



Universal Compute Platform User Guide

Version 5.07.01

9038933-00 Rev. AA
June 2024



Copyright © 2024 Extreme Networks, Inc. All rights reserved.

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

Preface.....	5
Text Conventions.....	5
Documentation and Training.....	6
Open Source Declarations.....	7
Training.....	7
Help and Support.....	7
Subscribe to Product Announcements.....	8
Send Feedback.....	8
Welcome to Universal Compute Platform.....	9
Navigating the User Interface.....	9
Dashboard.....	10
Dashboard Overview.....	10
Deployment Health.....	10
System Health Dashboard.....	11
Nodes Dashboard.....	11
Pods List.....	12
VMI List.....	12
Services List.....	12
Volumes List.....	13
Cluster Settings.....	15
Cluster Configuration.....	15
Deployment Type.....	15
Cluster Node Information.....	16
Pod Network Configuration.....	16
Certificates.....	17
Prepare to Replace a Node.....	18
Replace a Node.....	18
Add Node.....	19
Engines.....	21
Engine Options.....	21
ExtremeCloud Edge - Managed Orchestration.....	21
ExtremeCloud Edge - Self-Orchestration.....	24
Engine Upgrades.....	27
Upgrade an Application (Self-Orchestrated).....	28
Tools.....	29
Logs.....	29
Diagnostics.....	30
Network Utilities.....	30
TCP Dump Management.....	31

Administration.....	32
Manage User Accounts.....	32
Add a User Account.....	32
Modify a User Account.....	33
Delete a User Account.....	34
Account Settings.....	34
System Configuration.....	34
Configuration.....	35
System Logging.....	39
Maintenance.....	40
Network Setup.....	40
Network Time.....	45
Settings.....	45
Upgrade the Universal Compute Platform	46
System Information.....	51
Utilities.....	52
Index.....	53



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 <i>enter</i> and <i>type</i>	When you see the word <i>enter</i> 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 <i>type</i> .
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.
<i>italic text</i>	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, <i>member [member...]</i> .
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

[Current Product Documentation](#)

[Release Notes](#)

[Hardware and Software Compatibility](#) for Extreme Networks products

[Extreme Optics Compatibility](#)

[Other Resources](#) such as articles, white papers, and case studies

Open Source Declarations

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

Training

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

Help and Support

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

Extreme Portal

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

The Hub

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

Call GTAC

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

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

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

Subscribe to Product Announcements

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

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

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

Send Feedback

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

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

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

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




Welcome to Universal Compute Platform

[Navigating the User Interface](#) on page 9

The Universal Compute Platform serves as a service platform for an on-premises application offering. The Universal Compute Platform provides a performance validated hosting platform, supporting advanced orchestration of a catalog of applications. The Universal Compute Platform provides a container-based orchestration framework, in an Extreme Networks qualified and validated high-performance hardware configuration. The framework natively supports clustering, a distributed file system, and orchestration through Kubernetes, providing a highly resilient application operational base.

Navigating the User Interface

To open the navigation menu for the Universal Compute Platform user interface, select the navigation icon () from the top left of the interface header. From the navigation menu, you can select one of the menu options to go to the desired page.



Dashboard

[Dashboard Overview](#) on page 10

The topics in this section describe the dashboards that are available when you select the **Dashboard** menu option.

Dashboard Overview

Universal Compute Platform offers dashboards and lists that help you monitor the cluster configuration and performance.

Universal Compute Platform offers the following dashboards and reports:

- Deployment Health
- System Health
- Dashboard Nodes
- Pods List
- Services List
- Volumes List

Deployment Health

The **Deployment Health** Dashboard provides information about the overall health of the node cluster. The top pane highlights each piece of the cluster network:

- Nodes. The number of appliances in your network. You have the option of configuring individual stand-alone nodes or a cluster of three or more nodes. Stand-alone configuration is supported for all engine types except ExtremeCloud IQ.



Note

When using an ExtremeCloud™ IQ engine, you must configure a cluster of three or more nodes in multiples of three (for example, three, six, or nine nodes). ExtremeCloud IQ is not supported in stand-alone mode, requires a cluster, and does not support engine types other than ExtremeCloud IQ.

- Pods. 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.
- Services. Network Services running on the node cluster.
- Volumes. Storage that allows data to be accessible to containers within a pod.

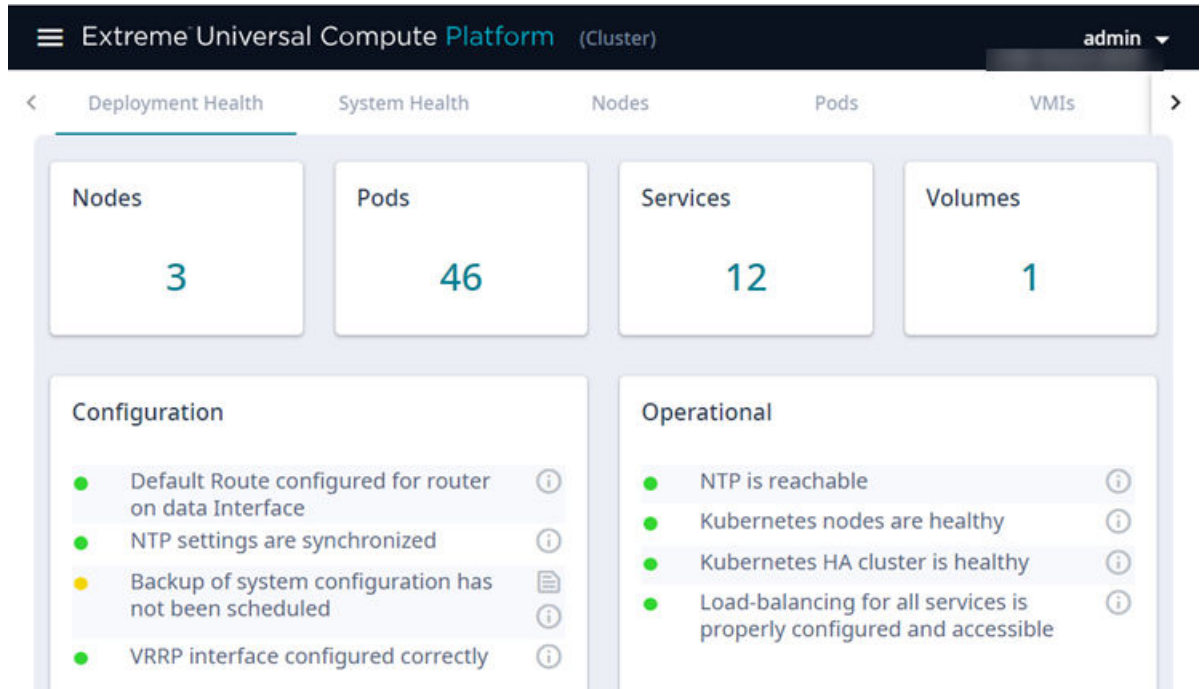


Figure 1: Deployment Health Dashboard

Deployment Health also provides best practice information for your Universal Compute Platform configuration. System Health checks are run against your configuration and operational setup to inform you of best practices.

- ● Green indicates that a best practice is being followed.
- ● Yellow indicates that your configuration is not optimal.
- ● Red indicates an error in your configuration.

Fix all error conditions. You have the option to ignore warnings. They are provided to inform and encourage best practice configuration.

- Select i for a description of each statement or warning.
- Select ☰ to list objects causing an issue, and to jump to that area of Universal Compute Platform to improve your configuration.

System Health Dashboard

The **System Health** dashboard provides the following information:

- System Uptime — The number of days and hours the system has been operational.
- CPU Utilization — CPU Utilization metrics over time.
- Memory Utilization — Memory Utilization metrics over time.

Nodes Dashboard

The **Nodes Dashboard** provides graphs for CPU utilization and memory utilization for each node in the cluster.

