



# Universal Compute Platform

User Guide

Version 5.01.01

9037348-00 Rev AA  
January 2022



Copyright © 2022 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

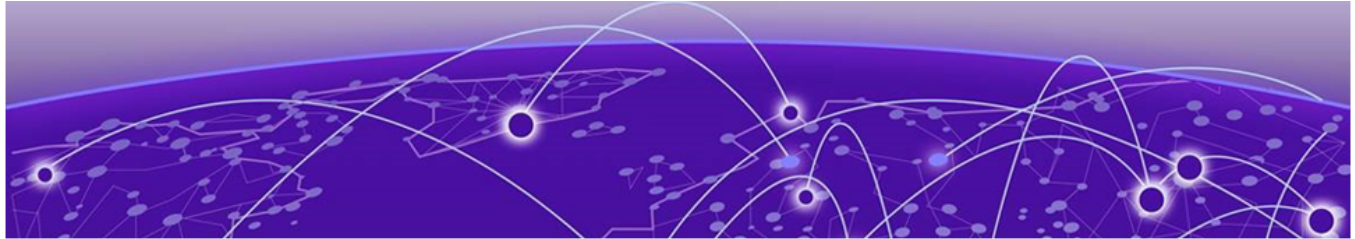
Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

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: [www.extremenetworks.com/company/legal/trademarks](http://www.extremenetworks.com/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/>

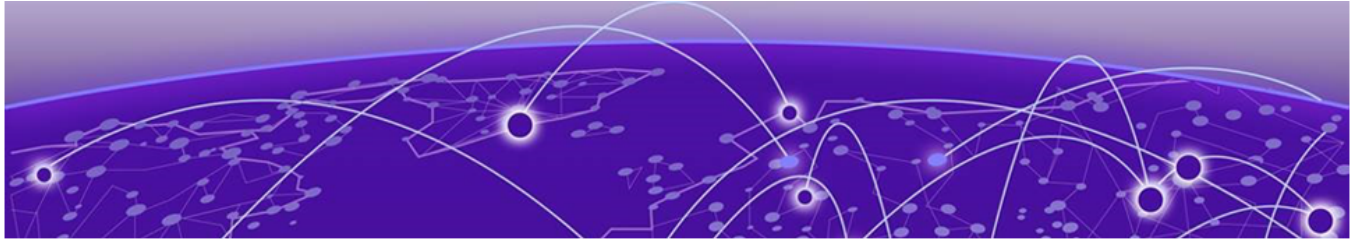


# Table of Contents

---

<b>Preface.....</b>	<b>5</b>
Text Conventions.....	5
Documentation and Training.....	6
Getting Help.....	7
Subscribe to Product Announcements.....	7
Providing Feedback.....	7
<b>Dashboard.....</b>	<b>9</b>
Dashboard Overview.....	9
Deployment Health.....	9
System Health Dashboard.....	10
Nodes Dashboard.....	11
Pods List.....	11
VMI List.....	12
Services List.....	12
Volumes List.....	12
<b>Settings.....</b>	<b>14</b>
Cluster Configuration.....	14
Network Configuration.....	14
Cluster Node Information.....	14
Cluster Configuration.....	14
Prepare to Replace a Node.....	15
Replace Node.....	15
<b>Engines.....</b>	<b>17</b>
Account Registration.....	17
Network Registration.....	18
<b>Tools.....</b>	<b>20</b>
Logs.....	20
Events.....	20
Audit Log.....	20
Diagnostics.....	21
Network Utilities.....	21
TCP Dump Management.....	21
<b>Administration.....</b>	<b>22</b>
Manage User Accounts.....	22
Add a User Account.....	22
Modify a User Account.....	23
Delete a User Account.....	24
Account Settings.....	24
System Configuration.....	25

Configuration.....	25
System Logging.....	28
Maintenance.....	29
Network Setup.....	30
Network Time.....	32
Cloud Settings.....	33
Upgrade Software.....	33
System Information.....	36
Utilities.....	37
<b>Glossary.....</b>	<b>39</b>
<b>Index.....</b>	<b>42</b>



# 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 ExtremeSwitching 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> .
<b>Key</b> names	Key names are written in boldface, for example <b>Ctrl</b> or <b>Esc</b> . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press <b>Ctrl+Alt+Del</b>
<i>Words in italicized type</i>	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.
<b>NEW!</b>	New information. In a PDF, this is searchable text.

**Table 3: Command syntax**

Convention	Description
<b>bold</b> text	Bold text indicates command names, keywords, and command options.
<i>italic</i> text	Italic text indicates variable content.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ <b>x</b>   <b>y</b>   <b>z</b> }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
<b>x</b>   <b>y</b>	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</i> [ <i>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 white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit [www.extremenetworks.com/education/](http://www.extremenetworks.com/education/).

---

## Getting Help

---

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 2826. For the support phone number in your country, visit: [www.extremenetworks.com/support/contact](http://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.

---

## Providing Feedback

---

The Information Development team at Extreme Networks has made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you. We welcome all feedback, but we especially want to know about:

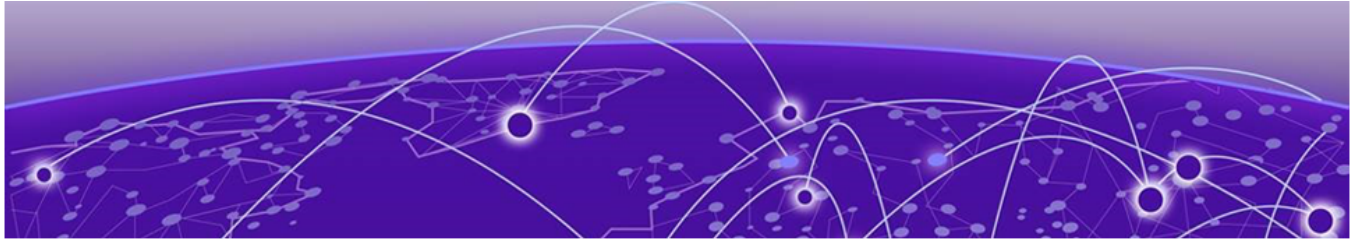
- Content errors, or confusing or conflicting information.

- Improvements that would help you find relevant information in the document.
- Broken links or usability issues.

If you would like to provide feedback, you can do so in three ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at <https://www.extremenetworks.com/documentation-feedback/>.
- Email us at [documentation@extremenetworks.com](mailto:documentation@extremenetworks.com).

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.



