Extreme Tunnel Concentrator Deployment Guide

Version 24.04

9038930-00 Rev. AA
May 2024

Legal Notice

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

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

Trademarks

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

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

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

Open Source Declarations

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

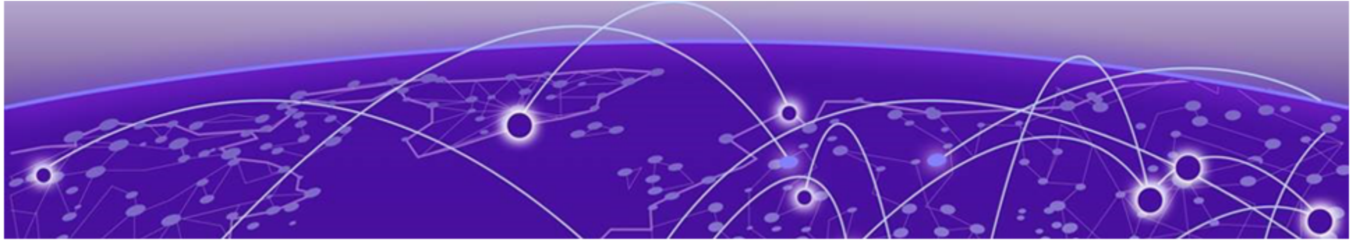
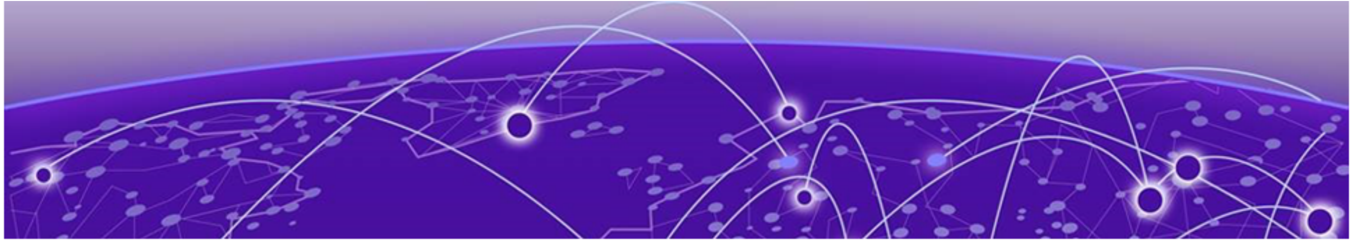


Table of Contents



Preface

Read the following topics to learn about:

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

Text Conventions

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

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

Table 1: Notes and warnings

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

Table 2: Text

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

Table 3: Command syntax

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

Documentation and Training

Find Extreme Networks product information at the following locations:

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

Open Source Declarations

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

Training

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

Help and Support

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

Extreme Portal

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

The Hub

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

Call GTAC

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

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

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

Subscribe to Product Announcements

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

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

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

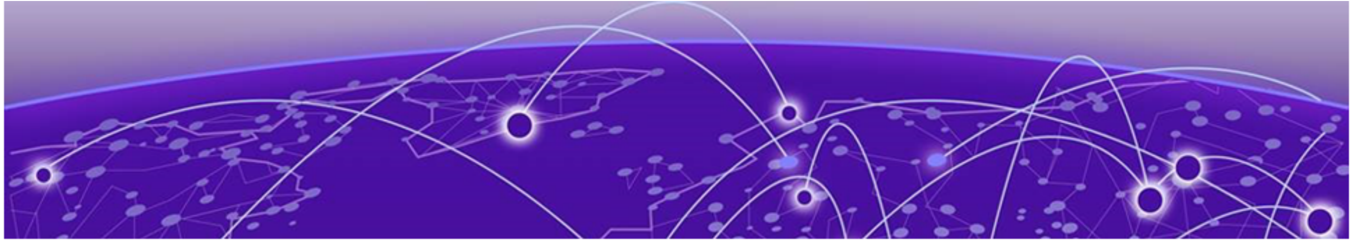
Send Feedback

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

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

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

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



Extreme Tunnel Concentrator

Extreme Tunnel Concentrator runs as a ExtremeCloud Edge - Self-Orchestrated application that is deployed on the Extreme Universal Compute Platform. The Extreme Tunnel Concentrator solution lets you configure Generic Routing Encapsulation (GRE) tunneling that directs wireless traffic from your access points to your traffic data center, where the traffic can be aggregated and processed.

Tunnel Concentrator provides the following benefits over existing wireless traffic solutions:

- 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.
- Creates tunneled traffic flows that do not need to cross a controller, removing the need to have Tunnel Concentrator in the same location as your access points.
- Provides an option for traffic aggregation in situations where it is cost prohibitive to deploy fabric mesh infrastructure or VxLAN switching.

How Tunnel Concentrator Works

Tunnel Concentrator lets you configure GRE 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 traffic to the data center, where the traffic can be aggregated.

To provision tunnels, administrators configure GRE tunneling settings for a given VLAN and map the VLAN across the WLAN network. All GRE tunneling sessions get initiated by the access point, which generates tunnels dynamically on a per user traffic flow basis for the VLAN. As a user's traffic flows across the AP, the AP adds the GRE encapsulation settings that were mapped to that VLAN, which generates the tunnel between the AP and Tunnel Concentrator. If IPSec is deployed, the AP also encrypts the GRE header. The AP then forwards the traffic through the tunnel towards Tunnel Concentrator.

