



# ForeScout

## Core Extensions Module: Packet Engine

### Configuration Guide

**Version 8.2**



## 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](mailto:documentation@forescout.com)

## Legal Notice

© 2020 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.

2020-02-26 15:52

## Table of Contents

<b>About the Packet Engine .....</b>	<b>4</b>
How It Works.....	5
<b>Requirements.....</b>	<b>6</b>
<b>Packet Engine Commands .....</b>	<b>6</b>
<b>Packet Engine Status.....</b>	<b>6</b>
<b>Configuration .....</b>	<b>7</b>
Ensure That the Component Is Running .....	8
<b>Performance Optimization.....</b>	<b>8</b>
Physical Appliances.....	8
Virtual Appliances.....	8
Endpoint Discovery.....	9
Host Properties .....	9
Packet Engine Rule Optimization .....	9
Packet Engine Rule Limitation .....	11
Number of Ranges in Each Packet Engine Rule .....	12
Outgoing Load Balancing.....	13
SPAN Configuration on Cisco Switches .....	13
RSPAN Configuration on Cisco Switches .....	13
RSPAN Support .....	14
<b>Packet Engine Considerations .....</b>	<b>14</b>
Network Configuration .....	14
Virtual Appliances.....	14
Policy Actions.....	14
IPv6 Endpoints.....	15
Deep Packet Inspection (DPI) .....	15
Ports for DICOM Parsing.....	15
Resources Required for DICOM Parsing .....	16
Control and Provisioning of Wireless Access Points (CAPWAP) .....	16
Packet Engine and CAPWAP Support .....	16
Requirements for CAPWAP Support.....	16
Enable the CAPWAP Parser .....	17
Disable the CAPWAP Parser .....	17
Verification Tools.....	17
<b>Core Extensions Module Information .....</b>	<b>18</b>
<b>Additional Forescout Documentation.....</b>	<b>18</b>
Documentation Downloads .....	18
Documentation Portal .....	19
Forescout Help Tools.....	19

## About the Packet Engine

The Packet Engine is a component of the Forescout Core Extensions Module. See [Core Extensions Module Information](#) for details about the module.

The Packet Engine provides unprecedented network visibility using real-time port mirroring in the network. Port mirroring – known in Cisco networks as Switched Port Analyzer (SPAN) configuration and in 3COM networks as Roving Analysis Port (RAP) configuration – allows the Forescout platform to directly monitor traffic in the network. This supplements other methods and sources – such as the Flow Collector, the Switch Plugin, the DHCP Classifier Plugin, and the DNS Plugin – that is used to learn information from the network.

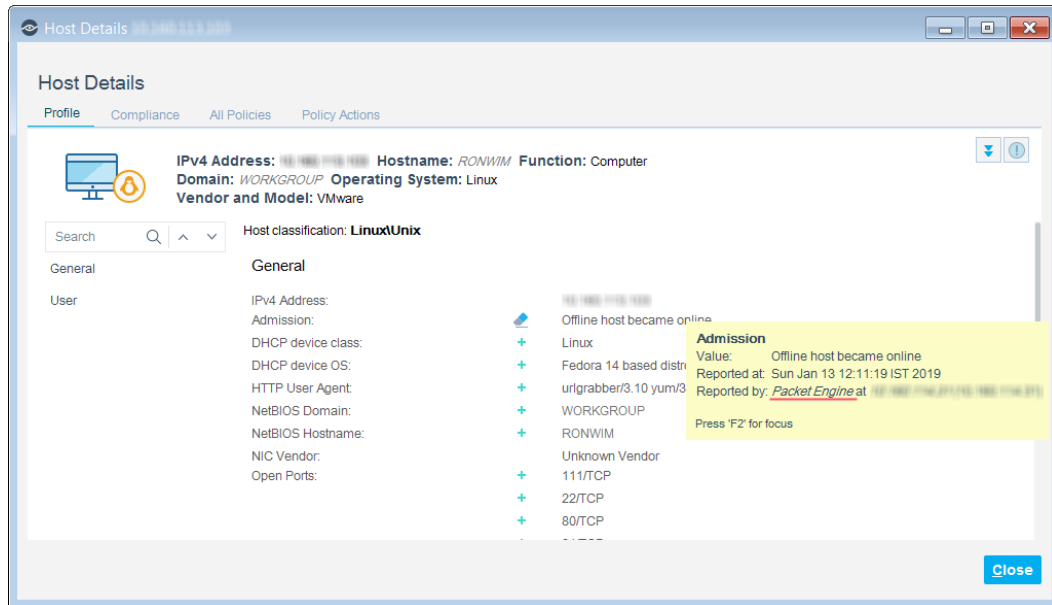
 *The Packet Engine does not support ERSPAN (Encapsulated Remote SPAN).*

