the plugin will forward requests to an upstream DNS server. If you clear the checkbox, you will need to include an additional IP address in the internal network list of DNS servers as a secondary server (in addition to the first DNS server address, which is the Target IP).

🗎 *By selecting this option, the plugin loses the ability to affect the Time to Live Interval of resolution responses.*

HTTPS Listener

You can enable or disable the HTTPS listener. Enabling the HTTPS listener effectively allows HTTPS access for endpoints that have an HTTP-based policy action applied to them (restricted endpoints). This option is disabled by default, meaning that HTTPS access is blocked by default.

When the plugin is used to implement HTTP actions, using a signed SSL certificate will not prevent endpoint users from receiving a browser security warning when they use HTTPS. Ensuring that the HTTPS listener is disabled will prevent the browser security warning from appearing by blocking HTTPS access.

HTTP Proxy Mode

You can proxy HTTP requests of unrestricted endpoints to ensure that endpoint users redirected by an HTTP action can access URLs containing the domain name that they browsed to.

After HTTP actions are successfully applied, endpoint users may be unable to access URLs containing the original domain name that they browsed to for an extended period of time because the DNS resolution is cached. For example, users who originally browsed to https://www.google.com were also unable to access https://www.google.com/preferences. Instead, an HTTP 404 error message appears.

This may occur as long as the original DNS resolution was cached on the endpoint. Many versions of Internet Explorer cache DNS resolutions indefinitely, ignoring the time-to-live (TTL) interval of the resolution. In such a case, the only way to circumvent this issue was for the end user to restart the browser.

Enabling this option may slightly increase the load on the plugin, potentially causing slower performance.

Whitelist of Excluded Domain Names

Even while the DNS Enforce Plugin is actively enforcing HTTP-based actions, you may want to allow access to certain corporate or other business essential internet sites. This can be performed by creating a whitelist of DNS redirect exceptions.

Exceptions must be defined as absolute, fully qualified domain names (FQDN), specifying all domain levels of the address.

You can use regular expressions to more easily manage the whitelist by implicitly including many sites or subdomains. To use a regular expression in the FQDN, select the **RegExp** checkbox. If selected, all characters entered will be evaluated according to regular expression syntax. Otherwise, only addresses that explicitly match the string will be excluded.

🗎 *The DNS Enforce Plugin list of excluded domain names is independent from the general HTTP Redirect Exceptions list. Values defined in one list do not automatically appear in the other. These lists should be up-to-date and configured appropriately according to your network setup and requirements. See the section on HTTP Preferences in the* Forescout Administration Guide *for more information. See Additional Forescout Documentation for information about how to access the guide.*

Verify That the Plugin Is Running

After configuring the plugin, verify that it 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.

Core Extensions Module Information

The DNS Enforce 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
Cloud Uploader
DHCP Classifier Plugin
Dashboards Plugin
Data Publisher
Data Receiver
Device Classification Engine
Device Data Publisher
DNS Client Plugin
DNS Enforce Plugin
DNS Query Extension Plugin
External Classifier Plugin
Flow Analyzer Plugin
Flow Collector
IOC Scanner Plugin
IoT Posture Assessment Engine
NBT Scanner Plugin
Packet Engine
Reports Plugin
Syslog Plugin
Technical Support Plugin
Web Client Plugin

The Core Extensions Module is a Forescout Base Module. Base Modules are delivered with each Forescout release. Upgrading the Forescout version or performing a clean installation installs this module automatically.

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 Technical Documentation Page, and from 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 Support Portal

🗎 *Software downloads are also available from these portals.*

To identify your licensing mode:

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

Technical Documentation Page

The Forescout Technical Documentation page provides a link to the searchable, web-based Documentation Portal, as well as links to a wide range of Forescout technical documentation in PDF format.

To access the Technical Documentation page:

- Go to https://www.Forescout.com/company/technical-documentation/

Product Updates Portal

The Product Updates Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend Modules. The portal also provides 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 Support Portal

The Downloads page on the Forescout Customer Support Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend Modules. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Customer Support 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.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

Forescout Help Tools

You can access individual documents, as well as the Documentation Portal, directly from the Forescout Console.

Console Help Buttons

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

Forescout Administration Guide

- Select **Administration Guide** from the **Help** menu.

Plugin Help Files

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

Content Module, eyeSegment Module, and eyeExtend Module Help Files

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

Documentation Portal

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