ExtremeCloud Tunnel Concentrator v25.01 Deployment Guide

9039192-00 Rev. AB
March 2025

Legal Notice

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

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

Trademarks

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

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

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

Open Source Declarations

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

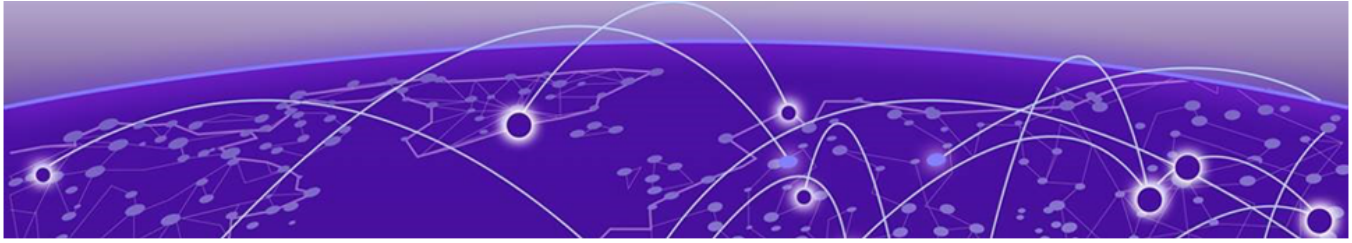
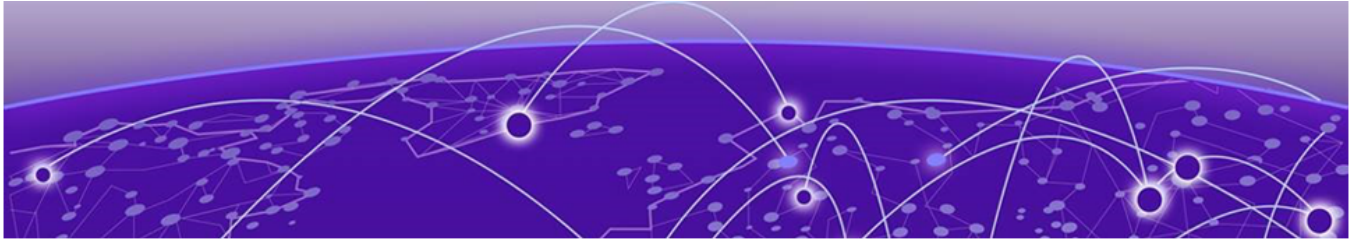


Table of Contents



Abstract

The ExtremeCloud Tunnel Concentrator v25.01 Deployment Guide provides comprehensive instructions for the installation, configuration, and management of the Tunnel Concentrator on the Universal Compute Platform. This revision of the guide provides more details about the Management Layer and the Data Layer. It explains how Tunnel Concentrator leverages different VRRP configurations for different purposes: Management Interface access and Data Plane High-Availability. There is also more information about LAG configuration on both the Universal Compute Platform and the management application. This deployment guide includes updates such as an installation example and procedures for migrating from VGVA tunneling to Tunnel Concentrator. Key features highlighted are traffic centralization, data traffic isolation, and redundancy options. The document details the configuration of Generic Routing Encapsulation (GRE) tunneling to direct wireless traffic from access points to data centers for aggregation. It outlines steps for deploying Tunnel Concentrator with ExtremeCloud IQ or ExtremeCloud IQ Controller, covering prerequisites, installation tasks, GRE topology configurations, VLAN assignments, and user profiles. Administrative tasks include user management, log reporting, and application upgrades. This guide is intended for network administrators and IT professionals.

Preface

Read the following topics to learn about:

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

Text Conventions

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

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

Table 1: Notes and warnings

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

Table 2: Text

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

Table 3: Command syntax

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

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware and Software Compatibility for Extreme Networks products
Extreme Optics Compatibility
Other Resources such as articles, white papers, and case studies

Open Source Declarations

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

Training

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

Help and Support

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

Extreme Portal

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

The Hub

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

Call GTAC

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

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

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

Subscribe to Product Announcements

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

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

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

Send Feedback

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

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

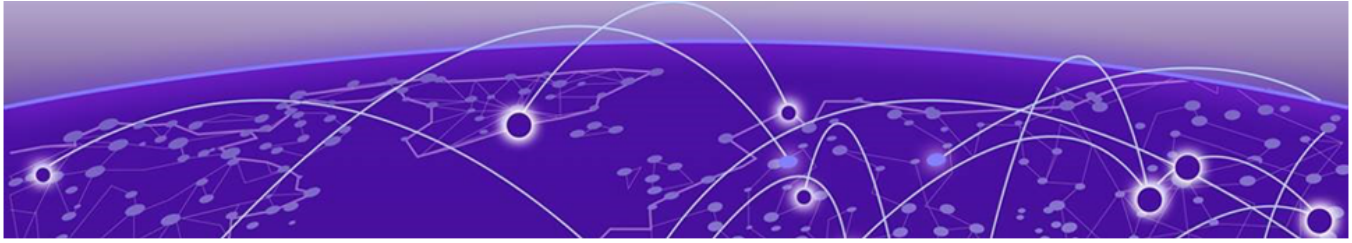
To send feedback, email us at documentation@extremenetworks.com.

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

Revision History

Table 4: Revision History

Date	Version	Revision
Mar 05, 2025	AA	• Initial publish
Mar 21, 2025	AB	• Updated *Installation Requirements* with information on reserved IP addressing. • Updated *Install ExtremeCloud Edge-Self-Orchestration Deployment* around Pod Network and Service Network configuration. .



Tunnel Concentrator

Extreme Tunnel Concentrator enables the setup of traffic ingress/egress from wireless users at specific points in the networks. Client Traffic is exchanged between the Access Points and the Tunnel Concentrator instance via tunnels. For deployments managed by ExtremeCloud IQ (XiQ) the tunneling supported is GRE (encapsulation). For deployments managed by ExtremeCloud IQ Controller (XIQC) the tunneling is supported as IPsec.

Tunnel Concentrator is delivered as an ExtremeCloud Edge – Self Orchestrated application. Customers obtain the installation image (or updates) from Support Portal and then deploy the instance on a choice of Universal Compute Platform hosts:.

- 1130C - Small (up to 1000 tunnels per appliance)
- 2130C - Medium (up to 5000 tunnels per appliance)
- 4120C - Large (up to 15,000 tunnels per appliance)

Tunnel Concentrator provides the following benefits:

- Centralizes wireless traffic.
- Isolates data traffic from management traffic.
- Extends the data center network to your edge devices.
- Provides a replacement for some VPN Gateway Virtual Appliance (VGVA) tunneling use cases.
- Enables traffic tunneling to specific points in the network, abstracting the location of the Access Points.

- Removes the need to have All Client access VLANs present at every access point.
- Provides an option for traffic aggregation in situations where it is cost prohibitive to deploy fabric mesh infrastructure or VxLAN switching.

For more product details on **Extreme Tunnel Concentrator**, see Product Details.

How to Use This Guide

Use the below process flow to guide you through the configuration and deployment process. Follow the prescribed chapter order to install, configure, and administer Tunnel Concentrator.

Before You Begin

Before you configure anything, review the chapter Tunnel Concentrator on page 10 for high-level information about Tunnel Concentrator. You can use this information to plan your deployment.

Table 5: Tunnel Concentrator Deployment Flow

	Chapter	Description
1	Installation on page 26	Use the procedures in this chapter to install and activate Tunnel Concentrator.
2	Select one of the following chapters: • ExtremeCloud IQ Configuration on page 36 • ExtremeCloud IQ Controller Configuration on page 49	Select either ExtremeCloud IQ or ExtremeCloud IQ Controller as the management application. Use the applicable chapter to provision tunneling for your deployment.
3	Administration on page 53	After installation and configuration, use this chapter to administer and maintain your deployment on an ongoing basis.

How Tunnel Concentrator Works

Tunnel Concentrator lets you configure point-to-point tunneling between wireless access points and the Tunnel Concentrator application, which runs on the Universal Compute Platform. Tunnel Concentrator serves as the tunnel termination point and forwards the received traffic on to the data center, where the traffic can be aggregated.

To provision tunneling, administrators configure tunneling settings for a given VLAN and map the VLAN across the WLAN network.

The transport method, whether GRE or IPSec, depends on the management solution. For deployments managed by ExtremeCloud IQ, only GRE encapsulation is supported. For wireless deployments managed by ExtremeCloud IQ Controller, IPSec is the default encapsulation, but GRE is also supported.

All tunneling sessions get initiated by the access point. If the traffic matches a GRE-based user policy that terminates at a Tunnel Concentrator, the access point adds the GRE headers automatically before forwarding the traffic. After receiving the

traffic, Tunnel Concentrator removes the GRE header, and forwards the traffic to the appropriate location in the traffic data center. For any response traffic, the process flow occurs in the reverse order.

Note
IPSec is supported only when you deploy Tunnel Concentrator with ExtremeCloud IQ Controller as the management application. With this option, the AP also encrypts the GRE header.

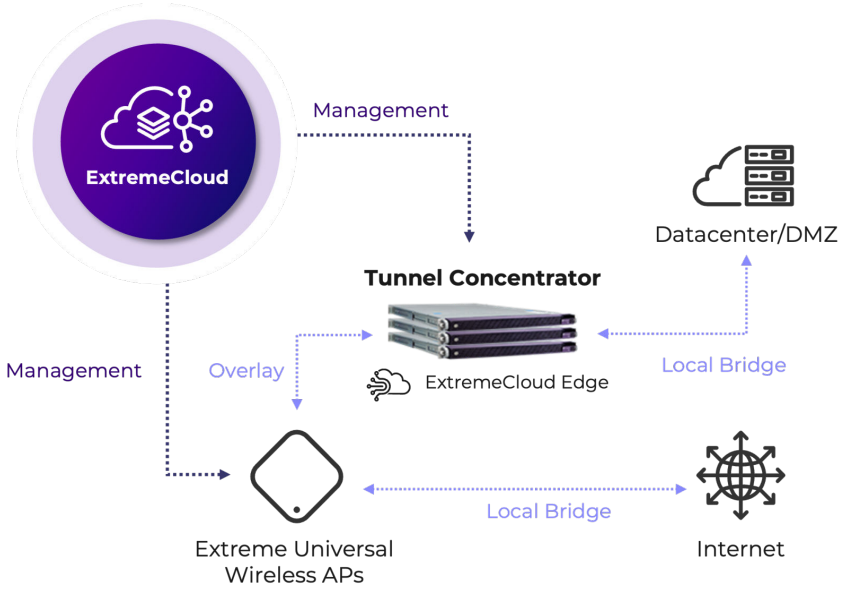


Figure 1: Tunnel Concentrator Deployment

Note
Tunneling is supported only between the access point and Tunnel Concentrator. It is not supported to deploy a NAT router in the middle of the tunnel.

Management Options for Provisioning

You must choose from one of the following two applications for configuring tunneling and mapping those settings to given VLANs across the WLAN network. All tunnel provisioning and configuration must be handled using one of these two applications.

Managed by ExtremeCloud IQ

Tunnels are configured and managed using the ExtremeCloud IQ user interface. Management of Tunnel Concentrator configuration by ExtremeCloud IQ is performed using an Inlets connection on TCP (HTTPS) port 8090. Access to the management entity is routed through the stack of the underlying Universal Compute Platform host. As a result, the routing stack configuration (i.e., the default gateway) path from the host is key to the connection path.

Managed by ExtremeCloud IQ Controller

Tunnels are configured and managed using the ExtremeCloud IQ Controller user interface. Tunnel Concentrator establishes an HTTPS connection to the controller on port 5825. The Concentrator uses stored read-only credentials to retrieve the configuration and to configure GRE/IPSec tunnels.

Note
To generate encryption and decryption keys when IPSec is deployed, the management entity generates a private, pre-shared key using the IKEv2 protocol and uses a secure connection to provision the key on Tunnel Concentrator and on the access points.

Supported Products and Capacities

The following table lists recommended versions for the components that make up the Tunnel Concentrator solution. We recommend that you run the latest version for each component.

