Universal Compute Platform

Version 5.05.01

ExtremeCloud Edge

Deployment Guide

9037986-00 Rev AA
December 2023

Legal Notice

, 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 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

and the logo are trademarks or registered trademarks of , 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 trademarks, see:

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/

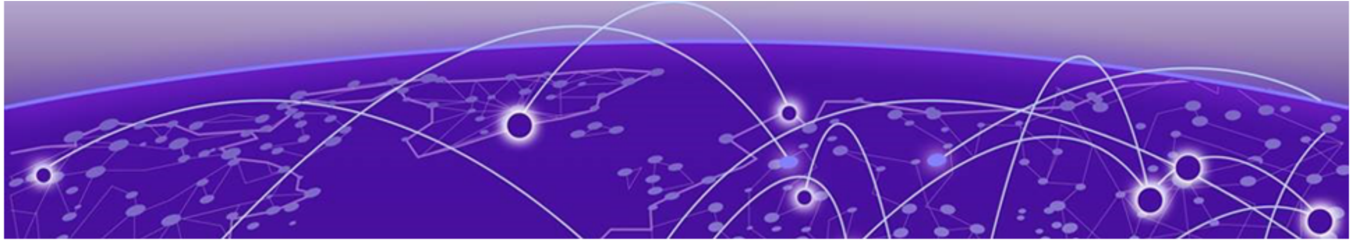
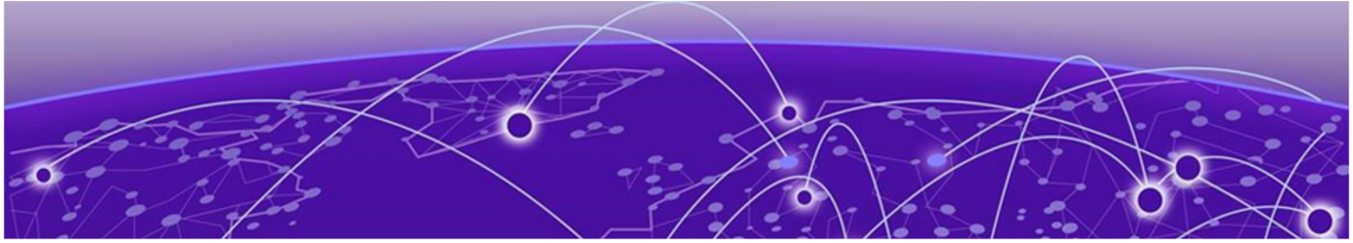


Table of Contents



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 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 customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by 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 for technical support, have the following information ready:

- Your service contract number, or serial numbers for all involved 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.

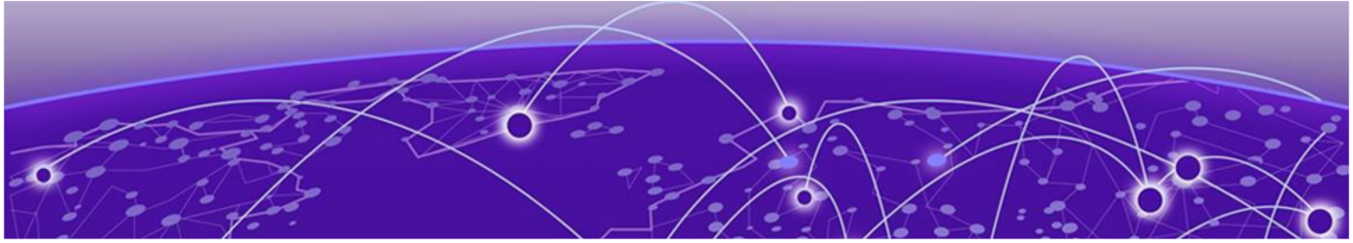
Send Feedback

The User Enablement team at 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 .

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 and Prerequisites

This guide provides the steps needed to bring a Universal Compute Platform cluster online. Universal Compute Platform leverages Kubernetes and Docker to deploy and manage the delivery of applications to the customer premises.

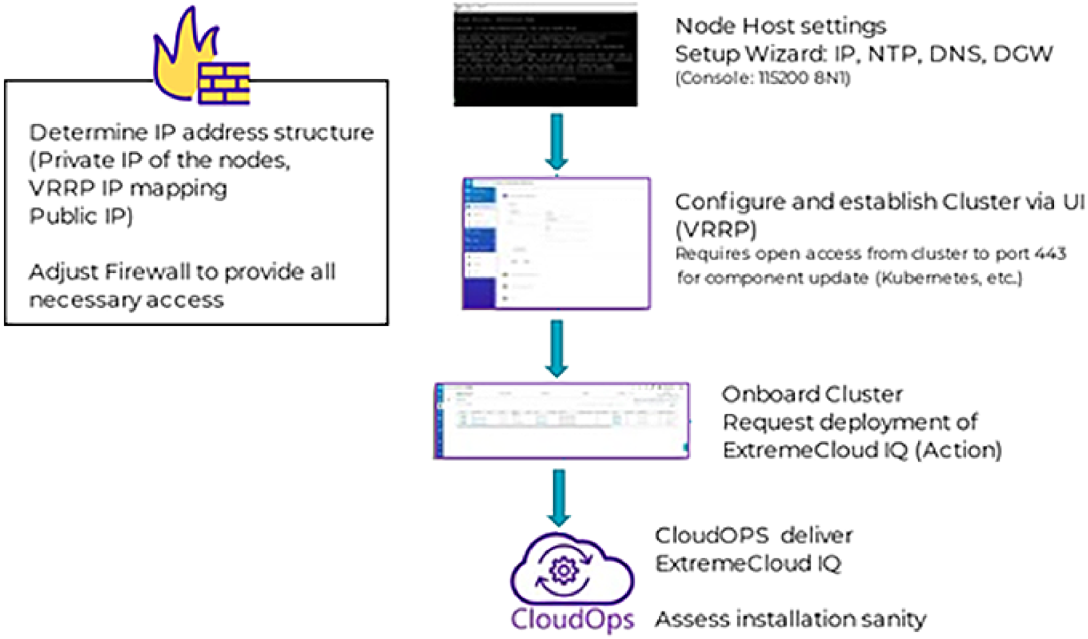
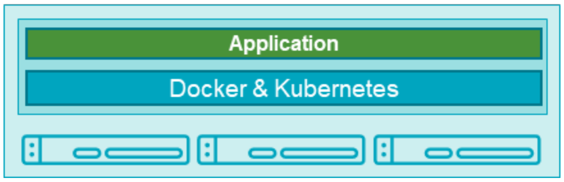

Determine IP address structure
(Private IP of the nodes,
VRRP IP mapping
Public IP)
Adjust Firewall to provide all necessary access
Node Host settings
Setup Wizard: IP, NTP, DNS, DGW
(Console: 115200 8N1)
Configure and establish Cluster via UI (VRRP)
Requires open access from cluster to port 443 for component update (Kubernetes, etc.)
Onboard Cluster
Request deployment of ExtremeCloud IQ (Action)
CloudOPS deliver ExtremeCloud IQ
CloudOps
Assess installation sanity

Figure 1: ExtremeCloud IQ Deployment Workflow

The following figure depicts the three physical host boxes required for Universal Compute Platform, with ports mapped as follows:



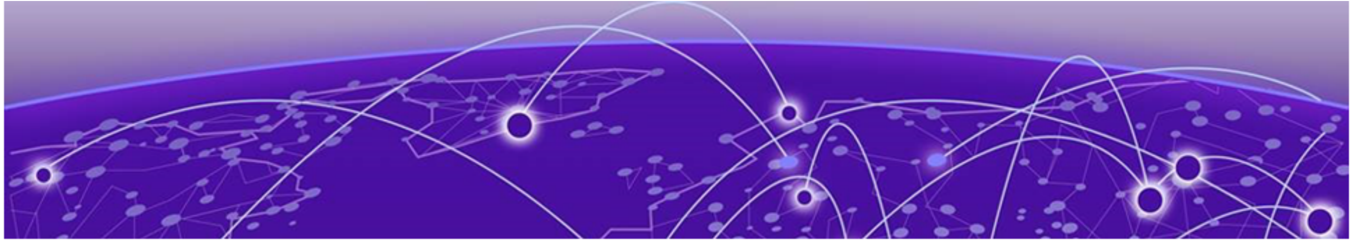
As an option, the system leverages VRRP (Virtual Router Redundancy Protocol) in order to provide support for both high-availability and load balancing, supported by an NGINX engine. All service operations to the cluster should be directed to the corresponding VRRP IP so that the load balancing logic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

Deployment configuration requirements vary over different applications deployed into the Universal Compute Platform. One main requirement in the establishment and operation of the cluster is the Inter-Cluster Connection. This connection operates as the backplane between nodes in the cluster. This backplane carries all the synchronization data between nodes for both component and data states. It is a best practice to deploy the interface as a segregated 10 Gbps inter-connect (separate switch port), allowing for the best performance in synchronization between nodes.

- Inter-Cluster Connection: Backend interaction and synchronization between all the members of a cluster. Minimum required connection requires 10 Gbps between nodes.
- The internal Kubernetes engine requires the reservation of two (2x) /16 subnets. This set of IP Address ranges is for internal use only by inter-component and framework operations. This reserved range can be anything, but customer should ensure that this IP address range does not conflict with any routable address space within the organization.

Related Topics

ExtremeCloud Edge on page 11



ExtremeCloud Edge

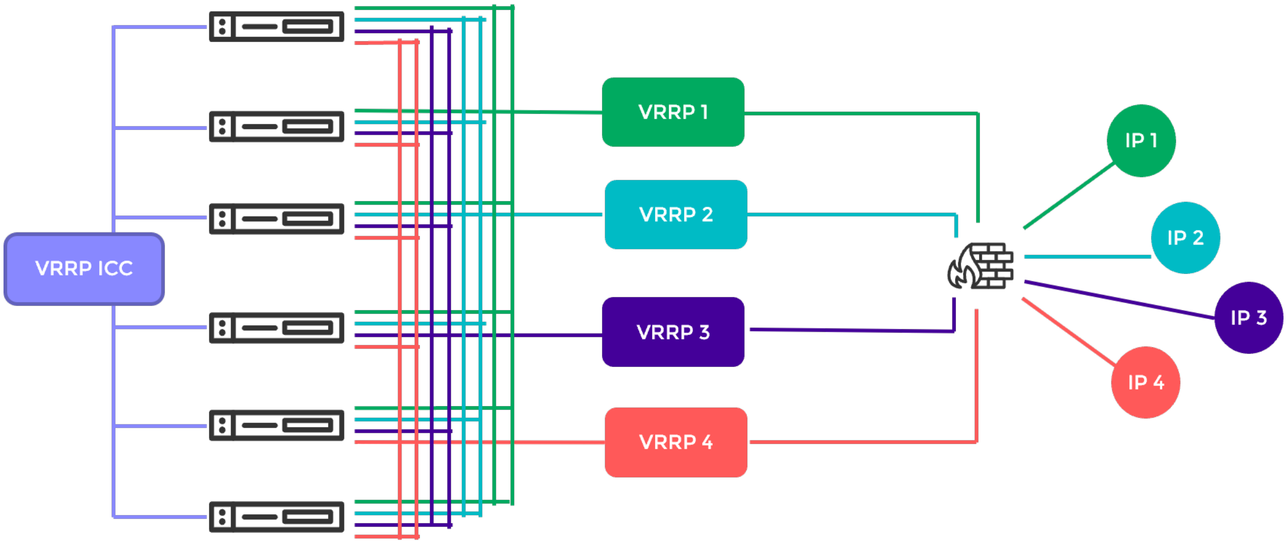
This guide outlines the steps required to prepare a cluster environment that will support deployment of ExtremeCloud Edge applications to the customers' premises.

