ForeScout

Work with IPv6 Addressable Endpoints

How-to Guide

Version 1.0.0

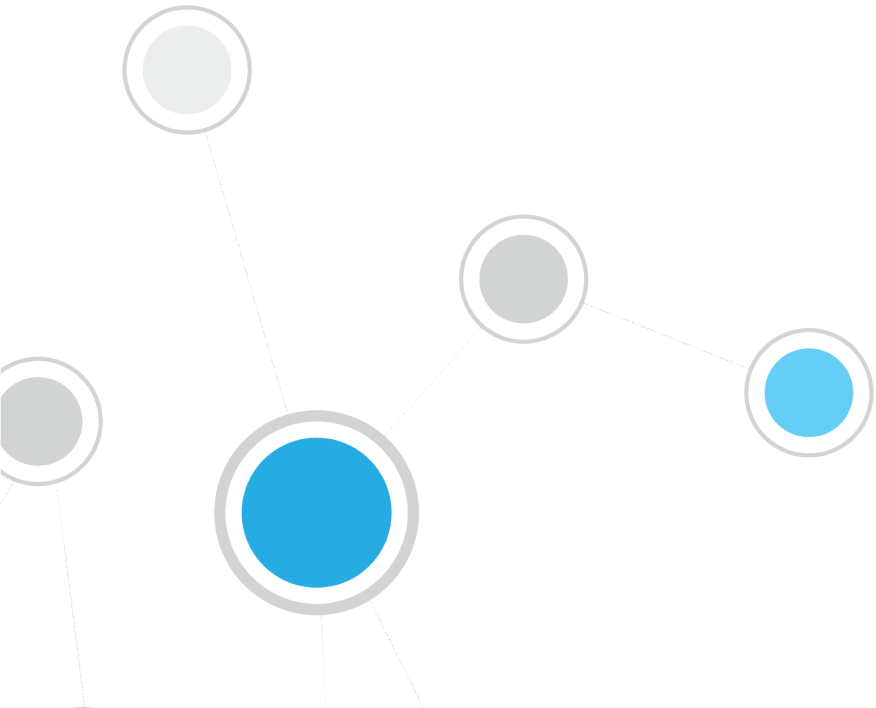


Table of Contents

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

Requirements for IPv6 Support

The following CounterACT components are required for IPv6 support:

- Reports Plugin 4.1.8 or above
- Switch Plugin 8.11.0 or above
- Wireless Plugin 1.7.0 or above
- Service Pack 3.0.0 or above

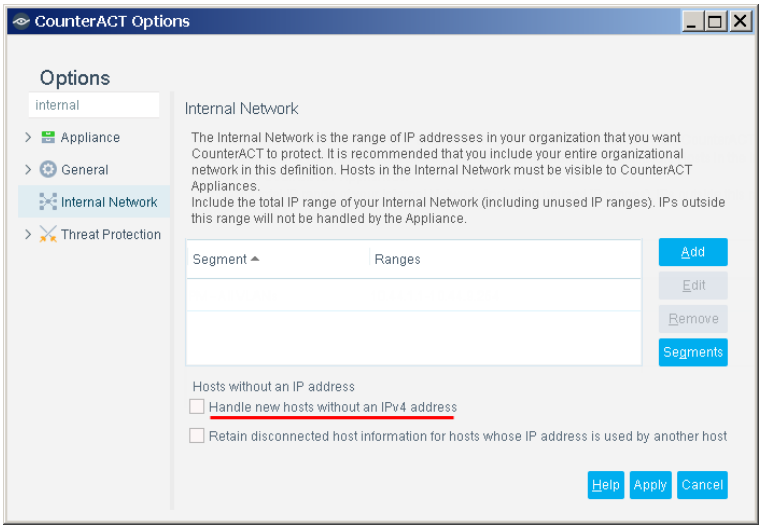
Switches and Controllers that Support IPv6 Address Detection

When you upgrade to the releases listed in Requirements for IPv6 Support, CounterACT reports IPv6 endpoint addresses detected by switches and wireless controllers, and reports them using new host properties. IPv6 addresses are detected for all endpoints that connect to the network through the following network devices:

- Cisco or Brocade/Foundry switches
- Juniper switches
- Cisco or Aruba wireless controllers

Enabling Support for IPv6-only Endpoints

IPv6 enabled environments can include IPv6-only endpoints that do not have IPv4 addresses. To support these endpoints, navigate to the Options tree of the Console, and enable the **Handle new hosts without an IP4 address** option in the Internal Network pane.



