ExtremeCloud Tunnel Concentrator v25.05.01 Deployment Guide

Installation, Configuration, and Management

9039543-00 Rev. AA
April 2026

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/

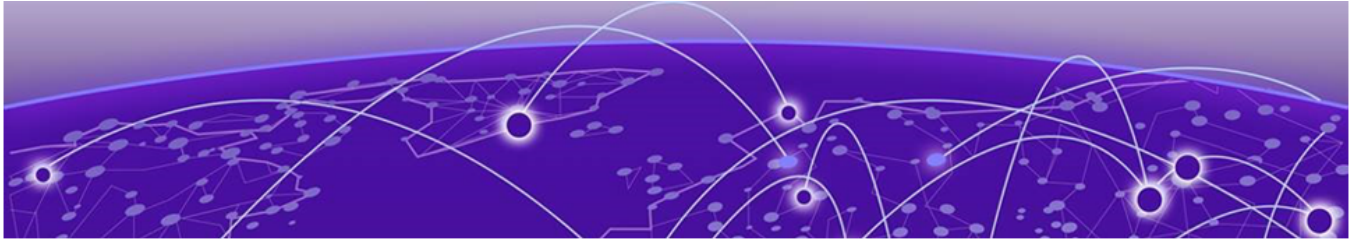


Table of Contents

Abstract v
How to Use This Guide vi
Preface vii
- Text Conventions vii
- Documentation and Training viii
  - Open Source Declarations ix
  - Training ix
- Help and Support ix
  - Subscribe to Product Announcements x
- Send Feedback x

Tunnel Concentrator Overview 11
- How Tunnel Concentrator Works 12
- Management Options for Provisioning 13
- Supported Products and Capacities 14
- Tunnel Concentrator Network Architecture 15
  - Management Layer Access 16
  - Data Layer 18
  - VRRP 19
- Redundancy Configuration 20
  - Redundancy with ExtremeCloud IQ 20
  - Redundancy with ExtremeCloud IQ Controller 22
- Deployment Considerations and Restrictions 23
- Broadcast and Multicast Controls 25
- ARP Proxy 25
- LAG Configuration Summary 26

Installation 28
- Installation Prerequisites 28
- Installation Task Flow 29
  - Install ExtremeCloud Edge-Self-Orchestration Deployment 30
  - Upload Tunnel Concentrator Image 32
  - Install Tunnel Concentrator 32
  - Change Default Admin Password 34
  - Generate the Activation License 35
  - Select the Management Option 35

ExtremeCloud IQ Configuration 37
- Quick Add Tunnel Concentrators 38
- Configure Tunnel Concentrator Service 39
  - Tunnel Concentrator Service Settings 40
- Configure Tunnel Policy 43
- Configure User Profile with Tunnel Concentrator 44

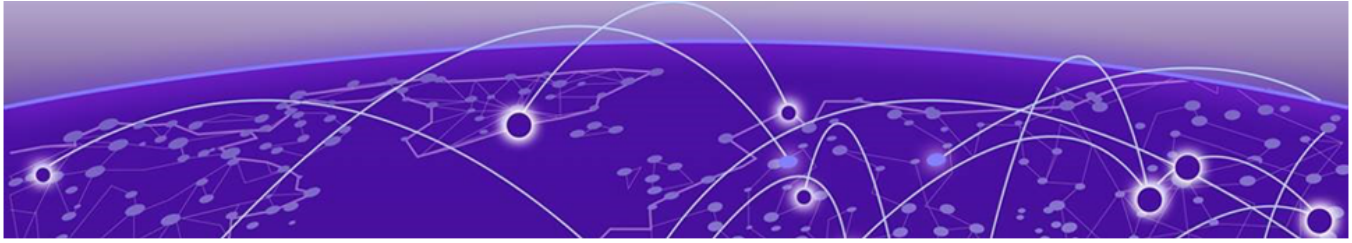
Configure SSIDs with Tunnel Concentrator User Profile....45
Deploy Network Policy....46
Additional Configurations....47
Edit Tunnel Concentrator Hostname....47
Migrations from VGVA Tunneling to Tunnel Concentrator....47

ExtremeCloud IQ Controller Configuration....51
Configure Tunnel Concentrator....52
Configure a GRE Topology for a VLAN....52
Assign the GRE Topology to the WLAN....54
Assign the GRE Topology to the Access Point Profile....54

Administration....56
Log in to Tunnel Concentrator....56
Tunnel Concentrator User Interface....57
User Management....58
Add User....59
Delete User....59
Change a User Password (Administrators only)....59
Change Your User Password....60
View Dashboards....60
View Logs....60
Configure Log Reporting....61
Log Reporting Field Descriptions....61
Configure Packet Captures....62
Ping a Node....62
Create Backup File....63
Upgrade Tunnel Concentrator....63

Appendix....65
Installation Example....65
ExtremeCloud IQ (Classic) Configuration Example (Alternative Flow)....68
Configuration Flow....69
Requirements and Assumptions....70
Configuration....70

Index....77



Abstract

The ExtremeCloud Tunnel Concentrator v25.05.01 Deployment Guide, issued in April 2026, provides comprehensive instructions for the installation, configuration, and management of the ExtremeCloud Tunnel Concentrator application on the Universal Compute Platform. This release introduces enhanced redundancy support for ExtremeCloud IQ-managed deployments with the ability to assign primary, secondary, and tertiary tunnels to a User Profile, along with the ability to configure keepalives for each Tunnel Concentrator service. In addition to updated procedures, the document also features a revised ExtremeCloud IQ configuration example. This 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.

How to Use This Guide

Follow the prescribed chapter order to plan, install, configure, and administer the ExtremeCloud Tunnel Concentrator application.

Table 1: ExtremeCloud Tunnel Concentrator Deployment Flow

	Chapter	Description
1	Tunnel Concentrator Overview on page 11	Review the overview information in this chapter to plan your deployment.
2	Installation on page 28	Use the procedures in this chapter to install and activate the Tunnel Concentrator application.
3	Select one of the following chapters: • ExtremeCloud IQ Configuration on page 37 • ExtremeCloud IQ Controller Configuration on page 51	After installation, provision tunneling using the chapter that applies to your management application.
4	Administration on page 56	Once everything is up and running, use this chapter to monitor and maintain your deployment on an ongoing basis.

Note
For installation and configuration examples, go to Appendix on page 65.

Preface

Read the following topics to learn about:

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

Text Conventions

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

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

Table 2: 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 3: 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 4: Command syntax

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

Documentation and Training

Find Extreme Networks product information at the following locations:

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

Open Source Declarations

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

Training

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

Help and Support

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

Extreme Portal

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

The Hub

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

Call GTAC

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

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

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

Subscribe to Product Announcements

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

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

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

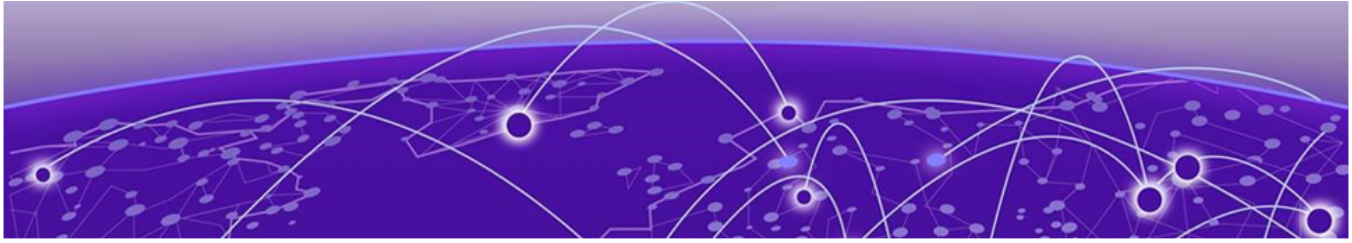
Send Feedback

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

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

To send feedback, email us at Product-Documentation@extremenetworks.com.

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



Tunnel Concentrator Overview

How Tunnel Concentrator Works on page 12
Management Options for Provisioning on page 13
Supported Products and Capacities on page 14
Tunnel Concentrator Network Architecture on page 15
Redundancy Configuration on page 20
Deployment Considerations and Restrictions on page 23
Broadcast and Multicast Controls on page 25
ARP Proxy on page 25
LAG Configuration Summary on page 26

ExtremeCloud Tunnel Concentrator enables the setup of traffic ingress/egress from wireless users at specific points in the network. Client traffic is exchanged between wireless access points and the Tunnel Concentrator instance via tunnels. For deployments that are managed by ExtremeCloud IQ, the tunneling supported is GRE (encapsulation). For deployments that are managed by ExtremeCloud IQ Controller, the tunneling is supported as IPsec.

ExtremeCloud Tunnel Concentrator is delivered as an ExtremeCloud Edge – Self Orchestrated application. Customers obtain the installation image (or updates) from the 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)
- 3150C - Medium (up to 5,000 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 **ExtremeCloud Tunnel Concentrator**, see Product Details.

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.

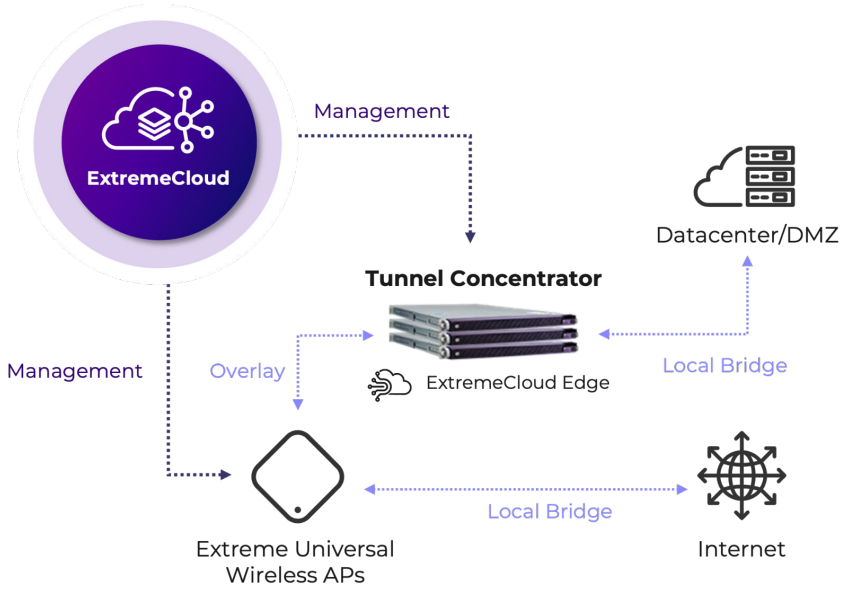


Figure 1: Tunnel Concentrator Deployment

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 (Classic) 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.

Note
Tunnel Concentrator supports ExtremeCloud IQ (Classic) and does not support ExtremeCloud IQ (New). All references in this guide to "ExtremeCloud IQ" mean "ExtremeCloud IQ (Classic)".

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 5: Supported Products and Versions

Solution Components	Supported Versions
Universal Compute Platform (1130C, 2130C, 3150C, or 4120C)	Universal Compute Platform v5.13.01 or later
ExtremeCloud IQ	ExtremeCloud IQ (Classic) v25.08 or later
ExtremeCloud IQ Controller	ExtremeCloud IQ Controller v10.18.01 or later
Access points	Tunnel Concentrator is supported on ExtremeCloud IQ (Classic). Universal access points and on IQ Engine access points. See ExtremeCloud IQ (Classic) 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 6: Supported Tunnel Concentrator Capacities per Universal Compute Platform Host

Installed on	Supported Capacities
1130C	• Single Tunnel Concentrator instance per appliance. • Maximum of 1,000 tunnels per Tunnel Concentrator instance.
2130C	• Single Tunnel Concentrator instance per appliance. • Maximum of 5,000 tunnels per Tunnel Concentrator instance.

Table 6: Supported Tunnel Concentrator Capacities per Universal Compute Platform Host (continued)

Installed on	Supported Capacities
3150C	• Single Tunnel Concentrator instance per appliance. • Maximum of 5,000 tunnels per Tunnel Concentrator instance.
4120C	• Up to three Tunnel Concentrator instances per appliance. • Maximum of 5,000 tunnels per Tunnel Concentrator instance. • Maximum of 15,000 tunnels per appliance.

Note
With ExtremeCloud IQ deployments, take the redundancy configuration into consideration when scaling your deployment. Note the following points:

- A single Tunnel Concentrator instance can handle up to its maximum capacity, irrespective of the number of user profiles that are configured to tunnel traffic to that instance.
- A redundant Tunnel Concentrator service in an HA pair configuration can handle the maximum capacity of the active instance. For example, if a single Tunnel Concentrator service includes an HA pair of instances that are both hosted on 2130Cs, the maximum capacity for that service is 5,000 tunnels.

Note
For ExtremeCloud IQ Controller deployments a Tunnel Concentrator instance can handle up to its maximum capacity, even if that instance is being used by multiple VLANs.

Tunnel Concentrator Network Architecture

The Tunnel Concentrator application consists of two distinct internal stacks or layers. Each stack has its own 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 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.