After receiving the traffic, Tunnel Concentrator decrypts received packets (if IPSec is deployed), 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.

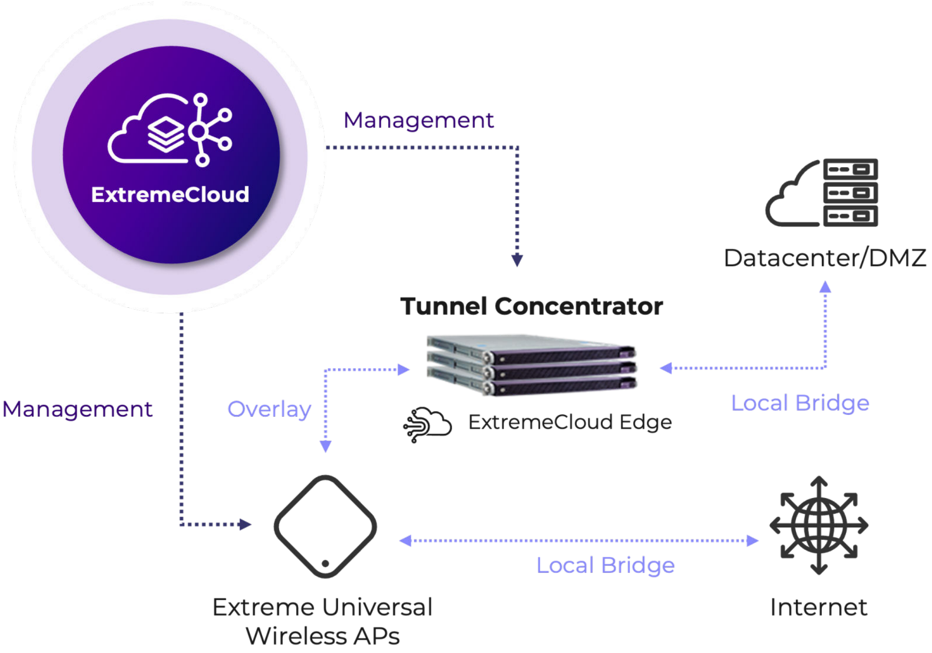


Figure 1: Tunnel Concentrator Deployment

Note
GRE 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 GRE 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 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.

Managed by ExtremeCloud IQ

Tunnels are configured and managed using the ExtremeCloud IQ user interface. For management, Tunnel Concentrator uses the inlets tunnel, which is maintained by the Universal Compute Platform, with access through port 8090.

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.

Redundancy

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.

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

Redundancy configuration and functionality depend on whether you use ExtremeCloud IQ Controller or ExtremeCloud IQ as the management entity.

Redundancy with ExtremeCloud IQ Controller

Configure redundancy using the GRE topology for a given VLAN. You can assign up to three prioritized Tunnel Concentrator instances to the topology. The AP attempts to send traffic to the highest ranked Tunnel Concentrator instance first. If that connection fails, the AP attempts to connect to the second instance, and if that connection fails, the AP attempts the third instance.

The priority ranking between multiple Tunnel Concentrator instances 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.

For an illustration of redundancy with ExtremeCloud IQ Controller, see Figure 2.

