Grandstream Networks, Inc.

Wi-Fi Access Points
GWN76xx – User Manual

WELCOME

Thank you for purchasing Grandstream GWN76XX Enterprise Wireless Access Point.

The GWN7630/GWN7615/GWN7610 are high-performance 802.11ac Wi-Fi access points for small to medium sized businesses, multiple floor offices, commercial locations, and branch offices. GWN7630 and GWN7615/GWN7610 offers respectively a Dual-Band 4×4:4 MIMO and a 3×3:3 MIMO technology and a sophisticated antenna design for maximum network throughput and expanded Wi-Fi coverage range. To ensure easy installation and management, the GWN7630/GWN7615/GWN7610 uses a controller-less distributed network management design in which the controller is embedded within the product's Web user interface. This allows each access point to manage a network of up to 50 GWN76XX independently without needing separate controller hardware/software and without a single point-of-failure.

The GWN7600 is a mid-tier Wave-2 802.11ac Wi-Fi access point for small to medium sized businesses, multiple floor offices, commercial locations, and branch offices. The GWN7600LR Outdoor Long-range 802.11ac Wave-2 Wi-Fi Access Point is designed to provide extended coverage support. Ideal for outdoor Wi-Fi solutions thanks to its waterproof casing and heat resistant technology. The GWN7600/GWN7600LR come equipped with dual-band, 2×2:2 MU-MIMO with beam-forming technology and a sophisticated antenna design for maximum network throughput and expanded Wi-Fi coverage range for both Indoor (GWN7600) and Outdoor deployment (GWN7600LR).

To ensure easy installation and management, the GWN7600/GWN7600LR uses a controller-less distributed network management design in which the controller is embedded within the product's web user interface. This allows each access point to manage a network of up to 30 GWN76XX series APs independently without needing separate controller hardware/software and without a single point-of-failure. This wireless access point can be paired with any third-party routers as well as Grandstream GWN series routers. With support for advanced QoS, low-latency real-time applications, 450+ concurrent client devices per AP and dual Gigabit network ports with PoE, the GWN7600/GWN7600LR is an ideal Wi-Fi access point for medium wireless network deployments with medium-to-high user density.

The GWN7630LR is an outdoor long-range Wi-Fi access point for medium to large businesses and enterprises who need to provide long-range coverage in both indoor and outdoor spaces. It offers weatherproof casing and heat resistant technology, dual-band 4×4:4 MU-MIMO technology, and a sophisticated antenna design for maximum network throughput that supports 200+ clients and an expanded 300-meter coverage range. the GWN7630LR is an ideal outdoor Wi-Fi access point for enterprises, multiple floor offices, warehouses, hospitals, schools and more.

The GWN7625 and GWN7605/GWN7605LR are a high-performance-to-price 802.11ac Wave-2 Wi-Fi access points for small to medium sized businesses, multiple floor offices, commercial locations, and branch offices. They offers respectively dual-band 4×4:4 and 2×2:2 MU-MIMO with beam-forming technology and a sophisticated antenna design for maximum network throughput and expanded Wi-Fi coverage range. To ensure easy installation and management, the GWN7625 and GWN7605/GWN7605LR uses a controller-less distributed network management design in which the controller is embedded within the product's web user interface. With a slight difference in the GWN7605LR which is an outdoor Wi-Fi access point that offers extended coverage range support for both indoor and outdoor deployments. All products are supported by GWN.Cloud and GWN Manager, Grandstream's cloud and on-premises Wi-Fi management platforms. Excellent Wi-Fi APs for voice-over-Wi-Fi deployments and offer a seamless connection with Grandstream's Wi-Fi-capable IP phones. With support for advanced QoS, low-latency real-time applications, mesh networks, captive portals, 100+ concurrent clients for the GWN7605/7605LR and 200+ concurrent clients for the GWN7625 and dual Gigabit network ports with PoE/PoE+, they are ideal Wi-Fi access points for medium wireless network deployments with medium user density.

The GWN7660/GWN7660LR is a high-efficiency, enterprise-grade 802.11ax Wi-Fi 6 access point, ideal for small-to-medium sized businesses, multiple floor buildings, residential settings, and commercial locations. It offers dual-band 2×2:2 MU-MIMO with DL/UL OFDMA technology and a sophisticated antenna design for maximum network throughput and expanded Wi-Fi coverage range. To ensure easy installation and management, the GWN7660/GWN7660LR uses a controller-less distributed network management design in which the controller is embedded within the product's Web user interface. GWN7660/GWN7660LR is also supported by GWN.Cloud and GWN Manager, Grandstream's cloud and on-premises Wi-Fi management platform. It is the ideal Wi-Fi AP for voice-over-Wi-Fi deployments and offers a seamless connection with Grandstream's Wi-Fi capable IP phones. With support for advanced QoS, low-latency real-time applications, mesh networks, captive portals, 256 concurrent clients per AP and dual Gigabit network ports with PoE/PoE+, GWN7660/GWN7660LR is an ideal Wi-Fi access point for medium wireless network deployments with medium-to-high user density.

The GWN7664 is a powerful, enterprise-grade 802.11ax Wi-Fi 6 access point, ideal for small-to-medium sized businesses, multiple floor buildings, residential settings, and commercial locations. It offers dual-band 4×4:4 MUMIMO with DL/UL OFDMA technology and a sophisticated internal antenna design for stronger anti-interference, more stable connection, maximum network throughput and expanded Wi-Fi cover age range. The GWN7664 is supported by GWN.Cloud and GWN Manager, Grandstream's cloud and on-premises Wi-Fi management platform that and makes managing your network or

several networks across multiple locations easier than ever before. It also uses a controller-less network management architecture in which the controller is embedded within the product's web user interface for easy administration of locally deployed Wi-Fi Aps. The GWN7664 is the ideal Wi-Fi AP for voice-over-Wi-Fi deployments and offers a seamless connection with Grandstream's Wi-Fi capable IP phones. With support for advanced QoS, low latency real-time applications, mesh networks, captive portals, 750 concurrent clients and dual Gigabit network ports with PoE/PoE+, the GWN7664 is an ideal Wi-Fi access point for business-grade wireless network deployments with medium-to-high user density. While the long range version GWN7664LR has even better coverage range up to 300 meters with IP66-level weatherproof capability when installed vertically for outdoor usage.

The GWN7624 is a small and compact in-wall Wi-Fi access point designed for small-to-medium-sized businesses, offices, residential and commercial locations, hotels, and more. It provides three Gigabit network ports to provide IP phones, IPTV, computers, and similar devices with Ethernet while also providing and uplink Gigabit network port with PoE/PoE+. While the GWN7602 has 3x 100Mbit Ports and an uplink Gigabit network port with PoE/PoE+. To ensure easy installation and management, the GWN7602 supports to be managed by GWN series APs (except GWN7602) with embedded controller or GWN Management Systems (GWN.Cloud / GWN Manager).

Caution

Changes or modifications to this product not expressly approved by Grandstream, or operation of this product in any way other than as detailed by this User Manual, could void your manufacturer warranty.

Note

"Out of the box" Grandstream Access Points are not affected by this issue. APs with old firmware are only affected after changing into client-bridge mode. Please refer to our white paper of "WPA Security Vulnerability" here.

PRODUCT OVERVIEW

Technical Specifications

Wi-Fi Standards	IEEE 802.11 a/b/g/n/**ac**
Antennas	**Internal Antennas:** 2x 5GHz + 2x (5GHz & 2.4GHz) **2.4GHz**, gain 3dBi; **5GHz**, gain 5dBi
Wi-Fi Data Rates	**2.4GHz:** **IEEE 802.11n**: 6.5Mbps to 300Mbps **IEEE 802.11b**: 1, 2, 5.5, 11 Mbps **IEEE 802.11g**: 6, 9, 12, 18, 24, 36, 48, 54 Mbps **5GHz:** **IEEE 802.11ac**: 6.5 Mbps to 1733 Mbps **IEEE 802.11n**: 6.5Mbps to 600Mbps **IEEE 802.11a**: 6, 9, 12, 18, 24, 36, 48, 54 Mbps *Actual throughput may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment and mix of devices in the network*
Frequency Bands	**2.4GHz Radio:** 2412 - 2484 MHz **5GHz Radio:** 5180 - 5825 MHz *Not all frequency bands can be used in all regions*
Channel Bandwidth	**2.4G**: 20 and 40 MHz **5G**: 20, 40 and 80 MHz
Wi-Fi and System Security	WEP, WPA/WPA2-PSK, WPA/WPA2 Enterprise (TKIP/AES); WPA3, anti-hacking secure boot and critical data/control lockdown via digital signatures, unique security certificate and random default password per

	device
MU-MIMO	**2×2:2** 2.4GHz (**MIMO**) **4×4:4** 5GHz (**MU-MIMO**)
Coverage Range	Up to **100 meters** *coverage range can vary based on environment*
Maximum TX Power	**5G**: 25dBm **2.4G**: 23dBm *Maximum power varies by country, frequency band and MCS rate*
Receiver Sensitivity	**2.4GHz** **802.11b:** -96dBm@1Mbps, -88dBm@11Mbps; **802.11g:** -93dBm @6Mbps, -75dBm@54Mbps; **802.11n 20MHz:** -73dBm @MCS7; **802.11n 40MHz:**-70dBm @MCS7 @MCS11 **5GHz** **802.11a:** -92dBm @6Mbps, -74dBm @54Mbps; **802.11n 20MHz:** -74dBm @MCS7; **802.11n 40MHz:**-71dBm @MCS7 **802.11ac 20MHz:** -67dBm@MCS8; **802.11ac: HT40:**- 63dBm @MCS9; **802.11ac 80MHz:** -59dBm @MCS9
SSIDs	**16 SSIDs total**, 8 per radio (2.4GHz & 5GHz)
Concurrent Clients	Up to **200**
Network Interfaces	**1x** 10/100/1000M uplink Ethernet port **with PoE/PoE+** **2x** 10/100/1000M Ethernet port **with PSE** **1x** 10/100/1000M Ethernet port
Auxiliary Ports	1x Reset Pinhole
Mounting	In-wall mountable
LEDs	1 tri-color LEDs for device tracking and status indication
Network Protocols	IPv4, IPv6, 802.1Q, 802.1p, 802.1x, 802.11e/WMM
QoS	802.11e/WMM, VLAN, TOS
Network Management	Embedded controller can manage up to 30 local GWN APs GWN.Cloud offers a free cloud management platform for unlimited GWN APs GWN Manager offers premise-based software controller for up to 3,000 GWN APs
Auto Power Saving	Self-power adaptation upon auto detection of PoE or PoE+
Power and Green Energy Efficiency	Support 802.3az PoE 802.3af/ 802.3at; PSE Maximum Output Per Port: 6W; Maximum Power Consumption: 25W
Environmental	Operation:-10°Cto 50°C Storage: -30°C to 60°C Humidity: 5% to 95% Non-condensing
Physical	Unit Dimension: 135mm(L)x86mm(W)x38.5mm(H) Entire Package Dimension: 176mm(L)x118.5mm(W)x65mm(H)
Package Content	GWN7624 In-Wall Wireless AP

	4x Screws(KB 3.5*26) Quick Installation Guide
Compliance	FCC, CE, RCM, IC, UKCA

GWN7624 Technical Specifications

Wi-Fi Standards	IEEE 802.11 a/b/g/n/ac/ax
Antennas	4 dual band external antennas **2.4GHz**, gain 3.5dBi **5 GHz**, gain 3.5dBi
Wi-Fi Data Rates	**2.4GHz:** **IEEE 802.11ax**: 8 Mbps to 1147 Mbps IEEE **IEEE 802.11n**: 6.5Mbps to 300Mbps **IEEE 802.11b**: 1, 2, 5.5, 11 Mbps **IEEE 802.11g**: 6, 9, 12, 18, 24, 36, 48, 54 Mbps **5GHz:** **IEEE 802.11ax**: 8 Mbps to 2402 Mbps IEEE **IEEE 802.11ac**: 6.5 Mbps to 1733 Mbps **IEEE 802.11n**: 6.5Mbps to 600Mbps **IEEE 802.11a**: 6, 9, 12, 18, 24, 36, 48, 54 Mbps ***Actual throughput may vary depending on many factors including environmental conditions, distance between devices, radio* *interference in the operating environment and mix of devices in the network*
Frequency Bands	**2.4GHz Radio:** 2412 - 2484 MHz **5GHz Radio:** 5180 - 5825 MHz **Not all frequency bands can be used in all regions*
Channel Bandwidth	**2.4G**: 20 and 40 MHz (x4) **5G**: 20, 40 and 80 MHz (x4)
Wi-Fi and System Security	WEP, WPA/WPA2-PSK, WPA/WPA2 Enterprise (TKIP/AES); WPA3, anti-hacking secure boot and critical data/control lockdown via digital signatures, unique security certificate and random default password per device
MU-MIMO	4×4:4 **2.4GHz** 4×4:4 **5GHz**
Coverage Range	Up to 300 meters **coverage range can vary based on environment*
Maximum TX Power	**5G**: 25dBm **2.4G**: 26dBm **Maximum power varies by country, frequency band and MCS rate*
Receiver Sensitivity	**2.4GHz** 802.11b: -96dBm@1Mbps, -88dBm@11Mbps; 802.11g: -93dBm @6Mbps, -75dBm@54Mbps; 802.11n 20MHz: -73dBm @MCS7; 802.11n 40MHz:-70dBm @MCS7 802.11ax 20MHz: -64dBm @ MCS11; 802.11ax 40MHz: -63dBm @MCS11 **5GHz** 802.11a: -92dBm @6Mbps, -74dBm @54Mbps; 802.11n 20MHz: -74dBm @MCS7; 802.11n 40MHz:-71dBm @MCS7 802.11ac 20MHz: -67dBm@MCS8; 802.11ac: HT40:- 63dBm @MCS9; 802.11ac 80MHz: -59dBm @MCS9 802.11ax 20MHz: -64dBm @ MCS11; 802.11ax 40MHz: -62dBm @MCS11;802.11ax 80MHz: -59dBm @MCS11

SSIDs	32 SSIDs total, 16 per radio (**2.4GHz & 5GHz**)
Concurrent Clients	750+
Network Interfaces	1x 1G Port and 1x 2.5G Port, support 3.5Gbps aggregate wired throughout
Auxiliary Ports	1x Reset Pinhole
Mounting	Wall mount or pole mount, kits included
LEDs	1 tri-color LEDs for device tracking and status indication
Network Protocols	IPv4, IPv6, 802.1Q, 802.1p, 802.1x, 802.11e/WMM, 802.11h
QoS	802.11e/WMM, VLAN, TOS
Network Management	Embedded controller can manage up to 50 local GWN APs GWN.Cloud offers a free cloud management platform for unlimited GWN APs GWN Manager offers premise-based software controller for up to 3,000 GWN APs
Auto Power Saving	Self-power adaptation upon auto detection of PoE or PoE+
Power and Green Energy Efficiency	PoE 802.3af/ 802.3at; Maximum Power Consumption: 18W
Environmental	Operation:-30°Cto 60°C Storage: -30°C to 60°C Humidity: 10% to 90% Non-condensing
Physical	Unit Dimension: 562.3mm(L)x140mm(W)x44.9mm(H); Unit + Mounting Kits Dimension: 562.3mm(L)x140mm(W)x66.9mm(H); Entire Package Dimension: 260mm(L)x218.5mm(W)x108mm(H);
Package Content	GWN7664LR 802.11ax Wireless AP, Mounting Kits, Quick Installation Guide
Weatherproof Grade	IP66-level weatherproof capability when installed vertically
Compliance	FCC, CE, RCM, IC, UKCA