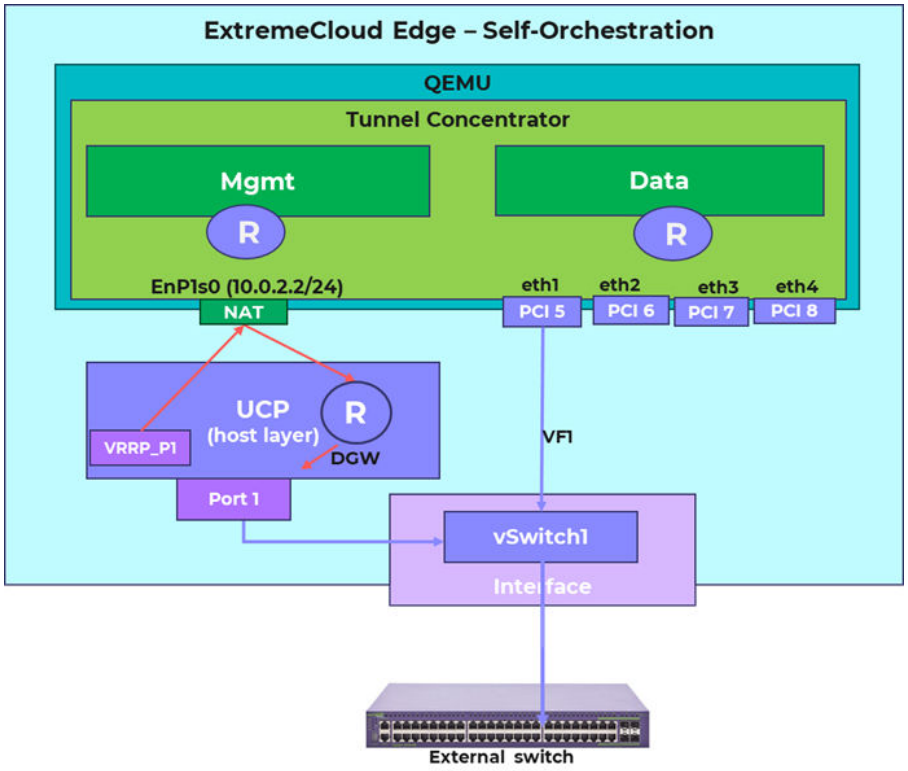


Figure 2: Tunnel Concentrator Internal Network Architecture

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 Inter-Cluster Connect (ICC) interfaces for network management is strongly discouraged. Although the ICC(s) can be seen as allowing for out-of-band physical management interface, they 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.

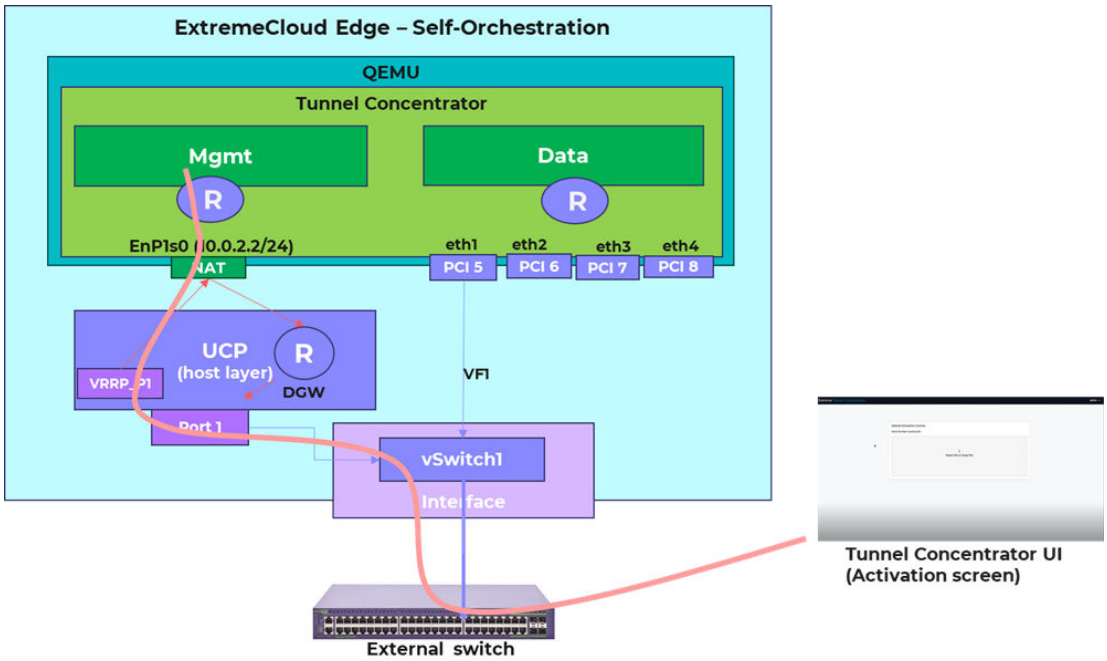


Figure 3: Management Access to User Interface

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.

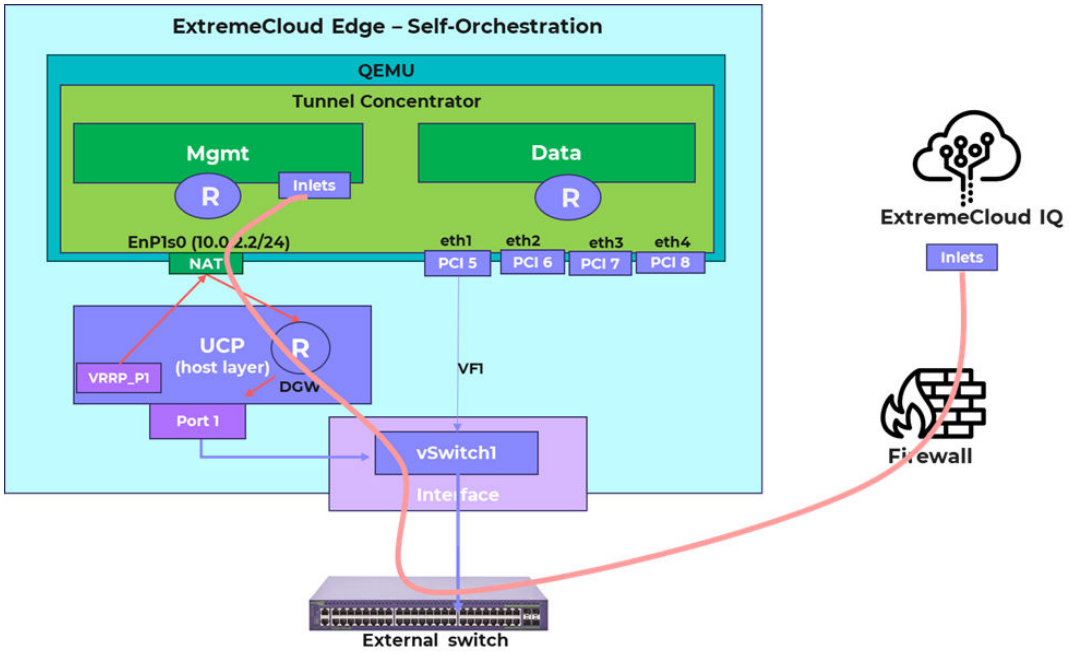


Figure 4: Management Stack to ExtremeCloud IQ using Inlets

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.

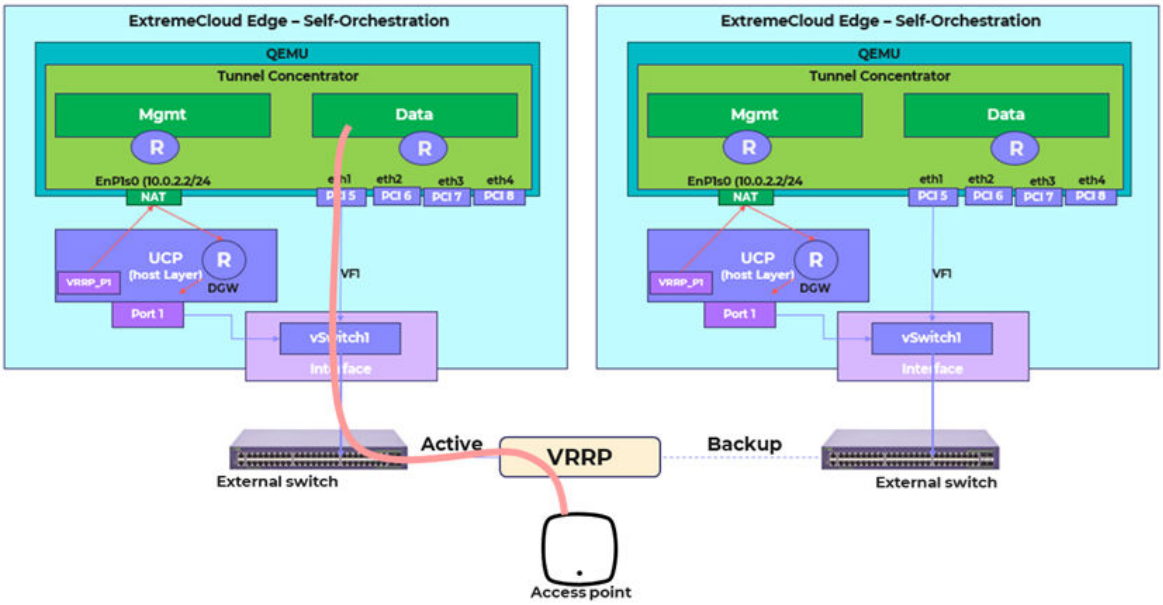


Figure 5: Data Flow from Access Point for HA Deployment

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:

Table 7: Summary of VRRP Configurations

VRRP Configured on...	Configuration Requirements
Data port of Universal Compute Platform host	This configuration can be used, irrespective of which management application you choose, or whether HA is deployed. The VRRP address provides access to the user interface, which can be used for initial activation. See Install ExtremeCloud Edge-Self-Orchestration Deployment on page 30.
Tunnel Concentrator Service of ExtremeCloud IQ	Required only if deploying redundant HA pairs when ExtremeCloud IQ is the management application. The VRRP address provides a single address that can be used to forward traffic to whichever Tunnel Concentrator instance is active. See Redundancy with ExtremeCloud IQ on page 20.

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.

Redundancy configuration and functionality depend on which management application you use. The subsequent sections describe the redundancy configurations for each deployment type.

Note
As a best practice, install redundant instances on different physical Universal Compute Platform boxes so that a server failure affects only a single instance.

Redundancy with ExtremeCloud IQ

Redundancy for Tunnel Concentrator deployments that are managed by ExtremeCloud IQ can be configured with the following two levels of redundancy, which can provide up to six Tunnel Concentrator instances for tunnel termination:

- Redundant tunnels (Primary, Secondary, Tertiary) where each tunnel points to a different Tunnel Concentrator service.
- Redundant HA pairs within a Tunnel Concentrator service.

The following image illustrates a redundant deployment where failovers have occurred at both levels of redundancy resulting in traffic being directed to the secondary tunnel's backup instance.

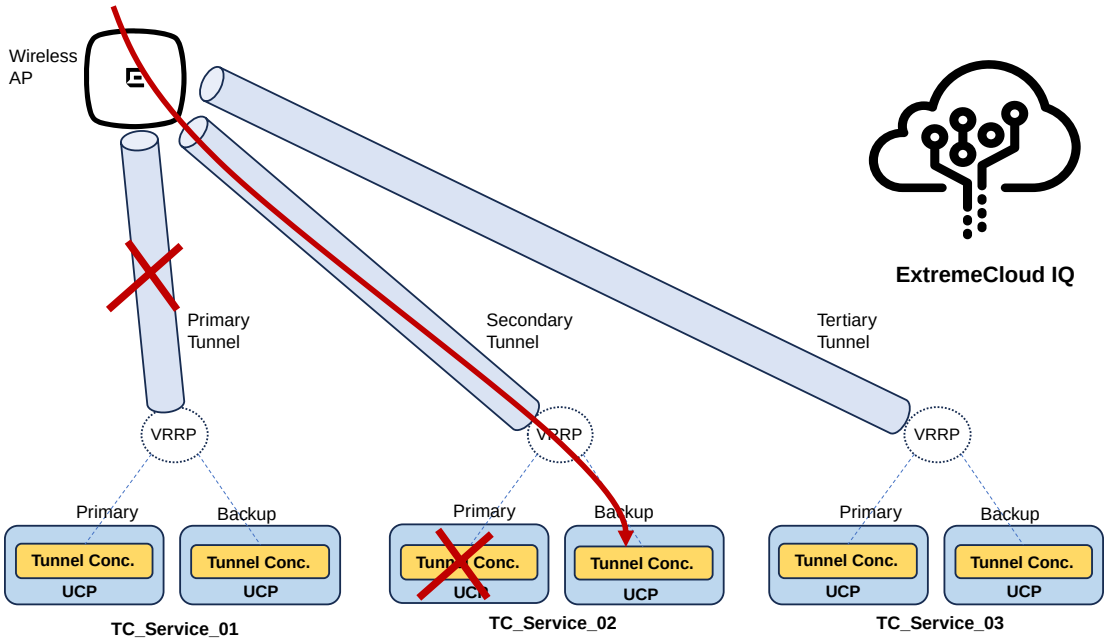


Figure 6: Redundancy for ExtremeCloud IQ Deployments

To assign **Primary**, **Secondary**, and **Tertiary** tunnel destinations, use the **User Profile** configuration on ExtremeCloud IQ. The following conditions apply:

- APs direct traffic to the highest priority tunnel destination that is currently active. The **Primary** tunnel has the highest priority ranking followed by the **Secondary** tunnel, and then the **Tertiary** tunnel.
- To detemine whether unused tunnels are active, APs use a keepalive process that involves sending a ping inside of each of the primary, secondary, and tertiary tunnels. The AP listens for responses from each tunnel to determine whether those tunnels are active or inactive. Keepalives are configured for each Tunnel Concentrator Service separately and there is no requirement that each service called by a single user profile use the same keepalive settings. See Configure Tunnel Concentrator Service on page 39 for more information.
- There is no requirement that the primary, secondary, and tertiary tunnel destinations within a user profile be on the same network segment or in the same data center. As a result, you can add geographic redundancy by pointing to Tunnel Concentrator services that are in geographically dispersed data centers.
- It is supported to have one tunnel destination that points to a redundant Tunnel Concentrator service while another tunnel destination in the same user profile points to a service that includes a single instance only.
- It is supported to use Tunnel Concentrator services that are installed on different hardware appliance models within the same user profile.
- It is supported to assign the same Tunnel Concentrator service to more than one user profile. For example, a service could be the primary tunnel destination in one profile, and the tertiary tunnel destination in a different profile.