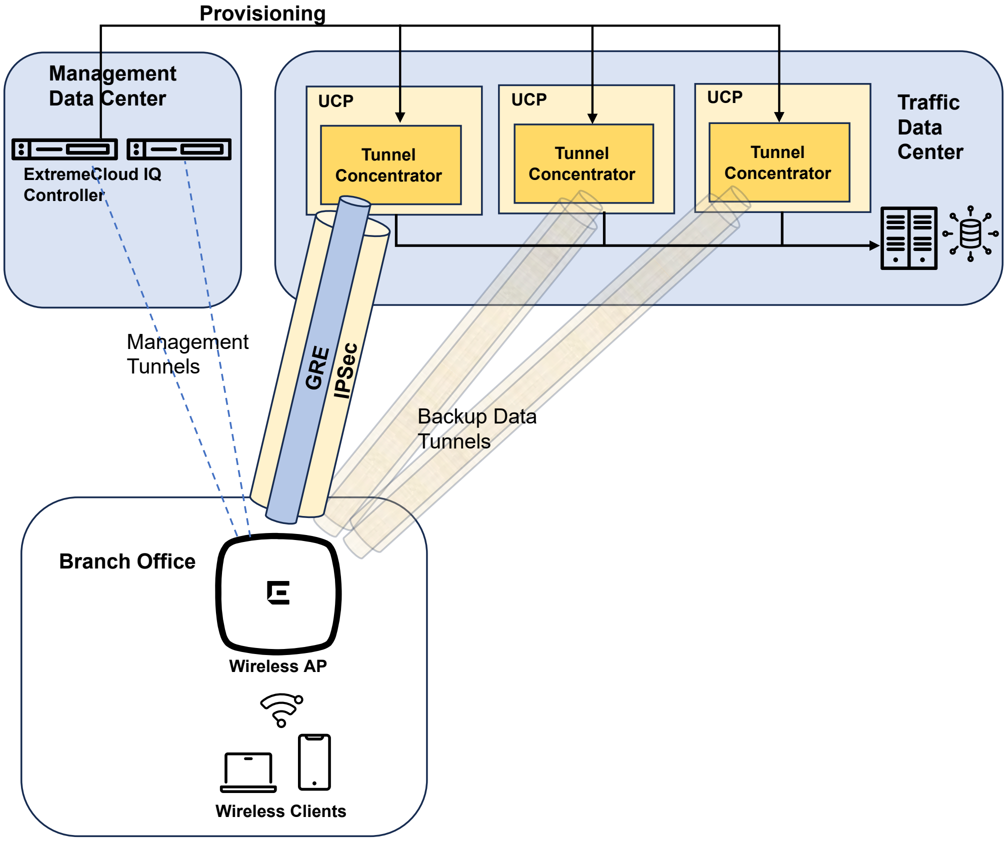


Figure 2: Tunnel Concentrator Redundancy with ExtremeCloud IQ Controller

Redundancy with ExtremeCloud IQ

Configure redundancy on ExtremeCloud IQ using the Tunnel Concentrator service and Tunnel Concentrator policy configurations. Redundancy uses a tunnel address that is shared using VRRP by both Tunnel Concentrator instances in a redundant pair. You can then assign primary and redundant instances, each with their own address, to that tunnel configuration.

When APs send data through a tunnel, they send the data to the shared VRRP address of the Tunnel Concentrator instances in the HA pair. The HA pair has an active Tunnel Concentrator instance and a standby instance with data being directed to the active instance. However, if the active instance goes down or becomes unavailable, the standby instance becomes active.

Figure 3 illustrates redundancy with three redundant pairs of Tunnel Concentrator instances spread across two Universal Compute Platform machines and with ExtremeCloud IQ as the management option.

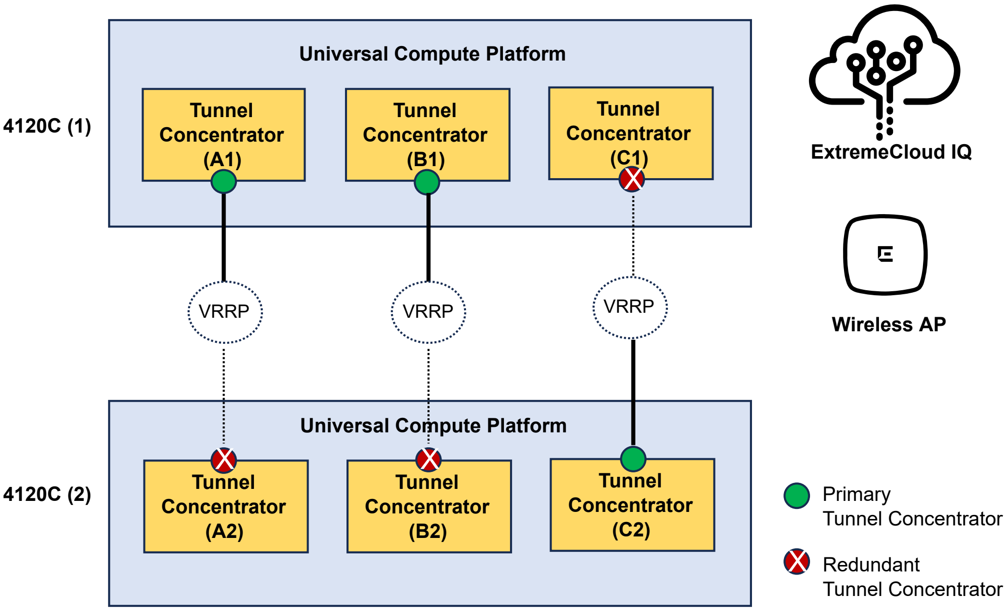


Figure 3: Tunnel Concentrator Redundancy (with ExtremeCloud IQ)

To add load balancing when using ExtremeCloud IQ, create more than one Tunnel Concentrator service under **Configure** > **Common Objects** > **Network** > **Tunnel Concentrator Services**.

Deployment Considerations

- Each Tunnel Concentrator instance supports up to 5,000 tunnels. If you deploy High Availability (HA) pairs, the 5,000 tunnel limit applies to the HA pair.
- Each Universal Compute Platform 4120C host can support up to three Tunnel Concentrator instances with a maximum of 15,000 tunnels per host.
- Tunnel Concentrator supports GRE tunneling (with IPSec encryption) only between wireless access points and Tunnel Concentrator. Note that IPSec is supported only if you deploy ExtremeCloud IQ Controller as the management application.
- Tunnel Concentrator does not support the use of a NAT router between the access point and Tunnel Concentrator.
- Tunnel Concentrator preserves DSCP markings for both upstream and downstream direction.
- Tunnel Concentrator blocks all broadcasts (except DHCP and ARP).
- Tunnel Concentrator does not support the use of LAG interfaces on the Universal Compute Platform.
- IPSec is supported only with APs that are managed by ExtremeCloud IQ Controller.

ARP Responder

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

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

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

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

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

Supported Products

The following table lists the products and supported versions for the applications that make up the Tunnel Concentrator solution.

