ExtremeCloud Edge - Self-Orchestration Deployment Guide

for Universal Compute Platform Version 5.06.01

9038107-00 Rev. AD
May 2024

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

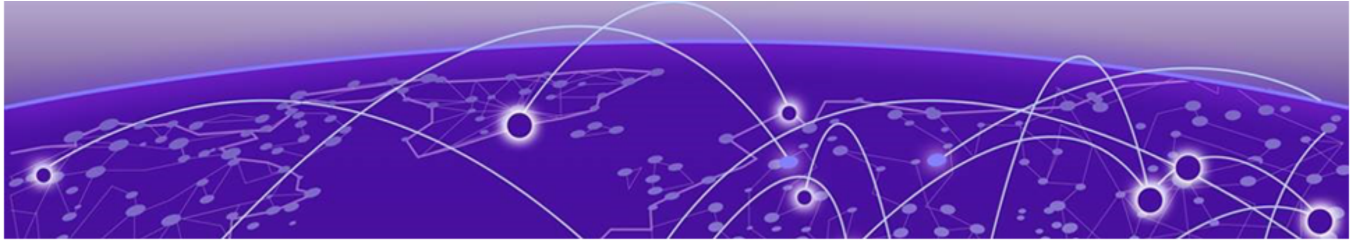
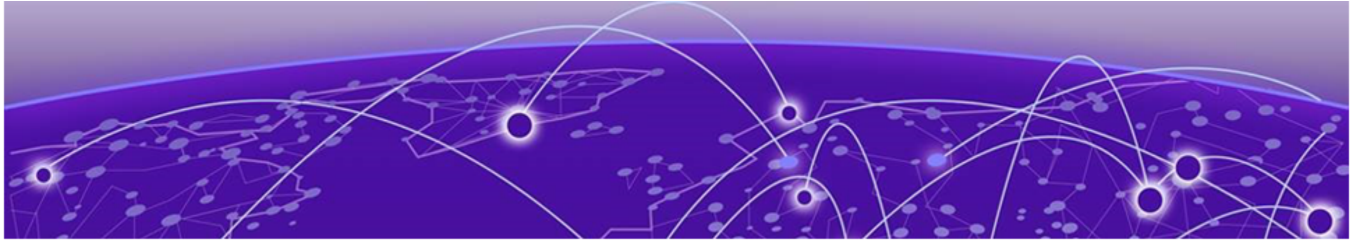


Table of Contents



Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
💡	Tip	Helpful tips and notices for using the product
🗒	Note	Useful information or instructions
➡	Important	Important features or instructions
⚠	Caution	Risk of personal injury, system damage, or loss of data
⚠	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
`{ x | y | z }`	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
`x | y`	A vertical bar separates mutually exclusive elements.
`< >`	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, `member[member...]`.
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation

Release Notes

Hardware and Software Compatibility for Extreme Networks products

Extreme Optics Compatibility

Other Resources such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

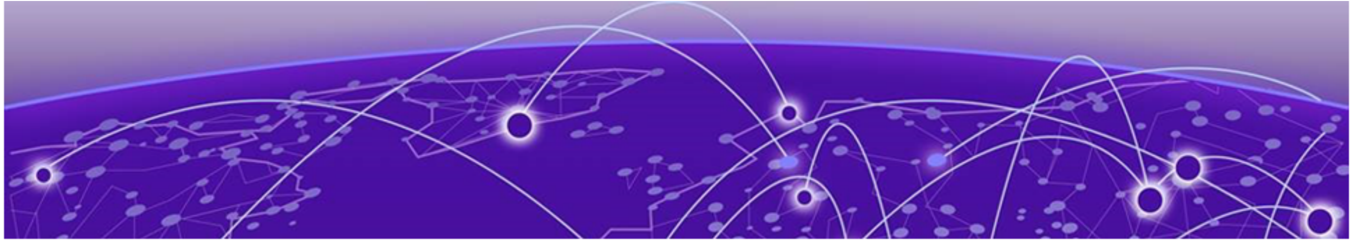
To send feedback, email us at documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.

Revision History

Table 4: Revision History

Revision #	Date	Description of updates
AA	March 12, 2024	• Original published version.
AB	April 23, 2024	• Added *Firewall Requirements* topic. • Also added process for onboarding a cluster to ExtremeCloud IQ.
AC	April 25, 2024	• Updated the GUI fields in th eprocedure for adding a cluster to ExtremeCloud IQ in the *Onboarding a Cluster to ExtremeCloud IQ* procedure.
AD	May 08, 2024	• Added revision history.



Introduction and Prerequisites

This guide provides the steps needed to bring a stand-alone Universal Compute Platform online. Universal Compute Platform leverages Kubernetes and Docker to deploy and manage the delivery of applications to the customer premises, providing the computing power, storage, high availability, and load-balancing for the system.

The system leverages VRRP (Virtual Router Redundancy Protocol) in order to provide support for both high-availability and load balancing, supported by an NGINX engine. All service operations to the cluster should be directed to the corresponding VRRP IP so that the load balancing logic can direct the request to the best node.

- The internal Kubernetes engine requires the reservation of two (2x) /16 subnets. Ensure that this IP address range does not conflict with any routable address space within the organization.

Related Topics

Stand-Alone Configuration on page 8

Stand-Alone Configuration

Deploy Universal Compute Platform in stand-alone mode with a set of Universal Container applications.

This deployment scenario includes the following application requirements for a stand-alone configuration:

- The use of the Virtual IP Address (VIP) is optional, but it provides a convenient way to expose services, from an instance of the UI (port 443) externally. Assign a VIP to each instance of an engine.
- Pod Network configuration settings — Pods are a group of managed containers that share networking and storage resources from the same node (appliance). Each pod is assigned an IP address. All the containers in the pod share the same storage, IP address, and network namespace.
    - Pod Network IP Address and CIDR

- ◦ Service Network IP Address and CIDR

  Note
  CIDR (*Classless Inter-Domain Routing*) is a method for allocating IP addresses and for IP routing.

Note
An Inter-Cluster Connection (ICC) is not required in a Standalone deployment.

Related Topics

Reserved IP Addressing on page 9
VRRP Configuration (Optional) on page 9

Reserved IP Addressing

Container orchestration by Kubernetes within the cluster requires reservation of private network segments for each Pod. Plan for network segmentation regardless of your deployment mode.

Note
Review the default IP range values for your pod and service networks in the following table. Use them if they are suitable and do not conflict with the deployed infrastructure network routing definitions. If there is a conflict, adjust the segment IP range as required.

Table 5: IP Address range for network segmentation

Restricted IP Range	Default Value	IP Address /Range
Pod Network IP Range	10.96.0.0/16	<reserved ip>/16
Service Network IP Range	10.97.0.0/16	<reserved ip>/16

VRRP operations require visual representation of where the IP addresses are allocated.

VRRP Configuration (Optional)

In support of load balancing and high-availability functions, the Universal Compute Platform relies on Virtual Router Redundancy Protocol (VRRP) to provide IP abstraction to key functionality. VRRP is critical in the configuration model.

The following operation settings must be defined as part of the VRRP configuration of member nodes:

- **Priority**— VRRP uses priority settings as a mechanism to arbitrate mastery of the state of exchanges across members of the cluster.
- **RouterID** — This setting allows segmentation of a routing domain, and it is important to separate from any other VRRP uses on the same network segment.

The assigned value is arbitrary, but the value must not overlap when another VRRP usage is visible in the attached network segments.

Note
In a stand-alone configuration, configure priority and router ID with a numeric value. However, in a stand-alone configuration, the specific value is not important. These attribute definitions are important in a multiple-node configuration.

Services VRRP Configuration

The VRRP configuration relates to the number of services you are exposing. Configure a VRRP IP address (VIP) for each service.

Table 6: Stand-Alone Configuration for Services VRRP Configuration

	Single Node (Port #)
Data Port (optional)	Node Port IP /CIDR
VLAN	VLAN Tagged/Untagged
Port type	Physical
VRRP (required)	
VRRP IP address (VIP)	VIP address
Priority	Numeric Value
Router ID	ID (1)

Firewall Requirements

The following connections are required during installation and upgrades so that Universal Compute Platform can download the appropriate packages.