To configure HA pairs within a single Tunnel Concentrator service, use the **Tunnel Concentrator Service** configuration on ExtremeCloud IQ. The following conditions apply:

- Both instances in a redundant service must be on the same network segment and in the same data center. L2 connectivity is required between each instance in the service.
- A VRRP address must be configured for the Tunnel Concentrator service if HA pairs are deployed within a the service. VRRP is not required if the service includes a single instance only.

Note
A VRRP address that provides a redundant Tunnel Concentrator service with high availability is different than the VRRP address that provides Tunnel Concentrator with its login address.

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.

Note
Each Tunnel Concentrator instance in the redundancy configuration must be on the same network segment and in the same data center.

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.

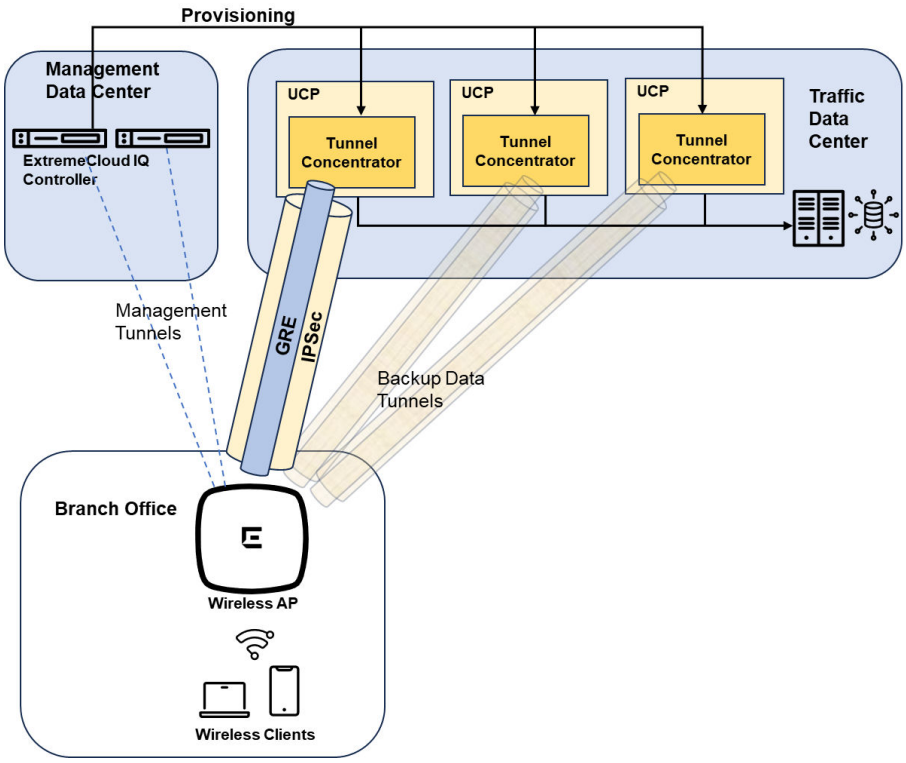


Figure 7: Redundancy Setup with ExtremeCloud IQ Controller

Deployment Considerations and Restrictions

Before deploying Tunnel Concentrator, consider the following:

- Tunnel Concentrator preserves DSCP markings for both upstream and downstream direction.
- By default, Tunnel Concentrator blocks non-essential broadcasts (everything except DHCP and ARP). When you disable this option, Tunnel Concentrator floods broadcasts to all APs.

  Note
  Use this setting with caution. Disabling this option may result in a significant amount of broadcast traffic being sent toward the APs.

- 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.

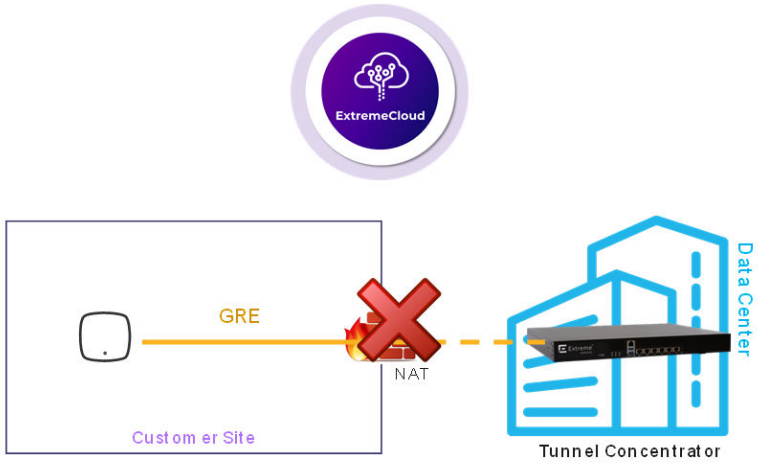


Figure 8: NAT Restriction with ExtremeCloud IQ as Management Application

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 recommend 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.

Broadcast and Multicast Controls

To help you manage the flow of traffic that crosses Tunnel Concentrator, configure settings that allow or deny specific broadcast and multicast traffic, thereby avoiding packet loss when traffic is at its peak. The following options are available:

- With broadcast traffic, you can configure Tunnel Concentrator to block non-essential broadcast traffic (this option is selected by default). When this option is selected, only ARP and DHCP broadcast traffic is forwarded. When this option is deselected, Tunnel Concentrator floods broadcast traffic to all APs.
- With multicast traffic, you can configure rules that allow multicasting for specific multicast addresses. You can assign multiple rules to a Tunnel Concentrator. Tunnel Concentrator forwards multicast traffic only if there is an assigned rule that allows the destination multicast address. Otherwise, Tunnel Concentrator blocks multicast packets.

To configure broadcast and multicast controls, use the following configurations:

- With ExtremeCloud IQ-managed deployments, configure broadcast and multicast control using the **Tunnel Concentrator Service** configuration on ExtremeCloud IQ.
- With ExtremeCloud IQ Controller-managed deployments, configure broadcast and multicast controls using **Advanced** settings for the **VLAN** with the GRE topology configuration that Tunnel Concentrator uses.

Note
The Broadcast and Multicast Controls configurations cover how Tunnel Concentrator handles broadcast and multicast traffic that attempts to crosses Tunnel Concentrator. Additional broadcast and multicast configurations that you apply throughout your network can impact the amount of broadcast and multicast traffic that attempts to cross Tunnel Concentrator.

ARP Proxy

Tunnel Concentrator supports ARP Proxy by default. Tunnel Concentrator stores its own local ARP lookup table and can proxy and respond to ARP requests. This feature is enabled by default. However, with ExtremeCloud IQ-managed deployments, you can disable the feature.

Note
Disabling ARP Proxy may cause ARP requests to flood to APs, resulting in significant ARP broadcast traffic. Use with caution.

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 8: 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 static LAG configuration matches the host's LAG configuration. **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 Service on page 39 For ExtremeCloud IQ Controller: Configure Tunnel Concentrator on page 52

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.

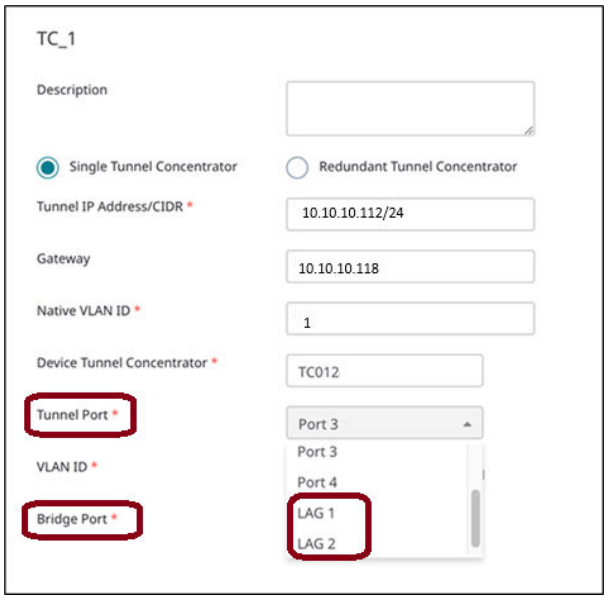
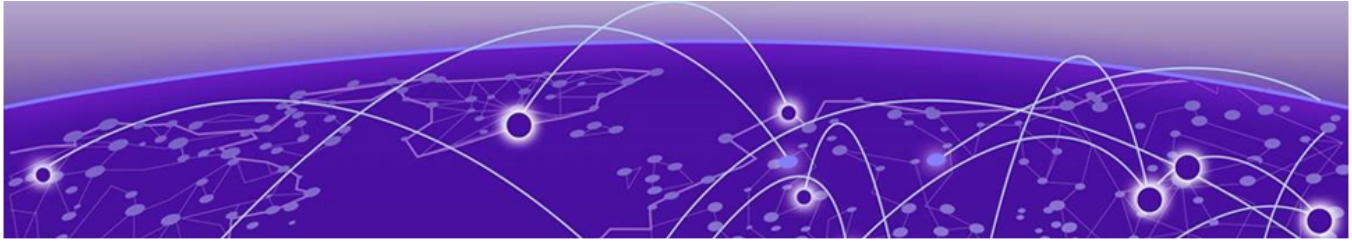


Figure 9: LAG Configuration for Tunnel Concentrator from ExtremeCloud IQ



Installation

Installation Prerequisites on page 28
Installation Task Flow on page 29

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 (Classic) 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 (Classic) 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.

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 9: 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	The Pod segment that you assigned on the host (the default range is 10.96.0.0/16)	This is the segment range for the Pod Network that was assigned on Universal Compute Platform during host cluster creation. Please review cluster configuration on host to confirm.

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 28 and make sure that you meet the full list of requirements for your deployment.

Table 10: Installation Task Flow

	Procedure	Description
1	Install ExtremeCloud Edge-Self-Orchestration Deployment on page 30	Install an ExtremeCloud Edge - Self-Orchestration deployment on Universal Compute Platform.
2	Upload Tunnel Concentrator Image on page 32	Upload Tunnel Concentrator image to Universal Compute Platform.
3	Install Tunnel Concentrator on page 32	Install the Tunnel Concentrator application on Universal Compute Platform.
4	Change Default Admin Password on page 34	As a best practice, change the default admin password immediately following the first login.
5	Generate the Activation License on page 35	Activate the license for your installation.
6	Select the Management Option on page 35	Select the management application for tunnel provisioning: • ExtremeCloud IQ • ExtremeCloud IQ Controller

Note
For an installation example with sample settings, see Installation Example on page 65.

Install ExtremeCloud Edge-Self-Orchestration Deployment

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

Make sure that your installation includes:

- VRRP configured on a data port (Required)—Configure a VRRP virtual IP address on one of the Universal Compute Platform data ports. The VRRP address provides Tunnel Concentrator with its login IP address and is required for initial Tunnel Concentrator activation. However, once the instance is onboarded to the cloud, the VRRP alias becomes optional.

For a full VRRP configuration, see the "Add a Port" procedure within the ExtremeCloud Edge - Self-Orchestration Deployment Guide.

Note

- For the VRRP address, use the data port that provides the best connectivity to the network. As a best practice, use the same segment that provides the default gateway for Universal Compute Platform.
- Make sure that the VRRP address does not overlap with existing addresses.
- If you are deploying multiple Tunnel Concentrator instances on a single host, you need separate VRRP addresses for each instance.

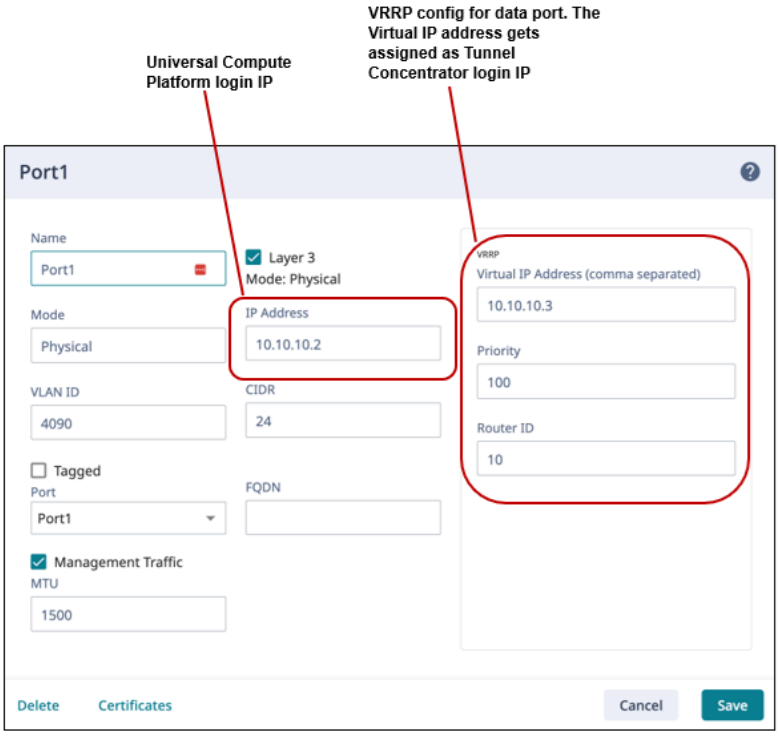


Figure 10: VRRP Configuration on Data Port of Universal Compute Platform

- ICC1 IP Address—Configure an ICC1 IP address, but leave ICC1 connectivity disabled. Make sure that the address does not overlap with existing routing domains. See Deployment Considerations and Restrictions on page 23 for more information.
- LAG (Optional)—If you want to deploy LAG ports on Tunnel Concentrator, configure LAG on Universal Compute Platform first. For more information, see LAG Configuration Summary on page 26.