Minimum Requirements for Installation

- 4 Public IP addresses esposed via the firewall and port-forwarded to the internal service sets
- Firewall adjustments to allow communication of system functions to external entities (licensing, component upgrades, device management) and CloudOPS access for lifecycle management of the intalled applications/software. Please refer to section Firewall Setup on page 14.
- 6 x 4120C-1 Universal Compute Platform appliances configured as a cluster.
- Network Connectivity for the hosts both in backplane (ICC) and application data operations (data ports). 10 Gbps minimimun links recommended.
- ICC: Interconnect (backplane) for cluster operations, component state and shared filesystem synchronization. Each node requires connection of ICC to common backplane network segment.
- Data: Interfaces that the applications will utilize with other devices or systems for operation management, such as remote device management (Access Points, Switches, etc..) and license services. Data interface is also utilized for remote lifecycle management of installed software.

Application requirements for the cluster configuration:

- 4 IP addresses representing the various services offered by the application to effectuate load balancing (Service Set 1 – 4).
- Each node in the cluster must map each of the services to a data interface, and all services can be mapped into the same interface. The same data interface can represent a direct point of reference for each of the front-end VRRP services.
- Four VRRP IP address are required to support port-overlap services for different services or a functional model (such as CAPWAP Master vs CAPWAP Server).



Service Set 1: Cluster Administration, Account Access (https), CAPWAP Master, Diagnostics

Table 4: Example port assignments for Service Set 1

Protocol	Port	Service	Description
TCP	443	NGINX	ExtremeCloud IQ Admin, software management
TCP	2083	IDM	IDM Auth
TCP	80	CAPWAP	CAPWAP Master
TCP	12222	CAPWAP	CAPWAP Master
TCP	1443	XAPI	ExtremeCloud IQ API

Service Set 2: AP Registration/CAPWAP Load Balancing

Table 5: Example port assignments for Service Set 2

Protocol	Port	Service	Description
TCP	80	CAPWAP	CAPWAP Master
TCP	12222	CAPWAP	CAPWAP Master
TCP	1443	XAPI	ExtremeCloud IQ API

Service Set 3: AP Registration/CAPWP Load Balancing

Table 6: Example port assignments for Service Set 3

Protocol	Port	Service	Description
TCP	80	CAPWAP	CAPWAP Master
TCP	12222	CAPWAP	CAPWAP Master
TCP	1443	XAPI	ExtremeCloud IQ API

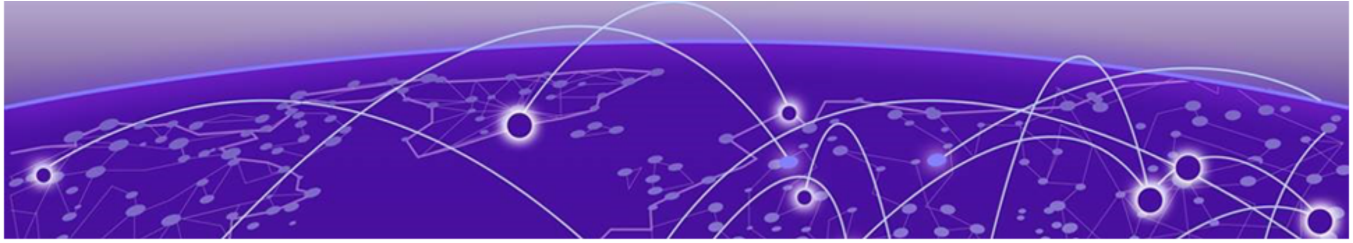
Service Set 4: AP Registration/CAPWP Load Balancing

Table 7: Example port assignments for Service Set 4

Protocol	Port	Service	Description
TCP	80	CAPWAP	CAPWAP Master
TCP	12222	CAPWAP	CAPWAP Master
TCP	1443	XAPI	ExtremeCloud IQ API

Related Topics

Firewall Setup on page 14



Firewall Setup

In a typical on-premise installation, the cluster is installed behind an access firewall, providing network address translations between the public and private address spaces. Always allow access for CloudOps management of the cluster. The standard deployment of ExtremeCloud Edge requires 4 Public IP addresses to front-end the installation. They are mapped to forward traffic into the four VRRP IP addresses of the service sets.

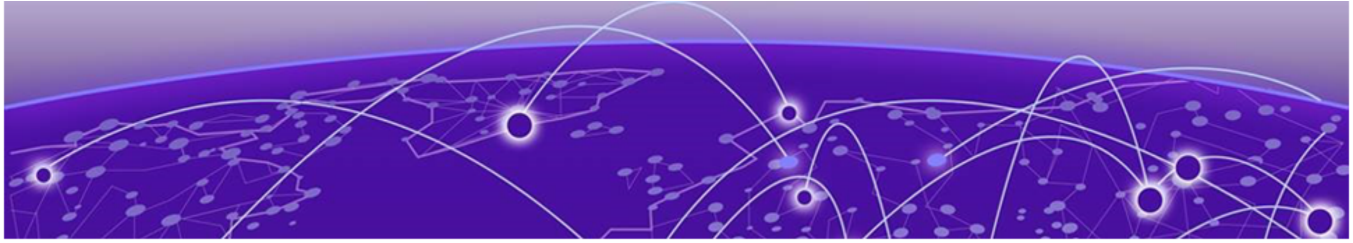
During system setup, the following configuration settings are critical to the deployment:

- Default Gateway: Each node in the cluster supports a single default gateway (0.0.0.0/0) definition. This gateway must be mapped to a next-hop attached on the data port interface.

  Note
  Do not configure the default gateway to map to the Inter-Cluster Connection (ICC) interface. The ICC is an internal connection between systems that is not used for management or operation of the cluster.

- DNS server: At least one reachable DNS server must be configurable, allowing the system to resolve several URLs during installation and interaction with ExtremeCloud IQ and CloudOps functions.
- Network Time Protocol (NTP) Servers: At least one reachable NTP, allowing the system to synchronize its time with a trusted time source. The same NTP must be configured, in the same order, on all nodes in the cluster.

  A best practice is to have two NTP definitions to support availability of the primary server. If there is an issue with the primary server, the system resorts to the alternate server.



Deployment Overview

This topic outlines the key deployment responsibilities for deploying ExtremeCloud Edge on Universal Compute Platform. Each of the following components have unique responsibilities:

- Customer On-Site Representative
- Extreme CloudOPS
- System Administrator of Universal Compute Platform

Customer On-Site Representative

Customer On-Site Representatives are responsible for the following tasks:

- Set up a firewall that enables cluster access to the appropriate internet ports (for example, port 443) and enables CloudOps access. Follow the firewall configuration guidelines under Firewall Setup on page 14.
- Configure each node for service — Provide the necessary IP, DNS, and Host addresses, ICC Configure and form cluster (VRRP).
- Register the cluster with an ExtremeCloud IQ Public account.
- Register an ExtremeCloud IQ deployment request. The request requires a valid XIQ-EDGEOPS-S-EW in good standing. This SKU is a required component of an ExtremeCloud Edge BOM quote.

For detailed information, see Introduction and Prerequisites on page 9.

Extreme CloudOps

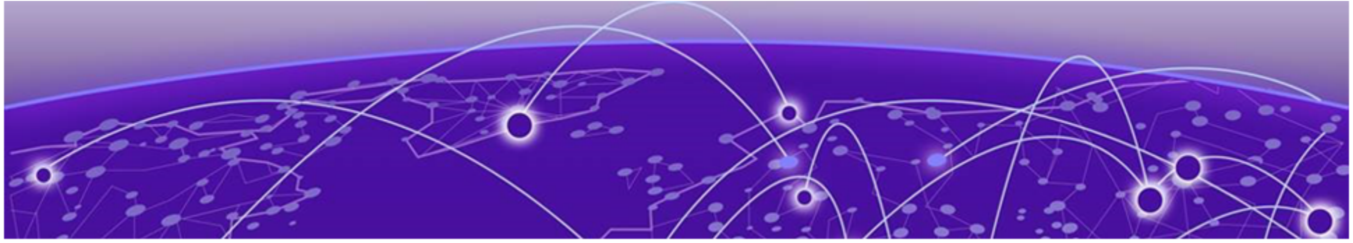
ExtremeCloud IQ CloudOps is responsible for the following tasks:

- Deploy ExtremeCloud applications (ExtremeCloud IQ, etc.) to the Universal Compute Platform cluster.
- Create monitoring and backup frameworks.
- Validate the state of all operational components.

Universal Compute Platform Administrator

Universal Compute Platform Administrators are responsible for the following tasks:

- Create ExtremeCloud IQ user accounts for end-device management.
- Onboard managed devices from the ExtremeCloud IQ local account.



Prerequisites for ExtremeCloud Edge Installation

Address planning is the fundamental step in successful deployment of the Universal Compute Platform to support installing ExtremeCloud applications such as ExtremeCloud IQ. It is important to understand the following:

- Decide how you will deploy and access the services offered by the cluster. Is the cluster going to serve applications that operate only within the on-premises installation? Or is application access going to require external access? Pre-determination of the IP address and connectivity structure are fundamental to a successful deployment. These deployment decisions drive the configuration choices.
- Consider the address plan of the installation, including how the cluster is going to be presented externally via a firewall.

  Each externally exposed address must be mapped to an internal VRRP of the cluster. You can either directly expose the VRRP IP addresses for the three service sets directly through a firewall, or in the case of NAT translation, ensure that the externally available IP addresses are mapped 1:1 to the internal services, and that the correponding application ports are allowed for access (per firewall rules definition).

Important
Before you begin step-by-step configuration, make sure that you clearly understand and document all the elements of the network presence and topology related to the deployment.

The Inter-Cluster Connection (ICC) IP address is critical to the continuous operation of the system. If address definitions for ICC require re-addressing, the entire cluster will need to be rebuilt and the application re-deployed in order to re-established all the correct references of services within the cluster.

It is strongly recommended that the *entire* IP address structure for all services be defined once and not changed. Re-addressing may expose internal dependencies on references to mapped services and therefore affect the integrity and stability of the deployed installation.

IP Addresses

The most important point of definition is to record the IP address relationship between the cluster’s direct interfaces (Node, Service Set, Virtual IP address (VIP)), and external access. Each node has it's own data interface IP address.

Table 8: IP address relationship between the cluster's direct interfaces and external access

Service Set	Virtual IP (VIP)	Public IP
Service Set 1 (cmudp, cmtcp, cmauth, https)	`VIP 1`	`Public IP 1`
Service Set 2 (csupd1, cstcp1)	`VIP 2`	`Public IP 2`
Service Set 3 (csudp2, cstcp2)	`VIP 3`	`Public IP 3`
Service Set 4 (csudp3, cstcp3)	`VIP 4`	`Public IP 4`

VRRP Configuration

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.