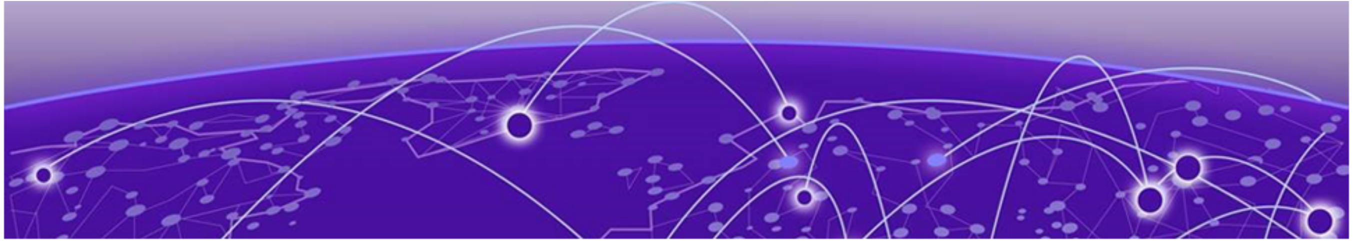
Table 7: Required Connections for Installs and Upgrades

Domain Name	IP Adresses	Protocol	Port
docker.io	Dynamic IP range	HTTPS	443
gcr.io	Dynamic IP range	HTTPS	443

The following connections are required if you connect to ExtremeCloud IQ.

Table 8: Required Connections for Cloud Deployments

Domain Name	IP Addresses	Protocol	Port	Description
hac.extremecloudiq.com	34.253.190.192 ~ 34.253.190.255	HTTPS	443	Onboarding to ExtremeCloud IQ
<rdc>-inlets.extremecloudiq.com	Dynamic IP range	TCP	8090	Ongoing connection to ExtremeCloud IQ



Configure an Appliance

Deployment of a Universal Compute Platform appliance involves the following steps:

1. Connect the 4120C hardware appliance to the network.
2. Run the Basic Configuration Wizard to deploy a fully-functioning appliance on a network.
3. Upgrade the Universal Compute Platform appliance firmware to the latest revision.
4. Validate the network settings and configure additional data plane interfaces if necessary.
5. Configure the Universal Compute Platform cluster creation.
6. Install and deploy the engine applications.

   You can install multiple instances of an application on an appliance.

After the engine application is deployed, refer to the documentation for the individual application for information on how to manage your network with that application.

Connect the Appliance Hardware

You can connect the appliance through the console port or through a serial port:

Connect to the Management Interface through the Console Port

Take the following steps to connect to the appliance through the console port:

1. Connect the laptop serial port to the 4120C console port.

   If the laptop does not support RS232 interface, then obtain a USB to RS232 converter cable, which then connects to the RJ45-DB9F cable.
2. Using PuTTY, TeraTerm, or another terminal emulator, connect to the serial port connection.

   Ensure that your serial connection is set properly with the following settings:

   - 115200 baud
   - 8 data bits

- 1 stop bit
- Parity none
- Flow control none

Note
The system's default gateway must be pointing to a next hop connection through the service ports.

3. Using the console session, access the Basic Configuration Wizard.

Related Topics

Use the Basic Configuration Wizard on page 13

Connect to the Management Interface through the ICC Port

You can retain the default IP address of the appliance management interface if you do not connect the appliance to your enterprise network. If you connect the appliance to your network, follow these steps:

1. Connect a laptop to the appliance management port.
2. Configure the Ethernet port of the laptop with a statically assigned unused IP address in the `192.168.10.0/24` subnet.
3. SSH to the appliance.

   `192.168.10.1` is the default IP address on the appliance management port).

   The Universal Compute Platform logon screen is displayed.
4. Using the console session, access the Basic Configuration Wizard.

Related Topics

Use the Basic Configuration Wizard on page 13

Basic Configuration Wizard

The Universal Compute Platform software provides a **Basic Configuration Wizard** that can help administrators configure the minimum settings necessary to deploy a fully functioning appliance on a network.

Administrators can use the wizard to quickly configure the appliances for deployment, and then after the installation is complete, continue to revise the configuration accordingly.

The wizard is automatically launched when an administrator logs on to the appliance for the first time, including after the system has been reset to the factory default settings.

The configuration wizard prompts with a set of **Yes** or **No** questions. The default value is indicated in parenthesis. To accept the default value, press **Enter**.

Related Topics

Use the Basic Configuration Wizard on page 13

Use the Basic Configuration Wizard

After logging into the appliance, the **Basic Configuration Wizard** displays. You are presented a set of **Yes** or **No** commands.

1. To begin the Admin password setup, press **Enter**. The **Admin Password Configuration** screen is displayed.

   The following is the default factory settings for a Universal Compute Platform appliance:

   - The default username is: admin
   - The default password is: abc123

   > Note
   > The values are case-sensitive.

   a. To change the password for the admin account, press **Enter**.

   b. Enter the new password for the admin account.

   > Note
   > The password must be between 8-24 characters.

   c. Repeat the new password for the admin account and press **Enter**.

   > Note
   > An Inter-Cluster Connection (ICC) is not required in a Standalone deployment.

2. Go to Data Port configuration.

Current Data Port Settings

After you set up the **Admin Password configuration**, you are prompted to set up the **Current Data Port Settings**:

1. Change Port 1 settings: Select the number that corresponds to the port you will configure as the data port, and press **Enter**.
2. Set the default IP address for the data port **`10.0.0.1`**, or type a new IP address and press **Enter**.

   The IP Address is selected.
3. Set the Netmask to the default **`255.255.255.0`**, or provide a new IP address and press **Enter**.

   The Netmask is set.
4. Default VLAN: Set the default VLAN ID, or provide a new VLAN ID and press **Enter**.
5. Tagged Frames: Set the tagged frames to **`No`**, or type `y` to set tagged frames.
6. Management Traffic (admin interface): Set `y` to enable management traffic on the interface, or type `n` to not enable management traffic, and press **Enter**.

7. To accept the changes and keep the data port settings you have chosen, press **Enter**.

   Note
   If you need to reconfigure the data port settings, enter `n` and select your data port again.

   The Data Port Interface is now set.

Current Host Attributes

To set up the current host attributes:

1. Press **Enter** to enter the host name for the appliance.

   Note
   The host name must be all lower case letters.

2. Type the IP address for the ICC port.
3. Domain name: Set the domain name to the default value **`extremenetworks.com`**, or enter a domain name and press **Enter**.
4. IP netmask: Set the IP netmask for the ICC port, or enter an IP address and press **Enter**.
5. Primary DNS server: Set the IP address for the primary DNS server, or enter another IP address and press **Enter**.
6. If you need a secondary DNS server, type `Y` and provide the IP address. Otherwise, press **Enter** to accept `No` as the default value.

   The updated Host Attribute settings are displayed.
7. To accept the changes you have made, press **Enter**.

   Note
   If you need to reconfigure the Host Attributes settings, enter `n` and enter the host name for the appliance again.

Current Global Default Gateway Settings

The global default gateway can be on any Admin or data port topology/subnet.

Note
The system's default gateway must be pointing to a next hop connection through the service ports.

Enter the default gateway:

1. Type an IP address.
2. Press **Enter** to accept the changes.

Current Time Settings

The Current Time Settings option allows you to change the time zone as per your location.

1. To set the Time Zone, press **Enter** . The Region number list is displayed.

   Important
   Ensure that Universal Compute Platform is configured with the correct Network Time Protocol (NTP) Server settings. Several system functions are dependent on an accurate timestamp.

2. Pick a number from those displayed on the screen that corresponds to the Continent. Then, enter a number that corresponds to the Region.

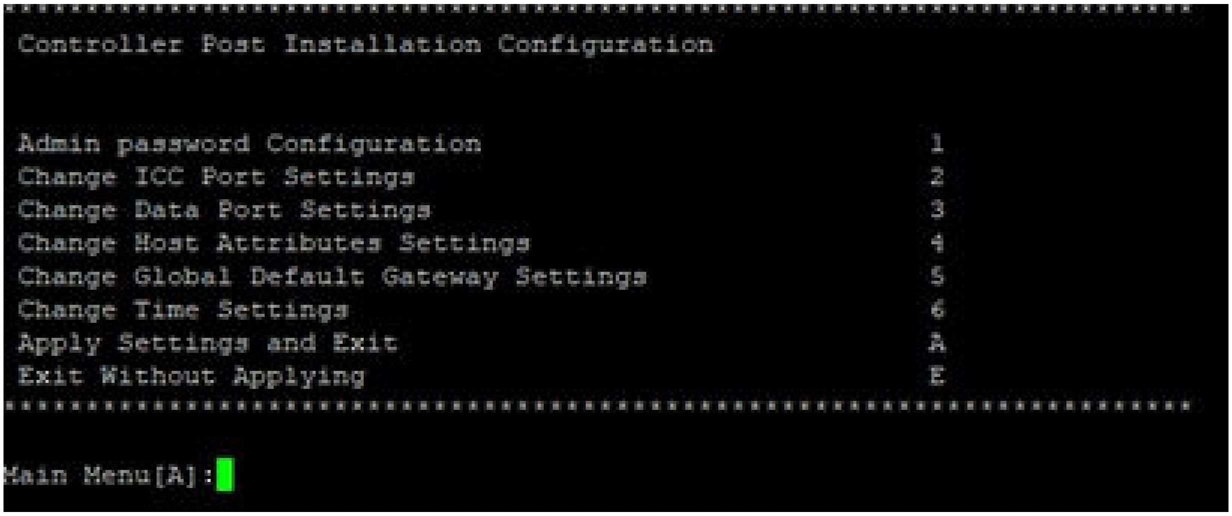
   You can enter **`n`** to move down the list, or **`p`** to move up the list. To go back to the Region selection, press **`c`**.

