ExtremeCloud Edge v5.12.01 Self-Orchestration Deployment Guide

Configuration and Management for Universal Compute Platform

9039417-00 Rev. AA
September 2025

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: https://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/

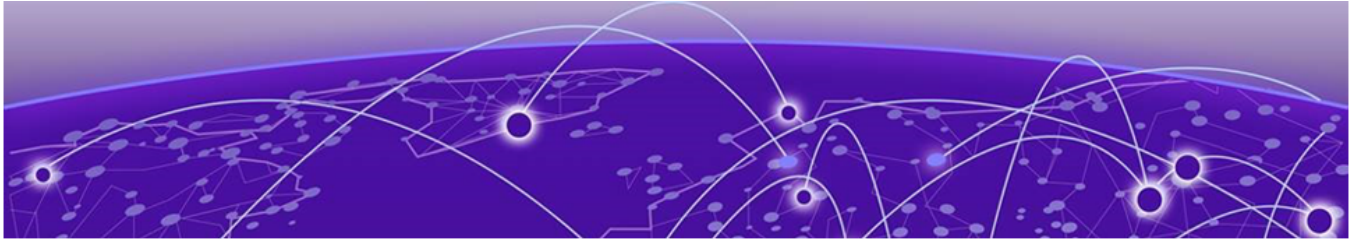
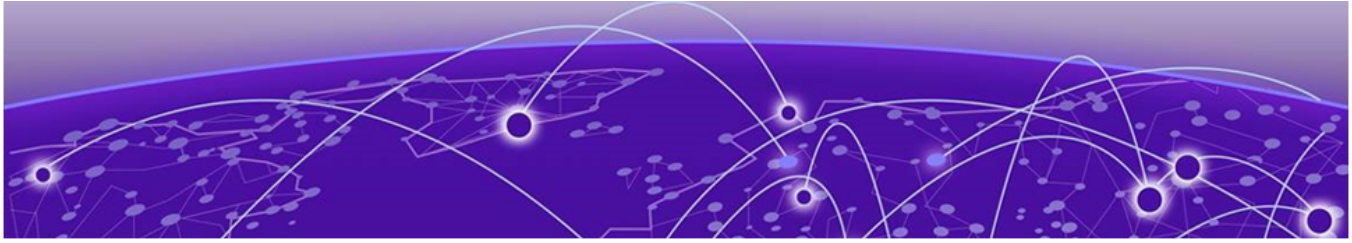


Table of Contents



Abstract

The ExtremeCloud Edge v5.12.01 Self-Orchestration Deployment Guide provides in-depth technical guidance for deploying the Universal Compute Platform with self-orchestration capabilities. This version of the guide features a revision to the prerequisite firewall rules. Architecture details for Self-Orchestration focus on the orchestration layer, automated provisioning pipelines, and integration with network and cloud infrastructures. Key deployment processes include configuring system prerequisites, establishing deployment pipelines, and executing end-to-end orchestration workflows. Advanced troubleshooting techniques, optimization strategies, and best practices are provided to resolve common deployment challenges and ensure optimal performance. This resource is designed for system architects and IT professionals overseeing large-scale, automated Universal Compute Platform implementations.

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, the product is referred to as *the switch*.

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 Product-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.

Introduction

This guide provides the steps needed to bring a stand-alone Universal Compute Platform online in ExtremeCloud Edge - Self-Orchestration mode. 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.

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

Self-Orchestration

Deploy Universal Compute Platform in ExtremeCloud Edge - Self-Orchestraton (standalone mode) with a set of Universal Container applications.

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

- All IP addresses must be unique within their corresponding segments.
- The use of the Virtual IP Address (VIP) is optional, but for some applications 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
It's mandatory to configure an IP address for the ICC1 port, even in a Standalone deployment. However, connectivity for the ICC1 port is not required.

Related Links

Reserved IP Addressing on page 18
VRRP Configuration (Optional) on page 18

Supported Hardware for Self-Orchestration

ExtremeCloud Edge - Self-Orchestration deployments of Universal Compute Platform support the following hardware appliances. Depending on the hardware, you may be able to install more than one instance of an application on a node.

Table 4: Supported Hardware for ExtremeCloud Edge - Self-Orchestration

Hardware Appliance	Details
1130C	Ports: • 2 x 1 Gbps ICC Ports/RJ45 • 4 x 1 Gbps Data 1-4/RJ45 Self-Orchestration deployment application capacity: • Tunnel Concentrator—One instance per node • ExtremeCloud IQ Controller (CE1000)—One instance per node For additional server specifications, along with hardware installation information, see Extreme Networks Universal Compute Platform Appliance 1130C Installation Guide.
2130C	Ports: • 2 x 1/10 Gbps ICC Ports/RJ45 • 2 x 10 Gbps Data Ports 1-2/SFP28 • 2 x 10/25 Gbps Data Ports 3-4/SFP28 Self-Orchestration deployment application capacity: • Tunnel Concentrator—One instance per node • ExtremeCloud IQ Controller (CE2000)—One instance per node • ExtremeCloud IQ - Site Engine—One instance per node • ExtremeControl—One instance per node • ExtremeAnalytics—One instance per node For additional server specifications, along with hardware installation information, see Extreme Networks Universal Compute Platform Appliance 2130C Installation Guide.

Table 4: Supported Hardware for ExtremeCloud Edge - Self-Orchestration (continued)

Hardware Appliance	Details
3150C	Ports: • 2 x 1/10 Gbps ICC Ports/RJ45 • 2 x 10/25 Gbps Data Ports 1-2/SFP28 • 2 x 10/25/50/100 Gbps Data Ports 3-4/QSFP28 Self-Orchestration deployment application capacity: • Tunnel Concentrator—One instance per node • ExtremeCloud IQ Controller (CE3000)—One instance per node For additional server specifications, along with hardware installation information, see Extreme Networks Universal Compute Platform Appliance 3150C Installation Guide
4120C/4120C-1	Ports: • 2 x 1/10 Gbps ICC Ports/RJ45 • 2 x 1/10 Gbps Data 1-2/RJ45 • 2 x 1/10/25/40/50 Gbps Data 3-4/QSFP Self-Orchestration deployment application capacity: • Tunnel Concentrator—Up to three instances per node. • ExtremeWireless WiNG (CX9000)—One instance per node For additional server specifications, along with hardware install information, see Extreme Networks Universal Compute Platform Appliance 4120C Installation Guide.