  The node with the higher priority defaults to the master. However, in the case of failovers of the master node, VRRP algorithms assign mastery to the next higher priority member of the cluster. Therefore, it is important to properly assign corresponding priority settings to each node, so that their hierarchical priority in terms of VRRP state ownership is clear.

  As a best practice:

  - Designate node 1 as the highest priority, node 2 for second highest priority, and nodes 3-6 as lower priority.
  - The same priority should be used across all services (ICC, Services)
- **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.

Inter-Cluster VRRP Configuration

An Inter-Cluster Connection refers to the back-end interaction and synchronization between all the members of a cluster. Minimum required connection requires 10 Gbps between nodes.

Table 9: Inter-Cluster Connection VRRP Configuration

	Nodes 1 -6 (Port #)
ICC	• Node 1 ICC IP /CIDR • Node 2 ICC IP/CIDR • Node 3 ICC IP/CIDR • Node 4 ICC IP/CIDR • Node 5 ICC IP/CIDR • Node 6 ICC IP/CIDR
VLAN	VLAN Tagged/Untagged
Port type	Physical
VRRP	
VRRP IP addresses	ICC VRRP IP
Priority	Set a unique priority for each node. For example: • Highest (200) • Next (150) • Medium (100) • Next (75) • Next (50) • Low (25)
Router ID	ID (2)

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 10: Services VRRP Configuration

	Nodes 1-6 (Port #)
Data Port	Node Port IP /CIDR. Unique Port IP for each node.
VLAN	VLAN Tagged/Untagged
Port type	Physical
VRRP	
VRRP IP address (VIP)	6 VIP addresses. Unique VIP for each node
Priority	Unique priority value for each VIP
Router ID	ID (1)

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 11: 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.

Port Information for Firewalls

Map the following service ports to the Service Set VRRP IP addresses listed in Table 8 on page 17.

- VLAN/VIP address for CAPWAP Master and API services (TCP 80/UDP 12222/TCP 2083/443)
- VLAN/VIP address for CAPWAP Server 1 service (TCP 80/UDP 12222)
- VLAN/VIP address for CAPWAP Server 2 (TCP 80/UDP 12222)

ExtremeCloud IQ on-premises installations require access to ExtremeCloud IQ core services. Make sure the firewall configuration allows for access to ExtremeCloud IQ core services.

The following tables list outbound ports for use when the firewall configuration requires rules that enable outbound traffic.

Basic Access for ExtremeCloud Services

This is required for ExtremeCloud applications to run properly on ExtremeCloud Edge RDC.

Table 12: Firewall Configuration Details (Outbound Traffic)

Domain Name	IPv4 Addresses	Protocol	Port
redirector.aerohive.com	54.172.0.252	TCP	80
		HTTPS	443
		UDP	12222

Table 12: Firewall Configuration Details (Outbound Traffic) (continued)

Domain Name	IPv4 Addresses	Protocol	Port
hac.extremecloudiq.com	34.253.190.192 ~ 34.253.190.255	HTTPS	443
hmupdates-ng.aerohive.com	54.86.95.132	HTTPS	443
extremecloudiq.com	34.253.190.192 ~ 34.253.190.255	HTTPS	443
	18.194.95.0 ~ 18.194.95.15		
	3.234.248.0 ~ 3.234.248.31		
	44.234.22.92 ~ 44.234.22.95		
mx.extremecloudiq.com	34.202.197.56/57	TCP	587
stun.extremecloudiq.com	3.234.248.28 - 29	UDP	12222
api.ip2location.com	Dynamic IP range	HTTPS	443
gcr.io	Dynamic IP range	HTTPS	443
Amazon S3	Dynamic IP range	HTTPS	443
NTP Service	<Any NTP Server IP>	UDP/TCP	123
extremeportal.force.com	Dynamic IP range	HTTPS	443
prod.extreme.sentinelcloud.com	Dynamic IP range	HTTPS	443
cloud-status.extremecloudiq.com	18.67.39.6	HTTPS	443
cloud-cdn2.extremecloudiq.com	Dynamic IP range	HTTPS	443
rest.nexmo.com	Dynamic IP range	HTTPS	443

Access for Continuous Service Operation

This is required for CloudOps team to handle service deployment and day to day operations and to maintain the service SLA.

Table 13: Inbound Traffic

Service	IPv4 Addresses	Protocol	Port
SSH	3.64.95.0/29	TCP	22
UCP Remote Access	134.141.117.45 134.141.4.8	HTTPS	5825

Note
Both inbound accesses are only needed on-demand. For the initial deployment, firmware upgrade, or issue troubleshooting.

Table 14: Outbound Traffic

Domain Name	IPv4 Addresses	Protocol	Port
lc-eu.extremecloudiq.com	3.64.95.0/29	HTTPS	443

Note
Rancher connection is required for day-to-day service operation. (It creates a tunnel to Kubernetes cluster for CloudOps remote access/management.)

For NAT deployments where you deploy your cluster with private addressing, you must provide the CloudOps team with direct admin access to the cluster nodes in your internal network. Use the mappings in the following table to map inbound ports on the public side of the NAT router to specific cluster nodes and ports in your private network.

Note
Make sure to let the CloudOps team know which IP address you are using for inbound connections. We recommend using the first public IP address, although you can use another address, including a public IP address that is dedicated to this connection type.

Table 15: Inbound Traffic Port Mapping (when using NAT)

Service	Source IP	Inbound IP (public NAT)	Inbound Port (public NAT)	Forward to UCP Node	On Port	Protocol
SSH	3.64.95.0/29 216.123.81.194	Your public IP address	20001	Node 1	22	TCP
			20002	Node 2	22	TCP
			20003	Node 3	22	TCP
			20004	Node 4	22	TCP
			20005	Node 5	22	TCP
			20006	Node 6	22	TCP

Table 15: Inbound Traffic Port Mapping (when using NAT) (continued)

Service	Source IP	Inbound IP (public NAT)	Inbound Port (public NAT)	Forward to UCP Node	On Port	Protocol
UCP Remote Access	134.141.117.45 134.141.4.8 216.123.81.194	Your public IP address	20501	Node 1	5825	HTTPS
			20502	Node 2	5825	HTTPS
			20503	Node 3	5825	HTTPS
			20504	Node 4	5825	HTTPS
			20505	Node 5	5825	HTTPS
			20506	Node 6	5825	HTTPS

Access for Production Sanity Verification

The Extreme QA team will run production santify verification after the release upgrade to make sure all of the services are still working properly.

Table 16: Inbound Traffic

Service	IPv4 Address	Protocol	Port
GDC Web Service	208.185.247.165/32 (San Jose) 216.123.81.194/32 (Thornhill) 14.143.116.18/32 (Bangalore)	HTTPS	443
RDC Web Service		HTTPS	443
CAPWAP Service		TCP	80
		UDP	12222
Radsecproxy		TCP	2083

Related Topics

Source Address Information on page 22

Source Address Information

For installations where APs are installed off-premises and connecting for service through a firewall, relax the access rules to specific service ports because source addresses are not always deterministic.

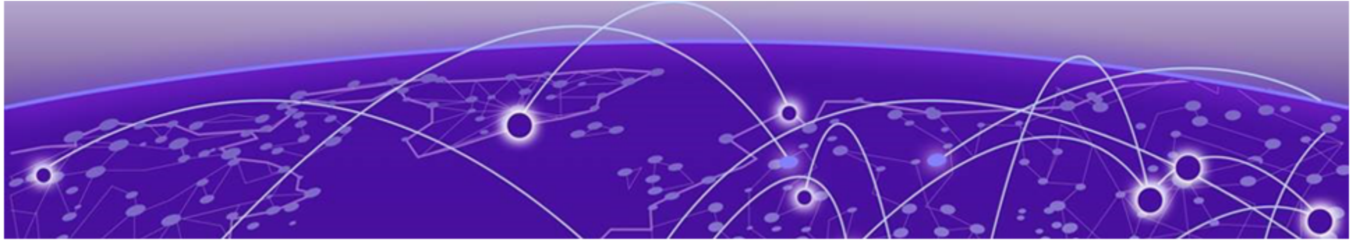
These settings are required to support remote diagnostics and to set up validation operations.

Table 17: Source address information (examples):

Source IP	Port	Description	Action
0.0.0.0/0	TCP 80	AP CAPWAP registration	Allow
0.0.0.0/0	TCP 443	ExtremeCloud IQ login access and software updates	Allow

Table 17: Source address information (examples): (continued)

Source IP	Port	Description	Action
0.0.0.0/0	TCP 2083	RADSEC	Allow
0.0.0.0/0	UDP 12222	AP CAPWAP	Allow
Restricted IP list Extreme Bastion servers: • Raleigh Bastion Host 134.141.117.45/32 • Salem Bastion Host 134.141.4.8/32 • San Jose: 208.185.247.165 • Thornhill: 216.123.81.194 • Bangalore AMR: 14.143.116.18 • Bangalore Bagmane: 121.244.44.28 • Bangalore Ecospace: 115.110.157.126	TCP 22	Support SSH Access	Allow
	TCP 5825	Cluster Admin GUI. Remote diagnostics	Allow



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.

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 25

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.

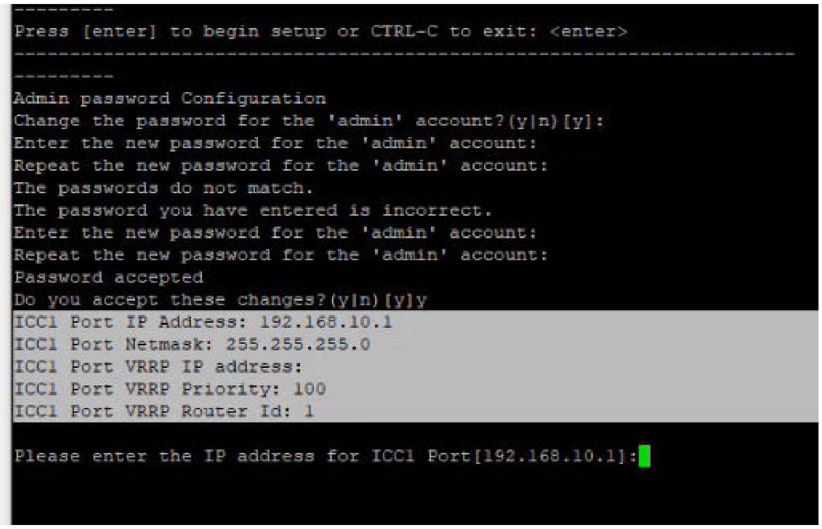
   a. To change the password for the admin account, press **Enter**.

   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**.