Pods List

The **Pods List** displays a list of pods in your cluster. A pod is a group of managed containers that share networking and storage resources from the same node. The following information is provided for each pod:

- Pod Name
- Ready status
- Status — Possible values are Running or Down.
- Restarts
- Age — Measured in minutes, hours, and days.
- IP address
- Node

Use the Search field to find a specific list item.

You can select the number of items to display on a page. Valid values are:

- 10
- 20
- 50
- 100

To jump to the next or previous page, or jump to the first or last page, select the arrows at the bottom of the page.

VMI List

VMI stands for Virtual Machine Instance. The following information is provided for each VMI:

- Name
- Phase
- Node Name
- QoS Class
- Namespace
- Created

Expand each VMI to display the following information:

- CPU: Cores
- Volumes
- Interfaces: IP Address and MAC

Services List

The **Services List** displays a list of all services running in the cluster. The Service Name and Namespace are provided for each service.

Use the Search field to find a specific list item.

SERVICE NAME	NAMESPACE
adspsvc	adsp-1
glusterfs-cluster	adsp-1
cdi-api	cdi
cdi-prometheus-metrics	cdi
cdi-uploadproxy	cdi
kubernetes	default
kube-dns	kube-system
metrics-server	kube-system
kubevirt-operator-webhook	kubevirt
kubevirt-prometheus-metrics	kubevirt
virt-api	kubevirt
wingsvc	wing-1

Figure 2: List of services running on the node cluster

You can select the number of items to display on a page. Valid values are:

- 10
- 20
- 50
- 100

To jump to the next or previous page, or jump to the first or last page, select the arrows at the bottom of the page.

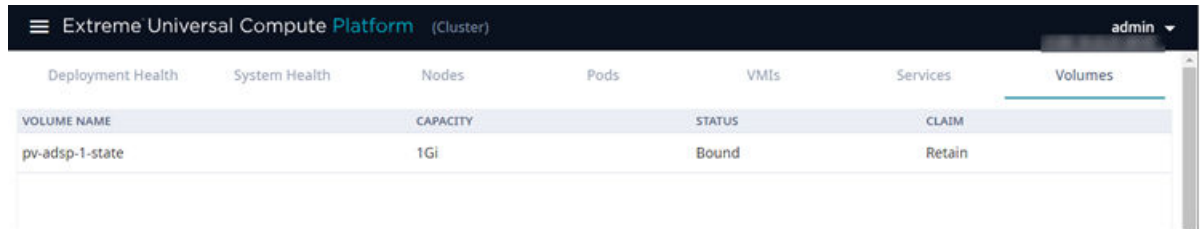
Volumes List

The **Volumes List** displays a list of all volumes in the cluster. A volume is storage that allows data to be accessible to containers within a pod. The following information is provided for each volume:

- Volume Name
- Capacity

- Status
- Claim. Associated with the volume type and how the data is handled in the volume. If the data will be retained, the Claim value is **Retain**.

Use the Search field to find a specific list item.



The screenshot shows the 'Volumes' tab in the Extreme Universal Compute Platform dashboard. The dashboard header includes 'Extreme Universal Compute Platform (Cluster)' and a user profile 'admin'. The navigation menu includes 'Deployment Health', 'System Health', 'Nodes', 'Pods', 'VMIs', 'Services', and 'Volumes'. The 'Volumes' table has the following data:

VOLUME NAME	CAPACITY	STATUS	CLAIM
pv-adsp-1-state	1Gi	Bound	Retain

Figure 3: List of Volumes associated with a node

You can select the number of items to display on a page. Valid values are:

- 10
- 20
- 50
- 100

To jump to the next or previous page, or jump to the first or last page, select the arrows at the bottom of the page.



Cluster Settings

[Cluster Configuration](#) on page 15

The topics in this section describe the options that are available under the **Cluster Settings** menu.

Cluster Configuration

The **Cluster Configuration** page outlines the settings provided when deploying the cluster.



Note

For information on how to deploy a Universal Compute Platform cluster, see the following guides:

- [ExtremeCloud Edge - Managed Orchestration Deployment Guide for Universal Compute Platform](#)
- [ExtremeCloud Edge - Self-Orchestration Deployment Guide for Universal Compute Platform](#)

Go to **Cluster Settings > Cluster Configuration** to view the cluster deployment settings.

The following information is provided:

Deployment Type

Select the desired deployment type. Universal Compute Platform supports the following deployment types:

Select the deployment type. Valid values are:

- **ExtremeCloud Edge - Managed Orchestration**—ExtremeCloud IQ as a distributed cloud application. Supported only on 4120C-1.
- **ExtremeCloud Edge - Self-Orchestration**—A variety of on-premise controller applications.

Select **Next**.

Cluster Node Information

Universal Compute Platform supports a stand-alone mode and a full-cluster mode. Stand-alone mode requires only one defined node, but a cluster can be deployed using multiples of three (for example, three, six, or nine nodes) depending on your resource requirements.

Configure only one node for stand-alone mode or configure a full cluster of nodes (using multiples of three).



Note

When using an ExtremeCloud™ IQ engine, you must configure a cluster of three or more nodes in multiples of three (for example, three, six, or nine nodes). ExtremeCloud IQ is not supported in stand-alone mode, requires a cluster, and does not support engine types other than ExtremeCloud IQ.

1. Provide the ICC IP Address for each node in the cluster.
2. Select **Next**.

When the Deployment Type is ExtremeCloud Edge - Self-Orchestration, you have a variety of engine options to choose from, including the following:

- ExtremeWireless WiNG™ Controller
- Extreme Tunnel Concentrator
- ExtremeCloud™ IQ Controller

Pod Network Configuration

Pods are groups of containers that share networking and storage resources from the same node.

1. Provide the following Pod Network configuration settings:
 - Pod Network IP Address
 - Pod Network CIDR
 - Service Network IP Address
 - Service Network CIDR
2. Select **Create Cluster**.

The cluster is created.

If a cluster previously existed, the cluster connections are reset. Then, you must reinstall the engines for each node in the cluster.

Related Topics

[Engine Options](#) on page 21

[Certificates](#) on page 17

Certificates

To ensure a secure website that takes advantage of encryption, Universal Compute Platform uses browser certificates for website security and RADIUS server certificates for certificate-based authentication to the network. The browser certificate ensures security between the wireless clients and a VLAN, and the RADIUS server certificates ensure security between the RADIUS server and Network Access Control.

Both types of certificates offer the option to generate a new certificate or use a certificate and key file that you have saved. You can also reset the network interface to the default certificate and key, which yields a Self-Signed certificate.

Universal Compute Platform offers a factory installed self-signed certificate, which is used by the user interface HTTP Server to terminate the HTTPS browser requests served on port 5825. The certificate common name is *Network Services Engine*.

Related Topics

[Generate Certificates](#) on page 17

Generate Certificates

Browser certificates are used for website security. Generate a certificate or use a saved certificate and key from one or more files.

1. Select **Certificates**.

The **Certificates** dialog displays.

2. Select the Certificate option:

- **Replace or Install Topology's certificate**

Select this option and select **Generate CSR**. Complete the online form, then generate and download the certificate that can be presented to a public certificate authority.

- **Replace or Install Topology's certificate and key from a single file**

Select this option and navigate to the saved certificate file. Provide the password key provided with that file.

- **Replace or Install Topology's certificate file and key from separate files**

Select this option and navigate to the saved certificate file and separate key file.

- **Reset to Topology's default certificate and key**

Select this option to clear previous certificates and reset the Universal Compute Platform to the default configuration of the Self-Signed certificate.



Note

When certificates are applied or reset on the Admin topology, a server restart is triggered, and the browser loses connectivity with the server for a few seconds. When certificates are applied or reset on System topologies where **Management Traffic** is enabled, the server is also restarted.

Prepare to Replace a Node

1. Gather the IP address settings of the failed node.

Unless stated otherwise, you will set the new node with the same IP address values as the unit being replaced:

- ICC Interface IP Address—For the ICC interface, you must assign a new IP address to the replacement node.
- Data Port Interface IP Address
- DNS Server Address
- NTP Server Address

2. Configure the VRRP priority for the replacement node.



Note

To ensure that the replacement node successfully joins the cluster, set the VRRP node priority of the replacement node to a value that is lower than the value of the existing nodes. This ensures that the VRRP address is pointing at a working node in the cluster during the joining process. After the replacement node has joined the cluster, you can set the VRRP node priority to first priority if desired, but this is not required.

