ForeScout CounterACT®

Work with IPv6 Addressable Endpoints

How-to Guide

Version 8.0

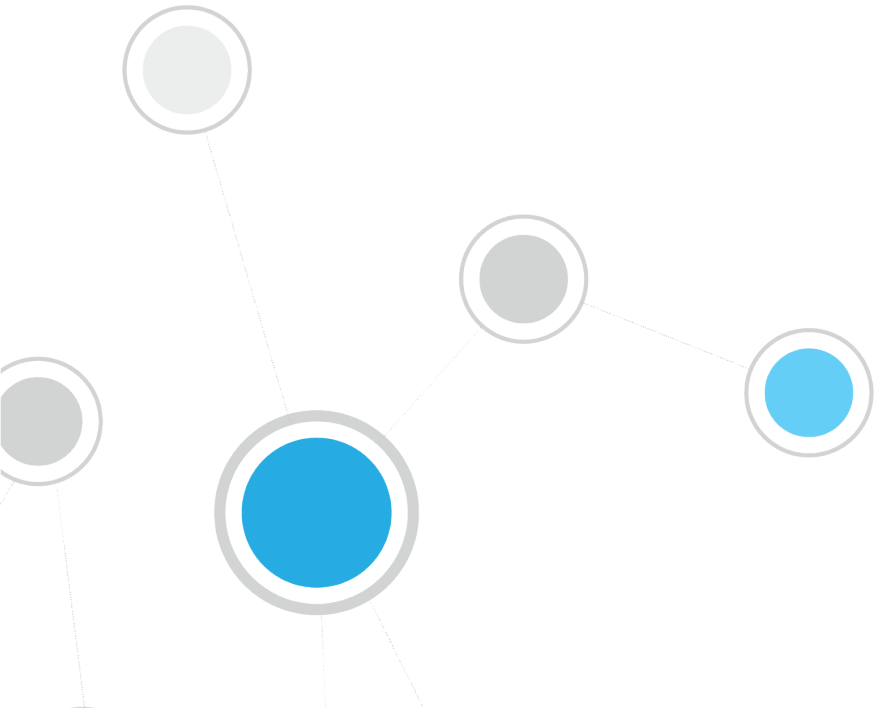


Table of Contents

About IPv6 Network Environments 3

About CounterACT IPv6 Support 3

Changes to Console Functionality for IPv6 Support 4

Display of IPv6 Information in CounterACT 4

Working with the Groups Manager 4

Specificying IP Subnets and Internal Network Segments 5

Host Properties for IP Addresses 6

Controlling Reporting and Retention of IPv6 Addresses 7

Disabling IPv6 Address Support 8

Limitations on IPv6 Support 8

Address Discovery on Windows XP Endpoints 8

Console Features That Do Not Support Configuring IPv6 Addresses 9

Actions Not Carried out by Packet Engine 9

Host Properties Not Resolved by Packet Engine 9

Additional CounterACT Documentation 10

Documentation Downloads 10

Documentation Portal 10

CounterACT Help Tools 11

About IPv6 Network Environments

The Internet Protocol (IP) provides a standard address format to identify endpoints in a network. Data networks have grown to consume the initial address space provided by version 4 of IP, and version 6 of the protocol defines a new format with a larger address space and other improvements. The IPv6 address format is gradually being adopted in network environments.

In today's transitional networks, nodes and gateways support both IPv4 and IPv6 addresses, including the following types of endpoints:

- IPv4-only endpoints are known to the network only by their IPv4 addresses.
- IPv6-only endpoints are known only by their IPv6 addresses.
- Dual-stack endpoints have both IPv4 and IPv6 addresses.

In addition, these endpoints typically have MAC addresses.

This document describes how ForeScout CounterACT® operates in an IPv6 enabled environment, and how you can use CounterACT to manage all endpoints in such a network.

About CounterACT IPv6 Support

CounterACT 8.0 introduces full support for dual-stack network environments. It removes limitations in IPv6 support that were present in earlier releases.