   For example, for Toronto select Americas (2) then Toronto (141).
3. Provide the fully qualified domain name or IP address of the NTP server. Press **Enter**.
4. You are prompted to enter a second NTP server and the default option is **`y`**. Type **`n`** and press **Enter**.

   NTP Client is enabled.
5. Accept the changes you have made to the time zone and NTP server by pressing **Enter**.

   Note
   If you need to reconfigure the current time settings, enter `n` and enter the settings again.

6. If you want to revisit any of the previous screens or exit without applying the configuration changes, enter one of the corresponding numbers/alphabets displayed on screen.



```
*************************************************************************
Controller Post Installation Configuration


Admin password Configuration                                   1
Change ICC Port Settings                                       2
Change Data Port Settings                                      3
Change Host Attributes Settings                                4
Change Global Default Gateway Settings                         5
Change Time Settings                                           6
Apply Settings and Exit                                        A
Exit Without Applying                                          E
*************************************************************************

Main Menu[A]:
```

Figure 1: Controller Post Installation Configuration Menu Screen

Table 9: Controller Post Installation Configuration Menu

Menu Option	Command
Admin password Configuration	1
Change ICC Port Settings	2
Change Data Port Settings	3
Change Host Attribute Settings	4
Change Global Default Gateway Settings	5
Change Time Settings	6
Apply Settings and Exit	A
Exit Without Applying	E

Note
An Inter-Cluster Connection (ICC) is not required in a Standalone deployment.

When you revisit any other screen, you will have to reconfigure all subsequent area settings. For example, if you decide to reconfigure the Admin Password, which is at the beginning of the configuration wizard, you will have to reconfigure all the subsequent configuration wizard settings.

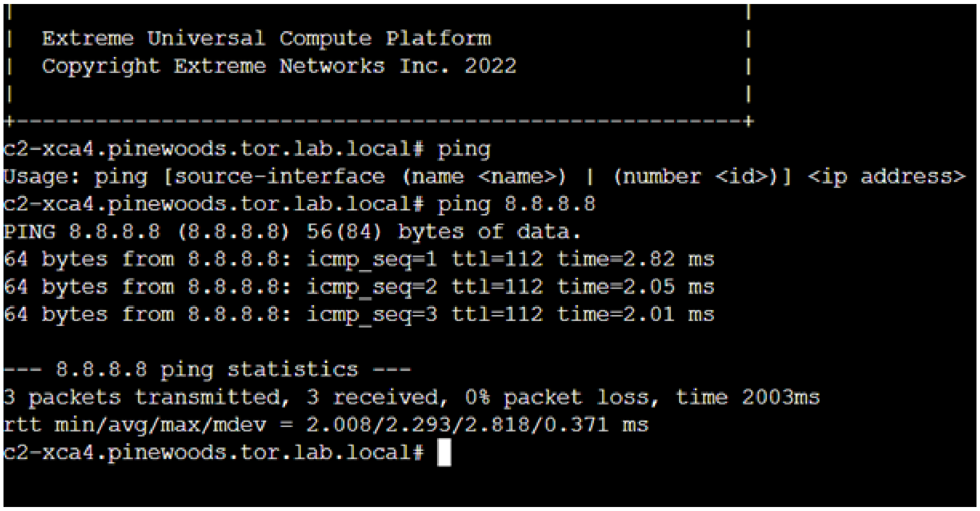
7. Press **Enter** to accept the settings. The default option for accepting the settings is `A`.

   Your settings are now applied successfully.

Test Connectivity

Test connectivity to the external services in the cluster using the `ping` command.

1. To test connectivity to external services such as DNS, ping the IP address of the DNS server.
2. Ping the cluster IP address to test connectivity.



```
|                                                       |
|  Extreme Universal Compute Platform                   |
|  Copyright Extreme Networks Inc. 2022                 |
|                                                       |
+-------------------------------------------------------+
c2-xca4.pinewoods.tor.lab.local# ping
Usage: ping [source-interface (name <name>) | (number <id>)] <ip address>
c2-xca4.pinewoods.tor.lab.local# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=112 time=2.82 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=112 time=2.05 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=112 time=2.01 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.008/2.293/2.818/0.371 ms
c2-xca4.pinewoods.tor.lab.local#
```

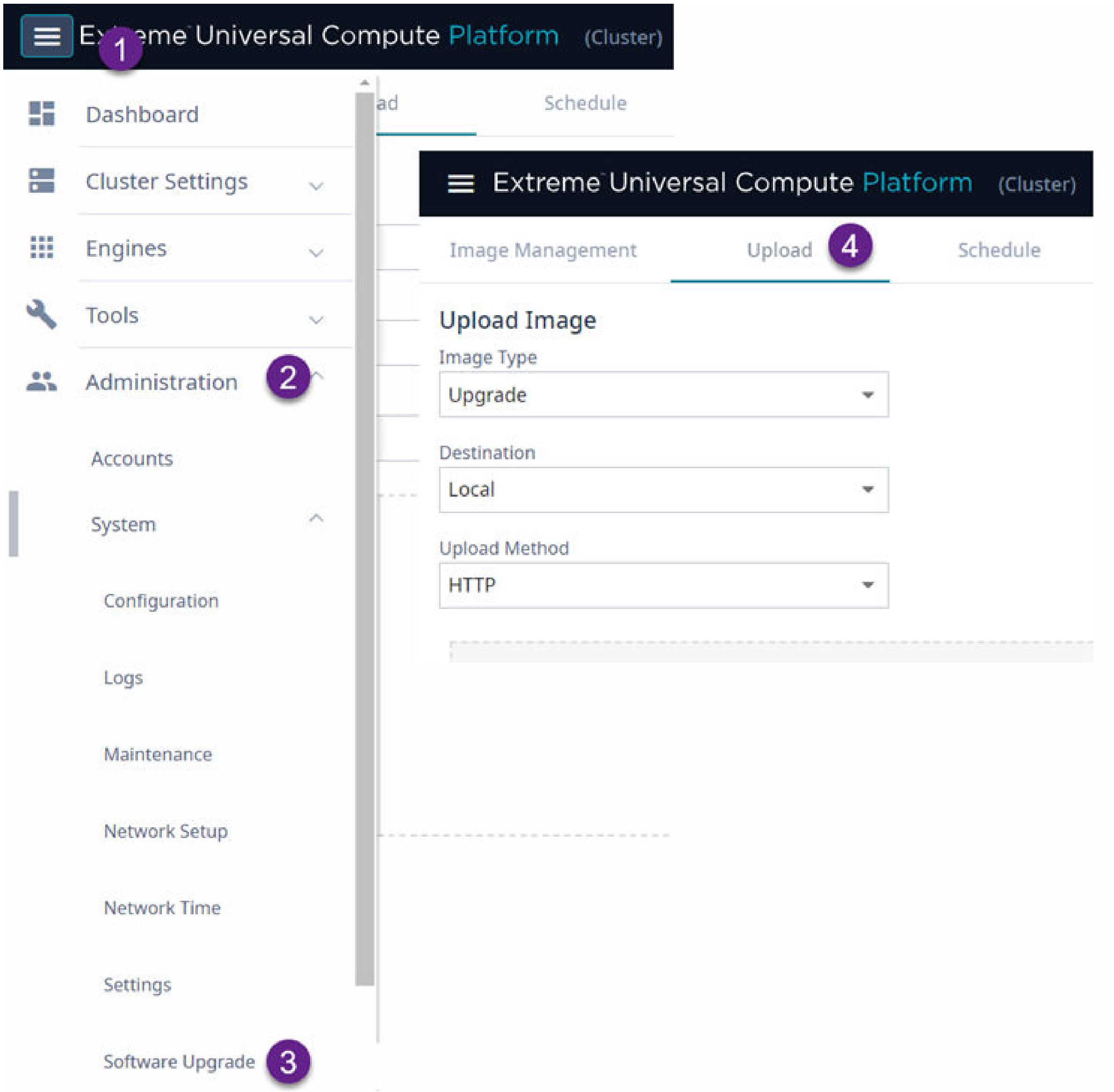
Figure 2: Example ping command

Upgrade the Appliance Universal Compute Platform

A best practice is to upgrade the appliance to the latest revision. Take the following steps to upgrade the Universal Compute Platform for the appliance:

1. Download the UCP image file from the Extreme Networks Support Portal. The image file extension is .rcx.
2. Log in to the appliance Admin user interface: https://*`node ip`*:5825

3. Go to **Administration** > **System** > **Software Upgrade** > **Upload**.



Upload Image

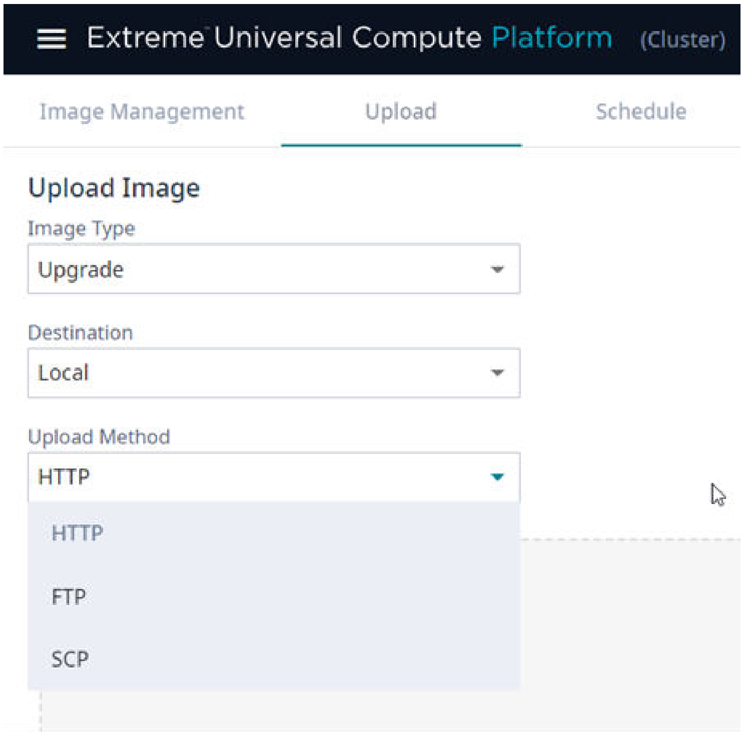
Image Type: Upgrade

Destination: Local

Upload Method: HTTP

Figure 3: Navigate to Universal Compute Platform Image Upload

4. Specify the Image upgrade settings:
   - Image Type
   - Destination
   - Upload Method. The available upload methods are HTTP, FTP, and SCP; HTTP is recommended.



Extreme Universal Compute Platform (Cluster)

Image Management | Upload | Schedule

Upload Image

Image Type: Upgrade

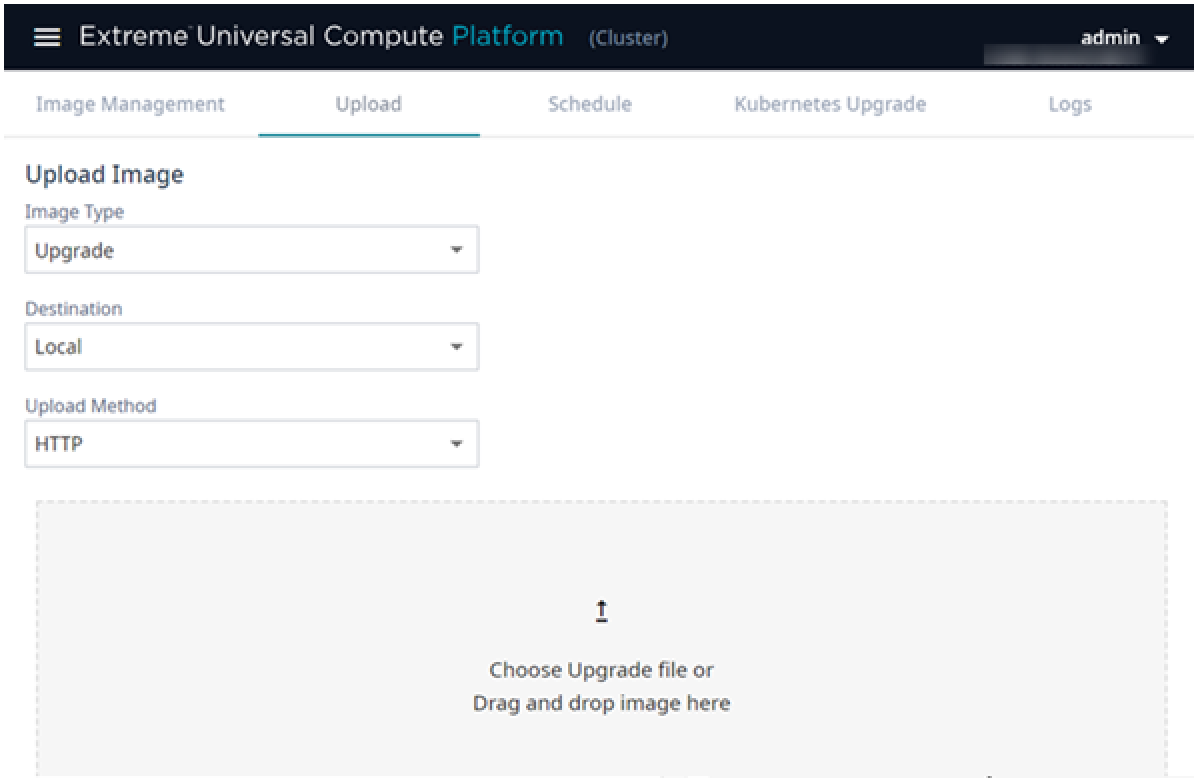
Destination: Local

Upload Method: HTTP

Figure 4: Upload Image Settings

5. Upload the desired revision of Universal Compute Platform.

   Select the **Choose Upgrade file pane** and navigate to the upgrade image or drag and drop the file on the upgrade pane.



Upload Image

Image Type: Upgrade

Destination: Local

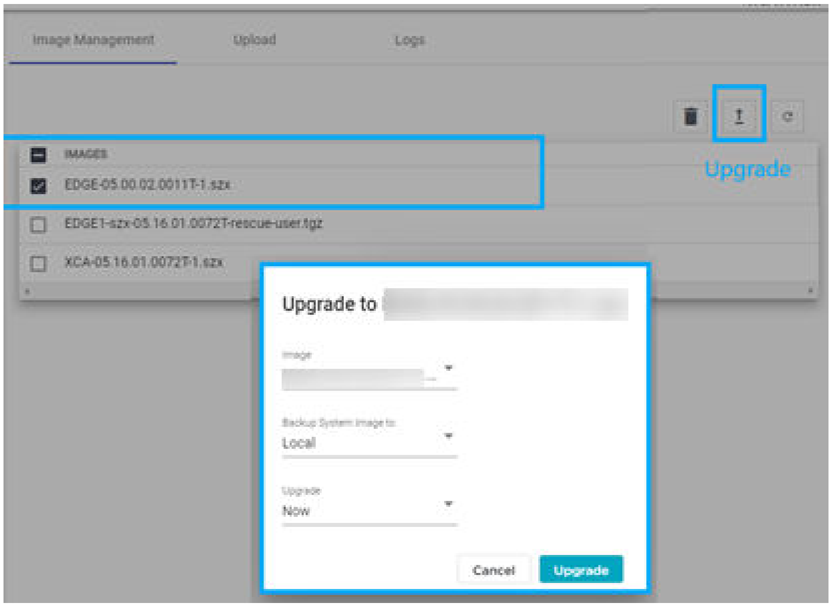
Upload Method: HTTP

Choose Upgrade file or
Drag and drop image here

Figure 5: Select the upgrade image

> Note
> The upgrade may take up to five minutes.

6. From the **Image Management** Tab, select the Upgrade image, and click **Upgrade**.



IMAGES

☑ EDGE-05.00.02.0011T-1.szx

□ EDGE1-szx-05.16.01.0072T-rescue-user.tgz

□ XCA-05.16.01.0072T-1.szx

Upgrade to

Image

Backup System Image to: Local

Upgrade: Now

Figure 6: Upgrade the selected image

When the cluster is upgraded to the latest revision, proceed to Validate the Network Address Configuration on page 21.

