



ExtremeCloud Tunnel Concentrator v25.05.01.0018 Release Notes

Enhancements, Fixes, and Supported Devices

9039544-00 Rev. AB
April 2026



Copyright © 2026 Extreme Networks, Inc. All rights reserved.

Legal Notice

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

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

Trademarks

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

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

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

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses.

End-user license agreements and open source declarations can be found at: <https://www.extremenetworks.com/support/policies/open-source-declaration/>

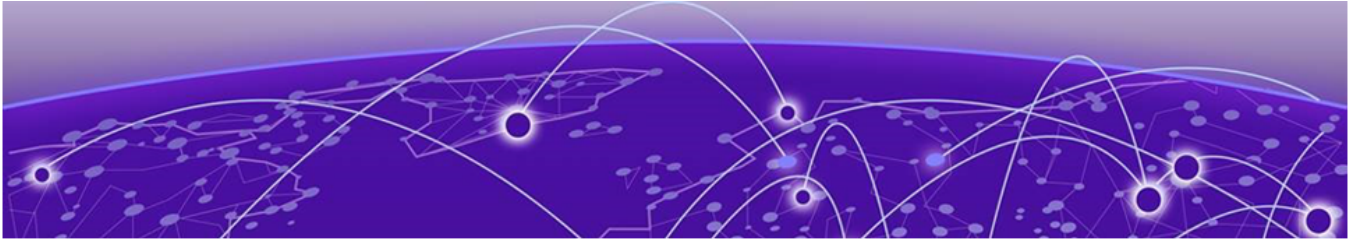


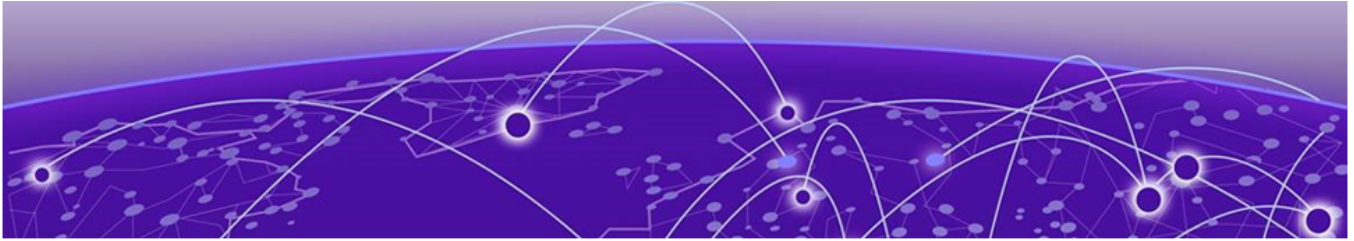
Table of Contents

Abstract.....	4
Revision History.....	5
General Release Information.....	6
New Features.....	6
Resolved Issues.....	7
Known Issues.....	8
Documentation.....	9
Help and Support.....	9
Subscribe to Product Announcements.....	10



Abstract

These release notes for ExtremeCloud Tunnel Concentrator version 25.05.01.0018, issued in April 2026, outline new features, resolved issues, known issues, and documentation resources. This release introduces enhanced redundancy and failover enhancements for deployments that are managed by ExtremeCloud IQ with the ability to assign primary, secondary, and tertiary tunnels to a Tunnel Concentrator-enabled user profile. In addition, you can now obtain the serial number for a freshly installed instance from Universal Compute Platform. For ExtremeCloud IQ-managed deployments, this update lets you handle onboarding and licensing from ExtremeCloud IQ without having to use the Tunnel Concentrator GUI. This document provides links to installation, configuration, and maintenance guides, and offers multiple channels for obtaining technical support and subscribing to product announcements. Revision AB features minor corrections to Known Issues.