3. Use the Basic Configuration Wizard to configure the replacement unit.

This is required if you are replacing the unit hardware. Node Replacement initially resets the node connections. It may not require new hardware.

For information about the Basic Configuration Wizard, see the appropriate Deployment Guide.

4. [Upgrade the Universal Compute Platform](#) on page 46 for the new node to the current software version.

After you have gathered the necessary information and verified the software version of all nodes in the cluster, you can run the [Replace a Node](#) on page 18 procedure.

Replace a Node

Replacing a node in a cluster is performed when a node has failed and must be replaced. The replacement node gets delivered in a reset state. After initializing the node for its network presence, the new node is added to the cluster and assumes the service load of the removed node.

From the primary node in the cluster (Node 1), take the following steps:

1. Go to **Cluster Services > Node Replacement**.

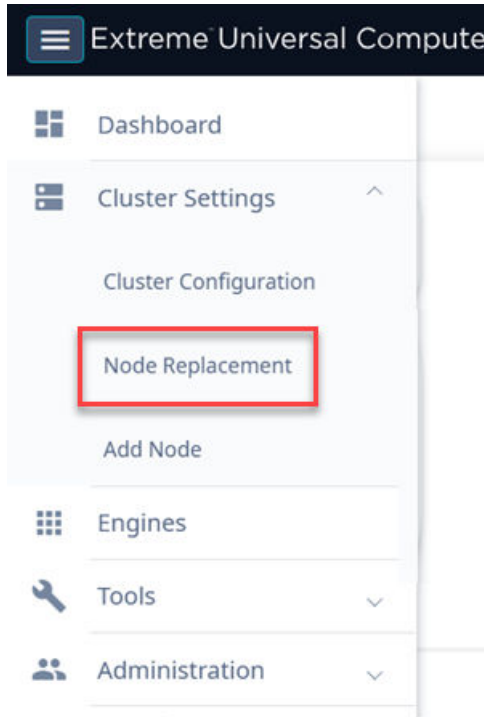


Figure 4: Node Replacement

2. Select the failed node and select **Next**.

Existing credentials are used to establish connection to the failed node.

Configuration and services information is transferred from the primary node to the failed node in an effort to re-establish a connection.

If it is necessary to replace the node hardware, refer to the [Universal Compute Platform Appliance 4120C Installation Guide](#) for detailed information.

Add Node



Note

Before adding a new node, you must configure the new controller and ensure that it is running the current software version. Refer to [Prepare to Replace a Node](#) on page 18.

**Note**

This option is not available in standalone deployments.

For detailed instructions on appliance installation and cluster planning and configuration, see the appropriate guide:

- [Universal Compute Platform 4120C Appliance Installation Guide](#)
- [ExtremeCloud Edge - Managed Orchestration Deployment Guide for Universal Compute Platform](#).

A node is one appliance. Universal Compute Platform clusters typically support up to three or more nodes, with the ability to scale up when the cluster reaches capacity.

To add a node to a cluster, take the following steps:

1. Go to **Cluster Settings > Add Node**.

The screenshot shows a dark header bar with a hamburger menu icon, the text 'Extreme Universal Compute Platform', and '(Cluster)'. Below this is a light gray dialog box. At the top left of the dialog is a teal circle with the number '1' and the text 'Add Node'. Below this is a label 'Node IP Address' and a text input field containing '10.48.4.51'. Underneath the input field is a teal button labeled 'Add Node'. At the bottom left of the dialog is a teal circle with a pencil icon and the text 'Finish'.

Figure 5: Add Node dialog

2. Provide the appliance IP address for the node and select **Add Node**.
The **Node Addition** confirmation dialog displays.

This will add the requested node to the cluster. Do you want to continue?

The screenshot shows a light gray dialog box with the text 'This will add the requested node to the cluster. Do you want to continue?'. At the bottom right of the dialog are two buttons: a gray 'Cancel' button and a teal 'Ok' button.

Figure 6: Add Node Confirmation Dialog

3. Select **OK** to begin the Add Node process.



Engines

[Engine Options](#) on page 21

[Engine Upgrades](#) on page 27

The topics in this section describe the options that appear under the **Engines** menu.

Engine Options

From the **Engines** menu you can install an engine and upgrade an engine application Docker image. The engines that are available depend on the deployment type that you selected under [Cluster Configuration](#) on page 15.

The following deployment types are available:

- [ExtremeCloud Edge - Managed Orchestration](#) (available on 4120C-1 only)
- [ExtremeCloud Edge - Self-Orchestration](#)

For more information, see:

- For documentation, see [Universal Compute Platform documentation](#).
- For training information, see [Managed Orchestration Deployment Training Videos](#).

ExtremeCloud Edge - Managed Orchestration

Install the Engine

In an ExtremeCloudEdge - Managed Orchestration deployment, ExtremeCloud™ IQ is the only available engine. Install ExtremeCloud IQ engine once to be automatically distributed across three nodes..

To install an engine instance:

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

After installation is complete, a confirmation notice is displayed and a single XIQ instance displays. A single instance is all that is required for the cluster.

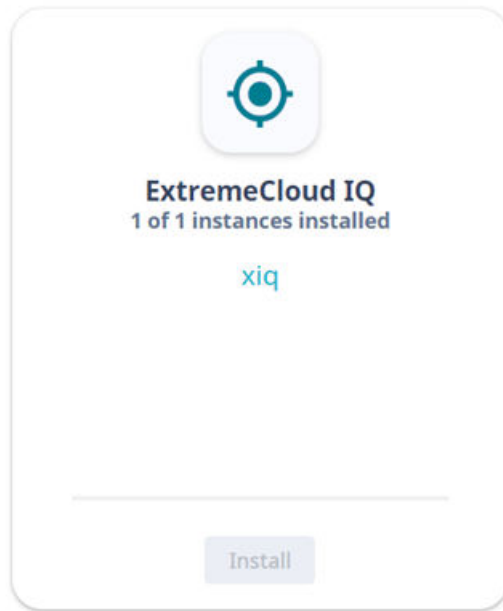


Figure 7: Installed ExtremeCloud IQ Engine Instance

Related Topics

[ExtremeCloud IQ Engine Settings](#) on page 22

ExtremeCloud IQ Engine Settings

When using an ExtremeCloud™ IQ engine, you must configure a cluster of three or more nodes in multiples of three (for example, three, six, or nine nodes). ExtremeCloud IQ is not supported in stand-alone mode, requires a cluster, and does not support engine types other than ExtremeCloud IQ.

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

- [Network Service Configuration](#)
- [Account Registration](#)

Network Service Configuration

The **Network Service Configuration** tab displays the mapping of each core service set to the corresponding Virtual Router Redundancy Protocol (VRRP).



Note

Network registration is configured during the initial Universal Compute Platform setup process. For complete instructions on registering a network account, see the .

ExtremeCloud IQ

Instance: xiq

Network Service Configuration Account Registration

Assign a VRRP address to the service set

Services	Assigned VRRP
auth, cmtcp, cmudp, https, sshproxy	10.48.40.24 ▼
cstcp1, csudp1	10.48.40.25 ▼
cstcp2, csudp2	10.48.40.26 ▼

SAVE

Figure 8: ExtremeCloud IQ Network Service Configuration Details

Account Registration

Create an ExtremeCloud IQ user account through Universal Compute Platform. Go to **Engines > Account Registration** and fill out the form in [Figure 9](#). Then, select **Register**.

You will receive an email confirming your registration.