      If the passwords match, the password gets accepted, and the ICC1 configuration is displayed.



```
----------
Press [enter] to begin setup or CTRL-C to exit: <enter>
-----------------------------------------------------------------------
----------
Admin password Configuration
Change the password for the 'admin' account?(y|n)[y]:
Enter the new password for the 'admin' account:
Repeat the new password for the 'admin' account:
The passwords do not match.
The password you have entered is incorrect.
Enter the new password for the 'admin' account:
Repeat the new password for the 'admin' account:
Password accepted
Do you accept these changes?(y|n)[y]y
ICC1 Port IP Address: 192.168.10.1
ICC1 Port Netmask: 255.255.255.0
ICC1 Port VRRP IP address:
ICC1 Port VRRP Priority: 100
ICC1 Port VRRP Router Id: 1

Please enter the IP address for ICC1 Port[192.168.10.1]:
```

Figure 2: Basic Configuration Wizard - ICC1 Configuration

2. To update the ICC1 (Admin Port):

   Use the information gathered under ExtremeCloud Edge on page 11 and accept the changes.

   - 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**. If you chose `y`, enter the ICC1 VRRP details.
   - Do you want to enable LAG on ICC1? Type `y` or `n` and press **Enter**.
3. Press **Enter** to accept the changes.

   > Note
   > If you need to reconfigure the ICC1 settings, enter `n` and enter a new IP address of the ICC 1 Admin Port.

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: Set `y` 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 Admin 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 Admin 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.

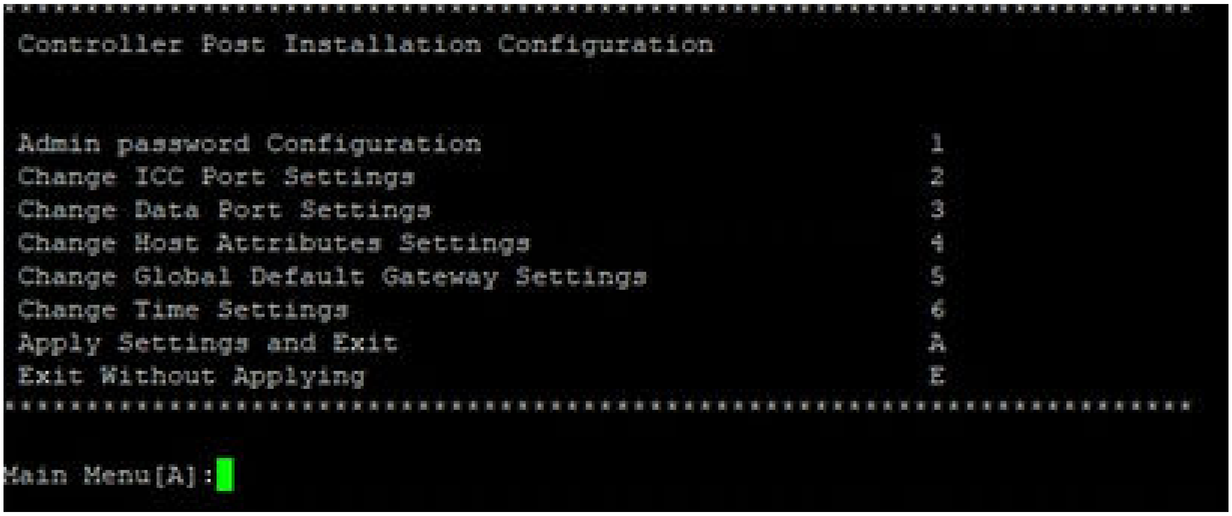
   You can enter **n** to move down the list, or **p** to move up the list. To go back to the Region selection, press **c**.

   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 3: Controller Post Installation Configuration Menu Screen

Table 18: 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

Table 18: Controller Post Installation Configuration Menu (continued)

Menu Option	Command
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.

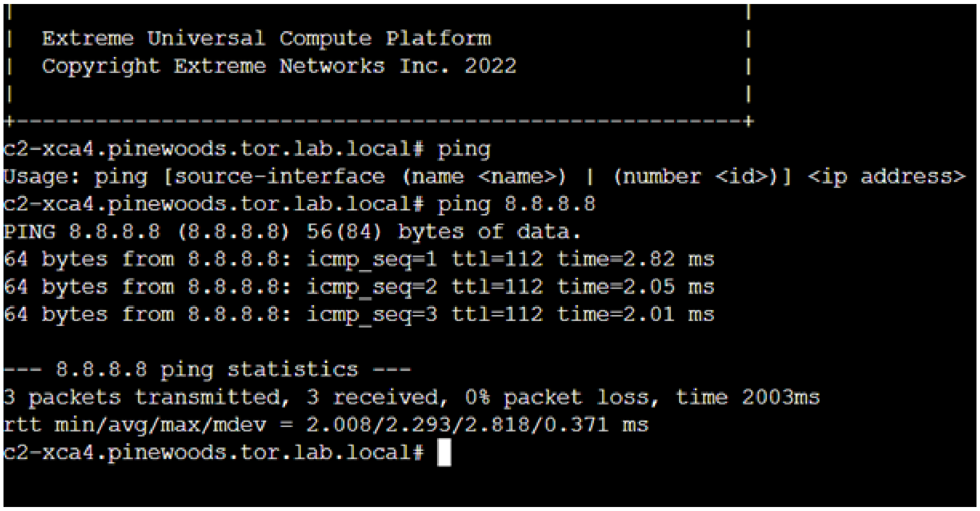
7. Press **Enter** to accept the settings. The default option for accepting the settings is **`A`**.

