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 a minimum of Forescout version 8.1.

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:

Component	Requirements	Features Enhancements	Fixed Issues	Known Issues	Upgrade Considerations
Advanced Tools Plugin 2.3.1			✓		
CEF Plugin 2.8.1					
Dashboard Plugin 1.1.1					
Device Classification Engine 1.3				✓	
DHCP Classifier Plugin 2.2.2			✓		
DNS Client Plugin 3.2					
DNS Enforce Plugin 1.3.1			✓		
DNS Query Extension Plugin 1.3					
External Classifier Plugin 2.2.4					
Flow Analyzer Plugin 1.4.1					
Flow Collector 1.0.1					✓
IOC Scanner Plugin 2.3					
IoT Posture Assessment Engine 1.1.2					
NBT Scanner Plugin 3.1.1					
Packet Engine 8.1.3			✓	✓	✓
Reports Plugin 5.1.2			✓	✓	
Syslog Plugin 3.5.2			✓		

Component	Requirements	Features Enhancements	Fixed Issues	Known Issues	Upgrade Considerations
Technical Support Plugin 1.2.4					
Web Client Plugin 1.1.1					

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

The Advanced Tools Plugin provides host properties and actions in ForeScout that enhance and extend existing functionality. For example, the plugin provides:

- More detailed endpoint detection
- Enhanced use of commands and scripts to retrieve endpoint information
- Use of labels and counters to implement complex policy logic, and to retain endpoint status across policy rechecks

Requirements

This section describes Forescout requirements for this release. Refer to the module Release Notes for updates regarding these requirements.

- Minimum of Forescout version 8.1.
- Minimum of Endpoint Module version 1.1 with the HPS Inspection Engine running.
- If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the component. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses.

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:

Hot Fix	Fix Content	Up to Version
2.2.3.1	Refer to Hotfix 2.2.3.1 Release Notes	2.2.3.1003
2.2.4.1	Refer to Hotfix 2.2.4.1 Release Notes	2.2.4.1018

CEF Plugin 2.8.1

The CEF Plugin lets the Forescout platform send policy compliance and other host information detected by the Forescout platform to SIEM systems using the CEF messaging format.

In addition, SIEM servers can trigger remediation actions by sending alert messages to the Forescout. This functionality uses the alert messaging function common to most SIEM servers, and non-CEF-standard text messages.

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

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.

- Merged Hotfixes

Merged Hotfixes

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

Hotfix	Fix Content	Up to Version
2.7.0.1	Refer to Hotfix 2.7.0.1 Release Notes	2.7.0.1003
2.8.0.1	Refer to Hotfix 2.8.0.1 Release Notes	2.8.0.1011

Known Issues

There are no known issues in this version.

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.

Issue	Description
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 2.2.2

The DHCP Classifier Plugin extracts host information from DHCP messages. Hosts communicate with DHCP servers to acquire and maintain their network addresses. The Forescout platform extracts host information from DHCP message packets and

uses DHCP fingerprinting to determine the operating system and other host configuration information.

The information retrieved by this plugin complements information sources used by the Forescout platform, such as the HPS Inspection Engine and Nmap queries.

- This plugin lets the Forescout platform retrieve host information when methods such as the Forescout Packet Engine or HPS Nmap scanner are unavailable, or in situations where the Forescout platform cannot monitor all traffic. For example, if traffic in a network segment cannot be monitored directly, a CounterACT appliance on another segment can extract host information based on relayed DHCP messaging.
- This plugin can be used in concert with the above discovery methods to obtain timely, complete host information.
- This plugin reveals DHCP properties that can be used to improve classification of unclassified devices obtained from DHCP-enabled network-connected devices.