Revision History

Table 1: Revision History

Publish Date	Revision	Updates
15 April 2026	AA	Initial publish
20 April 2026	AB	Minor corrections to Known Issues



General Release Information

- [New Features](#) on page 6
- [Resolved Issues](#) on page 7
- [Known Issues](#) on page 8
- [Documentation](#) on page 9
- [Help and Support](#) on page 9

New Features

Enhanced Redundancy for ExtremeCloud IQ Deployments

This release improves redundancy and failover support for Tunnel Concentrator deployments that are managed from ExtremeCloud IQ. You can now assign up to three Tunnel Concentrator services as tunnel destination (in Primary, Secondary, and Tertiary roles) for a tunneling-enabled user profile.

This update, when added to existing HA functionality within a Tunnel Concentrator service, provides up to six possible Tunnel Concentrators for tunnel termination within a single User Profile.

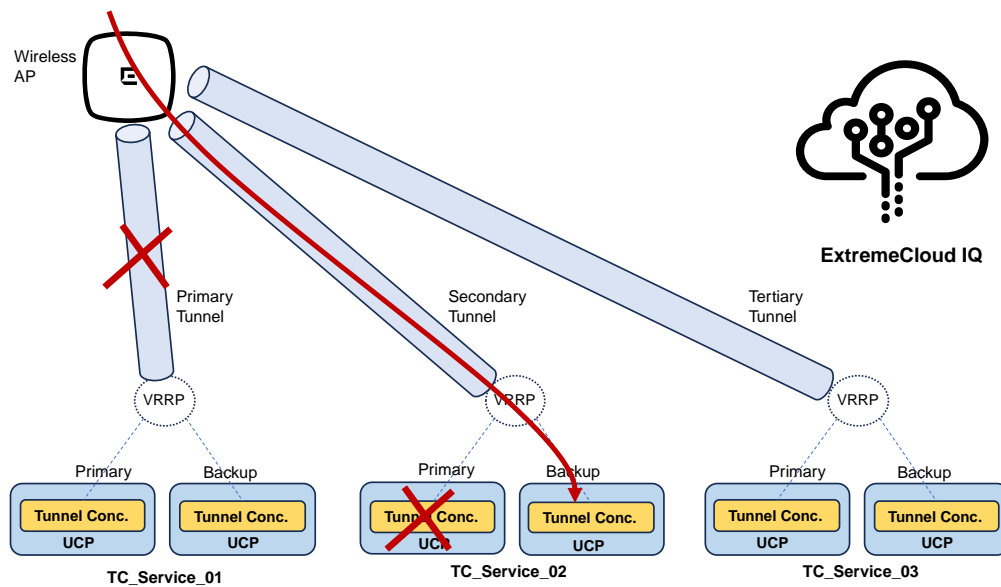


Figure 1: Enhanced Redundancy for ExtremeCloud IQ-Managed Deployments

Note the following feature conditions:

- You can add geographic redundancy by pointing to Tunnel Concentrator services in geographically dispersed data centers. There is no requirement that the primary, secondary, and tertiary Tunnel Concentrator services within a user profile be on the same network segment, or in the same data center.
- A keepalive process is introduced that allows APs to track which tunnels are active and inactive. For each Tunnel Concentrator service, you can configure both the keepalive interval and the number of keepalive retries before an AP deems a non-responsive tunnel to be inactive.

For details, see the *ExtremeCloud Tunnel Concentrator Deployment Guide*.

Tunnel Concentrator Serial Number Displays on Universal Compute Platform

You can now obtain the Serial Number for a freshly installed Tunnel Concentrator instance from the engine summary that displays on Universal Compute Platform immediately after you deploy the engine.

For Extreme Cloud IQ-managed deployments, this update removes the requirement to use the Tunnel Concentrator GUI for licensing. You can now obtain the serial number from Universal Compute Platform, onboard the unlicensed Tunnel Concentrator instance to ExtremeCloud IQ, and complete licensing and activation from ExtremeCloud IQ.

To do this, follow the existing ExtremeCloud IQ onboarding process to onboard the unlicensed Tunnel Concentrator instance. After onboarding, go to **Manage > Devices** in ExtremeCloud IQ, select the new Tunnel Concentrator instance to open the device Monitoring page for that instance, and then select **Appliance UI** to launch the embedded user interface. You can then upload the license from the embedded UI to activate the instance.