Table 6: Supported Products and Versions

Solution Components	Supported Versions
Universal Compute Platform (1130C, 2130C, or 4120C)	Universal Compute Platform v5.09.01
ExtremeCloud IQ	ExtremeCloud IQ v25.01
ExtremeCloud IQ Controller	ExtremeCloud IQ Controller v10.12.01 or later
Access points	Tunnel Concentrator is supported on ExtremeCloud IQ Universal access points and on IQ Engine access points. See *ExtremeCloud IQ Release Notes* for hardware and OS release information.

Refer to the following table for information on supported Tunnel Concentrator capacities for each Universal Compute Platform hardware option.

Table 7: Supported Capacities per Universal Compute Platform Host

Hardware appliance	Supported Capacities
1130C	• Single Tunnel Concentrator instance per appliance. • Maximum of 1,000 tunnels per Tunnel Concentrator instance (without HA) or per HA redundancy configuration (for example, up to 1,000 tunnels per HA pair).
2130C	• Single Tunnel Concentrator instance per appliance. • Maximum of 5,000 tunnels per Tunnel Concentrator instance (without HA) or per HA redundancy configuration (for example, up to 5,000 tunnels per HA pair)
4120C	• Up to three Tunnel Concentrator instances per appliance. • Maximum of 5,000 tunnels per Tunnel Concentrator instance (without HA) or per HA redundancy configuration (for example, up to 5,000 tunnels per HA pair). • Maximum of 15,000 tunnels per appliance.

Note
With ExtremeCloud IQ as the management application, redundancy is configured using HA pairs. With ExtremeCloud IQ Controller as the management application, you can add up to three Tunnel Concentrator instances to the redundancy configuration. For more information, see Redundancy Configuration on page 19.

Tunnel Concentrator Network Architecture

The Tunnel Concentrator application consists of two distinct internal stacks or layers. Each stack has its own set of IP addresses, interfaces, and routing table. There is no direct network access between the stacks, although they do communicate using an internal API. The two stacks are:

- Management layer
- Data layer

The following image provides a high-level of the two stacks for a Tunnel Concentrator instance, along with the internal connections and systems that allow Tunnel Concentrator to connect to an external devices, such as an external switch. The data layer can be accessed directly, but access to the management layer is hidden behind an internal NAT reference with access dependent on the underlying Universal Compute Platform routing table.

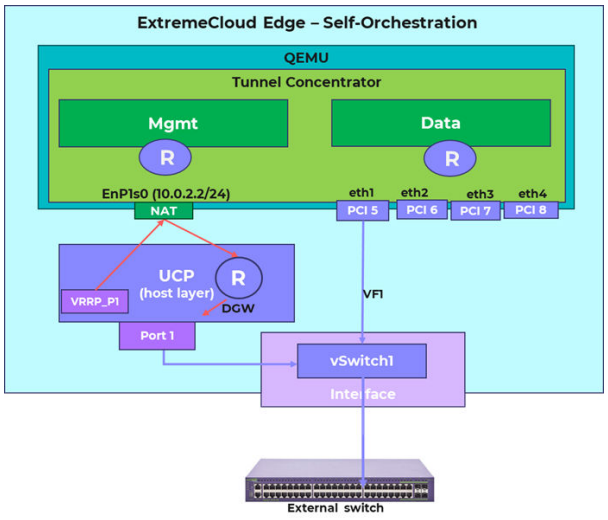


Figure 2: Tunnel Concentrator Internal Network Architecture

Management Layer Access

The management layer of Tunnel Concentrator handles functions related to managing the application. The management layer uses a NAT from the underlying host with a predefined internal address of 10.0.2.2/24, which is bound to the management layer of Tunnel Concentrator, and which cannot be seen from the external network. As a result, the management layer, by default, is not directly exposed for access.

To access the Management User Interface on Tunnel Concentrator, a VRRP address must be configured on one of the data ports of the Universal Compute Platform. This VRRP address can be used as a mapped alias to the application interface, allowing access to the Tunnel Concentrator user interface using that address. User interface access is required during the initial installation process in order to read the instance Activation ID and apply the corresponding Activation license.

Note
After the instance is activated and management by ExtremeCloud IQ has started, the VRRP-mapped alias can be removed because the configuration is exchanged programmatically via the Inlets connection.

Note
We recommend that you configure the Universal Compute Platform's default gateway through one of the available data ports.

Traffic that originates from the host, for example Inlets connections to higher layer management frameworks such as ExtremeCloud IQ, crosses this application interface linkage to the host, which creates a direct dependency between accessing the Tunnel Concentrator instance and the routing settings on the underlying Universal Compute

Platform host. Management traffic must flow through the Universal Compute Platform routing table to determine the path for network access.

Note
The use of ICC interfaces for network management is strongly discouraged. Although the ICC(s) can be seen as allowing for providing out-of-band physical management interface, this assumption, can only be leveraged with extreme care.

User Interface Access to Management Functions

Following activation, the Tunnel Concentrator instance interacts with redirector (hac.extremeiq.com) to discover the management Regional Data Center (RDC). After onboarding to ExtremeCloud IQ is complete, all functional management and configuration is performed from ExtremeCloud IQ.

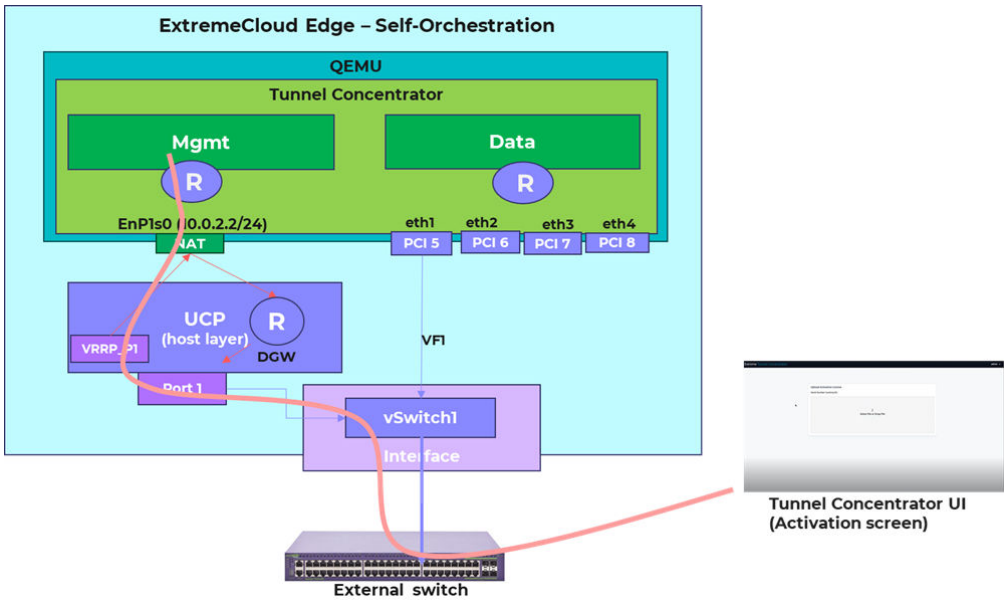


Figure 3: Management Access to User Interface

Note
Once the Tunnel Concentrator instance is managed by ExtremeCloud IQ, the VRRP-IP alias becomes optional, and is required only if you intend to access the user interface of the instance. However, as ExtremeCloud IQ is fully managing the instance state, this access is no longer required and can be removed. You can remove the binding from the port interface configuration window in Universal Compute Platform by removing the VRRP configuration.

Inlets Access for ExtremeCloud IQ Management

When Tunnel Concentrator is managed by ExtremeCloud IQ, the management configuration is exchanged using an Inlets connection. The connection relies on network configurations from the underlying Universal Compute Platform host (for example, the default gateway and interfaces) to discover the Regional Data Center (RDC) on which the management account resides. The Inlets connection

originates within the Tunnel Concentrator application and uses the redirector at (hac.extremecloudiq.com) to connect to the RDC.

The following image illustrates the traffic path that for access to the management layer using ExtremeCloud IQ and the Inlets tunnel.

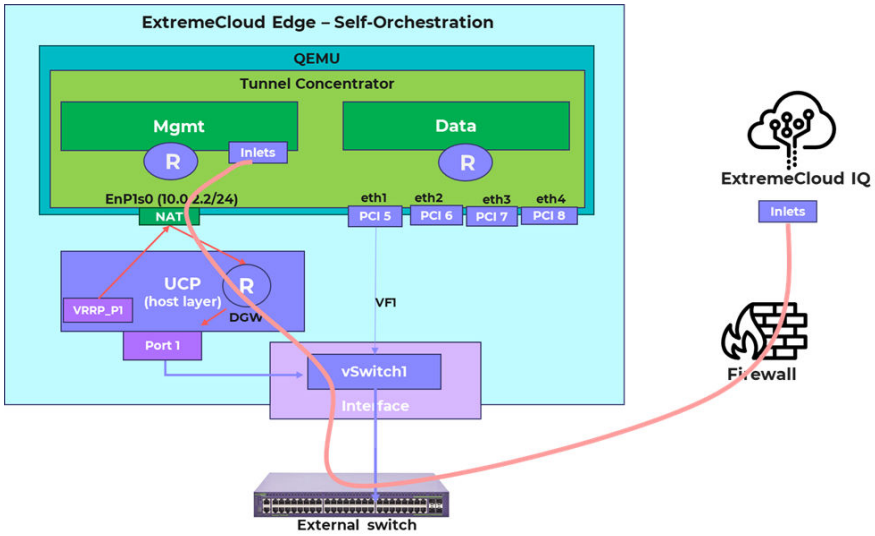


Figure 4: Management Stack to ExtremeCloud IQ using Inlets

Data Layer

The Data layer handles functions related to data traffic encapsulation and traffic forwarding. The data layer allows access using one of four data ports from the underlying host. Each port connects to a dedicated internal virtual switch that can connect to external network devices.

The following image provides an example of a flow between a wireless access point and a Tunnel Concentrator HA deployment that is managed by ExtremeCloud IQ. In this example, the two Tunnel Concentrators share a VRRP address that is configured from ExtremeCloud IQ for the Tunnel Concentrator service. Traffic fom the access point reaches the shared VRRP address and is redirected to the active Tunnel Concentrator in the HA pair. The traffic flows through the data ports into the Tunnel Concentrator data layer.

Note
The VRRP configuration that provides redundancy for an HA deployment is configured in ExtremeCloud IQ, and is different than the VRRP configuration on a data port that provides access to the management interface.

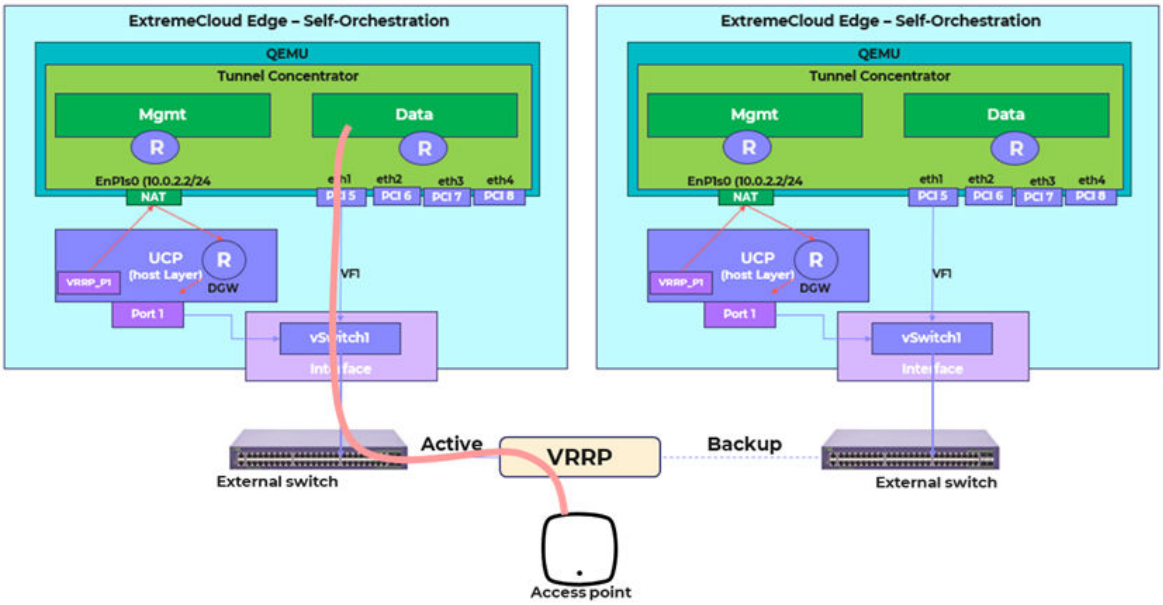


Figure 5: Data Flow from Access Point for HA Deployment

VRRP

Tunnel Concentrator leverages different VRRP configurations for different purposes:

- Management Interface access - User Interface access for activation
- Data Plane High-Availability

These functions are distinct, and should not be confused. Unique IP addresses and Router IDs are required for each function.