The synergistic use of port mirroring and other real time/low latency data sources provides the following advantages:

- Endpoint discovery from first communication on the network
- Detection of authentication and client/server sessions from the first query
- Passive learning of configuration settings and other endpoint properties
- Detection of NAT behavior, spoofing, port scanning, and other suspicious or malicious behavior patterns (for IPv4 addresses only)
- Network management using messages injected into the data stream via the mirror port, such as for virtual firewall enforcement (for IPv4 addresses only) and HTTP session redirection

The Packet Engine parses and analyzes mirrored traffic data packets for:

- Network traffic monitoring
- Endpoint discovery
- Endpoint property evaluation
- Traffic data accumulation for the Segmentation Manager connectivity matrix (if the eyeSegment Module is installed)



## How It Works

Information reported to Forescout eyeSight based on parsed traffic is stored as *host properties*. Host property values are displayed in Console views, and can be evaluated and examined by policies to trigger *actions* that restrict network access or manage/remediate endpoints.

To parse traffic in the different layers, the Packet Engine contains different parsers for common network protocols. Among these are:

- ARP
- CAPWAP
- DCE/RPC
- DHCP - the Packet Engine detects hosts that act as DHCP servers and DHCP relays
- DICOM
- HTTP
- NetBIOS/SMB

The Packet Engine parses most session-based protocol messaging to detect sessions as they are established, and to determine which entity acts as client and which acts as server.

For NAT detection, the Packet Engine leverages both passive traffic monitoring and the ability to send responses. Typical methods implemented by the Packet Engine include detection of behavior patterns such as port scanning, and injection of test messages similar to Nmap diagnostics.

The Packet Engine listens to HTTP traffic and notes the user agent header in HTTP requests. Based on defined translation rules, the user agent is used to resolve the value of the Network Function property.

The Packet Engine passively listens to SMB traffic. It determines the value of the Network Function property based on unique signatures in the traffic. This is useful for determining Windows Machine devices.

The Packet Engine performs passive fingerprinting of the SYN and SYN-ACK packets.

The Packet Engine resolves several endpoint properties, including:

- Traffic seen
- Host is Online
- HTTP User Agent (for IPv4 addresses only)
- Open Ports (for IPv4 addresses only)
- Network Function
- Admission
- Mac Address
- ARP Spoofing
- Sessions as Client (for IPv4 addresses only, and only resolved when used in a policy)
- Sessions as Server (for IPv4 addresses only, and only resolved when used in a policy)

## Requirements

This version of the Packet Engine requires the following Forescout release:

- Forescout version 8.2

## Packet Engine Commands

You can customize certain Packet Engine features, including default parser ports.

**To see the commands available for retrieving conf\_params:**

- Log in to the CounterACT device through the command-line interface (CLI) and run the following command:

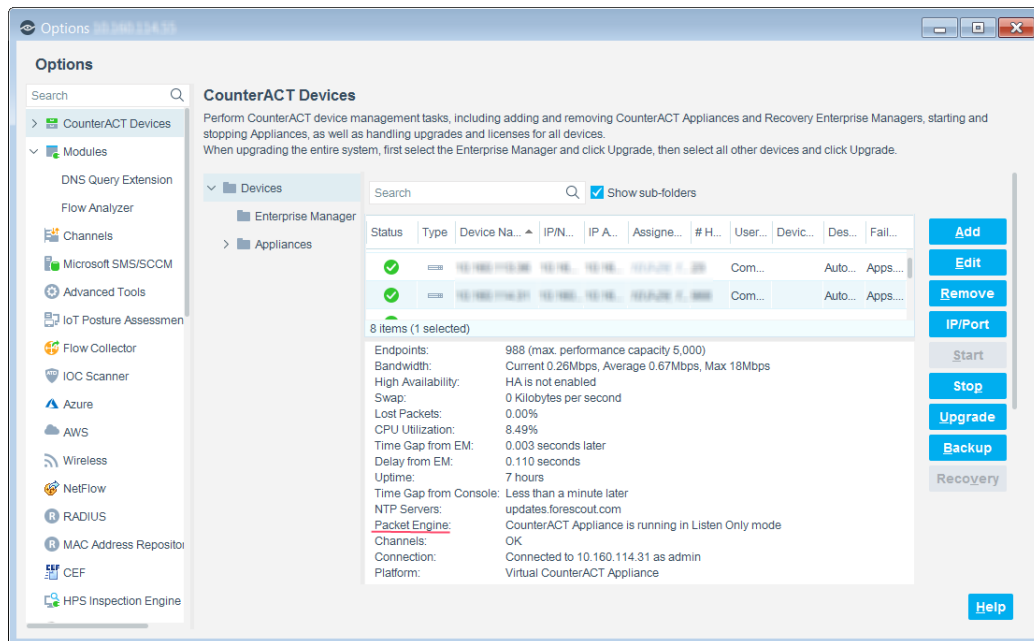
```
fstool pe help
```

## Packet Engine Status

**To view the Packet Engine status on an Appliance:**

1. Select **Tools > Options > CounterACT Devices**.

2. Select the Appliance. The Packet Engine status is included in the Appliance health information.



For information about the Packet Engine detailed status (ctDeviceEngine) in the SNMP MIB table, refer to the Forescout Administration Guide.

## Configuration

Refer to the *Forescout Administration Guide* for information about Packet Engine features, including:




- Per Appliance channel assignments
- Threat protection
- Legitimate scan
- Internal network vs. active response range
- Virtual Firewall action blocking rules
- HTTP actions:
  - HTTP Login
  - HTTP Sign Out
  - HTTP Localhost Login
  - HTTP Notification
  - HTTP Redirection to URL

📄 *When an IPv4 address is merged with an IPv6 address, an HTTP action that was applied to the IPv4 address replaces the HTTP action that was applied to the IPv6 address.*

## Ensure That the Component Is Running

After installing the component (and configuring it, if necessary), ensure that it is running.

### To verify:

1. Select **Tools > Options > Modules**.
2. Navigate to the component and hover over the name to view a tooltip indicating if it is running on Forescout devices in your deployment. In addition, next to the component name, you will see one of the following icons:
  -  - The component is stopped on all Forescout devices.
  -  - The component is stopped on some Forescout devices.
  -  - The component is running on all Forescout devices.
3. If the component is not running, select **Start**, and then select the relevant Forescout devices.
4. Select **OK**.

## Performance Optimization

For improved Packet Engine speed, follow these recommendations.

### Physical Appliances

Configure one or two 10Gb monitor ports in each physical Appliance that monitors traffic.

When an Appliance uses more than two monitor ports:

- Ensure that an even number of monitor ports is used.
- Do not mix interface types, such as a 1Gb network adapter together with a 10Gb network adapter.

### Virtual Appliances

When using Virtual Appliances:


- On VMWare, the VMXNET3 adapter type is preferred over the E1000 adapter type.
- Hyper-V Windows 2016 is preferable to Windows 2012.



## Endpoint Discovery

The host MAC address is not learned from ARP reply packets, but rather from ARP requests only. Use the following command to enable learning the MAC address from ARP reply packets:


```
fstool pe set_conf_param LearnEventMacReplyChangesOnly 0
```

 All `fstool pe set_conf_param` commands must be followed by a restart for the Packet Engine daemon: `fstool engine kill`

## Host Properties

By default, the Packet Engine learns Open Ports from a connection's packets, including reset packets. Use the following command to disable learning from reset packets:

```
fstool pe set_conf_param DontLearnFromReset 1
```

 All `fstool pe set_conf_param` commands must be followed by a restart for the Packet Engine daemon: `fstool engine kill`

