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
- DNS Enforce Plugin
- NBT Scanner Plugin
- CEF Plugin
- DNS Query Extension Plugin
- Packet Engine
- DHCP Classifier Plugin
- External Classifier Plugin
- Reports Plugin
- Dashboard Plugin
- Flow Analyzer Plugin
- Syslog Plugin
- Device Classification Engine
- Flow Collector
- Technical Support Plugin
- DNS Client Plugin
- IOC Scanner 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. Upgrading the Forescout version or performing a clean installation installs this module automatically.

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 8.1.2.

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

About This Release

This section describes updates and important information related to the components delivered in this version of the Core Extensions Module. This release also includes enhancements and fixes provided in previous releases.
The following table identifies the components that are updated in this module version:

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
<th>Features Enhancements</th>
<th>Fixed Issues</th>
<th>Known Issues</th>
<th>Upgrade Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Tools Plugin 2.3.1</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEF Plugin 2.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dashboard Plugin 1.1.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Classification Engine 1.3</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP Classifier Plugin 2.2.1</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Client Plugin 3.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Enforce Plugin 1.3.1</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Query Extension Plugin 1.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>External Classifier Plugin 2.2.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flow Analyzer Plugin 1.4.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flow Collector 1.0</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IOC Scanner Plugin 2.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IoT Posture Assessment Engine 1.1.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NBT Scanner Plugin 3.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packet Engine 8.1.2</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Reports Plugin 5.1.1</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Syslog Plugin 3.5.1</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Only components providing new features/enhancements are released with an updated configuration guide (help) that matches the updated version number of the component.

Advanced Tools Plugin 2.3.1

This section describes updates made to the Advanced Tools Plugin 2.3.1.

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

There are no feature enhancements provided in this version.

Fixed Issues

This section identifies the fixed issues for this version of the Advanced Tools Plugin.

- Merged Hotfixes

Merged Hotfixes

The following, previously released hotfixes are merged into this version of the Advanced Tools Plugin:

<table>
<thead>
<tr>
<th>Hotfix</th>
<th>Fix Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.3.1</td>
<td>Refer to Hotfix 2.2.3.1 Release Notes</td>
</tr>
<tr>
<td>2.2.4.1</td>
<td>Refer to Hotfix 2.2.4.1 Release Notes</td>
</tr>
</tbody>
</table>
CEF Plugin 2.8

*This plugin is not updated and retains its existing version number.*

**Requirements**

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

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.

*This plugin is not updated and retains its existing version number.*

**Requirements**

There are no unique requirements for this plugin.

Device Classification Engine 1.3

*This plugin is not updated and retains its existing version number.*

**Requirements**

- Device Profile Library. This is a Content Module that delivers a library of pre-defined device classification *profiles*, each composed of properties and corresponding values that match a specific device type. The Device Profile Library is upgraded periodically to improve the accuracy and breadth of classification. Install the latest version of the Device Profile Library to take advantage of the most current classifications.

**Known Issues**

This section describes known issues for this version of the Device Classification Engine.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
</table>
| DPL-597 | 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:  
  - They are displayed together with the pending classification changes.  
  - Their Set Classification action status is listed as Success.  
  - They will not take effect until the new library version is applied or rolled back. |
DHCP Classifier Plugin 2.2.1
This section describes updates made to the DHCP Classifier Plugin 2.2.1.

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
There are no feature enhancements provided in this version.

Fixed Issues
This section identifies the fixed issues for this version of the DHCP Classifier Plugin.

- Fixed for This Version

Fixed for This Version
The following issues are newly fixed in this version of the DHCP Classifier Plugin:

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP-167</td>
<td>Policies that included DHCP Classifier properties configured with the condition <em>Matches Any Value</em> failed when an evaluated endpoint was found to contain no property value. The existing policy workaround is to use the condition <em>NOT Matches &quot;none&quot;</em> for evaluating DHCP properties. These properties are now replaced by new DHCP Classifier properties that can be configured with <em>Matches Any Value</em>. For backward compatibility, DHCP Classifier properties such as <em>DHCP device OS</em> have been rewritten as <strong>DHCP Device OS (Obsolete)</strong> with the existing <em>NOT Matches &quot;none&quot;</em> condition maintained. While obsolete properties are still available within policies where they were already in use, new policies can only use the new properties.</td>
</tr>
</tbody>
</table>
DNS Client Plugin 3.2

This plugin is not updated and retains its existing version number.

Requirements

There are no unique requirements for this plugin.

DNS Enforce Plugin 1.3.1

This section describes updates made to the DNS Enforce Plugin 1.3.1.

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.

Feature Enhancements

There are no feature enhancements provided in this version.

Fixed Issues

This section identifies the fixed issues for this version of the DNS Enforce Plugin.

- Merged Hotfixes

Merged Hotfixes

The following, previously released hotfixes are merged into this version of the DNS Enforce Plugin:

<table>
<thead>
<tr>
<th>Hotfix</th>
<th>Fix Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.6.1</td>
<td>Refer to Hotfix 1.1.6.1 Release Notes</td>
</tr>
<tr>
<td>1.2.0.1</td>
<td>Refer to Hotfix 1.2.0.1 Release Notes</td>
</tr>
</tbody>
</table>

DNS Query Extension Plugin 1.3

This plugin is not updated and retains its existing version number.