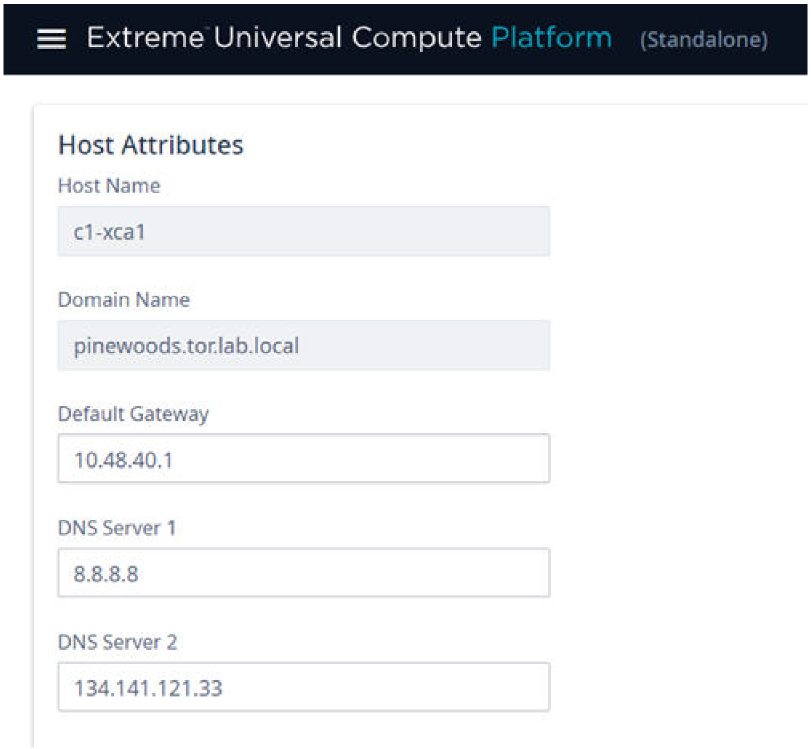
Validate the Network Address Configuration

Validate the IP addresses that you configured previously through the Configuration Wizard.

You can configure the engine instance IP address from the initial Configuration Wizard or from the Universal Compute Platform user interface.

To access the network settings in the user interface:

1. Go to **Administration** > **System** > **Network Setup**.
2. Verify the host attributes.



Extreme Universal Compute Platform (Standalone)

Host Attributes

Host Name: c1-xca1

Domain Name: pinewoods.tor.lab.local

Default Gateway: 10.48.40.1

DNS Server 1: 8.8.8.8

DNS Server 2: 134.141.121.33

Figure 7: Network Setup - Host Attributes

3. Select additional ports as necessary to display and verify the interface settings. If you make any changes to the additional interface settings, select **Save**.

> Note
> Configuring an engine instance IP address for the admin interface of the container application is useful for diagnostic purposes. The web interface can be accessed from the Engine Settings.

Related Topics

Use the Basic Configuration Wizard on page 13
(Optional) Add a Port on page 22
Engine Application Settings on page 32

(Optional) Add a Port

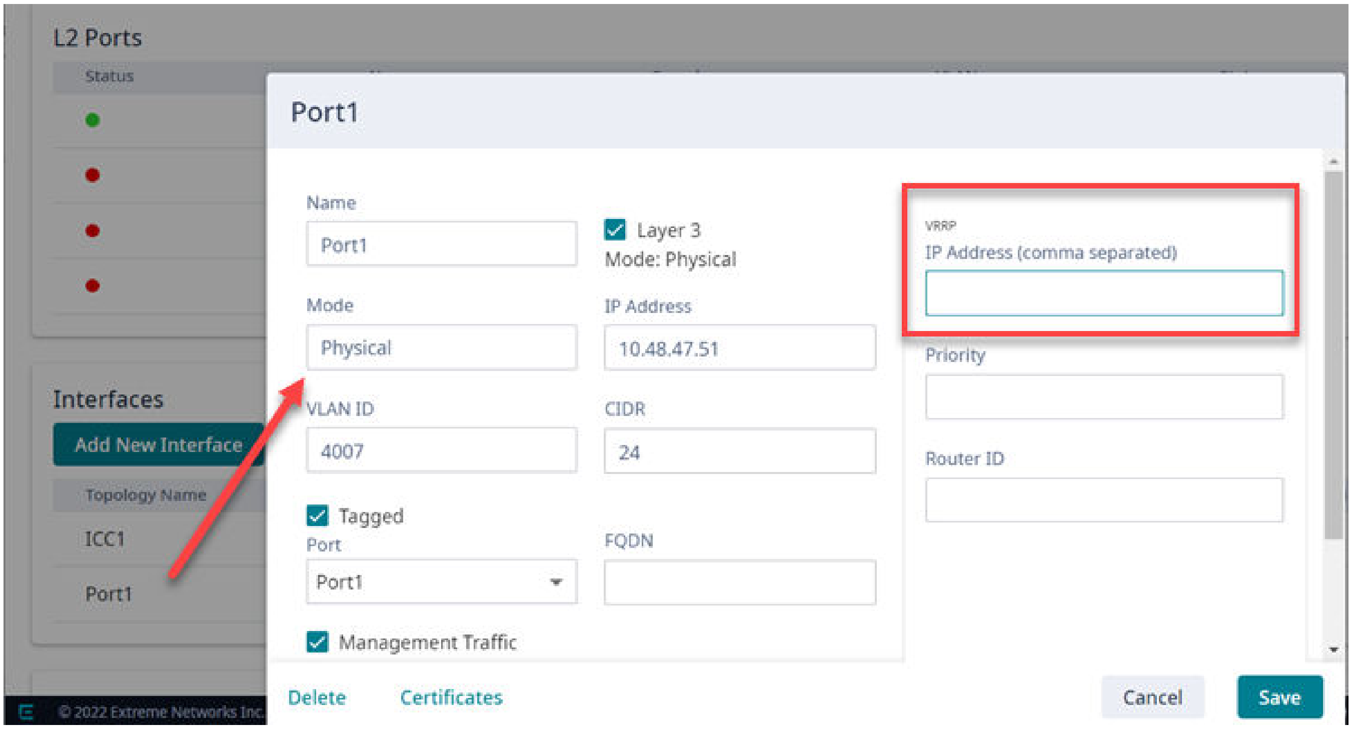
You have the option to add a port interface that provides access to the admin interface of the container application. This can be any data interface on the Universal Compute Platform.

> Note
> After you have defined an engine instance IP address for the container application admin interface, you are able to access that container application from a web browser through the defined IP address.

To add a new port interface, take the following steps:

1. Navigate to **Administration** > **System** > **Network Setup**.
2. From the **Interfaces** pane, select **Add New Interface**.
3. Configure the Interface Properties for the port.

   Provide a VIP for each engine instance in your deployment.



Name: Port1

☑ Layer 3
Mode: Physical

Mode: Physical

IP Address: 10.48.47.51

VLAN ID: 4007

CIDR: 24

☑ Tagged

Port: Port1

FQDN:

☑ Management Traffic

IP Address (comma separated):

Priority:

Router ID:

Figure 8: User Interface showing properties window for New Port

Related Topics

[Interface Properties] on page 23

Interface Properties

The following table provides details about Interface Properties.

Table 10: Interface Properties

Field	Description
Name	Name of the interface.
Mode	Describes how traffic is forwarded on the interface topology. Options are: • Physical - The topology is the native topology of a data plane and it represents the actual Ethernet ports. • Management - The native topology of the Universal Compute Appliance management port.
VLAN ID	ID for the virtual network.

Table 10: Interface Properties (continued)

Field	Description
Tagged	Indicates if the interface tags traffic. When traffic is tagged, the VLAN ID is inserted into the packet header to identify which VLAN the packet belongs to. Tagging can identify the port or interface to send a broadcast message to.
Port	Physical port on the Universal Compute Platform for the interface.
Management Traffic	Enable or disable Management Traffic through this interface. Enabling management provides access to SNMP (v1/v2c, v3), SSH, and HTTPs management interfaces.
MTU	Maximum Transmission Unit (MTU). Standard is 1500 bytes. Fixed value.
Layer 3	
IP Address	For an Admin topology, the Layer 3 check box is selected automatically. The IP address is mandatory for a Physical topology. This allows for IP Interface and subnet configuration together with other networking services.
CIDR	CIDR field is used along with IP address field to find the IP address range.
FQDN	Fully-Qualified Domain Name

Table 10: Interface Properties (continued)