GWN7664LR Technical Specifications

Wi-Fi Standards	IEEE 802.11 a/b/g/n/ac
Antennas	6 single frequency internal antennas **2.4GHz**, gain 3.5dBi **5GHz**, gain 4.5dBi
Wi-Fi Data Rates	**2.4GHz:** IEEE 802.11n: 6.5Mbps to 300Mbps IEEE 802.11b: 1, 2, 5.5, 11 Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps **5GHz:** IEEE 802.11ac: 6.5 Mbps to 1733 Mbps IEEE 802.11n: 6.5Mbps to 600Mbps IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps **Actual throughput may vary depending on many factors including environmental conditions, distance*

	between devices, radio *interference in the operating environment and mix of devices in the network*
Frequency Bands	**2.4GHz Radio:** 2412 - 2484 MHz **5GHz Radio:** 5180 - 5825 MHz **Not all frequency bands can be used in all regions*
Channel Bandwidth	**2.4GHz:** 20 and 40 MHz **5GHz:** 20, 40 and 80 MHz
Wi-Fi and System Security	WEP, WPA/WPA2-PSK, WPA/WPA2 Enterprise (TKIP/AES); WPA3, anti-hacking secure boot and critical data/control lockdown via digital signatures, unique security certificate and random default password per device
MIMO	2×2:2 **2.4GHz**(MIMO) 4×4:4 **5GHz**(MU-MIMO)
Maximum TX Power	**2.4GHz**: 23dBm **5GHz**: 25dBm **Maximum power varies by country, frequency band and MCS rate*
Receiver Sensitivity	**2.4GHz** 802.11b: -96dBm@1Mbps, -88dBm@11Mbps; 802.11g: -93dBm @6Mbps, -75dBm@54Mbps; 802.11n 20MHz: -73dBm @MCS7; 802.11n 40MHz:-70dBm @MCS7 **5GHz** 802.11a: -92dBm @6Mbps, -74dBm @54Mbps; 802.11n 20MHz: -74dBm @MCS7; 802.11n 40MHz:-71dBm @MCS7 802.11ac 20MHz: -67dBm@MCS8; 802.11ac: HT40:- 63dBm @MCS9; 802.11ac 80MHz: -59dBm @MCS9
SSIDs	16 SSIDs total, 8 per radio (**2.4GHz & 5GHz**)
Concurrent Clients	200
Network Interfaces	2x autosensing 10/100/1000 Base-T Ethernet Ports
Auxiliary Ports	1x Reset Pinhole, 1x Kensington lock
Mounting	Indoor wall mount or ceiling mount, kits included
LEDs	3 tri-color LEDs for device tracking and status indication
Network Protocols	IPv4, IPv6, 802.1Q, 802.1p, 802.1x, 802.11e/WMM, 802.11h
QoS	802.11e/WMM, VLAN, TOS
Network Management	Embedded controller can manage up to 30 local GWN APs GWN.Cloud offers a free cloud management platform for unlimited GWN APs GWN Manager offers premise-based software controller for up to 3,000 GWN APs
Auto Power Saving	Self-power adaptation upon auto detection of PoE or PoE+
Power and Green Energy Efficiency	Supports 802.3az PoE 802.3af/ 802.3at Maximum Power Consumption: <13W
Environmental	Operation: 0°C to 40°C Storage: -10°C to 60°C

	Humidity: 10% to 90% Non-condensing
Physical	Unit Dimension: 205.3mm(L)x205.3mm(W)x45.9mm(H); Unit Weight: 530g; Entire Package Dimension: 258mm(L)x247mm(W)x86mm(H); Entire Package Weight: 897.3g
Package Content	GWN7625 802.11ac Wave-2 Wireless AP, Mounting Kits, Quick Installation Guide
Compliance	FCC, CE, RCM, IC, UKCA

GWN7625 Technical Specifications

Wi-Fi Standards	IEEE 802.11 a/b/g/n/ac/ax.
Antennas	8 individual internal antennas, 4 per band 2.4GHz, gain 3dBi / 5 GHz, gain 4dBi
Wi-Fi Data Rates	**5G:** IEEE 802.11ax: 8 Mbps to 2402 Mbps IEEE 802.11ac: 6.5 Mbps to 1733 Mbps IEEE 802.11n: 6.5 Mbps to 600 Mbps IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps **2.4G:** IEEE 802.11ax: 8 Mbps to 1147 Mbps IEEE 802.11n: 6.5 Mbps to 600Mbps IEEE 802.11b: 1, 2, 5.5, 11Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps *Actual throughput may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment and mix of devices in the network.*
Frequency Bands	2.4GHz Radio: 2412 – 2484 MHz 5GHz Radio: 5180 – 5825 MHz *Not all frequency bands can be used in all regions
Channel Bandwidth	2.4G: 20 and 40 MHz (x4) 5G: 20, 40 and 80 MHz (x4)
Wi-Fi and System Security	WEP, WPA/WPA2-PSK, WPA/WPA2 Enterprise (TKIP/AES); WPA3, anti-hacking secure boot and critical data/ control lockdown via digital signatures, unique security certificate and random default password per device
MIMO	4×4:4 2.4GHz 4×4:4 5GHz

Coverage Range	Up to 175 meters *Coverage range can vary based on environment
Maximum TX Power	5G: 25dBm 2.4G: 26dBm *Maximum power varies by country, frequency band and MCS rate*
Receiver Sensitivity	**2.4G** 802.11b: -99dBm@1Mbps, -91dBm@11Mbps; 802.11g: -94dBm @6Mbps, -78dBm@54Mbps; 802.11n 20MHz: -75dBm @MCS7; 802.11n 40MHz:-71dBm @MCS7; 802.11ax 20MHz: -64dBm @ MCS11; 802.11ax 40MHz: -63dBm @MCS11 **5G** 802.11a: -95dBm @6Mbps, -77dBm @54Mbps; 802.11n 20MHz: -74dBm @MCS7; 802.11n 40MHz:-71dBm @MCS7 802.11ac 20MHz: -70dBm@MCS8; 802.11ac: HT40:- 66dBm @MCS9; 802.11ac 80MHz: -62dBm @MCS9; 802.11ax 20MHz: -64dBm @ MCS11; 802.11ax 40MHz: -62dBm @MCS11;802.11ax 80MHz: -59dBm @MCS11 *Receiver sensitivity varies by frequency band, channel width and MCS rate*
SSIDs	32 SSIDs total, 16 per radio (2.4GHz and 5GHz)
Concurrent Clients	750
Network Interfaces	1x 1G Port and 1x 2.5G Port, support 3.5Gbps aggregate wire throughput
Auxiliary Ports	1x Reset Pinhole, 1x Kensington lock
Mounting	Indoor wall mount or ceiling mount, kits included
LEDs	3 tri-color LEDs for device tracking and status indication
Network Protocols	IPv4, 802.1Q, 802.1p, 802.1x, 802.11e/WMM, 802.11h
QoS	802.11e/WMM, VLAN, TOS
Network Management	Embedded controller can manage up to 50 local GWN APs GWN.Cloud offers a free cloud management platform for unlimited GWN APs GWN Manager offers premise-based software controller for up to 3,000 GWN APs
Auto Power Saving	Self-power adaptation upon auto detection of PoE or PoE+

Power and Green Energy Efficiency	Power over Ethernet 802.3af/802.3at compliant Maximum Power Consumption: 17W.
Environmental	Operation: 0°C to 45°C Storage: -10°C to 60°C Humidity: 10% to 90% Non-condensing
Physical	Unit Dimension: 205.3mm(L)x205.3mm(W)x405.9mm(H); Unit Weight: 0.714Kg Entire Package Dimension: 258x247x86mm; Entire Package Weight: 1.06Kg
Package Content	GWN7664 802.11ax Wireless AP, Mounting Kits, Quick Start Guide
Compliance	FCC, CE, RCM, IC

GWN7664 Technical Specifications

Wi-Fi Standards	IEEE 802.11 a/b/g/n/ac/ax.
Antennas	2 dual band internal antennas 2.4GHz, gain 3dBi / 5 GHz, gain 4dBi
Wi-Fi Data Rates	**5G:** IEEE 802.11ax: 7.3 Mbps to 1201 Mbps IEEE 802.11ac: 6.5 Mbps to 867 Mbps IEEE 802.11n: 6.5Mbps to 300Mbps IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps **2.4G:** IEEE 802.11ax: 7.3 Mbps to 573.5 Mbps IEEE 802.11n: 6.5Mbps to 300Mbps IEEE 802.11b: 1, 2, 5.5, 11Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps *Actual throughput may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment and mix of devices in the network.*
Frequency Bands	2.4 GHz Radio: 2412 – 2484 GHz 5 GHz Radio: 5180-5825 GHz (FCC, IC, RCM)
Channel Bandwidth	2.4G: 20 and 40 MHz 5G: 20, 40 and 80 MHz

Wi-Fi and System Security	WEP, WPA3, WPA/WPA2-PSK, WPA/WPA2-Enterprise (TKIP/AES), anti-hacking secure boot and critical data/control lockdown via digital signatures, unique security certificate and random default password per device
MIMO	2×2:2 5GHz 2×2:2 2.4GHz
Coverage Range	575ft. (175 meters) *coverage range can vary based on environment*
Maximum TX Power	2.4G: 24 dBm 5G: 22 dBm *Maximum power varies by country, frequency band and MCS rate*
Receiver Sensitivity	**2.4G** 802.11b: -96dBm@1Mbps, -88dBm@11Mbps; 802.11g: -93dBm @6Mbps, -75dBm@54Mbps; 802.11n 20MHz: -73dBm @MCS7; 802.11n 40MHz:-70dBm @MCS7; 802.11ax 20MHz: -60dBm @ MCS11; 802.11ax 40MHz: -58dBm @MCS11 **5G** 802.11a: -92dBm @6Mbps, -74dBm @54Mbps; 802.11ac 20MHz: -67dBm@MCS8; 802.11ac: HT40:- 63dBm @MCS9; 802.11ac 80MHz: -59dBm @MCS9; 802.11ax 20MHz: -60dBm @ MCS11; 802.11ax 40MHz: -58dBm @MCS11;802.11ax 80MHz: -56dBm @MCS11 *Receiver sensitivity varies by frequency band, channel width and MCS rate*
SSIDs	32 SSIDs total, 16 per radio (2.4GHz and 5GHz)
Concurrent Clients	256
Network Interfaces	2x autosensing 10/100/1000 Base-T Ethernet Ports
Auxiliary Ports	1x Reset Pinhole, 1x Kensington lock
Mounting	Indoor wall mount or ceiling mount, kits included
LEDs	3 tri-color LEDs for device tracking and status indication
Network Protocols	IPv4, 802.1Q, 802.1p, 802.1x, 802.11e/WMM, 802.11h
QoS	802.11e/WMM, VLAN, TOS
Network Management	Embedded controller can manage up to 50 local GWN APs GWN.Cloud offers a free cloud management platform for unlimited GWN APs GWN Manager offers premise-based software controller for up to 3,000 GWN APs
Auto Power Saving	Self-power adaptation upon auto detection of PoE or PoE+

Power and Green Energy Efficiency	Power over Ethernet 802.3af/802.3at compliant Maximum Power Consumption: 9W.
Environmental	Operation: 0°C to 45°C Storage: -10°C to 60°C Humidity: 10% to 90% Non-condensing
Physical	Unit Dimension: 180.4mm x 180.4mm x 40.8mm; Unit Weight: 443g Entire Package Dimension: 228.5x220x79mm; Entire Package Weight: 774g
Package Content	GWN7660 802.11ax Wireless AP, Mounting Kits, Quick Start Guide
Compliance	FCC, CE, RCM, IC

GWN7660 Technical Specifications

Wi-Fi Standards	IEEE 802.11 a/b/g/n/ac/ax
Antennas	2 dual band external antennas 2.4GHz, gain 3.5dBi 5 GHz, gain 3.5dBi
Wi-Fi Data Rates	5G: IEEE 802.11ax: 7.3 Mbps to 1201 Mbps IEEE 802.11ac: 6.5 Mbps to 867 Mbps IEEE 802.11n: 6.5Mbps to 300Mbps IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps 2.4G: IEEE 802.11ax: 7.3 Mbps to 573.5 Mbps IEEE 802.11n: 6.5Mbps to 300Mbps IEEE 802.11b: 1, 2, 5.5, 11 Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps *Actual throughput may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment and mix of devices in the network
Frequency Bands	2.4GHz radio: 2412 – 2484 MHz 5GHz radio: 5180 – 5825 MHz *Not all frequency bands can be used in all regions.
Channel Bandwidth	2.4G: 20 and 40 MHz 5G: 20, 40 and 80 MHz
Wi-Fi and System Security	WEP, WPA/WPA2-PSK, WPA/WPA2 Enterprise (TKIP/AES); WPA3, anti-hacking secure boot and critical data/control lockdown via digital signatures, unique security certificate and random default password per device
MIMO	2×2:2 2.4GHz (MIMO) 2×2:2 5GHz (MU-MIMO))

Coverage Range	Up to 250 meters *coverage range can vary based on environment*
Maximum TX Power	5G: 26dBm 2.4G: 30dBm *Maximum power varies by country, frequency band, and MCS rate
Receiver Sensitivity	2.4G 802.11b: -99dBm@1Mbps, -90dBm@11Mbps; 802.11g: -93dBm @6Mbps, -77dBm@54Mbps; 802.11n 20MHz: -74dBm @MCS7; 802.11n 40MHz:-72dBm @MCS7; 802.11ax 20MHz: -64dBm @ MCS11; 802.11ax 40MHz: -62dBm @MCS11 5G 802.11a: -95dBm @6Mbps, -77dBm @54Mbps; 802.11ac 20MHz: -71dBm@MCS8; 802.11ac: HT40:- 67dBm @MCS9; 802.11ac 80MHz: -64dBm @ MCS9; 802.11ax 20MHz: -63dBm @ MCS11; 802.11ax 40MHz: -62dBm @MCS11;802.11ax 80MHz: -58dBm @MCS11
SSIDs	32 SSIDs total, 16 per radio (2.4GHz & 5GHz)
Concurrent Clients	256+
Network Interfaces	2× autosensing 10/100/1000 Base-T Ethernet Ports
Auxiliary Ports	1× Reset Pinhole
Mounting	Outdoor metal bar mount or wall mount, kits included
LEDs	1 tri-color LED for device tracking and status indication
Network Protocols	IPv4, 802.1Q, 802.1p, 802.1x, 802.11e/WMM, 802.11h
QoS	802.11e/WMM, VLAN, TOS
Network Management	Embedded controller can manage up to 50 local GWN APs GWN.Cloud offers a free cloud management platform for almost unlimited GWN Aps GWN Manager offers premise-based software controller for up to 3,000 GWN APs
Power and Green Energy Efficiency	POE 802.3af/ 802.3at; Maximum Power Consumption: 10.16W
Environmental	Operation: -30°C to 60°C Storage: -30°C to 70°C Humidity: 5% to 95% Non-condensing
Physical	Physical Unit Dimension: 358.3mm(L)*115mm(W)*45.3mm(H); Unit Weight: 500g Entire Package Dimension: 258 × 247× 86mm; Entire Package Weight:655.3g
Package Content	GWN7660LR 802.11ax Wave-2 Wireless AP, Mounting Kits, Quick Start Guide

Water Proof	IP66-level weatherproof capability when installed vertically
Compliance	FCC, CE, RCM, IC