# Dashboard

---

[Dashboard Overview](#) on page 9

## Dashboard Overview

---

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

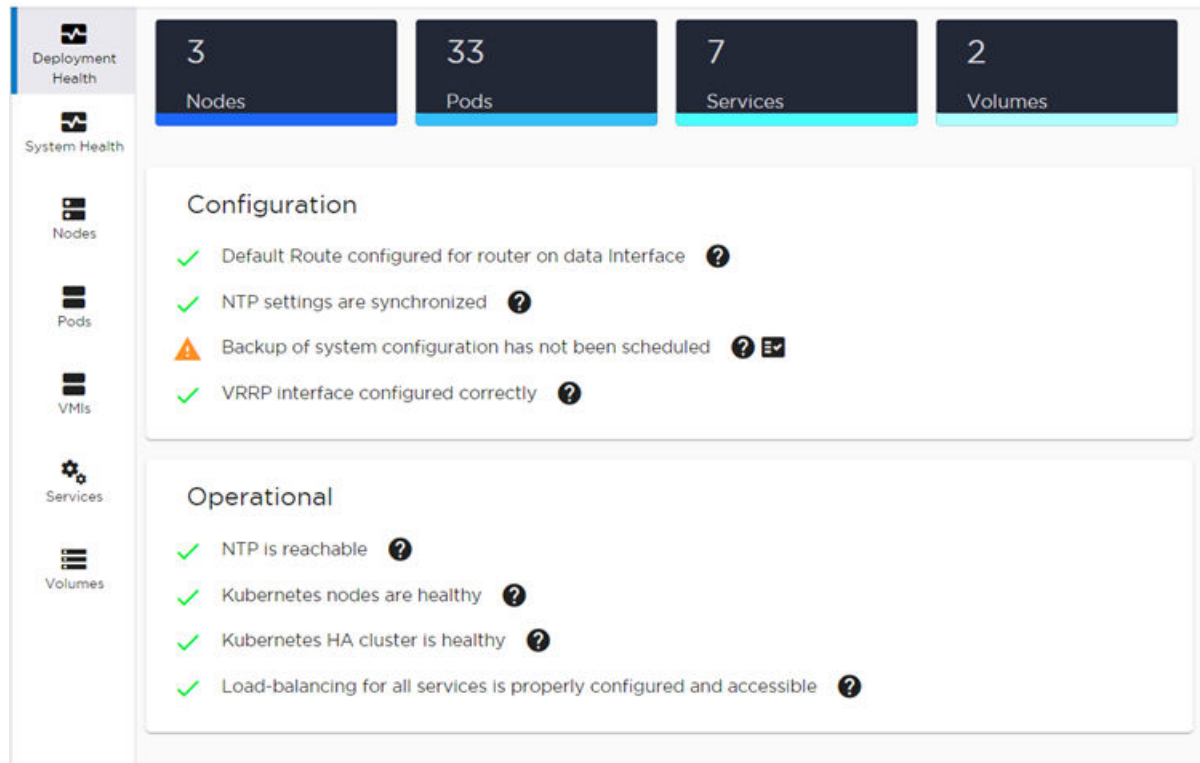
Universal Compute Platform offers the following dashboards and reports:

- 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. Universal Compute Platform requires exactly three nodes per deployment.
- 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.

- A green check mark indicates that a best practice is being followed.
- A yellow warning icon indicates that your configuration is not optimal.
- A red icon 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 to accept the warning.
- Select for a description of each statement or warning.
- Select to list objects causing an issue, and to jump to that area Universal Compute Platform to improve your configuration.

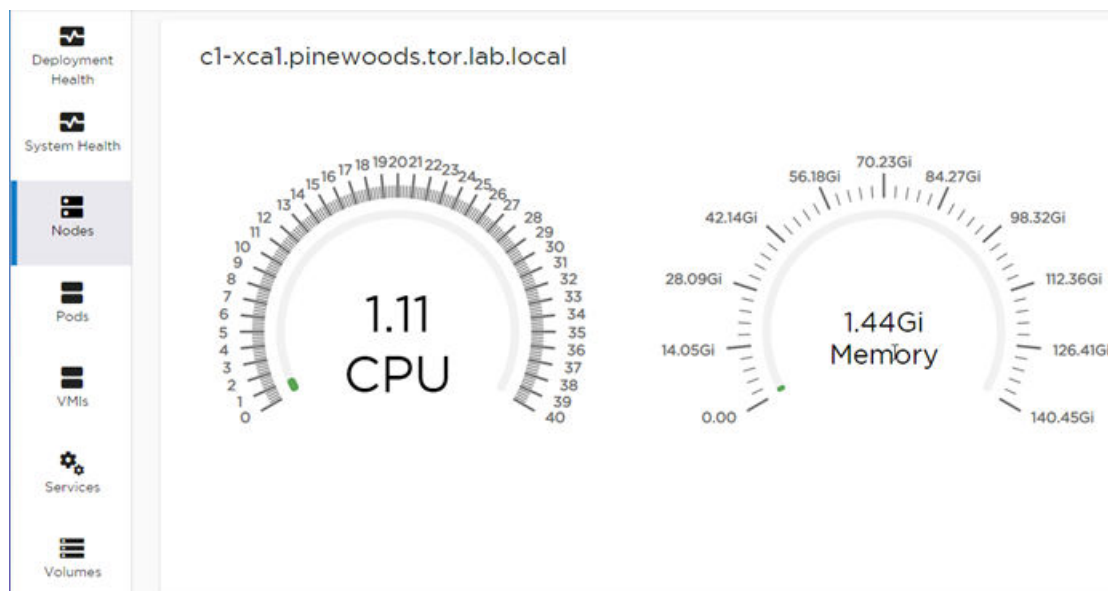
## System Health Dashboard

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.



**Figure 2: Node Information**

## 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.

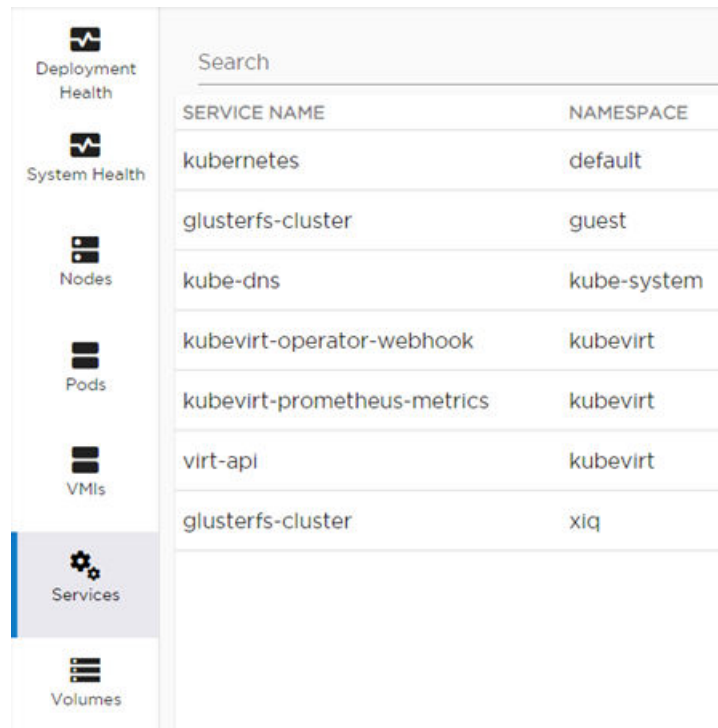
## VMI List

VMI stands for Virtual Machine Instance. VMIs will be supported in a future release.

## 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.



Search	
SERVICE NAME	NAMESPACE
kubernetes	default
glusterfs-cluster	guest
kube-dns	kube-system
kubevirt-operator-webhook	kubevirt
kubevirt-prometheus-metrics	kubevirt
virt-api	kubevirt
glusterfs-cluster	xiq

**Figure 3: 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.

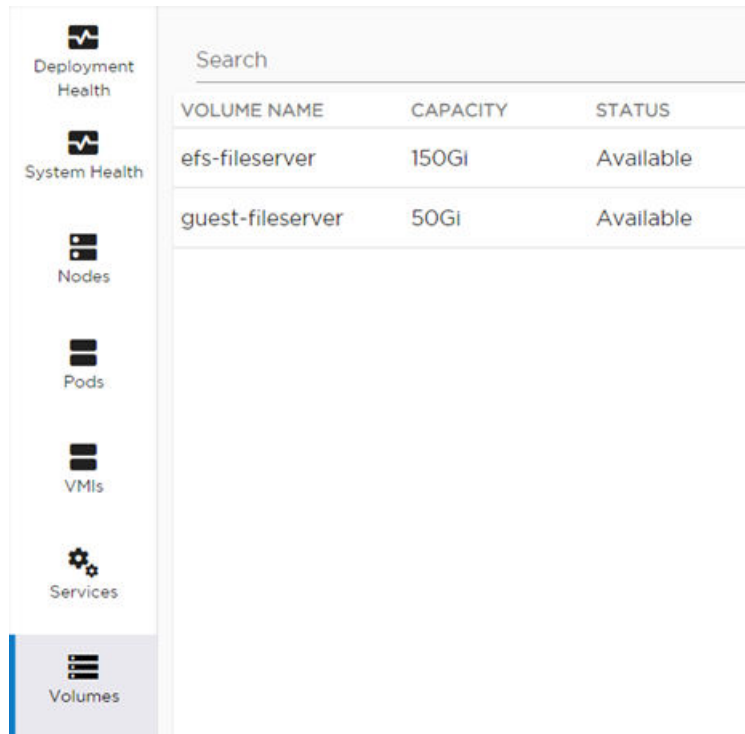
## Volumes List

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 **Retained**.

