FORESCOUT

Forescout

Core Extensions Module

Overview Guide

Version 1.1

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

https://www.forescout.com/support/

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the 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

2019-04-04 15:28

Table of Contents

About the Core Extensions Module

The Forescout Core Extensions Module provides network connectivity, visibility and control through the following components:

- Advanced Tools Plugin 2.3
- CEF Plugin 2.8
- Dashboard Plugin 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 1.1.1
- NBT Scanner Plugin 3.1
- Packet Engine 8.1
- Reports Plugin 5.1
- Syslog Plugin 3.5
- Technical Support Plugin 1.2.2
- Web Client Plugin 1.0

The Core Extensions Module is a Forescout Base Module. Base Modules are delivered with each Forescout release.

Module Requirements

Forescout version 8.1.

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

Install the Module

This module is automatically installed when you upgrade to Forescout version 8.1 or perform a Forescout version 8.1 clean installation. New module releases may become available between Forescout releases.

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.
- Upgrading to this module (or one of its components) from a version released prior to Forescout 8.1.

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.

Learn More about Module Components

This guide presents a short description of each module component. Detailed information about each component, such as requirements, features and configuration, is available in related guides.

Information about new and enhanced features as well as fixed, known and upgrade issues is available in the module Releases Notes.

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.

Advanced Tools Plugin 2.3

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

Advanced Tools Plugin Configuration Guide

Refer to the Forescout Advanced Tools Plugin Configuration Guide Version 2.3 for details about this plugin.

CEF Plugin 2.8

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.

CEF Plugin Configuration Guide

Refer to the Forescout CEF Plugin Configuration Guide Version 2.8 for details about this plugin.

Dashboard Plugin 1.1

The Dashboard is a web-based information center that delivers dynamic at-a-glance information about:

- Device compliance
- Device classification
- Device management status
- Network overview

This dashboard is designed for corporate executives who want a quick overview of important network activities and security administrators that would like to easily monitor their security state. This information is collected from Forescout policies and is periodically updated as endpoints are monitored and controlled by Forescout.

Refer to the Forescout Administration Guide Version 8.1 for details about the Dashboard.

Device Classification Engine 1.3

The Device Classification Engine is a core feature of Forescout 8.1 that resolves classification-related properties for comprehensive classification of each endpoint.

The key benefits of the Device Classification Engine are:

- Out-of-the-box precise classification of traditional IT devices as well as IoT, OT, mobile, and virtual endpoints connected to your network.
- Comprehensive view of all endpoints in the inventory across three new classification metrics.
- High level of granular classification of function, operating system and vendor.
- Broad and extensible Primary Classification policy template for device classification.
- Content updates that allow rapid accommodation of new endpoint categories and finer granularity in classification.
- Display of pending classification changes for evaluating the impact of Device Profile Library upgrades.
- Flexible classification paradigm that allows you to ensure complete classification coverage within your environment.

Device Classification Engine Configuration Guide

Refer to the Forescout Device Classification Engine Configuration Guide Version 1.3 for details about this plugin.

DHCP Classifier Plugin 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.

DHCP Classifier Plugin Configuration Guide

Refer to the Forescout DHCP Classifier Plugin Configuration Guide Version 2.2 for details about this plugin.

DNS Client Plugin 3.2

The DNS Client Plugin resolves the DNS host name of a given IP address. The **DNS Name** property stores the name returned by the DNS server. A companion Track Changes property is also defined.

DNS Client Plugin Configuration Guide

Refer to the Forescout DNS Client Plugin Configuration Guide Version 3.2 for details about this plugin.

DNS Enforce Plugin 1.3

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

DNS Enforce Plugin Configuration Guide

Refer to the Forescout DNS Enforce Plugin Configuration Guide Version 1.3 for details about this plugin.

DNS Query Extension Plugin 1.3

The DNS Query Extension Plugin is an internal component of the Forescout platform that provides a service for various features in the product. In addition, it provides stand-alone features that:

- Determine whether a given endpoint in the network is a DNS server.
- Check DNS lookups of specific domain names by endpoints in the network. For example, it can detect that an endpoint browsed to a specific website, and then trigger an action to block that endpoint.

The DNS Query Extension sees traffic via the SPAN port. It detects and parses DNS messages in the network that reference specific host names. It does not report other DNS interactions.

DNS Query Plugin Configuration Guide

Refer to the Forescout DNS Query Plugin Configuration Guide Version 1.3 for details about this plugin.

External Classifier Plugin 2.2.4

The External Classifier Plugin accesses a set of MAC addresses maintained in an FTP server or an LDAP server to:

- Assign a configured text label to any host whose MAC address matches a MAC address in the retrieved set.
- Use the assigned text label in a policy to follow up with required actions.

External Classifier Plugin Configuration Guide

Refer to the Forescout External Classifier Plugin Configuration Guide Version 2.2.4 for details about this plugin.

Flow Analyzer Plugin 1.4.1

The Flow Analyzer Plugin detects flow information regarding the endpoints in your environment. It collects a statistical sampling of data about the network traffic in your environment, such as average packet size, average packet rate per second, inbound and outbound bandwidth usage, and DNS resolutions.