Discovery of Endpoints in IPv6 Enabled Environments

This section describes how CounterACT detects and displays endpoints in IPv6 enabled environments. In general:

- IPv4 and dual-stack endpoints are discovered by CounterACT using their IPv4 and MAC addresses, and displayed using their IPv4 address.
- IPv6-only and MAC-only endpoints are discovered using their MAC addresses. A placeholder IPv4 address is displayed for these endpoints in Console views.
- IPv6 addresses are reported as host properties of IPv6 addressable endpoints. You can add columns to Console views to list these properties.

Deriving Unique Endpoints from Observed Addresses

CounterACT learns IPv4 and MAC addresses of endpoints and network nodes in the following ways:

- By inspecting network traffic
- By polling switches, controllers, domain controllers, and other network devices
- When optional plugins are installed, additional information sources such as NetFlow are used.

CounterACT analyzes this information to identify unique endpoints, and to correlate IPv4 and MAC addresses to each endpoint.

Note that:

- CounterACT data correlation logic uses only IPv4 addresses to identify unique endpoints. IPv6 addresses are not used to identify endpoints.
- When no IPv4 address correlates to a unique MAC address, CounterACT lists this MAC-only endpoint with a placeholder IPv4 address in Console views.

This discovery and correlation logic is unchanged when IPv6 addressable endpoints are supported:

- Dual-stack endpoints are detected and displayed by their IPv4 addresses.
- IPv6-only endpoints are detected by their MAC addresses, and displayed using a placeholder IPv4 address (as for MAC-only endpoints without an IPv4 address).

Endpoint Type	Discovery Source	Unique Endpoint Identity	Display in Console
IPv4-only	All data streams	By IPv4 address(es)	By IPv4 address
no IPs	All data streams	By MAC address	By placeholder IPv4 address
IPv6-only	Switches and Controllers only	By MAC address	By placeholder IPv4 address IPv6 addresses - optional column in Console views
Dual-stack	IPv4: all data streams IPv6: switches and controllers only	By IPv4 address(es)	By IPv4 address IPv6 addresses - optional column in Console views

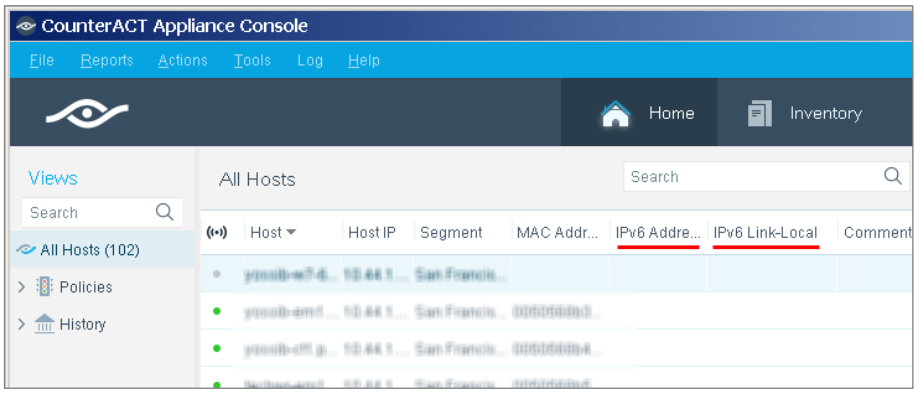
About IPv6 Addresses in CounterACT

When support for IPv6 addresses is enabled, CounterACT can only learn IPv6 addresses by polling network switches and controllers. Other discovery methods do not return IPv6 addresses. For more information, see Switches and Controllers that Support IPv6 Address Detection.

IPv6 address information is available in CounterACT as host properties of the endpoint.

Displaying IPv6 Addressable Endpoints in the Console

IPv4 addresses are the primary index used to display endpoints in Console views. You can add columns to Console views that show IPv6 addresses.



Policy-Based Management of IPv6 Addressable Endpoints

This section describes how CounterACT resolves properties, evaluates policies, and applies actions to endpoints with IPv6 addresses. The following considerations dictate how to work with IPv6 addressable endpoints in CounterACT:

- New Host Properties for IPv6 Endpoints contain IPv6 address information.
- CounterACT does not use IPv6 addresses to contact endpoints.

Dual-stack endpoints are managed using their IPv4 and MAC addresses. CounterACT can resolve all properties for these endpoints, and apply all actions.

You can use CounterACT policy conditions to match these endpoints based on IPv6 host properties. However, CounterACT contacts endpoints using IPv4 and MAC addresses to resolve other properties and to apply actions.