Table 4: Supported Products and Versions

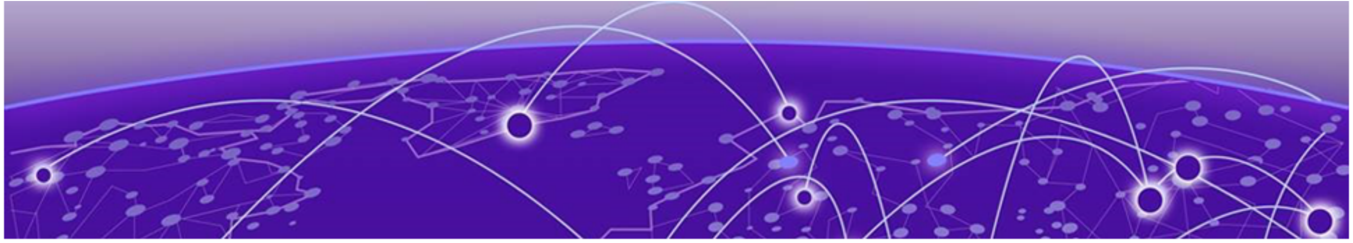
Products	Supported Versions for Tunnel Concentrator Support
Universal Compute Platform	5.06.01 minimum
ExtremeCloud IQ Controller	10.09.01 recommended
ExtremeCloud IQ	24.04 recommended
Access points	Tunnel Concentrator is supported on ExtremeCloud IQ Universal access points and on IQ Engine access points. See *ExtremeCloud IQ Release Notes* for hardware and OS release information.

How to Use this Guide

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

Table 5: Tunnel Concentrator Deployment Process Flow

	Chapter	Description
1	Installation on page 16	Use the procedures in this chapter to install Tunnel Concentrator.
2	Select one of the following chapters: • ExtremeCloud IQ Controller Configuration on page 21 • ExtremeCloud IQ Configuration on page 25	You must select either ExtremeCloud IQ Controller or ExtremeCloud IQ as the management application for GRE tunneling. Use only the chapter that applies to your deployment.
3	Administration on page 34	After installation and configuration, use this chapter to administer and maintain your deployment on an ongoing basis.



Installation

The procedures in this chapter describe how to install the Extreme 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:
  - Download the Extreme Tunnel Concentrator installation image from the portal at `Downloads/ExtremeCloud/Extreme Tunnel Concentrator`.
  - Purchase the Extreme Tunnel Concentrator activation SKU **EXTR-IQ-TC**.

Universal Compute Platform Prerequisites

- Deploy an ExtremeCloud Edge - Self-Orchestration Deployment on Universal Compute Platform. For information, see *ExtremeCloud Edge - Self-Orchestration Deployment Guide for Universal Compute Platform*.
- Configure a data interface on Universal Compute Platform. Note that Tunnel Concentrator does not support LAG interfaces.
- Select whether to deploy ExtremeCloud IQ Controller or ExtremeCloud IQ as the management application for tunnel provisioning. Refer to the subsequent prerequisite sections for additional prerequisites that are specific to those applications.

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, note that multiple read-only accounts are not mandatory.

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

ExtremeCloud IQ Prerequisites

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

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

Installation Task Flow

Complete the tasks in the following task flow to install an instance of Tunnel Concentrator on the Universal Compute Platform.

Table 6: Installation Task Flow

	Procedure	Description
1	Install Tunnel Concentrator on page 18	Load and install the Tunnel Concentrator image on the Universal Compute Platform.
2	Change Password on page 19	Change the admin password immediately after the first login.
3	Generate the Activation License on page 19	Activate the license for your install.
4	Select the Management Option on page 19	Select the application that you want to use to provision tunneling settings. You can select from: • ExtremeCloud IQ Controller • ExtremeCloud IQ

Install Tunnel Concentrator

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

1. Log in to the Universal Compute Platform.
2. Go to **Engines** > **Image Management**.
3. Locate the image file on your desktop.
4. Drag the image file onto the Universal Compute Platform desktop.

   The install file uploads automatically.
5. Go to **Engines** > **Installation**.
6. From the **Extreme Tunnel Concentrator** pane, select **Install**.
7. In the popup window, select **OK**.

   A new instance of Tunnel Concentrator displays on the **Engines** page along with a link.
8. Within the **Extreme Tunnel Concentrator** pane, select the link for your installation.
9. Configure the following settings:
   - **Node Affinity**—Select the Universal Compute Platform node on which this Tunnel Concentrator instance will run.
   - **Port 1**—Virtual function 01 on port 1 is used for licensing.

     Note
     The Tunnel Concentrator instance is locked to the VF number.
   - **Port (2, 3 and 4)**—You can set these ports to any VF option.
10. Select **Deploy**.

    After a delay of up to a few minutes to process the updates, the Extreme Tunnel Concentrator screen displays a set of four tabs.
11. Under the **Network Service Configuration** tab, select the **Assigned Virtual IP Address** drop-down and select an IP address for the Tunnel Concentrator service. This IP address also gets used to generate a URL for GUI access.
12. Select **Save**.

    After a few minutes, the screen displays an **Instance web interface** link.
13. Select the **Instance web interface** link to launch the Extreme Tunnel Concentrator GUI.
14. Log in using the default admin credentials.

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

Change Password

Use this procedure on Tunnel Concentrator to change the password that lets you log in to the GUI.

Note
This procedure can be used by admins to change the admin password and can also be used by users (non-admins) to change their user password.

1. Log in to the Extreme Tunnel Concentrator user interface.
2. In the top right corner of the header, select ▼.
3. Select **Change Password**.
4. In the **Password** box, enter the new password.
5. In the **Confirm Password** box, re-enter the password.
6. Select **Update**.

Generate the Activation License

All customers must generate and install an activation license. After you install Tunnel Concentrator, use this procedure to generate and install the activation package.

