www.zyxel.com

Release Note

USG LITE 60AX

Version V2.20(ACIP.0)C0

July 21, 2025

Contents

USG LITE 60AX

Release V2.20(ACIP.0)C0

Release Note

Date: July 21, 2025

Supported Platforms:

USG LITE 60AX

Versions:

Version: V2.20(ACIP.0) | 2025-07-17 15:12:28

Read Me First

1. Please download or upgrade to the latest Nebula Mobile for registering your USG LITE 60AX security router.
2. The system default configuration is summarized as below:
    a. The default device administration username is "admin", and the password can be found on the device back label (reminding that the login credentials will be re-assigned by Nebula after registering your device)
    b. Default LAN IP is 192.168.168.1
3. Please **DO NOT** turn off the power during the firmware upgrade. Please wait until the device reboots and the LED light display steady green.
4. To reset device to system default, user could press RESET button for 5 seconds and the device would reset itself to system default configuration and then reboot.

Design Limitations:

Note: Design Limitations described the system behavior or limitations in current version. They will be created into knowledge base.

1. Please be advised that you cannot configure the USG LITE 60AX as a repeater AP in the Smart MESH scenario.
2. The USG LITE 60AX does not report Ethernet client's intra-LAN traffic usage.
3. When you configured the first SSID to 5Ghz band only and the second SSID to 2.4Ghz band only, the WLAN security will turn to "Open" during the device boot up process (~3 mins) and wireless clients cannot obtain IP. Upon device booting up completely, the WLAN security will again turn to original setting e.g. WPA3.

Known Issues:

Note: These known issues listed below represent are not fixed in the current firmware release. And we already plan to fix them in the future firmware release.

Features: V2.20(ACIP.0)C0

Modifications in V2.20(ACIP.0)C0 - 2025/07/21

Feature

1. [New Feature] Support Traffic Log Archiving to SecuReporter. (Nebula Pro Pack or Elite Pack license is required)
2. [New Feature] Added Captive Portal and authentication utilizing Microsoft Entra ID for USG LITE 60AX.
3. [Feature Change] The system default setting now disables the FTP server. As a result, the device cannot be upgraded using the ZON Utility.

Bug Fix

1. [Bug Fix] eITS#250100928
   Fix: Specific application patrol setting caused the UTM to malfunction.
2. [Bug Fix] eITS#250200457
   Fix: USG Lite60AX device entered a boot loop after the firmware upgrade.
3. [Bug Fix] eITS#250101745
   Fix: USG LITE 60AX site to site VPN with IKEv1 rule missing after rekey.
4. [Bug Fix] eITS#250200222
   Fix: VPN routing is not functioning correctly after upgrading to the V2.10 FCS firmware.
5. [Bug Fix] eITS#250501449
   Fix: Site-2-Site connection not working after a period of time.

Features: V2.10(ACIP.0)C0

Modifications in V2.10(ACIP.0)C0 - 2025/01/03

Feature

1. [Enhancement] Improving PPPoE WAN type throughput and reducing latency by hardware NAT (HNAT) acceleration.
2. [Enhancement][eITS#240601148] Avoid packet acceleration by HNAT when SSID rate limit is turned on.
3. [Enhancement][eITS#240400978, 240401657] Hint user who is blocked by traffic management and threat management features.
4. [Enhancement][eITS#240400195] Support FTP active mode.

Bug Fix

1. [Bug Fix] eITS#240900059
   Fix: PPPoE ping latency is not stable during the Speedtest.
2. [Bug Fix] eITS#240901869
   Fix: Blocking ICMP from any source to the destination device will block the device's internet session.
3. [Bug Fix] eITS#240701525
   Fix: Remote Access VPN configuration file missing.
4. [Bug Fix] eITS#240901364
   Fix: Nebula shows that the upload and download values are reversed.
5. [Bug Fix] eITS#240700533
   Fix: Remote VPN routing issue.
6. [Bug Fix] eITS#240900158
   Fix: GeoIP incoming rule blocking outgoing traffic.
7. [Bug Fix] eITS#241100119
   Fix: Remote VPN internet issue.
8. [Bug Fix] eITS#241200285
   Fix: Logs not being cleaned up regularly cause a memory leak.

Common vulnerabilities and Exposures

V2.10 Patch0 C0 is no longer vulnerable to the following CVE References:

- CVE-2024-3596
- CVE-2024-12398

Features: V2.00(ACIP.4)C0

Modifications in V2.00(ACIP.4)C0 - 2024/09/09

Common vulnerabilities and Exposures

V2.00 Patch4 C0 is no longer vulnerable to the following CVE References:

- CVE-2024-7261

Features: V2.00(ACIP.3)C0

Modifications in V2.00(ACIP.3)C0 - 2024/08/01

Feature

1. [New Feature] Added support for IPTV.
   Note: Depending on IPTV feature configuration, the security features including Firewall & Threat Management bypass inspecting traffic flowing through the IPTV Port (port 1).

Bug Fix

1. [Bug Fix] eITS#240501483
   Fix: VPN connection shows incorrect Last Heartbeat time after device startup.
2. [Bug Fix] eITS#240601085
   Fix: Incorrect PPPoE configuration causes device to reboot every 15 minutes.
3. [Bug Fix] eITS#240700519
   Fix: Remote access VPN fails to establish after security router change to the other Nebula site.
4. [Bug Fix] eITS#240700554
   Fix: Remote access VPN clients experience low throughput when using PPPoE WAN.

Common vulnerabilities and Exposures

V2.00 Patch3 C0 is no longer vulnerable to the following CVE References:

- CVE-2024-6387

Features: V2.00(ACIP.2)C0

Modifications in V2.00(ACIP.2)C0 - 2024/06/07

First release.