Note

For a Tunnel Concentrator installation example that includes sample ExtremeCloud Edge settings, see Installation Example on page 65 .

Upload Tunnel Concentrator Image

Use this procedure to upload the Tunnel Concentrator application image to the Universal Compute Platform hardware appliance on which ExtremeCloud Edge is deployed.

Note

- The application image must have been downloaded from the portal. See Installation Prerequisites on page 28 for a complete list of requirements, including purchasing the SKU and obtaining the image.
- You only need to upload the image once per appliance. If the image was uploaded for a previous installation, you can skip this procedure.

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

   The **Image Management** page lists image files that are uploaded to the appliance. If the Tunnel Concentrator image appears, 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 a single instance of the Tunnel Concentrator application on the Universal Compute Platform host appliance.

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

Figure 11: Tunnel Concentrator Installation Pane

4. In the popup window, select **OK**.

   The engine installs. After the engine installs, a new Tunnel Concentrator instance displays in the **Extreme Tunnel Concentrator** pane.
5. Select the link for the new instance.
6. On the **Deploy Engine** page, 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, each port gets assigned the lowest unassigned VF on the internal virtual switch. 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.

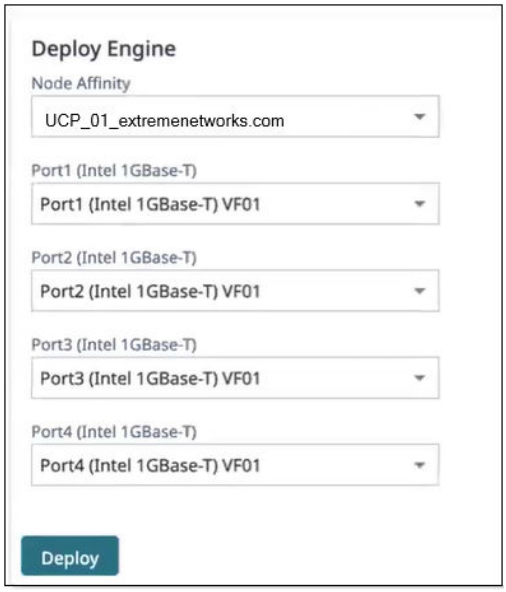


Figure 12: Deploy the Tunnel Concentrator Engine

7. Select **Deploy**.

   The application deploys. After a delay of up to a few minutes, the **Extreme Tunnel Concentrator** screen appears, displaying the following four tabs:
   - Network Service Configuration
   - Statistics
   - Logs
   - Console
8. Take a record of the instance Serial Number. You will need it later when you activate the instance.
9. Select the **Network Service Configuration** tab.

10. For **Assigned Virtual IP Address**, select a virtual IP address for the Tunnel Concentrator service.

    Note
    The **Assigned Virtual IP Address** field uses the VRRP virtual IP address that you assigned to the data port on Universal Compute Platform. This address provides Tunnel Concentrator with a login URL for the GUI.

11. Select **Save**.

    After a delay of up to a few minutes, the **Instance web interface** link gets added to the **Extreme Tunnel Concentrator** screen. For example, `https://10.10.10.2:5825`.

12. To lauch the Extreme Tunnel Concentrator management UI, select the **Instance web interface** link.

    The Tunnel Concentrator GUI login page displays.

13. 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 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.
2. 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 37
- ExtremeCloud IQ Controller Configuration on page 51

ExtremeCloud IQ Configuration

Quick Add Tunnel Concentrators on page 38
Configure Tunnel Concentrator Service on page 39
Configure Tunnel Policy on page 43
Configure User Profile with Tunnel Concentrator on page 44
Configure SSIDs with Tunnel Concentrator User Profile on page 45
Deploy Network Policy on page 46
Additional Configurations on page 47

If you selected ExtremeCloud IQ as your management application, complete the tasks in the following task flow on the ExtremeCloud IQ (Classic) interface to provision tunneling using Tunnel Concentrator.

Note
Tunnel Concentrator supports ExtremeCloud IQ (Classic) and does not support ExtremeCloud IQ (New). All references in this guide to "ExtremeCloud IQ" mean "ExtremeCloud IQ (Classic)".

Before you Begin

- Tunnel Concentrator(s) must be installed already with ExtremeCloud IQ selected as management entity. For details, see Installation on page 28.
- You must have a Network Policy and SSIDs configured on ExtremeCloud IQ already. For help with these configuration elements, see the *ExtremeCloud IQ (Classic) User Guide*.

Table 11: Tunnel Concentrator Task Flow from ExtremeCloud IQ

	Procedure	Description
1	Quick Add Tunnel Concentrators on page 38	Onboard your Tunnel Concentrators to ExtremeCloud IQ.
2	Configure Tunnel Concentrator Service on page 39	Configure a service that uses a single instance of Tunnel Concentrator or a redundant HA pair of instances.
3	Configure Tunnel Policy on page 43	(Optional) If you want Layer 2 roaming, configure a Tunnel Policy that points to your Tunnel Concentrator service.
4	Configure User Profile with Tunnel Concentrator on page 44	Assign the Tunnel Concentrator service(s) to a User Profile.

Table 11: Tunnel Concentrator Task Flow from ExtremeCloud IQ (continued)

	Procedure	Description
5	Configure SSIDs with Tunnel Concentrator User Profile on page 45	Assign your Tunnel Concentrator User Profile(s) to wireless SSIDs.
6	Deploy Network Policy on page 46	Complete a delta push to deploy the Network Policy to affected devices.

Note

- Each Tunnel Concentrator Service can reference up to two Tunnel Concentrator devices.
- 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.

Alternative Configuration Flow

If you don't want Layer 2 roaming, and aren't configuring a Tunnel Policy, you can use a streamlined configuration where you assign all settings from the Network Policy. See ExtremeCloud IQ (Classic) Configuration Example (Alternative Flow) on page 68 for a configuration example that uses this approach.

Quick Add Tunnel Concentrators

Use this task on the ExtremeCloud IQ (Classic) interface to quickly add Tunnel Concentrator instances to ExtremeCloud IQ and to 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.

Note
To open the Tunnel Concentrator application from ExtremeCloud IQ, select a Tunnel Concentrator from the **Devices** page to view the device details and go to one of the following locations:

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

Configure Tunnel Concentrator Service

Use this procedure to configure a Tunnel Concentrator Service that includes a single Tunnel Concentrator or a redundant HA pair of Tunnel Concentrators.

You can also configure optional broadcast and multicast controls to manage or restrict the volume of broadcast and multicast traffic that crosses Tunnel Concentrator.

Note
For detailed information on the following fields and their configuration options, see Tunnel Concentrator Service Settings on page 40.

1. On ExtremeCloud IQ (Classic), go to **Configure** > **Common Objects** > **Network** > **Tunnel Concentrator Service**.
2. Do either of the following:
   - Select an existing Tunnel Concentrator Service.
   - Select + (Add) to create a new Tunnel Concentrator Service.
3. Enter a **Name** for the service.
4. Select the type of service that you want to deploy:
   - **Single Tunnel Concentrator**—A service with a single instance.
   - **Redundant Tunnel Concentrator**—A service with a pair of instances in an HA configuration.
5. For **Tunnel IP Address/CIDR** enter the IP address and network mask that terminates the tunnel.
6. (Optional). For **Gateway**, enter the address of the default gateway.
7. (HA only). Enter the **VRRP Router ID**.
8. For **Native VLAN**, enter a VLAN ID.
9. Complete the following fields with details for each Tunnel Concentrator instance. If you are configuring HA, complete these fields separately for both instances:
   - **Device Tunnel Concentrator**—Select the Tunnel Concentrator device that you want to apply to this role.
   - **Tunnel Port**—Enter the port to be used for tunnel termination.
   - **VLAN ID**—Enter the VLAN ID for this instance.

- **IP Address** (HA only)—Enter the IP address of the tunnel termination point for this Tunnel Concentrator instance in the HA pair.
- **Bridge Port**—Select the bridge port for this instance.

10. Configure keepalive settings for this Tunnel Concentrator service:
    - **AP Keeplive Interval (seconds)**—Set the keepalive interval for the sending of keepalives to tunnels that aren't being used.
    - **AP Keepalive Retries**—Set the maximum number of times that the AP resends a failed keepalive before changing the tunnel status to **Inactive**.
11. (Optional). Expand **Broadcast/Multicast Control** to configure rules for broadcast and multicast traffic that crosses Tunnel Concentrator:
    a. Under **Permitted Multicast Rules**, configure rules that identify the multicast destination addresses that Tunnel Concentrator allows:
        - Select **Add New Rule** and then enter the IP address or network address that you want Tunnel Concentrator to allow for multicasting.
        - Select **Add Pre-defined Rule** and then select the system default rule that you want to assign to this Tunnel Concentrator service for multicasting.
    b. Select **Block Non-Essential Broadcast** if you want the service to block all broadcast traffic, except for DHCP and ARP. This is the default setting.
    c. Select **ARP Proxy** if you want Tunnel Concentrator to maintain an ARP table so that it can proxy and respond to ARP messages. This is the default setting.
12. Select **Save**.
13. Repeat this procedure if you want to configure additional Tunnel Concentrator services.

Tunnel Concentrator Service Settings

The following table describes the fields in the Tunnel Concentrator Service configuration. Note that each field is a required configuration, unless specified otherwise.

Table 12: Tunnel Concentrator Service

Field	Description
Name	Enter a name for the Tunnel Concentrator Service.
Description	(Optional) Enter a description for the Tunnel Concentrator Service.
Single Tunnel Concentrator Redundant Tunnel Concentrator	Select one of these options only: • Select **Single Tunnel Concentrator** if the service will use a single instance of Tunnel Concentrator. • Select **Redundant Tunnel Concentrator** if the service will use a pair of Tunnel Concentrator instances in an HA configuration.

Table 12: Tunnel Concentrator Service (continued)

Field	Description
Tunnel IP Address/ CIDR	Enter the IP address and network mask to which APs should direct tunneled traffic (for example, 10.10.10.3/24). Note that address functionality differs depending on whether or not you configured High Availability: • For a single Tunnel Concentrator service, this address is the tunnel termination point for this Tunnel Concentrator. • For a redundant Tunnel Concentrator service, this address is a VRRP address that is used by the service to provide High Availability. Tunneled traffic that arrives at this address is redirected to the IP address for the active Tunnel Concentrator in the pair.
Gateway	(Optional) Enter the address of the default gateway.
VRRP Router ID	(Redundant Tunnel Concentrator only) Enter 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	Enter the Native VLAN ID. This VLAN is untagged.
Note: The fields in the following section are relevant to a specific instance of Tunnel Concentrator. If you selected **Redundant Tunnel Concentrator Service**, these fields appear twice because the service includes a pair of instances. In this case, complete the fields separately with values that are relevant to each instance.	
Device Tunnel Concentrator	From the drop-down, select a specific Tunnel Concentrator device instance to assume this role in the service.
Tunnel Port	From the menu, select a port for the tunnel for this Tunnel Concentrator instance. If you are deploying LAG on this Tunnel Concentrator, select a LAG port.
VLAN ID	Select the tunneling VLAN ID for this Tunnel Concentrator instance. If the VLAN is untagged, select **Untagged**.
IP Address	(Redundant Tunnel Concentrator only) Enter an IP address to act as tunnel termination point for this instance in the HA pair. Data that goes from the AP to the Tunnel IP Address gets redirected to this IP Address when this Tunnel Concentrator is active.
Bridge Port	From the menu, select a bridge port for the tunnel for this Tunnel Concentrator instance. If you are deploying LAG on this Tunnel Concentrator instance, you may select a LAG port, although it's not mandatory.

Table 12: Tunnel Concentrator Service (continued)

Field	Description
AP Keepalive Interval (seconds)	This parameter specifies the interval that APs use for the sending of keepalives to Tunnel Concentrator. A keepalive consists of a ping that the AP sends inside a tunnel, after which the AP listens for a response. At each interval, the AP sends a keepalive down each tunnel that is not in use, and which leads to a Tunnel Concentrator service (primary, secondary, and tertiary tunnels). The AP listens for Tunnel Concentrator's response and tracks the results for each tunnel separately. • If the AP receives a response, the AP sets the tunnel status to **Active** and continues to send keepalives at scheduled intervals. • If the interval expires, and the AP has not received a response for a given tunnel, the AP sends another keepalive down that tunnel, but only changes the status to **Inactive** if the maximum number of keepalive retries for that tunnel has been met, as specified by the **AP Keepalive Retries** parameter. Possible values are 1-60 seconds. The default is 3 seconds. **Note:** APs send keepalives only to tunnels that are not in use. If the AP detects that the tunnel is in use, the AP sets the tunnel status to **Active**, but does not send a keepalive.
AP Keepalive Retries	This parameter specifies the maximum number of retry attemps for a failed keepalive before the AP changes the tunnel status to **Inactive**. A failed keepalive is a keepalive where the AP did not receive a response from Tunnel Concentrator within the allotted interval, as specified by **AP Keepalive Interval**. If a keepalive interval passes where the AP did not receive a keepalive response from a given tunnel: • If the number of previous keepalive retries for this tunnel is less than the value of **AP Keepalive Retries**, the AP retries the keepalive, but leaves the tunnel status unchanged. • If the number of previous keepalive retries for this tunnel matches the value of **AP Keepalive Retries**, the AP changes the tunnel status to **Inactive** and continues to send keepalives at regular intervals. Possible values are 1-10 retries. The default is 5 retries. **Note:** If an AP receives a keepalive response for an inactive tunnel, the AP changes the tunnel status to **Active** and continues to send keepalives at regular intervals. However, the number of previous keepalive retry attempts for this tunnel resets to 0.
Broadcast/Multicast Control	

Table 12: Tunnel Concentrator Service (continued)

Field	Description
Permitted Multicast IP Addresses	This section provides access rules for multicast packets that cross this Tunnel Concentrator serivce, based on the multicast address. The service allows multicast packets where the multicast destination is permitted by an assigned rule and discards multicast packets where none of the assigned rules permit multicast packets to that address. To add a multicast rule, select one of the following options: • **Add New Rule**—To assign an IP address or range of addreseses as allowed destination for multicast packets, select this option and then enter the IP address or network address. • **Add Pre-defined Rule**—To assign one of the preconfigured default rules to this Tunnel Concentrator service, select this option, and then select the rule. Within each rule, the **IP Address** field identifies either a specific IP address (e.g., 224.0.0.5) as a multicast destination, or a network address (e.g., 224.0.0.0/5) for a range of allowed addresses. If you enter a network address, Tunnel Concentrator allows multicast packets where the destination multicast address is encompassed by that range. To remove a rule, select the adjacent (Delete) icon.
Block Non-Essential Broadcast	When this setting is selected (the default setting), the Tunnel Concentrator service blocks broadcast traffic, except for ARP and DHCP traffic. When this setting is not selected, the Tunnel Concentrator service floods broadcast traffic to all APs.
ARP Proxy	When this setting is selected (the default setting), the Tunnel Concentrator service maintains an ARP table and can proxy and respond to ARP requests. When this setting is not selected, Tunnel Concentrator floods ARP requests to all APs.