## Packet Engine Rule Optimization

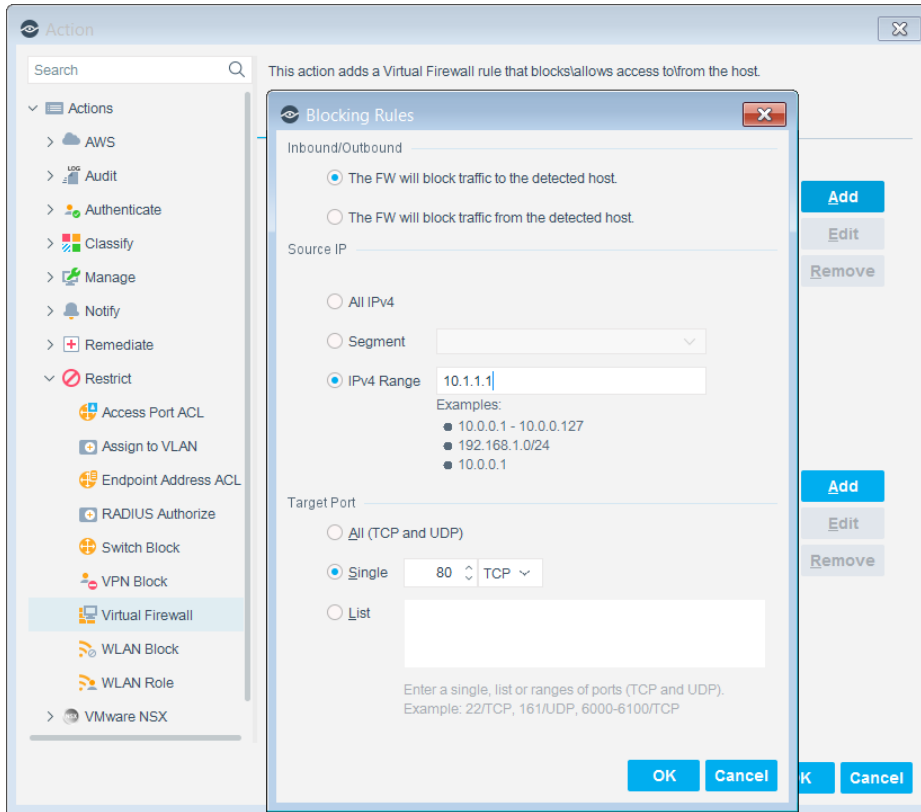
The Packet Engine uses *rules* that are different from standard Forescout policy rules. Each Packet Engine rule instructs the Forescout platform to carry out an action or to resolve a property.

There are four types of Packet Engine rules:

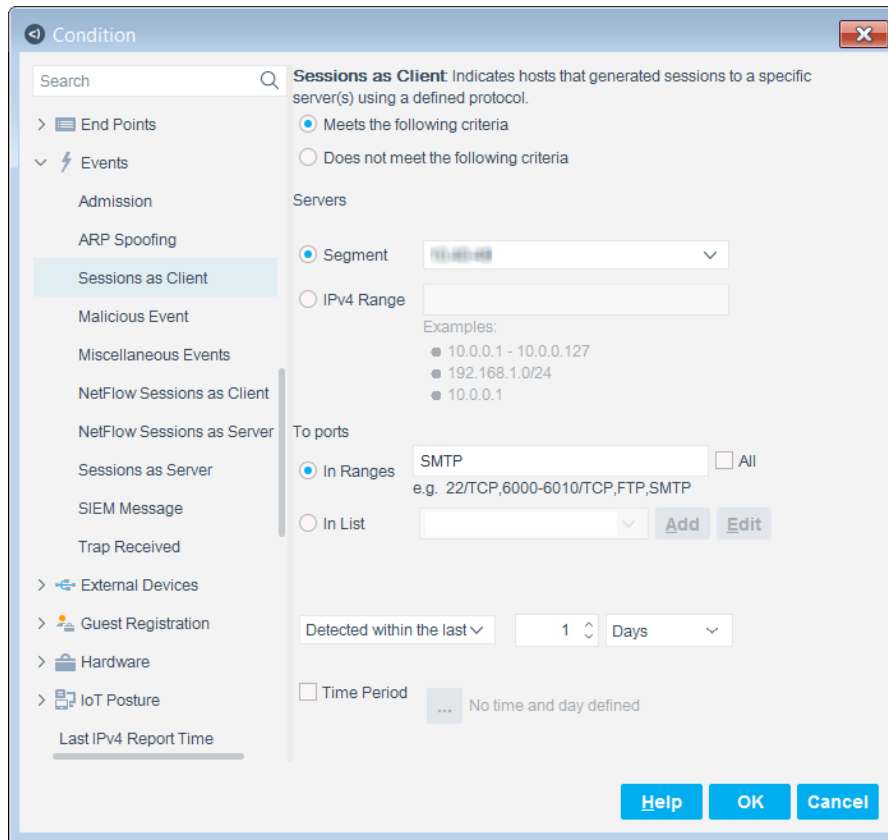
- **Virtual Firewall** rules can be defined statically at the **Tools > Options > Virtual Firewall** pane, or dynamically via a policy. These rules apply Virtual Firewall actions.
- **Sessions as Server/Client** rules can be defined dynamically via a policy. These rules resolve Sessions as Server/Client properties.
- **Legitimate Scan** rules can be defined statically at the **Tools > Options > Threat Protection > Legitimate Scan** pane. These rules apply Legitimate Scan threat protection actions.
- **HTTP redirection exception** rules can be defined statically at the **Tools > Options > NAC > HTTP Redirection** pane, or dynamically via a policy. These rules apply exceptions to HTTP redirection actions.