GWN7660LR Technical Specifications

Wi-Fi Standards	IEEE 802.11 a/b/g/n/ac (Wave-2).
Antennas	4x 2.4 GHz, gain 4dBi, internal antenna 4x 5 GHz, gain 5dBi, internal antenna
Wi-Fi Data Rates	IEEE 802.11ac: 6.5 Mbps to 1733Mbps IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps IEEE 802.11n: 6.5Mbps to 600Mbps IEEE 802.11b: 1, 2, 5.5, 11Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps *Actual throughput may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment and mix of devices in the network.*
Frequency Bands	2.4 GHz Radio: 2412 – 2484 GHz 5 GHz Radio: 5180-5825 GHz (FCC, IC, RCM)
Channel Bandwidth	2.4G: 20 and 40 MHz 5G: 20, 40, 80 MHz
Wi-Fi and System Security	WEP, WPA3, WPA/WPA2-PSK, WPA/WPA2-Enterprise (TKIP/AES), anti-hacking secure boot and critical data/control lockdown via digital signatures, unique security certificate and random default password per device
MIMO	4×4:4 2.4GHz (MIMO) 4×4:4 5GHz (MU-MIMO)
Coverage Range	575ft. (175 meters) *coverage range can vary based on environment*
Maximum TX Power	2.4G: 27 dBm 5G: 25 dBm *Maximum power varies by country, frequency band and MCS rate*

Receiver Sensitivity	**2.4G** 802.11b: -96dBm@1Mbps, -88dBm@11Mbps; 802.11g: -93dBm @6Mbps, -75dBm@54Mbps; 802.11n 20MHz: -73dBm @MCS7; 802.11n 40MHz:-70dBm @MCS7 **5G** 802.11a: -92dBm @6Mbps, -74dBm @54Mbps; 802.11ac 20MHz: -67dBm@MCS8; 802.11ac: HT40:- 63dBm @MCS9; 802.11ac 80MHz: -59dBm @MCS9; ** Receiver sensitivity varies by frequency band, channel width and MCS rate*
SSIDs	32 SSIDs total, 16 per radio (2.4GHz and 5GHz)
Concurrent Clients	200+
Network Interfaces	2x autosensing 10/100/1000 Base-T Ethernet Ports
Auxiliary Ports	1x Reset Pinhole, 1x Kensington lock
Mounting	Indoor wall mount or ceiling mount, kits included
LEDs	3 tri-color LEDs for device tracking and status indication
Network Protocols	IPv4, 802.1Q, 802.1p, 802.1x, 802.11e/WMM, 802.11h
QoS	802.11e/WMM, VLAN, TOS
Network Management	Embedded controller in GWN7630 allows it to auto-discover, auto-provision and manage up to 50 GWN76XX in a network GWN.Cloud offers a free cloud management platform for unlimited GWN APs
Auto Power Saving	Self-power adaptation upon auto detection of PoE or PoE+
Power and Green Energy Efficiency	Power over Ethernet 802.3af/802.3at compliant Maximum Power Consumption: 16.5W; Supports 802.3 az.
Environmental	Operation: 0°C to 40°C Storage: -10°C to 60°C Humidity: 10% to 90% Non-condensing
Physical	Unit Dimension: 205.3 x 205.3 x 45.9mm; Unit Weight: 590g Unit + Mounting Kits Dimension: 205.3 x 205.3 x 50.9mm; Unit + Mounting Kits Weight: 710g Entire Package Dimension: 258 x 247 x 86mm; Entire Package Weight:930g
Package Content	GWN7630 802.11ac Wireless AP, Mounting Kits, Quick Start Guide
Compliance	FCC, CE, RCM, IC

GWN7630 Technical Specifications

Wi-Fi Standards	IEEE 802.11a/b/g/n/ac (Wave-2)
Antennas	3 dual band internal antennas 2.4GHz, gain 3dBi 5 GHz, gain 3dBi
Wi-Fi Data Rates	IEEE 802.11ac: 6.5 Mbps to 1300Mbps IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps IEEE 802.11n: 6.5 Mbps to 450 Mbps IEEE 802.11b: 1, 2, 5.5, 11Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps *Actual throughput may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment and mix of devices in the network*
Frequency Bands	2.4 GHz Radio: 2412 – 2484 MHz 5 GHz Radio: 5180-5825 MHz
Channel Bandwidth	2.4G: 20 and 40MHz 5G: 20, 40, and 80MHz
Wi-Fi and System Security	WEP, WPA3, WPA/WPA2-PSK, WPA/WPA2 Enterprise, anti-hacking secure boot and critical data/control lockdown via digital signatures, unique security certificate and random default password per device
MIMO	3×3:3 2.4G(MIMO) 3×3:3 5G(MU-MIMO)
Coverage Range	Up to175 meters *coverage range can vary based on environment*
Maximum TX Power	**2.4G:** 26 dBm **5G:** 24 dBm
Receiver Sensitivity	**2.4G** 802.11b: -96dBm@1Mbps, -88dBm@11Mbps; 802.11g: -93dBm @6Mbps, -75dBm@54Mbps; 802.11n 20MHz: -73dBm @MCS7; 802.11n 40MHz:-70dBm @MCS7 **5G** 802.11a: -92dBm @6Mbps, -74dBm @54Mbps; 802.11ac 20MHz: -67dBm@MCS8; 802.11ac: HT40:-63dBm @MCS9; 802.11ac 80MHz: -59dBm @MCS9
SSIDs	32 SSIDs total, 16 per radio (2.4GHz and 5GHz)
Concurrent Clients	200+

Network Interfaces	2× autosensing 10/100/1000 Base-T Ethernet Ports
Auxiliary Ports	1× Reset Pinhole , 1× Kensington lock
Mounting	Indoor wall mount or ceiling mount, kits included
LEDs	1× tri-color LED for device tracking and status indication
Network Protocols	IPv4, 802.1Q, 802.1p, 802.1x, 802.11e/WMM, 802.11h
QoS	802.11e/WMM, VLAN, TOS
Network Management	≤ 50 APs: Light-weight Master in AP ≤ 3000 APs: On-Premises controller ≤ +∞ APs: Cloud management
Power and Green Energy Efficiency	POE 802.3af/ 802.3at; Max Consumption: 12.5W
Environmental	Operation: 0°C to 40°C Storage: -10°C to 60°C Humidity: 10% to 90% Non-condensing
Physical	Unit Dimension: 205.4 x 205.4 x 45.9mm; Unit Weight: 500g Entire Package Dimension: 258 x 247 x 86mm; Entire Package Weight: 867.3g
Package Content	GWN7615 802.11ac Wireless AP, Mounting Kits, Quick Start Guide
Compliance	FCC, CE, RCM, IC

GWN7615 Technical Specifications

Wi-Fi Standards	IEEE 802.11 a/b/g/n/ac
Antennas	3x 2.4 GHz, gain 3 dBi, internal antenna, 3x 5 GHz, gain 3 dBi, internal antenna
Wi-Fi Data Rates	IEEE 802.11ac: 6.5 Mbps to 1300 Mbps IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps IEEE 802.11n: 6.5 Mbps to 450 Mbps IEEE 802.11b: 1, 2, 5.5, 11 Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps *Actual throughput may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment and mix of devices in the network*

Frequency Bands	2.4GHz radio: 2.400 – 2.4835 GHz 5GHz radio: 5.150 – 5.250 GHz, 5.725 – 5.850 GHz (FCC, IC, RCM)
Channel Bandwidth	2.4G: 20 and 40 MHz 5G: 20,40 and 80 MHz
Wi-Fi and System Security	WEP, WPA3, WPA/WPA2-PSK, WPA/WPA2-Enterprise (TKIP/AES), anti-hacking secure boot and critical data/control lockdown via digital signatures, unique security certificate and random default password per device
MIMO	3×3:3 2.4GHz, 3×3:3 5GHz
Coverage Range	575ft. (175 meters) *coverage range can vary based on environment*
Maximum TX Power	5G: 26dBm (FCC) / 20dBm (CE) 2.4G: 26dBm (FCC) / 17dBm (CE) *Maximum power varies by country, frequency band and MCS rate*
Receiver Sensitivity	**2.4G** 802.11b:-92dBm@11Mbps; 802.11g:-76dBm@54Mbps; 802.11n 20MHz: -73dBm@MCS7; 802.11n 40MHz:-70dBm@MCS7 **5G** 802.11a:-94dBm@6Mbps; 801.11a:-77dBm@54Mbps; 802.11ac 20MHz: -69dBm@MCS8; 802.11ac HT40:-65dBm@MCS9; 802.11ac 80MHz: 1dBm@MCS9 * Receiver sensitivity varies by frequency band, channel width and MCS rate*
SSIDs	32 SSIDs total, 16 per radio (2.4GHz and 5GHz)
Concurrent Clients	250+
Network Interfaces	2x autosensing 10/100/1000 Base-T Ethernet Ports
Auxiliary Ports	1x USB 2.0 port, 1x Reset Pinhole, 1x Kensington lock
Mounting	Indoor wall mount or ceiling mount, kits included
LEDs	3 multi-color LEDs for device tracking and status indication
Network Protocols	IPv4, 802.1Q, 802.1p, 802.1x, 802.11e/WMM, 802.11h
QoS	802.11e/WMM, VLAN, TOS
Network Management	Embedded controller in GWN7610 allows it to auto-discover, auto-provision and manage up to 50 GWN76XX s in a network. GWN.Cloud offers a free cloud management platform for unlimited GWN Aps

Auto Power Saving	Self-power adaptation upon auto detection of PoE or PoE+
Power and Green Energy Efficiency	DC Input: 24VDC/1A Power over Ethernet 802.3af/802.3at compliant Maximum Power Consumption: 13.8W
Environmental	Operation: 0°C to 50°C Storage: -10°C to 60°C Humidity: 10% to 90% Non-condensing
Physical	Unit Dimension: 205.3 x 205.3 x 45.9mm; Unit Weight: 540g Unit + Mounting Kits Dimension: 205.3 x 205.3 x 50.9mm; Unit + Mounting Kits Weight: 600g Entire Package Dimension: 258 x 247 x 86mm; Entire Package Weight: 900g
Package Content	GWN7610 802.11ac Wireless AP, Mounting Kits, Quick Start Guide
Compliance	FCC, CE, RCM, IC

GWN7610 Technical Specifications

Wi-Fi Standards	IEEE 802.11 a/b/g/n/ac (Wave-2)
Antennas	2 dual band internal antennas 2.4GHz, gain 3dBi 5 GHz, gain 4dBi
Wi-Fi Data Rates	IEEE 802.11ac: 6.5 Mbps to 867 Mbps IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps IEEE 802.11n: 6.5Mbps to 300Mbps. IEEE 802.11b: 1, 2, 5.5, 11 Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps *Actual throughput may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment and mix of devices in the network
Frequency Bands	2.4GHz radio : 2412 – 2484 MHz 5GHz radio : 5180-5825 MHz
Channel Bandwidth	2.4G: 20 and 40 MHz 5G: 20,40 and 80 MHz
Wi-Fi and System Security	WEP, WPA3, WPA/WPA2-PSK, WPA/WPA2-Enterprise (TKIP/AES), anti-hacking secure boot and critical data/control lockdown via digital signatures, unique security certificate and random default password per device

MIMO	2×2:2 2.4GHz (MIMO) 2×2:2 5GHz (MU-MIMO)
Coverage Range	Up to 165 meters *coverage range can vary based on environment*
Maximum TX Power	5G: 24dBm 2.4G: 22dBm *Maximum power varies by country, frequency band and MCS rate*
Receiver Sensitivity	**2.4G** 802.11b: -96dBm@1Mbps, -88dBm@11Mbps; 802.11g: -93dBm @6Mbps, -75dBm@54Mbps; 802.11n 20MHz: -73dBm @MCS7; 802.11n 40MHz:-70dBm @MCS7 **5G** 802.11a: -92dBm @6Mbps, -74dBm @54Mbps; 802.11ac 20MHz: -67dBm@MCS8; 802.11ac: HT40:-63dBm @MCS9; 802.11ac 80MHz: -59dBm @MCS9 * Receiver sensitivity varies by frequency band, channel width and MCS rate*
SSIDs	16 SSIDs total, 8 per radio (2.4GHz and 5GHz) *GWN7605 when deployed as Master can only be added to 8 SSIDs.*
Concurrent Clients	100+
Network Interfaces	2x autosensing 10/100/1000 Base-T Ethernet Ports
Auxiliary Ports	1x Reset Pinhole, 1x Kensington lock
Mounting	Indoor wall mount or ceiling mount, kits included
LEDs	3 multi-color LEDs for device tracking and status indication
Network Protocols	IPv4, 802.1Q, 802.1p, 802.1x, 802.11e/WMM, 802.11h
QoS	802.11e/WMM, VLAN, TOS
Network Management	≤ 50 APs: Light-weight Master in AP ≤ 3000 APs: On-Premise controller ≤ +∞ APs: Cloud management
Power and Green Energy Efficiency	DC Input: 24VDC/1A Power over Ethernet 802.3af/802.3at compliant Maximum Power Consumption: 13.8W

Environmental	Operation: 0°C to 40°C
	Storage: -10°C to 60°C
	Humidity: 10% to 90% Non-condensing
Physical	Unit Dimension: 180.4mmx180.4mmx40.8mm; Unit Weight: 388.2g
	Entire Package Dimension: 228.5x220x79mm; Entire Package Weight: 719.3g
Package Content	GWN7610 802.11ac Wireless AP, Mounting Kits, Quick Start Guide
Compliance	FCC, CE, RCM, IC

GWN7605 Technical Specifications

Wi-Fi Standards	IEEE 802.11a/b/g/n/ac (Wave-2)
Antennas	2 dual band external antennas
	2.4GHz, gain 3.5dBi
	5 GHz, gain 3.5dBi
Wi-Fi Data Rates	IEEE 802.11ac: 6.5 Mbps to 867 Mbps
	IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
	IEEE 802.11n: 6.5Mbps to 300Mbps
	IEEE 802.11b: 1, 2, 5.5, 11Mbps
	IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
	Actual throughput may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment and mix of devices in the network
Frequency Bands	2.4GHz Radio: 2412 – 2484 MHz, 5 GHz Radio: 5180-5825 MHz
Channel Bandwidth	2.4G: 20 and 40MHz, 5G: 20, 40 and 80 MHz
Wi-Fi and System Security	WEP, WPA3, WPA/WPA2-PSK, WPA/WPA2 Enterprise, anti-hacking secure boot and critical data/control lockdown via digital signatures, unique security certificate and random default password per device
MIMO	2×2:2 2.4GHz (MIMO)
	2×2:2 5GHz (MU-MIMO))
Coverage Range	Up to 250 meters
	coverage range can vary based on environment
Maximum TX Power	2.4G: 24 dBm
	5G: 22dBm

Receiver Sensitivity	2.4G 802.11b: -96dBm@1Mbps, -88dBm@11Mbps; 802.11g: -93dBm @6Mbps, -75dBm@54Mbps; 802.11n 20MHz: -73dBm @MCS7; 802.11n 40MHz:-70dBm @MCS7 5G 802.11a: -92dBm @6Mbps, -74dBm @54Mbps; 802.11ac 20MHz: -67dBm@MCS8; 802.11ac: HT40:-63dBm @MCS9; 802.11ac 80MHz: -59dBm @MCS9
SSIDs	16 SSIDs total, 8 per radio (2.4GHz and 5GHz) *GWN7605LR when deployed as Master can only be added to 8 SSIDs.*
Concurrent Clients	100+
Network Interfaces	2× autosensing 10/100/1000 Base-T Ethernet Ports
Auxiliary Ports	1× Reset Pinhole
Mounting	Outdoor metal bar mount or wall mount, kits included
LEDs	1 tri-color LED for device tracking and status indication
Network Protocols	IPv4, 802.1Q, 802.1p, 802.1x, 802.11e/WMM, 802.11h
QoS	802.11e/WMM, VLAN, TOS
Network Management	Embedded controller can manage up to 50 local GWN APs GWN.Cloud offers a free cloud management platform for almost unlimited GWN Aps GWN Manager offers premise-based software controller for up to 3,000 GWN APs
Power and Green Energy Efficiency	POE 802.3af/ 802.3at; Maximum Power Consumption: 10.16W
Environmental	Operation: -30°C to 60°C Storage: -30°C to 70°C Humidity: 10% to 90% Non-condensing
Physical	Physical Unit Dimension: 358.3mm(L)*115mm(W)*45.3mm(H); Unit Weight: 500g Entire Package Dimension: 258 × 247× 86mm; Entire Package Weight:655.3g
Package Content	GWN7605LR 802.11ac Wave-2 Wireless AP, Mounting Kits, Quick Start Guide
Water Proof	IP66-level weatherproof capability when installed vertically
Compliance	FCC, CE, RCM, IC