Note
Support is for a single application type per node. Application mixing on a single appliance is not supported.

Kubernetes

Universal Compute Platform is built on Kubernetes middleware. Kubernetes provides a unifying structure for application delivery and provides integrated management of application state along with clustering capabilities.

Kubernetes components must be downloaded and installed during the cluster configuration stage. After you select the cluster type and initialize the cluster (a **Standalone** cluster for Self-Orchestration deployments), the appliance connects to Docker Hub to download and install the additional Kubernetes components based on your installation requirements.

Note
Internet access is required during installation so that the required components can be downloaded. For details, see Firewall Requirements on page 17.

After the Standalone cluster is created, Kubernetes binds to the ICC IP address (either the physical ICC IP address or VRRP IP, if it's configured). Due this binding, an ICC IP

address is required for all Self-Orchestrated deployments, although ICC connectivity is not required.

Note

- Because of the ICC binding, it's recommended to use the data ports for application management rather than the ICC ports.
- Do not change the ICC addressing scheme, the hostname, or the domain name, once they are assigned. If you change the ICC IP address or ICC VRRP address, the Kubernetes binding breaks, and the Kubernetes installation unwinds, effectively wiping out the installation. In this case, the only fix is to reinstall and reconfigure. The user interface prevents modification of these parameters to preserve the integrity of the system. If adjustments are required, the node must be reset.
- Kubernetes requires the reservation of two /16 subnets for use by the Pod and Service Networks (the default ranges are 10.96.0.0 and 10.97.0.0). Make sure that the ranges that you use do not overlap with routing domains.

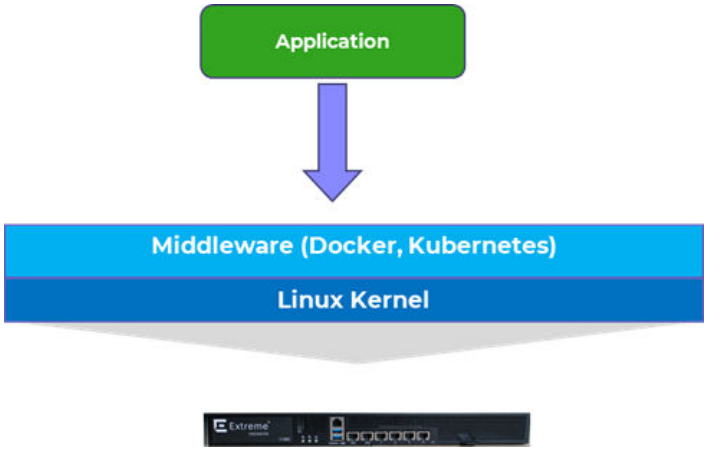


Figure 1: Kubernetes Middleware Layer

Network Architecture

Each Universal Compute Platform appliance has two ICC ports and four data ports.

Access to the data interface of Universal Compute Platform is abstracted through the use of internal virtual switches where each data port has a dedicated vSwitch (four in total). All external connections to the data interface pass through one of these vSwitches.

Each vSwitch has between eight and 16 virtual functions (VFs) that let you run multiple application instances over the same data port. Each VF + vSwitch combination has a unique MAC address. For each installed application, you must allocate a VF on each data port to that instance. Additional application instances must be assigned to a different VF. For example, if you assign the default VF assignments on all ports, a 4120C with three Tunnel Concentrator instances uses VF01, VF02, and VF03 on each port to manage the three application instances.

When you run multiple application instances on an appliance, the instances share the same port and switch, but the attachment point is different at the PCI level. The installed application instances attach to the vSwitch, but the applications see those attachment points as PCI interfaces that are mapped to a VF, and bound to a physical data port.

Note
The 1130C has eight VFs for each vSwitch. All of the other supported appliances have 16 VFs per vSwitch. For example, a 2130C has 70 MAC addresses: two MACs for the ICC ports, four MACs for the data ports, plus 64 VF-related MACs.