When you have completed your configuration, select **Save**.

Configure Tunnel Policy

Use this optional procedure to configure a tunnel policy that points to your Tunnel Concentrator service(s). If you want Layer 2 roaming, you can use the policy to quickly provision Tunnel Concentrator across multiple user profiles in different SSIDs.

Note
The Tunnel Policy is not a mandatory configuration as you can assign a Tunnel Concentrator service to a user profile directly.

1. On ExtremeCloud IQ (Classic), go to **Configure** > **Common Objects** > **Network** > **Tunnel Policies**.
2. Do one of the following:
   - Select an existing tunnel policy.
   - Select + (Add) to create a new tunnel policy.
3. Enter a **Name** for the policy.
4. Select **Tunnel Concentrator**.

5. Assign one or more Tunnel Concentrator services to provide the tunnel destination for this profile:
   - **Primary** (Required)—Assign a service that will provide the primary tunnel destination for this profile.
   - **Secondary** (Optional)—Assign a different service as secondary tunnel.
   - **Tertiary** (Optional)—Assign a third service as tertiary tunnel.

   Note

   Optionally, you can select the + (Add) icon to open a Tunnel Concentrator service configuration window where you can configure a new service that gets applied to the corresponding tunnel destination for the tunnel policy.

6. Select **Save**.

Tip

Assign this Tunnel Policy configuration to one or more user profiles to use the Tunnel Destination settings from this configuration in those user profiles.

Configure User Profile with Tunnel Concentrator

Use this procedure to assign Tunnel Concentrator services to a user profile.

Note

This procedure provides two methods to assign Tunnel Concentrator settings. You must use one of these methods to assign a Tunnel Concentrator service to the profile:

- Apply an existing tunnel policy that has the Tunnel Concentrator settings that you want. The policy's Tunnel Concentrator settings get applied to the user profile automatically.
- Apply the Tunnel Concentrator service(s) to the user profile directly.

1. On ExtremeCloud IQ (Classic), go to **Configure** > **Common Objects** > **Policy** > **User Profiles**.
2. Do either of the following:
   - To edit an existing user profile, select the profile.
   - To configure a new user profile, select + (Add).
3. Enter a **User Profile Name** and enter the VLAN for this profile.
4. Select the **Traffic Tunneling** tab, and set **Traffic Tunneling (GRE)** to **ON**.
5. Optional. If you have an existing Tunnel Policy that contains your desired Tunnel Concentrator configuration, assign that policy to the user profile:
   a. Select **Re-use Tunnel Policy** .
   b. Select the applicable tunnel policy.
   c. Click **Select**.

      The Tunnel Concentrator settings from the tunnel policy get assigned to the user profile.

6. Otherwise, assign the Tunnel Concentrator settings to the user profile directly.
   a. Select **Tunnel Concentrator**.
   b. Assign one or more Tunnel Concentrator services to the following fields to act as tunnel destination for this profile:
      - **Primary** (Required)—Assign the service that will be the primary tunnel destination for this profile.
      - **Secondary** (Optional)—Assign a different service to provide tunneling if the primary tunnel fails.
      - **Tertiary** (Optional)—Assign a third service to provide tunneling if the primary and secondary tunnels fail.

      Note
      Optionally, you can select the + (Add) icon to open a Tunnel Concentrator Service configuration window where you can configure a new service that gets applied to the corresponding tunnel destination for the user profile.

7. Select **Save User Profile**.

   Note
   For detailed information on User Profile Configuration, see *ExtremeCloud IQ (Classic) User Guide*.

Configure SSIDs with Tunnel Concentrator User Profile

Use this procedure to assign a user profile that includes Tunnel Concentrator settings to the wireless SSIDs that will use those tunneling settings.

1. On ExtremeCloud IQ (Classic), go to **Configure** > **Network Policy**.
2. Select your network policy.
3. Select **2 Wireless**.
4. Select the SSID to which you want to apply the Tunnel Concentrator settings.
5. Assign the Tunnel Concentrator user profile to the SSID:
   - To assign the profile as default user profile for this SSID:
     a. Under **Default User Profile**, click (Select).
     b. Select the user profile that includes the Tunnel Concentrator settings.
     c. Click **Select User Profile** The user profile displays as **Default User Profile** for this SSID.
   - To assign the profile as a non-default user profile:
     a. Select **Apply a different user profile to various clients and user groups**.
     b. Select the subsequent (Select).
     c. Select the user profile with the Tunnel Concentrator settings. You can select multiple profiles.
     d. Click **Select**. The selected user profiles display in the SSID Configuration, but not as the default user profile.

6. If you assigned a non-default user profile, associate an assignment rule to the non-default profile that specifies when that user profile gets applied ahead of the default user profile. For example, a rule that specifies that the non-default user profile gets applied to devices with a specific OS type.
   - To associate an existing assignment rule, select (Select a user profile assignment rule), select the rule, and select **Link**.
   - To configure a new assignment rule, select (Add user profile assignment rule) and do the following:
     a. Enter a **Name** for the rule.
     b. To add conditions to a new rule, select + and select a **Category**. Assign category-specific conditions for that category. The categories that you can select from include:
        - Advanced Guest Policy
        - Client OS Type
        - Client MAC Address
        - Client Location
        - Schedule
        - Client Config Group
     c. Repeat the previous step if you want to add additional categories and qualifiers.
     d. Select **Save** to save the assignment rule.

   The assignment rule appears adjacent to the non-default user profile.

   Note
   For more information on assignment rules, see the *ExtremeCloud IQ (Classic) User Guide*.

7. Select **Save** to save SSID settings.
8. Repeat this procedure if you want to assign the Tunnel Concentrator user profile to additional SSIDs.

Deploy Network Policy

Use this procedure to deploy the updated Network Policy with the Tunnel Concentrator configuration to affected APs and Tunnel Concentrators.

1. On ExtremeCloud IQ (Classic), go to **Configure** > **Network Policies**.
2. Select the updated policy.
3. Select **6 Deploy**.
4. Select the devices that you want to update.

   Note
   Use the **Assigned**, **Eligible**, and **Filtered** controls to limit the display to specific devices only.

5. Select **Upload**.

6. In the **Device Update** window, select **Update Network Policy and Configuration** and select the **Delta Configuration Push** option.
7. Select **Perform Update**.

Note
For additional Network Policy deployment options, see the "Configure Network Policies" chapter of the *ExtremeCloud IQ (Classic) User Guide*.

Additional Configurations

Edit Tunnel Concentrator Hostname

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

1. On ExtremeCloud IQ (Classic), go to **Manage** > **Devices**.
2. From the devices list, select the host name of the applicable Tunnel Concentrator instance.

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

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 49
- Migrate to Tunnel Concentrator using Classification Rules on page 48

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. On ExtremeCloud IQ (Classic), 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 Service on page 39.

   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 migrate to Tunnel Concentrator.

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

   Note
   - Push new settings to the APs only 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. Clone the existing SSIDs that you want to migrate:
   a. On ExtremeCloud IQ (Classic), 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.
2. 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 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 Service on page 39.

   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.
3. 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.

4. For the sites that you want to use the Tunnel Concentrator settings, assign the APs at the site to use the new Network Policy.
5. 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
When using cloud PPSKs (private pre-shared keys), make sure that you are aware of how the PPSKs are used in your Network Policy. A best practice is to create unique PPSK SSID combinations in each network policy and to reuse the user groups as needed.

ExtremeCloud IQ Controller Configuration

Configure Tunnel Concentrator on page 52
Configure a GRE Topology for a VLAN on page 52
Assign the GRE Topology to the WLAN on page 54
Assign the GRE Topology to the Access Point Profile on page 54

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 13: ExtremeCloud IQ Controller Configuration

	Procedure	Description
1	Configure Tunnel Concentrator on page 52	Configure settings for Tunnel Concentrator instances that you've onboarded to the controller.
2	Configure a GRE Topology for a VLAN on page 52	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 54	Assign the GRE topology as the default VLAN for the WLAN.
4	Assign the GRE Topology to the Access Point Profile on page 54	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.

Optionally, you can assign rules that manage the volume of multicast and broadcast traffic that crosses Tunnel Concentrator. For example, you can limit multicast traffic to a defined set of multicast addresses and broadcast traffic to essential broadcasts only.

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. (Optional). To configure rules for broadcast and multicast traffic, select **Advanced** and configure the following:
   a. Select **Multicast Bridging** if you want to be able to forward multicasts between the wired and wireless sides of the AP.
   b. If you enabled multicast bridging and want to customize a multicast rule, select **Add New Rule** and configure the following:

      IP

      Enter the multicast IP address (e.g., 224.0.0.5) or network address (e.g., 224.0.0.0) that identifies a range of allowed multicast addresses.

      CIDR

      For a network address, enter the number of network bits (e.g., 27) to define the network and host portion of the allowed range. All multicast addresses that are encompassed by the range are allowed.

      Wireless Replication

      Select this option to allow wireless replication of multicast packets. By default, this field is selected.
   c. If you enabled multicast bridging and want to assign a system default multicast rule, select **Add Predefined Rule**, select the rule, and then select **Add**.
   d. Select **Block Non-Essential Broadcast Traffic** if you want Tunnel Concentrator to block all broadcast traffic, except for DHCP and ARP (this is the default setting). Otherwise, Tunnel Concentrator floods broadcast traffic to all APs.
   e. Select **Close**.
5. Select **Save**.

Assign the GRE Topology to the WLAN

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

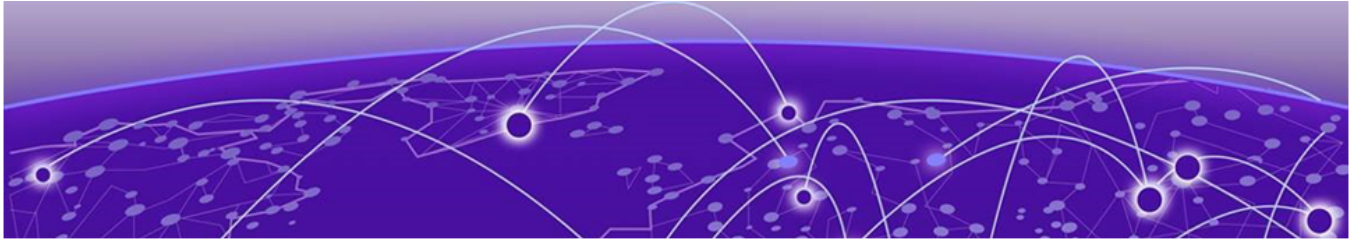
1. Log in to ExtremeCloud IQ Controller.
2. Go to **Configure** > **Networks** > **WLAN**.
3. Select the WLAN network.
4. Set the **Default VLAN** to the VLAN that you assigned to the GRE topology.
5. Select **Save**.

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

Log in to Tunnel Concentrator on page 56
Tunnel Concentrator User Interface on page 57
User Management on page 58
View Dashboards on page 60
View Logs on page 60
Configure Log Reporting on page 61
Configure Packet Captures on page 62
Ping a Node on page 62
Create Backup File on page 63
Upgrade Tunnel Concentrator on page 63

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 (Classic). The minimum release for this feature is 24.03.

From ExtremeCloud IQ (Classic), select a Tunnel Concentrator from the **Devices** page to view the device details and go to one of the following locations:

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

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 14: 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.
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

Figure 13 illustrates the Tunnel Concentrator User Interface. For a description of the various callouts, see Table 15, which follows the image.