GWN7605LR Technical Specifications

Wi-Fi Standards	IEEE 802.11 a/b/g/n/ac (Wave-2)

Antennas	2x 2.4 GHz, gain 3 dBi, internal antenna, 2x 5 GHz, gain 3 dBi, internal antenna
Wi-Fi Data Rates	IEEE 802.11ac: 6.5 Mbps to 877 Mbps IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps IEEE 802.11n: 6.5 Mbps to 300 Mbps; 400 Mbps with 256-QAM on 2.4GHz IEEE 802.11b: 1, 2, 5.5, 11 Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps *Actual throughput may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment and mix of devices in the network.*
Frequency Bands	2.4GHz radio : 2.400 – 2.4835 GHz 5GHz radio: 5.150 – 5.250 GHz, 5.725 – 5.850 GHz
Channel Bandwidth	2.4G: 20 and 40 MHz 5G: 20,40 and 80 MHz
Wi-Fi and System Security	WEP, WPA3, WPA/WPA2-PSK, WPA/WPA2-Enterprise (TKIP/AES), anti-hacking secure boot and critical data/control lockdown via digital signatures, unique security certificate and random default password per device.
MIMO	2×2:2 2.4GHz, 2×2:2 5GHz
Coverage Range	Up to 541ft. (165 meters) for GWN7600. *Coverage range can vary based on environment
Maximum TX Power	5G: 22dBm 2.4G: 22dBm *Maximum power varies by country, frequency band and MCS rate.
Receiver Sensitivity	**2.4G** 802.11b:-99dBm @1Mbps,-91dBm @11Mbps;802.11g:-93dBm @6Mbps,-75dBm @54Mbps; 80.11n 20MHz:-72dBm @MCS7;802.11n 40MHz:-69dBm @MCS7 **5G** 802.11a:-91dBm @6Mbps,-74dBm @54Mbps;802.11ac 20MHz:-67dBm @MCS8;802.11ac HT40:-63dBm @MCS9;802.11ac 80MHz:-60dBm @MCS9
BSSID	32 SSIDs total, 16 per radio (2.4GHz and 5GHz)
Concurrent Clients	450+
Network Interfaces	2x autosensing 10/100/1000 Base-T Ethernet Ports
Auxiliary Ports	1x USB 2.0 port, 1x Reset Pinhole, 1x Kensington lock
Mounting	Indoor wall mount or ceiling mount, kits included
LEDs	multi-color LEDs for device tracking and status indication

Network Protocols	IPv4, 802.1Q, 802.1p, 802.1x, 802.11e/WMM, 802.11h
QoS	802.11e/WMM, VLAN, TOS
Network Management	Embedded controller in GWN7600 allows it to auto-discover, auto-provision and manage up to 30 GWN76XX in a network GWN.Cloud offers a free cloud management platform for unlimited GWN APs
Power and Green Energy Efficiency	DC Input: 24VDC/1A Power over Ethernet (802.3af) compliant Maximum Power Consumption: 13.8W
Temperature & Humidity	Operation: 0°C to 40°C Storage: -10°C to 60°C Humidity: 10% to 90% Non-condensing
Physical	Unit Dimension: 205.3 x 205.3 x 45.9mm; Unit Weight: 526g Unit + Mounting Kits Dimension: 205.3 x 205.3 x 53.9mm; Unit + Mounting Kits Weight : 610g Entire Package Dimension: 228.5*220*79mm; Entire Package Weight: 854g
Package Content	GWN7600 Wave-2 802.11ac Wireless AP, Mounting Kits, Quick Installation Guide
Compliance	FCC, CE, RCM, IC

GWN7600 Technical Specifications

Wi-Fi Standards	IEEE 802.11 a/b/g/n/ac (Wave-2)
Antennas	2x 2.4 GHz, gain 4 dBi, internal antenna 2x 5 GHz, gain 5 dBi, internal antenna
Wi-Fi Data Rates	IEEE 802.11ac: 6.5 Mbps to 867 Mbps IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps IEEE 802.11n: 6.5 Mbps to 300 Mbps; 400Mbps with 256-QAM on 2.4GHz IEEE 802.11b: 1, 2, 5.5, 11 Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps *Actual throughput may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment and mix of devices in the network
Frequency Bands	2.4GHz radio: 2.400 – 2.4835 GHz 5GHz radio: 5.150 – 5.250 GHz, 5.725 – 5.850 GHz
Channel Bandwidth	2.4G: 20 and 40 MHz 5G: 20,40 and 80 MHz

Wi-Fi and System Security	WEP, WPA3, WPA/WPA2-PSK, WPA/WPA2 Enterprise (TKIP/AES), anti-hacking secure boot and critical data/control lockdown via digital signatures, unique security certificate and random default password per device
MIMO	2×2:2 2.4GHz (MIMO), 2×2:2 5GHz (MU-MIMO)
Coverage Range	Up to 984ft. (300 meters) *Coverage range can vary based on environment
Maximum TX Power	5G: 22dBm (FCC) / 20dBm (CE) 2.4G: 22dBm (FCC) / 17dBm (CE) *Maximum power varies by country, frequency band and MCS rate
Receiver Sensitivity	**2.4G** 802.11b: -99dBm@1Mbps, -91dBm@11Mbps; 802.11g:-93dBm@6Mbps, -75dBm@54Mbps; 802.11n 20MHz: -72dBm@MCS7; 802.11n 40MHz: -69dBm @MCS7 **5G** 802.11a: -91dBm@6Mbps, -74dBm@54Mbps; 802.11ac 20MHz: -67dBm@MCS8; 802.11ac; HT40: -63dBm@MCS9; 802.11ac 80MHz: -60dBm@MCS9
SSIDs	32 SSIDs total, 16 per radio (2.4GHz and 5GHz)
Concurrent Clients	450+
Network Interfaces	2x autosensing 10/100/1000 Base-T Ethernet Ports
Auxiliary Ports	1x Reset Pinhole
Mounting	Outdoor base bracket and cover bracket included
LEDs	multicolor LED for device tracking and status indication
Network Protocols	IPv4, 802.1Q, 802.1p, 802.1x, 802.11e/WMM, 802.11h
QoS	802.11e/WMM, VLAN, TOS
Network Management	Embedded controller in GWN7600LR allows it to auto-discover, auto-provision and manage up to 30 GWN76XX s in a network GWN.Cloud offers a free cloud management platform for unlimited GWN APs
Power and Green Energy Efficiency	Power over Ethernet 802.3af and 802.3at compliant Maximum Power Consumption: 12.9 W (PoE supply) | 23.0 W (PoE+ supply)
Temperature & Humidity	Operation: -30°C to 60°C Storage: -30°C to 70°C Humidity: 5% to 95% Non-condensing

Physical	Unit Dimension: 290×150×35mm; Unit Weight: 708g
	Unit + Mounting Kits Dimension: 290×150×56mm;
	Unit + Mounting Kits Weight: 1528.2g
	Entire Package Dimension: 423×187×97mm;
	Entire Package Weight: 1844g
Package Content	Enterprise 802.11ac Wave-2 Outdoor Long Range Wi-Fi Access Point, Mounting Kits, Quick Installation Guide
Waterproof Grade	IP66-level weatherproof capability when installed vertically
Compliance	FCC, CE, RCM, IC

GWN7600LR Technical Specifications

Wi-Fi Standards	IEEE 802.11 a/b/g/n/ac (Wave-2)
Antennas	4 detachable/changeable dual-band omnidirectional antennas 2.4GHz, gain 3.5dBi; 5GHz, gain 3.5dB
Wi-Fi Data Rates	IEEE 802.11ac: 6.5 Mbps to 1733Mbps IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps IEEE 802.11n: 6.5Mbps to 600Mbps IEEE 802.11b: 1, 2, 5.5, 11Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps *Actual throughput may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment and mix of devices in the network
Frequency Bands	2.4 GHz Radio: 2412 – 2484 MHz 5GHz Radio: 5150-5250MHz, 5250-5350MHz, 5470-5725MHz, 5725-5850MHz *Not all frequency bands can be used in all regions.
Channel Bandwidth	2.4G: 20 and 40 MHz; 5G: 20,40 and 80 MHz
Wi-Fi and System Security	WEP, WPA3, WPA/WPA2-PSK, WPA/WPA2 Enterprise, anti-hacking secure boot and critical data/control lockdown via digital signatures, unique security certificate and random default password per device
MIMO	4×4:4 2.4G (MIMO), 4×4:4 5G (MU-MIMO)
Coverage Range	Up to 984ft. (300 meters) *Coverage range can vary based on environment

Maximum TX Power	2.4G: 27 dBm
	5G: 25 dBm
	*Maximum power varies by country, frequency band and MCS rate
Receiver Sensitivity	**2.4G**
	802.11b: -96dBm@1Mbps, -88dBm@11Mbps; 802.11g: -93dBm @6Mbps, -75dBm@54Mbps; 802.11n 20MHz: -73dBm @MCS7; 802.11n 40MHz:-70dBm @MCS7
	5G
	802.11a: -92dBm @6Mbps, -74dBm @54Mbps; 802.11ac 20MHz: -67dBm@MCS8; 802.11ac: HT40:-63dBm @MCS9; 802.11ac 80MHz: -59dBm @MCS9
SSIDs	32 SSIDs total, 16 per radio (2.4GHz and 5GHz)
Concurrent Clients	200+
Network Interfaces	2x autosensing 10/100/1000 Base-T Ethernet Ports
Auxiliary Ports	1x Reset Pinhole
Mounting	Wall mount or pole mount – kits included
LEDs	1x tri-color LEDs for device tracking and status indication
Network Protocols	IPv4, 802.1Q, 802.1p, 802.1x, 802.11e/WMM, 802.11h
QoS	802.11e/WMM, VLAN, TOS
Network Management	Embedded controller can manage up to 50 local GWN APs
	GWN.Cloud offers a free cloud management platform for unlimited GWN APs
Power and Green Energy Efficiency	PoE 802.3af/ 802.3at;
	Max Consumption: 16.5W
Temperature & Humidity	Operation: -30°C to 60°C
	Storage: -30°C to 70°C
	Humidity: 5% to 95% Non-condensing
Physical	Unit Dimension: 533.1 × 115 × 40mm; Unit Weight: 564g
	Unit + Mounting Kits Dimension : 533.1×115 ×62mm; Unit + Mounting Kits Weight : 706g
	Entire Package Dimension: 258 × 247× 86mm; Entire Package Weight: 978g
Package Content	GWN7630LR 802.11ac Wireless AP, Mounting Kits, Quick Installation Guide
Waterproof Grade	IP66-level weatherproof capability when installed vertically
Compliance	FCC, CE, RCM, IC

Wi-Fi Standards	IEEE 802.11 a/b/g/n/**ac**
Antennas	2 Dual band internal antennas **Antenna 1 -** 2.4GHz: gain 3.0dBi, 5GHz: gain 3.5dBi **Antenna 2 -** 2.4GHz: gain 3.5dBi, 5GHz: gain 3.0dBi
Wi-Fi Data Rates	**2.4GHz:** **IEEE 802.11n**: 6.5Mbps to 300Mbps **IEEE 802.11b**: 1, 2, 5.5, 11 Mbps **IEEE 802.11g**: 6, 9, 12, 18, 24, 36, 48, 54 Mbps **5GHz:** **IEEE 802.11ac**: 6.5 Mbps to 1733 Mbps **IEEE 802.11n**: 6.5Mbps to 600Mbps **IEEE 802.11a**: 6, 9, 12, 18, 24, 36, 48, 54 Mbps *****Actual throughput may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment and mix of devices in the network
Frequency Bands	**2.4GHz Radio:** 2412 - 2484 MHz **5GHz Radio:** 5150-5250 MHz, 5250-5350 MHz, 5470-5725 MHz, 5725-5850 MHz *Not all frequency bands can be used in all regions. The band 5150-5350 MHz is restricted to indoor use only in all EU states**.**
Channel Bandwidth	**2.4G**: 20 and 40 MHz **5G**: 20, 40 and 80 MHz
System Security	WEP, WPA/WPA2-PSK, WPA/WPA2 Enterprise
Mesh	5G radio
Coverage Range	Up to **100 meters** *coverage range can vary based on environment
Maximum TX Power	**5G**: 21dBm **2.4G**: 21dBm *Maximum power varies by country, frequency band and MCS rate
Receiver Sensitivity	**2.4GHz** **802.11b:** -96dBm@1Mbps, -88dBm@11Mbps; **802.11g:** -93dBm @6Mbps, -75dBm@54Mbps; **802.11n 20MHz:** -73dBm @MCS7; **802.11n 40MHz:**-70dBm @MCS7 @MCS11 **5GHz** **802.11a:** -92dBm @6Mbps, -74dBm @54Mbps; **802.11n 20MHz:** -74dBm @MCS7; **802.11n 40MHz:**-71dBm @MCS7 **802.11ac 20MHz:** -67dBm@MCS8; **802.11ac: HT40:**- 63dBm @MCS9; **802.11ac 80MHz:** -59dBm @MCS9
SSIDs	**8 SSIDs total**, 5 per radio (2.4GHz & 5GHz)
Concurrent Clients	Up to **80**
Network Interfaces	**1x** 10/100/1000M uplink Ethernet port **with PoE/PoE+** **2x** 10/100M Ethernet port **with PSE** **1x** 10/100M Ethernet port
Auxiliary Ports	1x Reset Pinhole

Mounting	Wall mountable
LEDs	1 tri-color LEDs for device tracking and status indication
Network Protocols	IPv4, IPv6, 802.1Q, 802.1p, 802.1x, 802.11e/WMM, 802.11h
QoS	802.11e/WMM, VLAN, TOS
Network Management	GWN.Cloud offers a free cloud management platform for unlimited GWN APs GWN.Manager offers premise-based software controller for up to 3,000 GWN APs
Auto Power Saving	Self-power adaptation upon auto detection of PoE or PoE+
Power and Green Energy Efficiency	Support 802.3az PoE 802.3af/ 802.3at; PSE Maximum Output Per Port: 6W; Maximum Power Consumption: 20W
Environmental	Operation:0°Cto 40°C Storage: -10°C to 60°C Humidity: 10% to 90% Non-condensing
Physical	Unit Dimension:135 x 115 x 30mm; Unit Weight: 188g Entire Package Dimension: 171 x 140 x 33mm; Entire Package Weight: 278.5g
Package Content	GWN7602 802.11ac Wireless AP, Quick Start Guide
Compliance	FCC, CE, RCM, IC

GWN7602 Technical Specifications

INSTALLATION

Before deploying and configuring the GWN76XX, the device needs to be properly powered up and connected to the network. This section describes detailed information on installation, connection, and warranty policy of the GWN76XX.