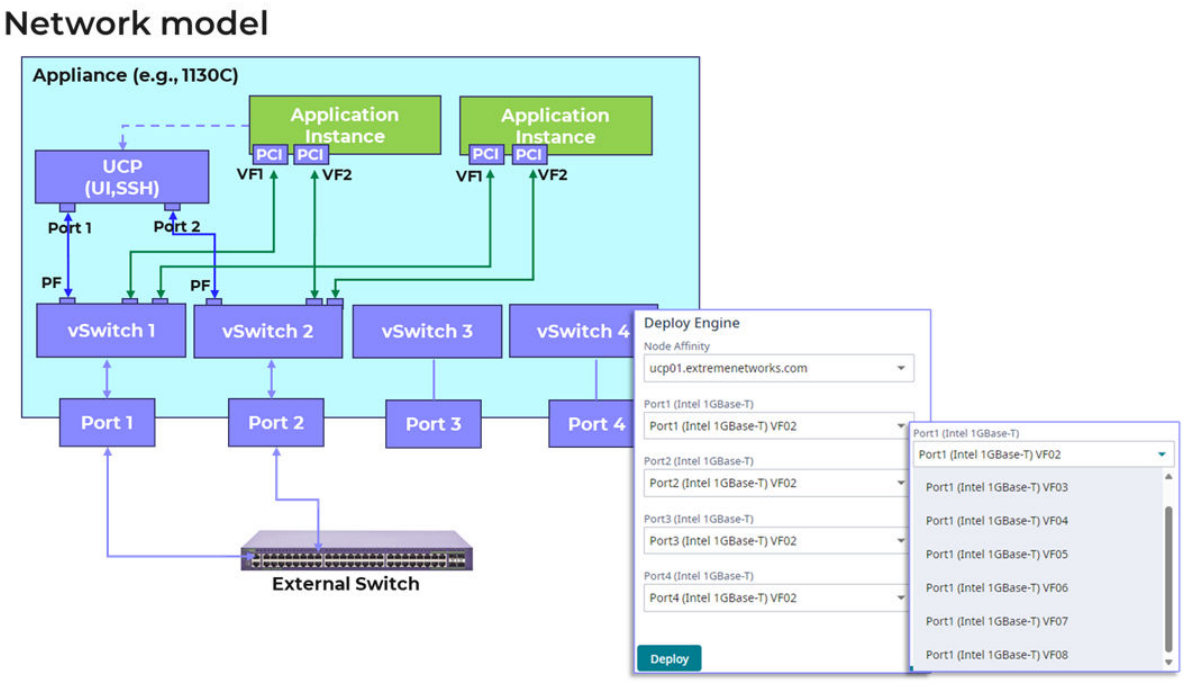
Universal Compute Platform OS Access

The Universal Compute Platform OS and management application shares access to resources with the installed applications. The Universal Compute Platform attaches to the physical function of the vSwitch, which provides more privileged access to port functions.

The installed applications have an internal hook to the Universal Compute Platform host through an internal NAT interface (10.0.2.2/24) back into the host. Application can use this connection for API REST calls to complete various tasks such as checking interfaces.

Example

The following image illustrates the network connections on an 1130C that has two application instances that use VF01 and VF02 respectively. The Universal Compute Platform OS attaches to the physical function (PF) of vSwitch 1 and vSwitch 2. The user interface callouts display how, for each data port, you can allocate one of eight VFs to that application instance.

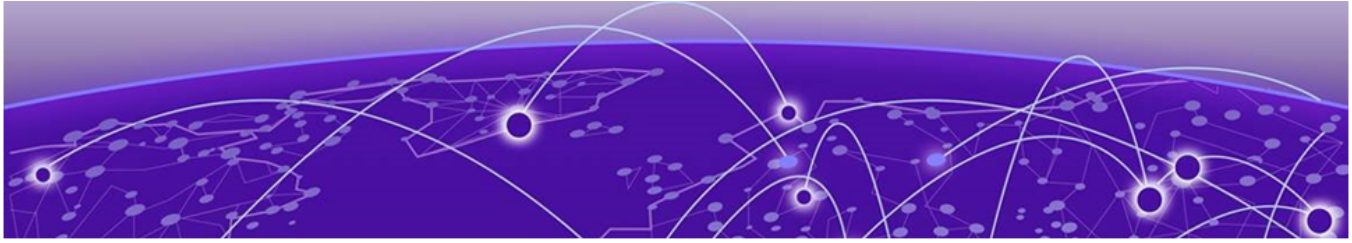


High Availability

Most Self-Orchestrated applications are not designed to use the clustering capability of Kubernetes. For these applications, High Availability is provided by the application, rather than by the Universal Compute Platform.

To configure High Availability for most Self-Orchestration applications, configure separate standalone clusters and then configure HA at the application level. For example, the following image displays a High Availability setup for a CE1000 Deployment of ExtremeCloud IQ Controller. In this example, High Availability is provided at the application level.

Figure 2: High Availability for Self-Orchestrated Applications



Requirements

Firewall Requirements

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

Table 5: 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
ghcr.io	Dynamic IP range	HTTPS	443
quay.io	Dynamic IP range	HTTPS	443
registry.k8s.io	Dynamic IP range	HTTPS	443

Internet connectivity is required in these situations:

- During installation and setup of the Universal Compute Platform appliance, up to and including the creation of the stand-alone cluster.
- Upgrades of Universal Compute Platform appliance software.
- For Cloud Connected use cases, connectivity to ExtremeCloud IQ services is required to facilitate the onboarding. For details, see Table 6.

Once the stand-alone cluster is created, internet connectivity is not required while installing, upgrading, or running application engines that run on the appliance (unless the specific application engine requires it, or unless you onboarded to the cloud).

Note
If the appliance is to be deployed as an air gap use case, the initial configuration of the host needs to take place in a staging location where internet services are available (for example, DNS, NTP and Docker access). Once the node is initialized to support the target application, the appliance can be moved to its target location.

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

Table 6: 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

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 7: 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
Application Network IP Range	10.0.2.0/24	<reserved ip>/24

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

VRRP Configuration (Optional)

The Universal Compute Platform relies on Virtual Router Redundancy Protocol (VRRP) to provide IP abstraction to key functionality. If you are using VRRP, the following settings must be defined per intended interface:

Note

- VRRP IPs must be within the same segment as configured for the interface.
- VRRP IP addresses must not overlap with any other address in use in the segment.

- **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.

Note
For some applications, access to their management interface, or user interface, is configured as a pass-through Universal Compute Platform data interface by leveraging VRRP to create an alias IP. Make sure that the VRRP IP addresses that you use are not in conflict with any other IP in the segment, including addresses that are assigned by the application.

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 8: 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)

Configure an Appliance

To configure the appliance for an ExtremeCloud Edge - Self-Orchestration deployment, complete the following tasks.

Table 9: Configure an Appliance Task Flow

Step	Procedure	Description
1	Connect to the Management Interface through the Console Port on page 21	Connect the hardware appliance to the network.
2	Use the Basic Configuration Wizard on page 22	Run the wizard to deploy a fully-functioning appliance on a network.
3	Upgrade the Appliance Universal Compute Platform on page 27	Upgrade the Universal Compute Platform appliance software to the latest revision
4	Validate the Network Address Configuration on page 29	Validate network settings and configure additional data plane interfaces, if necessary.
5	Configure the Stand-Alone Cluster Settings on page 33	Configure the Universal Compute Platform cluster creation.