ExtremeCloud IQ

Instance: xiq

Network Service Configuration

Account Registration

Registration

Instructions to complete the registration will be sent to the account e-mail

Host Name

Token

First Name

Last Name

Email Address

Organization

Job Title

Figure 9: ExtremeCloud IQ Account Registration Form

ExtremeCloud Edge - Self-Orchestration

Install an Engine

When the Deployment Type is ExtremeCloud Edge - Self-Orchestration, you have a variety of engine options to choose from, including the following:

- ExtremeWireless WING™ Controller
- Extreme Tunnel Concentrator

- ExtremeCloud™ IQ Controller

Initial Engine Application Installation

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

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

Download the Extreme Docker Application Image File

Download the application Docker image file from the Extreme Networks [support portal](#).

To obtain the Docker image file, go to the Extreme Networks [support portal](#) to download the application Docker image.

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

Upload the Docker Application Image File to the UCP

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

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

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

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

. To refresh the image file list, select .

Install an Engine Application

To install the engine application, take the following steps:

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



Note

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



Note

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

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

Deploy the Application Image File

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

To deploy the application:

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

Engine Application Settings

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

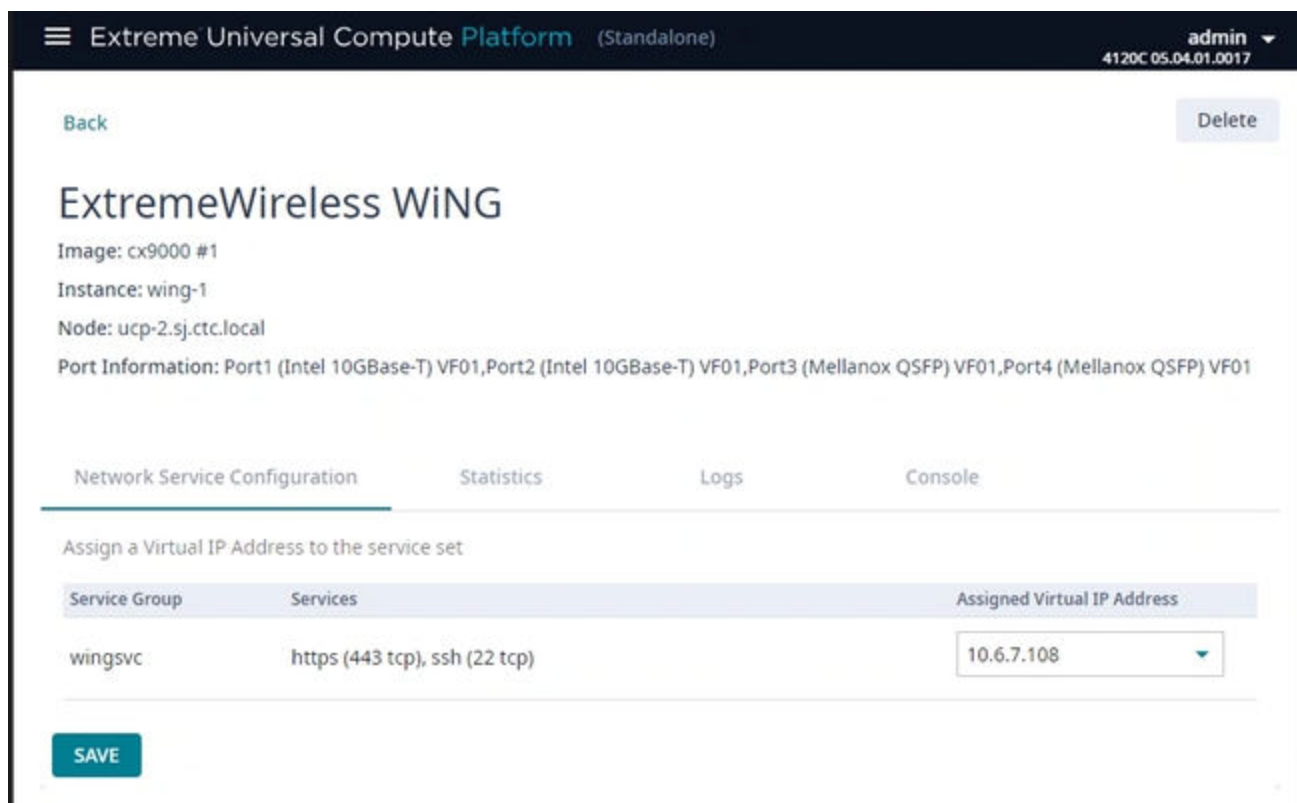


Figure 10: Example Engine Application Settings

Image

Controller image name.

Instance

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

Instance Web Interface

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

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

Network Service Configuration

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

Select the VIP that you configured for the selected port, where the Engine instance will reside. For more information on Interface Configuration, see [Add Interface](#) on page 41.

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**.

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 28.
- **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.



Tools

[Logs](#) on page 29

[Diagnostics](#) on page 30

The topics in this section describe the settings that appear under the **Tools** menu.

Logs

Universal Compute Platform offers Event and Audit logs to help you understand and troubleshoot the network.

Table 4: Log Types

Log Type	Details
Events	To view a list of network events, go to Tools > Logs > Events . The following information is displayed for each event: <ul style="list-style-type: none">• Time the event occurred• Type of event: Info, Minor, Major, or Critical• Component of Universal Compute Platform that was affected. For example, Rest API or Startup Manager• Description of the event
Audit Log	To view the Audit Log, go to Tools > Logs > Audit Logs . The following information is displayed in the Audit Log: <ul style="list-style-type: none">• Time logged item occurred• Username of system administrator• Context• Description of logged item

To filter the list for either log type, provide a start and end date to display only log items that occur within the date window. Select **Reset** to clear the filter.

Use the Search field to find a specific list item.

You can select the number of items to display on a page. Valid values are:

- 10
- 20
- 50
- 100

To jump to the next or previous page, or jump to the first or last page, select the arrows at the bottom of the page.

Diagnostics

Universal Compute Platform offers diagnostic tools to help you troubleshoot your network.

Related Topics

[Network Utilities](#) on page 30

[TCP Dump Management](#) on page 31

Network Utilities

Use wireless controller utilities to test a connection to the target IP address (or Fully-Qualified Domain Name) and record the route through the Internet between your computer and the target address. You can also use controller utilities to capture exception traffic, which can be useful for network administrators when debugging network problems.

Table 5: Network Utilities

Field	Description
Target IP Address or Fully-Qualified Domain Name (FQDN)	IP address or FQDN for the test target.
Use specific source interface	Indicates if a specific interface will be selected for the test. Select the interface from the Select Interface field. When this option is cleared, Universal Compute Platform runs the test based on the interface selected in the routing table.
Select Interface	Used with Specific Source Interface option. See list of possible interfaces on the Interface tab.
Ping	Initiate the Ping network utility to determine reachability of the IP address or FQDN that you specify.
Trace Route	Initiate the Trace route command, which traces the path of a packet from Universal Compute Platform to the IP address or FQDN that you specify. It lists the routers it passes until it reaches its destination, or fails to. It also indicates the length of each hop.

Related Topics

[TCP Dump Management](#) on page 31

TCP Dump Management

Table 6: TCP Dump Management

Field	Description
Interface	Target interface. See the list of possible interfaces on the Interface tab.
Filename	Specify the name of the dump file.
Save File To	Specify where to save the dump file.
Capture File Size (MB)	Specify the maximum limit of the dump file in MB. This feature enables you to control the size of the resulting dump file so the file does not become too large.
Capture Files	List of previously created dump files. Select a file to take action.



Administration

[Manage User Accounts](#) on page 32

[System Configuration](#) on page 34

The topics in this section describe the settings that appear under the **Administration** menu.

Manage User Accounts

This topic outlines how to manage user accounts on the Universal Compute Platform controller. For information about registering for an ExtremeCloud IQ user account, see [Account Registration](#) on page 23.