ExtremeCloud Edge - Self Orchestrated applications such as Tunnel Concentrator can take advantage of the native support of VRRP in the underlying Universal Compute Platform host (UCP) in order to create interface aliases. Aliases can then be bound to the application to provide a direct linkage between the alias-IP presentation and the application instance to which it is intended to map.

One key aspect when creating VRRP based IP aliases, is to ensure that the VRRP address does not overlap any other address that is allocated to the network segment. Otherwise, you end up creating a VRRP Group as an active/backup configuration, which is not what's intended in terms of using the IPs as direct 'pointers' into the address of specific application instances.

Configuration Requirements

The following table summarizes the VRRP configurations that apply to Tunnel Concentrator and the requirements.

Table 8: Summary of VRRP Configurations

VRRP Configured on...	Configuration Requirements
Data port of Universal Compute Platform host	Required configuration for all Tunnel Concentrator instances. Provides access to the user interface, which is required for initial activation. See Install ExtremeCloud Edge-Self-Orchestration Deployment on page 28.
Tunnel Concentrator Service of ExtremeCloud IQ	Required only if deploying redundant HA pairs when ExtremeCloud IQ is the management application. See Redundancy with ExtremeCloud IQ on page 19.

Note
There is also a VRRP configuration for the ICC1 interface that appears when you run the Basic Configuration wizard on Universal Compute Platform. This VRRP setting should be left disabled.

Redundancy Configuration

Tunnel Concentrator supports tunnel redundancy and failover between multiple instances of the application. Redundancy ensures that tunneling services remain active even if a Tunnel Concentrator instance fails, or if the server on which the application is installed goes down.

Redundant Tunnel Concentrator instances must be in the same network segment with layer 2 connectivity so that services are not affected by a server failure. As a best practice, use instances that are installed on different physical Universal Compute Platform boxes so that a server failure affects only a single instance.

Redundancy configuration and functionality depend on whether you use or ExtremeCloud IQ or ExtremeCloud IQ Controller as the management entity. The subsequent sections describe the redundancy configurations for each deployment type.

Redundancy with ExtremeCloud IQ

Configure redundancy on ExtremeCloud IQ by creating redundant pairs of Tunnel Concentrator instances where each instance in an HA pair shares a single VRRP address, and the pair has an active and standby instance.

When APs send data through a tunnel, they send the data to the shared VRRP address of the HA pair, with data being directed to the active Tunnel Concentrator instance

in the pair. However, if the active instance goes down or becomes unavailable, the standby instance becomes active so that data can be directed to that instance instead.

Note
The VRRP configuration for HA is applied using the Tunnel Concentrator service configuration on ExtremeCloud IQ for a pair of Tunnel Concentrators. This VRRP configuration applies to both Tunnel Concentrators in a pair and should not be confused with the VRRP configuration for the data interface on Universal Compute Platform that gives an individual Tunnel Concentrator instance its login IP address.

The following image illustrates an example of a redundancy setup with ExtremeCloud IQ. This example uses three redundant pairs of Tunnel Concentrator instances that are spread across two Universal Compute Platform 4120C appliances.

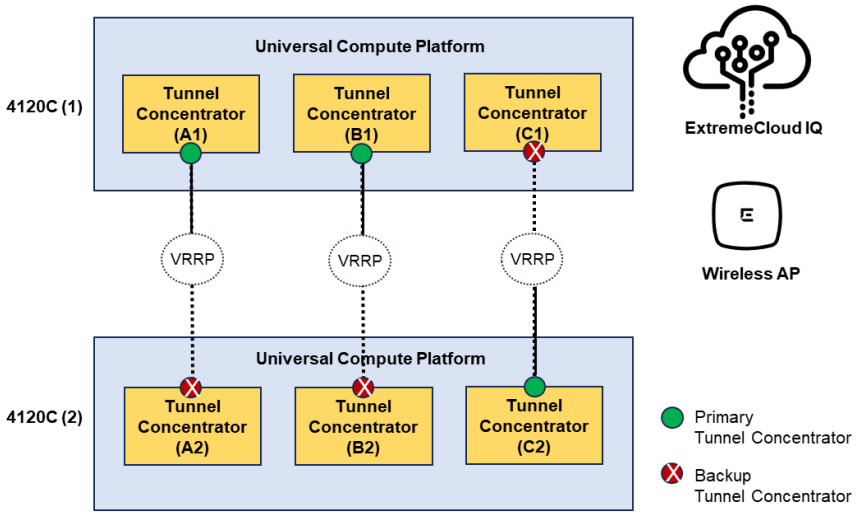


Figure 6: Redundancy Setup with ExtremeCloud IQ

To configure redundancy on ExtremeCloud IQ, use the Tunnel Concentrator Service configuration under **Configure** > **Common Objects** > **Network** > **Tunnel Concentrator Services**. The following image displays the configuration fields. The highlighted fields in the middle of the screen show where VRRP is configured for HA.

To add load balancing, create more than one Tunnel Concentrator service.

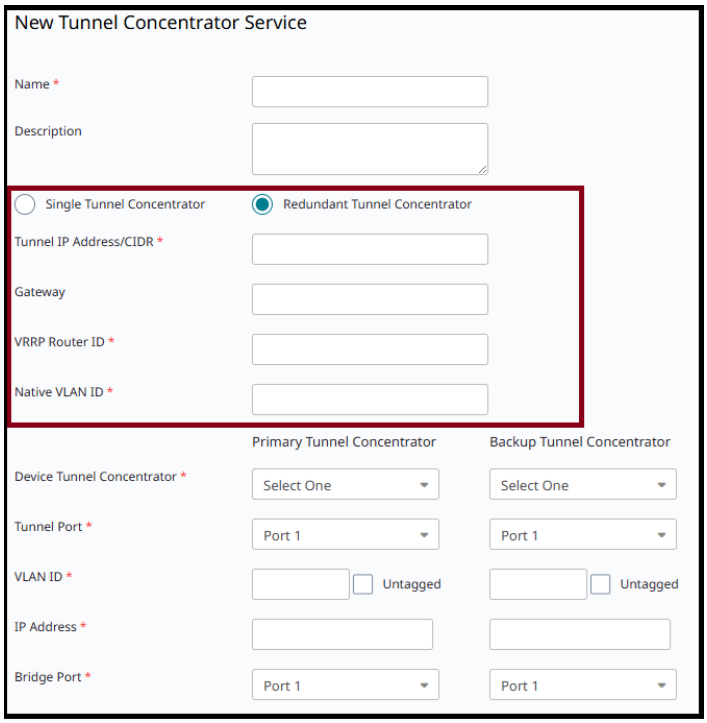


Figure 7: VRRP on Tunnel Concentrator Service of ExtremeCloud IQ

Redundancy with ExtremeCloud IQ Controller

Configure redundancy on ExtremeCloud IQ Controller by configuring GRE tunneling mode for a VLAN with multiple Tunnel Concentrator instances (up to three). You can then assign the VLAN to one or more WLAN networks.

The AP attempts to send traffic for that VLAN to the highest ranked Tunnel Concentrator instance. If that connection fails, the AP attempts to connect to the second higest ranked instance, and if that connection fails, the AP attempts the third instance. The priority ranking depends on whether you also select load balancing:

- If load balancing **is** selected — The priority ranking of the three Tunnel Concentrator instances is selected randomly to ensure that the traffic load gets balanced evenly across the instances.
- If load balancing **is not** selected — The first Tunnel Concentrator instance in the list is given the highest priority ranking followed by the second instance and then the third instance.

Note
ExtremeCloud IQ Controller must be configured to allow an ICMP ping between the access point and the controller. The ping is required for tunnel failover to work.

See the following illustration for a redundancy setup example that uses ExtremeCloud IQ Controller as the management application. This example uses three Tunnel Concentrator instances that are spread across three Universal Compute Platform boxes.

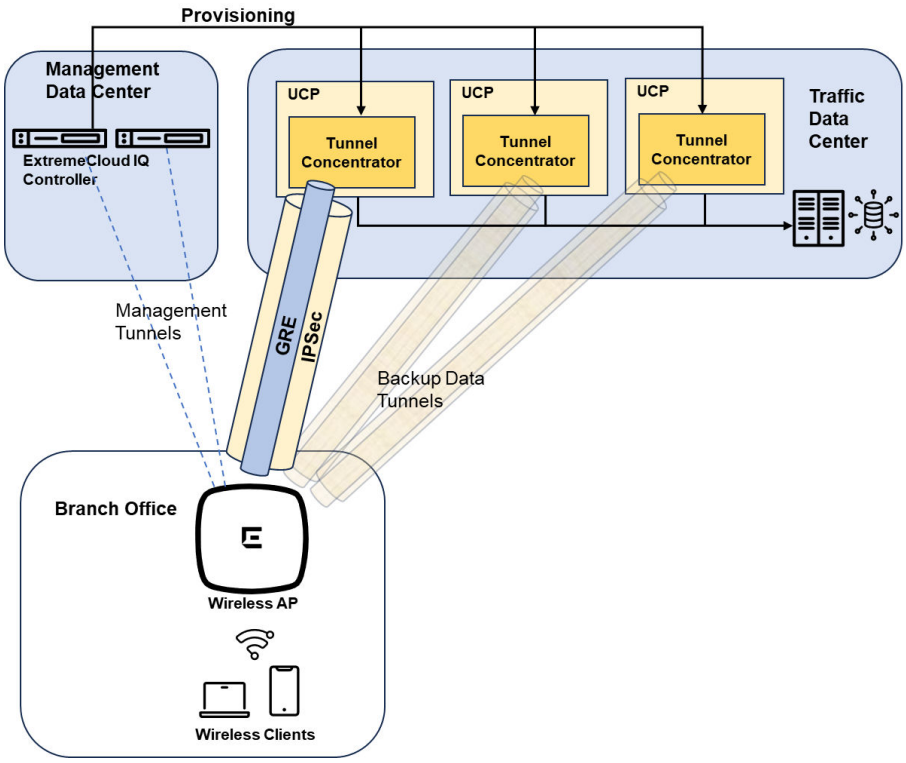


Figure 8: Redundancy Setup with ExtremeCloud IQ Controller

Deployment Considerations and Restrictions

Before deploying Tunnel Concentrator, consider the following:

- Tunnel Concentrator preserves DSCP markings for both upstream and downstream direction.
- Tunnel Concentrator blocks all broadcasts (except DHCP and ARP).
- IPSec is supported only with APs that are managed by ExtremeCloud IQ Controller.
- The VLAN and subnet that you apply to the tunnel termination point on Tunnel Concentrator must be different than the VLAN and subnet for client traffic.
- Tunnel Concentrator does not support the use of a NAT router between the access point and Tunnel Concentrator if the deployment is managed by ExtremeCloud IQ. Tunnel Concentrator must be on the same side of the firewall as the access point as illustrated in the following image.

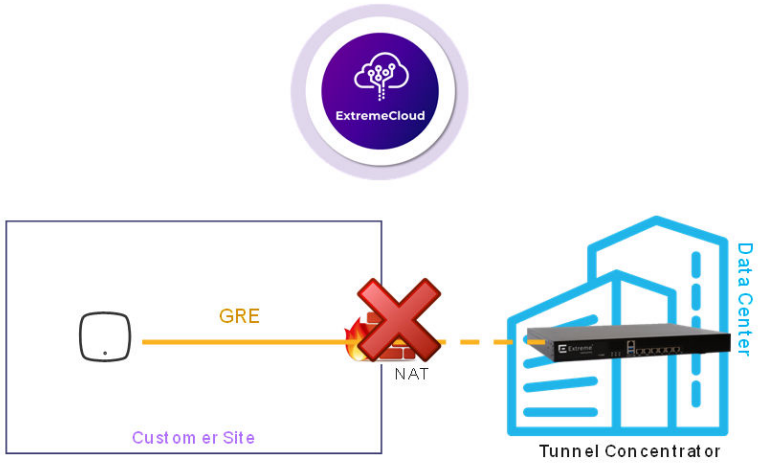


Figure 9: NAT Restriction with ExtremeCloud IQ as Management Application

Note
The NAT restriction does not apply to Tunnel Concentrator deployments that are managed by ExtremeCloud IQ Controller.