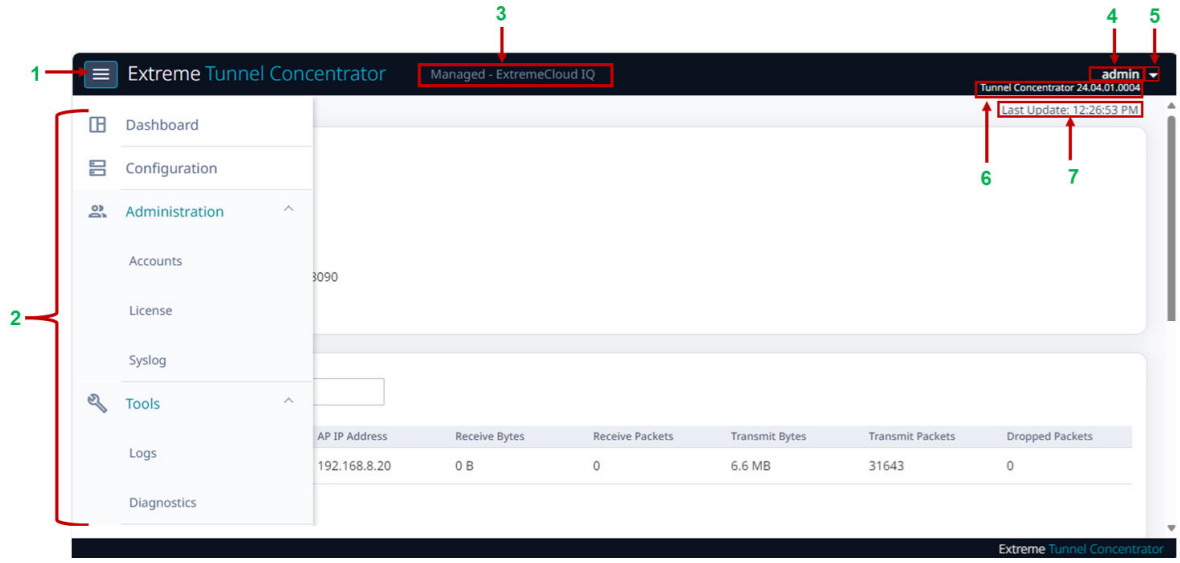


Figure 13: Tunnel Concentrator User Interface

Table 15: Tunnel Concentrator User Interface Callout Items

Callout	Description
1	(Navigation icon)—Select this 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.
4	Username of the logged-in user.
5	(User Actions)—Select this icon to view the user-specific menu options such as logout or change password.
6	Version—Displays the full Tunnel Concentrator version number with the build number appended.
7	Time of the last page refresh.

User Management

You can take the following actions to manage users:

- Add User
- Delete User
- Change a User Password (Administrators only)
- Change Your User Password

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 60.

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**.

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.

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 61.

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 16: 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.

Table 16: Log Reporting Field Descriptions (continued)

Field	Description
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 a packet captures that captures traffic on all active ports.

1. Log in to Tunnel Concentrator.
2. Go to **Tools** > **Diagnostics**.
3. Under **Packet Capture**, enter the **Filename** to use for saved the packet capture file.
4. Drag the scrollbar until you reach the desired maximum for the number of packets to capture.
5. To start the packet capture, select **START**.
6. 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.

Note
A TZSP header is added to the beginning of each frame in the capture file. Port and RX/TX information will be visible in the TZSP “Capture Location” tag.

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**.

Create Backup File

Use this procedure to create a backup file for this Tunnel Concentrator instance. You can save the backup file to a local file or save the file to a remote FTP or SCP server.

1. Log in to Tunnel Concentrator.
2. Go to **Administration** > **Maintenance**.
3. Select **Backup**.
4. For the **Destination**, select where you want to save the backup file:
   - **Download Locally**—Your backup file is saved to a file on the local drive.
   - **FTP Server**—Your backup file is saved to a remote FTP server.
   - **SCP Server**—Your backup file is saved to a remote SCP server.
5. For FTP or SCP backups, add the details of the remote server. This step is not required for local backups.
   - **Server IP**—Enter the IP address of the server where the file is to be saved.
   - **Username**—Enter the username of an account that has write access to the server.
   - **Password**—Enter the password that authenticates the user on that server.
   - **Directory**—Enter the directory where the backup file is to be saved.
   - **Filename**—Enter the filename that you want to use for the backup file.
6. Select **Generate backup / tech support** to begin the backup.

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. From the **Extreme Tunnel Concentrator** pane, select the application instance that you want to upgrade.
   c. Select **Upgrade application**.
   d. Select **OK**.

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

Appendix

Installation Example on page 65
ExtremeCloud IQ (Classic) Configuration Example (Alternative Flow) on page 68

Installation Example

This example provides sample settings for an installation of a single instance of Tunnel Concentrator on ExtremeCloud Edge.

The first three sets of settings are configured on Universal Compute Platform during ExtremeCloud Edge - Self-Orchestration configuration that prepares the host for Tunnel Concentrator. The remaining settings are part of the Tunnel Concentrator installation and engine deployment.

Note
This example provides sample settings, but not detailed procedures. For step-by-step procedures, see Installation Task Flow on page 29.

Basic Configuration Wizard (on Universal Compute Platform)

When you login to Universal Compute Platform for the first time, the Basic Configuration Wizard starts. Assign the following settings:

```
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=UCP_01
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
```

Standalone Cluster Creation (on Universal Compute Platform)

On the Universal Compute Platform GUI, go to **Cluster Settings** > **Cluster Configuration** and create the standalone cluster with the following settings:

- Deployment Type=ExtremeCloud Edge - 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

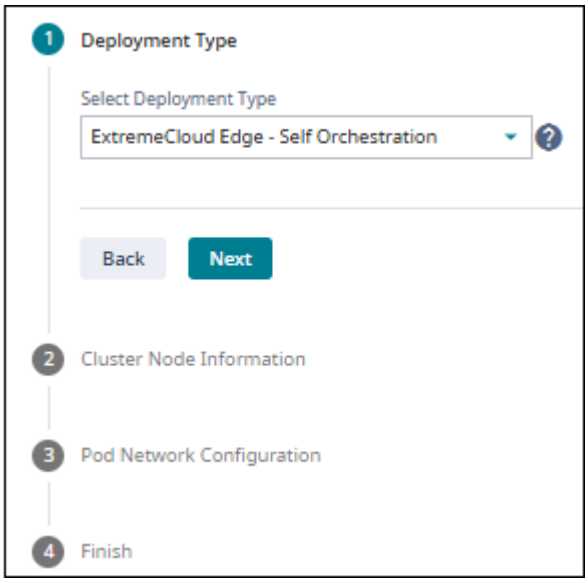


Figure 14: Cluster Configuration Wizard - Select the Deployment Type

VRRP Configuration (on Data Port of Universal Compute Platform)

After the cluster is created, go to **Administration** > **System** > **Network Setup** and configure VRRP on the data port that you configured using the wizard. Add the following VRRP settings to the existing port configuration:

- Virtual IP Address=10.10.10.2
- Priority=100
- Router ID=10

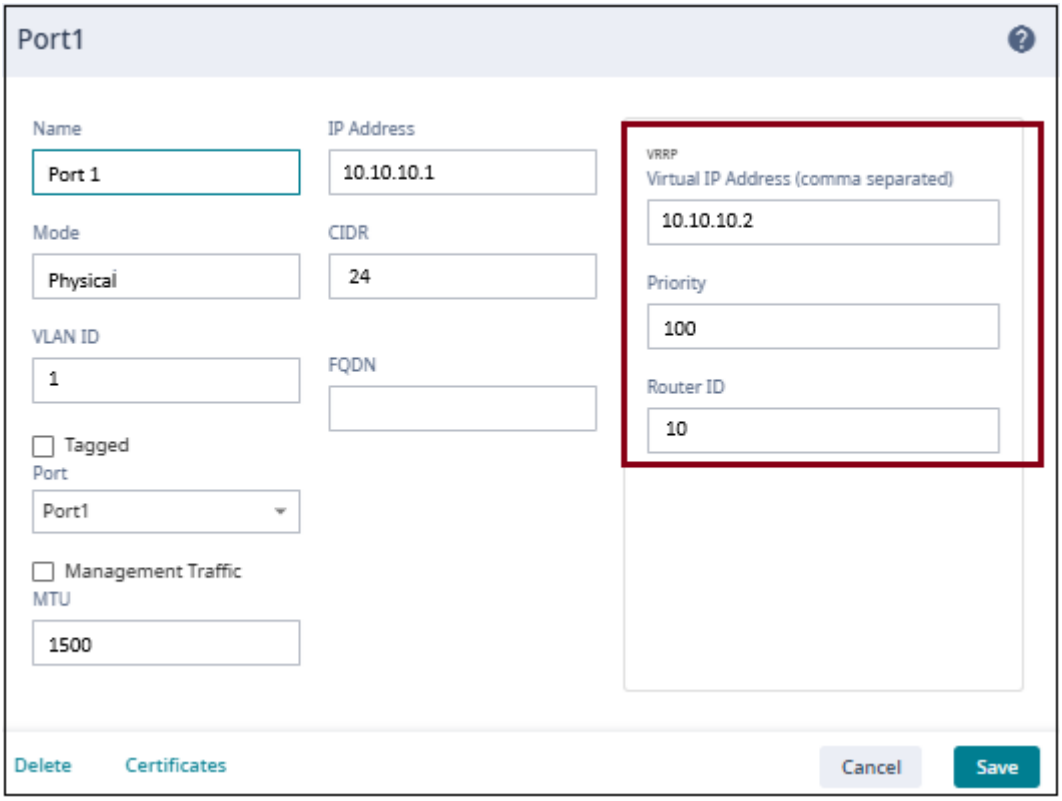


Figure 15: Configure VRRP on Data Port

Tunnel Concentrator Installation and Engine Deployment

On Universal Compute Platform, go to **Engines** > **Installation** and **Install** the Tunnel Concentrator application.

After installation, select the link for the freshly installed instance. On the **Deploy Engine** page, assign the following engine settings and deploy the engine:

- Node Affinity=UCP_01.extremenetworks.com
- Port1=Port1(Intel GBase-T) VF01
- Port2=Port2(Intel GBase-T) VF01
- Port3=Port3(Intel GBase-T) VF01
- Port4=Port4(Intel GBase-T) VF01

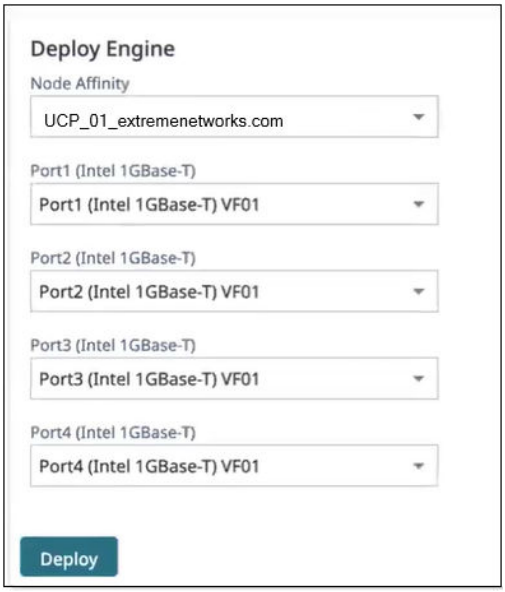


Figure 16: Deploy Tunnel Concentrator Engine

Assign a Virtual IP Address

Take a record of the serial number and then select the **Network Service Configuration** tab. Assign the VRRP address that you assigned in the port configuration to Tunnel Concentrator using the following setting:

- Assigned Virtual IP Address=10.10.10.2

Select the **Instance web interface** link (`https://10.10.10.2:5825`) to launch the Tunnel Concentrator GUI at the login screen.

ExtremeCloud IQ (Classic) Configuration Example (Alternative Flow)

The following image illustrates a sample topology for a redundant Tunnel Concentrator deployment where ExtremeCloud IQ (Classic) is the management application. This deployment includes redundant tunnels with each tunnel leading to a Tunnel Concentrator service that includes an HA pair of instances.

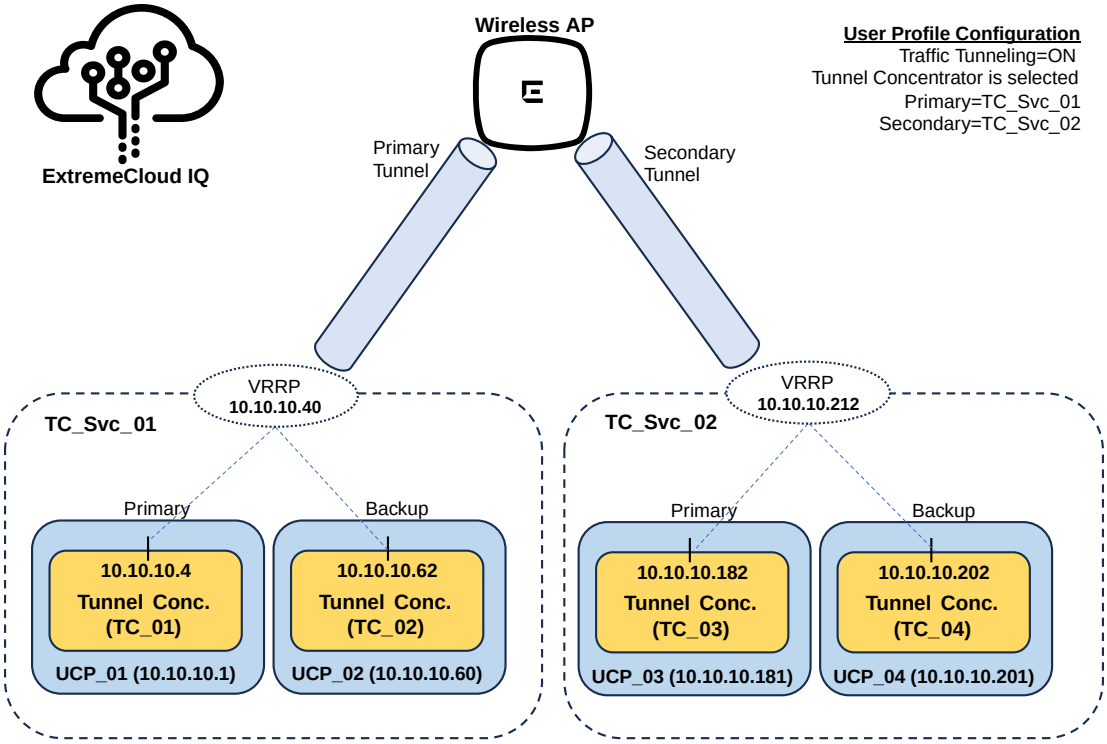


Figure 17: Redundant Tunnel Concentrator Configuration Example for ExtremeCloud IQ

Table 17: Address Settings and Where they are Assigned

Universal Compute Platform			ExtremeCloud IQ				
Hostname	IP Address	Tunnel Conc. Instance	Tunnel Conc Service	Tunnel IP Address (VRRP)	IP Address (tunnel termination)	Role in HA Pair (per instance)	Tunneling Role in User Profile (per service)
UCP_01	10.10.10.1	TC_01	TC_Svc_01	10.10.10.40	10.10.10.4	Primary	Primary
UCP_02	10.10.10.60	TC_02			10.10.10.62	Backup	
UCP_03	10.10.10.181	TC_03	TC_Svc_02	10.10.10.212	10.10.10.182	Primary	Secondary
UCP_04	10.10.10.201	TC_04			10.10.10.202	Backup	

Configuration Flow

This example uses an alternative configuration flow that differs from the configuration that is presented in the *ExtremeCloud IQ (Classic) Configuration* chapter. Because the configuration example does not use Layer 2 roaming or a tunnel policy, you can complete the configuration from the network policy by drilling down into multiple configuration layers, assigning settings, and then reversing out, while saving the configuration in the reverse order from which it was applied.