What to do Next

Go to the chapter Engine Application Installation on page 35 to install and deploy the engine application.

Connect to the Management Interface through the Console Port

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

Note
Alternatively, you can also use the ICC interface. For details, see Connect to the Management Interface through the ICC1 Port on page 21.

1. Connect the laptop serial port to the console port on the hardware appliance.

   Note
   If the laptop does not support RS232 interface, then obtain a USB to RS232 converter cable, which then connects to one of the following connections:
   - RJ45-DB9F cable—for 1130C, 4120C
   - Null Modem DB9 F-F (Female to Female)—for 2130C, 3150C

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.

Connect to the Management Interface through the ICC1 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.

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.

Note
The wizard prompts you with a series of yes or no, multiple choice, or manual entry questions that you must answer with the desired configuration settings. The following conventions apply:

- The value in the `[square brackets]` represents the default value that gets applied if you press `Enter` without making a specific selection.
- Settings in the `(round brackets)` represent a list of options from which you must make a single selection, for example `(y|n)[y]` where `y` and `n` are options, and `y` is the default.
- You must press the `Enter` key after each entry to input the selection.
- For IP address and netmask settings where a `[default]` value displays, press `Enter` to select the default value, or enter a new value. If a `[default]` value doesn't display, you must enter a new value.
- After you assign all settings within a group, you must accept the changes for that group before moving to the next group of settings. Otherwise, you can reject the changes for that group and reconfigure the settings.

Related Links

Use the Basic Configuration Wizard on page 22

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**.
d. Press **Enter** to accept the changes

2. To update the ICC1 (Admin Port):

Note
- An IP address configuration for the ICC1 port is required, though ICC1 network connectivity is not required. In most cases, the ICC1 interface's factory-default settings are sufficient. However, if these defaults conflict with existing routing paths within your organization, modify the configuration to prevent any overlap.
- VRRP and LAG are not required for Standalone deployments.

- Enter the new IP address of the ICC1 Admin Port.
- Enter the new IP netmask for the ICC1 port.
- Do you you want to configure VRRP? Type `y` or `n` and press **Enter** (n is the default). If you chose `y`, enter the ICC1 VRRP details.
- Do you want to enable LAG on ICC1? Type `y` or `n` and press **Enter** (n is the default).

Note
Do not change the ICC addressing configuration once it is assigned. If you change the ICC IP address or ICC VRRP address, the Kubernetes binding breaks, and the Kubernetes installation unwinds, effectively wiping out the installation. In this case, the only fix is to reinstall and then reconfigure.

3. Press **Enter** to accept the changes.
4. 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: Configure the domain name that is relevant to your enterprise environment 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
   Once the node's cluster state is configured, the ICC IP address, hostname, and domain name become immutable. To modify any of these settings, the node must first be reset.

   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 best practice is to define the default gateway to route via the data port topology/ subnet.

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

To configure the default gateway:

1. At the prompt, type the IP address for the default gateway.
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.

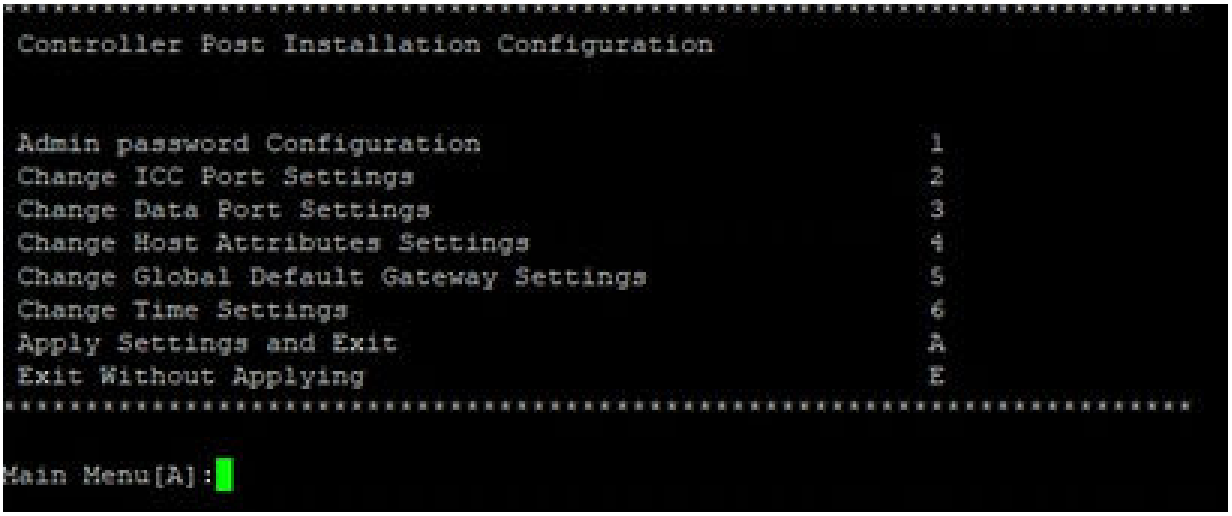


Figure 3: Controller Post Installation Configuration Menu Screen

Table 10: 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

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.