Use the Search field to find a specific list item.



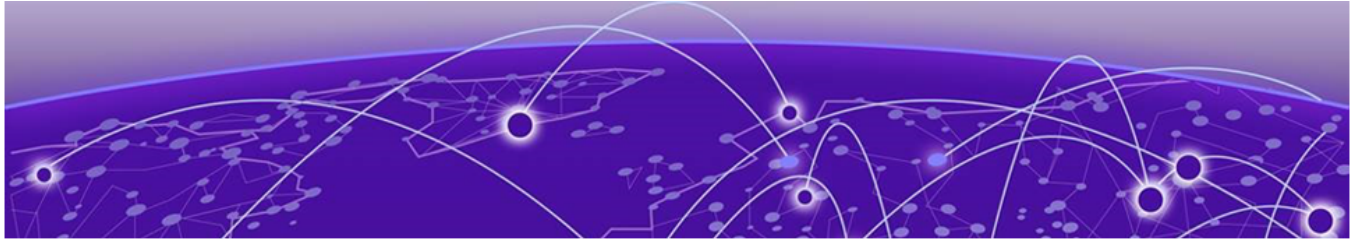
Search		
VOLUME NAME	CAPACITY	STATUS
efs-fileserver	150Gi	Available
guest-fileserver	50Gi	Available

**Figure 4: 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.



# Settings

---

[Cluster Configuration](#) on page 14  
[Prepare to Replace a Node](#) on page 15

## 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 *Universal Compute Platform Deployment Guide*.

Go to **Settings > Cluster Configuration** to view the cluster deployment settings. The following information is provided:

### Network Configuration

- Network topology name
- IP address
- CIDR (Classless Inter-Domain Routing)
- VRRP (Virtual Router Redundancy Protocol)
  - IP addresses
  - Priority
  - Router ID

You can generate CSR Certificates and replace or install a new certificate.

### Cluster Node Information

View or modify the ICC IP Address for each node in the cluster.

### Cluster Configuration

View or modify the following cluster configuration settings:

- Pod Network IP Address
- Service Network IP Address

- Pod Network CIDR
- Service Network CIDR

Reset Cluster

## Prepare to Replace a Node

Before you can replace a node in a cluster, consider the following. For detailed information about cluster configuration, refer to the *Universal Compute Platform Deployment Guide*.

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

The following settings must match the values of the unit being replaced:

- ICC Interface IP Address
- 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.

4. Upgrade the controller for the new node to the current firmware version. For more information, see [Upgrade Software](#) on page 33.

After you have gathered the necessary information and verified the firmware version of all nodes in the cluster, you can run the Node Replacement procedure.

### Related Topics

[Replace Node](#) on page 15

## Replace Node

Replacing a node in a cluster is performed when a connection fails between a node and the other nodes in the cluster. The Node Replacement procedure deletes and resets all connection information for the failed node. It may not be necessary to physically replace the hardware.

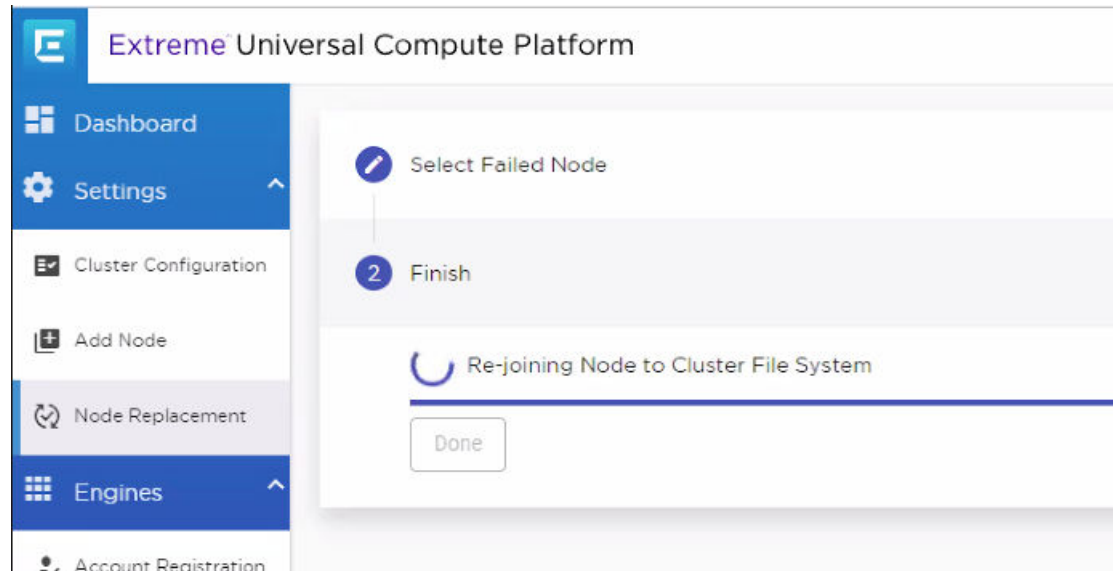
From the primary node in the cluster (Node 1), take the following steps:

1. Go to **Services > 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.

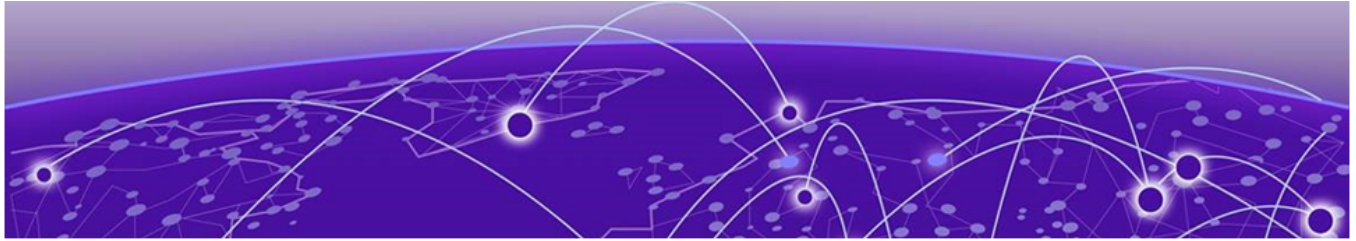
If it is necessary to replace the node hardware, refer to the *Universal Compute Platform Deployment Guide* for detailed information.