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

Select the Management Option

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

1. Log in to Extreme 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.

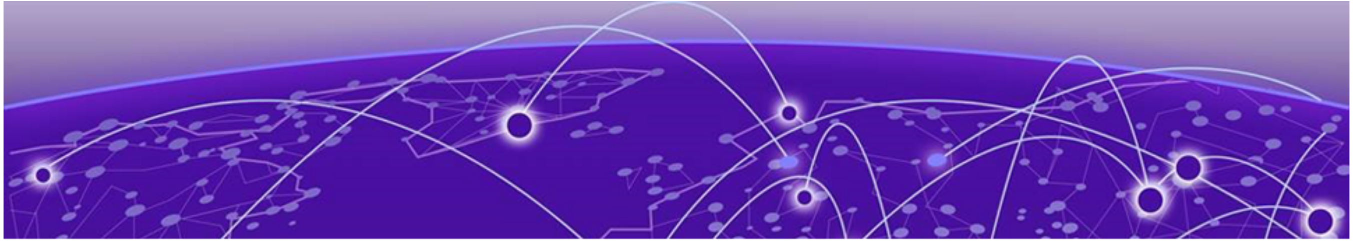
   You can also obtain the application key from the **Administration** > **Accounts** page of ExtremeCloud IQ Controller.

5. Select **Save**.

What to do Next

Go to the configuration flow that matches the management application that you selected:

- ExtremeCloud IQ Controller Configuration on page 21
- ExtremeCloud IQ Configuration on page 25



ExtremeCloud IQ Controller Configuration

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

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

Table 7: ExtremeCloud IQ Controller Configuration

	Procedure	Description
1	Configure Tunnel Concentrator on page 22	Configure settings for Tunnel Concentrator instances that you've onboarded to the controller.
2	Configure a GRE Topology for a VLAN on page 22	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 23	Assign the GRE topology as the default VLAN for the WLAN.
4	Assign the GRE Topology to the Access Point Profile on page 24	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 Serial Number of the Tunnel Concentrator 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.

   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.
7. Select **Save**.
8. Repeat this procedure if you have additional Tunnel Concentrator instances to configure.

Configure a GRE Topology for a VLAN

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

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

   VLAN Name

   Name of the GRE VLAN

   Mode

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

VLAN ID

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

Tagged

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

Tunnel Concentrators

List of Tunnel Concentrators.

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

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

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

Load Balance

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

4. Select **Save**.

Assign the GRE Topology to the WLAN

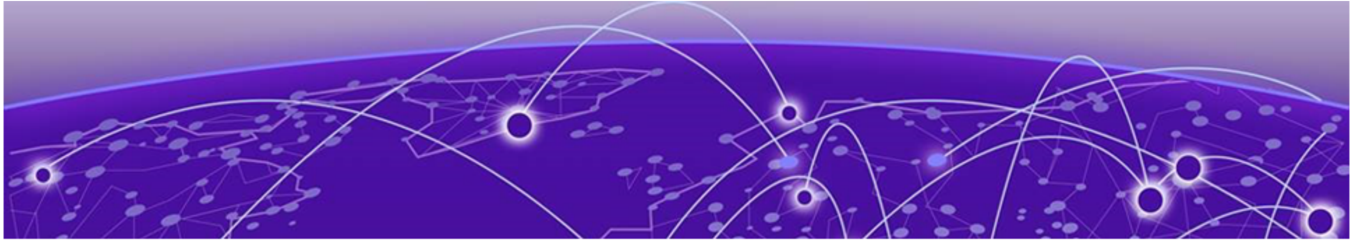
Assign the VLAN with the GRE topology as the default VLAN for the WLAN.

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

Assign the GRE Topology to the Access Point Profile

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

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



ExtremeCloud IQ Configuration

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

> Note
> Before you complete the following configuration tasks, complete the procedures in the Installation chapter, and see Considerations on page 26:

Table 8: ExtremeCloud IQ Configuration

	Procedure	Description
1	Quick Add Tunnel Concentrators on page 26	Onboard Tunnel Concentrator instances as devices to ExtremeCloud IQ. This task registers the instance serial numbers.
2	Configure Tunnel Concentrator Services on page 27	Add and configure a Tunnel Concentrator Service to serve as a **Tunnel Destination** for network policies. A Tunnel Concentrator Service can be single or redundant.
3	• Configure Tunnel Policies on page 29 • Configure a User Profile for Traffic Tunneling on page 30 • Apply Different User Profiles to Clients and User Groups on page 30	Use network and user policies to direct traffic to the Tunnel Concentrator. While editing an existing network policy or creating a new one, edit the **User Access Settings** to apply different profiles to clients and user groups.

> Note
> See Configuration Example on page 31 for an example of a redundant Tunnel Concentrator deployment with ExtremeCloud IQ. The example provides sample IP address assignments for Universal Compute Platform and Tunnel Concentrator.

Considerations

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

Related Topics

Quick Add Tunnel Concentrators on page 26
Configure Tunnel Concentrator Services on page 27
Configure Tunnel Policies on page 29
Configure a User Profile for Traffic Tunneling on page 30
Apply Different User Profiles to Clients and User Groups on page 30

Quick Add Tunnel Concentrators

First deploy the Tunnel Concentrators instances. For more information, see Installation on page 16.

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

1. Log in to ExtremeCloud IQ.
2. Go to **Manage** > **Devices**.
3. Select +, then select **Quick Add Devices**.
4. Select **Manage your devices directly from the cloud**.
5. For **Device Type**, select **Real**.
6. For **Entry Type**, select **Manual**.
7. Type the **Serial Number** of the device.
8. From the **Device Make** menu, select **Tunnel Concentrator**.
9. (Optional) From the **Policy** menu, select an existing network policy.