Examples of Packet Engine rules:

- A Virtual Firewall action to block all HTTP traffic to a specific server



- A Session as Client policy condition to identify all SMTP clients in a segment



Consider the following Packet Engine rule performance guidelines.

- [Packet Engine Rule Limitation](#)
- [Number of Ranges in Each Packet Engine Rule](#)

## Packet Engine Rule Limitation

The number of rules that the Packet Engine holds in its memory can dramatically impact performance. ***It is recommended to run no more than 100,000 Packet Engine rules per Appliance for each of the following:***

- 'Virtual Firewall' actions
- 'Sessions as Server/Client' conditions
- 'Legitimate Scan' rules
- Exceptions to HTTP redirection actions

You can use `fstool` commands to determine how many Packet Engine rules are in the system.

- `fstool pe check_rules -e`

Each of the **Total Rules in Rulebase** fields shows the number of rules that are currently loaded into the Packet Engine for the rule type. Ensure that the number in each of these fields does not exceed 100,000.

📄 *Use this command only when the Packet Engine is running.*

- **fstool pe check\_rules**

Each of the **Number of rules** fields shows the number of rules for the rule type that the Packet Engine will enforce after it is reloaded. Ensure that the number in each of these fields does not exceed 100,000.

📄 *Ignore the **Number of rules in Container** and **Number of rules in Hash** fields.*

## Number of Ranges in Each Packet Engine Rule

Forescout rules are translated to one or more Packet Engine rules, depending on the policy scope. The number of Packet Engine rules that are created depends on the following rule parameters:

- IP addresses in the policy scope – Only Sessions as Server/Client rule type
- Source or target ranges –All rule types
- Port ranges –All rule types

It is recommended to minimize the number of effective ranges within all rule parameters. For example, it is preferable for a parameter to have 8 different ranges than for it to have 40 different ranges.

Perform the following best practices:

- Combine different ranges into a single continuous range.
- If a rule parameter must include many more than 10 different ranges, divide it into two or more different rules.

### Minimal Items in One of the Rule Parameters

Ensure that at least one rule parameter in each Packet Engine rule includes *less than 10* items. The following examples are acceptable because one of the parameters includes only one or two items:

- Policy Scope: 10.1.1.1,40.1.1.4      To: segment-HQ      Port Range: 1-1024
- Policy Scope: segment-HR      To: segment-HQ      Port Range: 80

📄 *If it is not feasible to limit any of the rule parameters to less than 10, contact Forescout support for additional solutions.*

### Packet Engine Rules Generated by 'Virtual Firewall' Actions

When using the Virtual Firewall action in a policy, each matched endpoint generates a separate Packet Engine rule. To minimize the number of Packet Engine rules generated:

- Narrow the policy scope as much as possible.
- Define precise policy conditions for Virtual Firewall actions.

## Packet Engine Rules Generated by 'Sessions as Server/Client' Conditions

Each time a Sessions as Server/Client condition is used in a policy, the number of Packet Engine rules generated depends on the complexity of the ranges or segments specified in the condition.

## Outgoing Load Balancing

To help prevent bottlenecks that can cause outgoing Packet Engine rule packets to be dropped, follow these recommendations.

- In a Layer 2 multi-channel network, use a different response Ethernet interface for each channel setting.
- In a Layer 3 multi-channel network, define each Appliance's routing table to send response packets for different subnets over different Ethernet interfaces.

## SPAN Configuration on Cisco Switches

For information about configuring port mirroring on Cisco switches, refer to the following documents:

- *Configuring the Catalyst Switched Port Analyzer (SPAN)*, available from Cisco.
- "Setting Up Switch Connections" guidelines in the *Forescout Installation Guide's* Network Setup chapter. To access the guide, see [Additional Forescout Documentation](#).