   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.



```
|                                                         |
|  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 4: Example ping command

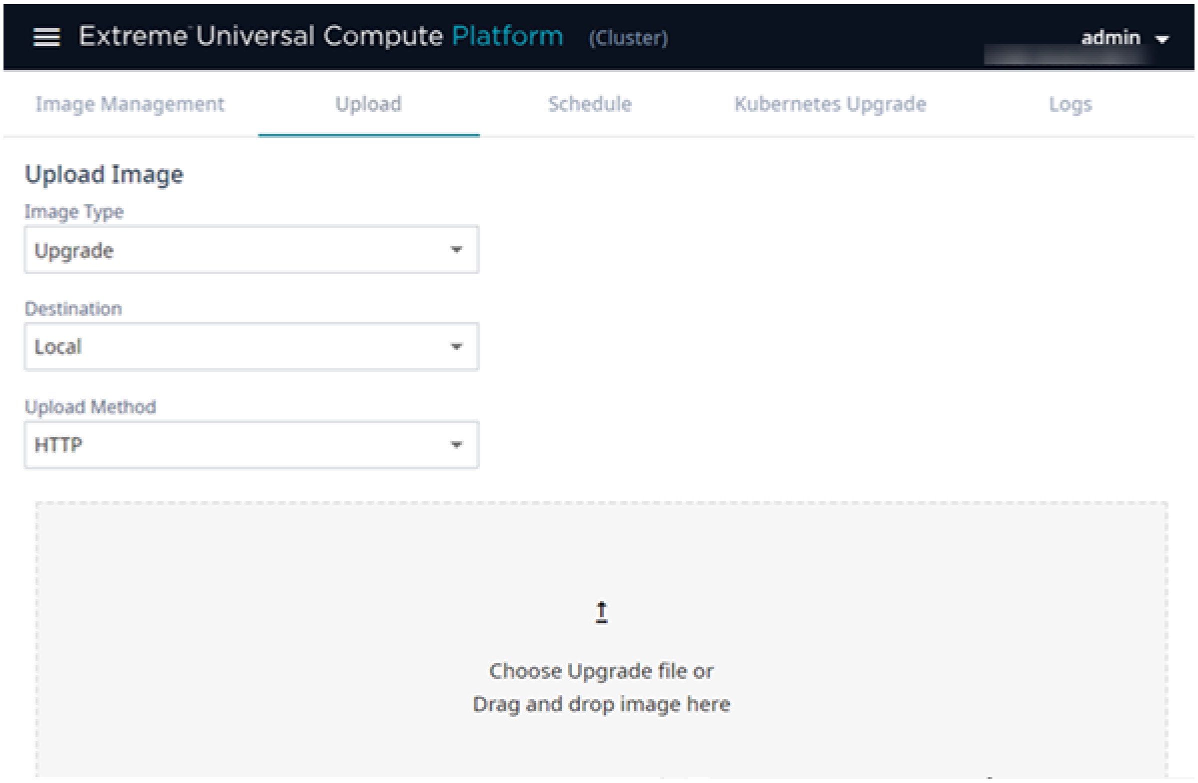
Upgrade the Appliance Firmware

Before configuring the cluster, use your Extreme Support account to download the latest revision of Universal Compute Platform firmware from the support portal: https://extremeportal.force.com/. At this time, UCP 5.04.01 is the minimum required revision.

1. Log in to the controller Admin user interface: https://*`node ip`*:5825
2. Go to **Administration** > **System** > **Software Upgrade** > **Upload**.

3. Upload the desired revision of Universal Compute Platform.

   Note
   A best practice is to upgrade each of the nodes on a new cluster to the latest revision before proceeding with the cluster set up and configuration.



Upload Image

Image Type: Upgrade

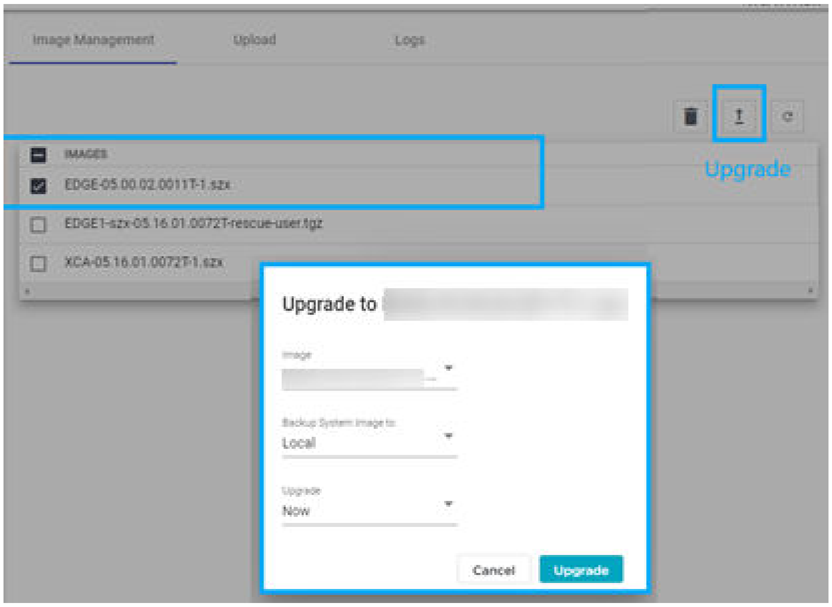
Destination: Local

Upload Method: HTTP

Choose Upgrade file or
Drag and drop image here

Figure 5: Select the upgrade image

4. From the **Image Management** Tab, select the Upgrade image, and select ↥ .



■ 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 all nodes in the cluster are upgraded to the latest revision, proceed to IP Address Configuration on page 31.

IP Address Configuration

Use the configuration wizard to initialize nodes in a cluster to the pre-determined IP addresses.

> Note
> IP address configuration for interfaces on the cluster must be set only once. If you change IP addresses after initial deployment (for example, due to a cluster relocation), you must rebuild and re-deploy the cluster, and re-install the application.

The following is example information that must be gathered during the prerequisite stages for each node in the cluster, and for the ICC VRRP:

IP Address

A unique IP address for each node. Example:192.227.109.81

Mask

Common Mask. Example:/26 (255.255.255.192)

Gateway

Common Gateway. Example:192.227.109.65

VRRP Precedence

Common Router ID with a unique precedence level for each node. Provide a unique precedence value for each node.

For example:

- Node1 - 100 Router ID1
- Node2 - 75 Router ID1
- Node3 - 50 Router ID1
- Node4 - 25 Router ID1
- Node5 - 10 Router ID1
- Node6 - 01 Router ID1

Related Topics

Use the Basic Configuration Wizard on page 25

Configure VRRP (VIP)

Take the following steps to configure the Virtual Router Redundancy Protocol (VRRP) IP addresses.

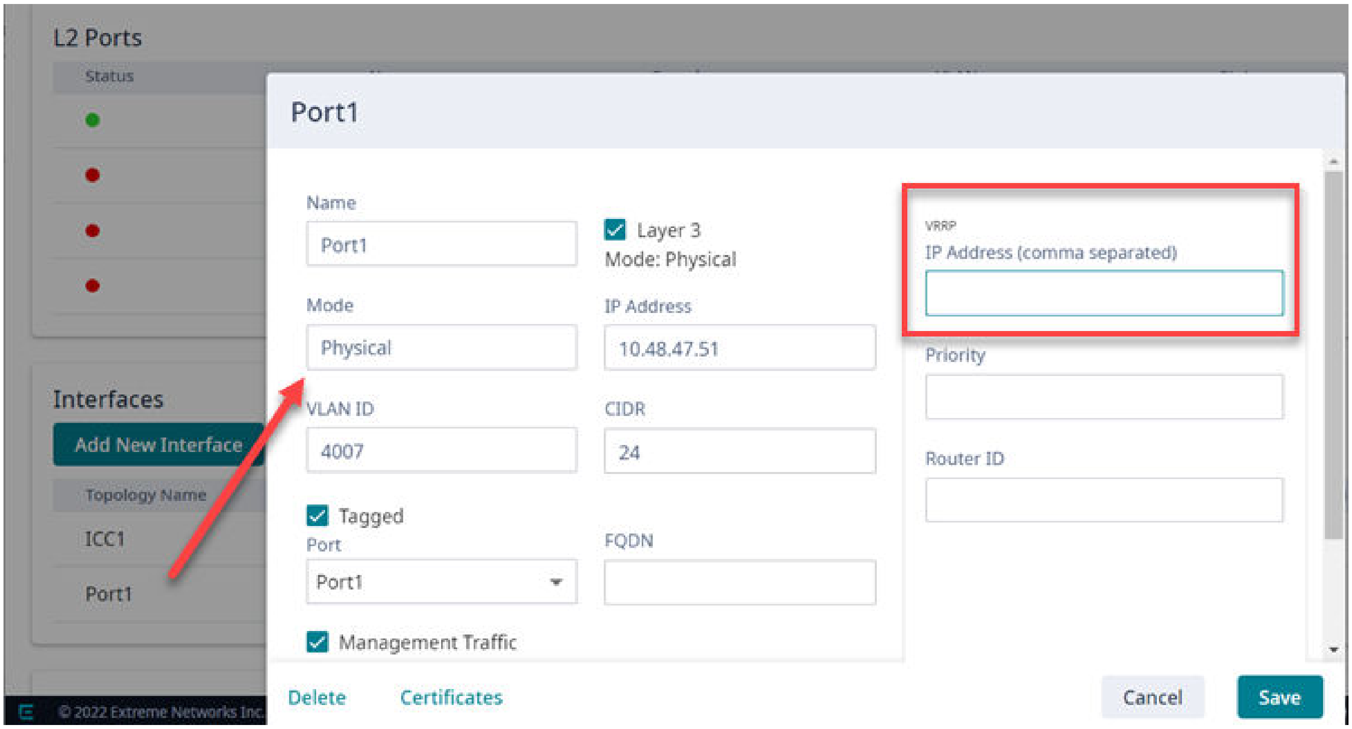
1. Navigate to **Administration** > **System** > **Network Setup**.
2. From the **Interfaces** list, select the data access interface that you configured from the **System Startup Wizard** for (Port 1).

   The **Port Configuration Settings** menu displays.
3. Provide a list of IP addresses that will be offered via VRRP.

4. Set the Router Priority and Router ID for each node.

   Each node must have the same list of IP addresses and the same Router ID.

   Each node must have the same list of IP addresses and the same Router ID, but have a unique Priority setting. The Priority setting determines which node in the cluster is the Primary node. The node with the higher priority is considered the default Primary node.



Port1

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

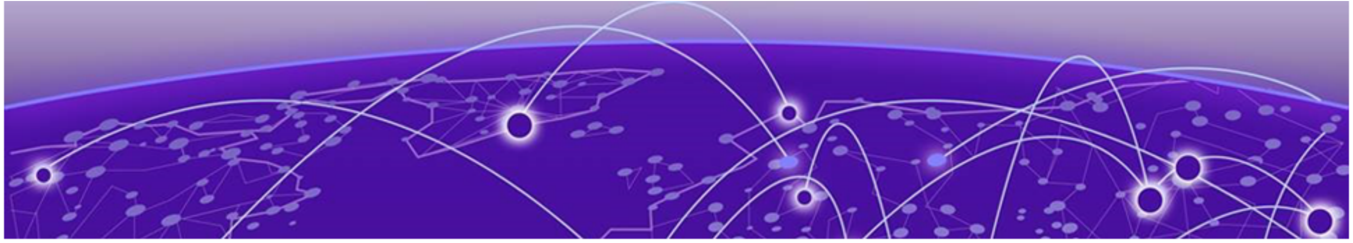
VRRP
IP Address (comma separated):

Priority:

Router ID:

Figure 7: User Interface showing properties window for Port 1

5. Repeat this process in each of the nodes of the cluster.



Configure the Cluster Settings