IPv6-only endpoints are managed using their MAC addresses. This limits the properties that can be resolved and the actions that can be applied. For these endpoints:

- All properties resolved by the Switch Plugin and Wireless Plugin are reported.
- Properties that can be resolved using only the MAC address can be resolved.
- Actions applied by the Switch Plugin or Wireless Plugin are supported when they use endpoint MAC addresses and not IPv4 addresses. These include the following actions:
  - Assign to VLAN
  - Switch Block
  - Endpoint address ACL (when based on MAC address)
  - WLAN Block
  - WLAN Role
- Actions that send Syslog messages, email messages or HTTP notifications to administrators or 3rd party management platforms regarding IPv6 endpoints are supported. IPv6 property information can be included in these messages as for other host properties. An IPv6-only endpoint cannot be the recipient of these notifications.
- The Add to Group action is supported.

Switch/Wireless devices themselves can only be managed via IPv4.

Host Properties for IPv6 Endpoints

Three new host properties contain IPv6 related information:

IPv6 Address	Indicates IPv6 address(es) of an endpoint. This information is reported by the Switch Plugin and Wireless Plugin.
IPv6 Addresses Added/Removed	A Track Changes property for the IPv6 Address property.

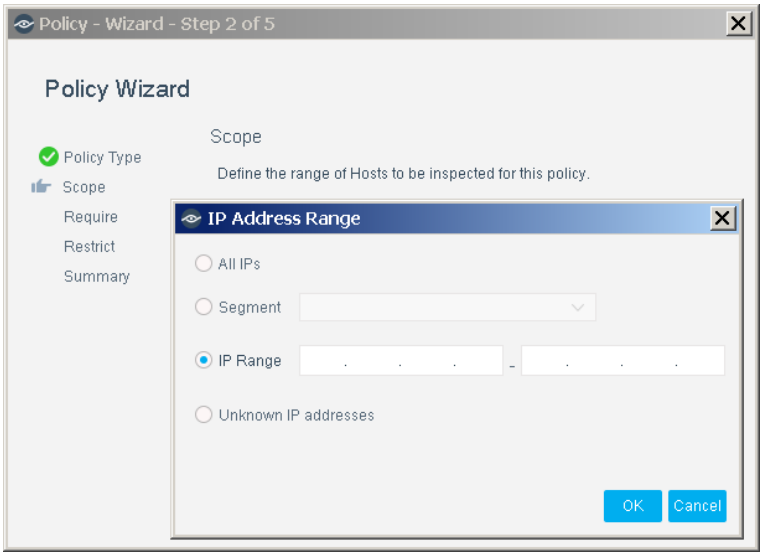
IPv6 Link-Local Address	Indicates Link-Local IPv6 address(es) of an endpoint. This information is reported by the Switch Plugin and Wireless Plugin.

Using CounterACT Policies to Detect IPv6 Endpoints

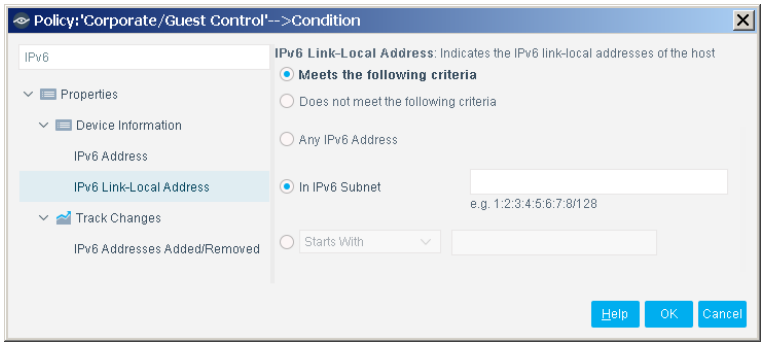
When you create CounterACT policies inIPv6 enabled environments, note that the Scope settings of the CounterACT policy wizard only refer to IPv4 addresses.

However, it is easy to use existing settings to scope various types of endpoints in an IPv6 enabled environment.

- To include IPv6-only endpoints in the policy scope, define only one Scope range using the **Unknown IP addresses** option. Endpoints with no known *IPv4* addresses are included in the scope of the policy. This means that:
  - IPv6-only endpoints are included.
  - Dual-stack endpoints are excluded because they have an IPv4 address.
  - MAC-only endpoints are also included.
- To include dual-stack endpoints in the policy scope, define a Scope range using the **Unknown IP addresses** option, and define another Scope range using one of the other Scope options.



To apply actions to endpoints based on IPv6 information, define matching conditions in policy rules based on IPv6 host properties.



Enabling and Disabling IPv6 Address Reporting

When you upgrade to the releases listed in Requirements for IPv6 Support, the Switch Plugin and Wireless Plugin detect and report IPv6 addresses by default.

Use the following procedure to enable or disable IPv6 reporting on switches or controllers that are managed by a specific CounterACT device.

To enable or disable IPv6 address reporting:

1. Log in to the CounterACT device CLI.
2. Submit one or both of the following commands:

   To control reporting by switches:

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

   To control reporting by wireless controllers:

   `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.

Legal Notice

2017-07-04 11:33