ForeScout CounterACT®

Core Extensions Module

Overview Guide

Version 1.0

Table of Contents

About the Core Extensions Module

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

- Advanced Tools Plugin
- CEF Plugin
- DHCP Classifier Plugin
- DNS Client Plugin
- DNS Enforce Plugin
- DNS Query Extension Plugin
- Device Classification Engine
- External Classifier Plugin
- Flow Analyzer Plugin
- IOC Scanner Plugin
- IoT Posture Assessment Engine
- NBT Scanner Plugin
- NetFlow Plugin
- Reports Plugin
- Syslog Plugin
- Technical Support Plugin
- Web GUI Plugin (Dashboard)

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

Module Requirements

CounterACT version 8.0.

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

Install the Module

This module is automatically installed when you upgrade to CounterACT version 8.0 or perform a CounterACT version 8.0 clean installation. New module releases may become available between CounterACT releases.

Rollback and Upgrade the Module

Plugins included in this module are installed and rolled back with the module.

If you are working with version 1.0 of this module, you cannot roll back the module. Information regarding module upgrade and rollback will be available with the next module release.

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.

Configuration Guides for each module component are available on the Documentation page of the ForeScout Customer Portal.

Advanced Tools Plugin

The Advanced Tools Plugin provides host properties and actions in CounterACT 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

CEF Plugin

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

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

DHCP Classifier Plugin

The DHCP Classifier Plugin extracts host information from DHCP messages. Hosts communicate with DHCP servers to acquire and maintain their network addresses. CounterACT 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 CounterACT such as the HPS Inspection Engine and Nmap queries.

- This plugin lets CounterACT retrieve host information when methods such as the CounterACT packet engine or HPS Nmap scanner are unavailable, or in situations where CounterACT 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.

DNS Client Plugin

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 Enforce Plugin

The DNS Enforce Plugin lets CounterACT 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 Query Extension Plugin

The DNS Query Extension Plugin is an internal component of CounterACT 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.

Device Classification Engine

The Device Classification Engine is a core feature of CounterACT 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.

External Classifier Plugin

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.

Flow Analyzer Plugin

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 *Data Sharing for the ForeScout Research and Intelligent Analytics Program* in the CounterACT 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 CounterACT 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.

IOC Scanner Plugin

The IOC Scanner Plugin leverages threat detection and threat prevention mechanisms of third-party systems with the network visibility and enforcement capabilities of CounterACT.

This alliance ensures that you accelerate response time, automate workflows, achieve major operational efficiency and provide superior security.

CounterACT weighs in with its complete real-time visibility and agentless capabilities to fill the void of third-party threat detection and threat prevention systems which may not have full visibility and consequently may overlook important endpoint activity.

Specifically, the plugin serves as:

- A mechanism for scanning all CounterACT-managed Windows endpoints for Indicators of Compromise (IOC).

A centralized repository of all threats and their IOCs reported to CounterACT or added manually.

IoT Posture Assessment Engine

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.

NBT Scanner Plugin

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.

NetFlow Plugin

The NetFlow Plugin integrates the NetFlow reporting protocol with CounterACT.

NetFlow is a widely supported protocol that allows switches and routers to capture and report IP network traffic statistics.

The plugin listens to NetFlow data streams and analyzes them to detect endpoints or endpoint property values that the CounterACT Packet Engine might not learn.

This capability becomes more relevant in large scale deployments, where the CounterACT packet engine is limited in its ability to detect activity in remote sites and branch offices. Use of information reported by NetFlow improves visibility and speeds detection of new endpoints.

Reports Plugin

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.

Syslog Plugin

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.

Technical Support Plugin

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.

Web GUI Plugin (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 CounterACT policies and is periodically updated as endpoints are monitored and controlled by CounterACT.

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

Additional CounterACT Documentation

For information about other CounterACT features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** - Product Updates Portal
- ***Centralized Licensing Mode*** - Customer Portal

🗎 *Software downloads are also available from these portals.*

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

The Product Updates Portal provides links to CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

1. Go to https://updates.forescout.com/support/index.php?url=counteract.

2. Select the CounterACT version you want to discover.

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, 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. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to https://forescout.force.com/support/.
2. Select **Downloads** or **Documentation**.

Documentation Portal

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

🗎 *If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.*

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

CounterACT Administration Guide

Select **CounterACT Help** from the **Help** menu.

Plugin Help Files

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.
2. Select the plugin and then select **Help**.

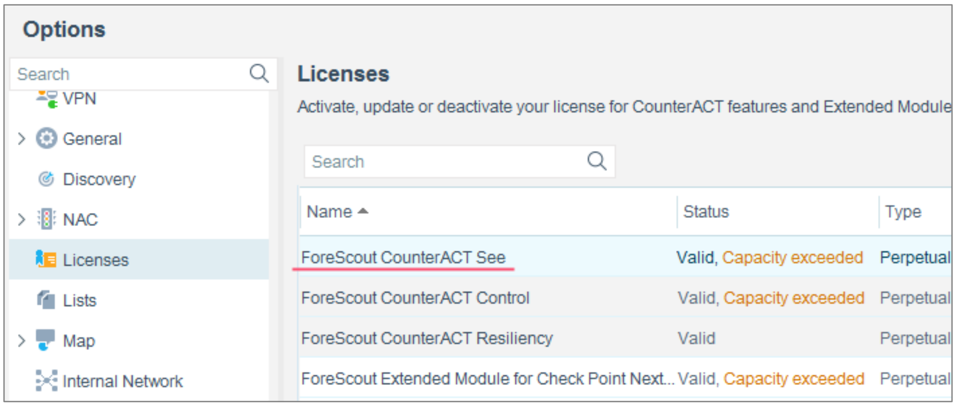
Documentation Portal

Select **Documentation Portal** from the **Help** menu.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Licenses

Activate, update or deactivate your license for CounterACT features and Extended Module

Name ▲	Status	Type
ForeScout CounterACT See	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
ForeScout Extended Module for Check Point Next...	Valid, Capacity exceeded	Perpetual

Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

These products are based on software developed by ForeScout. The products described in this document may be protected by one or more of the following U.S. patents: #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Send comments and questions about this document to: support@forescout.com

2018-03-27 18:24