**Figure 5: Node Replacement**

#### Related Topics

[Prepare to Replace a Node](#) on page 15



# Engines

---

[Account Registration](#) on page 17

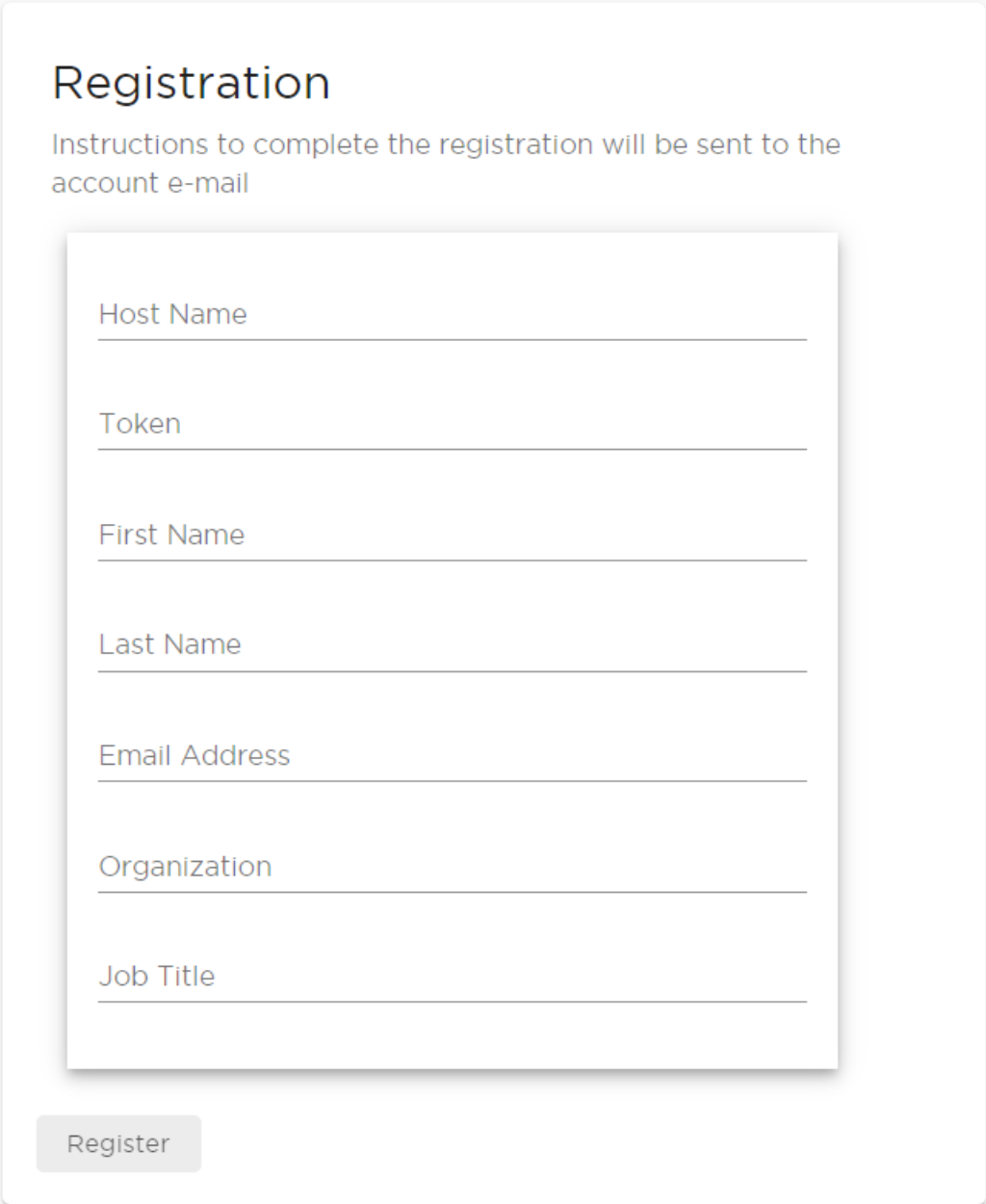
[Network Registration](#) on page 18

## Account Registration

---

Create an ExtremeCloud IQ user account through Universal Compute Platform. Go to **Engines > Account Registration** and fill out the form in [Figure 6](#). Then, select **Register**.

You will receive an email confirming your registration.



The registration form is titled "Registration" and includes a sub-header stating: "Instructions to complete the registration will be sent to the account e-mail". The form contains several input fields: "Host Name", "Token", "First Name", "Last Name", "Email Address", "Organization", and "Job Title". Each field is represented by a text label followed by a horizontal line for input. A "Register" button is located at the bottom left of the form area.

**Figure 6: ExtremeCloud IQ Account Registration Form**

## Network Registration

The **Network Service Configuration** dialog 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 *Universal Compute Platform Deployment Guide*.

To view or modify Universal Compute Platform network registration details, go to **Engines > Network Registration**.

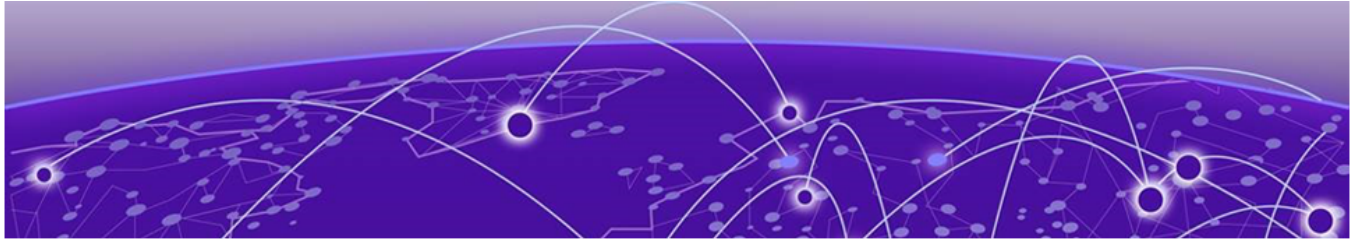
### Network Service Configuration

Assign the VRRP to the service set

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

SAVE

**Figure 7: ExtremeCloud IQ Network Registration Details**



# Tools

---

[Logs](#) on page 20

[Diagnostics](#) on page 21

## Logs

---

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

### Events

To view a list of network events, go to **Tools > Logs > Events**. The following information is displayed for each event:

- Time the event occurred
- Type of event: Minor or Major
- 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:

- Time logged item occurred
- Username of system administrator
- Context
- Description of logged item

To filter the Audit Log, 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.

Go to **Tools > Diagnostics**.

### Related Topics

[Network Utilities](#) on page 21

[TCP Dump Management](#) on page 21

## 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.

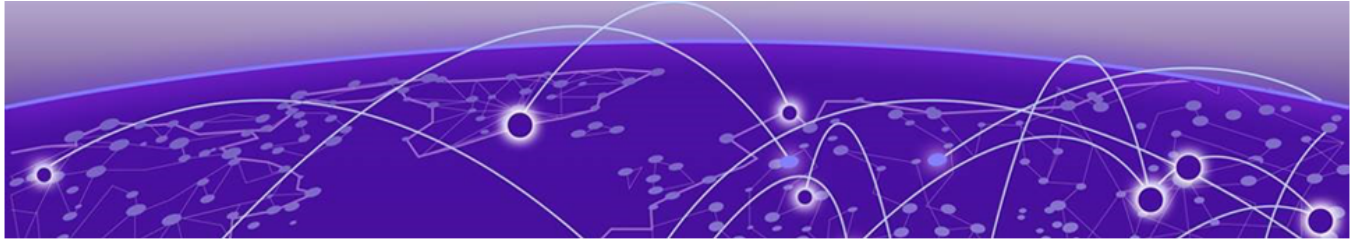
### Related Topics

[TCP Dump Management](#) on page 21

## TCP Dump Management

**Table 4: TCP Dump Management**

Field	Description
Interface	Target interface. See the list of possible interfaces on the <b>Interface</b> 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 22

[Account Settings](#) on page 24

[System Configuration](#) on page 25

## 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 17.

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:

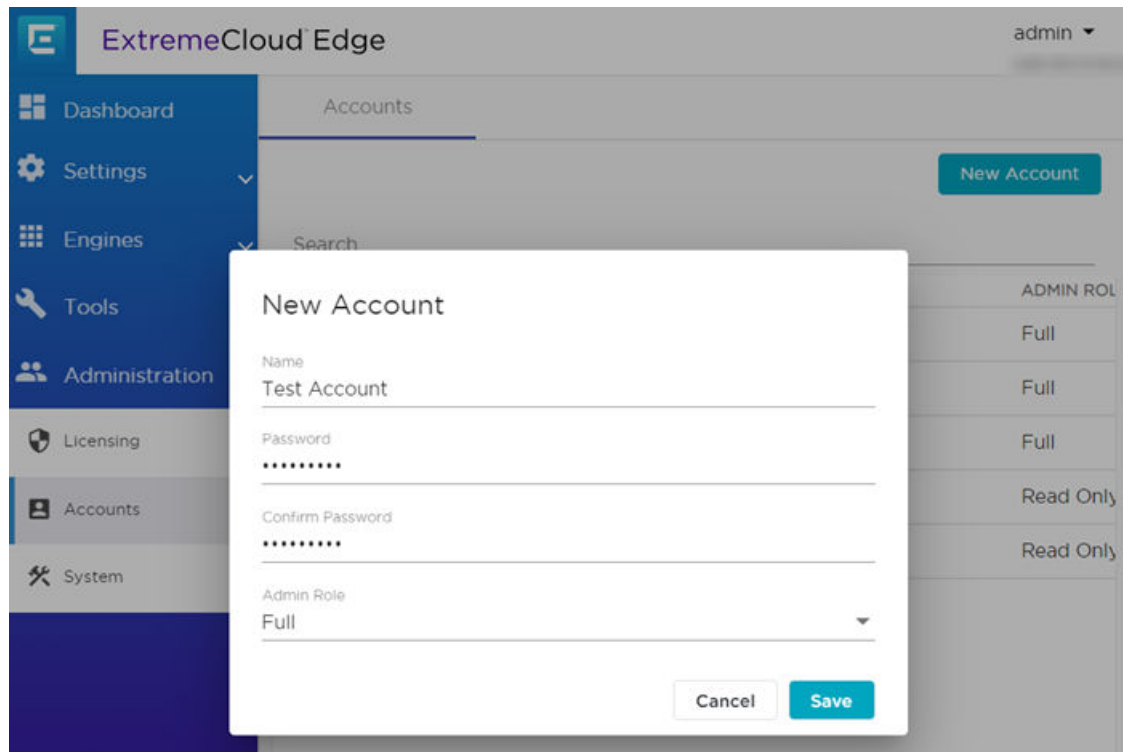
- Add new accounts
- Modify account settings
- Delete user accounts

## Add a User Account

To add a user account:

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

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



The screenshot shows the ExtremeCloud Edge web interface. On the left is a navigation menu with options: Dashboard, Settings, Engines, Tools, Administration, Licensing, Accounts, and System. The 'Accounts' section is selected. The main area shows a table of accounts with columns for Name, Password, Confirm Password, and Admin Role. A 'New Account' modal is open in the center, containing the following fields:

- Name: Test Account
- Password: (masked with dots)
- Confirm Password: (masked with dots)
- Admin Role: Full (selected from a dropdown menu)


At the bottom of the modal are 'Cancel' and 'Save' buttons. In the background, a table of accounts is visible with the following data:

ADMIN ROLE
Full
Full
Full
Read Only
Read Only

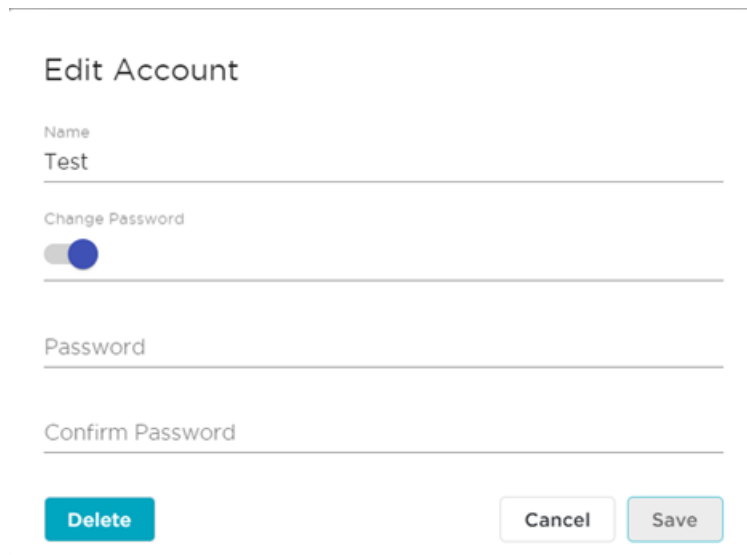
**Figure 8: Create New Account**

## 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 image shows a dialog box titled "Edit Account". It contains several input fields: "Name" with the value "Test", "Change Password" with a toggle switch turned on, "Password", and "Confirm Password". At the bottom, there are three buttons: "Delete" (blue), "Cancel" (light gray), and "Save" (light gray).

**Edit Account**

Name  
Test

Change Password  
☒

Password

Confirm Password


Delete Cancel Save

**Figure 9: 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 24

## 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 software upgrades and system maintenance
- Configure availability mode for network failover and redundancy
- View system logs and information.

## Configuration

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

### Related Topics

[Perform a Backup](#) on page 25

[Restore Backup File](#) on page 26

[Schedule a Backup](#) on page 27

### *Perform a 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

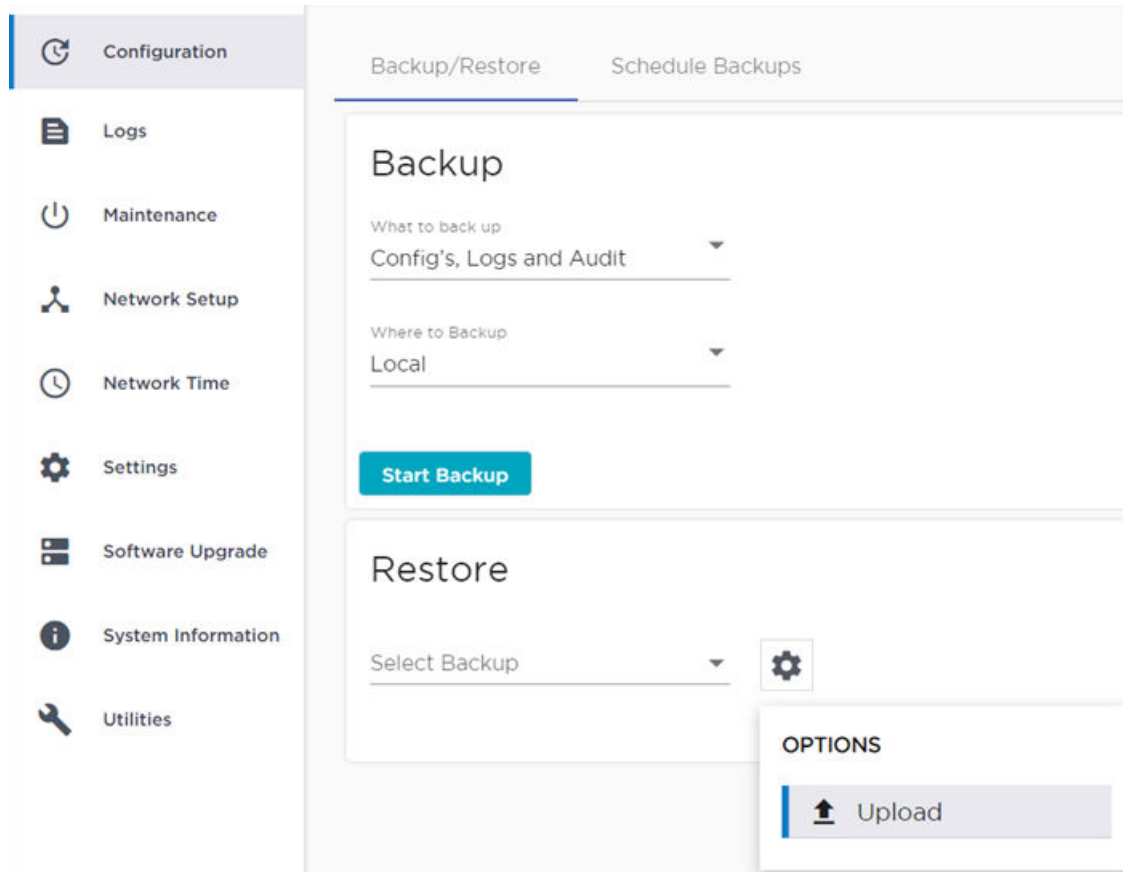
[Schedule a Backup](#) on page 27

[Remote Server Properties](#) on page 28

### Restore Backup File

Restore the appliance from a selected backup file.