The following image illustrates the configuration flow for this example.

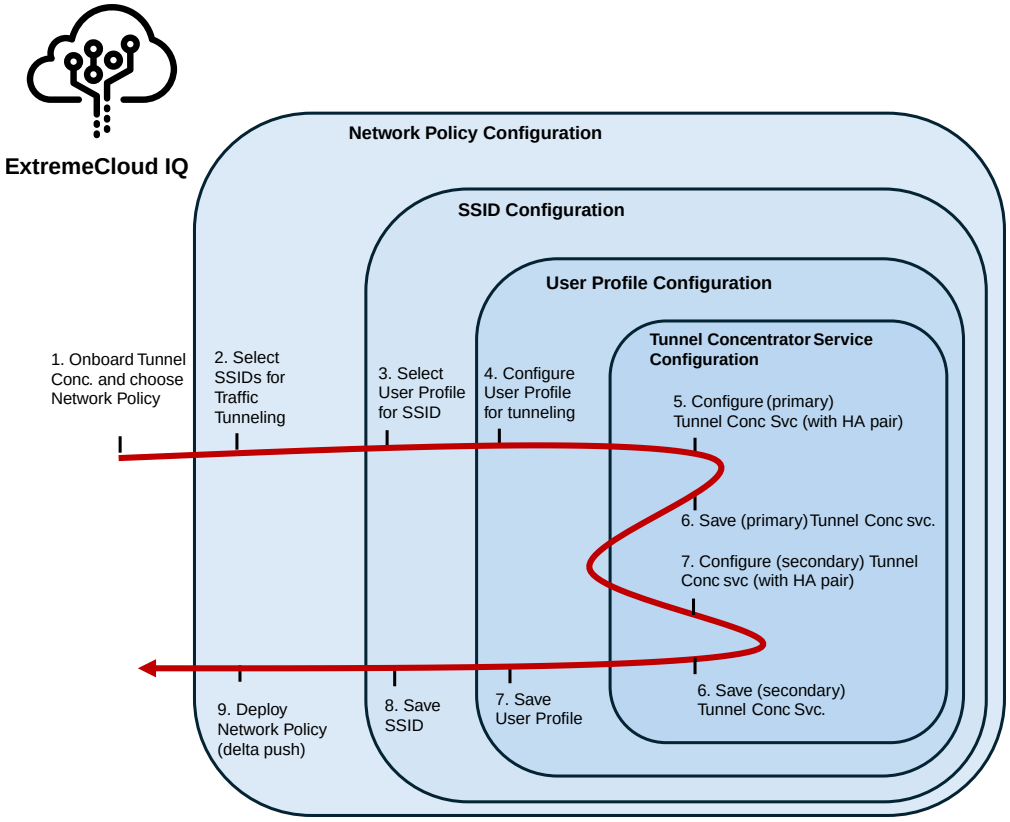


Figure 18: Tunnel Concentrator Configuration using Network Policy (ExtremeCloud IQ)

Requirements and Assumptions

Before you start configuration, note the following:

- You require four new Tunnel Concentrator installations that are installed on different appliances, but which are not onboarded to ExtremeCloud IQ. For this example, assume that the four Serial Numbers are: `TC_01`, `TC_02`, `TC_03`, and `TC_04`.
- You require existing Network Policy and SSID configurations in place on ExtremeCloud IQ so that you can add Tunnel Concentrator settings to these configuration elements. This example uses `Sample_Network` and `Sample_SSID` as the existing configurations.
- The example assumes that you want to configure a new user profile and a new Tunnel Concentrator service. However, you have the option to edit existing configurations.
- The example assumes that you are not using a tunnel policy and are not configuring Layer 2 roaming.

Configuration

The configuration consists of two main stages:

- Tunnel Concentrator onboarding to ExtremeCloud IQ

- Network Policy configuration and deployment

Tunnel Concentrator Onboarding to ExtremeCloud IQ

Use the Quick Add Devices option to onboard all Tunnel Concentrator installations to ExtremeCloud IQ using the Serial Numbers.

1. On ExtremeCloud IQ (Classic), go to **Manage** > **Devices**.
2. Select + (Add) and then **Quick Add Devices** > **Manage Devices from Cloud**.
3. In the **Serial Number** field, enter each Tunnel Concentrator serial number, separated by a comma.

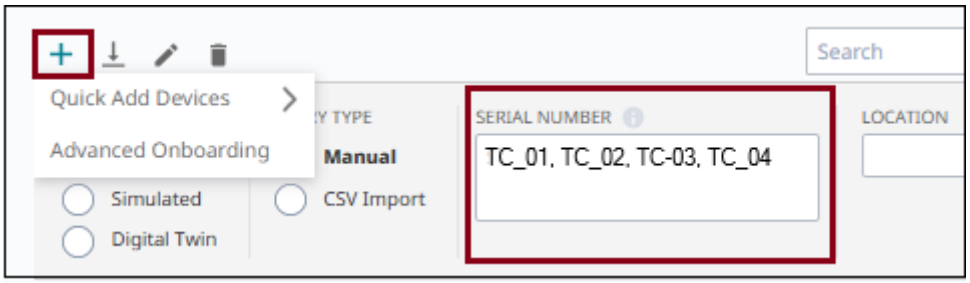


Figure 19: Quick Add Tunnel Concentrators to ExtremeCloud IQ

4. From the **Policy** drop-down, select the network policy.
5. Select **Add Devices**.

   Each device gets onboarded to ExtremeCloud IQ, and gets assigned to your network policy.

Network Policy Configuration and Deployment

The remaining configuration can be completed from the Network Policy configuration.

1. Go to **Configure** > **Network Policies** and select your network policy. For example, `Sample_Network`.

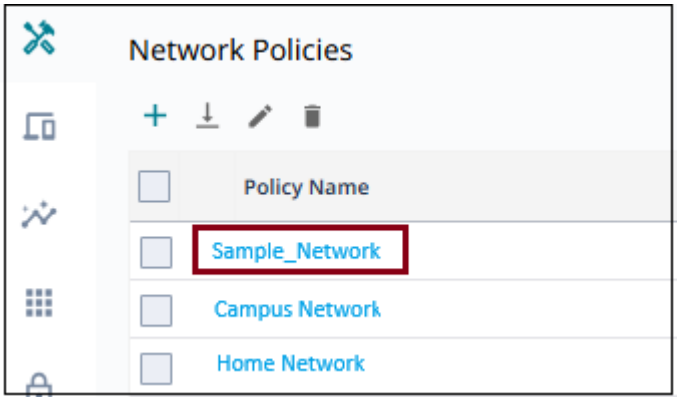


Figure 20: Select your Network Policy

2. Select **2 Wireless**.

3. Select the SSID to which you want to apply Tunnel Concentrator settings. For example, `Sample_SSID`.

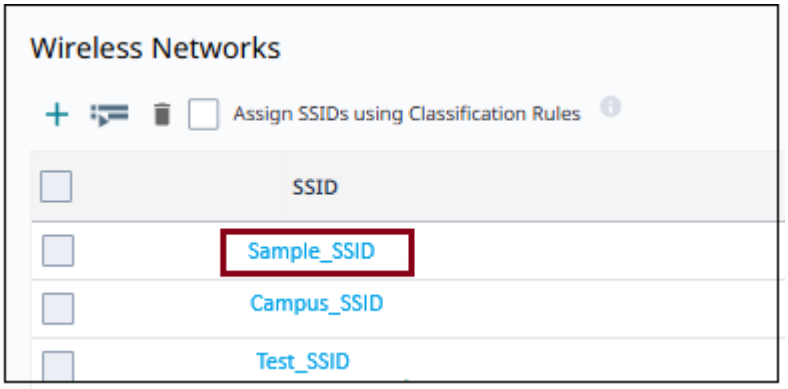


Figure 21: Select the SSID that will use Tunnel Concentrator

4. Under **User Access Settings**, and for the **Default User Profile**, select the adjacent + to create a new default user profile to hold the Tunnel Concentrator settings.

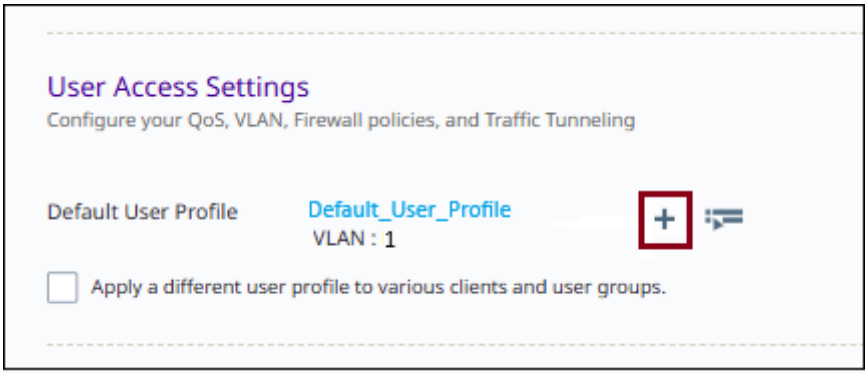


Figure 22: Assign Default User Profile to SSID

Note

- In this example, you are creating a new user profile. However, you can also select and edit an existing profile.
- To assign your user profile as non-default profile, select **Apply a different user profile to various clients and groups**, then select or create the user profile. Next, configure assignment rules to determine when the non-default profile gets applied instead of the default profile

5. For the newly created user profile, configure the following settings.
   a. Enter a **Name** for the new profile. For example, `Sample_User_Profile`.
   b. For **Connect to**, select **VLAN** and assign a VLAN ID. For example, `1530`.

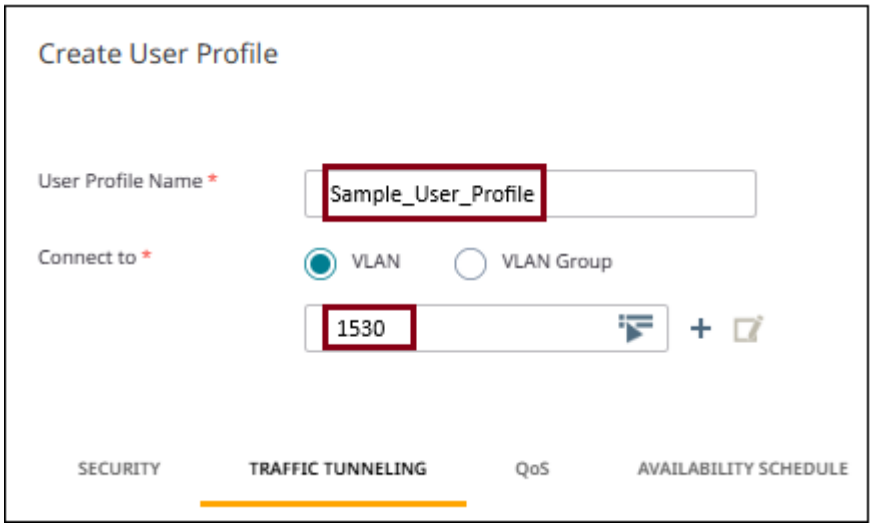


Figure 23: Create a New User Profile

c. Select the **Traffic Tunneling** tab and toggle **Traffic Tunneling (GRE)** to **ON**.

> **Note**
> If you have an existing tunnel policy that points to a Tunnel Concentrator service, you can reuse that policy's Tunnel Concentrator settings in the user profile. Select **Re-use Tunnel Policy** and select the policy. The Tunnel Concentrator service from the policy gets assigned as **Tunnel Destination** in the user profile.

d. Select **Tunnel Concentrator** and then configure the tunnel destination with primary and secondary tunnels.

   i. For **Primary**, select the adjacent + to create a new Tunnel Concentrator service to act as primary tunnel destination for this profile.