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

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

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

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

Related Topics

Configure Tunnel Concentrator Services on page 27

Configure Tunnel Policies on page 29

Configure a User Profile for Traffic Tunneling on page 30

Configure Tunnel Concentrator Services

Add the Tunnel Concentrator as a device type. See Quick Add Tunnel Concentrators on page 26.

Perform this procedure to configure a new Tunnel Concentrator service.

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

   See Settings for a Single Tunnel Concentrator on page 27 or Settings for a Redundant Tunnel Concentrator on page 28.
4. Select **Save**.

Related Topics

Quick Add Tunnel Concentrators on page 26

Tunnel Concentrator Services Settings on page 27

Tunnel Concentrator Services Settings

Settings for a Single Tunnel Concentrator

Table 9: Single Tunnel Concentrator

Field	Description
Name	(Required) Type a name to identify the new Tunnel Concentrator service.
Description	(Optional) Provide a description that might be helpful when troubleshooting.
Single Tunnel Concentrator	(Required) Select this option to create a single Tunnel Concentrator without redundancy.
Tunnel IP Address/CIDR	(Required) Type the IP Address for the tunnel (CIDR).
Gateway	(Optional) Type the IP address of the gateway.
Native VLAN ID	(Required) Type the Native VLAN ID. The Native VLAN is untagged.

Table 9: Single Tunnel Concentrator (continued)

Field	Description
Device Tunnel Concentrator	(Required) Select a Tunnel Concentrator from the menu.
Tunnel Port	(Required) Select a port from the menu.
VLAN ID	(Required) Type the VLAN ID. (Optional) For an untagged VLAN, select the corresponding check box.
Bridge Port	(Required) Select a bridge port for the tunnel from the menu.

Settings for a Redundant Tunnel Concentrator

Table 10: Primary and Backup Tunnel Concentrators

Field	Description
Name	(Required) Type a name to identify the new Tunnel Concentrator service.
Description	(Optional) Provide a description that might be helpful when troubleshooting.
Redundant Tunnel Concentrator	(Required) Select this option to create a redundant Tunnel Concentrator.
Tunnel IP Address/CIDR	(Required) Type the IP Address for the tunnel (CIDR).
Gateway	(Optional) Type the IP address of the gateway.
VRRP Router ID	(Required) Type the ID for the VRRP router. ExtremeCloud IQ configures the same VRRP Router ID for both the primary and backup Tunnel Concentrators (range 1-255). The **VRRP Router ID** must be different for each cluster of VRRP devices.
Native VLAN ID	(Required) Type the Native VLAN ID. The Native VLAN is untagged.
Device Tunnel Concentrator	(Required—Primary and Backup) Select a primary Tunnel Concentrator from the menu. Select a backup Tunnel Concentrator from the menu.

Table 10: Primary and Backup Tunnel Concentrators (continued)

Field	Description
Tunnel Port	(Required—Primary and Backup) Select a port for the tunnel from the menu for the primary Tunnel Concentrator from the menu. Select a port for the tunnel from the menu for the backup Tunnel Concentrator from the menu.
VLAN ID	(Required—Primary and Backup) Type the VLAN ID for the primary and for the backup Tunnel Concentrators. (Optional) For an untagged VLAN, select the corresponding check box.
IP Address	(Required—Primary and Backup) Type the IP address for the primary and the backup Tunnel Concentrators.
Bridge Port	(Required—Primary and Backup) Select a bridge port for the tunnel from the menu for the primary Tunnel Concentrator. Select a bridge port for the tunnel from the menu for the backup Tunnel Concentrator.

Configure Tunnel Policies

Add the Tunnel Concentrators and configure the Tunnel Concentrator services.

Use the following steps to add a new tunnel policy to support Layer 2 roaming with Tunnel Concentrator. Alternately, you can skip this step and create a user policy with Traffic Tunneling (GRE) to Tunnel Concentrator. See Configure a User Profile for Traffic Tunneling on page 30.

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

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

   Although optional, descriptions can be helpful when you are troubleshooting your network.
6. Select **Tunnel Concentrator** and then select the **Tunnel Destination** from the drop-down list.

   You can add a new Tunnel Concentrator service by selecting +, or select ✎ for an existing instance. For more information, see Configure Tunnel Concentrator Services on page 27.

7. Select **Save**.

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

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

Related Topics

Quick Add Tunnel Concentrators on page 26
Configure a User Profile for Traffic Tunneling on page 30
Configure Tunnel Concentrator Services on page 27

Configure a User Profile for Traffic Tunneling

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

1. Log in to ExtremeCloud IQ.
2. Go to **Configure** > **Common Objects** > **Policy** > **User Profiles** and either create a new user profile, or select an existing profile to edit.

   Select an existing profile from the **Re-use Tunnel Policy** menu.
3. On the **Traffic Tunneling** tab, turn on **Traffic Tunneling (GRE)**, and then select the type of traffic tunneling.
4. For **Tunnel Concentrator**, select the **Tunnel Destination** from the drop-down list.

   You can add a new Tunnel Concentrator service by selecting ✚, or select ✎ to modify an existing instance. For more information, see Configure Tunnel Concentrator Services on page 27.
5. Select **Save**.