## RSPAN Configuration on Cisco Switches

Remote Switched Port Analyzer (RSPAN) is Cisco technology that lets you mirror traffic from a *source* (an interface or VLAN associated with a specified switch) onto a *destination* VLAN which is used exclusively for this purpose. You can then monitor that mirrored traffic on the target VLAN switch.

RSPAN is useful when you want to monitor traffic on a downlink switch. This is often the case in OT/ICS environments. Many devices at the lower levels of Purdue Enterprise Reference Architecture (PERA) rarely engage with traffic that must be routed. In these cases, Forescout eyeSight misses the opportunity to monitor the traffic that passes only between endpoints on the same switch. RSPAN mirrors the VLAN and analyses the mirrored traffic.

This allows Forescout products to be deployed centrally, in a local environment, and still receive mirrored traffic that would otherwise not be detected. RSPAN provides an additional discovery method as well as traffic analysis.

Configuration is done on the Cisco switches. For more information see [SPAN Configuration on Cisco Switches](#).

### Important Considerations

- Select **Tools > Options > Channels > Edit Channel > Advanced**, and ensure that **Advanced VLAN Options** is set to **Untagged**. For more information on Channel configuration, refer to the *Working with Appliance Channel Assignments* section in the *Forescout Administration Guide*.
- It is recommended to configure RSPAN VLANs on switch trunk ports only.
- Devices are often stripped of their MAC addresses in RSPAN VLANs.
- Ensure that the RSPAN VLAN does not exceed the WAN. This could significantly increase bandwidth utilization.
- **If you are using a virtual CounterACT Appliance**, ensure that the RSPAN configuration does not terminate the mirroring session on an intermediate switch before it reaches the virtual switch that the CounterACT Appliance is connected to.

### RSPAN Support

- Forescout *eyeSight* supports RSPAN and uses it for discovery and endpoint traffic analysis purposes.
- Forescout *eyeControl* does not support RSPAN and cannot use it for enforcement purposes.

## Packet Engine Considerations

Consider the following Packet Engine behaviors.

### Network Configuration

Whenever channel definition interfaces are reconfigured, an Appliance reboot is required.

### Virtual Appliances

Hyper-V affinity configuration is not supported.

### Policy Actions

- Each Appliance can support up to 200 hijack actions per minute.
- Virtual Firewall is not an inline router. As a result:
  - The effectiveness of restrict actions depends on the proximity of the Appliance to the client or server being restricted.
  - UDP traffic blocking is not guaranteed per packet.

- By default, the Virtual Firewall restrict action is session-based. Use the following command to configure it as packet-based:  
`fstool pe set_conf_param packetBaseBlocking 1`
  - 📖 All `fstool pe set_conf_param` commands must be followed by a restart for the Packet Engine daemon: `fstool engine kill`
- *Partial Enforcement* mode is recommended for evaluation purposes only. This mode lets you monitor network traffic, but it limits your ability to respond to it. Specifically, the Threat Protection, HTTP Actions, and Virtual Firewall options are disabled in this mode.
  - 📖 *Host profiles in the Console do not indicate that these actions are not run.*

## IPv6 Endpoints

The following features are not supported for IPv6 endpoints:

- Virtual Firewall
- Threat protection

## Deep Packet Inspection (DPI)

### Ports for DICOM Parsing

DICOM protocol inspection is supported on TCP only. The Packet Engine is hard-coded to use this feature on port 11112. By default, the DICOM parser works also on the following TCP ports:


- 104
- 4000
- 4006
- 4100
- 7100
- 12000
- 12200

Use the following commands to configure DICOM parsing to apply to additional TCP ports:

- Get value command:  
`fstool pe get_conf_param Plugin_Extra_Ports_dicom`
- Set value command:  
`fstool pe set_conf_param Plugin_Extra_Ports_dicom {comma-separated list of all ports to support this feature, not including the hard-coded port}`

For example, if you want to add ports 4242 and 4444 to the list of TCP ports that support DICOM parsing, use the following command:

```
fstool pe set_conf_param Plugin_Extra_Ports_dicom  
104,4000,4006,4100,7100,12000,12200,4242,4444
```

 All `fstool pe set_conf_param` commands must be followed by a restart for the Packet Engine daemon: `fstool engine kill`

## Resources Required for DICOM Parsing

When heavy DICOM traffic consumes almost all of an Appliance's maximum traffic monitoring rate, other features, such as endpoint and switch management, might slow.