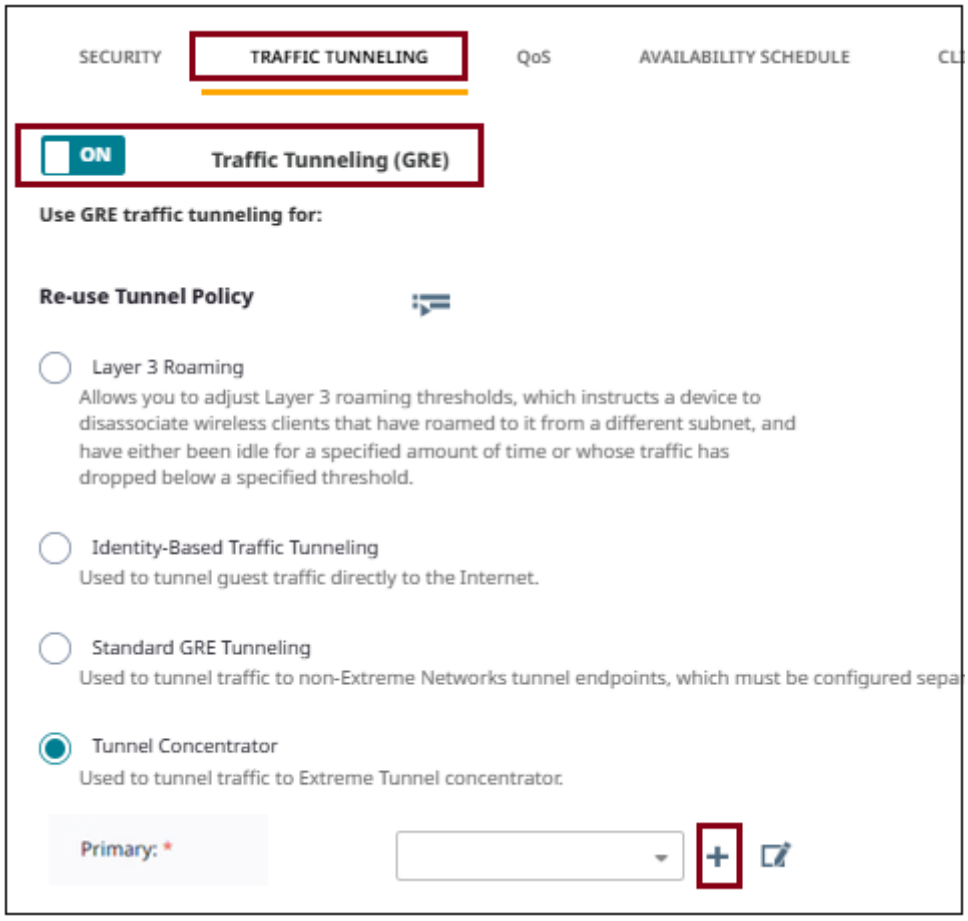


Figure 24: Assign Tunneling to New User Profile

ii. In the **New Tunnel Concentrator Service** window, assign the following settings:

For Tunnel Concentrator Service:

- Name=TC_Svc_01
- Redundant Tunnel Concentrator
- Tunnel IP Address/CIDR=10.10.10.40/24
- VRRP Router ID=1
- Native VLAN ID=1530

For Primary Tunnel Concentrator:

- Device Tunnel Concentrator=TC_01
- Tunnel Port=Port 1
- VLAN ID= 15
- IP Address=10.10.10.4
- Bridge Port=Port 3

For Backup Tunnel Concentrator:

- Device Tunnel Concentrator=TC_02
- Tunnel Port=Port 1
- VLAN ID=15
- IP Address=10.10.10.62
- Bridge Port=Port 3

Leave the keepalive settings at their default values.

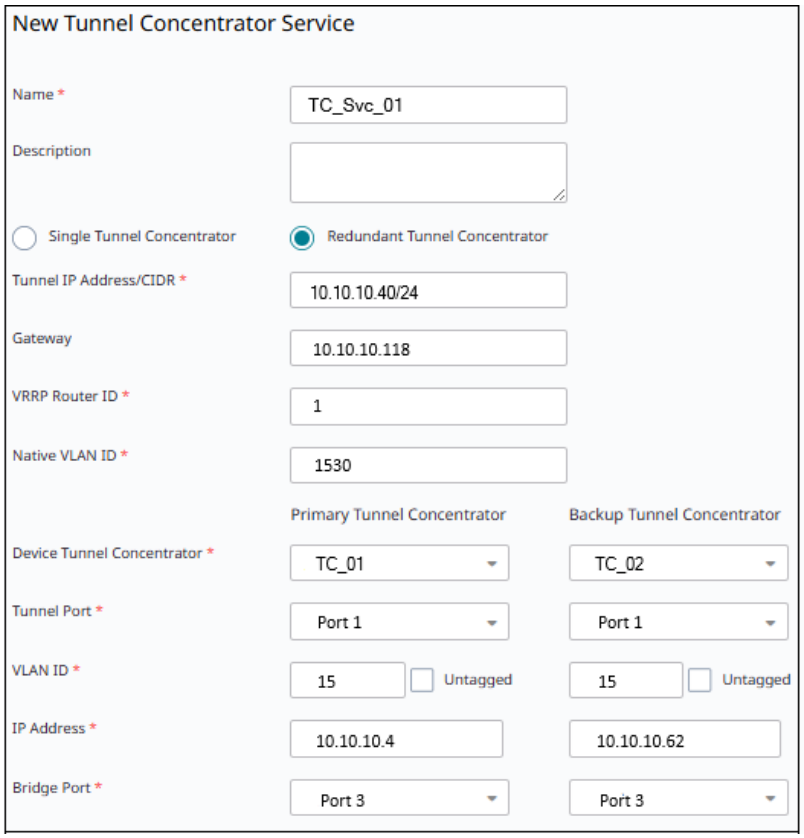


Figure 25: Configure New Redundant Tunnel Concentrator Service

iii. Select **Save** to save the new Tunnel Concentrator service.

The new Tunnel Concentrator service displays as **Primary** tunnel destination within the User Profile configuration.

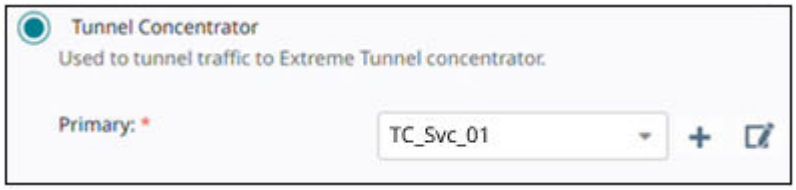


Figure 26: New Tunnel Destination for User Profile

iv. For **Secondary**, select the adjacent + and create the secondary Tunnel Concentrator service using the TC_03 and TC_04 instances and the addressing from Figure 17 on page 69.

e. Once the Primary and Secondary tunnel destinations are assigned, select **Save User Profile**.

The new user profile with the Tunnel Concentrator settings displays as **Default User Profile** within the SSID configuration. The VLAN from the user profile is default VLAN for the SSID.

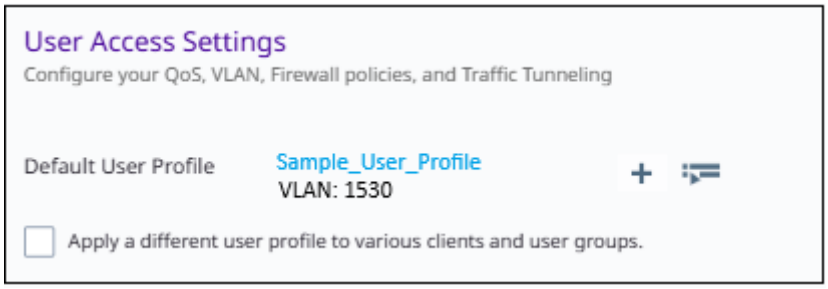
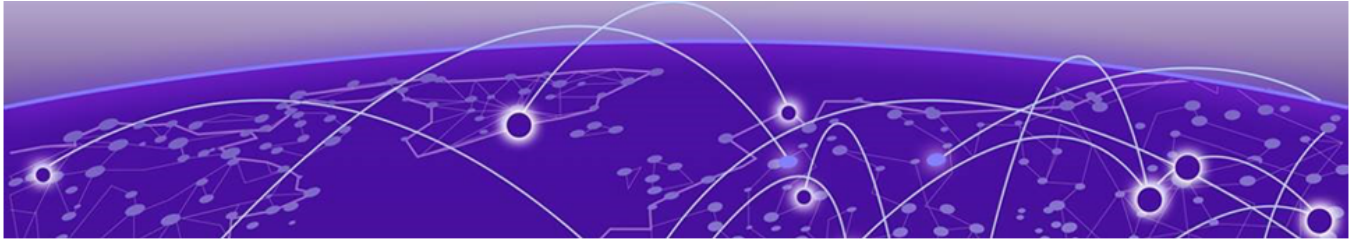


Figure 27: New Default User Profile for SSID

6. Select **Save** to save the SSID configuration.
7. Deploy the network policy to affected APs and Tunnel Concentrators using a delta push.



Index

A

about Tunnel Concentrator 11
add user 59
admin password
    change 34
administration 56
announcements ix, x
arp proxy
    configure 39
    disable on ExtremeCloud IQ 40
    overview 25
assign GRE topology to WLAN using ExtremeCloud IQ Controller 54

B

backup
    create backup file 63
benefits of Tunnel Concentrator 11
broadcast and multicast control
    on ExtremeCloud IQ 39
broadcast controls on Tunnel Concentrator 25
broadcast traffic
    how tunnel concentrator handles 23

C

configure
    assignment rules that specify which user profile gets used 45
    broadcast and multicast control on ExtremeCloud IQ 39
    GRE topology for a VLAN in ExtremeCloud IQ Controller 52
    log reporting 61
    packet captures 62
    secure tunnel in ExtremeCloud IQ Controller 52
    SSIDs with Tunnel Concentrator user profile 45
    Tunnel Concentrator in ExtremeCloud IQ Controller 52
    Tunnel Concentrator Services on ExtremeCloud IQ 39
    tunnel policy 43
    User Profile for Tunnel Concentrator 44
conventions
    notice icons vii
    text vii
create backup file 63

D

dashboards on Tunnel Concentrator 60
data ports
    handles traffic encapsulation and forwarding 18
    recommended for management access 16, 17
default gateway
    configure through data ports 16, 17
delete user 59
deployment workflow vi
documentation
    feedback x
    location viii, ix
DSCP support 23

E

edit Tunnel Concentrator hostname 47
encryption key creation 13
examples
    config example for ExtremeCloud IQ 68–70
    installation example 65
ExtremeCloud Edge - Self-Orchestration
    install and configure 30
    installation example 65
ExtremeCloud IQ configuration
    alternative configuration flow 68–70
    configure Tunnel Concentrator service 39
    quick add tunnel concentrators 38
ExtremeCloud IQ Controller configuration
    assign GRE topology to WLAN network 54
    assign VLAN with GRE topology to AP profile 54
    configure GRE topology for VLAN 52
    read-only account requirement 28, 35
    requirements 28
    task flow 51

F

feedback x

H

hardware
    supported appliances 14
    supported capacities per appliance 14
high availability
    vrrp required on ExtremeCloud IQ 20
    with ExtremeCloud IQ Controller 22
hostname

hostname *(continued)*
edit for Tunnel Concentrator from ExtremeCloud IQ 47
how to use this guide vi
how tunnel concentrator works 12
how tunnels get created 12

I

ICC ports
connectivity not required 30
kubernetes binding to ICC address 23
not recommended for management access 16, 17
reasons not to use for management 23
image management
upload Tunnel Concentrator image 32
install
ExtremeCloud Edge - Self-Orchestration 30
installation example 65
installation requirements 28
installation task flow 29
select management application 35
Tunnel Concentrator activation license 35
Tunnel Concentrator application 32
IPsec
configure secure tunnel 52
supported for ExtremeCloud IQ Controller only 23

L

LAG configuration summary 26
licensing
generate activation license 35
purchase activation SKU 28
requirements 28
limitations 23
load balancing
with ExtremeCloud IQ 20
with ExtremeCloud IQ Controller 22
log in to Tunnel Concentrator 56
logs
configure log reporting 61
log reporting field descriptions 61
view logs 60

M

maintenance tabs on Tunnel Concentrator 56
management layer
inlets access 16, 17
VRRP required to access 16, 17
management options for tunnel provisioning 13
migrations from VGVA Tunelling
using Classification Rules 48
using Network Policy 49
multicast
add rule on ExtremeCloud IQ 39
multicast controls on Tunnel Concentrator 25

N

NAT not supported 23
network architecture
data layer 18
management layer 16, 17
network policy
deploy 46
notices vii

O

onboard to ExtremeCloud IQ Controller 35

P

packet captures 62
password
change admin password 34
change for a user (administrators only) 59
change your user password 60
ping a node 62
product announcements ix, x
provisioning
select management application for 35

Q

quick add Tunnel Concentrators to ExtremeCloud IQ 38

R

redundancy
layer 2 connectivity 20
summary for ExtremeCloud IQ 20
summary for ExtremeCloud IQ Controller 22
vrrp required on ExtremeCloud IQ 20
Runnel Concentrator user interface 57

S

scalability and supported capacities 14
select management option 35
settings
Tunnel Concentrator Service 40
stacks
data stack 18
management stack 16, 17
support
supported appliances 14
supported capacities and scalability 14
supported products and recommended versions 14
technical support ix, x

T

technical support

technical support *(continued)*
contacting ix, x
transport method options 12
troubleshooting
create backup file 63
packet captures 62
ping a node 62
view dashboards 60
view logs 60
Tunnel Concentrator Service settings 40
tunnel policy configuration 43
tunnel provisioning 12
tunneling method
GRE with ExtremeCloud IQ 12
IPsec with ExtremeCloud IQ Controller 12

U

Universal Compute Platform requirements 28
upgrade Tunnel Concentrator 63
upload Tunnel Concetrator image 32
user interface
Tunnel Concentrator 57
user management (for administrators)
add user 59
change password for a user 59
delete user 59
user password
change your user password 60
user profile
set tunnel destination to Tunnel Concentrator 44

V

view dashboards 60
view logs 60
VRRP (Virtual Router Redundancy Protocol)
cofiguration on data port 30
configuration summary 19, 20
on data port for management access 19, 20
on Tunnel Concentrator service for HA 19, 20
used for HA with ExtremeCloud IQ 18

W

warnings vii