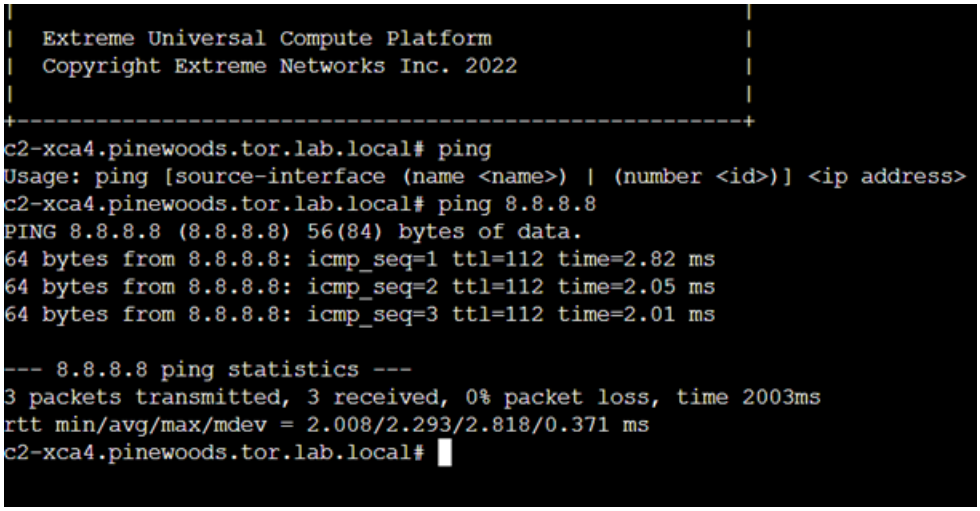


Figure 4: Example ping command

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 Universal Compute Platform image file from the Extreme Networks Support Portal. The image file extension is one of the following file types:
   - .asx (for 1130C)
   - .gbx (for 2130C)
   - .ygx (for 3150C)
   - .rcx (for 4120C)
2. Log in to the appliance Admin user interface: https://*node ip*:5825

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

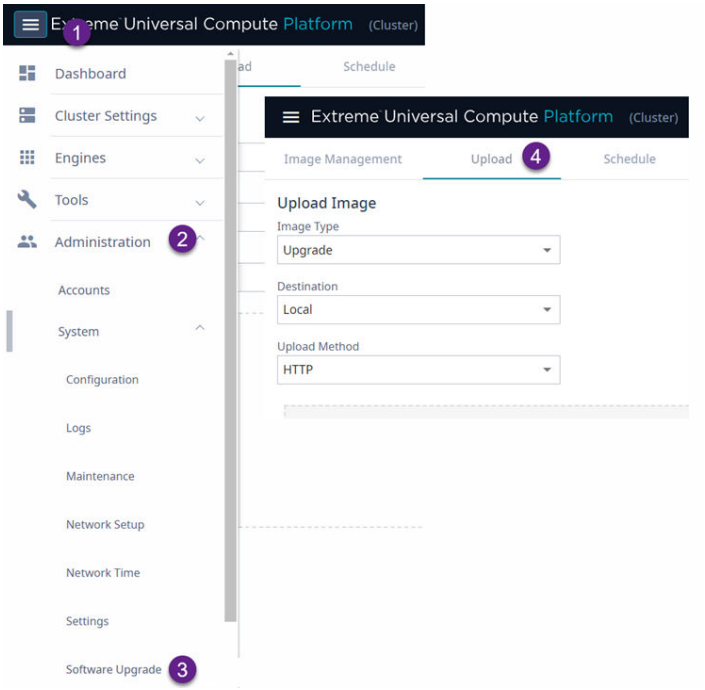


Figure 5: Navigate to Universal Compute Platform Image Upload

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

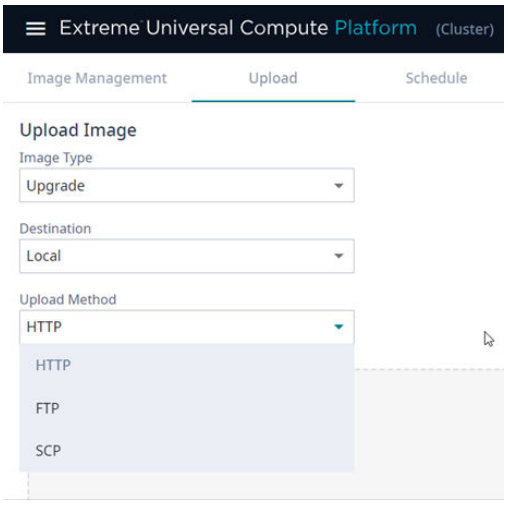


Figure 6: Upload Image Settings

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.

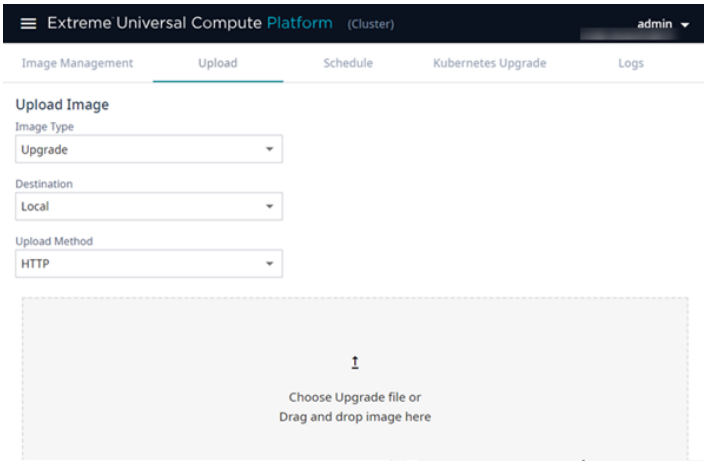


Figure 7: Select the upgrade image

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

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

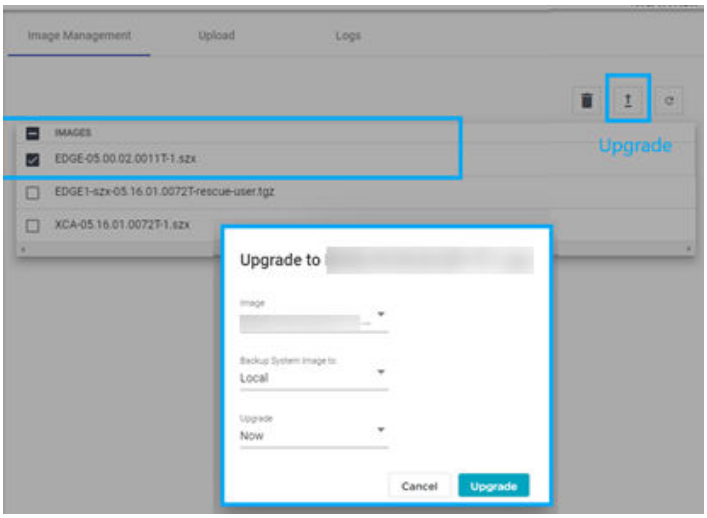


Figure 8: Upgrade the selected image

When the cluster is upgraded to the latest revision, proceed to Validate the Network Address Configuration on page 29.

