

Release Note

Important Notice:

This release includes security enhancements for cloud management. Downgrading to an earlier firmware version may cause cloud authentication, cloud management, or cloud-based firmware upgrade features to become unavailable. If issues occur after a downgrade, please contact technical support.

Version Info:

1. Firmware Version: 1.20.3 Build 20260717 Rel.17075

2. Applied Model:

- a) SG5452XMPP(UN) v1.0
- b) SG5452XMPP(UN) v1.6
- c) SG5452XMPP(UN) v1.20
- d) SG5452XMPP(UN) v1.26
- e) SG5452XMPP(IN) v1.28

3. Minimum FW Version for Update:

- a) UN v1.0: 1.0.0 Build 20250301 Rel.54304
- b) UN v1.6: 1.0.0 Build 20250301 Rel.54304
- c) UN v1.20: 1.0.0 Build 20250301 Rel.54304
- d) UN v1.26: 1.0.0 Build 20250301 Rel.54304
- e) IN v1.28: 1.0.0 Build 20250301 Rel.54304

4. Recommended Omada Controller version: 6.2.14

5. Recommended Omada App version: N/A

6. For downloading any firmware version, please refer to [Omada Download Center](#).

New Features:

1. Added support for a high-strength password hashing algorithm, improving the security of password data.

Enhancements:

1. Optimized the authentication and configuration delivery mechanisms between the device and Cloud-Based/Local Controller.
2. Optimized the authentication mechanism when devices are initially onboarded to the cloud management platform.

Bug Fixed:

1. Fixed an issue where, in scenarios with a large number of LAG/LACP groups, some member ports occasionally failed to aggregate or became blocked during firmware upgrades or master/backup switchover.

Additional Information:

1. SHA-256 Value:

192b29795481c2162abdaf595e147a287cef9d3761feb6589be2927c3d8aeec4

2. SHA-512 Value:

12dbb7b58a14df63a94c730543dd8501830aad20c1cab11da43cd0d67b384e69
2908d9ad5664c048b89a82f0f45d3c5fd39db368cd7c9a0c14105fdbd971c5d4