ExtremeCloud SD-WAN Appliance Firmware ipe 24.5.6 Release Notes

New Features, Improvements, and Known Issues

9039321-03 Rev. AA

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/

Abstract

This release notes document for ExtremeCloud™ SD-WAN Appliance Firmware ipe 24.5.6 describes resolved defects, known issues, and operational guidance for enterprise SD-WAN appliances managed through ExtremeCloud SD-WAN Orchestrator. The release introduces no new features and instead concentrates on stability, correctness, and performance under production traffic conditions. Addressed issues include correcting false Internet path state reporting when using L3 WAN breakout without overlays, resolving incomplete password change workflows in the Orchestrator UI, and ensuring successful configuration deployment during onboarding when WAN1 is disabled. Additional fixes improve handling of WAN resource exhaustion, DPI object cleanup behavior, alarm accuracy, BGP advertisement of management IPs, and throughput limitations on specific appliance models. Known issues document conditions that may trigger repeated WAN resource, DPI, ISIS adjacency, or end-to-end connectivity alarms under high latency, packet loss, or heavy traffic scenarios, with guidance such as BFD timeout tuning to mitigate impact. The content targets experienced network administrators and support engineers responsible for deployment, monitoring, and troubleshooting of SD-WAN appliance firmware in large-scale or high-load environments.

General Release Information

Current Release: ipe 24.5.6

New Features in ipe 24.5.6

There are no new features in this ExtremeCloud SD-WAN Appliance Firmware ipe 24.5.6 release.

Addressed Issues in ipe 24.5.6

Addressed Issue in ipe 24.5.6

Issue ID	Description
CFD-16075	DWS may show the Internet path as *Impossible* when an L3 WAN interface is used for Internet breakout with WSG or DTI rules and no overlay is configured. This occurred because the Internet IBA was not mounted on the interface.
CFD-15967	The option to change the appliance password was shown in the Orchestrator interface but the password update could not be completed. This could have caused confusion for users. This issue was resolved by correcting the interface behavior to match the supported functionality.
CFD-14321	During appliance onboarding, configuration deployment could fail when the WAN1 interface was disabled, even though the appliance successfully connected to the Orchestrator. As a result, the configuration status was shown as failed. This issue was resolved, and configuration deployment now completes successfully even when WAN1 is disabled.

Known Issues in ipe 24.5.6

Known Issues in ipe 24.5.6

Issue ID	Description
CFD-16526	The WAN Out of Resource and Out of Context alarm may be triggered repeatedly under high traffic conditions. This behavior can occur when inactive DPI entries are not cleared quickly enough, causing the number of DPI objects to reach the platform limit. When the alarm is active, users may experience degraded network performance such as slowness or intermittent disconnections.
CFD-15990	In Fabric deployments using WAN links with high latency or packet loss (for example, wireless connectivity), ISIS adjacency loss alarms may be observed intermittently even when the IPsec tunnel remains up. This behavior can occur due to aggressive BFD timeout settings, which may cause routing flaps under degraded link conditions. Increasing the BFD timeout value may help stabilize adjacent in such environments.
CFD-14353	Appliances may report repeated End-to-End Connectivity Lost alarms even though site connectivity and user traffic are not affected. This behavior may occur due to incorrect ingress connectivity state detection for certain remote NAP paths, resulting in false alarm indications.

Global Support

By Phone: +1 800-998-2408 (toll-free in U.S. and Canada)

For the toll-free support number in your country:
https://extremeportal.force.com/

By Email: support@extremenetworks.com

By Web: https://extremeportal.force.com/

For information regarding the latest software release, recent release note revisions and documentation, or if you require additional assistance, please visit the Extreme Networks Support website.