Requirements

- Minimum of 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:

Issue	Description
DHCP-185	DHCP-166 created modified DHCP Classifier properties, duplicating them and re-naming the preexisting ones by appending "(Obsolete)" to their names, modifying the copied properties to remove the NULL_VALUE attribute. DHCP-185 adds attribute **SOURCE_DETAILS_DISPLAY** to the "obsolete" properties keeping them from appearing in the console GUI. These issues are related to CA-24143, which modifies the DHCP Classifier properties displayed under the "General" category in the host profile on the console GUI by removing the "obsolete" properties, and adding the new ones created under DHCP-166.

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 plugin is not updated and retains its existing version number.

Requirements

- Minimum of 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:

Hotfix	Fix Content	Up to Version
1.1.6.1	Refer to Hotfix 1.1.6.1 Release Notes	1.1.6.1003
1.2.0.1	Refer to Hotfix 1.2.0.1 Release Notes	1.2.0.1002

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 1.0.1

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:

- Minimum of 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

- Minimum of Endpoint Module version 1.1 with the HPS Inspection Engine running
- Minimum of 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 3.1.1

Requirements

There are no unique requirements for this 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.

- **Error! Reference source not found.**

Merged Hotfixes

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

Hotfix	Fix Content	Up to Version
3.0.4.1	Refer to Hotfix 3.0.4.1 Release Notes	3.4.0.1003
3.0.6.1	Refer to Hotfix 3.0.6.1 Release Notes	3.6.0.1003
3.1.0.1	Refer to Hotfix 3.1.0.1 Release Notes	3.1.0.1013

Packet Engine 8.1.3

This section describes updates made to the Packet Engine 8.1.3.

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
- Fixed for this Version

Merged Hotfixes

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

Hotfix	Fix Content	Up to Version
8.0.1.2	Refer to Hotfix 8.0.1.2 Release Notes	N/A
8.1.2.1	Refer to Hotfix 8.1.2.1 Release Notes	8.1.2.1013

Fixed for This Version

Issue	Description
PE-664	HTTP messages did not include the host key in communication with Counteract.

Known Issues

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

Issue	Description
PE-521	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.
PE-644	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*.
PE-761	The Packet Engine experiences a core dump in the audit trails due to a segmentation fault. This issue is extremely intermittent.

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 8.1.3, the Packet Engine stops running and the automatic recalculation of these values is disabled.

Reports Plugin 5.1.2

This section describes updates made to the Reports Plugin 5.1.2.

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

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

Hotfix	Fix Content	Up to Version
5.0.1.2	Refer to Hotfix 5.0.1.2 Release Notes	5.0.1.2002
5.1.1.1	Refer to Hotfix 5.1.1.1 Release Notes	5.1.1.1002

Known Issues

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

Issue	Description
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 3.5.2

This section describes updates made to the Syslog Plugin 3.5.2.

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:

Hotfix	Fix Content	Up to Version
3.5.0.1	Refer to Hotfix 3.5.0.1 Release Notes	3.5.0.1001

Technical Support Plugin 1.2.4

The Technical Support Plugin provides an infrastructure used to automatically analyze an extensive range of log files on your system and send them to the ForeScout support team for further investigation.

Analysis of log files is carried out on a wide range of issues, for example service restarts, database issues, plugin errors, issues dealing with policies, internal processes, reports or any other issue occurring on your CounterACT system.

The plugin provides a CLI command that analyzes and sends system log files for each of your CounterACT devices. You should run the tool on the device you want to troubleshoot.

Requirements

There are no unique requirements for this plugin.

Fixed Issues

This section identifies the fixed issues for this version of the Technical Support Plugin.

- Merged Hotfixes

Merged Hotfixes

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

Hotfix	Fix Content	Up to Version
1.2.3.1	Refer to Hotfix 1.2.3.1 Release Notes	1.2.3.1008

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 cannot proceed unless you agree to the license agreement.

   - *The installation begins 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-release-notes-1-1-2/

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:

- 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 only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Forescout Customer Portal:

- Go to https://Forescout.force.com/support/ and select **Downloads**.

Documentation Portal

The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

Use context-sensitive *Help* buttons to 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

2019-11-19 15:07