Validate the Network Address Configuration

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

To access the network settings in the user interface:

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

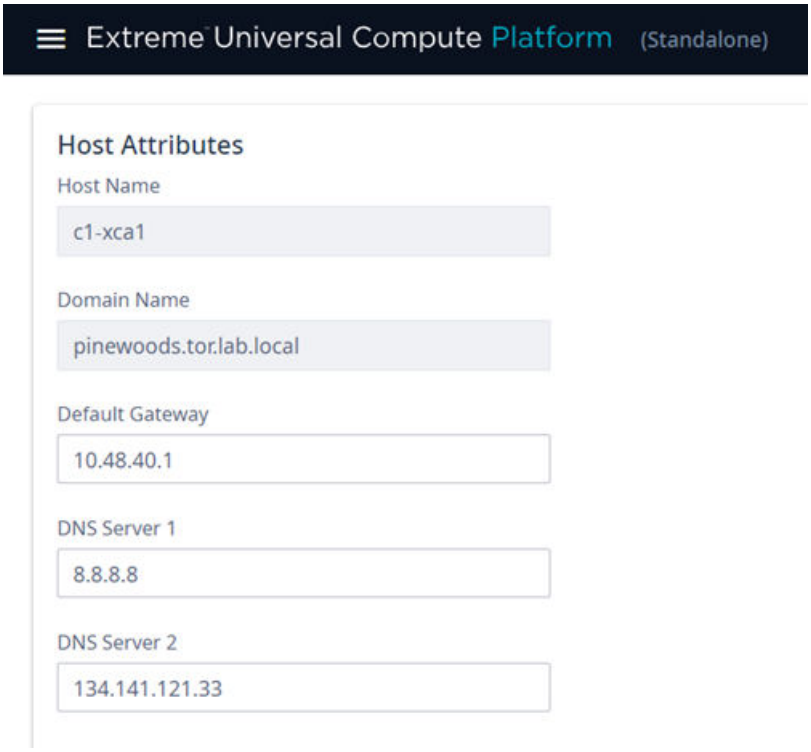


Figure 9: Network Setup - Host Attributes

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 Links

Use the Basic Configuration Wizard on page 22
Add a Port on page 31
Engine Application Settings on page 37

Add a Port

Use this optional procedure 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
Some container applications, such as Tunnel Concentrator, require you to configure a VRRP address on one of the Universal Compute Platform data ports. The VRRP address, which gets assigned to the container application during installation, creates an alias that provides access to the underlying management interface for the application instance.

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. For help with the fields and their settings, see Create New Interface Settings on page 32.

   Provide a VIP for each engine instance in your deployment.

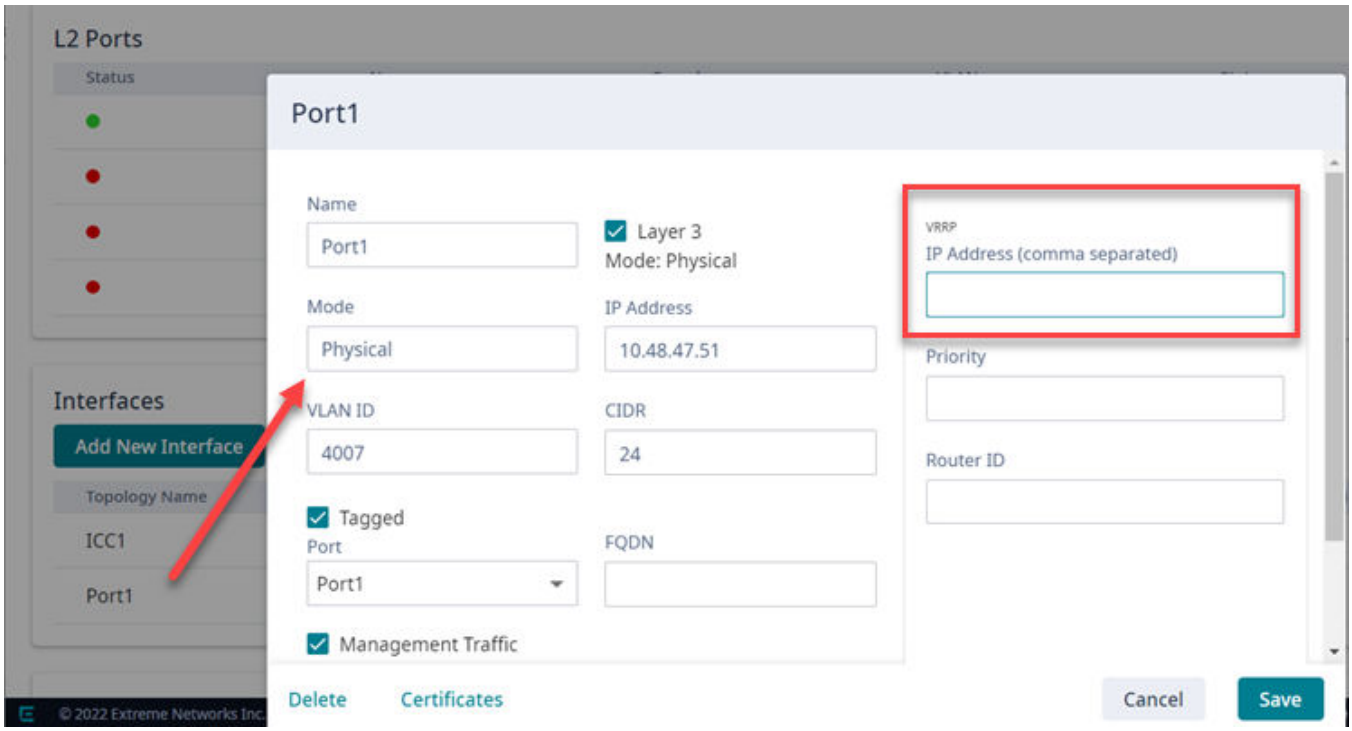


Figure 10: User Interface showing properties window for New Port

4. Optional. To create an interface alias using **VRRP**, configure the following settings:
   - Virtual IP Address
   - Priority
   - Roouter ID
5. Select **Save**.

