

## About the 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	Dashboard Plugin
DHCP Classifier Plugin	DNS Client Plugin	DNS Enforce Plugin
DNS Query Extension Plugin	Device Classification Engine	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. This module is automatically installed when you upgrade the ForeScout version or perform a clean installation.

Refer to the relevant configuration guides for detailed information about how to work with and configure components included with this module. See [Additional ForeScout Documentation](#) for information about how to access these guides, and other documentation.

## ForeScout Requirements

This module requires ForeScout version 8.1.1.

Components described in this document may have additional requirements and dependencies.

## About This Release

This section describes updates and important information related to components delivered in this version of the Core Extensions Module.

- [Advanced Tools Plugin 2.3](#)
- [CEF Plugin 2.8](#)
- [Dashboard Plugin 1.1.1](#)
- [Device Classification Engine 1.3](#)
- [DHCP Classifier Plugin 2.2](#)
- [DNS Client Plugin 3.2](#)

- [DNS Enforce Plugin 1.3](#)
- [DNS Query Extension Plugin 1.3](#)
- [External Classifier Plugin 2.2.4](#)
- [Flow Analyzer Plugin 1.4.1](#)
- [Flow Collector 1.0](#)
- [IOC Scanner Plugin 2.3](#)
- [IoT Posture Assessment Engine 1.1.2](#)
- [NBT Scanner Plugin 3.1](#)
- [Packet Engine 8.1.1](#)
- [Reports Plugin 5.1](#)
- [Syslog Plugin 3.5](#)
- [Technical Support Plugin 1.2.2](#)
- [Web Client Plugin 1.1.1](#)

This release also includes enhancements and fixes provided in previous releases.

## Advanced Tools Plugin 2.3

There are no fixed issues for this release.

### Requirements

- Endpoint Module version 1.1 with the HPS Inspection Engine running
- (Flexx licensing) A valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the plugin/component. If you do not have this license, these actions will be disabled in the Console. Refer to the *ForeScout Flexx Licensing How-to Guide* for more information about managing Flexx licenses and how to request/purchase this license.

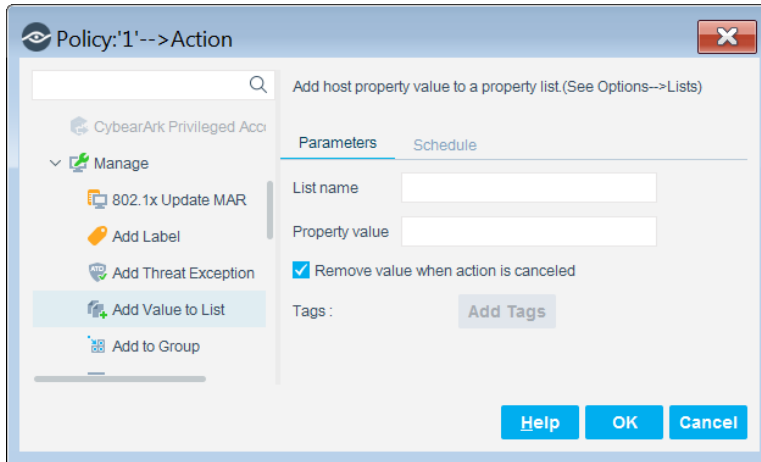
### Feature Enhancements

This section describes feature enhancements for this release.

#### Add Property Values to a List

A new action has been added that helps you work with property values and lists in policies.

Use the Add Value to List action to place property values that match a policy condition into a list. For example, place all logged-in users of hosts at which a malicious event was detected by Forescout 8.1 into a 'Malicious Users' list. You can then use this list to define a policy that performs a restrict action on other hosts where the user logged-in to.



In the **List name** field, enter the name of the list that you want to add the property value to. The list name you enter must match the name of a previously defined list.

In the **Property value** field, use tags to define endpoint-specific property values. Select **Add Tags** to insert data tags that resolve to host property values.

Select the **Remove value when action is canceled** option to remove the value from the list when the action is cancelled (i.e. when the host no longer matches the policy rule).

## CEF Plugin 2.8

There are no fixed issues for this release.

### Requirements

- Target SIEM servers must parse CEF messages.
- Target SIEM servers must be able to receive messages from CounterACT Appliances and Enterprise Managers.

### Feature Enhancements

This release supports Certification Compliance mode. For information about this mode, refer to the *ForeScout Installation Guide*.