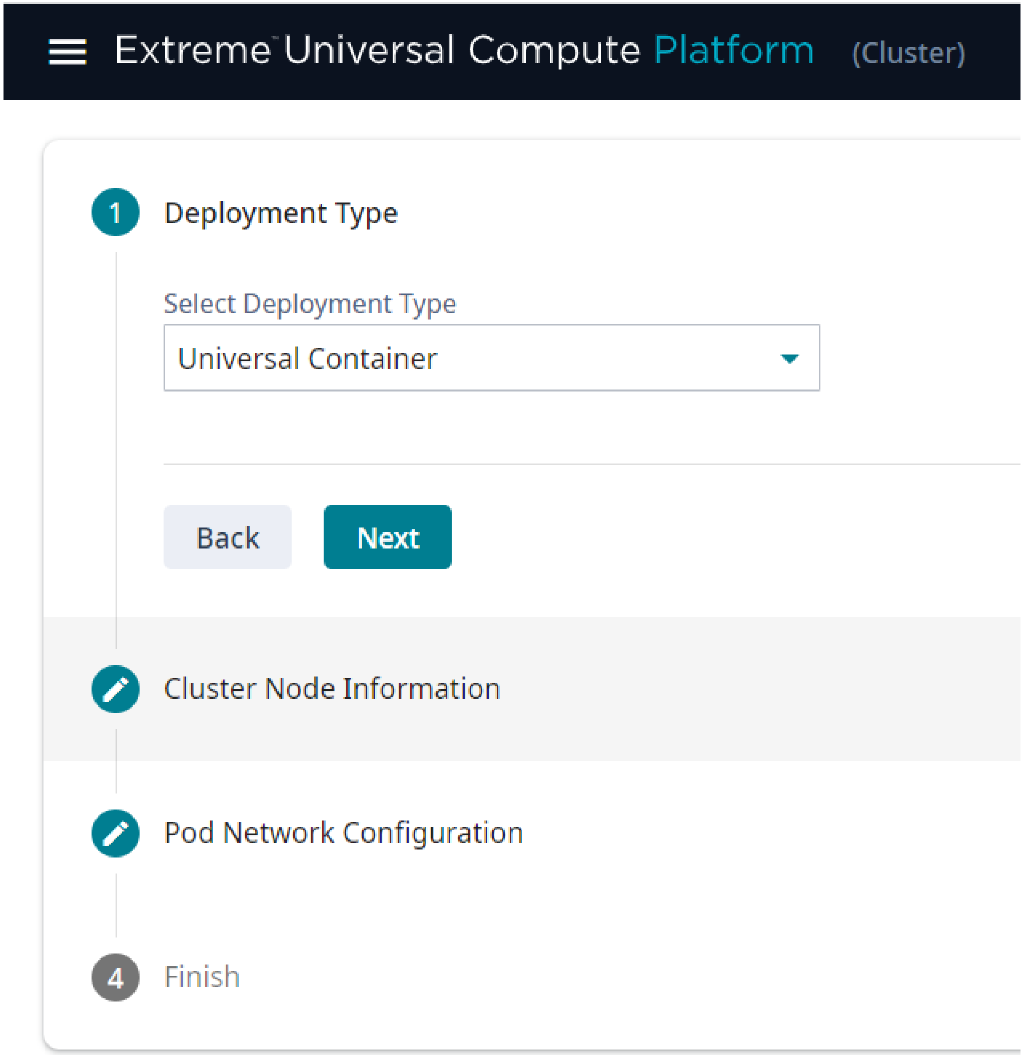
Field	Description
DHCP	Dynamic Host Configuration Protocol allows network administrators to centrally manage and automate the assignment of IP addresses on the corporate network. DHCP sends a new IP address when a computer is plugged into a different place in the network. The protocol supports static or dynamic IP addresses and can dynamically reconfigure networks in which there are more computers than there are available IP addresses. Valid values are: • None • Local Server. Indicates that the Universal Compute Appliance is used for managing IP addresses.
VRRP	Supports load balancing and high-availability functions for the Universal Compute Platform cluster. IP Addresses Record the IP address relationship between the cluster's direct interfaces, VRRP, and external access. Priority VRRP uses priority settings as a mechanism to arbitrate mastery of the state of exchanges across members of the cluster. Router ID Allows segmentation of a routing domain. Note: In a stand-alone configuration, configure priority and router ID with a numeric value. However, in a stand-alone configuration, the specific value is not important. These attribute definitions are important in a multiple-node configuration.

Configure the Stand-Alone Cluster Settings

An engine is an instance of a containerized application. This process follows the user interface to configure the orchestration engine settings for a stand-alone deployment. From the management IP address, log into the user interface using the admin credentials that you configured under Use the Basic Configuration Wizard on page 13.

Go to **Cluster Settings** > **Cluster Configuration** and configure the stand-alone cluster following the order shown on screen:

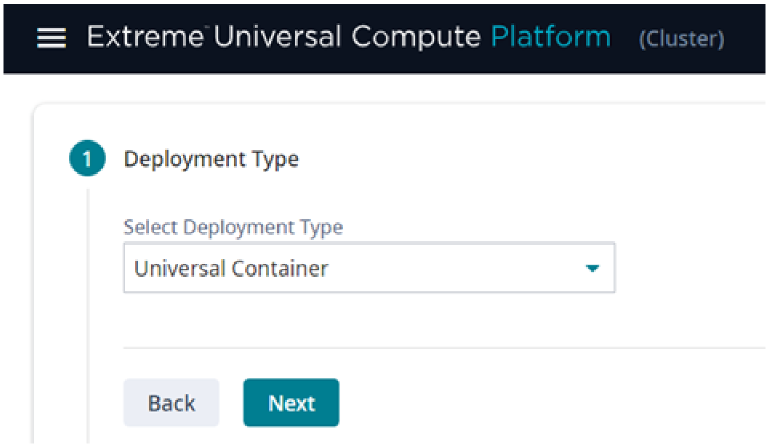
1. Deployment Type
2. Cluster Node Information
3. Pod Network Configuration
4. Finish


Extreme Universal Compute Platform (Cluster)
1 Deployment Type
Back
Next
Cluster Node Information
Pod Network Configuration
4 Finish

Select Deployment Type: Universal Container

Figure 9: Configure Cluster Settings for a Stand-Alone Deployment

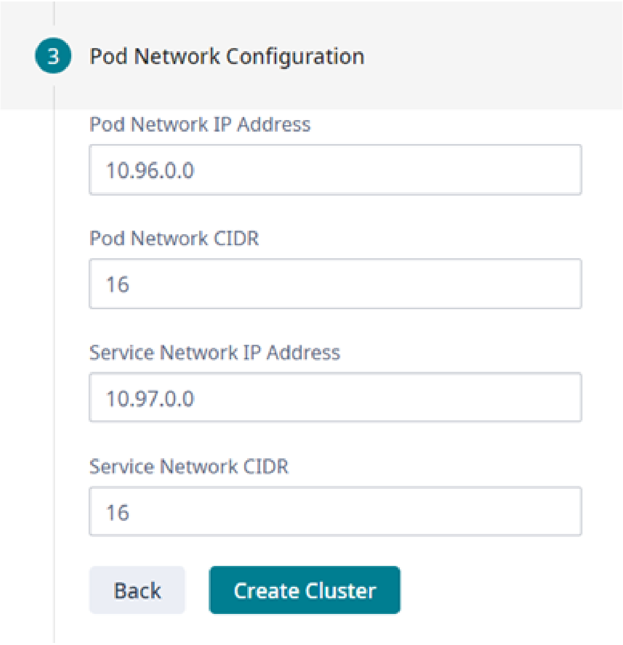
1. Select the **Deployment Type**. For this deployment, select **Universal Container**.



Select Deployment Type: Universal Container

Figure 10: Deployment Type Selection

2. In the **Cluster Node Information** section, select **Standalone** mode and click **Next**.
3. Provide the settings for **Pod Network Configuration**:
    - Pod Network IP Address
    - Pod Network CIDR
    - Service Network IP Address
    - Service Network CIDR



3 Pod Network Configuration

Pod Network IP Address: 10.96.0.0

Pod Network CIDR: 16

Service Network IP Address: 10.97.0.0

Service Network CIDR: 16

Figure 11: Pod Settings

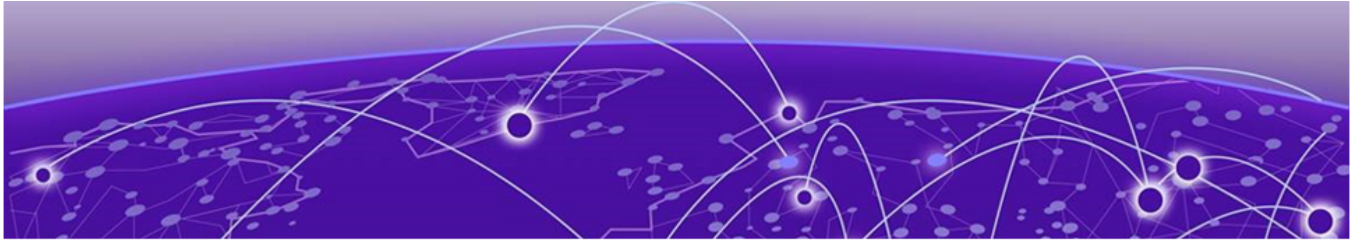
4. Select **Create Cluster**.
5. Select **Done**.