1. Go to **Administration > System > Configuration**.
2. Select the **Backup/Restore** tab.
3. Next to **Restore**, select  to upload a file from your local drive.



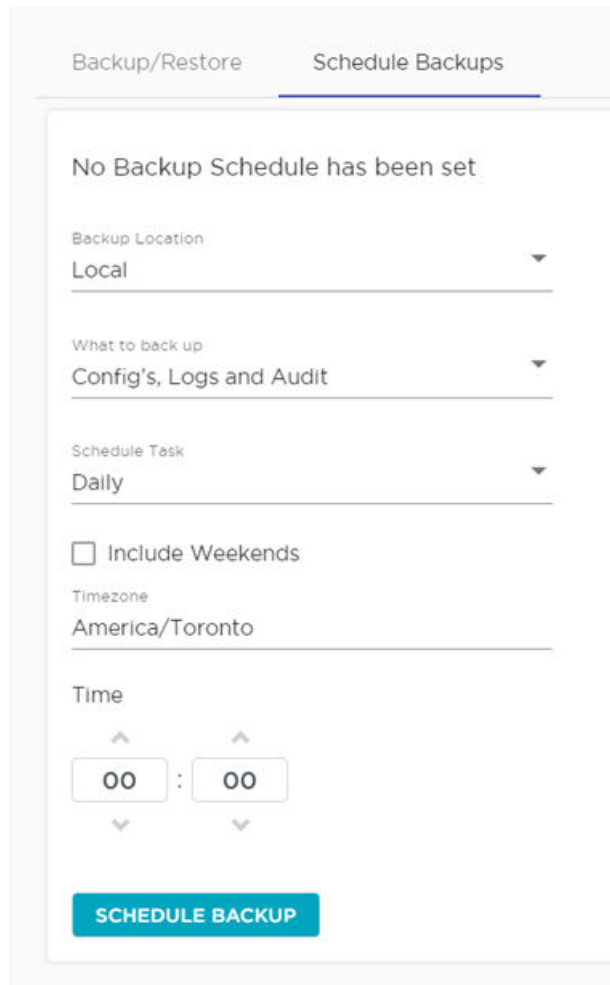
**Figure 10: Upload Restore Image**

4. Select the file to restore.

### 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.



**Figure 11: Schedule Backup Dialog**

2. Configure the following parameters:

#### Backup Location

Indicates where to send the backup file. Valid values are: Local, Remote, Flash. 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, CDRs, 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

[Remote Server Properties](#) on page 28

#### *Remote Server Properties*

You can copy files to and from a remote server for configuration backup, system restore, and system upgrades. Configure the following parameters:

**Table 5: Remote Server Properties**

Field	Description
Protocol	Indicates the transfer protocol to use to transfer the backup file. Valid values are: FTP (File Transfer Protocol) or SCP (Secure Copy Protocol).
Server IP	IP Address of the server.
Username	User name to log into the server.
Password	Password to log into the server.
Directory	Destination or source location of file on the server.

#### Related Topics

[Schedule a Backup](#) on page 27

## 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 and AP. 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 20

## 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**

Full system configuration reset.

**Restart System**

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

**Halt System**

The system enters the halted state, which stops all functional services, the application, and associated wireless APs. 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 file system for the pod.

**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.

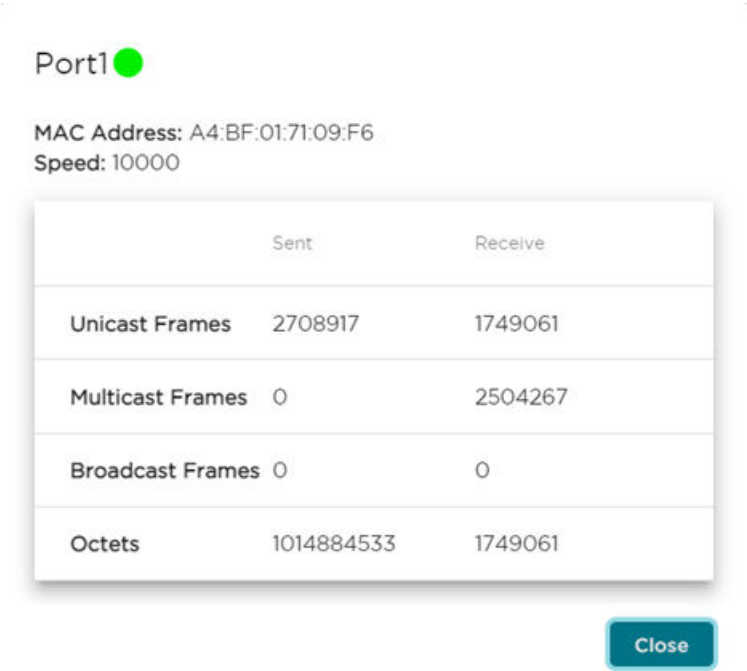


Figure 12: Port Statistics

Interfaces

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

### 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**.

### Add Interface

You must be a system administrator to add a network interface. Take the following steps:

1. Go to **Administration > System**.
2. Under Interfaces select **Add**.  
The **Create New Interface** dialog displays.
3. Configure the following parameters:

**Table 6: Interface Parameters**

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"> <li>Physical - The topology is the native topology of a data plane and it represents the actual Ethernet ports.</li> <li>Management - The native topology of the Universal Compute Appliance management port.</li> </ul>
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.
Enable Device Registration	Enable or disable AP registration through this interface. When enabled, wireless APs use this port for discovery and registration. Other Universal Compute Appliances can use this port to enable inter-Universal Compute Appliance device mobility if this port is configured to use SLP or the Universal Compute Appliance is running as a manager and SLP is the discovery protocol used by the agents.
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.
<b>Layer 3</b>	
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 6: Interface Parameters (continued)**

Field	Description
FQDN	Fully-Qualified Domain Name
DHCP	<p>Dynamic Host Configuration Protocol allows network administrators to centrally manage and automate the assignment of IP addresses on the corporate network. DHCP sends a new IP address when a computer is plugged into a different place in the network. The protocol supports static or dynamic IP addresses and can dynamically reconfigure networks in which there are more computers than there are available IP addresses. Valid values are:</p> <ul style="list-style-type: none"> <li>• None</li> <li>• Local Server. Indicates that the Universal Compute Appliance is used for managing IP addresses.</li> </ul>
VRRP	<p>Supports load balancing and high-availability functions for the Universal Compute Appliance cluster. For more detailed information, see the <i>Universal Compute Platform Deployment Guide</i>.</p> <p><b>IP Addresses</b></p> <p>Record the IP address relationship between the cluster's direct interfaces (ICC, Service/Data ports), VRRP, and external access.</p> <p><b>Priority</b></p> <p>VRRP uses priority settings as a mechanism to arbitrate mastery of the state of exchanges across members of the cluster.</p> <p><b>Best Practice:</b></p> <ul style="list-style-type: none"> <li>• Designate node 1 as the highest priority, node 2 for second highest priority, and node 3 as the lowest priority.</li> <li>• The same priority should be used across all services (ICC, Services).</li> </ul> <p><b>Router ID</b></p> <p>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.</p>

## 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.



#### Note

Network Time settings on each appliance of an availability pair must be identical for the configuration update process to be successful.

## Cloud Settings

To enable Cloud Visibility:

1. Go to **Administration > System > Settings**.
2. Provide the fully-qualified host name of the ExtremeCloud IQ server.

This information is available from your ExtremeCloud IQ account. For example:

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

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



#### Note

The reporting interval is 5 minutes.

## Upgrade Software

To upgrade the image file on one or more of your appliances, go to **Administration > System > Software Upgrade**.