## Dashboard Plugin 1.1.1

The Dashboard Plugin delivers the **Dashboard** application that ForeScout users access through the **ForeScout Web Client**. See [Web Client Plugin 1.1.1](#).

### Feature Enhancements

#### UI Enhancements

The following GUI improvements have been made in the dashboard drill-down view:

- The discovery bar was removed
- The widget title is now the page title
- The widget border was removed
- A border now surrounds the Host List pane and Host Details pane
- The Host List and the Host Details are now the full page height

Track to WG-464

## Device Classification Engine 1.3

There are no feature enhancements or fixed issues for this release.

### Known Issues

This section describes known issues for this release.

Issue	Description
<b>DPL-597</b>	<p>It is not recommended to perform Set Classification actions after a new Device Profile Library version is installed and before it is applied or rolled back. If these actions are performed:</p> <ul style="list-style-type: none"> <li>▪ They are displayed together with the pending classification changes.</li> <li>▪ Their Set Classification action status is listed as Success.</li> <li>▪ They will not take effect until the new library version is applied or rolled back.</li> </ul>

## DHCP Classifier Plugin 2.2

There are no fixed issues for this release.

### Requirements

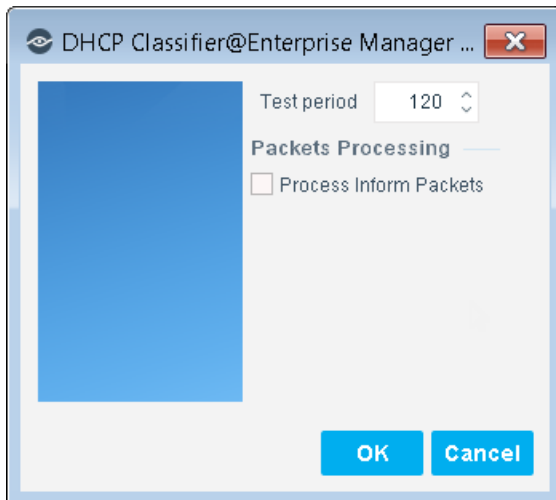
- Endpoint Module version 1.1 with the HPS Inspection Engine running. The DHCP Classifier Plugin relies on information from *Primary Classification* templates and policies provided by the HPS Inspection Engine.
- The endpoint (computer or any other network-aware device) must be configured to send a DHCP broadcast query requesting necessary information to a DHCP server.
- For endpoint DHCP classification, the DHCP Classifier Plugin must be running on a CounterACT device capable of receiving the DHCP client requests from traffic inspection or explicit message forwarding.

### Feature Enhancements

This section describes feature enhancements for this release.

### Process Inform Packets Configuration Option

**Process Inform Packets** is a new check-box option in the plugin configuration. When this checkbox is selected, DHCP *Inform* messages are also parsed by the DHCP Classifier Plugin.



## DNS Client Plugin 3.2

There are no feature enhancements or fixed issues for this release.

## DNS Enforce Plugin 1.3

There are no feature enhancements or fixed issues for this release.

### Requirements

- Endpoint Module version 1.1 with the HPS Inspection Engine running.
- The plugin-specified Target IP address must be defined in the DHCP server as the primary DNS server.

## DNS Query Extension Plugin 1.3

There are no feature enhancements or fixed issues for this release.

## External Classifier Plugin 2.2.4

There are no feature enhancements or fixed issues for this release.

## Requirements

- Files and query results must contain MAC addresses in the following format:  
XX:XX:XX:XX:XX:XX  
Where X is any one of the following characters: 0-9, A-F (case insensitive).

## Flow Analyzer Plugin 1.4.1

There are no feature enhancements or fixed issues for this release.

## Requirements

- It is recommended to have the Forescout Flow Collector installed and running

## Flow Collector 1.0

This section describes the new Flow Collector, version 1.0.

Flow Collector version 1.0 is installed with Forescout 8.1, but it is disabled by default. After it is enabled, it produces session data that can be accessed by other components.

The Flow Collector analyzes the traffic flows exported by network devices, such as switches, firewalls, and routers. It reports flow session data that is used to resolve endpoint properties and that can be used to map visualized traffic patterns. The flow session data can also be used by other Forescout modules.

The Flow Collector can detect endpoints or endpoint property values that the Forescout Packet Engine might not learn. This capability is relevant in large scale deployments where the Packet Engine is limited in its ability to detect activity in remote sites and branch offices. Use of the information reported by the Flow Collector improves visibility and speeds detection of new endpoints.