An engine is an instance of a containerized application. This process follows the user interface to configure the orchestration engine settings. 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 25.

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

1. Deployment Type
2. Cluster Node Information

3. Pod Network Configuration
4. Finish

Figure 8: Configure Cluster Settings

1. Select **Distributed Cloud Deployment** in the **Deployment Type** drop-down list.

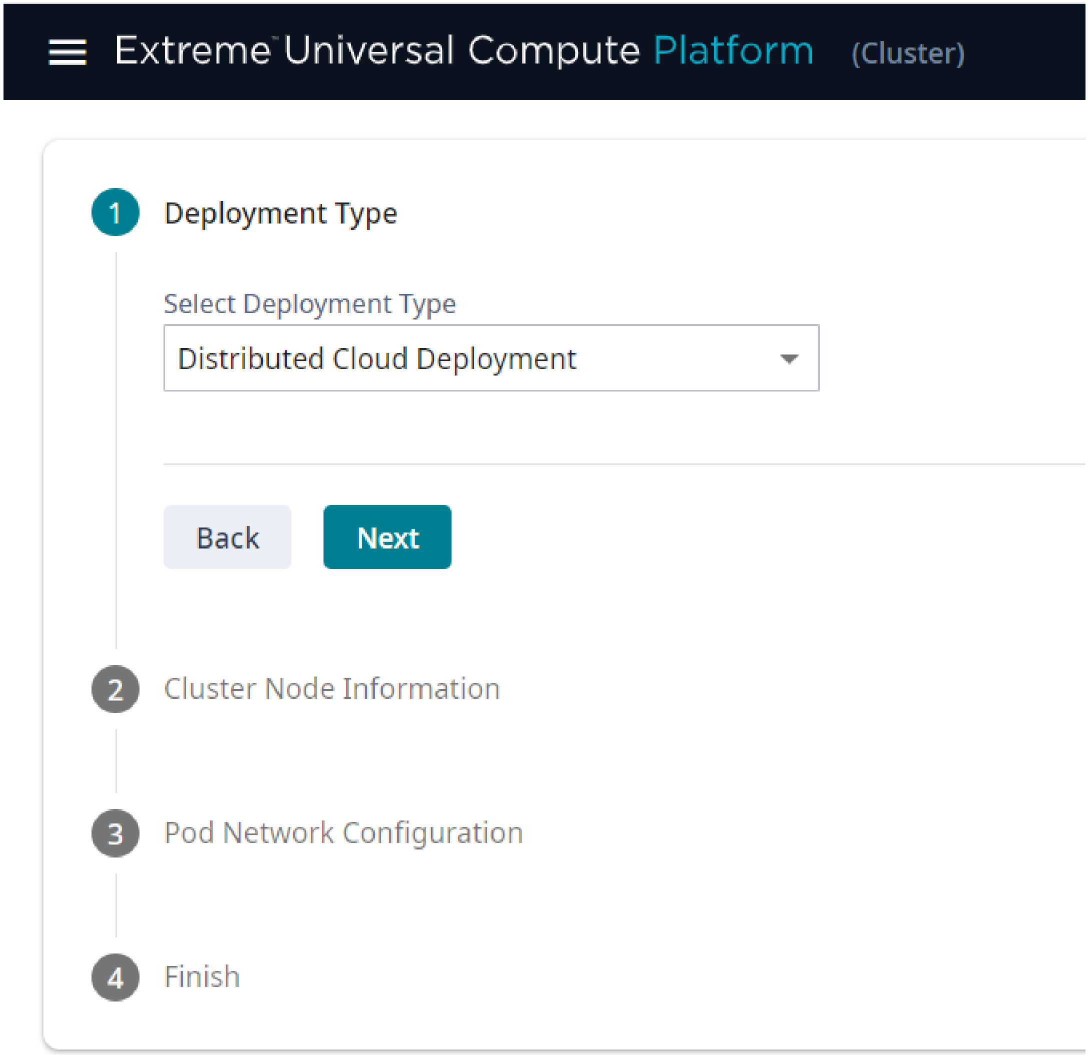
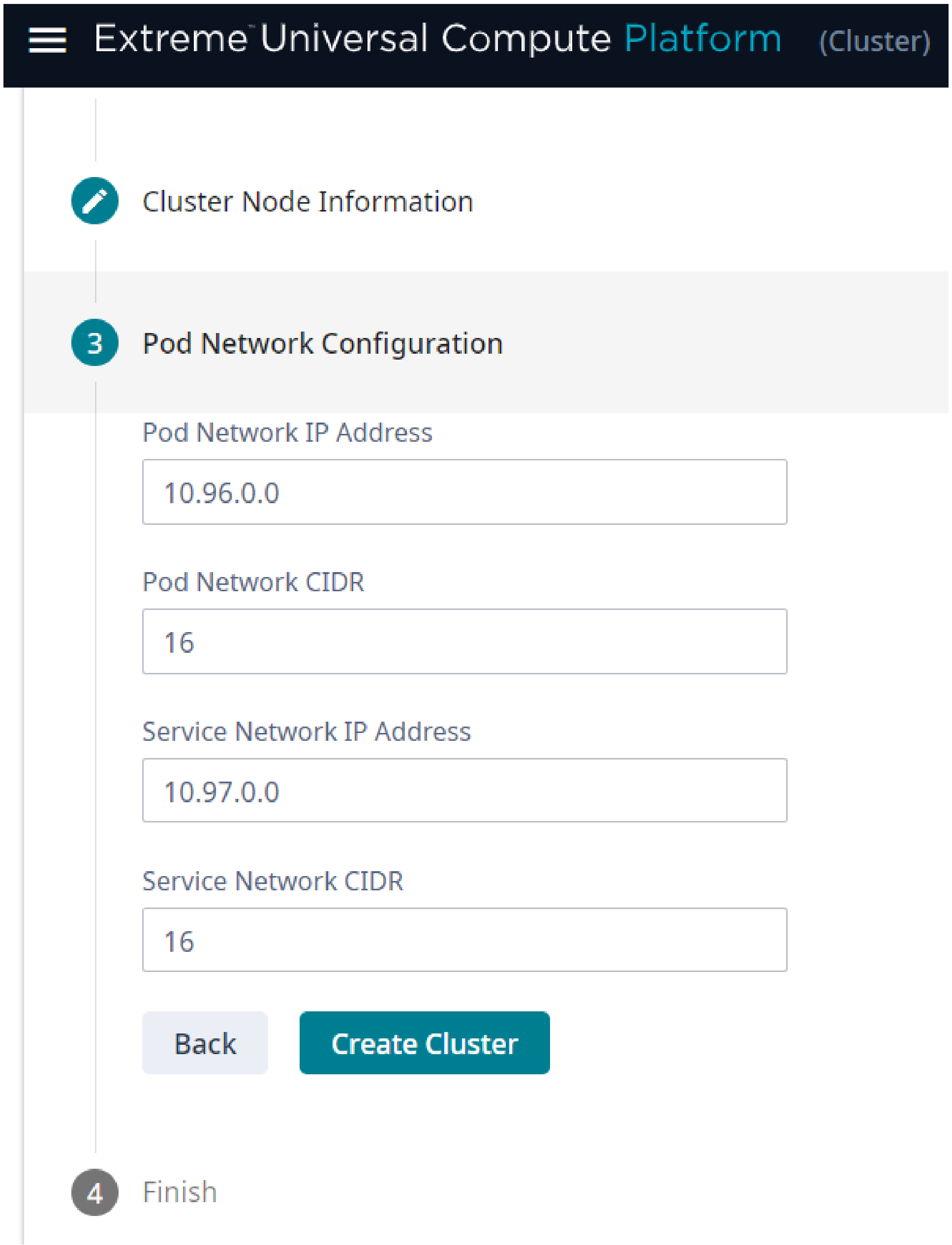

Extreme Universal Compute Platform (Cluster)
1 Deployment Type
Select Deployment Type
Distributed Cloud Deployment
Back
Next
2 Cluster Node Information
3 Pod Network Configuration
4 Finish

Figure 9: Deployment Type Selection

2. Provide the settings for **Pod Network Configuration**:
   - Pod Network IP Address
   - Pod Network CIDR
   - Service Network IP Address
   - Service Network CIDR


Extreme Universal Compute Platform (Cluster)
Cluster Node Information
3 Pod Network Configuration
Back
Create Cluster
4 Finish

Pod Network IP Address: 10.96.0.0

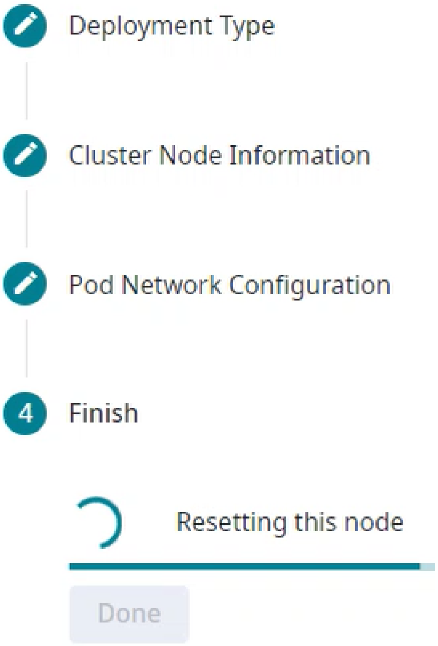
Pod Network CIDR: 16

Service Network IP Address: 10.97.0.0

Service Network CIDR: 16

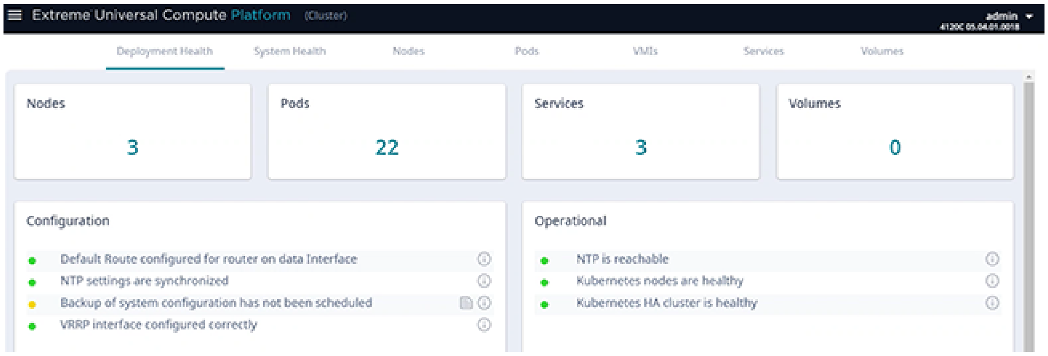
Figure 10: Pod Settings

3. Select **Create Cluster**.



Resetting this node

4. Select **Done**.



Nodes 3

Pods 22

Services 3

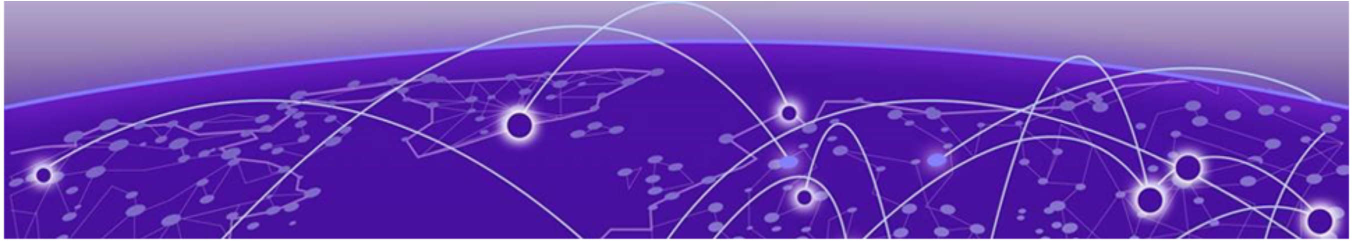
Volumes 0

Configuration

- Default Route configured for router on data Interface
- NTP settings are synchronized
- Backup of system configuration has not been scheduled
- VRRP interface configured correctly

Operational

- NTP is reachable
- Kubernetes nodes are healthy
- Kubernetes HA cluster is healthy



Select an Engine

From the **Engines** page, select the engine type for your cluster.

ExtremeCloud™ IQ is the only available engine for an ExtremeCloud Edge deployment. An Edge Cloud deployment of ExtremeCloud IQ must be configured in a cluster of six or more nodes without other engine types.

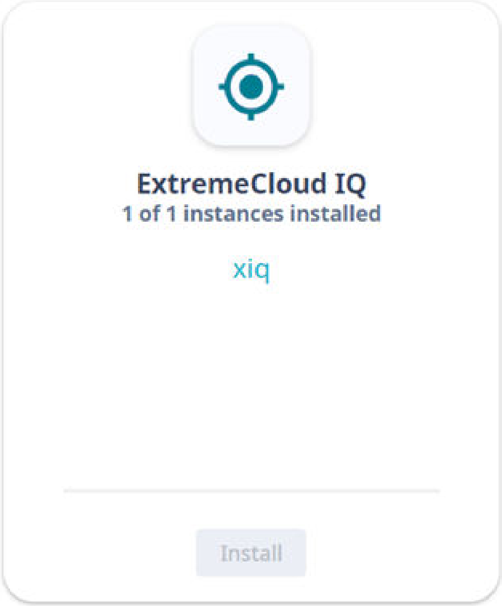
Install an Engine Instance

Install ExtremeCloud IQ engine once from a single node.

To install an engine instance:

1. Go to **Engines**.
2. From the ExtremeCloud IQ pane, select **Install**.

   After installation is complete, a confirmation notice is displayed and the XIQ instance displays.



ExtremeCloud IQ

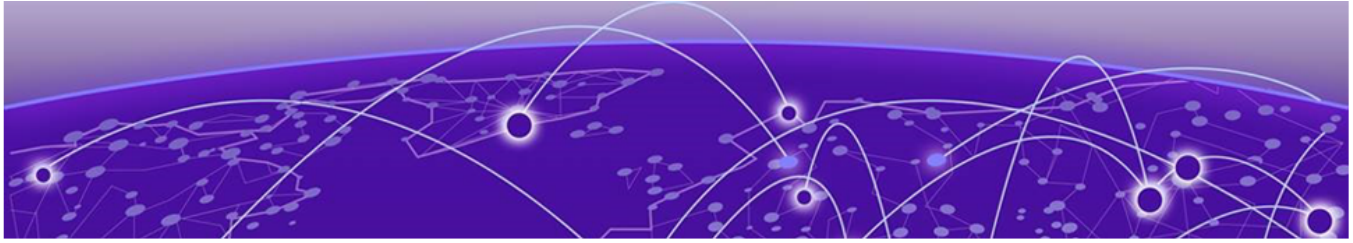
1 of 1 instances installed

xiq

Figure 11: Installed ExtremeCloud IQ Engine Instance

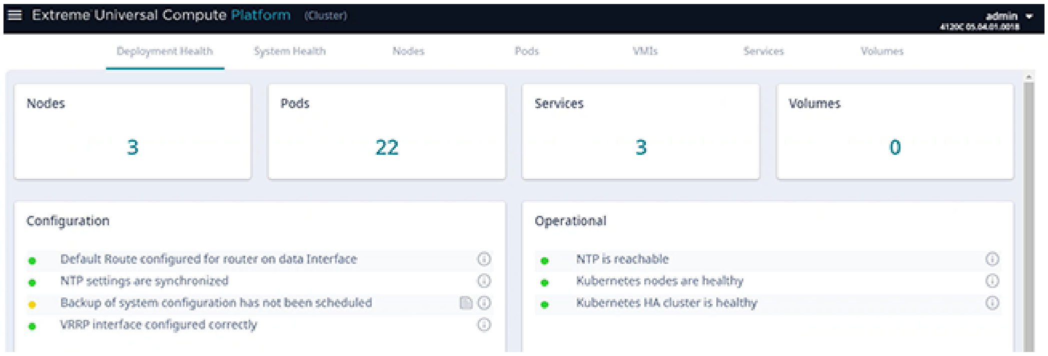
Network Service Configuration

Map each core service set to the corresponding Virtual Router Redundancy Protocol (VRRP). Assign a VRRP virtual router address for each set of services. VRRP enables a virtual router to act as the default network gateway, improving host network reliability and performance.



Validate the Cluster

Click the **Deployment Health** tab for information.



Nodes 3

Pods 22

Services 3

Volumes 0

Configuration

- ● Default Route configured for router on data Interface
- ● NTP settings are synchronized
- ● Backup of system configuration has not been scheduled
- ● VRRP interface configured correctly

Operational

- ● NTP is reachable
- ● Kubernetes nodes are healthy
- ● Kubernetes HA cluster is healthy

Onboard the Cluster to ExtremeCloud IQ

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

- From Universal Compute Platform, configure cloud visibility.
- Onboard the cluster to your ExtremeCloud IQ account.
- Initiate action for the ExtremeCloud IQ Operations team to deploy a Regional Data Center (RDC) for the cluster.
- Register your ExtremeCloud IQ account.
- Onboard your devices and operate the account.

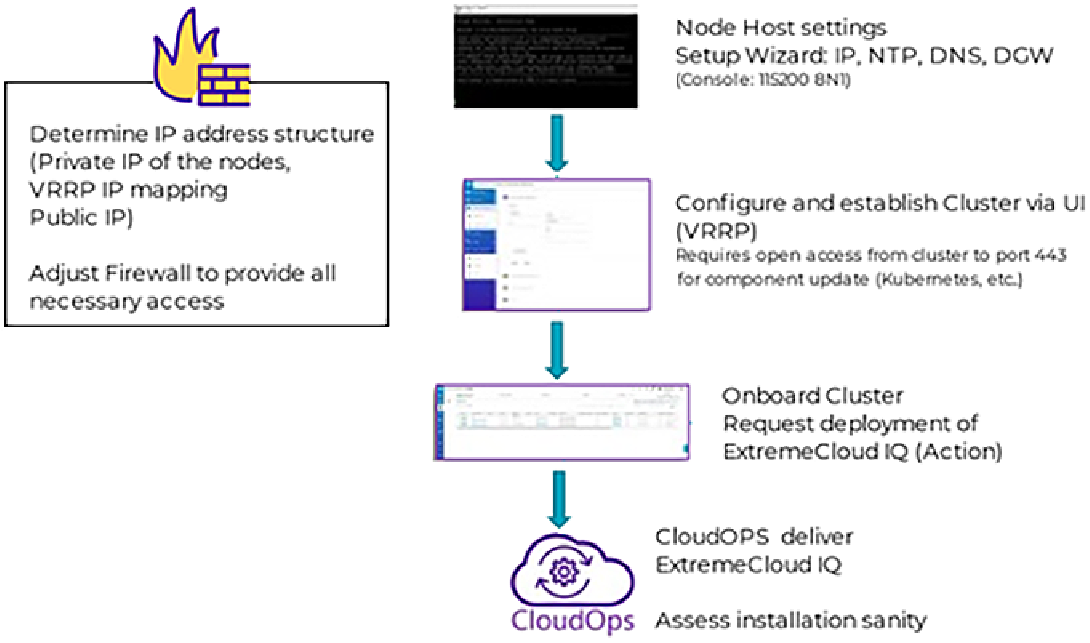
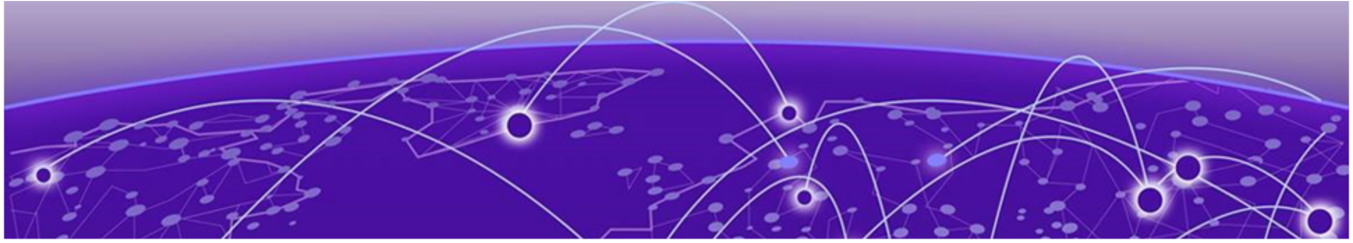