Related Topics

Configure Tunnel Concentrator Services on page 27

Apply Different User Profiles to Clients and User Groups

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

While editing an existing network policy or creating a new one, use this procedure to apply different user profiles to clients and user groups. With user-profile assignment rules, you can assign clients to user profiles that match all configured conditions. The available conditions are as follows:

- Advanced Guest Policy
- Client OS Type
- Client MAC Address
- Client Location

- Schedule
- Cloud Config Group

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

1. Go to **Configure** > **Network Policies**, select a preconfigured policy, and then select **Next**.
2. Under **User Access Settings**, select **Apply a different user profile to various clients and user groups**.
3. Select ☰ to choose an existing user profile, or select + to add a new profile.
4. To add an existing user profile assignment rule, select ↖.
   a. Select one of the existing rules.
   b. Select **Link**.
5. To add a new user profile assignment rule, select ⊞.
   a. Type a **Name** for the user profile assignment rule.
   b. (Optional) Type a description.
   c. Select + and choose a category.
   d. Complete the configuration for the selected category.

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

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

Configuration Example

Figure 4 provides an example of a redundant Tunnel Concentrator deployment with ExtremeCloud IQ as the management application. The example provides sample IP address assignments for the deployment.

With this example, Tunnel Concentrator is installed on Universal Compute Platform 4120C hardware, which supports up to three instances per server.

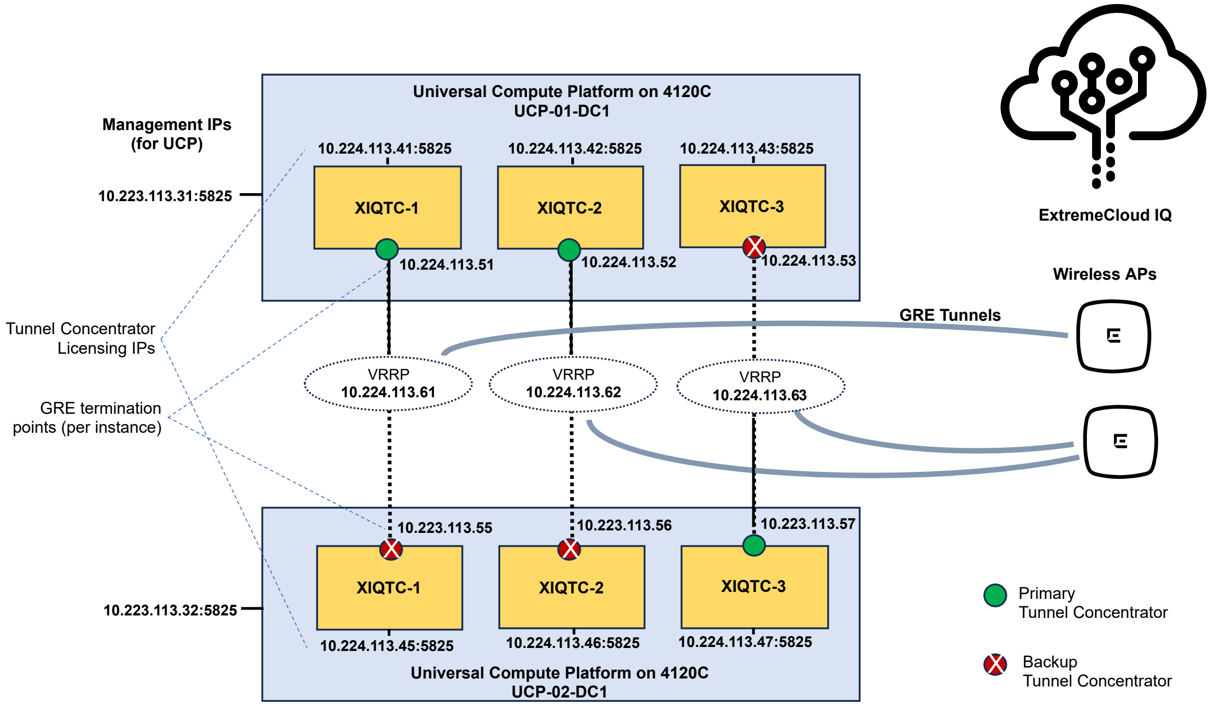


Figure 4: Configuration Example with ExtremeCloud IQ and Redundancy

Table 11 provides more information on the IP address assignments.

Table 11: IP Address Assignments

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

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

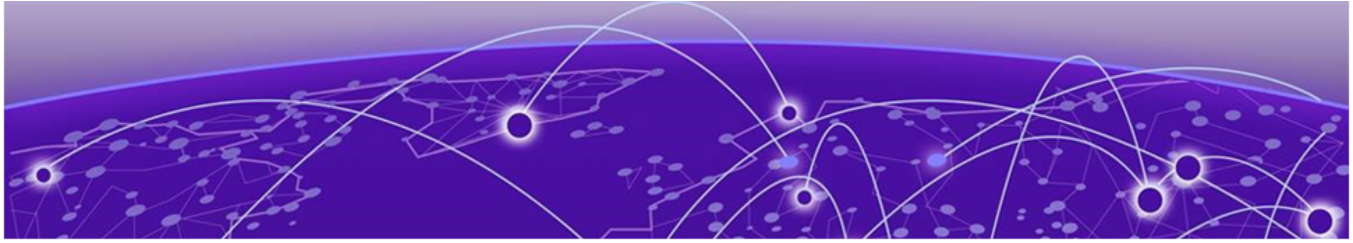
- Universal Compute Platform—This example uses two hardware servers.
- Management IP (for Universal Compute Platform)—This IP address is configured on Universal Compute Platform as part of your prerequisites for a Tunnel Concentrator

installation. This IP address allows administrators to access the Universal Compute Platform user interface.