## Requirements

This section describes requirements for this component.

### Supported Flow Protocols

The Flow Collector supports the following protocols, with or without Flexible NetFlow technology:

- NetFlow v9
- IPFIX
- sFlow

### Networking Requirements

Enable the flow protocol on Layer 3 network devices in the network segments of interest. Flow exporting network devices that are in these segments must be configured to report flow data to the CounterACT device that monitors the segment.

### Port Availability

To support flow data communication to Forescout 8.1:

- Ensure that the communication ports are open on enterprise firewalls.
- Define exceptions for these ports in the Virtual Firewall action.

You can configure the Flow Collector port assignments. By default, the flow exporting network devices use the following ports to communicate with the Flow Collector.

- For NetFlow v9: port 4729 UDP
- For IPFIX: port 4739 UDP
- For sFlow: port 6343 UDP

### Integrate with or Replace the Legacy NetFlow Plugin

With the introduction of the Forescout Flow Collector, the legacy NetFlow Plugin has been deprecated. The Flow Collector provides more accurate and stable traffic flow detection and more scalable bandwidth capabilities than the NetFlow Plugin. For networks running the NetFlow Plugin with flow protocol higher than v5, it is recommended to configure and enable the Flow Collector, and then stop and uninstall the NetFlow Plugin. If your network uses NetFlow v5, do not replace the NetFlow Plugin with the Flow Collector until your network is upgraded to a newer flow protocol.

If both plugins run concurrently, ensure that the **Port for NetFlow communication** field in the NetFlow Plugin configuration does not contain any of the ports used by the Flow Collector. By default, these are ports 4729, 4739 and 6343.

## IOC Scanner Plugin 2.3

There are no fixed issues for this release.

### Requirements

- Endpoint Module version 1.1 with the HPS Inspection Engine running.
- Core Extensions Module 1.1 with the DNS Query Extension Plugin running.
- (Flexx licensing) A valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the plugin/component. If you do not have this license, these actions will be disabled in the Console. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses and how to request/purchase this license.

### Feature Enhancements

This release supports Certification Compliance mode. For information about this mode, refer to the *Forescout Installation Guide*.

## IoT Posture Assessment Engine 1.1.2

There are no feature enhancements for this release.

### Requirements

- IoT Posture Assessment Library. This is a Content Module that delivers a library of pre-defined login credentials that are used by the IoT Posture Assessment Engine to aid in determining the security risk of devices. The IoT Posture Assessment Library is upgraded periodically to increase the breadth of the devices for which factory default credentials are known and to update the list of commonly used credentials. Install the latest version of the IoT Posture Assessment Library to take advantage of the most current updates.

### Fixed Issues

This section describes fixed issues for this release.

Issue	Description
PA-115	Fixed a possible false positive result for an SSH scan in which the implementation of the SSH server does not follow the SSH protocol specification.

## NBT Scanner Plugin 3.1

There are no feature enhancements for this release.

### Fixed Issues

For information about the following fixed issues from the recently released NBT Scanner Plugin hotfixes that are incorporated into this plugin version, refer to the following:

- Hotfix 3.0.6.1:
  - NBT-90

<https://forescout.force.com/support/s/article/NBT-Scanner-HF-3-0-6-1xxx-Builds>


## Packet Engine 8.1.1

The Packet Engine was a built-in component of CounterACT. Beginning with release v8.1, it is an independent plugin.

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 Forescout 8.1 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 ForeScout 8.1 uses to learn information from the network.

 *The Packet Engine does not support RSPAN (Remote SPAN) or 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 and HTTP session redirection (for IPv4 addresses only)

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)

## Feature Enhancements

### UI Enhancement

The **Continue** button is no longer displayed in the Login Notification window. If **Auto-redirect on success** is not selected in the Options > NAC > HTTP Redirection window, users must open another tab to continue browsing.

*Track to PE-444.*

### Fixed Issues

This section describes fixed issues for this release.

Issue	Description
<b>PE-497</b>	The Packet Engine sometimes restarted when a device using an IPv6 address tried to connect to an external HTTP server.
<b>PE-500</b>	The Packet Engine sometimes restarted when there were many ARP requests in the internal network.

## Performance Optimization

Refer to the *Core Extensions Module 1.1.0 Release Notes* for information about Packet Engine performance optimization.