### Related Topics

[Image Management](#) on page 34

[Upload Image](#) on page 34

[Schedule Upgrade](#) on page 34




[Kubernetes Upgrade](#) on page 35

[Upgrade Logs](#) on page 35

## Image Management

The **Image Management** tab displays a list of software image files.

Select an image and take one of the following actions:

-  Delete image file.
-  Upgrade appliance.
-  Refresh image list.

### Related Topics

[Upload Image](#) on page 34

[Schedule Upgrade](#) on page 34

[Kubernetes Upgrade](#) on page 35

[Upgrade Logs](#) on page 35

## Upload Image

Select the **Upload** tab to upload a new image file to the appliance.

Configure the following parameters:

### Image Type

Indicates the type of image file used. Valid values are:

- Upgrade
- Backup

### Destination

Destination of the uploaded image file:

- Local

### Upload Method

Method used to upload image file to the appliance. Valid values are:

- HTTP — Indicates to upload from a local workstation.

### Copy Image from Local Drive

Drag the image onto Universal Compute Platform or select the field to navigate to a local file directory.

### Related Topics

[Image Management](#) on page 34

[Schedule Upgrade](#) on page 34

[Kubernetes Upgrade](#) on page 35

[Upgrade Logs](#) on page 35

## Schedule Upgrade

From the **Schedule** tab configure an upgrade schedule. Configure the following parameters:

### Select Image

Name of the upgrade image file.

**Backup Location**

Indicates where to save the backup image file. Local is currently the only supported value. Save the backup image locally on Universal Compute Platform.

**Backup File Name**

Name of the backup file.

**Timezone**

Timezone of the appliance.

**Time**

The time of the scheduled upgrade in 24-hour format, HH-MM.

**Date**

The date of the scheduled upgrade in Month-Day format (MM-DD).

**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.

Select **Schedule**.

**Related Topics**

[Image Management](#) on page 34

[Upload Image](#) on page 34

[Kubernetes Upgrade](#) on page 35

[Upgrade Logs](#) on page 35

*Kubernetes Upgrade*

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

**Related Topics**

[Image Management](#) on page 34

[Upload Image](#) on page 34

[Schedule Upgrade](#) on page 34

[Upgrade Logs](#) on page 35

*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 13: 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 📋.

#### Related Topics

[Image Management](#) on page 34

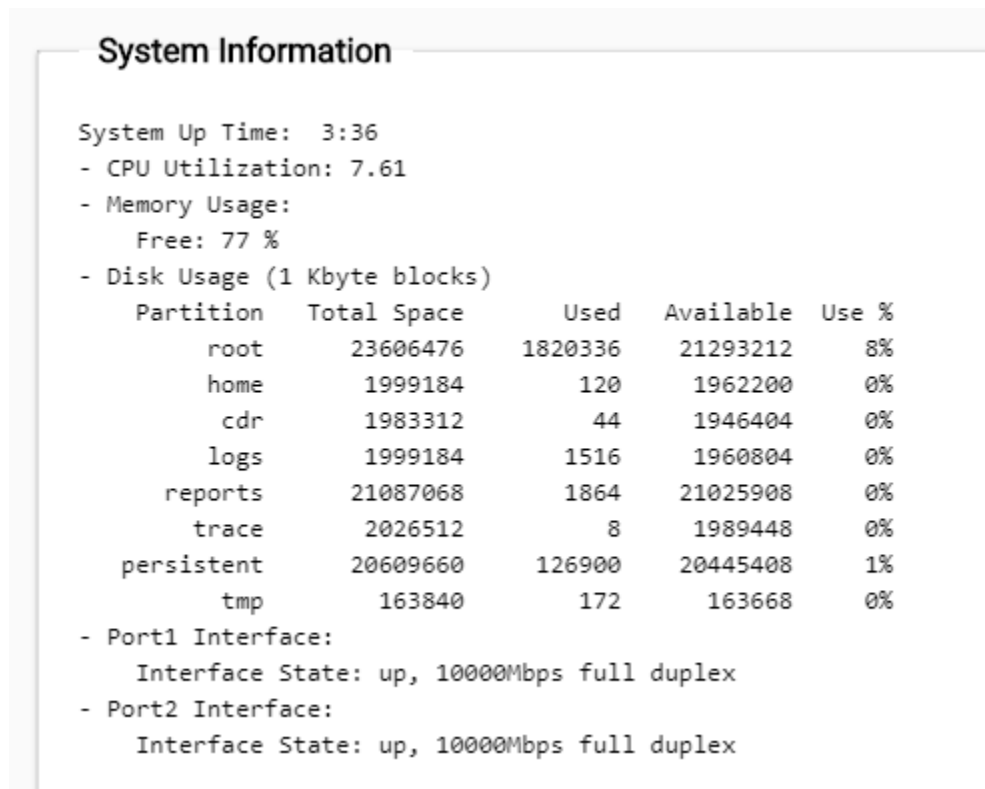
[Upload Image](#) on page 34

[Schedule Upgrade](#) on page 34

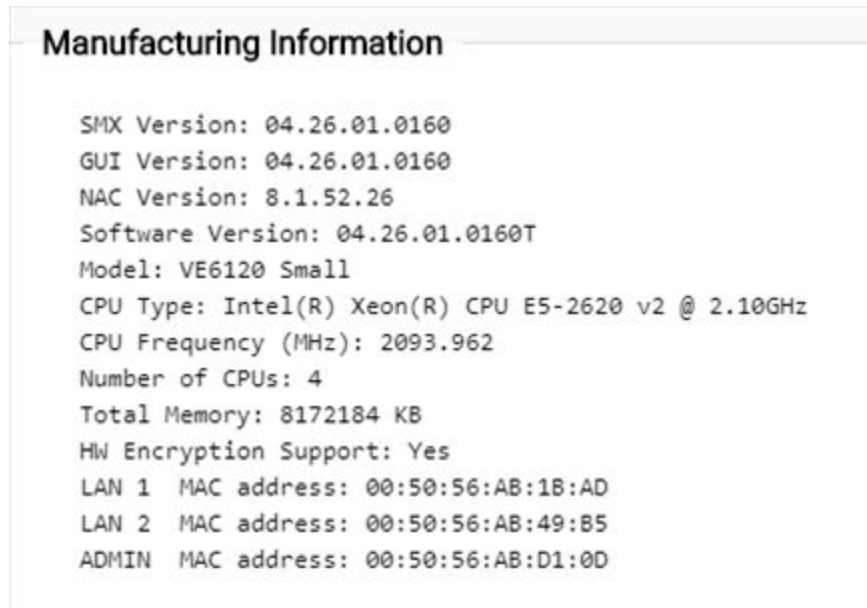
[Kubernetes Upgrade](#) on page 35

## System Information

Go to **Admin > System > System Information** to view the following information about your system.



**Figure 14: Example System Information**

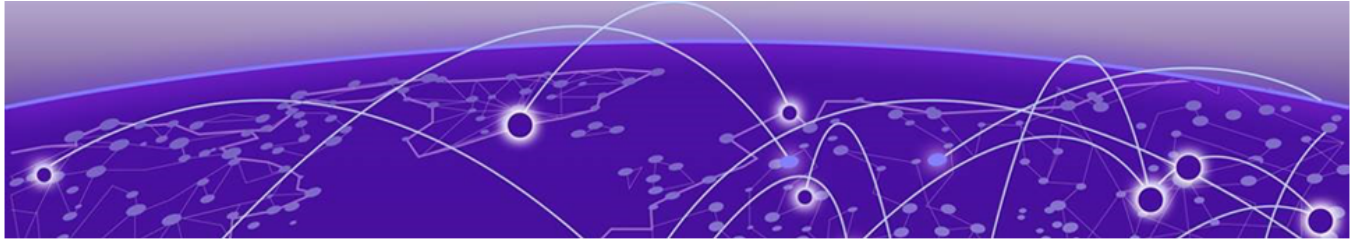


**Figure 15: Example Manufacturing Information**

## 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**.



# Glossary

---

## Chalet

Chalet is a web-based user interface for setting up and viewing information about a switch, removing the need to enter common commands individually in the CLI.