Note

This update forms Phase 1 of a larger initiative to add the Tunnel Concentrator user interface to ExtremeCloud IQ. Future releases will simplify the process.

Resolved Issues

Table 2: Resolved Issues

JIRA	Description
CFD-15151	Addressed issue that was resulting in NTP requests being sent to NTP servers that were not explicitly assigned on the Universal Compute Platform. NTP requests will be sent only to servers that are assigned on Universal Compute Platform.
IQVPN-284	Addressed issue that was causing the packet capture feature to truncate frames within the capture file for captured data.

Table 2: Resolved Issues (continued)

JIRA	Description
XIQ-41152	Addressed issue where manual intervention from an admin was required to reset the Tunnel Concentrator configuration on an AP after that AP's IP settings were reset due to a power cycle on the AP or router. With this update, ExtremeCloud IQ pushes an updated Tunnel Concentrator configuration automatically to APs that have had their IP settings reset.
CFD-16169 IQVPN-328	Addressed issue on 4120C that was resulting in both the primary and secondary Tunnel Concentrators ending up in a backup state.

Known Issues

Table 3: Known Issues

Issue	Description
CFD-14254 and IQVPN-279	There is an issue with the Network Usage calculation for Tunnel Concentrator. Some APs have reported a high network usage during periods where no clients are connected.
CFD-16364	When Tunnel Concentrator receives a large volume of multicast traffic (for example, mDNS traffic) from the client traffic bridge port, Tunnel Concentrator may become unresponsive. <i>Workaround:</i> A workaround is to block multicast traffic on the switch port that is connected directly to Tunnel Concentrator.
CFD-16486	Tunnel Concentrator statistics are showing packets being transmitted for inactive tunnels
CFD-16801	There is an issue with pushing configuration from ExtremeCloud IQ to Tunnel Concentrator where there is a large number of APs. A fix for this issue is being provided in an upcoming ExtremeCloud IQ patch release.
IQVPN-210	Tunnel Concentrator may drop packets at ~50-second intervals when the Dashboard is accessed or viewed; this behavior occurs only during Dashboard use.
IQVPN-220	Spanning Tree BPDUs are replicated by Tunnel Concentrator to all tunnels, resulting in extra frames being sent to clients but no functional side effects.

Table 3: Known Issues (continued)

Issue	Description
IQVPN-247	Changing VLAN Settings on a data port of Universal Compute Platform (host) after Tunnel Concentrator installed may cause networking access issues to the application. This issue has been experienced on 1130C platforms. Rebooting the Universal Compute Platform host may be required to re-establish connectivity. This issue will be resolved in a future revision.
IQVPN-336	When a multicast ACL is enabled but contains no entries, Tunnel Concentrator mistakenly allows all multicast traffic (for example, allowing mDNS). The correct behavior is to block all multicast traffic. <i>Workaround:</i> Add at least one multicast IP address to the ACL (for example, 224.0.0.200). Once an address is configured, the ACL allows that multicast address and blocks all other multicast traffic, including mDNS (224.0.0.251, UDP port 5353).

Documentation

Refer to the following documents for information on how to install, configure, and maintain the ExtremeCloud Tunnel Concentrator application:

Tunnel Concentrator Documents

- [ExtremeCloud Tunnel Concentrator Deployment Guide](#)—Contains information on how to install, configure, and maintain Tunnel Concentrator on Universal Compute Platform.

Related Extreme Networks Documents

- [ExtremeCloud Edge - Self-Orchestration Deployment Guide for Universal Compute Platform](#)—An ExtremeCloud Edge -Self-Orchestration deployment on Universal Compute Platform is a mandatory prerequisite for installing the Tunnel Concentrator application. Refer to this guide for deployment information.
- [ExtremeCloud IQ Controller User Guide](#)—If you are deploying ExtremeCloud IQ Controller as the management application for Tunnel Concentrator, refer to this guide for ExtremeCloud IQ Controller information.
- [ExtremeCloud IQ \(Classic\) User Guide](#)—If you are deploying ExtremeCloud IQ (Classic) as the management application for Tunnel Concentrator, refer to this guide for ExtremeCloud IQ information.

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.