Universal Compute Platform offers the following levels of user access on the controller:

- Full Admin
- Read Only

Full Administrators can create and manage controller user accounts. This guide outlines the following procedures:

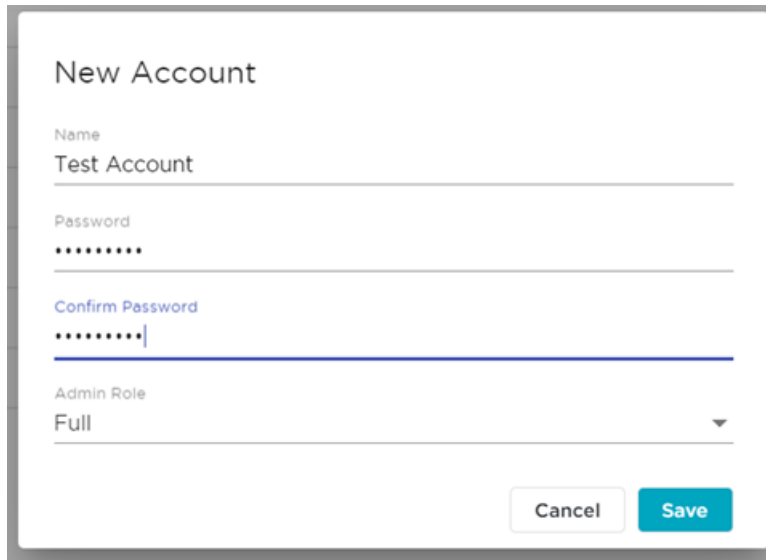
- Add new accounts
- Modify account settings
- Delete user accounts

Add a User Account

To add a user account:

1. Go to **Administration** > **Accounts**.
2. Select **New Account**.

3. Configure the [account settings](#).




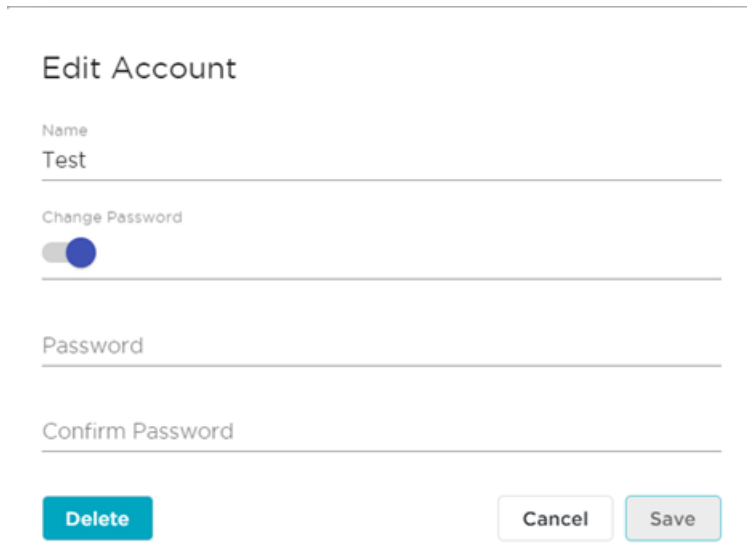
The 'New Account' dialog box features a title bar at the top. Below it, there are four input fields: 'Name' with the text 'Test Account', 'Password' with masked characters, 'Confirm Password' with masked characters, and 'Admin Role' with a dropdown menu showing 'Full'. At the bottom right, there are two buttons: 'Cancel' and 'Save'.

Figure 11: Create New Account

Modify a User Account

To modify a user account:

1. Go to **Administration > Accounts**.
2. Select  next to the account that you want to modify.
3. Select **Change Password**.



The 'Edit Account' dialog box has a title bar. Below it, there are four input fields: 'Name' with the text 'Test', 'Change Password' with a toggle switch, 'Password', and 'Confirm Password'. At the bottom, there are three buttons: 'Delete', 'Cancel', and 'Save'.


Figure 12: Edit Account Details Dialog

4. In the Password field, enter a password.
5. In the Confirm Password field, enter the same password again.

6. Select **Save**.

Delete a User Account

To delete a user account:

1. Go to **Administration > Accounts**.
2. Select  next to the account that you want to delete.
The **Account Settings** dialog opens.
3. Select **Delete**.
A confirmation dialog displays.
4. Select **OK** to confirm that you want to delete the account.

Related Topics

[Account Settings](#) on page 34

Account Settings

Configure the following user account settings:

Name

Name for the user account.

Password

Password for the user account. The password must be between 8 and 24 characters.

Confirm Password

Enter the password for the user account a second time.

Admin Role

The access level for the user account. Valid values are:

- Full Admin
- Read Only

System Configuration

System administrators can do the following from the **Administration > System** menu:

- Configure network interfaces and network time
- Manage Universal Compute Platform upgrades and system maintenance
- Configure availability mode for network failover and redundancy
- View system logs and information.

Related Topics

[Configuration](#) on page 35

[System Logging](#) on page 39

[Maintenance](#) on page 40

[Network Setup](#) on page 40

[Network Time](#) on page 45

[Cloud Visibility](#) on page 45

[Upgrade the Universal Compute Platform](#) on page 46

[System Information](#) on page 51

[Utilities](#) on page 52

Configuration

Go to **System > Configuration** to back up and restore the appliance, and schedule the backup procedure.

Related Topics

[Perform a Configuration Backup](#) on page 35

[Restore Backup File](#) on page 35

[Schedule a Backup](#) on page 38

Perform a Configuration Backup

This backup and restore procedure is limited to configuration files and, optionally, logs and audit files. A system backup is a different procedure. A system backup is a full system snapshot rescue file (*-rescue-user.tgz). Creating a full system rescue file is an option during the system upgrade process.

Before you perform a backup procedure, decide what to back up and where to save the backup file:

- Select back up configs, logs, and audit or back up configuration only.
- Select a location to store the backup file.
- Select **Local** as the backup location.
- (Optional) Configure a backup schedule.



Note

It is a best practice to set up a scheduled backup for all managed appliances.

On-demand backups can only be stored locally, while scheduled backups can be stored on a mounted flash drive or on a remote server.

Related Topics

[Schedule a Backup](#) on page 38

Restore Backup File

Restore the appliance from a selected backup file.

1. Go to **Administration > System > Configuration**.
2. Select the **Backup/Restore** tab.

3. Select the file to restore.

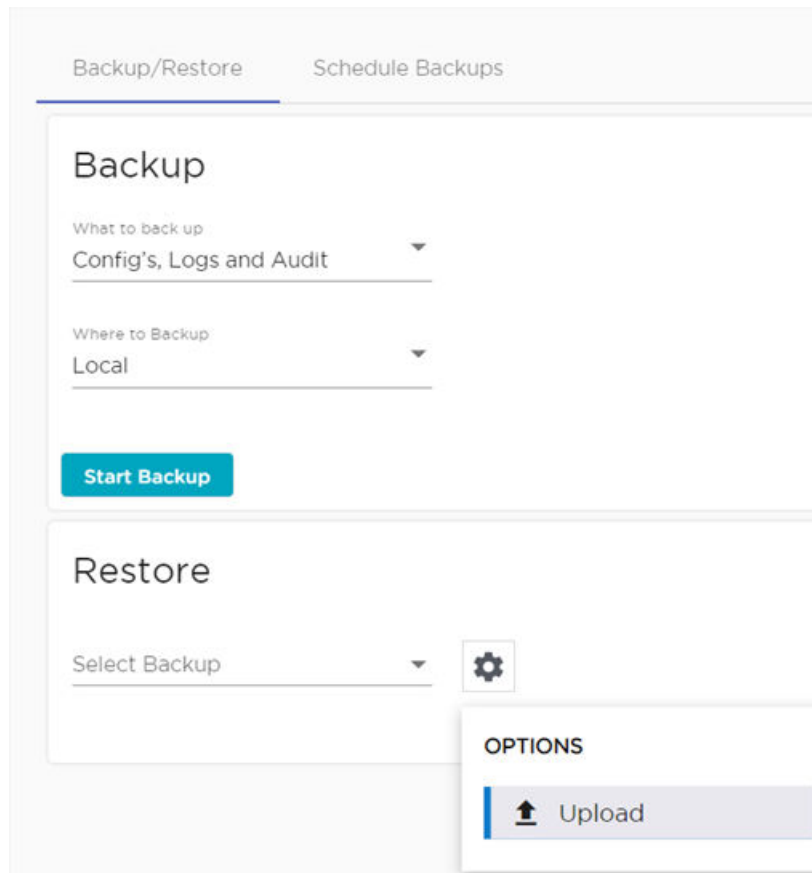



Figure 13: Upload Restore Image

4. Next to **Restore**, select , then select **Upload**.
5. Select the **Upload Method**. Valid values are:
 - HTTP
 - FTP
 - SCP