## CLI

Command Line Interface. The CLI provides an environment to issue commands to monitor and manage switches and wireless appliances.

## Extreme Campus Controller

ExtremeCloud Appliance has been rebranded to Extreme Campus Controller. The new Extreme Campus Controller supports Campus/Centralized sites only. Support for Distributed sites remains in ExtremeCloud Appliance v4.76.02 and later.

The Extreme Campus Controller is a next generation orchestration application offering all the mobility services required for modern unified access deployments. The Extreme Campus Controller extends the simplified workflows of the ExtremeCloud public cloud application to on-prem/private cloud deployments.

The Extreme Campus Controller includes comprehensive critical network services for wireless and wired connectivity, wireless device secure onboarding, distributed and centralized data paths, role-based access control through the Application Layer, integrated location services, and IoT device onboarding through a single platform.

Built on architecture with the latest technology, the embedded operating system supports application containers that enable future expansion of value added applications for the unified access edge.

## Extreme Defender for IoT

Extreme Defender for IoT provides unique in-line security for mission critical and/or vulnerable IoT devices. Placed between the IoT device and the network, the Defender for IoT solution helps secure and isolate IoT devices protecting them from internal and external hacking attempts, viruses, malware and ransomware, DDoS attacks, and more. Designed to be simple and flexible, Defender for IoT can be deployed over any network infrastructure to enable secure IoT management without significant network changes.

The solution is comprised of the Extreme Defender Application Software and the Defender Adapter (SA201) or AP3912i access point. Extreme Campus Controller™ is the supported platform for the Extreme Defender Application.

For more information, see <https://www.extremenetworks.com/product/extreme-defender-for-iot/>.

## ExtremeAnalytics

ExtremeAnalytics™, formerly Purview™, is a network powered application analytics and optimization solution that captures and analyzes context-based application traffic to deliver meaningful intelligence about applications, users, locations, and devices. ExtremeAnalytics provides data to show how applications are being used. This can be used to better understand customer behavior on the network, identify the level of user engagement, and assure business application delivery to optimize the user experience. The software also provides visibility into network and application performance allowing IT to pinpoint and resolve performance issues in the infrastructure whether they are caused by the network, application, or server. Learn more about ExtremeAnalytics at <http://www.extremenetworks.com/product/extremeanalytics/>.

### **ExtremeCloud IQ - Site Engine**

ExtremeCloud™ IQ - Site Engine (formerly known as Extreme Management Center and Netsight), is a web-based control interface that provides centralized visibility into your network. ExtremeCloud™ IQ - Site Engine reaches beyond ports, VLANs, and SSIDs and provides detailed control of individual users, applications, and protocols. When coupled with wireless and Identity & Access Management products, ExtremeCloud™ IQ - Site Engine becomes the central location for monitoring and managing all the components in the infrastructure. Learn more at <https://www.extremenetworks.com/product/extremecloud-iq-site-engine/>.

### **ExtremeCloud™ IQ**

ExtremeCloud™ IQ is an industry-leading and visionary approach to cloud-managed networking, built from the ground up to take full advantage of the Extreme Networks end-to-end networking solutions. ExtremeCloud IQ delivers unified, full-stack management of wireless access points, switches, and routers and enables onboarding, configuration, monitoring, troubleshooting, reporting, and more. Using innovative machine learning and artificial intelligence technologies, ExtremeCloud IQ analyzes and interprets millions of network and user data points, from the network edge to the data center, to power actionable business and IT insights, and deliver new levels of network automation and intelligence. Learn more about ExtremeCloud IQ at <https://www.extremenetworks.com/support/documentation/extremecloud-iq/>.

### **ExtremeControl**

ExtremeControl, formerly Extreme Access Control™ (EAC), is a set of management software tools that use information gathered by a hardware engine to control policy to all devices on the network. The software allows you to automate and secure access for all devices on the network from a central dashboard, making it easier to roll out security and identity policies across the wired and wireless network. Learn more about ExtremeControl at <https://www.extremenetworks.com/product/extremecontrol/>.

### **ExtremeSwitching**

ExtremeSwitching is the family of products comprising different switch types: **Modular** (X8 and 8000 series [formerly BlackDiamond] and S and K series switches); **Stackable** (X-series and A, B, C, and 7100 series switches); **Standalone** (SSA, X430, and D, 200, 800, and ISW series); and **Mobile Backhaul** (E4G). Learn more about ExtremeSwitching at <http://www.extremenetworks.com/products/switching-routing/>.

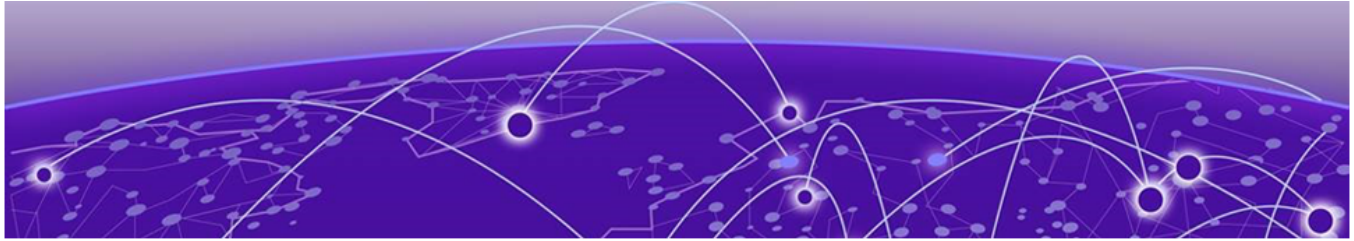
### **ExtremeWireless**

ExtremeWireless products and solutions offer high-density Wi-Fi access, connecting your organization with employees, partners, and customers everywhere they go. The family of wireless products and

solutions includes APs, wireless appliances, and software. Learn more about ExtremeWireless at <http://www.extremenetworks.com/products/wireless/>.

### **ExtremeXOS**

ExtremeXOS, a modular switch operating system, is designed from the ground up to meet the needs of large cloud and private data centers, service providers, converged enterprise edge networks, and everything in between. Based on a resilient architecture and protocols, ExtremeXOS supports network virtualization and standards-based SDN capabilities like VXLAN gateway and OpenStack Cloud orchestration. ExtremeXOS also supports comprehensive role-based policy.



# Index

---

## B

- backup and restore the appliance 25
- backup files
  - performing a backup 25
  - scheduled backups 27

## C

- cloud visibility 33
- configuration settings 14
- conventions
  - notice icons 5
  - text 5

## D

- Dashboards
  - Deployment Health 9
  - Nodes 11
  - Pods List 11
  - Services List 12
  - System Health 10
  - Volumes List 12
- diagnostic tools 21
- documentation
  - feedback 7
  - location 6

## E

- ExtremeCloud IQ 33
- ExtremeCloud IQ registration
  - network registration 18
  - user account registration 17

## F

- feedback 7

## I

- Image Management 34
- interface, add 31
- interfaces, configuring 30, 31

## K

- Kubernetes upgrade 35

## L

- logs 20, 28

## M

- managing accounts 22

## N

- network accounts
  - ExtremeCloud IQ registration 18
- network time, configuring 32
- network utilities 21
- node replacement 15
- notices 5

## R

- remote server properties, software upgrade 28
- restoring backup file 26

## S

- SSH Console 37
- support, *see* technical support
- system information, viewing 36
- system maintenance 29

## T

- technical support
  - contacting 7

## U

- upgrade logs 35
- upgrade schedule 34
- upgrade software 33
- upload image file 34
- user accounts
  - add 22
  - delete 24
  - edit 23
  - ExtremeCloud IQ registration 17
  - managing 22
  - settings 24

### V

VMI 12

### W

warnings 5