Extreme Tunnel Concentrator v26.01.01.0016 Release Notes

Enhancements, Fixes, and Supported Devices

9041274-00 Rev. AA
October 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/

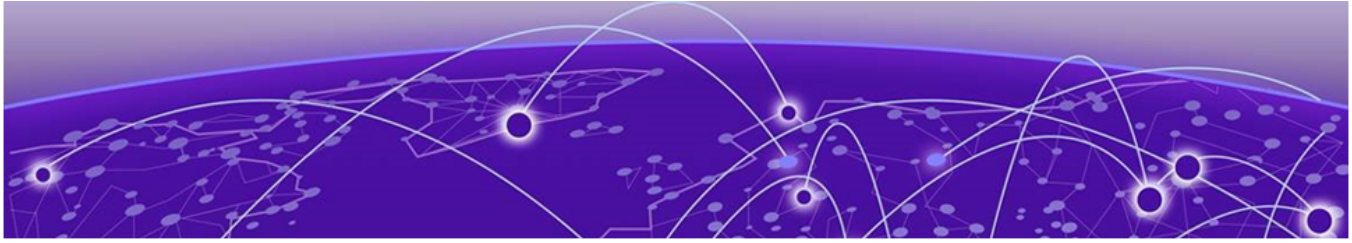


Table of Contents

Abstract **4**

General Release Information **5**

New Features 5

Resolved Issues 6

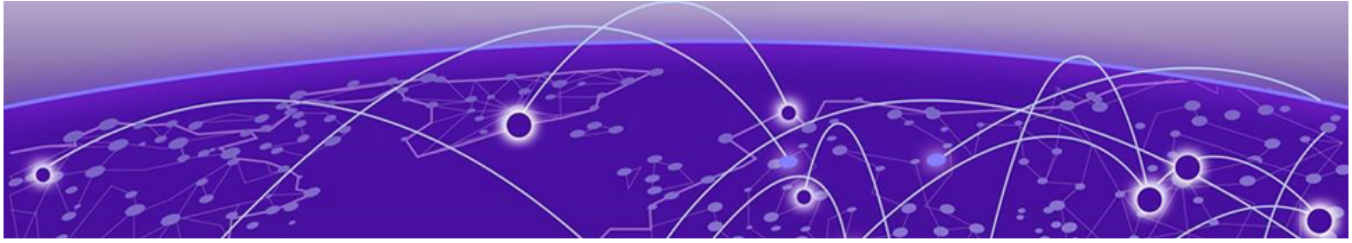
Known Issues 7

Feature Limitations in v26.01.01 7

Documentation 7

Help and Support 8

Subscribe to Product Announcements 9



Abstract

This release notes document for Extreme Tunnel Concentrator version 26.01.01.0016 provides technical information on new features, resolved defects, known issues, deployment limitations, and operational guidance for cloud-managed tunnel networking environments. Intended for network administrators and deployment engineers, it introduces support for Extreme Platform ONE™ Networking as a management platform for tunnel provisioning. This release also introduces the following features, all of which are targeted exclusively to Extreme Platorm ONE Networking deployments: IPSec-encrypted GRE tunnels, RADIUS-based client authentication, Tunnel Concentrator Address Pool (TCAP) services enabling AP communication with data center resources, and MTU status detection and reporting for tunnel validation and troubleshooting. The release addresses issues involving excessive multicast traffic causing service unresponsiveness and inaccurate tunnel transmit statistics. Security enhancements include IPSec encryption and RADIUS authentication integration, while deployment guidance highlights TCAP prerequisites for RADIUS-based environments. The document details known issues affecting network usage reporting, AP synchronization, configuration propagation, VLAN changes, and multicast ACL behavior. Feature limitations require disabling multicasting, unsupported broadcast forwarding, and ARP proxy functionality. The release also references supporting deployment and management documentation for Universal Compute Platform, Extreme Platform ONE, and ExtremeCloud management environments, providing troubleshooting and maintenance guidance for production deployments.

General Release Information

New Features on page 5
Resolved Issues on page 6
Known Issues on page 7
Feature Limitations in v26.01.01 on page 7
Documentation on page 7
Help and Support on page 8

New Features

All of the features that are introduced with this version are targeted exclusively to deployments that are managed by Extreme Platform ONE™ Networking.

Extreme Platform ONE Networking as a Management Application

This release of Tunnel Concentrator introduces support for Extreme Platform ONE Networking as a management application for tunnel provisioning. Extreme Platform ONE Networking supports the same feature set that is supported in ExtremeCloud™ IQ (Classic), but in a streamlined interface that also includes AI integration using Extreme Agent ONE™ Coworker.