6. You can select the center pane and navigate to the backup file or drag and drop the file on the center pane.

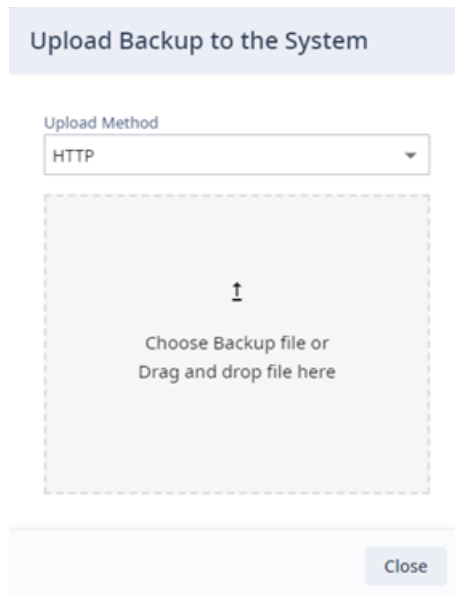


Figure 14: Upload Controller Image

Schedule a Backup

When you schedule a backup, you can choose to upload the backup to a server or have the scheduled backup saved locally or on an external flash drive. To schedule a backup:

1. Go to **Administration > System > Configuration > Schedule Backups**.
The **Schedule Backup** dialog displays.

The screenshot shows the 'Schedule Backups' dialog box. At the top, there are two tabs: 'Backup/Restore' and 'Schedule Backups', with the latter being active. Below the tabs, a message states 'No Backup Schedule has been set'. The dialog contains several configuration fields: 'Backup Location' is a dropdown menu set to 'Local'; 'What to back up' is a dropdown menu set to 'Config's, Logs and Audit'; 'Schedule Task' is a dropdown menu set to 'Daily'; there is an unchecked checkbox labeled 'Include Weekends'; 'Timezone' is a dropdown menu set to 'America/Toronto'; and 'Time' is a time picker set to '00:00'. At the bottom of the dialog is a blue button labeled 'SCHEDULE BACKUP'.

Figure 15: Schedule Backup Dialog

2. Configure the following parameters:

Backup Location

Indicates where to send the backup file. Valid values are: Local or Remote. When sending a backup to a remote server, configure the server properties.

What to back up

Indicates the content of the backup file. Valid values are: Configs, Logs and Audit (which is a full backup), or Configuration files only.

Schedule Task

Indicates when the backup task runs. Valid values are: Daily, Weekly, Monthly.

Include Weekends

Select this check box to include weekends in the backup schedule.

Time

Set the time of day for the scheduled backup.

3. Select **Schedule Backup**.

Related Topics

[Perform a Configuration Backup](#) on page 35

System Logging

Syslog event reporting uses the syslog protocol to relay event messages to a centralized event server on the enterprise network. In the protocol, a device generates messages, a relay receives and forwards the messages, and a syslog server receives the messages.

System Log Level

Determines the error severity that is logged for the appliance. Select the least severe log level that you want to receive: Information, Minor, Major, Critical. For example, if you select Minor, you receive all Minor, Major and Critical messages. If you select Major you receive all Major and Critical messages. The default is Minor.

Syslog

Provide the IP Address of 1-3 syslog servers and enable the type of messages that you want to send to the syslog servers.

- **Send all Service Messages**
- **Send Audit Messages**



Note

To synchronize the logs, the syslog daemon must be running on both the appliance and on the remote syslog server. When you change the log level on the appliance, you must modify the appropriate setting in the syslog configuration on remote syslog server.

Facility Codes

Facility codes identify log streams in the remote syslog server. Select a unique facility code (local.0 - local.6) for each Universal Compute Platform facility to differentiate the log streams and facilitate the filtering of messages.

The facility code applies to all servers. Select a facility code for each of the following:

- Application Facility
- Service Facility
- Audit Facility

Related Topics

[Logs](#) on page 29

Maintenance

Perform cluster maintenance and tech support from the **Maintenance** menu. Go to **Administration > System > Maintenance** .

System Actions

Reset the cluster configuration, restart the appliance, or shut down the appliance.

Reset Configuration

- Resets all user configurations
- Provides the option to reset the ICC (management) port configuration
- Resets the Kubernetes node
- Resets the shared file system

Reboot

The Universal Compute Appliance shuts down, then reboots. A warning message is displayed, asking you to confirm your selection.

Shut Down

The system enters the halted state, which stops all functional services and the application. A warning message is displayed, asking you to confirm your selection. To restart the system, the power to the system must be reset.

Cluster Actions

Reset Node:

- Resets the Kubernetes node
- Resets the shared file system

Session

Determines the web session inactive window before the session times out. Enter the value as hours : minutes. The range is 1 minute to 168 hours (7 days).

Tech Support

Generate a tech support file for troubleshooting. Select the file criteria: **Appliance**, **Log**, or **All**. (All is the default value.).

1. Select **Generate Tech Support File**.

The generated file displays in the list.

2. To download the file, select the file and select .

Network Setup

Host Attributes

Attributes that define your network: Host Name, Domain Name, Default Gateway, and your DNS servers.

The Default Gateway IP address is the global default IP route setting for the appliance. Valid values are: the Admin topology gateway address and any IP address on the physical Interfaces or Bridge at AC VLAN topology subnets.

L2 Ports

Use the L2 Ports information to understand the OSI Layer 2 (Data Link Layer) physical topology of the data plane. These ports represent the actual Ethernet ports.

Select  to display port statistics.

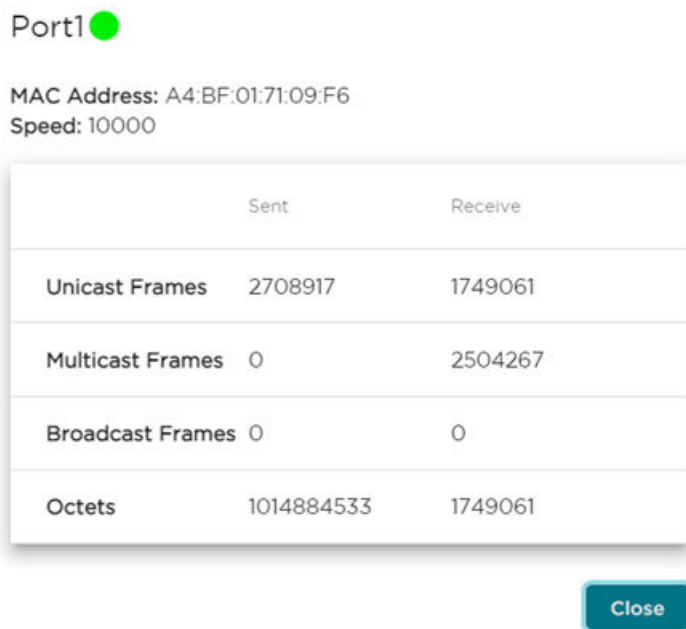


Figure 16: Port Statistics

Interfaces

Add network topologies. Topologies represent the networks with which the Universal Compute Appliance interacts. The attributes of a topology are: VLAN ID, Port, IP address, Mode, and certificates. To add an interface, select **Add New Interface**.

Static Routes

Use static routes to set the default route of the Universal Compute Appliance so that device traffic can be forwarded to the default gateway. To add a static route, select **Add New Route**.

Related Topics

[Interface Properties](#) on page 42

[Static Route Properties](#) on page 45

Add Interface

1. Go to **Administration > System > Network Setup**.
2. Under Interfaces select **Add New Interface**.
The **Create New Interface** dialog displays.
3. Configure the Interface Properties.