## Packet Engine Considerations

Refer to the *Core Extensions Module 1.1.0 Release Notes* for information about Packet Engine considerations.

## Known Issues

This section describes known issues for this release.

Issue	Description
<b>PE-521</b>	When Forescout 8.1 is deployed on KVM virtual systems, the maximum bandwidth of Packet Engine traffic monitoring is 500 Mb/s. If traffic exceeds this amount, virtual firewall functionality and device discovery may be affected.

## Reports Plugin 5.1

There are no feature enhancements or fixed issues for this release.

## Requirements

- JavaScript must be enabled on your browser

## Known Issues

This section describes known issues for this release.

Issue	Description
<b>REP-662</b>	Report generation fails if the report exceeds 5,000 pages. To accommodate longer reports, run the following command from the command line interface: <code>fstool set_property jasper.report.max.report.pages &lt;n&gt;</code> Where <n> is the maximum number of pages required for the report. <b>Note:</b> You do not have to restart the machine after running this command.
<b>REP-662</b>	Generating a very large report might cause memory and PDF download problems.

## Syslog Plugin 3.5

There are no feature enhancements for this release.

## Requirements

There are no additional requirements for this component.

## Fixed Issues

This section describes fixed issues for this release.

Issue	Description
<b>SYS-410</b>	In the <i>IP Address</i> field of the <b>Receive From</b> tab, the plugin accepts a source's FQDN to be a valid entry. However, when the plugin then received a syslog message from that defined source, it erroneously treated the received IP address as an unconfigured source.

## Technical Support Plugin 1.2.2

There are no feature enhancements or fixed issues for this release.

## Web Client Plugin 1.1.1

The Web Client Plugin delivers the **Forescout Web Client** (FWC). The FWC is a presentation framework for accessing Forescout web applications. With this plugin version, the following web applications are available for user access:

- The **Dashboard**. See [Dashboard Plugin 1.1.1](#)

Users access Forescout web applications that are presented within the FWC, either from the Console toolbar or via a web browser > login page.

## Requirements

There are no additional requirements for this component.

## Feature Enhancements

The plugin provides several new fstool commands to control user access to the FWC that results in the control of user access to the Forescout web applications presented within the FWC. Refer to the *Forescout 8.1 Release Notes* for information about these new fstool commands.

## Upgrading the Module


New module releases may become available between Forescout releases. This section describes how to install the module when a new release becomes available.


**To install the module:**

1. Navigate to one of the following Forescout download portals, depending on the licensing mode your deployment is using:
  - [Product Updates Portal](#) - **Per-Appliance Licensing Mode**
  - [Customer Portal, Downloads Page](#) - **Flexx Licensing Mode**

To identify your licensing mode, select **Help > About ForeScout** from the Console.

2. Download the module .fpi file.
3. Save the file to the machine where the Console is installed.
4. Log into the Console and select **Options** from the **Tools** menu.
5. Select **Modules**. The Modules pane opens.
6. Select **Install**. The Open dialog box opens.
7. Browse to and select the saved module .fpi file.
8. Select **Install**. The Installation screen opens.
9. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement, and select **Install**. The installation will not proceed if you do not agree to the license agreement.

 *The installation will begin immediately after selecting Install, and cannot be interrupted or canceled.*

 *In modules that contain more than one component, the installation proceeds automatically one component at a time.*

10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

 *Some components are not automatically started following installation.*

## Module and Component Rollback

The following rollback/upgrade activities are not supported:

- Rolling back this module (or one of its components) to a version released prior to Forescout 8.1.
- If you are running a version of Forescout lower than 8.1 with the corresponding version of this module installed, you cannot upgrade to this module version (or one of its components).

If you upgrade to a newer module or component version that becomes available after this release, you may be able to roll it back. When rollback is supported, the Rollback button is enabled in the Console.

Modules/components on Appliances connected to the Enterprise Manager are rolled back to the selected version. Modules/components on Appliances that are not

connected to the Enterprise Manager during the rollback are rolled back when the Enterprise Manager next reconnects to the Appliances.

**To roll back the module or component:**

1. Select **Options** from the Console **Tools** menu.
2. Navigate to the **Modules** folder.
3. In the Modules pane, select the module or component to be rolled back.
4. Select **Rollback**. A dialog box opens listing the versions to which you can roll back.
5. Select a version and select **OK**. A dialog box opens showing you the rollback progress.

## 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/](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)

## 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](mailto: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.

2019-06-20 18:42