Currently, the core CounterACT product and the following components fully support IPv6 addressable endpoints:

- The following Endpoint Module components:
  - HPS Inspection Engine

    *SecureConnector™ for HPS Inspection Engine is **not** supported.*
  - Linux Plugin
  - OS X Plugin
- The following Network Module components:
  - Switch Plugin
  - Wireless Plugin

  For vendor-specific details of IPv6 support see the *Network Module Release Notes* and related Plugin Configuration Guides.
- Authentication Module - all components
- The following Core Extensions Module components:
  - DNS Client Plugin
  - Reports Plugin
  - Device Classification Engine
  - External Classifier
  - Syslog Plugin

- Related databases and profile libraries, including:
  - Device Profile Library
  - NIC Vendor DB
  - Security Policy Templates
  - Windows Applications
  - Windows Vulnerability DB

Subsequent CounterACT 8.x releases may include IPv6 support for additional CounterACT components. Currently, IPv6 support has not been implemented or verified for such components. Typically the properties, actions, and policy templates provided by these components currently ignore or do not detect IPv6-only endpoints.

For details of IPv6 support in ForeScout modules and other components, refer to the Release Notes of the CounterACT 8.x release that is running in your environment.

Changes to Console Functionality for IPv6 Support

This section describes changes to Console options or to general CounterACT functionality that were motivated by IPv6 support.

This section also describes minor limitations in working with IPv6 addresses.

Display of IPv6 Information in CounterACT

IPv6 addresses are displayed by default in the panes of the Console Home View, and in the Host Log table. In other tables, columns with IPv6 addresses may be disabled by default to conserve space. You can enable columns based on properties that report IPv6 addresses. See Host Properties for IP Addresses.

Working with the Groups Manager

Use the Groups Manager to edit group structure and to view and edit static content.

- Use the Groups Manager to *permanently* assign IP or MAC addresses to groups.
- Use the *Add to Group* action in a policy to *conditionally* place endpoints in groups.

When you use the Groups Manager, you can use the IPv4 address, the IPv6 address, or the MAC address as the key value for a group. Endpoints are added to the group based on their IPv4 or IPv6 addresses. However, when you use the *Add to Group* action to add an endpoint to a group, only the IPv4 and the MAC addresses of the endpoint can be used as a key value.

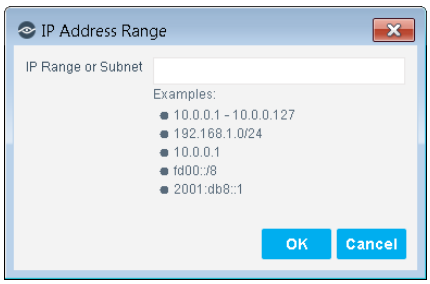
Specificying IP Subnets and Internal Network Segments

Until now, CounterACT used the words *range* and *segment* loosely to describe both segments of the user's network environment, and the Internal Network segments you define in CounterACT for management purposes using Segment Manager. This sometimes led to confusion when working with IP Allocation, Segment Manager and related features.

In addition, new conventions have emerged to specify segments of the large address space in IPv6 environments.

The following changes are introduced to avoid confusion in large networks and/or dual-stack environments:

- Field labels and descriptions have been generalized to include both IPv4 and IPv6 addresses. The term *IP addresses* is used when any IPv4/IPv6 address or subnet can be specified.
- The term *Internal Network segment* replaces the term *segment* and refers to segments defined in CounterACT using Segment Manager.
- For clarity, the term *subnet* is used in addition to the term *range*, and instead of the term *segment* in some fields that accept both IP ranges and subnets.
- CIDR notation can be used in fields to specify IPv4 and IPv6 subnets.



As of this release, language changes have not been implemented in all Console windows, or in all CounterACT documentation. Ongoing updates are planned for upcoming releases.

In some interactions, you can no longer directly specify IP address ranges on the fly. Define and use Internal Network segments to specify groups of IP addresses. For example:

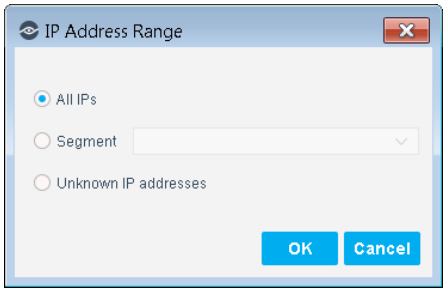
- In the Internal Network pane, you can only add or remove Internal Network segments that you defined in Segment Manager.

  Existing IP address ranges in the Internal Network are preserved during upgrade.

  You can directly specify IP ranges when you first define the Internal Network with the Initial Setup wizard.

- In the IP Allocation and Failover pane, you can only specify Internal Network segments when you map IP addresses to CounterACT devices.

- In policy wizards and some other areas, the IP Range option has been removed. Select an existing Internal Network segment or define a new Internal Network segment in Segment Manager.