Requirements

There are no unique requirements for this plugin.
External Classifier Plugin 2.2.4

This plugin is not updated and retains its existing version number.

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

This plugin is not updated and retains its existing version number.

Requirements

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

Flow Collector 1.0

This plugin is not updated and retains its existing version number.

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 system requirements, including:

- Forescout Requirements
- Supported Flow Protocols
- Networking Requirements
- Port Availability

Forescout Requirements

The Flow Collector requires the following Forescout release:

- Forescout version 8.1
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

If the NetFlow Plugin is running, ensure that it is not configured to use any of the ports used by the Flow Collector. Refer to the section on integration or replacement of the NetFlow Plugin in the Core Extensions Module: Flow Collector 1.0 Configuration Guide.

Upgrade Considerations

This section describes upgrade considerations for this release.

Integrate with or Replace the Legacy NetFlow Plugin

With the availability of the Forescout Flow Collector, the legacy NetFlow Plugin is 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

This plugin is not updated and retains its existing version number.

Requirements

- Endpoint Module version 1.1 with the HPS Inspection Engine running
- Core Extensions Module 1.1 with the DNS Query Extension Plugin running

IoT Posture Assessment Engine 1.1.2

This plugin is not updated and retains its existing version number.

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.

NBT Scanner Plugin 3.1

This plugin is not updated and retains its existing version number.

Requirements

There are no unique requirements for this plugin.

Packet Engine 8.1.2

This section describes updates made to the Packet Engine 8.1.2.

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

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

Requirements

There are no unique requirements for this plugin.

Feature Enhancements

There are no feature enhancements provided in this version.
Fixed Issues
This section identifies the fixed issues for this version of the Packet Engine.

- Merged Hotfixes

Merged Hotfixes
The following, previously released hotfixes are merged into this version of the Packet Engine:

<table>
<thead>
<tr>
<th>Hotfix</th>
<th>Fix Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.0.1.2</td>
<td>Refer to <a href="#">Hotfix 8.0.1.2 Release Notes</a></td>
</tr>
</tbody>
</table>

Known Issues
This section describes known issues for this version of the Packet Engine.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PE-521</td>
<td>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.</td>
</tr>
<tr>
<td>PE-644</td>
<td>Even after SecureConnector was successfully installed in Linux endpoints, application of the HTTP Redirection action on these endpoints results in the following erroneous action status Hosts traffic not monitored.</td>
</tr>
</tbody>
</table>

Upgrade Considerations
For efficiency and to prevent packet loss, the following values are now automatically recalculated whenever the Packet Engine restarts:

- number of dispatcher threads
- affinity per thread

If you manually change either of these values after installing or upgrading to Packet Engine 8.1.2, the Packet Engine stops running and the automatic recalculation of these values is disabled.

Reports Plugin 5.1.1
This section describes updates made to the Reports Plugin 5.1.1.

Requirements
- JavaScript must be enabled on your browser

Feature Enhancements
There are no feature enhancements provided in this version.
**Fixed Issues**
This section identifies the fixed issues for this version of the Reports Plugin.

- [Merged Hotfixes](#)

**Merged Hotfixes**
The following, previously released hotfixes are merged into this version of the Reports Plugin:

<table>
<thead>
<tr>
<th>Hotfix</th>
<th>Fix Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.1.1</td>
<td>Refer to <a href="#">Hotfix 5.0.1.1 Release Notes</a></td>
</tr>
<tr>
<td>5.0.1.2</td>
<td>Refer to <a href="#">Hotfix 5.0.1.2 Release Notes</a></td>
</tr>
</tbody>
</table>

**Known Issues**
This section describes known issues for this version of the Reports Plugin.

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

**Syslog Plugin 3.5.1**
This section describes updates made to the Syslog Plugin 3.5.1.

**Requirements**
There are no unique requirements for this plugin.

**Feature Enhancements**
There are no feature enhancements provided in this version.

**Fixed Issues**
This section identifies the fixed issues for this version of the Syslog Plugin.

- [Merged Hotfixes](#)
Merged Hotfixes

The following, previously released hotfixes are merged into this version of the Syslog Plugin:

<table>
<thead>
<tr>
<th>Hotfix</th>
<th>Fix Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2.1.0</td>
<td>Refer to Hotfix 3.2.1.0 Release Notes</td>
</tr>
</tbody>
</table>

Technical Support Plugin 1.2.3

*This plugin is not updated and retains its existing version number.*

Requirements

There are no unique requirements for this plugin.

Web Client Plugin 1.1.1

*This plugin is not updated and retains its existing version number.*

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 unique requirements for this plugin.

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.

**Previous Module Versions**

Installing this module version also installs fixes and enhancements provided in the previous module versions listed in this section. To view Release Notes for previous module versions, see:

https://www.forescout.com/company/resources/core-extensions-module-1-1-1-release-notes/

https://www.forescout.com/company/resources/core-extensions-module-1-1-release-notes/

**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**

Access documentation downloads 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:**

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 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/](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 access information about tasks and topics quickly.

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

**Plugin Help Files**
- After installing the plugin, 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

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.

2019-08-13 14:03