Determine IP address structure
(Private IP of the nodes,
VRRP IP mapping
Public IP)
Adjust Firewall to provide all necessary access
Node Host settings
Setup Wizard: IP, NTP, DNS, DGW
(Console: 115200 8N1)
Configure and establish Cluster via UI (VRRP)
Requires open access from cluster to port 443 for component update (Kubernetes, etc.)
Onboard Cluster
Request deployment of ExtremeCloud IQ (Action)
CloudOPS deliver ExtremeCloud IQ
Assess installation sanity
CloudOps

Figure 12: ExtremeCloud Edge Deployment Workflow

Related Topics

[Cloud Visibility](#) on page 42

[Account Registration](#) on page 47



Cloud Visibility

Generally, the connection between Universal Compute Platform and your ExtremeCloud IQ Regional Data Center (RDC) will be made through automatic discovery. If necessary, follow these steps 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.

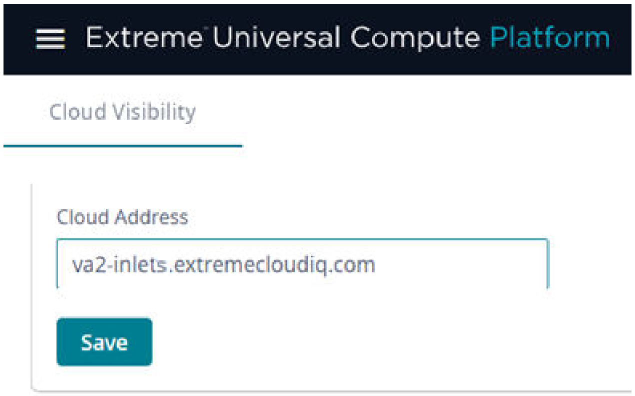
   ```
   rdc-inlets.host address
   ```

   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

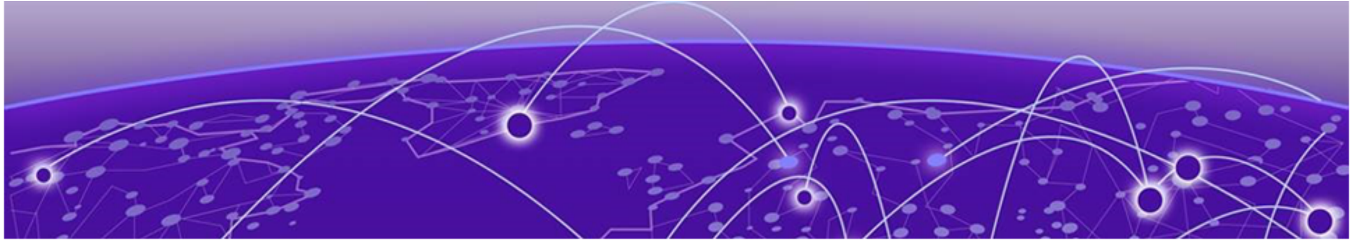
   Figure 13: Cloud Visibility: ExtremeCloud IQ Address

3. Select **Save**.

NEW! Add Web Proxy Server

For enhanced data security, you can add a web proxy server. A proxy server is an additional server in a client-server deployment that provides additional data security boundaries, protecting users from malicious activity on the internet.

1. Select the navigation menu ☰ and select **Administration** > **System** > **Settings**.
2. Select the **Web Proxy** tab.
3. Enter the **IP Address** of the proxy server along with the server **Port** to which you should connect.
4. If the proxy server requires authentication, select **Authentication** and enter the **Username** and **Password** for an account that has access to the proxy server.
5. Select **Save**.



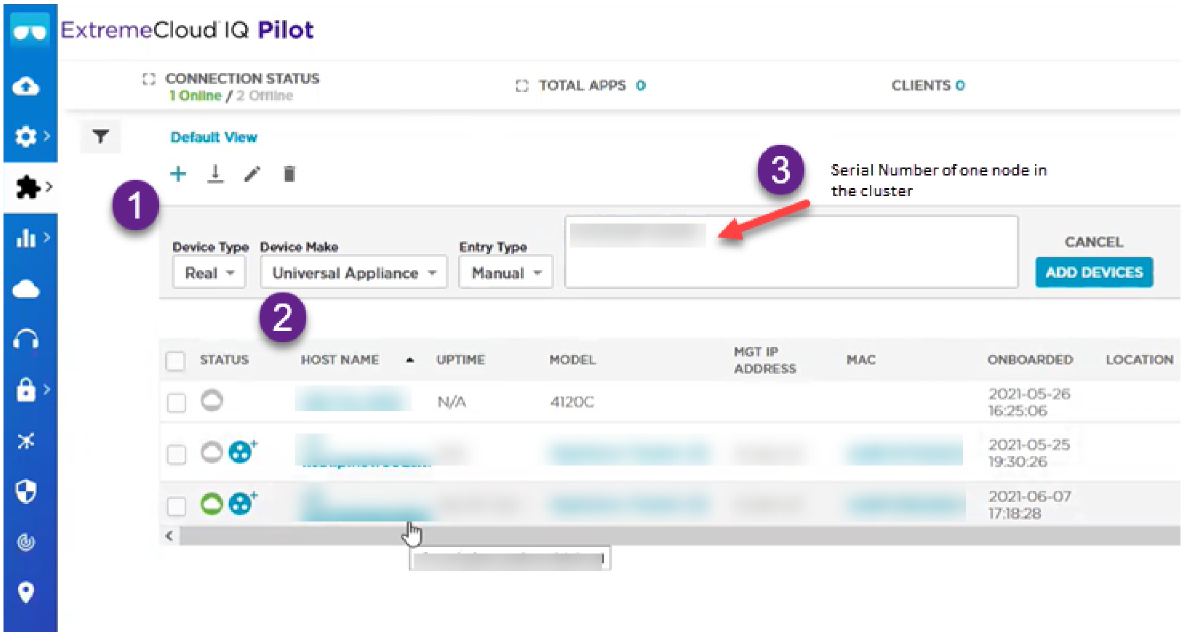
Onboarding a Cluster to ExtremeCloud IQ

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 Devices**.
2. Select **Quick Add** (+).
3. In the Serial Number field, enter the serial number for one node in the cluster.

   The **Device Make** field displays.
4. From the Device Make field, select **Universal Appliance**.

   Figure 14: Manually adding a cluster to ExtremeCloud IQ



Device Type: Real
Device Make: Universal Appliance
Entry Type: Manual
Serial Number: [redacted]

	STATUS	HOST NAME	UPTIME	MODEL	MGT IP ADDRESS	MAC	ONBOARDED	LOCATION
□	○	[redacted]	N/A	4120C			2021-05-26 16:25:06	
□	○	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2021-05-25 19:30:26	
□	○	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2021-06-07 17:18:28	

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.

6. Select **Actions** > **Applications** > **ExtremeCloud IQ Manage**.

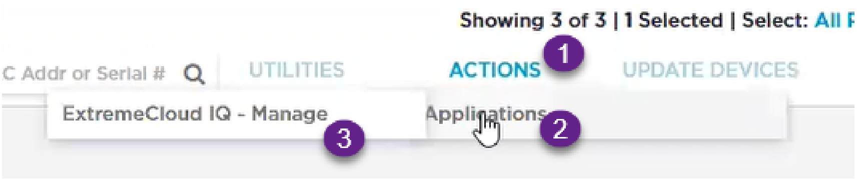
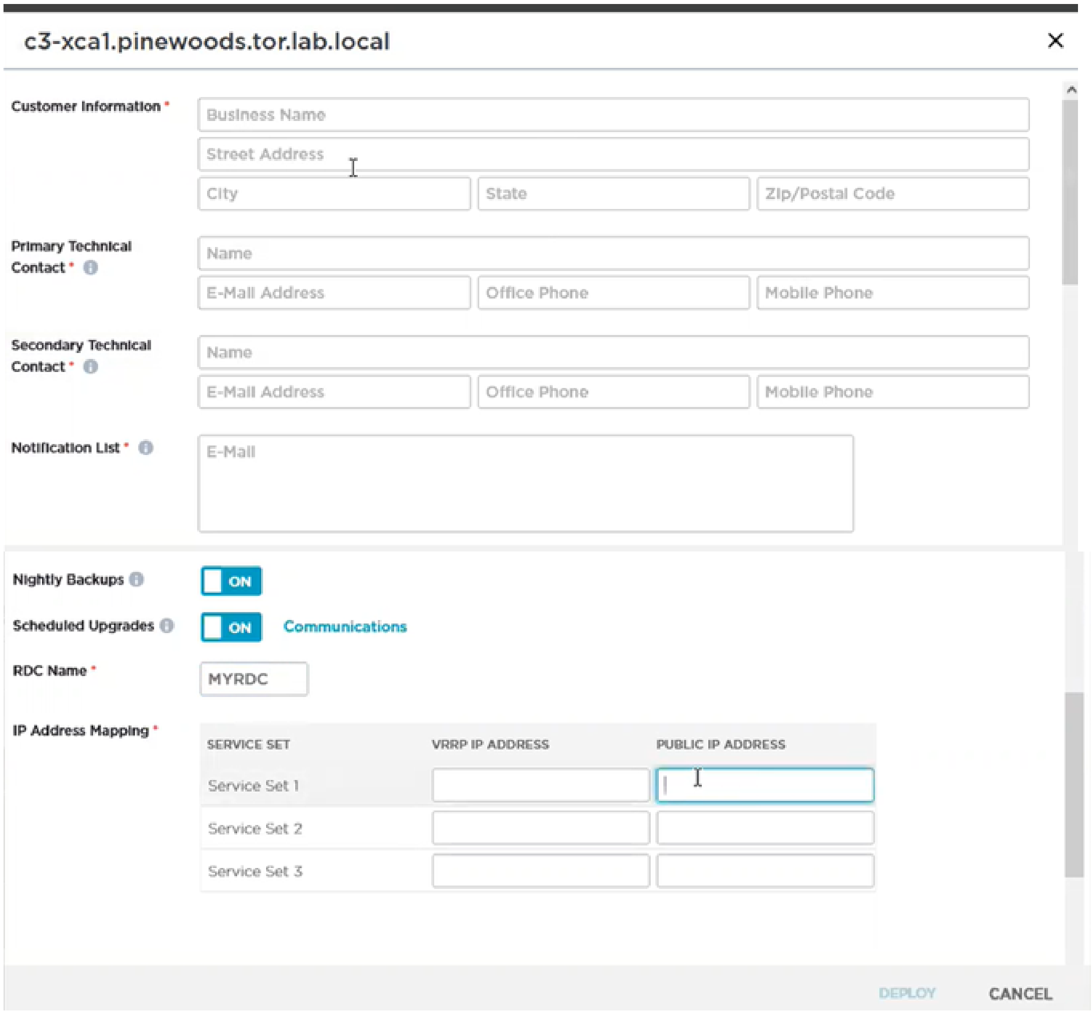
   

   Figure 15: ExtremeCloud IQ Actions menu

   This initiates the action for ExtremeCloud IQ OPs to deploy a Regional Data Center (RDC) for the cluster.
7. Fill out the online form:

   Note
   Required fields are noted with an asterisk.

   - Customer Information
   - Primary Technical Contact
   - Secondary Technical Contact
   - Notification List — Provide a list of email addresses for notification.
   - Nightly Backup
   - Scheduled Upgrades
   - RDC Name — Provide a meaningful name, up to 6 characters. The system will verify that the name is available.
   - IP Address Mapping — Provide the mapping between the external Public IP Address to the internal virtual VRRP IP Address for each service set.



c3-xca1.pinewoods.tor.lab.local ✕

Customer Information *: Business Name | Street Address | City | State | Zip/Postal Code

Primary Technical Contact *: Name | E-Mail Address | Office Phone | Mobile Phone