Some Console features do not allow specification of IPv6 address ranges. See Console Features That Do Not Support Configuring IPv6 Addresses.

Host Properties for IP Addresses

The following properties report IPv4 and IPv6 addresses detected on endpoints:

Access IP	Indicates the endpoint IP address that CounterACT used the last time it connected successfully to the endpoint.
IPv4 Address **IPv6 Address**	Indicates one or more IP addresses of an endpoint. Matching criteria include: ▪ Any IP address ▪ Addresses in a named CounterACT Internal Network segment ▪ Addresses in a specific IP range or subnet ▪ IP addresses that start with, end or match a certain numerical expression ▪ Endpoints without a known IPv4 address (endpoints will be detected when CounterACT discovers their MAC address). The IPv6 Address property has a parallel Track Changes property.
IPv6 Addresses Added/Removed	A Track Changes property for the **IPv6 Address** property.
Last Known IPv4 Address	Indicates an IPv4 Address that once referred to this endpoint, but was assigned to another endpoint. See "Working with Hosts Whose IPv4 Address is Used by Another Host" in the *CounterACT Administration Guide.* This property was previously named **Last Known IP Address**.
Number of IPv4 Addresses **Number of IPv6 Addresses**	Indicates the number of IP addresses of each type that CounterACT detected for an endpoint. You can specify IPv4 addresses to ignore when calculating the Number of IPv4 Addresses property. See *Tuning* in the *HPS Inspection Engine Configuration Guide*. The count of IPv6 addresses depends on the purge timeout defined for inactive IPv6 addresses. See Controlling Reporting and Retention of IPv6 Addresses There are parallel Track Changes properties.

The following property has been deprecated:

IPv6 Link-Local Address	Indicates Link-Local IPv6 address(es) of an endpoint reported by the Switch Plugin and Wireless Plugin.

Controlling Reporting and Retention of IPv6 Addresses

In environments that use IPv6 Addresses, auto-configuration and other management strategies can generate large numbers of temporary addresses. This section describes how to tune the way CounterACT reports and retains IPv6 addresses to maintain current, valid address information.

To control the number of IPv6 addresses reported for Windows endpoints:

1. Log in to the CounterACT device CLI.
2. Submit the following command:

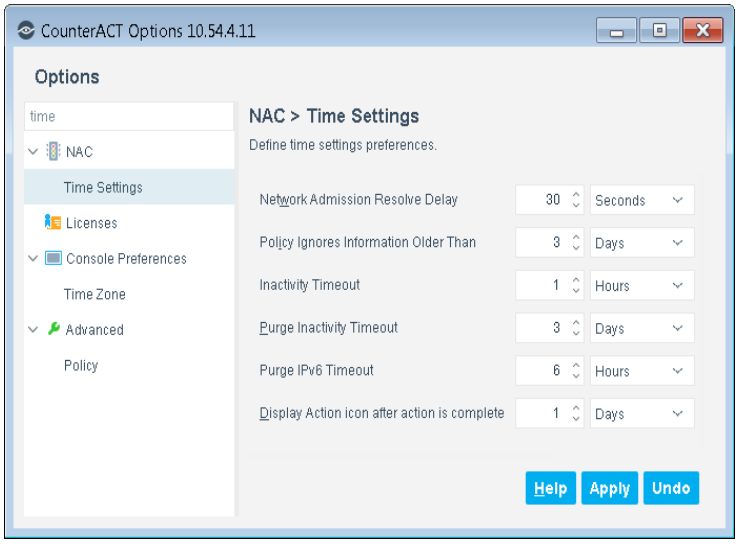
   `fstool va set_property config.number_of_ipv6_to_report.value` *n*

   Where *n* is an integer. The default value is 10.

   The HPS Inspection Engine reports up to *n* IPv6 addresses for each Windows endpoint.

To control how long CounterACT retains IPv6 addresses:

1. Log in to the CounterACT Console as an administrator.
2. Select **Options** from the toolbar, or select **Tools > Options** from the menu.
3. In the Options tree select **NAC > Time Settings**.



4. Configure the **Purge IPv6 Timeout** setting.

   This setting determines how long CounterACT associates an IPv6 address with an endpoint. This timeout is measured from the time CounterACT learns the IPv6 address. If CounterACT does not detect this address or its related MAC address in the network during the time period specified:

   – It no longer associates the address with the endpoint. This address no longer appears in the **IPv6 Address** host property for the endpoint.
   – If the endpoint has no other IP or MAC address, it is purged completely from CounterACT.