Create New Interface Settings

The Universal Compute Platform enables the creation of additional logical interfaces to support multi-homed deployments. Use the **Create New Interface** wizard to configure the required settings. The following table describes the settings.

Table 11: 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.
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.

Table 11: Interface Properties (continued)

Field	Description
FQDN	Fully-Qualified Domain Name
VRRP	Supports load balancing and high-availability functions for the Universal Compute Platform cluster. You can also assign VRRP settings to create an IP alias that provides access to the underlying management interface for an application instance. **IP Addresses** Record the IP address relationship between the cluster's direct interfaces, VRRP, and external access. If you want to create an IP alias, enter the virtual IP address that you want to assign to the management interface of the application instance. **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 standalone configuration, the specific value is not important. These attributre definitions are important in 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 22.

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

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

To configure the cluster, do the following:

1. For the **Deployment Type**, select **ExtremeCloud Edge - Self-Orchestration**.
2. In the **Cluster Mode** section, select **Standalone** 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

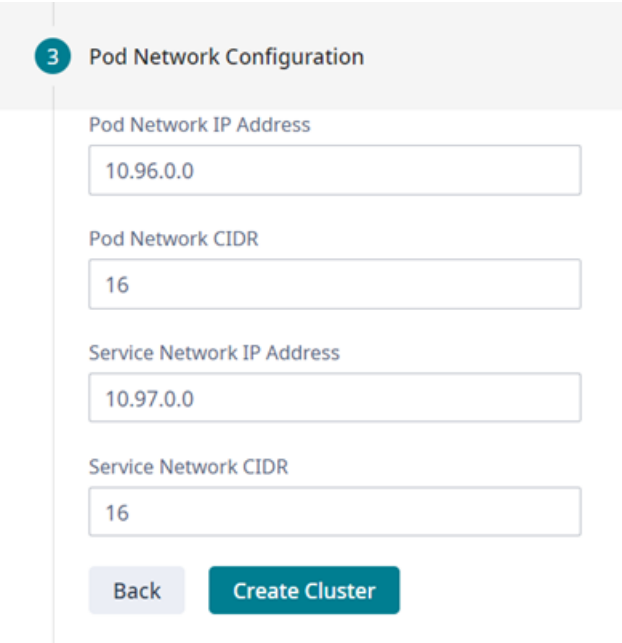


Figure 11: Pod Settings

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

Note
The cluster state is bound to the IP Adress 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.

Engine Application Installation

To install an engine application, complete the following tasks.

Table 12: Engine Application Installation

Step	Procedure	Description
1	Download the Docker Application Image on page 35	Download the Docker application image from the Extreme Networks support portal.
2	Upload Application Image to Appliance on page 35	Upload the Docker application image to the appliance.
3	Install Engine Application on page 36	Install the engine application on the Universal Compute Platform appliance.
4	Deploy Application on page 36	Deploy the application on the appliance.
5	Engine Upgrades on page 36	Upgrade the application software. Select the upgrade method that fits your application type.
6	Engine Application Settings on page 37	Configure application image settings.

Download the Docker Application Image

To obtain the application 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 `rtxcx-9000.tar`.

Upload Application Image to Appliance

Upload the Docker application image file to the Universal Compute Platform appliance.

1. Go to **Engines** > **Image Management**.

2. Complete either of the following options:
   - Select the **Choose Image File** pane and navigate to the image file.
   - Drag and drop the image file onto the **Image File** pane.

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

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

Install Engine Application

Install the Docker application image file on the appliance.

1. Go to **Engines** > **Installation**.
2. From the application pane for the intended application, select **Install**.

Note
- If you have not yet uploaded the application Docker image file, you will be prompted to do so.
- The installation time will depend on a variety of factors, be prepared for it to take some time.

A confirmation notice displays after the installation completes. Only one instance is required for the cluster.

Deploy Application

After you have installed the engine on the appliance, 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 37.
- **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:

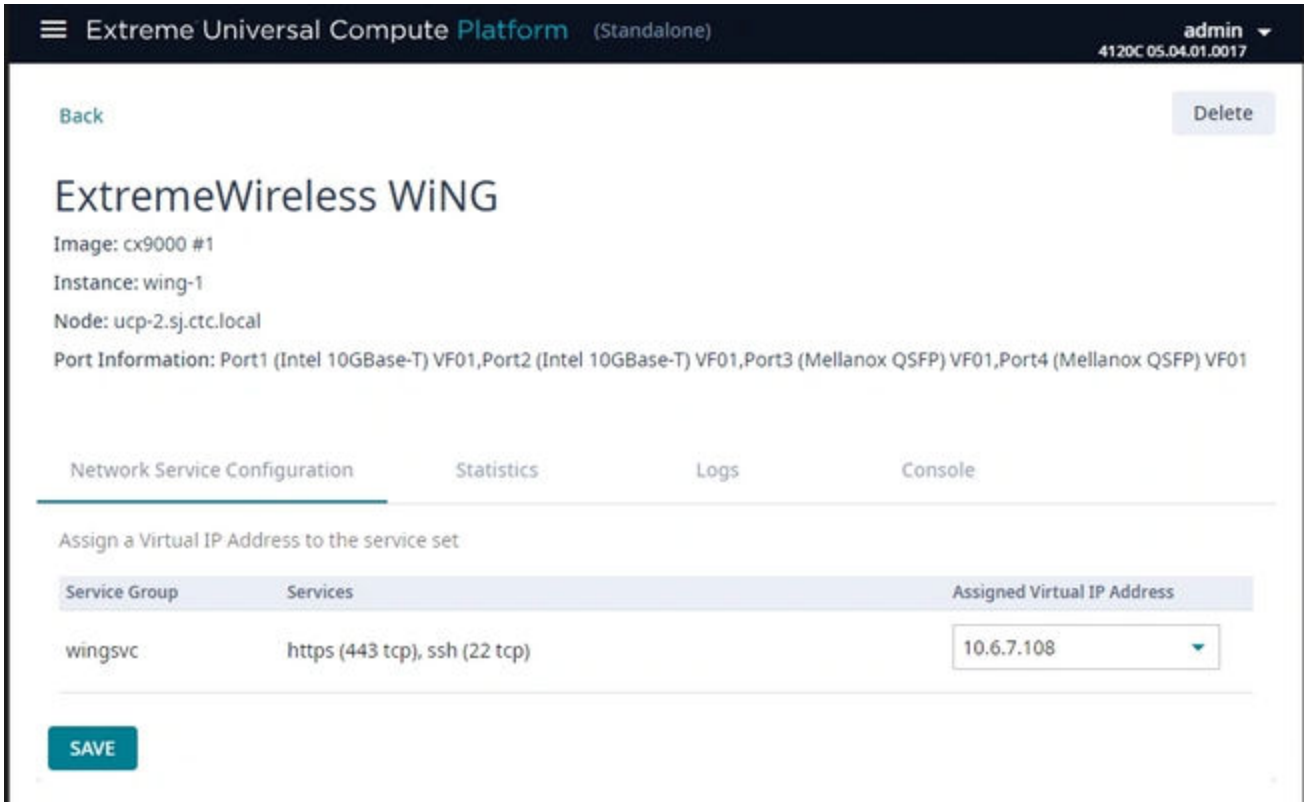


Figure 12: Example Engine Application Settings

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 Addres**s 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**.

Note
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

Related Links

Add a Port on page 31

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. Onboard the cluster to your ExtremeCloud IQ account. See Onboarding a Cluster to ExtremeCloud IQ on page 40.
2. Onboard your devices and operate the account.

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.

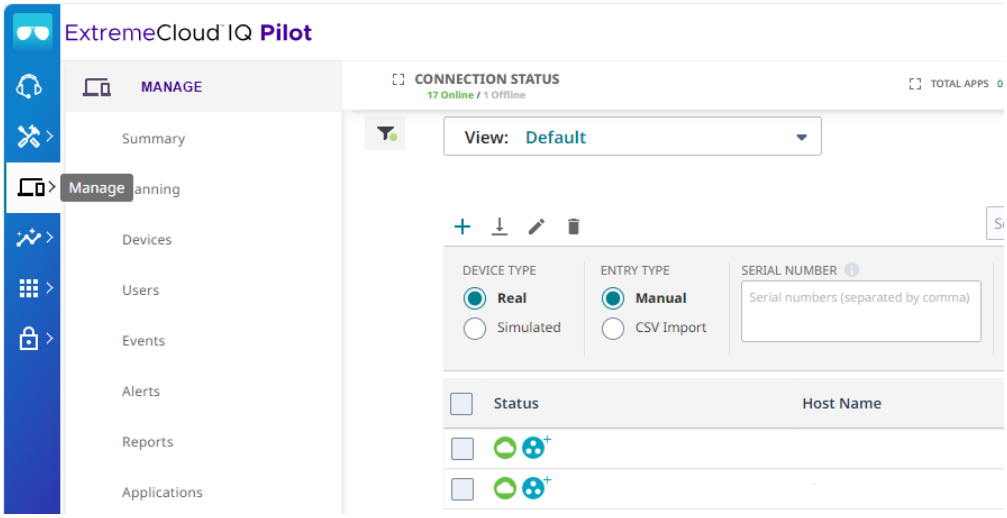


Figure 13: Add Cluster to ExtremeCloud IQ

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.

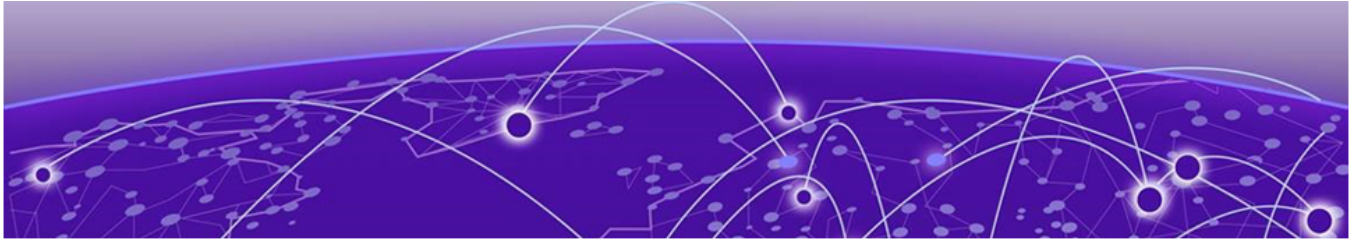
Note
To view details about the cluster, select the **Host Name** link.

Cloud Visibility

If your deployment is onboarded to ExtremeCloud IQ, you can view the cloud address from **Administration** > **System** > **Settings**. This page populates automatically when you onboard the cluster to ExtremeCloud IQ. For example, the URL may look like:

`<RDC name>-cw.extremecloudiq.com` where:

- `<RDC name>` is your Regional Data Center (RDC) information available under **About ExtremeCloud IQ**.
- `-cw` indicates a Universal Compute Platform appliance.
- `.extremecloudiq.com` is the ExtremeCloud IQ host address.



Index

N

O

P

R

S

T

U

V

W