- The use of the ICC1 interface for Out-of-Band management of Tunnel Concentrator is not recommended for the following reasons:
  - The ICC1 interface is intended for backplane inter-connect for multi-node cluster configurations. This configuration is not currently supported for Self-Orchestration deployments.
  - ExtremeCloud Edge leverages Kubernetes to manage the state of installed applications. The Kubernetes "cluster" is bound to the address of ICC interfaces (or VRRP if it's provisioned). However, if those addresses change, or need to be modified, Kubernetes recognizes that the existing configuration binding is no longer valid and unwinds the installation, resulting in the purging of the installed applications. In other words, if the ICC IP addresses are modified, the system resets to a pre-deployment state. As a protection against accidental destruction, the Universal Compute Platform user interface prevents modifications to ICC addresses once the deployment type is initialized, which occurs when the standalone cluster is created.
  - Tunnel Concentrator relies on the routing table of the Universal Compute Platform host to be able to reach the management entity. Often, the routing path for out-of-band management segments is constrained and does not provide the necessary access to the internet, which is required for ExtremeCloud IQ.

  For these reasons, ICC1 IP settings must be configured, but we strongly recommended to leave network connectivity disabled. Instead, we recommend that you configure the interface settings to a non-overlapped network segment, preferably a reserved and not-in-use address space. Configure the host to default all network access to a default gateway path through one of the data ports.

ARP Responder

Tunnel Concentrator supports ARP Responder by default. Tunnel Concentrator stores its own local ARP lookup table and can proxy and respond to ARP requests. No configuration is required to enable this feature

To update its ARP table, Tunnel Concentrator uses the following logic:

- Tunnel Concentrator updates its ARP table using IP address - MAC address mappings that it learns from DHCP packets, or from the source IP address of packets that ingress over a GRE tunnel.
- Tunnel Concentrator does not store mappings that it learns from the bridged portion of the network.

To respond to ARP requests, Tunnel Concentrator does a lookup of its ARP table for a MAC address that maps to the target IP address from the ARP request and responds as per these rules:

- If the ARP lookup succeeds, Tunnel Concentrator returns an ARP response to the sender directly with the correct MAC address.
- If the ARP lookup fails, Tunnel Concentrator forwards the ARP broadcast to the bridged network. Tunnel Concentrator does not forward ARP broadcasts to GRE tunnels.

LAG Configuration Summary

Tunnel Concentrator supports Link Aggregation (LAG) for the data ports. LAG interfaces increase link throughput and provide redundancy in case of a link failure.

To deploy the feature on Tunnel Concentrator, you must first configure LAG for Universal Compute Platform. The LAG port members that you configure on Universal Compute Platform get synced to Tunnel Concentrator automatically. To complete the setup, configure Tunnel Concentrator to use the LAG port. Once the feature is configured, LACP LAG on Universal Compute Platform creates and manages the aggregated link, and static LAG from Tunnel Concentrator runs on that link.

Note
Tunnel Concentrator supports static LAG only. Universal Compute Platform supports LACP LAG only.

To configure LAG, assign the settings in the following table. For step 2, complete only the configuration for your management application.

Table 9: LAG Configuration Summary

Step	Task	For a procedure...
1	**On the Universal Compute Platform** host: Configure LACP LAG for the data interface.	"Configure LAG Ports" in Universal Compute Platform User Guide
2	Configure static LAG for Tunnel Concentrator from your management application. Make sure the LAG configuration matches the configuration from the host. **On ExtremeCloud IQ**, assign the LAG port to the Tunnel Concentrator service: • Set **Tunnel Port** to the LAG port (required setting). • Set **Bridge Port** to the LAG port (optional setting). **On ExtremeCloud IQ Controller**, assign the LAG port to Tunnel Concentrator device: • Under **GRE/IPSec tunnel termination point**, set **Port** to the LAG port (required setting). • Under **GRE/IPSec bridge interface**, set **Port** to the LAG port (optional setting).	For ExtremeCloud IQ: Configure Tunnel Concentrator Services on page 38 For ExtremeCloud IQ Controller: Configure Tunnel Concentrator on page 50

The following image shows the Tunnel Concentrator LAG configuration when ExtremeCloud IQ is the management entity. From the **Tunnel Concentrator Service** window, set **Tunnel Port** to the LAG port that you configured on Universal Compute Platform. Optionally, you can also set **Bridge Port** to the LAG port, but it's not required.

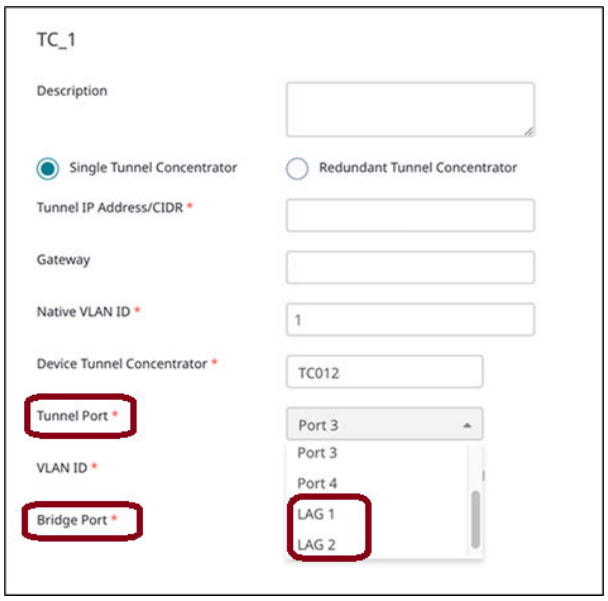
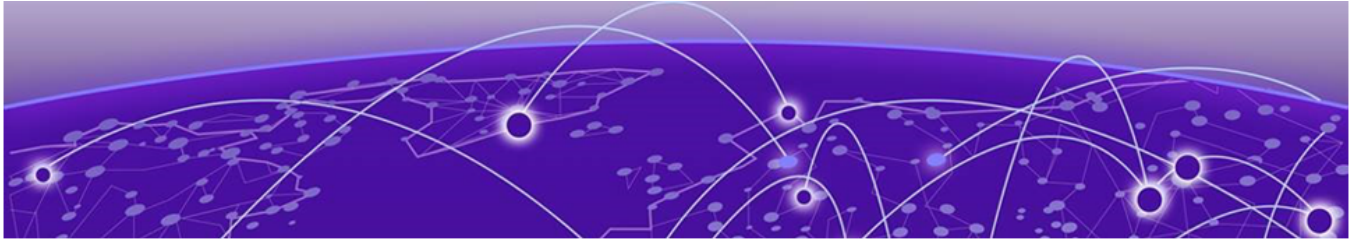


Figure 10: LAG Configuration for Tunnel Concentrator from ExtremeCloud IQ



Installation

The procedures in this chapter describe how to install the Tunnel Concentrator application as a container on the Universal Compute Platform.

Installation Prerequisites

Before you install Tunnel Concentrator, make sure that you meet the following requirements:

Licensing and Activation Prerequisites

Complete the following install and license requirements on the Extreme Networks Support Portal:

- Purchase the Tunnel Concentrator activation SKU **EXTR-IQ-TC**.
- Download the Tunnel Concentrator installation image from the portal at `Downloads/ExtremeCloud/Extreme Tunnel Concentrator`.

Universal Compute Platform Prerequisites

Install and connect the hardware appliance. Refer to the Installation Guide model for your selected model:

- 1130C
- 2130C
- 3150C
- 4120C

ExtremeCloud IQ Prerequisites

If you choose to deploy ExtremeCloud IQ as the management application, note the following:

- You must provide connectivity from the Universal Compute Platform to the internet over port 8090. This is required for the connection to ExtremeCloud IQ.
- For ExtremeCloud IQ configuration information, see *ExtremeCloud IQ User Guide*.
- We recommend that you also onboard your Universal Compute Platform deployment to ExtremeCloud IQ, although this is not mandatory. For details, see

ExtremeCloud Edge - Self-Orchestration Deployment Guide for Universal Compute Platform.

ExtremeCloud IQ Controller Prerequisites

If you choose to deploy ExtremeCloud IQ Controller, note the following:

- You must configure connectivity to the controller from the Universal Compute Platform over TCP port 5825.
- Configure a read-only user account on the controller that is different than the standard admin account.

Tip
As a best practice, set up separate read-only accounts for each Tunnel Concentrator instance. For example, if you have six different Tunnel Concentrator instances, configure six dedicated read-only accounts and the standard admin account. However, while multiple read-only accounts is a best practice, it's not mandatory.

- For ExtremeCloud IQ Controller configuration information, see *ExtremeCloud IQ Controller User Guide*.

Reserved IP Ranges

The following table displays the reserved IP addressing ranges for use with Tunnel Concentrator.

Table 10: Reserved IP Ranges

Purpose	IP Range	Details
Tunnel Concentrator Application Network	10.0.2.0/24	This range is non-configurable. The range forms the attachment point for management access to the Tunnel Concentrator application.
Pod Network	10.0.96.0/16 (default)	During ExtremeCloud Edge installation, assign the default range, or another range that meets your network needs.
Service Network	10.0.97.0/16 (default)	During ExtremeCloud Edge installation, assign the default range, or another range that meets your network needs.

Installation Task Flow

Complete the tasks in the following flow to complete the installation and initial setup of Tunnel Concentrator on the Universal Compute Platform.

Before you Begin

Review Installation Prerequisites on page 26 and make sure that you meet the full list of requirements for your deployment.

Table 11: Installation Task Flow

	Procedure	Description
1	Install ExtremeCloud Edge-Self-Orchestration Deployment on page 28	Install ExtremeCloud Edge - Self-Orchestration deployment on Universal Compute Platform. Tunnel Concentrator will be installed on this deployment.
2	Upload Tunnel Concentrator Image on page 31	Upload Tunnel Concentrator application image to Universal Compute Platform.
3	Install Tunnel Concentrator on page 31	Install the Tunnel Concentrator application on Universal Compute Platform.
4	Change Default Admin Password on page 32	As a best practice, change the default admin password immediately following the first login.
5	Generate the Activation License on page 33	Activate the license for your installation.
6	Select the Management Option on page 33	Select which management application you will use for tunnel provisioning: • ExtremeCloud IQ • ExtremeCloud IQ Controller

Install ExtremeCloud Edge-Self-Orchestration Deployment

Before you install Tunnel Concentrator, you must deploy an ExtremeCloud Edge - Self-Orchestration deployment on a Universal Compute Platform appliance. For installation procedures, see the document ExtremeCloud Edge - Self-Orchestration Deployment Guide.

Make sure that your installation includes the following settings:

- Deployment Type=Self-Orchestration
- Cluster Node Information=Standalone
- ICC1 IP Address — Configure an ICC1 IP address, but leave ICC1 connectivity disabled. Make sure the address does not overlap with existing routing domains. For additional detail, see ICC1 information in Deployment Considerations and Restrictions on page 22.
- Pod Network IP Address — Configure a reserved IP range for use by the Pod network. The default is 10.96.0.0.
- Pod Network CIDR=16
- Service Network IP Address — Configure a reserved IP range for use by the Service network. The default is 10.97.0.0.
- Service Network CIDR=16
- VRRP configured on a data port — Configure a VRRP virtual IP address on one of the Universal Compute Platform data ports. This address will later be assigned to the

installed Tunnel Concentrator instance, providing that instance with an IP address. This configuration is required for initial Tunnel Concentrator activation.

Note

- For the VRRP configuration, see the "Add a Port" procedure within the ExtremeCloud Edge - Self-Orchestration Deployment Guide.
- For the VRRP address, use the data port that provides the best connectivity to the network. It's recommended to use the same segment that provides the default gateway for the Universal Compute Platform host.
- Make sure that the VRRP address does not overlap with existing addresses.
- When deploying multiple Tunnel Concentrator instances on a single host, configure a VRRP address for each instance..