## Control and Provisioning of Wireless Access Points (CAPWAP)

CAPWAP networking protocol enables a central wireless LAN Controller (WLC) to manage a collection of wireless access points (APs), and it encapsulates the traffic data for the devices connected to the APs. CAPWAP runs on UDP port 5246 for control, and port 5247 for data.

### Packet Engine and CAPWAP Support

The Packet Engine uses two ports for CAPWAP data:

- 5247
- 5248 for CAPWAP multicast data

#### Limitations

The Packet Engine does not support encrypted CAPWAP (DTLS).

The Packet Engine does not parse CAPWAP control information.

### Requirements for CAPWAP Support

- The Forescout Appliance must be connected to the switch SPAN port used for communication between the APs and the WLC.
- The SPAN port channel must be configured on the connected Appliance.
- For encapsulated traffic to be detected, the IP addresses of the following devices must be configured in the internal network and assigned to the connected Appliance:
  - the AP
  - the WLC
  - the host that sent the data through the tunnel



## Enable the CAPWAP Parser

The CAPWAP parser is enabled by default.

### To enable the CAPWAP parser:

1. On the connected Appliance, run:  

```
fstool pe capwap enable
```
2. Run the following to restart the packet engine:  

```
fstool engine kill
```

## Disable the CAPWAP Parser

### To disable the CAPWAP parser:

1. On the connected Appliance, run:  

```
fstool pe capwap disable
```
2. Run the following to restart the packet engine:  

```
fstool engine kill
```

## Verification Tools

Use fstool commands to verify that CAPWAP is able to encapsulate the traffic data for the devices connected to the APs.

### To verify that CAPWAP data is being parsed:

1. Verify that the CAPWAP parser is enabled. On the connected Appliance, run:  

```
fstool pe get_conf_param UseCapwapPlugin
```

  - If the CAPWAP parser is enabled, the result is:  


```
UseCapwapPlugin | 1 | 1 | set by fstool pe
```
  - If the CAPWAP parser is disabled, the result is:  

```
UseCapwapPlugin | 0 | 0 | set by fstool pe
```
2. Identify which ports are enabled for CAPWAP. On the connected Appliance, run:  

```
fstool pe get_conf_param Plugin_Extra_Ports_capwap
```

  - The enabled ports are displayed:  

```
Plugin_Extra_Ports_capwap | 5247/udp,5248/udp | 5247/udp,5248/udp  
| Enable Capwap ports
```

 *Ports can be enabled for CAPWAP even when the CAPWAP parser is disabled.*
3. Verify that the traffic on the CAPWAP ports is not filtered. On the connected Appliance, run:  

```
fstool pe get_conf_param FilteringIgnorePorts
```

- If the CAPWAP parser is enabled and its ports are not filtered, the CAPWAP ports identified in step [2](#) are included in the result. For example:  
`FilteringIgnorePorts | 67/udp,547/udp,5247/udp,5248/udp | 67/udp,547/udp,5247/udp,5248/udp | Ports ignore list (e.g. 67/udp,3124/tcp,8080/tcp)`
- If the CAPWAP parser is disabled or if its ports are filtered, the CAPWAP ports identified in step [2](#) are *not* included in the result. For example:  
`FilteringIgnorePorts | 67/udp,547/udp | 67/udp,547/udp | Ports ignore list (e.g. 67/udp,3124/tcp,8080/tcp)`

## Core Extensions Module Information

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	Device Data Publisher	IoT Posture Assessment Engine
CEF Plugin	DNS Client Plugin	
Cloud Uploader	DNS Enforce Plugin	NBT Scanner Plugin
DHCP Classifier Plugin	DNS Query Extension Plugin	Packet Engine
Dashboards Plugin	External Classifier Plugin	Reports Plugin
Data Publisher	Flow Analyzer Plugin	Syslog Plugin
Data Receiver	Flow Collector	Technical Support Plugin
Device Classification Engine	IOC Scanner 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 [Forescout Technical Documentation Page](#), and 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**.

### Forescout Technical Documentation Page

The Forescout Technical Documentation Page provides access to a searchable, web-based [Documentation Portal](#) as well as PDF links to the full range of technical documentation.

**To access the Technical Documentation Page:**

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

### 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 Support Portal

The Downloads page on the Forescout Customer Support 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 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/](https://updates.forescout.com/support/files/counteract/docs_portal/)

### 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 **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**.

***Documentation Portal***

- Select **Documentation Portal** from the **Help** menu to access the [Documentation Portal](#).