ExtremeCloud IQ - Site Engine Configuration Considerations

Review the following configuration consideration when installing and configuring the ExtremeCloud IQ - Site Engine suite of network management applications. The following section describes support for IPv6 in the ExtremeCloud IQ - Site Engine suite of applications.

Enabling IPv6 on your OS

IPv6 must be enabled in your operating system for ExtremeCloud IQ - Site Engine to be able to use it. Most current operating systems ship with IPv6 enabled by default. To verify that your operating system has IPv6 enabled, refer to your operating system documentation for more information.

Enabling IPv6 in ExtremeControl

ExtremeControl uses the NetSNMP stack to add support for IPv6 to the product suite. To enable IPv6 you must use the Advanced SNMP suite option to enable IPv6.

1. Open the **Administration** tab.
2. Select the **Options** tab.
3. Expand the Access Control option, and select **Advanced** in the left-panel tree.

   The Advanced options open in the right-panel.
4. Select the **Enable IPv6 Addresses for End-Systems** option checkbox.
5. Click the **Save** button or select the **Auto** checkbox at the bottom of the panel.

   The setting is saved.
6. For this setting to take effect, the ExtremeCloud IQ - Site Engine Server must be restarted.
7. If you are binding to an IPv6 address, edit the .netsight file to bind to the server's hostname. You must use the server's hostname instead of IP address when connecting to the server from a remote client machine.

IPv6 Addressing Notations Supported

ExtremeCloud IQ - Site Engine supports all of the following IPv6 addressing notations.

The following information is taken from RFC 4291, "IP Version 6 Addressing Architecture." To read the complete RFC, see http://www.ietf.org/rfc/rfc4291.txt.

There are three conventional forms for representing IPv6 addresses as text strings:

1. The preferred form is x:x:x:x:x:x:x:x, where the 'x's are one to four hexadecimal digits of the eight 16-bit pieces of the address.
   Examples:

   ABCD:EF01:2345:6789:ABCD:EF01:2345:6789

   2001:DB8:0:0:8:800:200C:417A

   Note it is not necessary to write the leading zeros in an individual field, but there must be at least one numeral in every field (except for the case described in 2.).
2. Due to some methods of allocating certain styles of IPv6 addresses, it is common for addresses to contain long strings of zero bits. In order to make writing addresses containing zero bits easier, a special syntax is available to compress the zeros. The use of "::" indicates one or more groups of 16 bits of zeros. The "::" can only appear once in an address. The "::" can also be used to compress leading or trailing zeros in an address.

   For example, the following addresses:

`2001:DB8:0:0:8:800:200C:417A`	`a unicast address`
`FF01:0:0:0:0:0:0:101`	`a multicast address`
`0:0:0:0:0:0:0:1`	`the loopback address`
`0:0:0:0:0:0:0:0`	`the loopback address`

   may be represented as

2001:DB8::8:800:200C:417A	a unicast address
FF01::101	a multicast address
::1	the loopback address
::	the loopback address

3. An alternative form that is sometimes more convenient when dealing with a mixed environment of IPv4 and IPv6 nodes is x:x:x:x:x:x:d.d.d.d, where the 'x's are the hexadecimal values of the six high-order 16-bit pieces of the address, and the 'd's are the decimal values of the four low-order 8-bit pieces of the address (standard IPv4 representation). Examples:

   0:0:0:0:0:0:13.1.68.3
   0:0:0:0:0:FFFF:129.144.52.38

   or in compressed form:

   ::13.1.68.3
   ::FFFF:129.144.52.38

ExtremeCloud IQ - Site Engine Features that Support IPv6 Addressing

Core ExtremeCloud IQ - Site Engine Features

The following core ExtremeCloud IQ - Site Engine features support IPv6 addresses:

- Fabric Connect:
  - Configure IPv6 CLIP addresses
  - Read IPv6 addresses (CLIP, VLAN, MGMT, BROUTER) from a device
  - Assign an IPv6 CLIP address to be used as the ISIS IPv6 Source IP Address
  - Enable/disable IPv6 IP Shortcuts on the device
- Firmware Upgrades
- Archives
- MIB Tools
- Device Manager
- Device Tree functionality

- Add Device (not Device Discovery)
- Device Import and Export
- FlexViews
- IPv6 SNMP Status polling and Ping polling (ICMP on Linux, TCP echo on windows)
- Syslog parsing with IPv6 addresses
- IPv6 Ping support
- Telnet and SSH support for IPv6 (using PuTTY)
- ExtremeCloud IQ - Site Engine server binding to IPv6 address
- SNMP Redirect
- Client/Server detection of IPv6 support to allow Warning users about limitations
- IPv6 support for the Command Script tool

Compass Support for Searching IPv6 Devices

- Support for ipNetToPhysical (RFC 4293)
- Support for ipv6NetToMedia (RFC 2465)
- Support for inetCidrRouteTable (RFC 4292)

Policy Tab Support

Policy tab functionality supports enforcing to devices modeled with an IPv6 address. The Policy tab also supports IP to Role Mapping using IPv6 addresses, and the following IPv6 rules:

- IPv6 Address Source, IPv6 Address Destination, and IPv6 Address Bilateral rules.
- IPv6 Socket Source, IPv6 Socket Destination, and IPv6 Socket Bilateral rules.
- IPv6 Flow Label rules.
- ICMPv6 rules.
- IP UDP Port Source, IP UDP Port Destination, IP UDP Port Bilateral rules using an IPv6 address.
- IP TCP Port Source, IP TCP Port Destination, IP TCP Port Bilateral rules using an IPv6 address.

Access Control Tab Support

The Administration tab provides an advanced option (Administration > Options > Access Control > Advanced) to enable IPv6 end-system support. Enabling this option allows ExtremeControl to collect, report, and display IPv6 addresses for end-systems in the end-systems table. When this option is changed, you must enforce your engines before the new settings take effect. In addition, end-systems need to rediscover their IP addresses in order to reflect the change in the end-system table. This can be done by either deleting the end-system or performing a Force Reauth on the end-system.

Only end-systems that have a valid IPv4 address as well as one or more IPv6 addresses are supported. End-systems that have only IPv6 addresses are not supported.

The following end-system functionality is available for end-systems with a valid IPv4 address as well as one or more IPv6 addresses:

- End-System table display of IPv6 addresses*
- NAC Dashboard display of IPv6 addresses
- Force Reauth
- Add to MAC Group
- Lock MAC
- Port Monitor
- End-System Summary
- Basic End-System Search
- Delete End-System
- Edit Custom Information
- Registration
- Hostname Resolution
- OS Detection

*Old IPv6 addresses are not automatically cleared from the end-system table. If an end-system's IPv6 address changes, the old IPv6 address may continue to be displayed.

The following end-system functionality is not available for end-systems that have a valid IPv4 address as well as one or more IPv6 addresses:

- Add to IP Group
- Assessment
- Remediation

Configuration Evaluation Tool
Advanced End-System Search
IPv6 rules
Ping
NetBIOS

Known Limitations

General Limitations

- IPv6 devices cannot be reached from clients not running IPv6 protocol stacks on their NICs.
- When IPv6 is enabled, Windows sends TCP Echo instead of ICMP packets for Ping polling status for both IPv4 and IPv6 devices.
- Stackable devices do not currently support setting an IPv6 RADIUS server address.

Device Limitations

Not all devices support IPv6. Refer to your device Firmware Release Notes to determine if the device supports IPv6 and has the required MIBs.

05/2021
21.04.10
PN: 9037050-00