Note
The cluster state is bound to the IP Adresss of the ICC interface. If the ICC IP address is changed, the cluster state (even if Stand-Alone) is reset. Cluster configuration will need to be re-initialized and any installed applications will need to be re-installed.

Next, download the Docker image file to the specified node in the Universal Compute Platform deployment.

Related Topics

Initial Engine Application Installation on page 28



Initial Engine Application Installation

Installing an engine application in a Universal Container deployment involves the following tasks:

1. Download the Extreme Docker Application Image File.
2. Upload the Docker Application Image File to the UCP.
3. Install the application engine.
4. Deploy the application Docker image file.

Download the Extreme Docker Application Image File

Download the application Docker image file from the Extreme Networks support portal.

To obtain the Docker image file, go to the Extreme Networks support portal to download the application Docker image.

For example, from the ExtremeWireless WiNG™ product page, download `cx-9000.tar`.

Upload the Docker Application Image File to the UCP

To upload an engine application Docker image, take the following steps:

1. Go to **Engines** > **Image Management**.
2. Choose one of the following:
   - Select the **Choose Image File** pane and navigate to the image file. Or,
   - Drag and drop the image file onto the **Image File** pane.

   A list of uploaded image files is displayed below the **Choose Image File** pane.

To delete an uploaded image, select the check box next to the image file. Then, select 🗑. To refresh the image file list, select ⟳.

Install an Engine Application

To install the engine application, take the following steps:

1. Go to **Engines** > **Installation**.
2. From the pane for the application that you want to install, select **Install**.

   Note
   If you have not yet uploaded the application Docker image file, you will be prompted to do so.

   Note
   The installation time will depend on a variety of factors, be prepared for it to take some time.

   A confirmation notice is displayed after installation is complete. Only one instance is required for the cluster.

Deploy the Application Image File

After you have uploaded the application image file and installed the application Docker image, deploy the application to a node.

To deploy the application:

1. Go to **Engines** > **Installation**.
2. Select the engine instance link. For example, "cx9000 #1".
3. Select **Deploy**.
4. Save your changes.

Engine Upgrades

Universal Compute Platform has multiple methods for upgrading container applications. Select the upgrade method that fits your application type:

- Self-Orchestrated applications—For self-orchestrated applications that support external upgrades, see Upgrade an Application (Self-Orchestrated) on page 30.
- Applications with built-in upgrade functionality—For applications with built-in upgrade functionality, you can upgrade from the application interface. Refer to the application documentation for details.
- Applications that do not support either upgrade method—For these applications, uninstall the current image and then install the new image. Note that this method requires you to reconfigure your settings.

Upgrade an Application (Self-Orchestrated)

Use this procedure to upgrade a self-orchestrated engine application from the Universal Compute Platform user interface. This procedure upgrades the application while retaining existing settings.

> Note
> You must have the new application image file. For Extreme Networks applications, download the install image from the *Extreme Networks Support Portal* and save it to a local drive.

1. Log in to the Universal Compute Platform interface.
2. Upload the new application image file:
   a. Go to **Engines** > **Image Management**.

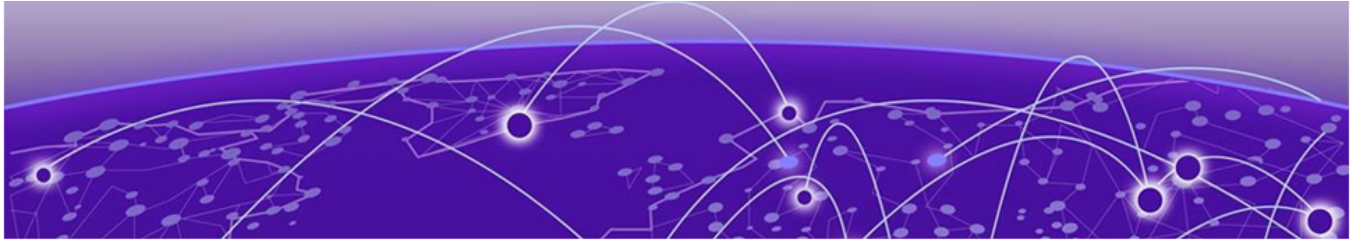
      A list of uploaded images displays under the **Choose Image File** pane.

   b. To upload the new image, complete either of the following steps:
      - Select **Choose Image File**, then browse to the image file and select it. Or,
      - Drag the image from your local drive and drop it on the **Choose Image File** pane.

      > Note
      > To delete an image file, select the check box next to the image and select 🗑.

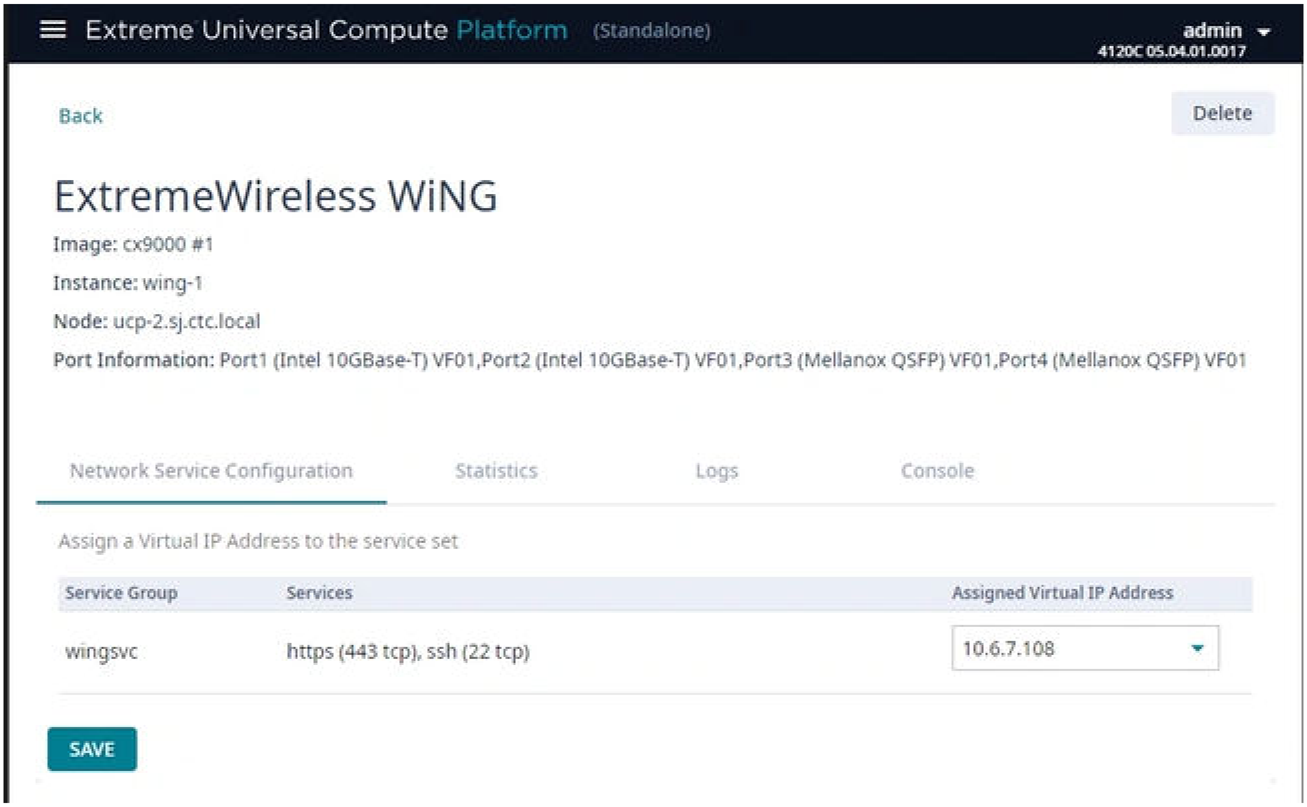
3. Upgrade the application:
    a. Go to **Engines** > **Installation**.
    b. Select the application instance that you want to upgrade.
    c. Select **Upgrade application**.
    d. Select **OK**.

       Universal Compute Platform creates a new container with the upgraded application image and existing settings. The old container is terminated.



Engine Application Settings

For each engine instance, select the instance link to configure the application settings and view the following information:


Extreme Universal Compute Platform (Standalone)
admin
4120C 05.04.01.0017
Back
Delete
Network Service Configuration
Statistics
Logs
Console
SAVE

ExtremeWireless WiNG

Image: cx9000 #1

Instance: wing-1

Node: ucp-2.sj.ctc.local

Port Information: Port1 (Intel 10GBase-T) VF01,Port2 (Intel 10GBase-T) VF01,Port3 (Mellanox QSFP) VF01,Port4 (Mellanox QSFP) VF01

Assign a Virtual IP Address to the service set

Service Group	Services	Assigned Virtual IP Address
wingsvc	https (443 tcp), ssh (22 tcp)	10.6.7.108

Figure 12: Example Engine Application Settings

Image

Controller image name.