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

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

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



Administration

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

Log in to Tunnel Concentrator

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

> Note
> If you deploy ExtremeCloud IQ as the management application, you can also open the Tunnel Concentrator user interface from ExtremeCloud IQ (the minimum release for this feature is 24.03). For more information, see Quick Add Tunnel Concentrators on page 26.

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 12: Tunnel Concentrator Maintenance Tabs on Universal Compute Platform

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

Table 12: Tunnel Concentrator Maintenance Tabs on Universal Compute Platform (continued)

Tab	Description
Logs	Use this tab to access logs for this instance of Tunnel Concentrator.
Console	Use this tab and then select **Attach** to open a command line console from which you can access the application for debugging purposes. Select **Detach** to remove the command line interface

4. Select the **Instance Web Interface** link.

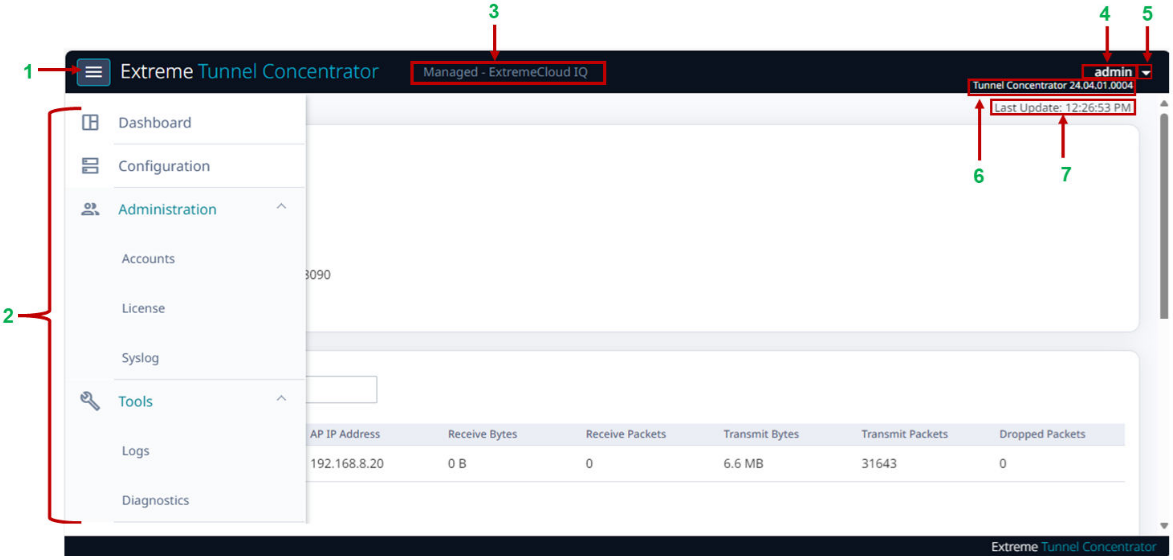
   The Extreme Tunnel Concentrator interface opens at the login screen.

5. 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**.

Extreme Tunnel Concentrator User Interface

Navigate the Extreme Tunnel Concentrator User Interface as displayed in Figure 5. For descriptions of the callout items, refer to Table 13, which follows the image.



AP IP Address	Receive Bytes	Receive Packets	Transmit Bytes	Transmit Packets	Dropped Packets
192.168.8.20	0 B	0	6.6 MB	31643	0

Figure 5: Tunnel Concentration User Interface

Table 13: Tunnel Concentrator Interface Callout Items

Callout	Description
1	☰—Select the navigation icon to open the navigation menu.
2	Navigation menu—Select one of the menu items to open the applicable configuration page.
3	Management mode—Displays the application that is selected currently as the management application for Tunnel Concentrator.

Table 13: Tunnel Concentrator Interface Callout Items (continued)

Callout	Description
4	Username of the logged-in user.
5	▼—Select the user settings icon to view the user-specific menu options such as log out or change password.
6	Version—Displays the full Tunnel Concentrator version number with the build number appended.
7	Time of the last page refresh.

View Dashboards

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

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

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

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

User Management

Add User

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

1. Log in to Extreme 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 Extreme 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**.

Update Password (Administrator)

Administrators with admin privileges can use this procedure to change a user password to the Tunnel Concentrator user interface on behalf of a user.

> Note
> This procedure requires admin privileges. If you do not have admin privileges and want to change your user password, use Change Password on page 19.

1. Log in to Extreme Tunnel Concentrator.
2. Go to **Administration** > **Accounts**.
3. Select the user whose password you want to update.
4. Select the Update Password icon.
5. Enter the new password.
6. Re-enter the password.
7. Select **Save**.

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 38.

1. Log in to Extreme 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 14: 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 14: 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 packet capturing on either the listening interface or bridge interface of Tunnel Concentrator.

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

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

Ping a Node

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

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

Upgrade Tunnel Concentrator

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

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

1. Log in to the Universal Compute Platform interface.
2. Upload the new application image file:
    a. Go to **Engines** > **Image Management**.

       A list of uploaded images displays under the **Choose Image File** pane.

    b. To upload the new image, complete either of the following steps:
        - Select **Choose Image File**, then browse to the image file and select it. Or,
        - Drag the image from your local drive and drop it on the **Choose Image File** pane.

       Note
       To delete an image file, select the check box next to the image and 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.

Index