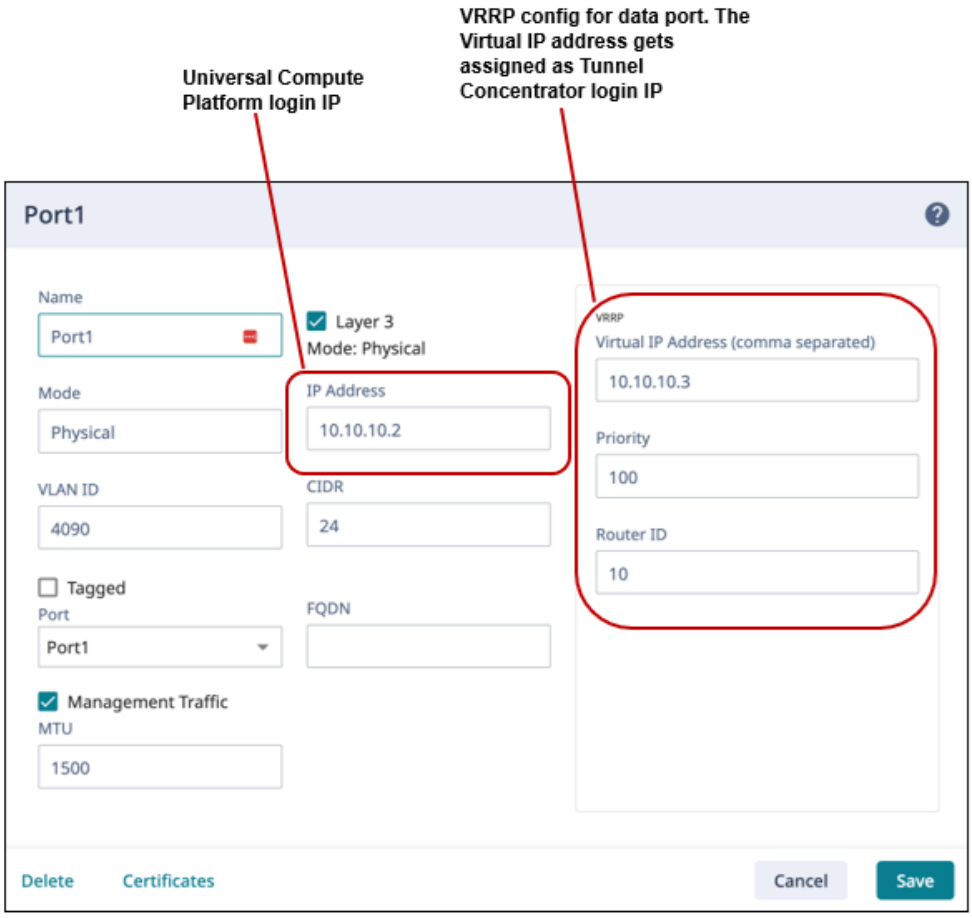


Figure 11: VRRP Configuration on Data Port of Universal Compute Platform

Note
If Tunnel Concentrator is managed by ExtremeCloud IQ, the VRRP-IP alias is required for activation, but once the instance is onboarded to the cloud, the alias becomes optional.

- LAG (Optional)—If you want to deploy LAG ports on Tunnel Concentrator, configure LAG on Universal Compute Platform first. For more information about LAG, see LAG Configuration Summary on page 24.

Note
For an ExtremeCloud Edge and Tunnel Concentrator installation example with sample settings, see Installation Example on page 34.

Upload Tunnel Concentrator Image

Use this procedure to upload the Tunnel Concentrator application image to the Universal Compute Platform hardware appliance.

Note

- Make sure that you're completed all Installation Prerequisites on page 26, including purchasing the SKU and downloading the application image from the portal.
- You need to upload the image to the appliance once only per appliance. If this is the second or third Tunnel Concentrator installation on this appliance, and you uploaded previously, you can skip this procedure.

1. Log in to the Universal Compute Platform.
2. Go to **Engines** > **Image Management**.

   The **Image Management** page lists the image files that are uploaded to Universal Compute Platform If the Tunnel Concentrator appears, then you can skip this procedure.
3. Upload the image using either of these methods:
   - Select **Choose image file or Drag and Drop here**, browse to the application image file on your local drive and select it.
   - On your local drive, select the image file and drag the file onto the Universal Compute Platform desktop.

   The file uploads automatically. You can proceed to install the application.

Install Tunnel Concentrator

Use this procedure to install the Tunnel Concentrator application on the Universal Compute Platform appliance.

1. Log in to the Universal Compute Platform.
2. Go to **Engines** > **Installation**.
3. From the **Extreme Tunnel Concentrator** pane, select **Install**.
4. In the popup window, select **OK**.

   A new instance of Tunnel Concentrator displays on the **Engines** page along with a link.
5. Within the **Extreme Tunnel Concentrator** pane, select the link for your installation.

6. Configure the following settings:
   - **Node Affinity**—Select the Universal Compute Platform node on which this Tunnel Concentrator instance will run.
   - **Ports (1, 2, 3 and 4)**—By default, the lowest unassigned VF on the switch is assigned. We recommend that you retain the defaults, although you can assign any unassigned VF.

     Note
     The Tunnel Concentrator instance is locked to the VF number. By default, the first application instance on a host uses VF01 for all ports, the second application uses VF02, and the third uses VF03. We recommend that you retain the default VF assignments.

7. Select **Deploy**.

   The application deploys. After a delay of up to a few minutes, the Tunnel Concentrator screen displays the following four tabs:
   - Network Service Configuration
   - Statistics
   - Logs
   - Console
8. Under the **Network Service Configuration** tab, select the **Assigned Virtual IP Address** drop-down and select an IP address for the Tunnel Concentrator service. This IP address will be used to generate the login URL.
9. Select **Save**.

   After a delay of up to a few minutes, the screen displays an **Instance web interface** link.
10. Select the **Instance web interface** link to launch the Tunnel Concentrator GUI.
11. Log in using the default admin credentials:
    - username: admin
    - password: abc123

What to do Next

As a best practice, change the default admin password immediately after you login for the first time.

Change Default Admin Password

Use this procedure to change the default admin password for the Tunnel Concentrator user interface.

Note
As a best practice, change the admin password immediately after you login for the first time.

1. Log in to the Tunnel Concentrator user interface using the default admin credentials.
2. Select (User Actions icon) from the top right of the header.

3. Select **Change Password**.
4. In the **Password** box, enter the new admin password.
5. In the **Confirm Password** box, re-enter the new admin password.
6. Select **Update**.

Generate the Activation License

After you install Tunnel Concentrator, use this procedure to generate and install the activation package on Tunnel Concentrator to activate the application instance.

Note

- The activation file is signed to the Serial Number of the Tunnel Concentrator instance, which is read from the instance. The activation file is provided as part of the voucher redemption workflow.
- Installing the activation package also installs Extreme device certificates that allow secure communication with the management entity.

1. Obtain the Locking ID of the Tunnel Concentrator instance:
   a. Log in to the Tunnel Concentrator instance
   b. Under **Upload Activation License**, copy the **Serial Number (Locking ID)** value.
2. Obtain the activation file:
   a. Log in to the *Extreme Networks Support Portal* .
   b. Go to **Assets** > **Licenses Home** and select the Tunnel Concentrator Voucher ID line item from the list.
   c. On the **Voucher Details** page, select **Generate Activation Key**.
   d. Provide the serial number for the Tunnel Concentrator activation.
   e. Select the box to accept **Terms and Conditions** and click **Submit** to generate the activation file.
   f. Download the activation file.
3. Install the activation file on Tunnel Concentrator:
   a. If you signed out of Tunnel Concentrator, sign back in.
   b. Upload the license file to the **Upload Activation License** pane of Tunnel Concentrator.

What to do Next

Select the management application for GRE tunnel provisioning.

Select the Management Option

Select the management application that you want to use to provision tunnels for Tunnel Concentrator.

1. Log in to Tunnel Concentrator.
2. Go to **Configuration**.

3. Select the tab that matches your management entity:
   - **Managed by ExtremeCloud IQ Controller**
   - **Managed by ExtremeCloud IQ**
4. If you chose ExtremeCloud IQ Controller, complete the controller onboarding fields:
   - **Primary Controller IP Address**
   - **Backup Controller IP Address** ((only if a backup controller exists).
   - **Application Key**—Enter the application key of the controller. If you do not have a key, you can generate one from Tunnel Concentrator. For details, see the subsequent Note.
   - **Application Password**—Enter the login password for the controller.

   Note

   If you do not have an application key, select **Generate Application Key**, complete the following fields with controller login information, and then select **Generate**:
   - **Primary Controller IP address**
   - **Admin Username**
   - **Admin Password**
   - **Read-only account**—Enter the username for the read-only account for this Tunnel Concentrator instance.

   You can also obtain the application key from the **Administration** > **Accounts** page of ExtremeCloud IQ Controller.

5. Select **Save**.

What to do Next

Go to the configuration chapter that matches your choice of management application. Use the applicable chapter to provision tunneling for your deployment:

- ExtremeCloud IQ Configuration on page 36
- ExtremeCloud IQ Controller Configuration on page 49

Installation Example

The following configuration example provides sample settings for a Tunnel Concentrator installation on Universal Compute Platform.

Note

For procedures on how to install ExtremeCloud Edge-Self-Orchestration Deployment on Universal Compute Platform, see ExtremeCloud Edge - Self-Orchestration Deployment Guide.

Universal Compute Platform Settings

Configuration Wizard:

```
ICC1 Port IP Address=192.168.100.14
ICC1 Port Netmask =255.255.255.0
```

```
ICC1 Port VRRP IP Address=
ICC1 Port VRRP Priority=100
ICC1 Port VRRP Router ID=1
Enable Lag on ICC1 Port=n
Data Port=Port 1
IP address=10.10.10.1
Netmask=255.255.255.0
VLAN ID=1
Tagged frames=n
Management on this interface=y
Host Name=universalcomputeplat
Domain Name=extremenetworks.com
Primary DNS server=8.8.8.8
Default Gateway=192.168.100.1
Timezone=America/Detroit
NTP server 1=time.nist.gov
```

Cluster Configuration (from user interface):

```
Deployment Type=Self-Orchestration
Cluster Node Information=Standalone
ICC IP Address 192.168.100.14
Pod Network IP Address = 10.96.0.0
Pod Network CIDR 16
Service Network IP Address = 10.97.0.0
Service Network CIDR = 16
```

VRRP Configuration for Data Port 1 (from user interface):

```
VRRP: Virtual IP Address=10.10.10.2
Priority=100
Router ID=10
```

Tunnel Concentrator Initial Settings:

```
Node Affinity=universalcomputeplat.extremenetworks.com
Port 1=VF01
Port 2=VF01
Port 3=VF01
Port 4=VF01
Assigned Virtual IP Address=10.10.10.2
```

ExtremeCloud IQ Configuration

If you are using ExtremeCloud IQ as your management option, complete the following configuration tasks on ExtremeCloud IQ to provision tunnels for Tunnel Concentrator.

Note
Before you complete the following configuration tasks, complete the procedures in the Installation chapter.

Table 12: ExtremeCloud IQ Configuration

	Procedure	Description
1	Quick Add Tunnel Concentrators on page 37	Onboard Tunnel Concentrator instances as devices to ExtremeCloud IQ. This task registers the instance serial numbers.
2	Configure Tunnel Concentrator Services on page 38	Add and configure a Tunnel Concentrator Service to serve as a **Tunnel Destination** for network policies. A Tunnel Concentrator Service can be single or redundant.

Table 12: ExtremeCloud IQ Configuration (continued)

	Procedure	Description
3	• Configure Tunnel Policies on page 41 • Configure a User Profile for Traffic Tunneling on page 42 • Apply Different User Profiles to Clients and User Groups on page 42	Use network and user policies to direct traffic to the Tunnel Concentrator. While editing an existing network policy or creating a new one, edit the **User Access Settings** to apply different profiles to clients and user groups.
4	Edit Tunnel Concentrator Hostname on page 43	Optional. Edit the hostname of the Tunnel Concentrator instance.

Note
See Configuration Example on page 43 for an example of a redundant Tunnel Concentrator deployment with ExtremeCloud IQ. The example provides sample IP address assignments for Universal Compute Platform and Tunnel Concentrator.