Related Topics

[Interface Properties](#) on page 42

Interface Properties

The following table provides details about Interface Properties.

Table 7: Interface Properties

Field	Description
Name	Name of the interface.
Mode	Describes how traffic is forwarded on the interface topology. Options are: <ul style="list-style-type: none"> 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 7: Interface Properties (continued)

Field	Description
FQDN	Fully-Qualified Domain Name
VRRP	<p>Supports load balancing and high-availability functions for the Universal Compute Platform cluster.</p> <p>IP Addresses Record the IP address relationship between the cluster's direct interfaces (ICC, Service/Data ports), VRRP, and external access.</p> <p>Priority VRRP uses priority settings as a mechanism to arbitrate mastery of the state of exchanges across members of the cluster.</p> <p>Best Practice:</p> <ul style="list-style-type: none"> • Designate node 1 as the highest priority, node 2 for second highest priority, and node 3 as the lowest priority. • The same priority should be used across all services (ICC, Services). <p>Router ID Allows segmentation of a routing domain.</p> <p>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.</p> <p>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.</p>

LAG Interfaces

Universal Compute Platform supports the IEEE 802.3ad implementation of Dynamic Link Aggregation Group (LAG), with control managed by the Link Aggregation Control Protocol (LACP). When you join two or more ports into a LAG interface, the network bonds the ports and treats them as a single logical port interface. LAG interfaces increase link throughput and provide redundancy in case of a link failure.

Consider the following when configuring LAG:

- Supported port combinations are: ICC1 and ICC2, and any combination of two to four data ports so long as the ports are configured to run at the same speed.
- An ICC port and a data port cannot be combined into the same LAG interface.
- A single port cannot be added into more than one LAG interface.
- The LAG interface inherits VLAN assignments automatically from newly added port members.

Configure LAG Ports

Use this procedure to configure Link Aggregation Group (LAG) interfaces on Universal Compute Platform.



Note

Make sure to configure LAG on the switch that connects to the LAG ports. Otherwise, the LAG connection fails.

1. Go to **Administration > System > Network Setup**.
2. Under **L2 Ports**, assign data ports to each LAG interface:
 - a. For **LAG1**, select each data port that you want to add to this LAG.
 - b. For **LAG2**, select each data port that you want to add to this LAG.
 - c. Select **Save** and then select **OK**.
The LAG interface inherits the VLAN assignments automatically from newly added port members.
3. To aggregate the ICC ports, under **ICC Interfaces**, select **LAG**.
4. Complete the LAG interface configuration for each new LAG interface:
 - a. Under **Interfaces**, select the new LAG interface.
 - b. Configure the interface settings. For more information, see [Interface Properties](#) on page 42.
 - c. Select **Save**.

Add Static Route

Static Routes define the default route to Universal Compute Platform for legitimate wireless traffic. You must be a system administrator to add a static route.



Note

Static Routes affect the settings for the Default Gateway IP address under **Host Attributes**. Adding a default static route (0.0.0.0/0) changes the Default Gateway IP address.

To add a static route, take the following steps:

1. Go to **Administration > System > Network Setup**.
2. Under Static Routes select **Add New Route**.
The **New Static Route** dialog displays.
3. Configure the Static Route Properties.

Related Topics

[Static Route Properties](#) on page 45

Static Route Properties

Details about Static Route Properties.

Table 8: Static Route Parameters

Field	Description
Destination	IP address of the destination Universal Compute Platform.
CIDR	CIDR field is used along with IP address field to find the IP address range.
Gateway	Gateway address of the Universal Compute Platform for any Admin or physical interfaces (B@AC L3 VLAN).

Related Topics

[Add Static Route](#) on page 44

Network Time

System administrators can configure network time and the NTP servers. Go to **Administration > System > Network Time**.

System Time — Displays the current system date and time.

Configured Time Zone — Displays current time zone settings.

Set New Time Zone — From the drop-down field, select a time zone, and select **Save** to manually change system date and time.

NTP — Check **NTP** to configure servers for Network Time Protocol (NTP).

NTP is an Internet Standard Protocol that assures accurate synchronization to the millisecond of computer clock times in a network of computers.

NTP Reachable — An icon indicates if the NTP server is reachable:

- Green. The server is reachable.
- Red. The server is not reachable. Check your NTP server settings. Universal Compute Platform has lost connectivity.

Settings

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.

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**.

Upgrade the Universal Compute Platform

You can access options that let you upgrade Universal Compute Platform software at **Administration > System > Software Upgrade**.

The user interface displays information under the following tabs:

- **Image Management**—This tab lets you view the software images that have been uploaded to this appliance. You can select an image and select one of the following icons to complete an action using that image:
 -  (Copy to Nodes)—Copy this image to other nodes in the cluster.
 -  (Delete)—Delete the image from the appliance.
 -  (Upgrade)—Start an upgrade using this image.
 -  (Refresh)—Refresh the screen.
- **Upload**—This tab lets you upload new images for Universal Compute Platform.
- **Schedule**—This tab lets you configure an upgrade schedule.
- **Kubernetes Upgrade**—This tab displays a list of nodes with the current Pod version and Kubernetes version for each node. All nodes should be running the same Pod and Kubernetes version.
- **Logs**—This tab contains logs with information about upgrade history, upgrade details, and restore history.

Go to [Upgrade Universal Compute Platform Task Flow](#) on page 46 to initiate the upgrade process.

NEW! Upgrade Universal Compute Platform Task Flow

To upgrade Universal Compute Platform, complete the tasks in the following task flow.

Table 9: Upgrade Universal Compute Platform Task Flow

	Procedure	Description
1	Upload Software Image on page 47	Upload the new software image to a Universal Compute Platform cluster node.
2	Copy Image to All Nodes on page 48	(Clustered deployments only). Copy the uploaded image to other cluster nodes.
3	Upgrade the cluster nodes using either of these procedures: <ul style="list-style-type: none"> • Upgrade Nodes on page 49 • Schedule an Upgrade on page 49 	You can initiate an immediate (on-demand) upgrade of cluster nodes or schedule the upgrade for the future. Note: With either option, you must upgrade the nodes one node at a time.
4	Kubernetes Upgrade on page 50	Check that your Kubernetes version is up to date and that all pods are running the same version.



Note

- For information on past upgrades, see [Upgrade Logs](#) on page 50.
- For information on how to upgrade container applications, see [Engine Upgrades](#) on page 27.

Upload Software Image

Use this procedure to upload a new image file to a Universal Compute Platform node. You must upload the image before you can use the image to complete an upgrade.



Note

The software image must be accessible from your local computer.

1. Go to **Administration > System > Software Upgrade**.
2. Select **Upload**.
3. For **Image Type**, select **Upgrade** or **Backup**, depending on the type of image.
4. For the **Destination**, select **Local**.
5. Select the **Upload Method** (HTTP, FTP, or SCP).
6. Complete one of the following actions according to the selected upload method
 - For **HTTP** uploads, complete one of the following options to upload the file:
 - Select and drag the image file to the Universal Compute Platform desktop.
 - Select the **↑** (Choose Upgrade File) icon and then browse to the image file and select it.

- For **FTP** or **SCP** uploads, complete the additional server fields that display according to the below requirements and then select **Upload Image**:
 - **Server IP**—Enter the IP address of the server where the image is stored.
 - **Username**—Enter a username for an account that has access to the server.
 - **Password**—Enter the password for the preceding user account.
 - **Directory**—Enter the directory where the software image is stored.
 - **Filename**—Enter the filename of the software image file.

The image file uploads to Universal Compute Platform.

What to do Next

For clustered deployments, [Copy Image to All Nodes](#) on page 48. Otherwise, upgrade this node using one of the following procedures:

- [Upgrade Nodes](#) on page 49
- [Schedule an Upgrade](#) on page 49


NEW! *Copy Image to All Nodes*

For clustered deployments, use this procedure to copy the software image from one cluster node to other nodes in the cluster.



Note

- The image must be uploaded already to the source node for the Copy.
- The Copy feature applies to Universal Compute Platform software installation images only.