Equipment Packaging

Main Case (GWN7625, GWN7664,GWN7660, GWN7630, GWN7610, GWN7615, GWN7605, GWN7600)	Yes (1)
Mounting Bracket	Yes (1)
Ceiling Mounting Bracket	Yes (1)
Plastic Expansion Bolt	Yes (3)
M3 NUT	Yes (3)
Screw (PM 3 x 50)	Yes (3)
Screw (PM 3.5 x 20)	Yes (3)
Quick Installation Guide	Yes (1)

GWN76xx Equipment Packaging
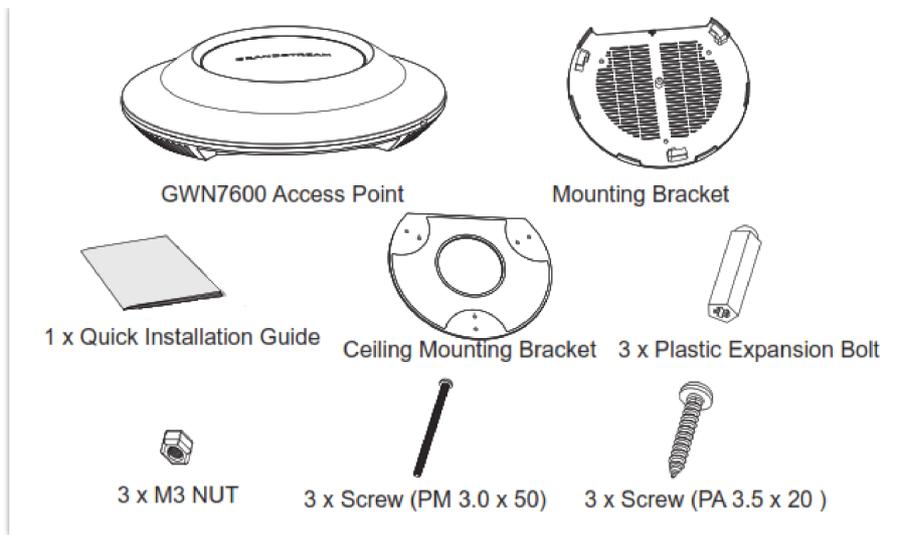
GWN76xx Equipment Packaging

Below is the equipment packaging for GWN7600LR model.

Main Case	Yes (1)
Cover Interface	Yes (1)
Base Bracket	Yes (1)
Cover Bracket	Yes (1)
Assembled Screw	Yes (4)
Locknut	Yes (4)
Anchors + Screws	Yes (4)
Screw (PM8 x 115)	Yes (4)
Quick Installation Guide	Yes (1)

GWN7600LR Equipment Packaging
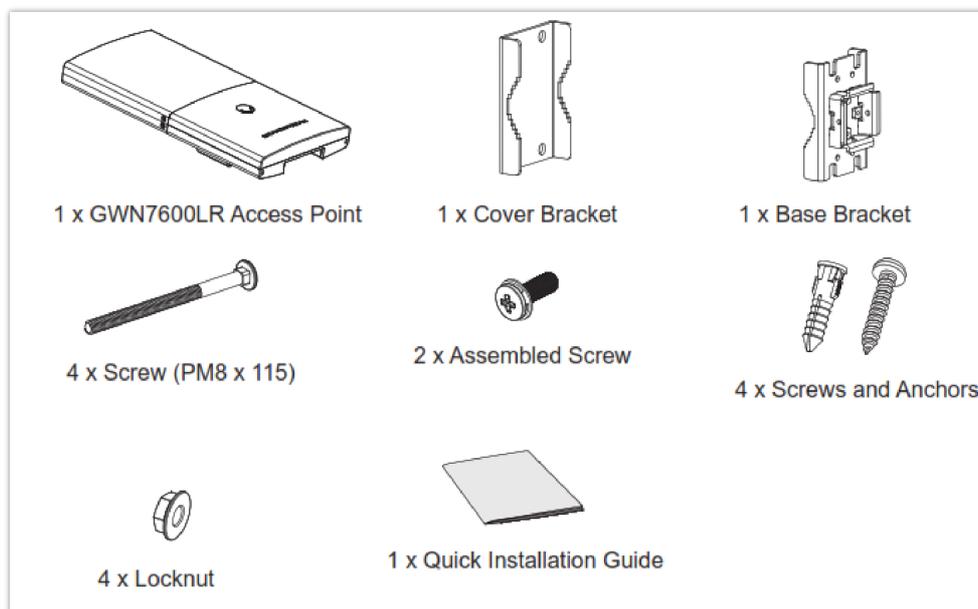
GWN7600LR Equipment Package

Below is the equipment packaging for GWN7630LR, GWN7605LR, GWN7660LR and GWN7664LR models.

Main Case	Yes (1)
Antenna	GWN7630LR: Yes (4) GWN7605LR: Yes (2) GWN7660LR: Yes (2) GWN7664LR: Yes (4)
Base Bracket	Yes (1)
Screw (PM 3.0×7)	Yes (4)
Expansion Screw	Yes (4)
Metal Strap	Yes (2)
Quick Installation Guide	Yes (1)

GWN76xxLR Equipment Packaging
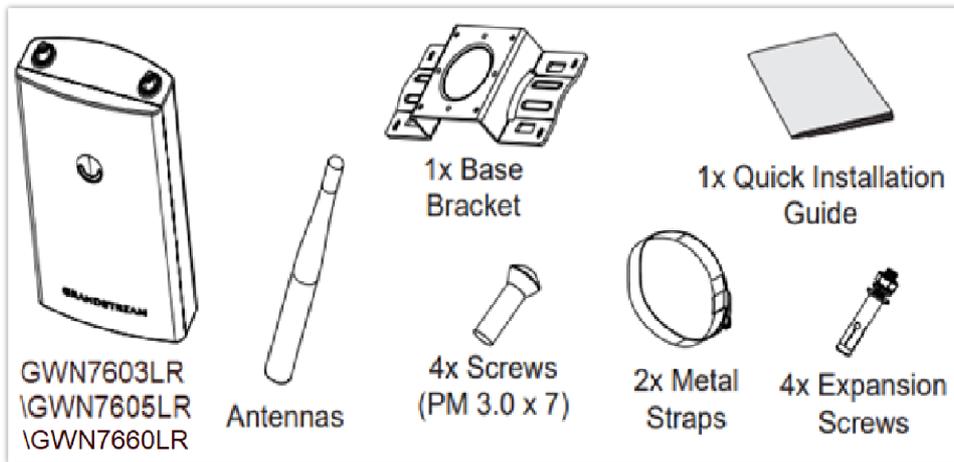
GWN7630LR/GWN7605LR/GWN7660LR /GWN7664LR Equipment Package

Below is the equipment packaging for GWN7624 model.

Main Case	Yes (1)
Screw PM 2.5*6*4 mm	Yes (2)
Screw KB 2.6*6	Yes (1)
Screw KB 3.5*26	Yes (4)
Quick Installation Guide	Yes (1)

GWN7624 Equipment Packaging

GWN7624 Equipment Package

The equipment packaging for GWN7602 model.

Main Case	Yes (1)
PA3.5*20 Screws	Yes (2)
Anchors Screws	Yes (2)
Quick Installation Guide	Yes (1)

GWN7602 Equipment Packaging

GWN7602 Equipment Package

GWN76XX Access Point Ports
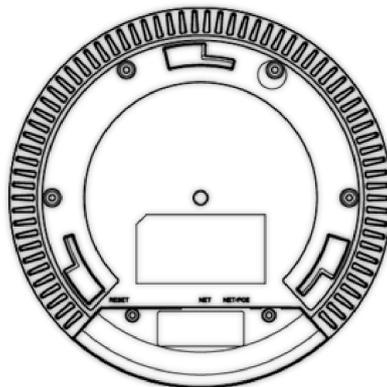
GWN76xx Ports
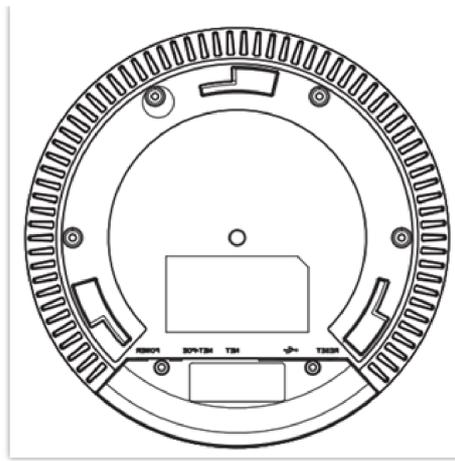
GWN7610/GWN7600 Ports
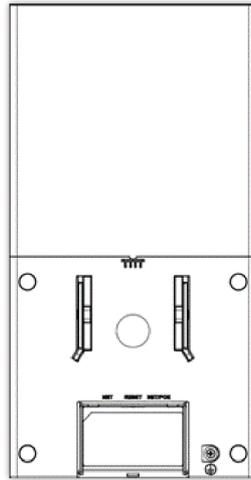
GWN7600LR Ports
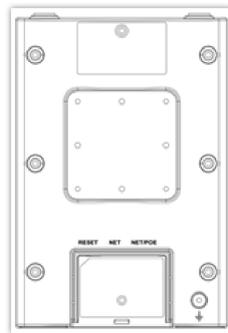
*GWN7630LR
/GWN7605LR/GWN7660LR/GWN7664LR
Ports*
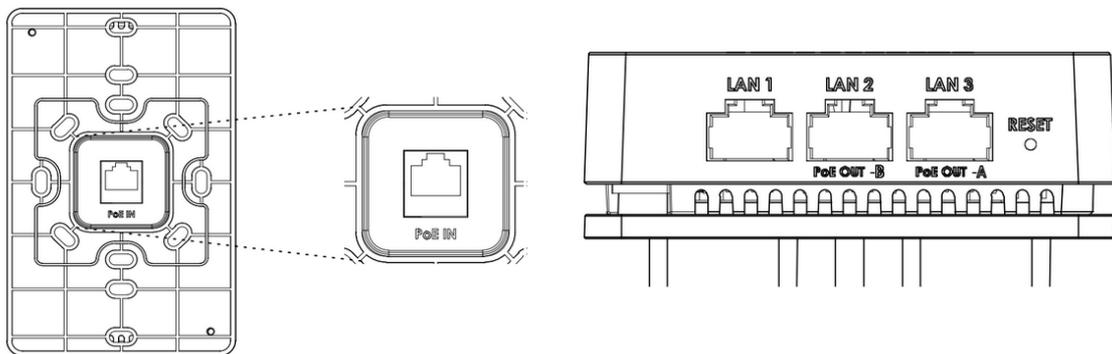
GWN7624 Ports
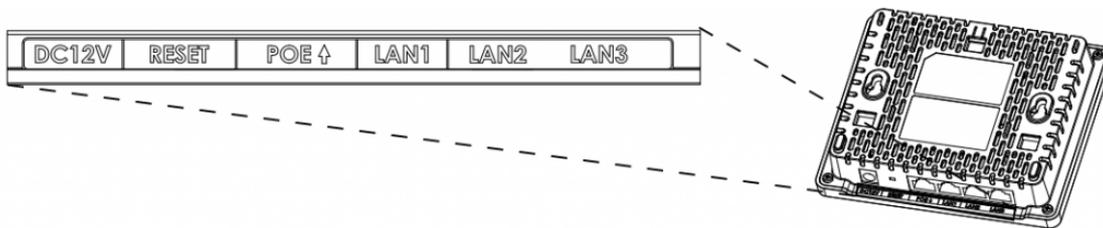
GWN7602 Ports

Port	Description
Power	Power adapter connector (12V, 2A) for GWN7610 Power adapter connector (24V, 1A) for GWN7600 and GWN7602
NET/PoE	Ethernet RJ45 port (10/100/1000Mbps) supporting PoE/PoE+. * GWN7600 supports PoE (802.3af) only * GWN7624 supports 2x 10/100/1000Mbps Ethernet ports with PSE. • The maximum output of each PSE port is 6W. • If powered by PoE+, both LAN 2(PoE OUT -B) and LAN 3(PoE OUT -A) can be used as PSE. • If powered by PoE, only LAN 3(PoE OUT -A) can be used as PSE.
NET	Ethernet RJ45 port (10/100/1000Mbps) to your router or another GWN76XX series. * GWN7664 supports 1x 2.5G Port * GWN7602 LAN1,2 and 3 are 10/100M Ethernet Ports
	USB 2.0 port (for future IOT & location-based applications) * Available on GWN7610 and GWN7600 only
RESET	Factory reset button. Press for 7 seconds to reset factory default settings. Quick press will only reboot the unit.

GWN76XX AP Ports Description

Power and Connect GWN76XX Access Point

Step 1:

Connect one end of a RJ-45 Ethernet cable into the NET or PoE/NET port of the GWN76XX unit.

Step 2:

Connect the other end of the Ethernet cable(s) into a LAN port to your Network. (Use PoE/PoE+ switch for GWN76XX).

Step 3:

For GWN7610/GWN7600 and GWN7602, connect the 24V DC power adapter into the power jack on the back of the access point. Insert the main plug of the power adapter into a surge-protected power outlet. Otherwise, PoE can be used if the switch port does provide PoE power.

Notes

GWN7624/GWN7625/GWN7664/GWN7660/GWN7660LR/GWN7664LR/GWN7630/GWN7615/GWN7610/GWN7605/GWN7605LR/GWN7600LR/GWN7630LR can be powered using PoE(802.3af)/PoE+(802.3at) switch via PoE/NET port while GWN7600 can be powered using PoE (802.3af) switch via PoE/NET port. In this case, both power and network connectivity will be provided over the PoE/NET port.

GWN7600/GWN7610 has a PoE detection daemon that will monitor the status and update maximum allowable power for USB ports in real time.

Step 4:

Wait for the GWN76XX to boot up and acquire an IP address from the DHCP Server.
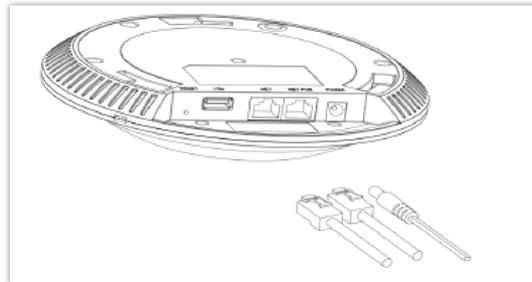
FConnecting GWN AP – GWN7600 as example

Warranty

If the GWN76XX Wireless Access Point was purchased from a reseller, please contact the company where the device was purchased for replacement, repair, or refund.

If the device was purchased directly from Grandstream, contact our Technical Support Team for an RMA (Return Materials Authorization) number before the product is returned. Grandstream reserves the right to remedy warranty policy without prior notification.

Wall/Ceiling Mount Installation GWN76XX

GWN7625/GWN7664/GWN7660/GWN7630/GWN7610/GWN7615/GWN7600/GWN7605 can be mounted on the wall or ceiling, please refer to the following steps for the appropriate installation. This is the GWN7600 example:

Wall Mount

Step1:

Position the mounting bracket at the desired location on the wall with the arrow pointing up.
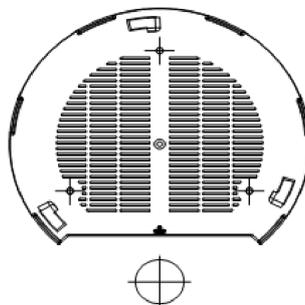
Wall Mount – Steps 1 & 2

Step 2:

Use a pencil to mark the four mounting holes (screw holes DIA 5.5mm, reticle hole DIA 25mm).