Secondary Technical Contact *: Name | E-Mail Address | Office Phone | Mobile Phone

Notification List *: E-Mail

Nightly Backups: ON

Scheduled Upgrades: ON Communications

RDC Name *: MYRDC

IP Address Mapping *

SERVICE SET	VRRP IP ADDRESS	PUBLIC IP ADDRESS
Service Set 1		
Service Set 2		
Service Set 3		

Figure 16: ExtremeCloud IQ Deploy a Cluster Form

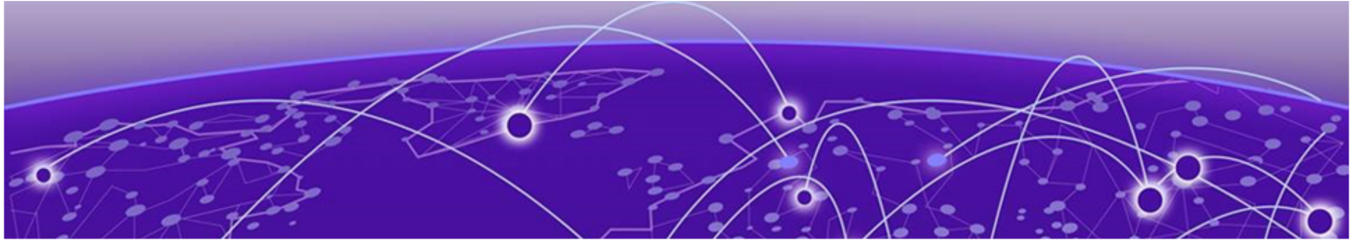
8. Select **Deploy**.

   A ticket is generated for ExtremeCloud IQ OPs. Operations personnel will provide an estimate for the expected deployment schedule.

   During deployment OPs team will do the following:

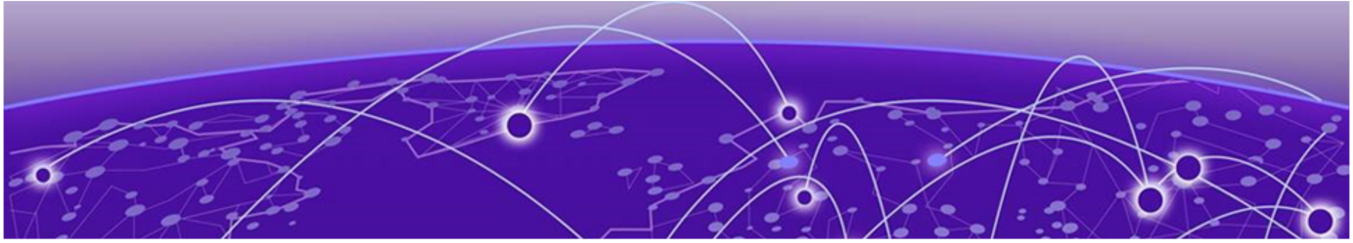
   - Deploy ExtremeCloud IQ software to the on-premise hosts
   - Validate the deployment to ensure the site is deployed and operating correctly
   - Once validated, OPs will provide notification of readiness
   - Provide the installation token that enables customers to create accounts directly on the newly deployed ExtremeCloud IQ private Regional Data Center (RDC).

9. You can view the status of the deployment process from the **Application Status** column on the **Device List**.



Account Registration

For information about creating accounts after you set up ExtremeCloud Edge, consult the Managed Service Partner (MSP) documentation.



Appendix: Migrate Virtual IQ Account

This Appendix describes how to migrate a Virtual IQ (VIQ) account to a new Regional Data Center (RDC). To migrate the account, complete each of the subsequent procedures in order:

1. Export VIQ Account
2. Import VIQ Account

> Note
> Moving the VIQ account also moves the account inventory (for example, devices, floor plans, private pre-shared keys) as well as configurations and assignments.

Export VIQ Account

Use this procedure to create and download an export file for a VIQ account.

1. In ExtremeCloud IQ Pilot, go to **Global Settings** and select **VIQ Management.**
2. Create a backup of the current VHM:
    a. Under **VIQ Management**, select **BACK UP NOW**.
    b. Select **YES**.

       VIQ suspends itself until the backup completes.
3. Export the VHM to a local drive:
    a. Go to **Global Settings** and select **VIQ Management**.
    b. Select **Export VIQ**.
    c. In the **VIQ Export** popup window, select **Export Now**.
    d. Click **YES**. VIQ suspends itself until the Export completes.
    e. Once the export completes successfully, select **OK**.

    > Note
    > If the export fails, click the **Detailed Report** link to get a detailed report on the issue.

What to do Next

After the export file downloads, you can import the file into a different Regional Data Center (RDC).

Import VIQ Account

Use this procedure to import the VIQ export file into the new RDC. Note the following:

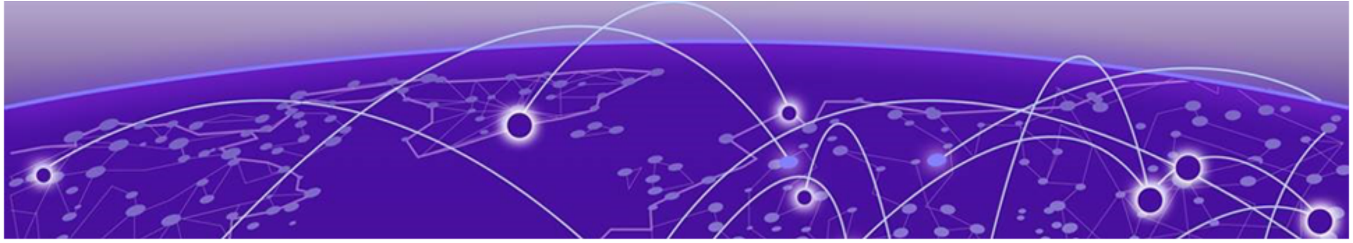
- If a conflict occurs, imported objects get renamed.
- Source and destination VHMs must be the same version. Otherwise, an incompatible data scheme occurs.

1. From ExtremeCloud IQ Pilot, go to **Global Settings** > **VIQ Management**.
2. Create a backup of the current VHM:
    a. Under **VIQ Management**, select **BACK UP NOW**.
    b. Select **YES**.

    VIQ suspends itself until the backup completes.
3. Import the VHM export file that you created in the preceding procedure:
    a. Select **Import VIQ**.
    b. Select **Import VIQ from ExtremeCloud IQ**.
    c. Select **Choose** and then browse and select the VHM export file.
    d. Select **Import Now**.
    e. After the import completes, select **OK**.

    Note

    - If the import fails, download the log file for information on the issues.
    - If you need to roll back the import, restore the backup.



Index