1. Log in to the Universal Compute Platform node where the image is uploaded.
2. Go to **Administration > System > Software Upgrade**.
3. Select **Image Management**.
4. Select the image that you want to copy and then select the  (Copy to Nodes) icon.
5. In the **Copy image to nodes** popup, set the following fields:
 - **Image**—Make sure that the correct file is selected.
 - **Copy Image to**—Select each destination node for the copy. You can select multiple nodes.



Note

The destination nodes must be running version 5.07.01 or later.

6. Select **Copy**.

The software image copies to the selected nodes.

What to do Next

Upgrade the cluster nodes using one of these procedures:

- [Upgrade Nodes](#) on page 49

- [Schedule an Upgrade](#) on page 49

NEW! Upgrade Nodes

Use this procedure to initiate an on demand upgrade of Universal Compute Platform nodes. You can upgrade each node in the cluster from a single node.



Note

- You cannot upgrade more than one node in the cluster at the same time.
- The software installation image must be uploaded already to the local node (the node on which you've logged in). If you're upgrading a different node than the local node, the software installation image must have been uploaded to that node as well.

1. From any cluster node, go to **Administration > System > Software Upgrade**.
2. Select **Image Management**.
3. Select the image that you want to use for the upgrade and then select the **↑** (Upgrade) icon.
4. Set the following fields in the **Software Upgrade** popup:
 - **Image**—Make sure that the image that you want to use is selected.
 - **Backup System Image to**—Select **Local**.
 - **Upgrade**—Select **Now**.
 - **Node**—Select the node that you want to upgrade.
5. Select **Upgrade**.

The upgrade process begins.

After the upgrade finishes, restart the procedure and select a different node for upgrade.

Schedule an Upgrade

Configure an upgrade schedule for the local Universal Compute Platform image.



Note

- You can schedule an upgrade for the local node only. For clusters, you must configure an upgrade schedule for each node separately from that node.
- You can upgrade only one node in the cluster at a given time.
- The software image must be uploaded already to the local node.

1. Go to **Administration > System > Software Upgrade**.
2. Select **Schedule**.
3. Select the **Image** that you want to use for the upgrade.

4. From the **Backup System to** drop-down, select the destination for the backup file:
 - **Local**—Backup file is saved locally.
 - **Flash**—Backup file is saved to flash.
 - **No Backup**—No backup file is created.
5. Assign the following details to the backup:
 - **Backup Filename** that you want to assign.
 - **Timezone** of the appliance.
 - **Time** of the upgrade in 24 hour format HH-MM.
 - **Date** of the upgrade in MM/DD format.

**Note**

When you supply a Date and Time that is in the past, the schedule is set for the following year at the specified date and time.

6. Select **Schedule**.

Repeat this procedure on the other cluster nodes to schedule upgrades for those nodes.

Kubernetes Upgrade

The **Kubernetes Upgrade** tab displays a list of nodes with the current Pod version and Kubernetes version for each node. All nodes should be running the same Pod and Kubernetes version.

Upgrade Logs

The **Logs** tab displays the following information for the appliance:


- Upgrade History
- Upgrade Details
- Restore Details

Upgrade History	Logs regarding upgrade history	🔄	▼
Upgrade Details	Logs regarding details of previous upgrades	→☰	▼
Restore Details	Logs regarding restore	→☰	▼

Figure 17: Logs tab

Select ^ to expand each log file.

You can copy text from each log file.

1. Select ^ to expand the log file.
2. Select the log text you want to copy and select .

System Information

Go to **Administration > System > System Information** to view the following information about your system:

- System Up Time
- CPU Utilization
- Memory Usage
- Disk Usage
- System Temperature
- Fan Speed
- Power Supply
- Port Interface Status

System Information	Manufacturing Information
<pre> System Up Time: 6 days, 1:00 - CPU Utilization: 19.60 - Memory Usage: Free: 36 % - Disk Usage (1 Kbyte blocks) Partition Total Space Used Available Use % root 50246500 8214768 41508560 17% tmp 163840 15640 148200 10% persistdata 227034492 231520 226740452 0% home 1999248 96 1962288 0% logs 4031424 5784 3968292 0% cdr 2031440 8 1994080 0% reports 53588732 60 53517812 0% trace 4047424 8 3990068 0% persistent 103179552 80239164 22871576 78% - System Temperature System Board (BB Lft Rear) Temperature: 42 C System Board (BB P1 VR) Temperature: 46 C Front Panel Board (Front Panel) Temperature: 29 C </pre>	

Figure 18: Example System Information

```
System Information      Manufacturing Information

Manufacturing ID (Serial Number): XC012027P-70008
BIOS Version: SE5C620.86B.02.01.0011.C00EC.032620200659
Hardware Revision: 01
VF MAC base: F4CE48F61BC0-64
SMX Version: 05.02.01.0017
GUI Version: 05.03.01.0001
Software Version: 05.03.01.0001T
Model: 4120C
CPU Type: Intel(R) Xeon(R) Silver 4114T CPU @ 2.20GHz
CPU Frequency (MHz): 2200.000
Number of CPUs: 40
Total Memory: 147272704 KB
LAN1 (10Gbps) MAC address: A4:BF:01:70:32:56
LAN2 (10Gbps) MAC address: A4:BF:01:70:32:55
LAN3 (50Gbps) MAC address: 1C:34:DA:7C:A5:83
LAN4 (50Gbps) MAC address: 1C:34:DA:7C:A5:82
ICC1 (10Gbps) MAC address: A4:BF:01:70:32:53
```

Figure 19: Example Manufacturing Information

Utilities

Universal Compute Platform provides a remote console to a node controller. Use the remote console to open a live SSH console session.

To open a remote console, go to **Administration > System > Utilities**.



Note

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**.

Select each engine instance to display engine settings and the **Console** tab for that instance.



Index

A

- Access Control
 - certificates 17
- add node 19
- announcements 7, 8

B

- backup and restore the appliance 35
- backup files
 - performing a backup 35
 - scheduled backups 38

C

- certificates 17
- certificates, generate 17
- cloud visibility 45
- configuration settings 15, 16
- container engine application settings 26
- conventions
 - notice icons 5
 - text 5
- copy image to other nodes 48

D

- Dashboards
 - Deployment Health 10
 - Nodes 11
 - Pods List 12
 - Services List 12
 - System Health 11
 - Volumes List 13
- diagnostic tools 30
- documentation
 - feedback 8
 - location 6, 7

E

- engines 21
- ExtremeCloud IQ 45
- ExtremeCloud IQ container installation 21
- ExtremeCloud IQ engine settings 22
- ExtremeCloud IQ registration
 - network registration 22
 - user account registration 23

F

- feedback 8

I

- image
 - copy software to other nodes 48
- install a container 24, 25
- Interface Properties 42
- interface, add 41
- interfaces, configuring 40, 41

K

- Kubernetes upgrade 50

L

- LAG 43
- LAG ports 44
- Link aggregation 44
- logs 29, 39

M

- managing accounts 32

N

- navigation menu 9
- network accounts
 - ExtremeCloud IQ registration 22
- network time, configuring 45
- network utilities 30
- node replacement 18
- node, add 19
- notices 5

P

- product announcements 7, 8
- proxy server
 - add 46

R

- restoring backup file 35

S

- schedule an upgrade 49
- software image
 - copy to other cluster nodes 48
- SSH Console 52
- Static Route Properties 45
- static route, add 44
- support, *see* technical support
- system configuration 34
- system information, viewing 51
- system maintenance 40

T

- technical support
 - contacting 7, 8

U

- Universal Container
 - install 24, 25
- upgrade
 - schedule 49
- upgrade application
 - self-orchestrated 28
- upgrade cluster task flow 46, 47
- upgrade logs 50
- upgrade nodes
 - on demand 49
- upgrade platform 46
- upload software image 47
- user accounts
 - add 32
 - delete 34
 - edit 33
 - ExtremeCloud IQ registration 23
 - managing 32
 - settings 34

V

- VMI 12

W

- warnings 5
- web proxy
 - add 46