Considerations

- Each Tunnel Concentrator Service can reference one Tunnel Concentrator device.
- Primary and backup Tunnel Concentrators must belong to the same network policy.
- For a redundant Tunnel Concentrator, the IP addresses of both the primary and redundant Tunnel Concentrators must belong to the same subnet as the **Tunnel IP Address/CIDR**.
- The Gateway IP Address must belong to the same subnet as the **Tunnel IP Address/CIDR**.

Related Links

Quick Add Tunnel Concentrators on page 37
Configure Tunnel Concentrator Services on page 38
Configure Tunnel Policies on page 41
Configure a User Profile for Traffic Tunneling on page 42
Apply Different User Profiles to Clients and User Groups on page 42

Quick Add Tunnel Concentrators

First deploy the Tunnel Concentrators instances. For more information, see Installation on page 26.

Use this task to quickly add Tunnel Concentrator instances as devices and register the serial number for each instance.

1. Log in to ExtremeCloud IQ.
2. Go to **Manage** > **Devices**.
3. Select +, then select **Quick Add Devices**.
4. Select **Manage your devices directly from the cloud**.

5. For **Device Type**, select **Real**.
6. For **Entry Type**, select **Manual**.
7. Type the **Serial Number** of the device.
8. From the **Device Make** menu, select **Tunnel Concentrator**.
9. (Optional) From the **Policy** menu, select an existing network policy.

   If you do not already have an existing policy configured for this purpose, skip this step and add the policy later.
10. Select **Add Devices**.

After you complete this procedure, you can open the Tunnel Concentrator application from ExtremeCloud IQ.

Select a Tunnel Concentrator from the **Devices** page to view the device details. To open the Tunnel Concentrator application, go to one of the following locations:

- **Device Details** > **Monitoring** > **Overview**
- **Device Details** > **Monitoring** > **System Information**

Related Links

Configure Tunnel Concentrator Services on page 38
Configure Tunnel Policies on page 41
Configure a User Profile for Traffic Tunneling on page 42

Configure Tunnel Concentrator Services

Add the Tunnel Concentrator as a device type. See Quick Add Tunnel Concentrators on page 37.

Perform this procedure to configure a new Tunnel Concentrator service.

1. Log in to ExtremeCloud IQ.
2. Go to **Configure** > **Common Objects** > **Network** > **Tunnel Concentrator Services**.
3. Configure the settings for the Tunnel Concentrator Service.

   See Tunnel Concentrator Services Settings on page 39.
4. Select **Save**.

Related Links

Quick Add Tunnel Concentrators on page 37
Tunnel Concentrator Services Settings on page 39

Tunnel Concentrator Services Settings

Settings for a Single Tunnel Concentrator

Table 13: Single Tunnel Concentrator

Field	Description
Name	(Required) Type a name to identify the new Tunnel Concentrator service.
Description	(Optional) Provide a description that might be helpful when troubleshooting.
Single Tunnel Concentrator	(Required) Select this option to create a single Tunnel Concentrator without redundancy.
Tunnel IP Address/CIDR	(Required) Type the IP Address for the tunnel (CIDR).
Gateway	(Optional) Type the IP address of the gateway.
Native VLAN ID	(Required) Type the Native VLAN ID. The Native VLAN is untagged.
Device Tunnel Concentrator	(Required) Select a Tunnel Concentrator from the menu.
Tunnel Port	(Required) Select a port from the menu. If you are deploying LAG, you must select a LAG port.
VLAN ID	(Required) Type the VLAN ID. (Optional) For an untagged VLAN, select the corresponding check box.
Bridge Port	(Required) Select a bridge port for the tunnel from the menu. If you are deploying LAG, you may select a LAG port, although it's not mandatory.

Settings for a Redundant Tunnel Concentrator

Table 14: Redundant (Primary and Backup) Tunnel Concentrators

Field	Description
Name	(Required) Type a name to identify the new Tunnel Concentrator service.
Description	(Optional) Provide a description that might be helpful when troubleshooting.

Table 14: Redundant (Primary and Backup) Tunnel Concentrators (continued)

Field	Description
Redundant Tunnel Concentrator	(Required) Select this option to create a redundant Tunnel Concentrator.
Tunnel IP Address/CIDR	(Required) Type the VRRP IP Address for the tunnel (CIDR).
Gateway	(Optional) Type the IP address of the gateway.
VRRP Router ID	(Required) Type the ID for the VRRP router. ExtremeCloud IQ configures the same VRRP Router ID for both the primary and backup Tunnel Concentrators (range 1-255). The **VRRP Router ID** must be different for each cluster of VRRP devices. In addition, the ID must be different than the VRRP Router IDs that were configured on the data ports for the individual Tunnel Concentrator instances.
Native VLAN ID	(Required) Type the Native VLAN ID. The Native VLAN is untagged.
Device Tunnel Concentrator	(Required—Primary and Backup) Select a primary Tunnel Concentrator from the menu. Select a backup Tunnel Concentrator from the menu.
Tunnel Port	(Required—Primary and Backup) Select a port for the tunnel from the menu for the primary Tunnel Concentrator from the menu. If you are deploying LAG on this Tunnel Concentrator, select a LAG port. Select a port for the tunnel from the menu for the backup Tunnel Concentrator from the menu. If you are deploying LAG on this Tunnel Concentrator, select a LAG port.
VLAN ID	(Required—Primary and Backup) Type the VLAN ID for the primary and for the backup Tunnel Concentrators. (Optional) For an untagged VLAN, select the corresponding check box.

Table 14: Redundant (Primary and Backup) Tunnel Concentrators (continued)

Field	Description
IP Address	(Required—Primary and Backup) Type the IP address for the primary and the backup Tunnel Concentrators.
Bridge Port	(Required—Primary and Backup) Select a bridge port for the tunnel from the menu for the primary Tunnel Concentrator. If you are deploying LAG on this Tunnel Concentrator, you may select a LAG port, although it's not mandatory. Select a bridge port for the tunnel from the menu for the backup Tunnel Concentrator. If you are deploying LAG on this Tunnel Concentrator, you may select a LAG port, although it's not mandatory.

Configure Tunnel Policies

Add the Tunnel Concentrators and configure the Tunnel Concentrator services.

Use the following steps to add a new tunnel policy to support Layer 2 roaming with Tunnel Concentrator. Alternately, you can skip this step and create a user policy with Traffic Tunneling (GRE) to Tunnel Concentrator. See Configure a User Profile for Traffic Tunneling on page 42.

Use the following steps to add a new tunnel policy to support Layer 2 roaming with Tunnel Concentrator. Alternately, you can skip this step and create a user policy with Traffic Tunneling (GRE) to Tunnel Concentrator.

1. Log in to ExtremeCloud IQ.
2. Go to **Configure** > **Common Objects** > **Network** > **Tunnel Policies**.
3. Select the plus sign.
4. Enter a name for this policy.
5. Enter an optional description for the policy.

   Although optional, descriptions can be helpful when you are troubleshooting your network.
6. Select **Layer 3 Roaming** to adjust Layer 3 roaming thresholds.

   You can add a new Tunnel Concentrator service by selecting +, or select for an existing instance. For more information, see Configure Tunnel Concentrator Services on page 38.
7. Select **Save**.

   The **Tunnel Policies** table displays the following information for the configured tunnel policies in your network:

   - **Name**: The name of the tunnel policy.
   - **Description**: An optional description of the policy.
   - **Used by**: The number of network policies to which the tunnel policy is applied. Hover over a number in this column to see the names of the network policies.

Related Links

Quick Add Tunnel Concentrators on page 37
Configure a User Profile for Traffic Tunneling on page 42
Configure Tunnel Concentrator Services on page 38

Configure a User Profile for Traffic Tunneling

Use the following procedure to configure GRE traffic tunneling using Tunnel Concentrator for a user profile.

1. Log in to ExtremeCloud IQ.
2. Go to **Configure** > **Network Policies** or to **Configure** > **Common Objects** > **Policy** > **User Profiles**, and either create a new user profile, or select an existing profile to edit.
3. On the **Traffic Tunneling** tab, turn on **Traffic Tunneling (GRE)**.
4. Select an existing profile from the **Re-use Tunnel Policy** menu, and then select the type of tunneling.
5. For **Tunnel Concentrator**, select the **Tunnel Destination** from the drop-down list.

   You can add a new Tunnel Concentrator service by selecting +, or select to modify an existing instance. For more information, see Configure Tunnel Concentrator Services on page 38.
6. Select **SAVE**.

Related Links

Configure Tunnel Concentrator Services on page 38

Apply Different User Profiles to Clients and User Groups

Before you can apply different user profiles, configure the SSID for the network. For more information, see *ExtremeCloud IQ User Guide*.

With user-profile assignment rules, you can assign clients to user profiles that match all configured conditions. The available conditions are as follows:

- Advanced Guest Policy
- Client OS Type
- Client MAC Address
- Client Location
- Schedule
- Cloud Config Group

Use the following procedure to map the VLAN to the GRE tunnel VLAN for Tunnel Concentrator.

1. Go to **Configure** > **Network Policies**.
2. Select an existing policy, and then select , or select +.
3. After you save the **Policy Details**, select **NEXT** or **2 Wireless**.
4. Under **User Access Settings**, select **Apply a different user profile to various clients and user groups**.

5. Select to choose an existing user profile, or select + to add a new profile.
6. To add an existing user profile assignment rule, select .
   a. Select one of the existing rules.
   b. Select **Link**.
7. To add a new user profile assignment rule, select .
   a. Type a **Name** for the user profile assignment rule.
   b. (Optional) Type a description.
   c. Select + and choose a category.
   d. Complete the configuration for the selected category.

      For more information, see *ExtremeCloud IQ User Guide*.

   You can add multiple assignment rules to create more granular control.
8. Select **Save**.

Edit Tunnel Concentrator Hostname

Use this optional procedure to change the hostname of a Tunnel Concentrator instance that is managed from ExtremeCloud IQ.

1. Log in to ExtremeCloud IQ.
2. Go to **Manage** > **Devices**.
3. From the devices list, select the host name of the applicable Tunnel Concentrator instance.

   The Device Details page opens for the Tunnel Concentrator instance.
4. Select the **Configure** tab.
5. From the **Configuration** menu, select **Device Configuration**.
6. Edit the value of the **Host Name** field.
7. Select **Save Device Configuration**.

Configuration Example

The following image provides an example of a redundant Tunnel Concentrator deployment with ExtremeCloud IQ as the management application. The example provides sample IP address assignments for the deployment.

With this example, six Tunnel Concentrator application instances are deployed in HA pairs across two different Universal Compute Platform 4120C hosts.

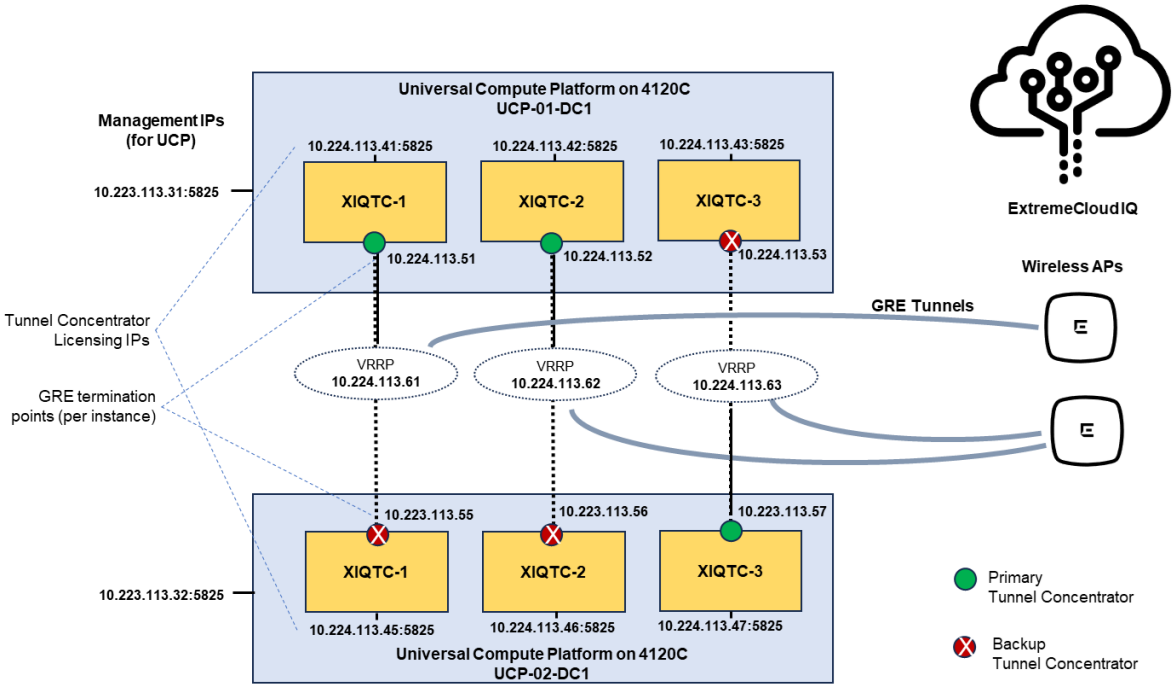


Figure 12: Configuration Example with ExtremeCloud IQ and Redundancy

Configuration Example on page 43 provides more information on the IP address assignments.