Step 3:

Insert screw anchors into the 5.5 mm holes. Attach the mounting bracket to the wall by inserting the screws into the anchors.
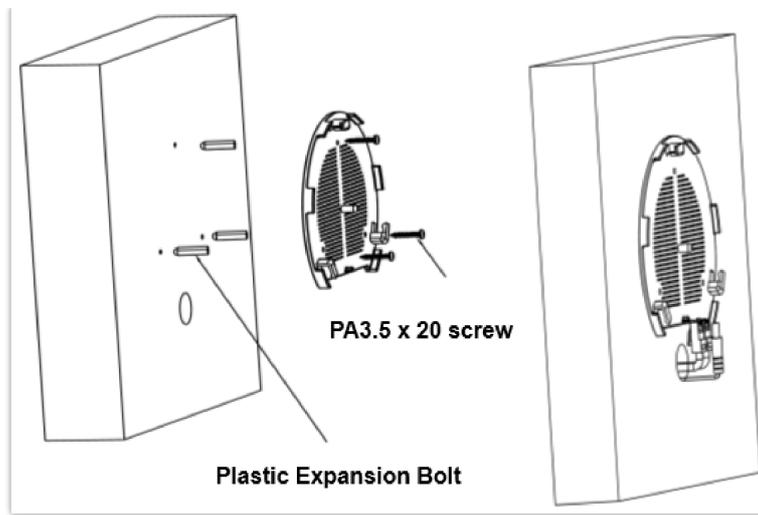
Wall Mount – Steps 3 & 4

Step 4:

Connect the power cable and the Ethernet cable (RJ45) to the correct ports of your GWN7664/GWN7660/GWN7660LR/GWN7664LR/GWN7630/GWN7610/ GWN7615/GWN7605/GWN7600/GWN7625

Step 5:

Align the arrow on the GWN AP with the arrow on the locking tab of the mounting bracket and ensure that your GWN is firmly seated on the mounting bracket.
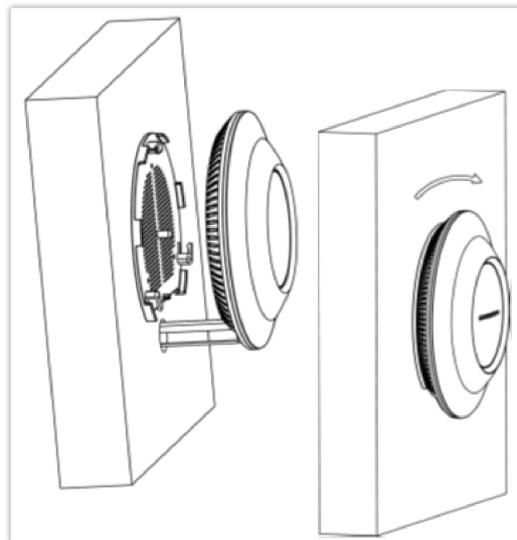
Wall Mount – Steps 5 & 6

Step 6:

Turn the GWN clockwise until it locks into place and fits the locking tab.

Ceiling Mount

Step 1:

Remove the ceiling tile.
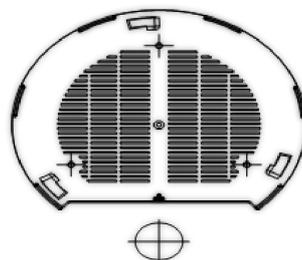
Step 2:

Place the ceiling backing plate in the center of the ceiling tile and mark the mounting screw holes (screw holes DIA 5.5mm, reticle hole DIA 25mm).

Step 3:

Insert the screws through the mounting bracket.
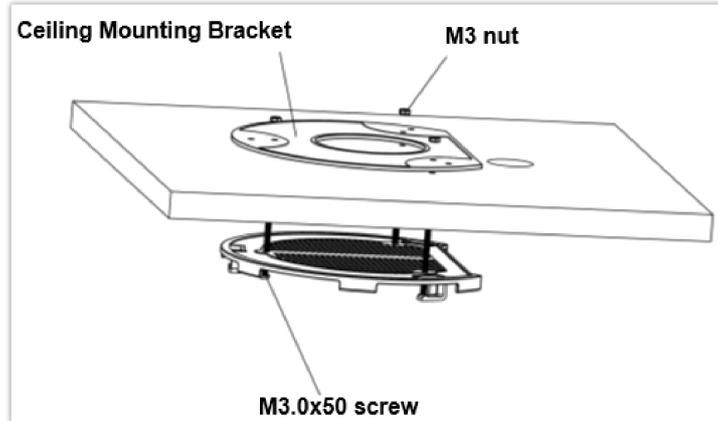
Ceiling Mount – Step 3

Step 4:

Connect the power cable and the Ethernet cable (RJ45) to the correct ports of your GWN76XX.
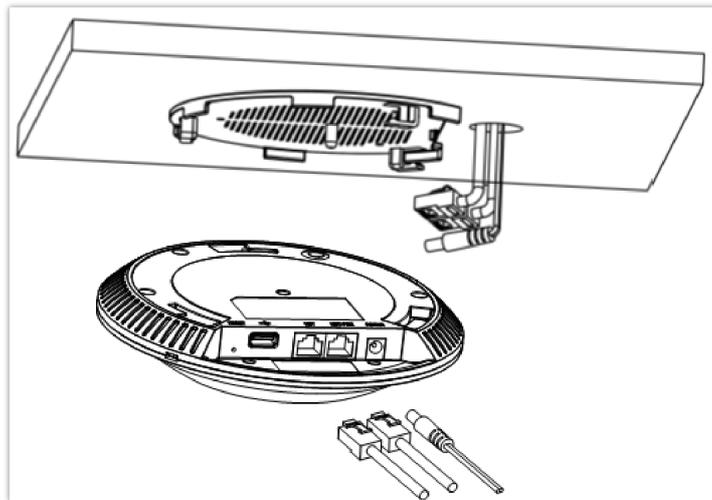
Ceiling Mount – Step 4

Step 5:

Align the arrow on the GWN AP with the arrow on the locking tab of the mounting bracket and ensure that your GWN is firmly seated on the mounting bracket and connect the network and power cables.
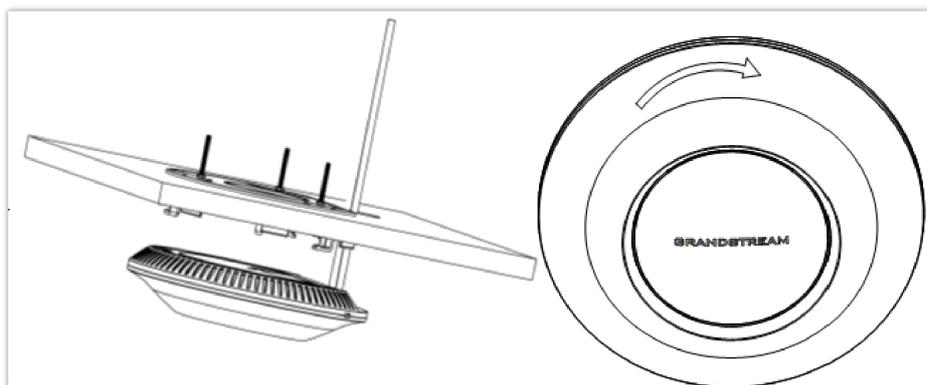
Ceiling Mount – Steps 5 & 6

Step 6:

Turn the GWN clockwise until it locks into place and fits the locking tab.

> **Note**
>
> Ceiling mounting is recommended for optimal coverage performance.

Mounting Instructions for GWN7600LR

Please refer to the following steps for the mounting your GWN7600LR correctly.

1. Prepare the Cover Bracket by inserting the 4 screws (PM8) into corresponding holes.
2. Attach the Cover Bracket with screws on the vertical/horizontal Mounting Bolt were GWN7600LR will be installed.
3. Assemble the Base Bracket with the Cover Bracket using provided locknuts and screws (PM8).
4. Connect the Ethernet cable (RJ45) to the correct ports of your GWN7600LR.
5. Align the GWN7600LR with the Base Bracket and pull it down to the right position.
6. Install the 2x Assembled screws to fix GWN7600LR on the Mounting Bolt.
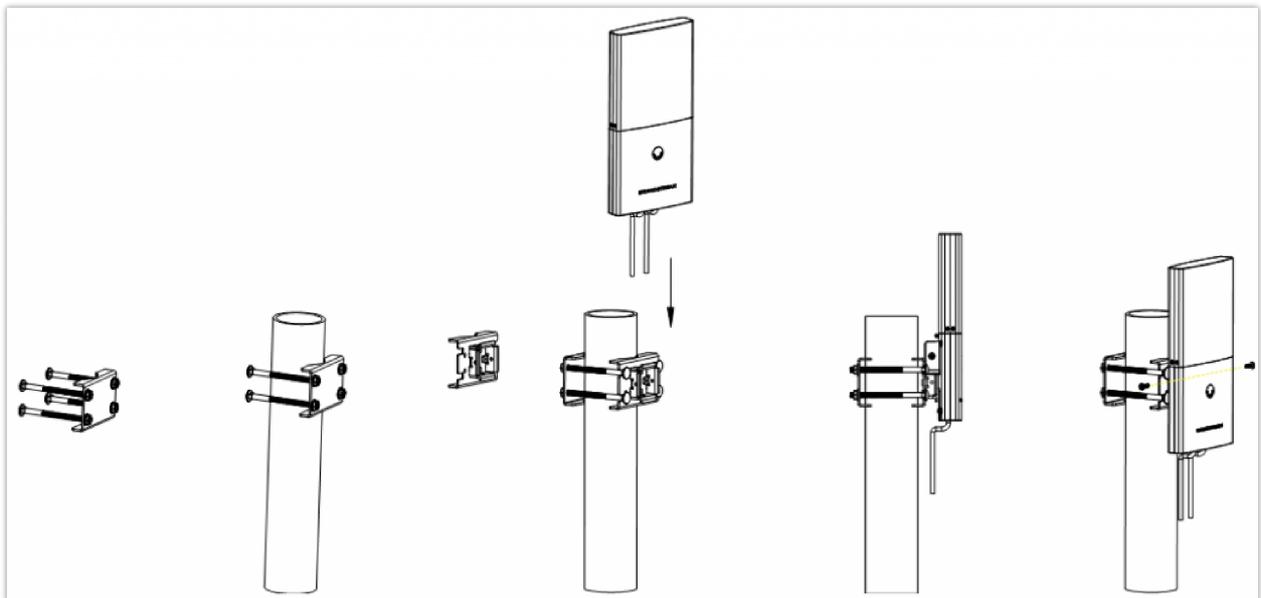
GWN7600LR Vertical Mounting
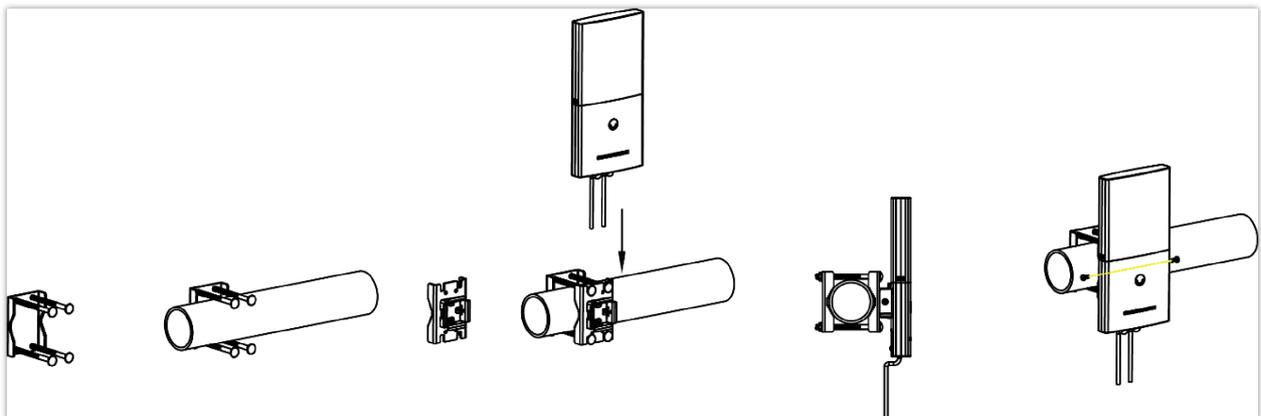
GWN7600LR Horizontal Mounting

Mounting Instructions for GWN7630LR/GWN7605LR/GWN7660LR/GWN7664LR

GWN7630LR can be mounted on the wall or on a metal bar. Please refer to the following steps for the appropriate installation.
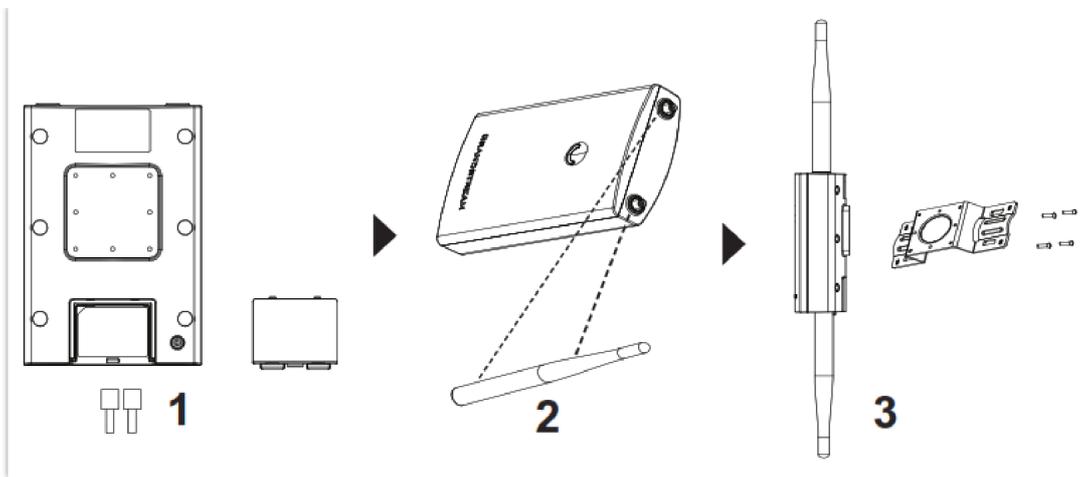
GWN7630LR/GWN7605LR/GWN7660LR /GWN7664LR Mounting Instructions

1. Connect the Ethernet cable (RJ45) to the correct port of your GWN7630LR/GWN7605LR/GWN7660LR/GWN7664LR and insert the cover bracket.

2. Connect each antenna to an antenna connector by rotating it clockwise.

3. Attach the Base bracket with screws (PM 3.0×7) on the back of GWN7630LR /GWN7605LR/GWN7660LR/GWN7664LR access point.

Wall Mount
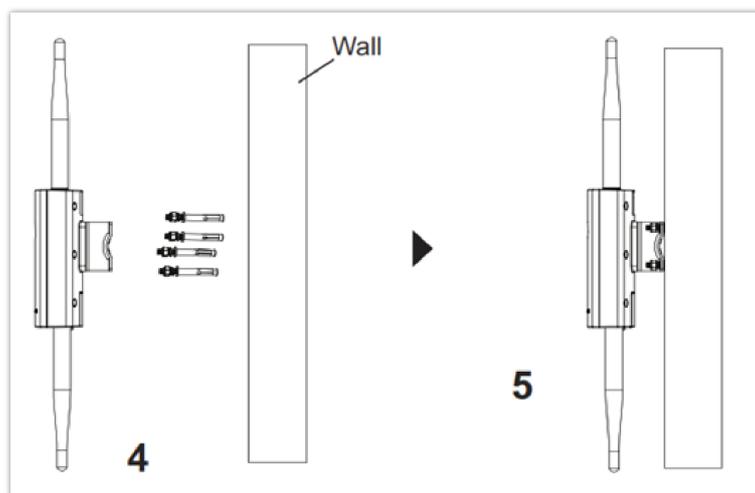
GWN7630LR/GWN7605LR/GWN7660LR Wall Mount

1. Drill four holes on the wall referring to the positions of the ones on the base bracket. Then, fix an expansion screw in each hole.

2. Attach the GWN7630LR/GWN7605LR/GWN7660LR/GWN7664LR access point by securing the Base Bracket with the expansion screws on the wall.