Forescout researchers continually attempt to provide better classification and posture assessment services to customers. Customers who opt to allow the anonymous information detected by the Flow Analyzer in their environments to be shared with Forescout provide an important contribution to the Forescout Research and Intelligent Analytics Program. For more information about the program, see the section on *The Forescout Research and Intelligent Analytics Program* in the Forescout Administration Guide.

By default, after you accept the Forescout Research and Intelligent Analytics Program participation terms, your CounterACT devices share selected endpoint properties with Forescout. The purpose of the Flow Analyzer is to provide additional properties to be shared with Forescout. Properties resolved by the Flow Analyzer are not available to Forescout users from the Policy Manager.

The Forescout Research and Intelligent Analytics Program is a voluntary program. Customers are under no obligation to share their data to help Forescout improve classification. The Forescout Research and Intelligent Analytics Program and the Flow Analyzer provide no immediate benefits to an individual customer. In the long term, the program benefits customers in the form of more precise classification profiles.

Flow Analyzer Plugin Configuration Guide

Refer to the Forescout Flow Analyzer Plugin Configuration Guide Version 1.4.1 for details about this plugin.

Flow Collector 1.0

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.

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

- NetFlow v9
- IPFIX
- sFlow

With the introduction of the Flow Collector in this release, 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.

Flow Collector Configuration Guide

Refer to the Forescout Flow Collector Configuration Guide Version 1.0 for details about this plugin.

IOC Scanner Plugin 2.3

The IOC Scanner Plugin combines the threat detection mechanisms of third-party products with the network visibility and compliance enforcement capabilities of the Forescout platform to multiply the benefits of working with a threat detection or prevention product.

The plugin serves as a centralized database and scanning hub for other plugins in the Forescout Advanced Threat Detection Integration Module and in the Forescout Intel Security Integration Module.

IOC Scanner Plugin Configuration Guide

Refer to the Forescout IOC Scanner Plugin Configuration Guide Version 2.3 for details about this plugin.

IoT Posture Assessment Engine 1.1.1

The IoT Posture Assessment Engine assesses the security risk associated with IoT devices based on their use of weak login credentials.

The key benefits of the IoT Posture Assessment Engine are:

- Helps you determine which devices in your network are vulnerable to attack due to their use of weak credentials.
- Helps you determine which devices and servers in your network are configured to use credentials that are common within the company and should be considered insecure.
- Provides extensible IoT Posture Assessment policy templates for SNMP, SSH, and Telnet credential vulnerabilities.

IoT Posture Assessment Engine Configuration Guide

Refer to the Forescout IoT Posture Assessment Engine Configuration Guide Version 1.1.1 for details about this plugin.

NBT Scanner Plugin 3.1

The NBT Scanner Plugin obtains the user that is logged in to a given host and the MAC address of that host and also discovers the NetBIOS name of the host, based on port 137 traffic on the network. It is installed and started by default. Various policy and Assets Portal features will not work properly if the plugin is stopped.

NBT Scanner Plugin Configuration Guide

Refer to the Forescout NBT Scanner Plugin Configuration Guide Version 3.1 for details about this plugin.

Packet Engine 8.1

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, installed applications, and other endpoint properties
- Detection of NAT behavior, spoofing, port scanning, and other suspicious or malicious behavior patterns
- 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)

Packet Engine Configuration Guide

Refer to the Forescout Packet Engine Configuration Guide Version 8.1 for details about this plugin.

Reports Plugin 5.1

The Reports Plugin lets you generate reports with real-time and trend information about policies, host compliance status, vulnerabilities, device details, assets and network guests.

Use reports to keep network administrators, executives, the Help Desk, IT teams, security teams or other enterprise teams well-informed about network activity. Reports can be used, for example, to help you understand:

- Long term network compliance progress/trends
- Immediate security needs
- Compliance with policies
- Status of a specific policy
- Network device statistics

You can create reports and view them immediately, save reports or generate schedules to ensure that network activity and detections are automatically and consistently reported.

In addition, you can use any language supported by your operating system to generate reports. Reports can be viewed and printed as either PDF or CSV files.

Reports Plugin Configuration Guide

Refer to the Forescout Reports Plugin Configuration Guide Version 5.1 for details about this plugin.

Syslog Plugin 3.5

The Syslog Plugin lets you send, receive and format event messages to/from external Syslog servers. You can send messages from one CounterACT device to one or more Syslog servers. You can receive messages from up to three Syslog servers.

Syslog Plugin Configuration Guide

Refer to the Forescout Syslog Plugin Configuration Guide Version 3.5 for details about this plugin.

Technical Support Plugin 1.2.2

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 Forescout 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.

Technical Support Plugin Configuration Guide

Refer to the Forescout Technical Support Plugin Configuration Guide Version 1.2.2 for details about this plugin.

Web Client Plugin 1.0

The Web Client Plugin delivers the Forescout Web Client. The Forescout Web Client provides users the following page:

- Dashboard

The Dashboard is a web-based information center that delivers dynamic at-a-glance information about:

- Device compliance
- Device classification
- Device management status
- Network overview

This dashboard is designed for corporate executives who want a quick overview of important network activities and security administrators that would like to easily monitor their security state. This information is collected from Forescout policies and is periodically updated as endpoints are monitored and controlled by Forescout.

Refer to the *Forescout Administration Guide* for details about the Dashboard.

Web Client Plugin Configuration Guide

Refer to the Forescout Web Client Plugin Configuration Guide Version 1.0 for details about this plugin.

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/ 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).