Table 15: IP Address Assignments

Universal Compute Platform (UCP) on 4120C	Management IP (for UCP)	Tunnel Concentrator Instances	Tunnel Concentrator Licensing IPs	GRE Termination Points (per instance)	VRRP IPs
UCP-01-DC1	10.224.113.31:5825	XIQTC-1	10.224.113.41:5825	10.224.113.51 (primary)	10.224.113.61
		XIQTC-2	10.224.113.42:5825	10.224.113.52 (primary)	10.224.113.62
		XIQTC-3	10.224.113.43:5825	10.224.113.53 (backup)	10.224.113.63
UCP-02-DC1	10.224.113.32:5825	XIQTC-1	10.224.113.45:5825	10.224.113.55 (backup)	10.224.113.61
		XIQTC-2	10.224.113.46:5825	10.224.113.56 (backup)	10.224.113.62
		XIQTC-3	10.224.113.47:5825	10.224.113.57 (primary)	10.224.113.63

The following details provide information on how to configure each column:

- Universal Compute Platform—This example uses two hardware servers.
- Management IP (for Universal Compute Platform)—This IP address is configured on Universal Compute Platform as part of your prerequisites for a Tunnel Concentrator installation. This IP address allows administrators to access the Universal Compute Platform user interface.
- Tunnel Concentrator Instances—The engine instance gets assigned automatically when you install the Tunnel Concentrator application.
- Tunnel Concentrator Licensing IPs—During Tunnel Concentrator installation, this address is configured as the **Assigned Virtual IP Address** and is required to license the application. After licensing is complete, you have the option to unconfigure this address and use ExtremeCloud IQ to access the Tunnel Concentrator user interface.
- GRE Termination Points (per instance)—Configure this address on ExtremeCloud IQ as part of the Tunnel Concentrator service configuration. Select the **Redundant Tunnel Concentrator** option and assign these addresses to the **IP Address** field for the **Primary Tunnel Concentrator** and **Backup Tunnel Concentrator** instances. The (primary) and (backup) designation in the table indicates whether the instance is configured as the primary or backup Tunnel Concentrator.

  Note
  For each service, assign one Tunnel Concentrator instance from each Universal Compute Platform server. With this example, you must configure three services, which reflects the three High Availability pairs.

- VRRP IPs— On ExtremeCloud IQ, during the Tunnel Concentrator service configuration, assign the VRRP IP address to the **Tunnel IP Address** field for the redundant High Availability pair.

Migrations from VGVA Tunneling to Tunnel Concentrator

To migrate from a VGVA identity-based traffic tunneling deployment that is managed by ExtremeCloud IQ to Tunnel Concentrator, complete either of the following procedures:

- Migrate to Tunnel Concentrator using a Network Policy on page 47
- Migrate to Tunnel Concentrator using Classification Rules on page 46

Note

- As a best practice, deploy a migration using a phased approach. Migrate a few sites to the new settings and run those sites for at least a few days to verify that everything works before you migrate other sites.
- Assign all configuration changes during a maintenance window so that your APs can reboot to the new configuration settings.

Migrate to Tunnel Concentrator using Classification Rules

Use this procedure to migrate a VGVA identity-based tunneling deployment that is managed by ExtremeCloud IQ to Tunnel Concentrator using classification rules. This migration method does not require a new Network Policy.

1. Configure classification rules for the Network Policy:
   a. Go to **Configure** > **Common Objects** > **Policy** > **Classification Rules**.
   b. Create two classification rules and configure classification categories for each that specify which APs and sites to migrate during phase 1 of the migration:
      - Rule 1 contains existing VGVA tunneling settings (for example, VGVA) and applies to the sites that remain under current settings for Phase 1.
      - Rule 2 contains Tunnel Concentrator settings (for example, Tunnel Concentrator) and applies to sites and APs that you want to migrate during Phase 1.
2. Clone the SSIDs that you want to migrate:
   a. Go to **Configure** > **Common Objects** > **Policy** > **SSID**.
   b. Select the SSID that the wireless network uses.
   c. Select (Clone) to create a new SSID based on the existing SSID settings.
   d. For the new SSID, assign a unique **SSID Name** and **Broadcast Name** as these fields must have unique names within a single Network Policy.
3. Clone the default User Profile that the SSID uses:
   a. Go to **Configure** > **Common Objects** > **Policy** > **User Profiles**.
   b. Select the default **User Profile** that your original SSID uses.
   c. Select (Clone) to create a new User Profile based on settings of the original profile.
   d. In the new **User Profile**, under **Traffic Tunneling**, select **Tunnel Concentrator**.
   e. For **Tunnel Destination**, select a Tunnel Concentrator.

      Note
      If you need to create the Tunnel Concentrator, select (+) and complete the configuration. For details, see Configure Tunnel Concentrator Services on page 38.

   f. Return to the SSID configuration for the SSID clone that you created in Step 2 and set the default **Default User Profile** to use the new User Profile clone that you just created.
4. Assign classification rules to the APs at your sites:
   a. Go to **Configure** > **Network Policy**.
   b. Select the existing Network Policy and then select **2 Wireless**.
   c. Make sure that the list of SSIDs includes both the existing and cloned SSIDs. If any SSIDs are missing, select (Select icon) and add them.
   d. For each SSID, select and assign the appropriate classification rule to the SSID:
      - Assign the VGVA rule to SSIDs that will remain on existing VGVA settings.
      - Assign the Tunnel Concentrator rule to SSIDs that will to move to Tunnel Concentrator.

5. Save all settings and push the new settings to the APs.

   Note

   - You should only push new settings to the APs during a maintenance window.
   - Run the new configuration for a few days to verify the new settings.

6. After the migration is verified, update the classification rule categories so that all sites and APs that you want to migrate use the Tunnel Concentrator rule and then push those settings to the APs.

Migrate to Tunnel Concentrator using a Network Policy

Use this procedure to migrate a VGVA identity-based tunneling deployment that is managed by ExtremeCloud IQ to Tunnel Concentrator by switching to a new Network Policy.

1. Login to ExtremeCloud IQ.
2. Clone the existing SSIDs that you want to migrate:
   a. Go to **Configure** > **Common Objects** > **Policy** > **SSIDs**.
   b. Select the SSID that the wireless network uses.
   c. Select (Clone) to create a new SSID based on the existing settings.
   d. For the new SSID, assign a unique **SSID Name** and **Broadcast Name** as these fields must have unique names within a single Network Policy.
3. Clone the default User Profile that the SSID uses:
   a. Go to **Configure** > **Common Objects** > **Policy** > **User Profiles** .
   b. Select the default **User Profile** that you your original SSID uses
   c. Select (Clone) to create a new profile based on existing settings.
   d. In the new User Profile, under **Traffic Tunneling**, select **Tunnel Concentrator**.
   e. For **Tunnel Destination**, select a Tunnel Concentrator.

      Note
      If you need to create the Tunnel Concentrator, select (+) and complete the configuration. For details, see Configure Tunnel Concentrator Services on page 38.

   f. Return to the SSID configuration for the new SSID clone and set **Default User Profile** to the new User Profile that you just created.
4. Configure a new Network Policy with the Tunnel Concentrator settings:
   a. Go to **Configure** > **Network Policy**.
   b. Select **Add Network Policy**.

c. Configure a new policy that includes the network settings that you want to assign to Tunnel Concentrator.
d. Under **2 Wireless**, add the SSID clones that you want to migrate to the new Network Policy.

Note
The original SSIDs should all be in your existing Network Policy.

5. For the sites that you want to use the Tunnel Concentrator settings, assign the APs at the site to use the new Network Policy.
6. Run the new configuration for a few days to verify the new settings. After the migration is verified, assign the new Network Policy to APs at the other sites.

Note
If you are using cloud PPSKs (private pre-shared keys), make sure that you are aware of how those PPSKs are used in the SSIDs that are included in your Network Policy, but which are not part of the migration. We recommend that you create unique PPSK SSIDs for each Network Policy and reuse existing User Groups as needed.

ExtremeCloud IQ Controller Configuration

If you are using ExtremeCloud IQ Controller as your management application, complete the following configuration tasks on the ExtremeCloud IQ Controller user interface to configure GRE tunneling with Tunnel Concentrator for specific VLANs on the WLAN network.

Note

Before you complete the following configuration tasks, complete the procedures in the Installation chapter to install Tunnel Concentrator instances on the Universal Compute Platform and then onboard those instances to the controller.

Table 16: ExtremeCloud IQ Controller Configuration

	Procedure	Description
1	Configure Tunnel Concentrator on page 50	Configure settings for Tunnel Concentrator instances that you've onboarded to the controller.
2	Configure a GRE Topology for a VLAN on page 50	Configure GRE tunneling for a given VLAN and assign Tunnel Concentrator instances to the VLAN.
3	Assign the GRE Topology to the WLAN on page 51	Assign the GRE topology as the default VLAN for the WLAN.
4	Assign the GRE Topology to the Access Point Profile on page 52	Make sure that the access point configuration profile includes the GRE topology.

Configure Tunnel Concentrator

Use this procedure on ExtremeCloud IQ Controller to configure settings for a Tunnel Concentrator instance that you onboarded to the controller.

1. Log in to ExtremeCloud IQ Controller.
2. Go to **Configure** > **Devices** > **Tunnel Concentrators**.
3. Select the Tunnel Concentrator instance whose **Name** matches the Serial Number (locking ID) of the instance that you installed and onboarded.
4. Select **Managed** and configure the following settings.
   Serial Number

   The Serial Number, or Locking ID of the Tunnel Concentrator instance.

   Name

   Set this field to the desired name for the Tunnel Concentrator instance. By default, the field is set to the Serial Number of the instance.

   Description

   Optional. Enter a text description of the instance.

   Secure Connection (IPSec)

   For added security, select this setting to apply a secure tunnel with encryption.
5. Under **GRE/IPSec tunnel termination point**, configure the following:
   Port

   Enter the data port of the listening interface on Tunnel Concentrator. If you are deploying LAG on this Tunnel Concentrator, you must select a LAG port.

   VLAN ID

   Specify the VLAN ID (or untagged) for the tunnel termination point of Tunnel Concentrator.

   IP Address

   The IP address of this Tunnel Concentrator instance. IPv6 is not supported.

   Gateway

   Optional. The IP address of the gateway.
6. Under **GRE/IPSec bridge interface**, select the port for the bridged interface. Optionally, if you are deploying LAG, this could be a LAG port.
7. Select **Save**.
8. Repeat this procedure if you have additional Tunnel Concentrator instances to configure.

Configure a GRE Topology for a VLAN

Configure a Generic Routing Encapsulation (GRE) tunnel topology for a given VLAN and assign Tunnel Concentrator instances to the VLAN.

1. Log in to ExtremeCloud IQ Controller.
2. Go to **Configure** > **Policy** > **VLAN**.
3. Configure the following parameters:
   VLAN Name

Name of the GRE VLAN

Mode

Select **GRE** for a Generic Routing Encapsulation (GRE) tunnel.

VLAN ID

The ID of the VLAN. This value must be unique.

Tagged

Specify if the egress port traffic is tagged or untagged. Most GRE VLAN topologies must be tagged. Each concentrator can support only one *untagged* topology. Select **Tagged** to tag the topology.

Tunnel Concentrators

List of Tunnel Concentrators.

Select a concentrator from the list, then select **Add**. You can add up to three concentrators to a single topology. When more than one termination point is added to the list, failover is supported.