Pole Mount
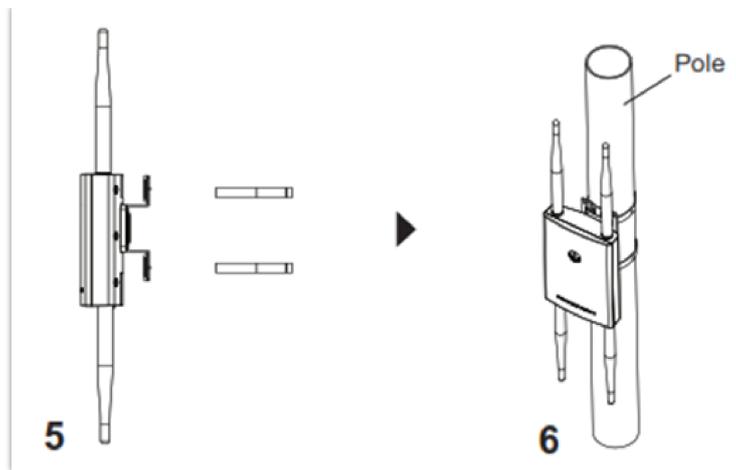
GWN7630LR/GWN7605LR/GWN7660LR /GWN7664LR Pole Mount

1. Open the metal straps by turning the locking mechanism counter-clockwise. You can loosen it by hand or use a flathead screwdriver.

2. Straighten out the end of the metal straps and slide it through the back of the base bracket.

3. Wrap the metal strap around the pole and use a flathead screwdriver to tighten the locking mechanism by turning it clockwise.

Mounting Instructions for GWN7624

GWN7624 can be mounted on the wall, Please refer to the following steps for the appropriate installation.

Wall Mount (GWN7624)

1. Use a measuring tape to measure the distance between the four wall mount slots on the back of the GWN7624 access point and use a pencil to mark the mounting screw holes on the wall.

2. Drill the holes in the spots that you have marked, then attach the wall mount to the wall via the wall mount slots.

3. Use the black screws to mount the GWN7624 main body on the wall mount after mounting the wall mount on the wall.

Wall Mount
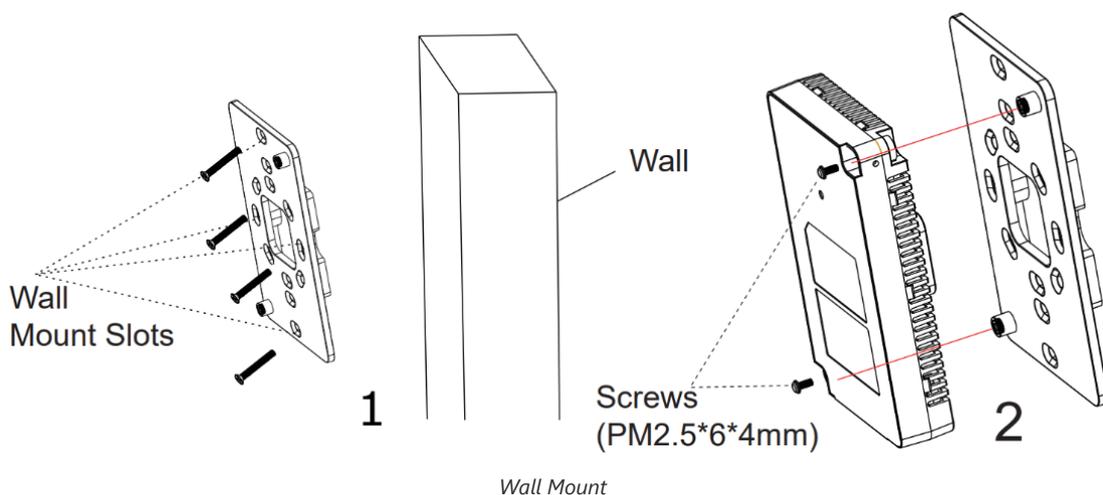
4. Attach the front cover with the GWN7624 body and then the grey screw on the side.
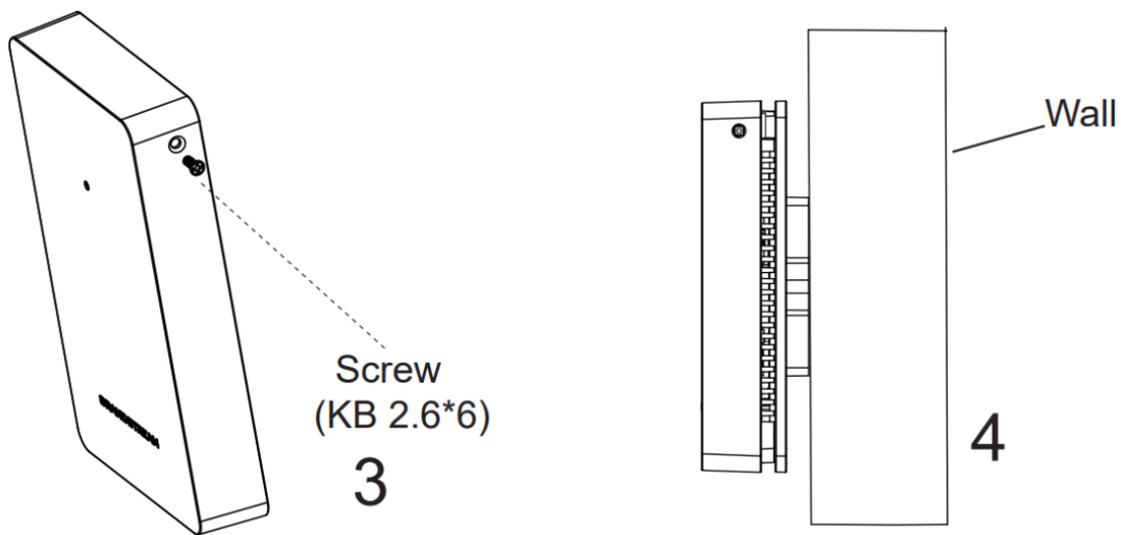
GWN7624 Wall Installation

Mounting Instructions for GWN7602

GWN7602 can be mounted on the wall, Please refer to the following steps for the appropriate installation.

Wall Mount (GWN7602)

1. Use a measuring tape to measure the distance between the two wall mount slots on the back of the GWN7602 access point and use a pencil to mark the mounting screw holes on the wall.

2. Drill the holes in the spots that you have marked and slide the anchors into the wall. Attach the GWN7602 access point to the wall via the wall mount slots.
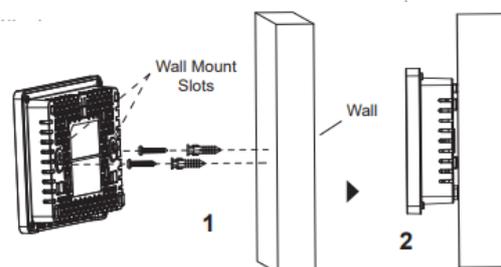
GWN7602 Wall Mount

GETTING STARTED

The GWN76XX Wireless Access Point provides an intuitive web GUI configuration interface for easy management to give users access to all the configurations and options for the GWN76XX's setup.

This section provides step-by-step instructions on how to read LED patterns, discover the GWN76XX and use its Web GUI interface.

LED Patterns

The panel of the GWN76XX has different LED patterns for different activities, to help users read the status of the GWN76XX whether it is powered up correctly, provisioned, in upgrading process and more, for more details please refer to the below table.

LED Status	Indication
OFF	Unit is powered off or abnormal power supply

Blinking green	Firmware update in progress
Solid green	Firmware update successful
Blinking red	Delete paired slave – Factory reset initiated
Solid red	Firmware update failed
Solid purple	Unit not provisioned
Blinking blue	Unit provisioning in progress
Solid blue	Unit is provisioned successfully
Blinking White	Used for Access Point location feature
Solid Yellow	Mesh disconnection

LED Patterns

Discover the GWN76XX

Once the GWN76XX is powered up and connected to the Network correctly, users can discover the GWN76XX using one of the below methods:

Method1: Discover the GWN76XX using its MAC address

1. Locate the MAC address on the MAC tag of the unit, which is on the underside of the device, or on the package.
2. From a computer connected to same Network as the GWN76XX , type in the following address using the GWN76XX's MAC address on your browser https://gwn_<mac>.local

Example

if a GWN76XX has the MAC address 00:0B:82:8B:58:30, this unit can be accessed by typing https://gwn_000b828b5830.local/ on the browser.
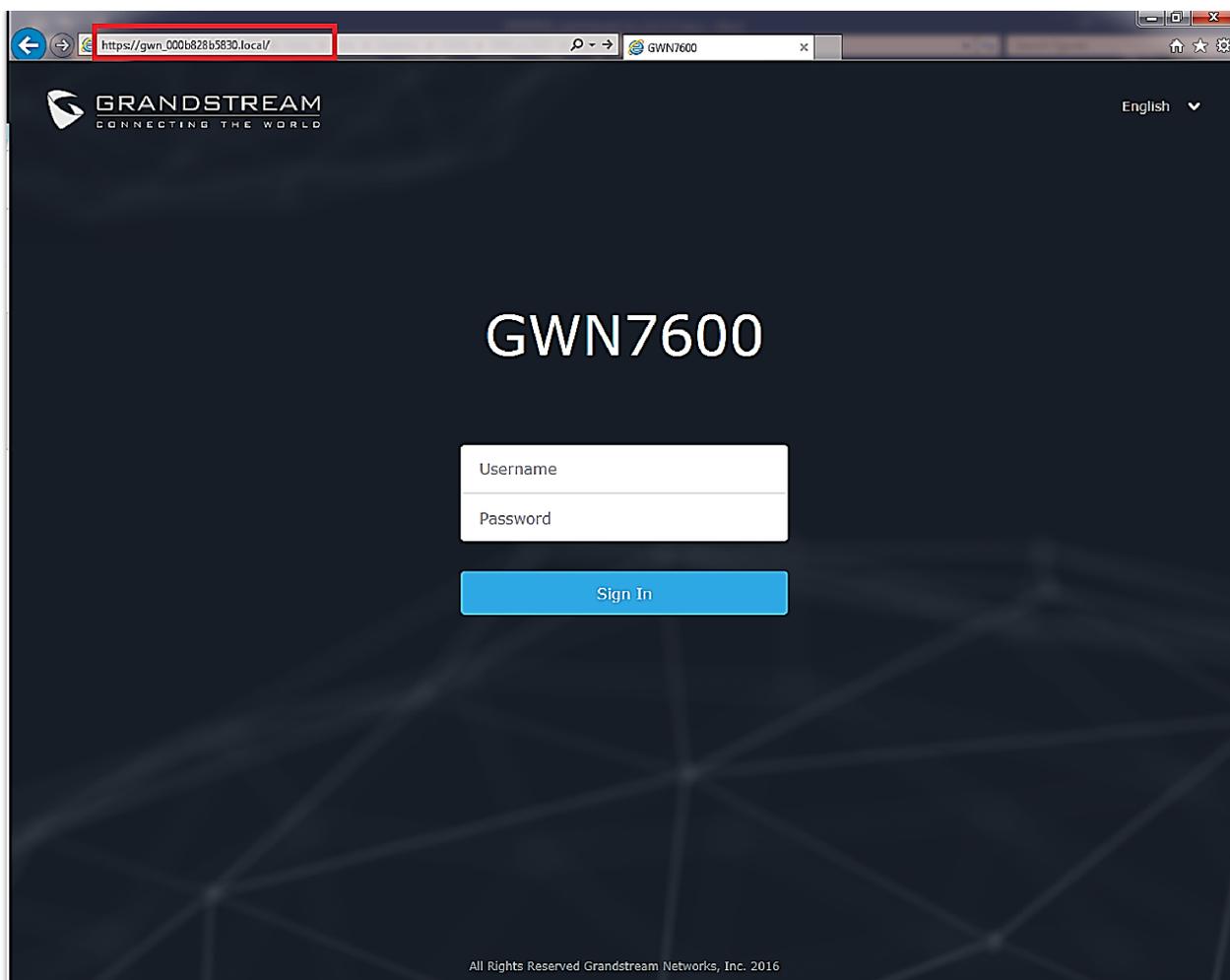
Discover the GWN76XX using its MAC Address

Method 2: Discover the GWN76XX using GWN Discovery Tool

1. Download and install **GWN Discovery Tool** from the following link: https://www.grandstream.com/support/tools

2. Open the GWNDiscoveryTool, click on **Select** to define the network interface, then click on **Scan**.

3. The tool will discover all GWN76XX Access Points connected on the network showing their MAC, IP addresses and firmware version.

4. Click on **Manage Device** to be redirected directly to the GWN76XX's configuration interface, or type in manually the displayed IP address on your browser.

GWN Discovery Tool

Use the Web GUI

Users can access then the GWN76XX using its WebGUI, the following sections will explain how to access and use the Web Interface.

Access Web GUI

The GWN76XX embedded Web server responds to HTTPS GET/POST requests. Embedded HTML pages allow users to configure the device through a Web browser such as Microsoft IE, Mozilla Firefox, Google Chrome and etc.

To access the Web GUI:

1. Make sure to use a computer connected to the same local Network as the GWN76XX.

2. Ensure the device is properly powered up.

3. Open a Web browser on the computer and type in the URL using the MAC address as shown in [Discover the GWN76XX] or the IP address using the following format: ***https://IP_Address***

4. Enter the administrator's login and password to access the Web Configuration Menu. The default administrator's username is always "admin" and password is the unique default *Wi-Fi Password* available on the sticker on the back of the unit.

   Note

   GWN AP's web UI access will be locked for 15 mins after 5 login failures

   Note:

   GWN7602 doesn't support embedded Web server, it can only be managed through another GWN access point as a slave, GWN Cloud or GWN Manager.