Disabling IPv6 Address Support

When you upgrade to CounterACT version 8.0 and its related components, IPv6 addressable endpoints are supported by default. This section describes configuration settings that disable IPv6 support.

To enable or disable IPv6 address reporting for switches, wireless controllers and the HPS Inspection Engine:

1. Log in to the CounterACT device CLI.
2. To control reporting by switches, submit the command:

   `fstool sw set_property config.read_ipv6_neighbor_table.value` *[0 | 1]*

   To control reporting by wireless controllers, submit the command:

   `fstool wireless set_property conf.read_ipv6_table.value` *[0 | 1]*

   where the value *0* disables reporting, and the value *1* enables reporting.

   Reporting of IPv6 addresses is enabled or disabled for all switches and/or controllers that are managed by this CounterACT device.
3. To control reporting by the HPS Inspection Engine, submit the command:

   `fstool va set_property resolved.resolve_all false`

   The HPS Inspection Engine no longer learns IPv6 addresses on endpoints.

Limitations on IPv6 Support

This section describes limitations in CounterACT support for IPv6-addressable endpoints.

Address Discovery on Windows XP Endpoints

Currently, CounterACT endpoint detection and discovery methods cannot discover IPv6 addresses on endpoints running Windows XP. CounterACT can connect to and manage these endpoints using IPv6 addresses discovered by switches, traffic monitoring, and other sources.

Console Features That Do Not Support Configuring IPv6 Addresses

The following Console features do not allow specification of IPv6 address ranges. Only IPv4 address ranges are supported. If you specify Internal Network segments, only the IPv4 ranges of the segment are included in the specified addresses. IPv6 subnets are ignored (this may change in subsequent releases).

- When you define the Active Response range for Threat Protection features (**Options > Threat Protection > Advanced > Active Repose Range**).
- When you define the Scope of a Console User Profile (**Options > Console User Profiles**)
- When you define/edit IP-based exceptions to HTTP Redirection (**Options > NAC > HTTP Redirection**)
- When you define/edit Virtual Firewall rules (**Options > Virtual Firewall**). Similarly, you can only specify IPv4 addresses when you use the **Virtual Firewall** action.
- When you specify Windows endpoints that download information from the Windows Updates website or a WSUS, you cannot directly specify IPv6 addresses, but IPv6 subnets are included with IPv4 ranges. For details see "Windows Updates" in the *HPS Inspection Engine Configuration Guide*.

Actions Not Carried out by Packet Engine

The following actions are not carried out by the Packet Engine for endpoints that only have IPv6 addresses:

- HTTP actions (for example, *HTTP Login* and *Start SecureConnector*)
- Virtual Firewall

These actions may, however, be carried out by other CounterACT components.

Host Properties Not Resolved by Packet Engine

The following host properties are not resolved by the Packet Engine for endpoints that only have IPv6 addresses:

- Authentication Login (Admission event property)
- Authentication Server (Admission event property)
- HTTP User Agent
- Open Ports
- Sessions as Client
- Sessions as Server

These properties may, however, be resolved by other CounterACT components.

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**.

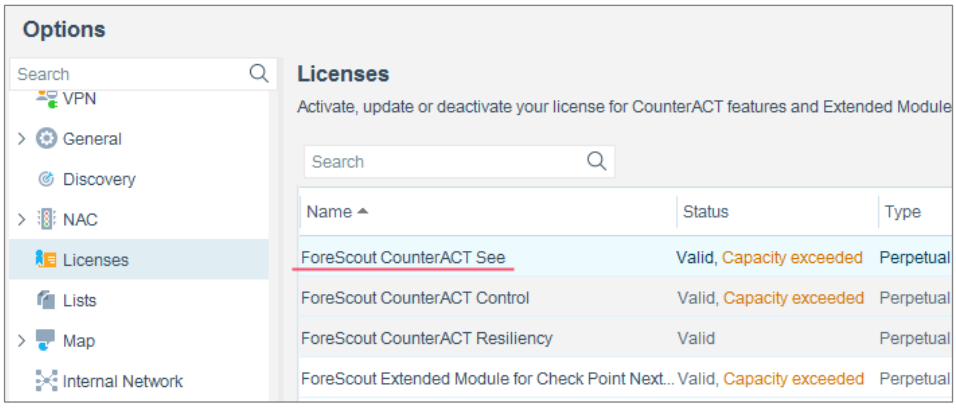
Documentation Portal

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.



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

Legal Notice

2018-04-15 11:36