Instance

Name of the node instance (provided by Universal Compute Platform)

Instance Web Interface

The assigned IP address of the Engine instance. This option provides the ability to log into the specific Engine instance.

1. Configure the interface from the **Interfaces** pane. Go to **Administration** > **Network Setup**.

2. Select the configured IP address from the **Assigned Virtual IP Address** field. Note, only IP addresses configured through **Network Setup > Interfaces** will appear in the drop-down list.
3. Log in through the console.

Network Service Configuration

The mapping of each core service set to the corresponding Virtual Router Redundancy Protocol (VRRP).

VRRP enables a virtual router to act as the default network gateway, improving host network reliability and performance.

Statistics

Compute statistics and node drive volume statistics are available for CPU usage and memory usage.

Logs

A log file is available for each node instance. Log entries include the following:

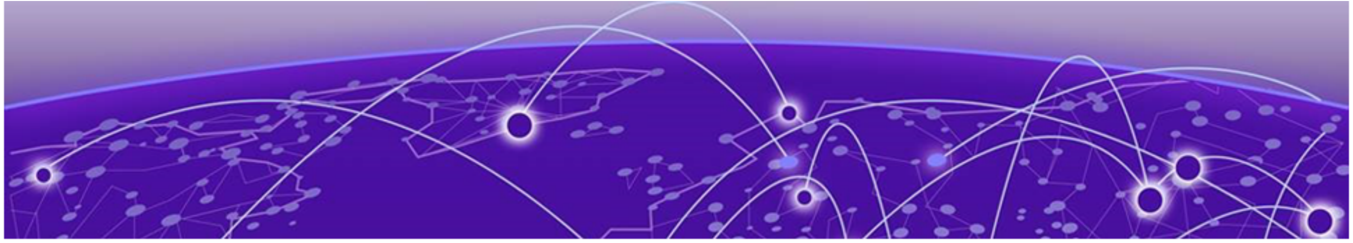
- Timestamp of log entry
- System Component
- Message log level
- Message content

Console

A live console is available from each engine instance for diagnostics and troubleshooting. To open a live console and connect to a container or virtual machine instance (VMI), from the engine **Console** tab, select **Attach**.

Related Topics

(Optional) Add a Port on page 22



Onboard Cluster to ExtremeCloud IQ

Note
For Self-Orchestrated deployments, onboarding to ExtremeCloud IQ is optional. Use the topics in this section only if you plan to onboard to ExtremeCloud IQ.

After the Universal Compute Platform cluster is installed, associate the node cluster with your ExtremeCloud IQ account:

1. From Universal Compute Platform, configure cloud visibility. See Cloud Visibility on page 34.
2. Onboard the cluster to your ExtremeCloud IQ account. See Onboarding a Cluster to ExtremeCloud IQ on page 35.
3. Onboard your devices and operate the account.

Cloud Visibility

Typically, the connection between Universal Compute Platform and your ExtremeCloud IQ Regional Data Center (RDC) is made through automatic discovery. Use this procedure to create the connection manually.

1. From the Universal Compute Platform user interface, go to **Administration** > **System** > **Settings** > **Cloud Visibility**.
2. In the **Cloud Address** field, enter your ExtremeCloud IQ account address, which is derived from your ExtremeCloud IQ URL.

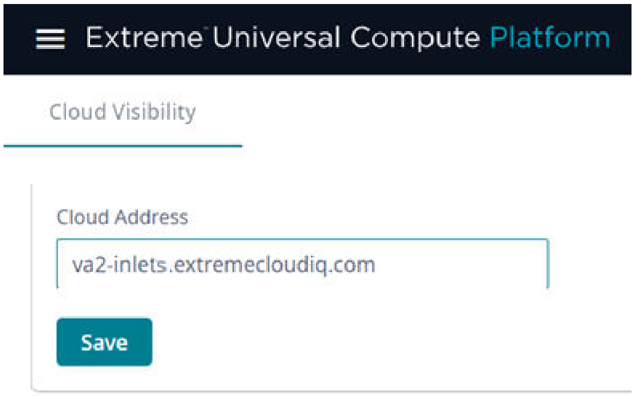
   ```
   rdc-inlets.host address
   ```

   For Example:

   Derive the Cloud Address from the following ExtremeCloud IQ URL: *https://va2.extremecloudiq.com/*

   Cloud Address: `va2-inlets.extremecloudiq.com`, where:

   - va2 is the cloud account RDC
   - **-inlets** is added after the RDC
   - .extremecloudiq.com is the host address



Cloud Address: va2-inlets.extremecloudiq.com

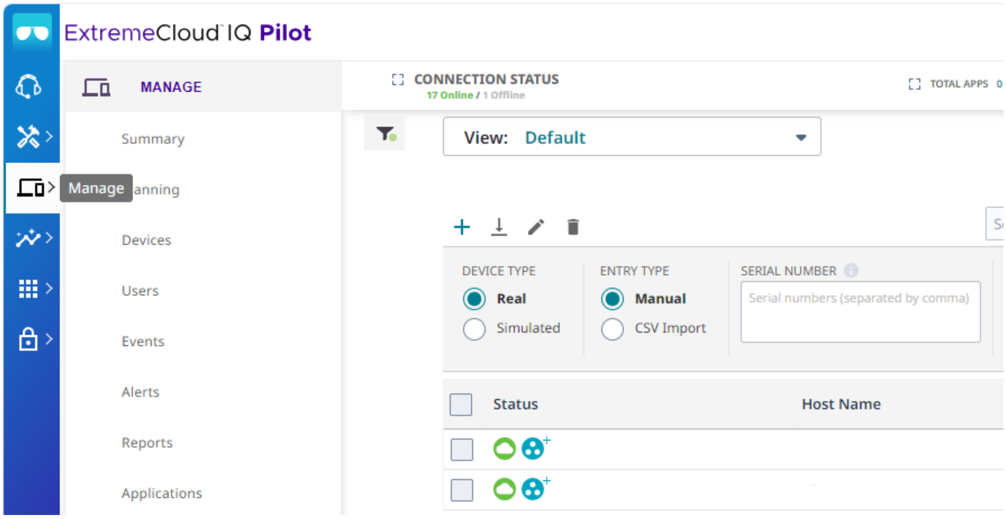
Figure 13: Cloud Visibility: ExtremeCloud IQ Address

3. Select **Save**.

Onboarding a Cluster to ExtremeCloud IQ

To onboard a Universal Compute Platform cluster into ExtremeCloud IQ use the ExtremeCloud IQ Quick Add function:

1. From the ExtremeCloud IQ main navigation pane, select (Manage), and then select **Devices**.
2. Select + **(Add)** and then select **Quick Add Devices** > **Manage your devices directly from the cloud**.
3. In the **Serial Number** field, enter the serial number for one node in the cluster.



View: Default

DEVICE TYPE: ● Real ○ Simulated

ENTRY TYPE: ● Manual ○ CSV Import

SERIAL NUMBER: Serial numbers (separated by comma)

Figure 14: Add Cluster to ExtremeCloud IQ

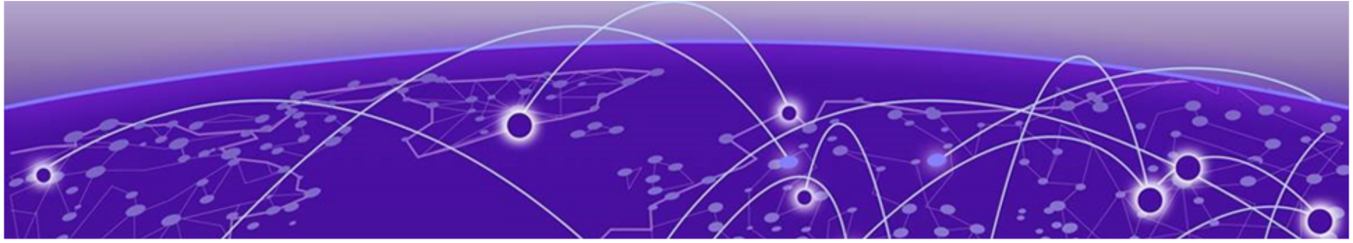
The **Device Make** field displays.

4. From the **Device Make** menu, select **Universal Appliance**.

5. Select **Add Devices**.

   The full cluster is added based on the serial number of a single node in the cluster.

   Note
   To view details about the cluster, select the **Host Name** link.



Index