To use Extreme Platform ONE Networking, you must select the **Managed by ExtremeCloud** option from the Tunnel Concentrator user interface.

Secure Tunneling with IPSec

Tunnel Concentrator deployments that are managed by Extreme Platform ONE Networking support IPSec-encrypted tunneling. To deploy this feature, select the **Secure Connection (IPSec)** setting within the **Tunnel Concentrator Service** configuration. When this option is selected, IPSec encryption is added to the GRE headers.

RADIUS Authentication Support

Tunnel Concentrator deployments that are managed by Extreme Platform ONE Networking support the use of a RADIUS server for client authentication. To deploy this option, you must configure the following:

- A RADIUS server that is provisioned using Extreme Platform ONE Networking. You must apply the server to the SSID that contains the Tunnel Concentrator configuration.
- A Tunnel Concentrator Address Pool (TCAP). The pool allows APs to communicate with back-end RADIUS servers within the data center.

Tunnel Concentrator Address Pool (TCAP)

The **Tunnel Concentrator Service** configuration on Extreme Platform ONE Networking includes an option to configure a pool of addresses that you can assign to clients that use the service. This feature gives APs the ability to communicate with any back-end servers that are located within the Data Center. This feature is required if you are deploying a RADIUS server with Tunnel Concentrator.

MTU Status Detection and Reporting

Tunnel Concentrator deployments that are managed by Extreme Platform ONE Networking support MTU status detection. With this feature, the management application monitors MTU statuses in tunnels between cloud APs and Tunnel Concentrator. If any MTU mismatches are detected, admins are alerted so that they can make the necessary corrections.

Resolved Issues

Table 1: Resolved Issues

Issue	Description
CFD-16364	Resolved issue that was causing Tunnel Concentrator to become unresponsive with excessive multicast traffic being seen.
CFD-16486	Closed issue where Tunnel Concentrator was reporting transmit packets for inactive tunnels. This is expected behavior as tunnels do not maintain a current state up or down status.
CFD-16687	Resolved issue where clients connected to the same SSID across different APs were unable to communicate with each other using Tunnel Concentrator. This was caused by an L2 forwarding problem within the subnet.
CFD-16801	Resolved issue where ExtremeCloud™ IQ was sending an incomplete AP configuration to Tunnel Concentrator if the configuration was pushed to many APs at once resulting in some APs being left out of the configuration.
CFD-17234	Resolved issue where ExtremeCloud IQ sent an empty AP list to Tunnel Concentrator if the network policy had no SSID.
CFD-17483	Resolved issue where Tunnel Concentrator did not create all all the configured tunnels. Some APs were missing from the TC configuration after a config push.
CFD-17737	Resolved issue where Tunnel Concentrator became unresponsive approximately ten minutes after a config push from ExtremeCloud IQ. The HSRP virtual MAC had been aging out of the layer 2 FIB table on BVI interfaces. As a result, reply packets were dropped.
CFD-18148	Resolved issue causing periodic packet loss (about every 60 seconds) on the backup Tunnel Concentrator's VRRP IP address. It was caused by a problem in how the secondary unit handled broadcast traffic.

Known Issues

Table 2: 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-18164	Adding a new AP to the network does not automatically sync to Tunnel Concentrator. *Workaround*: When you add APs, manually push a complete configuration to the Tunnel Concentrator.
CFD-18411	Primary Tunnel Concentrator does not dynamically learn or update when an AP's IP address changes.
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-242	An issue has been observed where upgrading Tunnel Concentrator and then making changes, RX and TX counters do not reflect changes.
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. *Workaround*: Multicasting is not supported in this release. Disable all multicasts.

Feature Limitations in v26.01.01

Tunnel Concentrator v26.01.01 has the following feature limitations:

- **Multicasting**—Multicasting is not supported in this release. The **Permitted Multicast Address** (for Extreme Platform ONE and ExtremeCloud IQ) and **Multicast Bridging** (for ExtremeCloud IQ Controller) settings must be left disabled.
- **Block Non-Essential Broadcasts**—It is not supported in this release to disable this setting. When this setting is enabled, Tunnel Concentrator blocks all broadcasts except DHCP and ARP. This is the default setting.
- **ARP Proxy**—It is not supported in this release to disable ARP Proxy. This setting is enabled by default.

Documentation

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

Tunnel Concentrator Documents

- *Extreme 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.
- Extreme Platform ONE Networking User Guide—If you are deploying Extreme Platform ONE Networking as your management application, refer to this guide for Extreme Platform ONE Networking 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.
- *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.

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.