The order of the termination points is significant. The primary concentrator must be the first termination point in the list. The AP issues a ping request to the first termination point. If that request fails, it pings the second point, and then the third point. With this organization, you can use the same three concentrators for multiple VLANs, and by varying the termination point order for each VLAN, you can balance the traffic load.

Note
It is a best practice to configure more than one Tunnel Concentrator per VLAN topology for failover. A topology that uses a single generic (non-encrypted) GRE tunnel, without configured backups, is not using the available mechanisms to detect if a Tunnel Concentrator is down. Therefore, no AP alarms, related to the tunnel connectivity, are generated for such a topology.

Load Balance

This checkbox is visible only when the list of concentrators has more than one element. Check **Load Balance** to load balance APs between concentrators.

4. Select **Save**.

Assign the GRE Topology to the WLAN

Assign the VLAN with the GRE topology as the default VLAN for the WLAN.

1. Log in to ExtremeCloud IQ Controller.
2. Go to **Configure** > **Networks** > **WLAN**.
3. Select the WLAN network.
4. Set the **Default VLAN** to the VLAN that you assigned to the GRE topology.
5. Select **Save**.

Assign the GRE Topology to the Access Point Profile

Make sure that the **Profile** that is assigned to the access point includes the VLAN with the GRE topology.

1. Log in to ExtremeCloud IQ Controller.
2. Go to **Devices** > **Access Points**.
3. Select the access point.
4. Select **Profile**.
5. Make sure that the VLAN with the GRE topology appears in the list and has the **Referenced** box selected.
6. If the VLAN with the GRE topology does not appear with the **Referenced** box selected, select the **Additional** box that is adjacent to the GRE topology and select **Save**.

Administration

Use the tasks in this section to administer, monitor, and debug Tunnel Concentrator.

Log in to Tunnel Concentrator

Use this procedure to log in to the Tunnel Concentrator user interface from the Universal Compute Platform host where the application is installed.

Note
If you deploy ExtremeCloud IQ as the management application, you can also open the Tunnel Concentrator user interface from ExtremeCloud IQ (the minimum release for this feature is 24.03). For more information, see Quick Add Tunnel Concentrators on page 37.

1. Log in to the Universal Compute Platform.
2. Go to **Engines** > **Installation**.
3. Under **Extreme Tunnel Concentrator**, select the applicable instance.

   The **Extreme Tunnel Concentrator** page of Universal Compute Platform opens. You can select from the following tabs:

Table 17: Tunnel Concentrator Maintenance Tabs on Universal Compute Platform

Tab	Description
Network Service Configuration	Use this tab to view the services that are running for this instance. You can assign an IP address to each service.
Statistics	Use this tab to access statistics for this instance of Tunnel Concentrator.

Table 17: Tunnel Concentrator Maintenance Tabs on Universal Compute Platform (continued)

Tab	Description
Logs	Use this tab to access logs for this instance of Tunnel Concentrator.
Console	Use this tab to access a console window that uses command line entries. You can use the console for initial configuration and for debugging purposes. • Select **Attach** to open the console window. • Select **Detach** to close the console window.

4. Select the **Instance Web Interface** link.
5. To log in to the interface, enter your admin **Username** and **Password** and then select **Authenticate**.

Note
To log out of Tunnel Concentrator, select your username in the top right of the header and then select **Logout**.

Tunnel Concentrator User Interface

Navigate the Tunnel Concentrator User Interface as displayed in Tunnel Concentrator User Interface on page 54. For descriptions of the callout items, refer to Tunnel Concentrator User Interface on page 54, which follows the image.

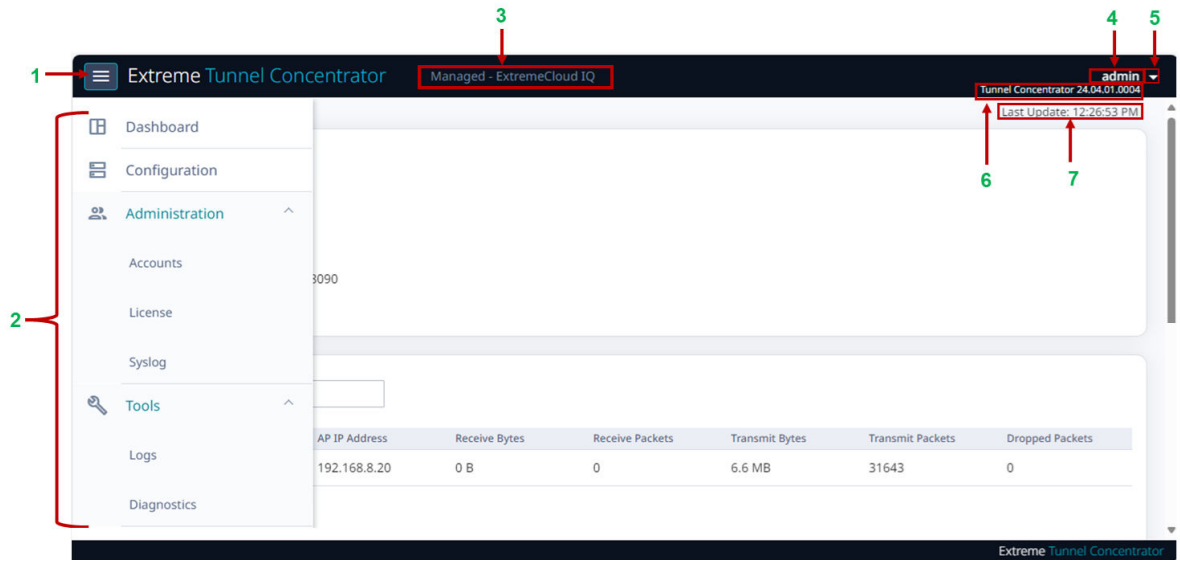


Figure 13: Tunnel Concentrator User Interface

Table 18: Tunnel Concentrator User Interface Callout Items

Callout	Description
1	—Select the navigation icon to open the navigation menu.
2	Navigation menu—Select one of the menu items to open the applicable configuration page.
3	Management mode—Displays the application that is selected currently as the management application for Tunnel Concentrator.
3	Username of the logged-in user.
5	—Select the user settings icon to view the user-specific menu options such as log out or change password.
6	Version—Displays the full Tunnel Concentrator version number with the build number appended.
7	Time of the last page refresh.

View Dashboards

Tunnel Concentrator contains a variety of dashboards and figures that help you maintain your system, such as the list of tunnels, transmit/receive statistics per tunnel, and information on the connection to the management application.

Note
Management application information is provided for ExtremeCloud IQ Controller only.

1. Log in to Tunnel Concentrator.
2. Go to **Dashboard**.

View Logs

Use the Tunnel Concentrator user interface on the Universal Compute Platform to view logs.

1. Log in to Tunnel Concentrator.
2. Go to **Tools** > **Logs**.
3. From the list of logs, select the log that you want to view.

Note
You can use the filtering options to filter the list by the Start and End dates of the log.

User Management

Add User

Use this procedure to add a new user account to Tunnel Concentrator.

1. Log in to Tunnel Concentrator.
2. Go to **Administration** > **Accounts**.
3. Select the (Add User) icon.
4. Complete the following fields:
   - **Username**—Enter the username for the new account.
   - **Sign On Type**—Select the account type: **Admin** or **Read Only**.
   - **Password**—Enter the password for this account.
   - **Confirm Password**—Re-enter the password.
5. Select **Create**.

Note
A **Read Only** user can log in to Tunnel Concentrator and view settings, but cannot make any edits.

Delete User

Use this procedure to delete an existing user from Tunnel Concentrator.

1. Log in to Tunnel Concentrator.
2. Go to **Administration** > **Accounts**
3. From the user list, select the user account that you want to delete.
4. Select the (Delete User) icon.
5. Select **Delete**.

Change a User Password (Administrators only)

Users with **Admin** privileges can use this procedure to change a Tunnel Concentrator login password on behalf of any user for whom their privileges provide access.

Note
If you do not have **Admin** privileges and want to change your own user password, see Change Your User Password on page 57.

1. Log in to Tunnel Concentrator.
2. Go to **Administration** > **Accounts**.
3. Select the user whose password you want to update. You can select yourself or any other user.
4. Select the (Update Password) icon.
5. Enter the new password.
6. Re-enter the new password.
7. Select **Save**.

Change Your User Password

Use this procedure to change your login password for the Tunnel Concentrator user interface.

Note
This procedure can be used by any user, including admin users and users with read only privileges.

1. Log in to the Tunnel Concentrator user interface.
2. Select (User Actions icon) from the top right of the header.
3. Select **Change Password**.
4. In the **Password** box, enter your new password.
5. In the **Confirm Password** box, re-enter your new password.
6. Select **Update**.

Configure Log Reporting

Use this procedure to configure settings for system log and syslog reporting on Tunnel Concentrator.

Note
For help with the fields and their settings, see Log Reporting Field Descriptions on page 58.

1. Log in to Tunnel Concentrator.
2. Go to **Administration** > **Syslog**.
3. Set the **System Log Level** to the desired severity threshold for system log messages.
4. Under **Syslog**, configure settings for syslog reporting:
   a. Set the **Application Facility** to the desired facility for syslog messages.

b. Under **Servers**, assign up to three syslog servers. For each server, assign the following fields:

- **Server**—Enter the IPv4 address of the syslog server.
- **Port**—Enter the port on the syslog server for log reporting. The default is 514.
- **Protocol**—Select UDP or TCP as the transport protocol for syslog reporting.
- **Level**—Set the desired severity threshold for message reporting to this syslog server.

5. Select **Save**.

Log Reporting Field Descriptions

Table 19: Log Reporting Field Descriptions

Field	Description
System Log Level	The system log covers local log reporting.
Log Level	The minimum severity level for the System Log. System messages that meet or exceed this severity level get reported in the System Log while messages that don't meet this severity level get ignored. The list of severity levels, in order of most severe to least severe are: • Critical • Major • Minor • Information • Debug
Syslog	Syslog reporting logs messages to a syslog server.
Application Facility	Set the facility code that gets used to label syslog messages. The range of values are from local0—local6.
Servers	You can assign up to three syslog servers.
Server	The IPv4 address of the syslog server.
Port	The port on the syslog server that is used for log reporting. The default is 514.
Protocol	The protocol for syslog reporting to this syslog server. The values are UDP (the default setting) or TCP.
Level	The minimum severity level for message logging to this syslog server. Syslog messages with a severity that meets or exceeds this level get logged whereas syslog messages with a severity that falls below this level do not get logged on this server. The list of severity levels, in order of most severe to least severe are: • Critical • Major • Minor • Information • Debug

Configure Packet Captures

From the **Diagnostics** menu, configure packet capturing on either the listening interface or bridge interface of Tunnel Concentrator.

1. Log in to Tunnel Concentrator.
2. Go to **Tools** > **Diagnostics**.
3. Under **Packet Capture**, select the Tunnel Concentrator interface on which you want to capture packets:
   - Listening
   - Bridging
4. Enter the **Filename** for the saved packet capture file.
5. Drag the scrollbar until you reach the desired maximum for the number of packets to capture.
6. To start the packet capture, select **START**.
7. To stop the packet capture, select **STOP**.

   Captured files display under **Capture Files**. To download a file capture, hover your cursor over a captured file and select the Download icon.

Ping a Node

Use this procedure to ping a node from the Tunnel Concentrator user interface.

1. Log in to Tunnel Concentrator.
2. Go to **Tools** > **Diagnostics**.
3. In the **Target IP or FQDN** box, enter the IP address or fully-qualified domain name of the node that you want to ping.
4. Select **PING**.

Upgrade Tunnel Concentrator

Use this procedure to upgrade a Tunnel Concentrator application instance from the Universal Compute Platform user interface. This procedure upgrades the application while retaining existing settings. There is no need to stop or uninstall the existing application instance.

Note
Download the new Tunnel Concentrator install image from the *Extreme Networks Support Portal* at `Downloads/ExtremeCloud/Extreme Tunnel Concentrator`.

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 adjacent check box and then select .

3. Upgrade the application:
   a. Go to **Engines** > **Installation**.
   b. Select the application instance that you want to upgrade.
   c. From the **Extreme Tunnel Concentrator** pane, select the application instance that you want to upgrade.
   d. Select **Upgrade application**.
   e. Select **OK**.

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