WEB GUI Languages

Currently the GWN76XX series web GUI supports 17 languages including English, Chinese, Spanish etc. Users can select the displayed language at the upper right of the web GUI either before or after login.
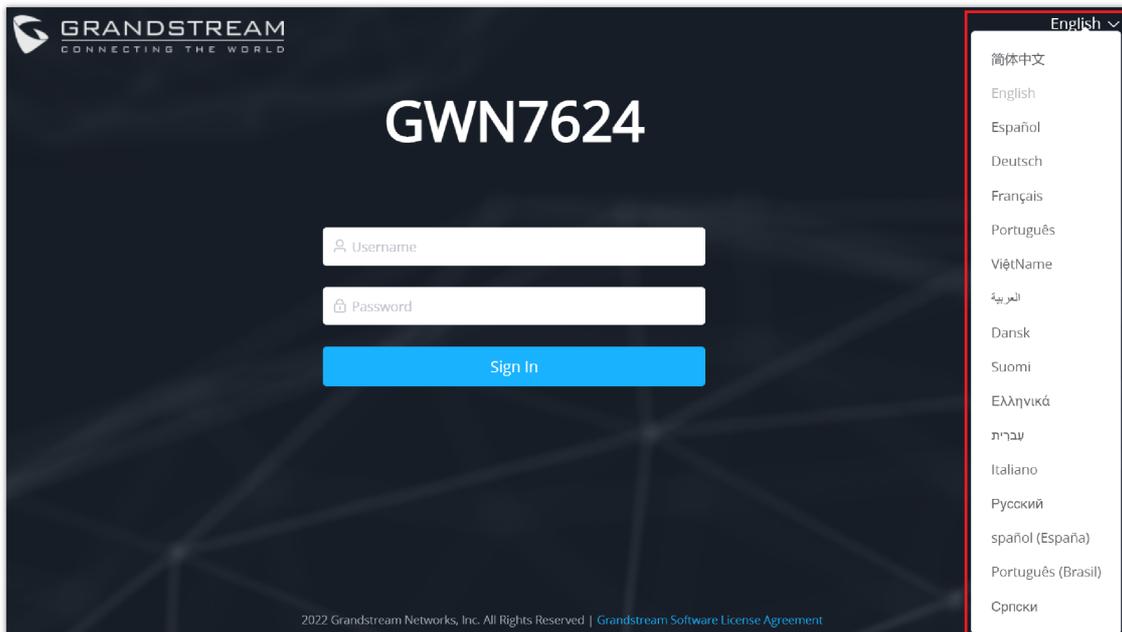
GWN76XX Web GUI Langage (Login page)
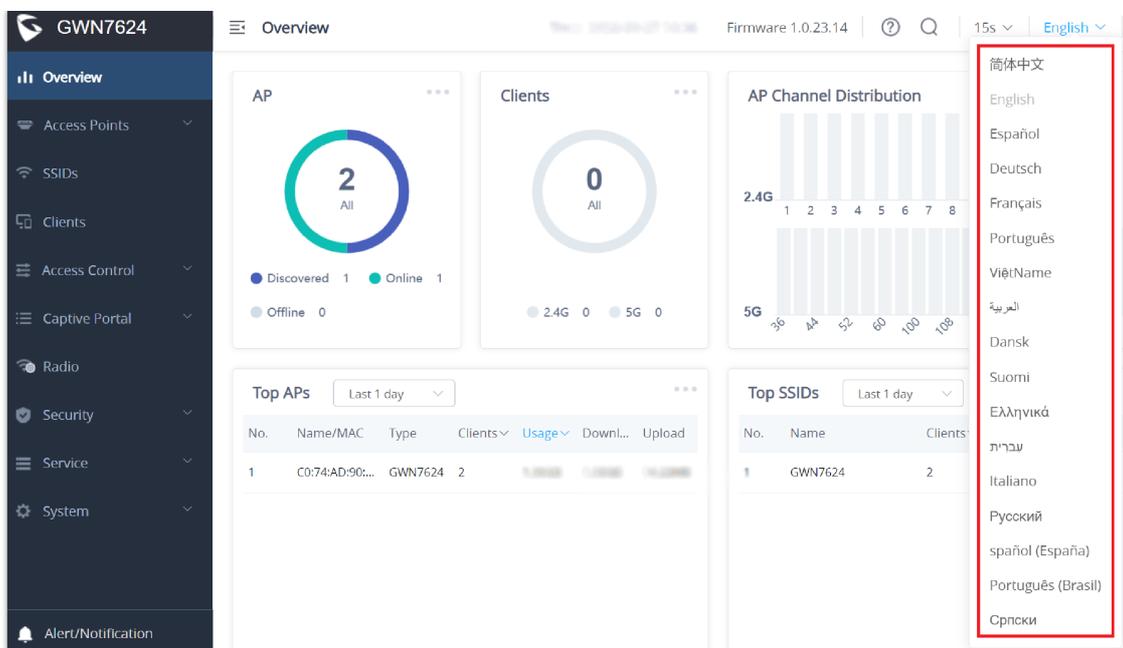
GWN76XX Web GUI Language (Web Interface)

Overview Page

Overview is the first page shown after successful login to the GWN76XX's Web Interface. Overview page provides an overall view of the GWN76XX information presented in a Dashboard style for easy monitoring along with firmware version and date-time information at the top.
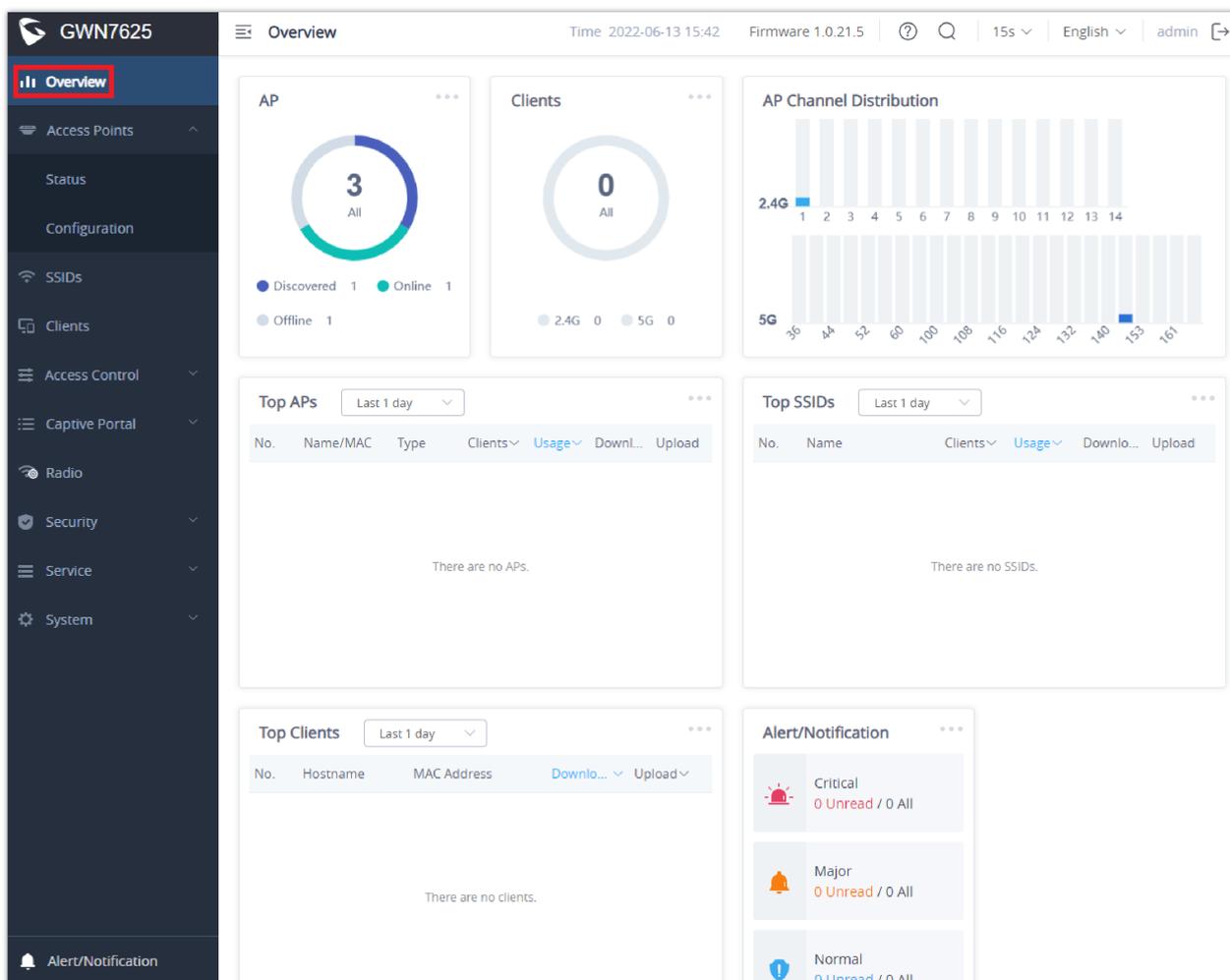
GWN76XX Dashboard (GWN7625 as example)

Users can quickly see the status of the GWN76XX for different items, please refer to the following table:

AP	Shows the number of Access Point that are Discovered, Paired (Online) and Offline. Users may click on ••• to go to Access Points page for basic and advanced configuration options for the APs.
Clients	Shows the total number of connected clients, and a count for clients connected to each Channel. Users may click on ••• to go to Clients page for more options.
AP Channel Distribution	Shows the Channel used for all APs that are paired with this Access Point.
Top AP	Shows the Top APs list, users may assort the list by number of clients connected to each AP or data usage combining upload and download. Users may click on ••• to go to Access Points page for basic and advanced configuration options for the APs.
Top SSID	Shows the Top SSIDs list, users may assort the list by number of clients connected to each SSID or data usage combining upload and download. Users may click on ••• to go to SSID page for more options.
Top Clients	Shows the Top Clients list, users may assort the list of clients by their upload or download. Users may click on ••• to go to Clients page for more options.
Alert/Notification	Shows 3 types of Alert/Notifications: Critical, Major and Normal. Users can click ••• to pop up the list of Alert and Notifications.

Overview

Note

Note that Overview page in addition to other tabs can be updated each 15s, 1min ,2min and 5min or Never by clicking ⌄ in the upper bar menu (Default is 15s).

New Firmware Notification: Starting from firmware version 1.0.5.13/1.0.5.14, and once a different OFFICIAL firmware is released on Grandstream Networks website, the master AP will popup reminder notification to the administrator in order to upgrade the device. You can click on *New* button in order to be redirected to the release note of the new firmware version, for upgrading steps please refer to section [UPGRADING AND PROVISIONING].

Save and Apply Changes

When clicking on "Save" button after configuring or changing any option on the web GUI pages. A message mentioning the number of changes will appear on the upper menu. Click **Apply** button to apply changes.

You have **2 changes** not applied. **Apply** **Revert**

Apply Changes

GWN MANAGEMENT PLATFORMS

GWN.Cloud

Starting from firmware 1.0.6.41/1.0.6.43, the GWN76XX can be managed by your **GWN.Cloud** account, **GWN.Cloud** web interface now can be accessed at https://www.gwn.cloud.

GWN.Cloud Architecture

GWN Manager

Starting from firmware 1.0.13.1, the GWN76XX can be managed and monitored by your **GWN Manager** account, GWN Manager On-premises Access Points Controller platform can be installed using the link below:

https://www.grandstream.com/support/firmware

GWN Manager Architecture

Note:

GWN Manager installation is supported on virtual machines. Please refer to GWN Management Platform User Guide for more detailed information.

USING GWN76XX AS STANDALONE ACCESS POINT

The GWN76XX can be used in Standalone mode, where it can act as Master Access Point Controller or in Slave mode and managed by another GWN76XX Master.

This section will describe how to use and configure the GWN76XX in standalone mode.

Connect to GWN76XX Default Wi-Fi Network

GWN76XX can be used as standalone access point out of box, or after factory reset with Wi-Fi enabled by default.

After powering the GWN76XX and connecting it to the network, GWN76XX will broadcast a default SSID based on its MAC address GWN [MAC's last 6 digits] and a random password.

Note that GWN76XX's default SSID and password information are printed on the MAC tag of the unit as shown on the below figure.
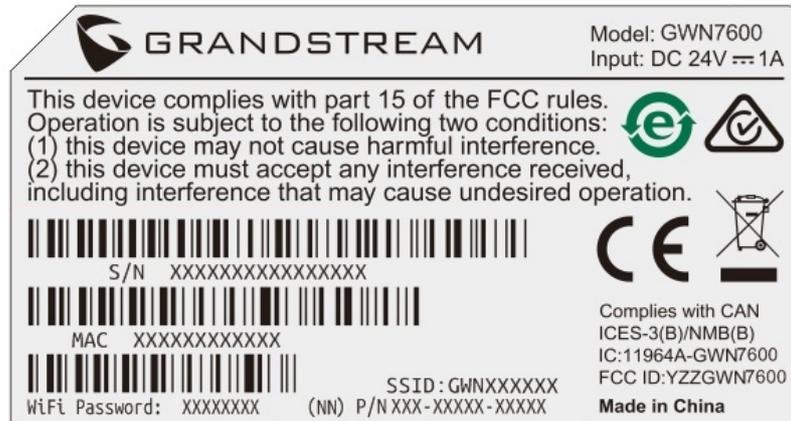
MAC Tag Label

USING GWN76XX AS MASTER ACCESS POINT CONTROLLER

Master Mode allows a GWN76XX to act as an Access Point Controller managing other GWN76XX access points. This will allow users adding other access points under one controller and managing them in an easy and a centralized way

Master/Slave mode is helpful with large installations that needs more coverage area zones with the same controller.

Login Page

Login Page

After login, users can use the Setup Wizard tool to go through the configuration setup or exit and configure it manually. Setup Wizard can be accessed anytime by clicking on while on the web interface.
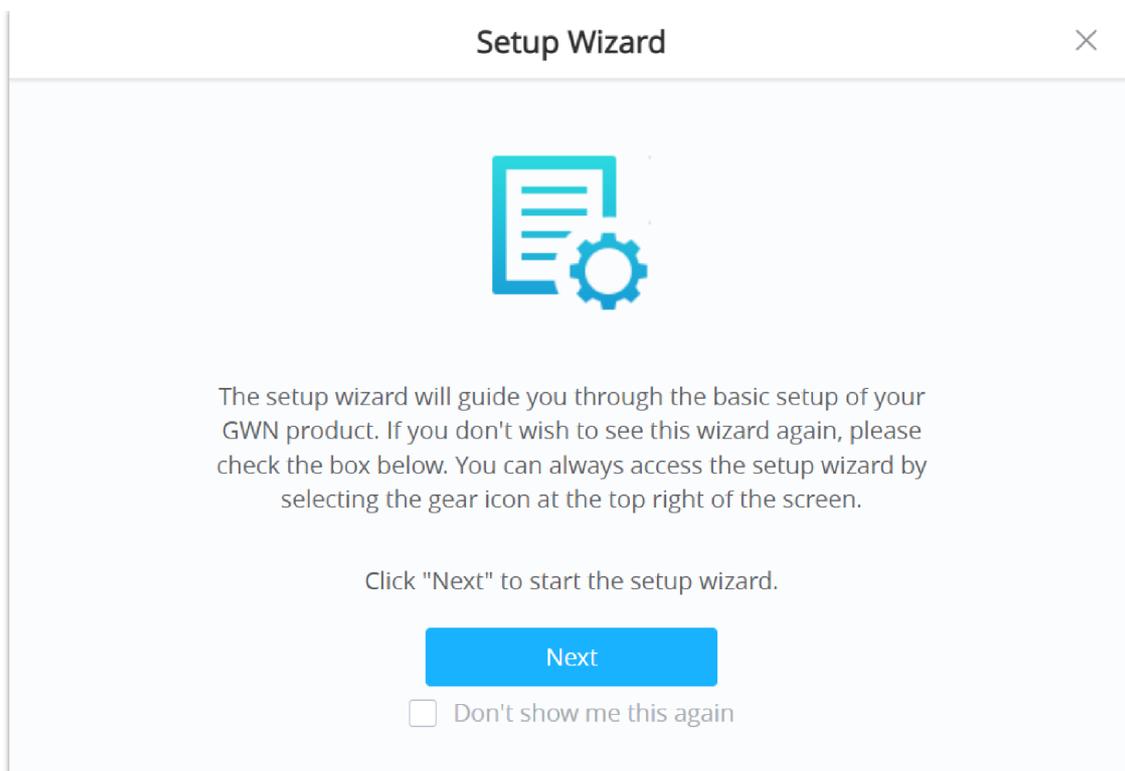
Setup Wizard

Discover and Pair Other GWN76xx Access Point

First, note that by default the GWN controller access point will automatically discover all APs connected to the same LAN (broadcast domain), there is also a possibility to pair and provision remote APs using DHCP option 43 with master direction explained below.

Master Direction

To pair and manage access points located on remote networks, the admin needs to configure the IP address of master AP on DHCP option 43 which will be send to the slave access point during booting stage and allow the save/master connection to be established remotely. GWN76xx accepts option 224 encapsulated in option 43, and the syntax is in TLV format. A simple example of DHCP 43 configuration would be:

224(Type)12(Length)10.157.0.234(Value) translated into Hex as e00c31302e3135372e302e323334

Scenario example: a company has two offices connected via VPN (master AP located on network 192.168.1.0/24 and slave AP located on remote network 192.168.2.0/2). On remote network the admin can set DHCP option 43 using GWN70xx router as following value:

encap:43,224,"192.168.1.100".

The slave AP has the option "Allow DHCP Option 43 to override GWN Manager Address" enabled by default.
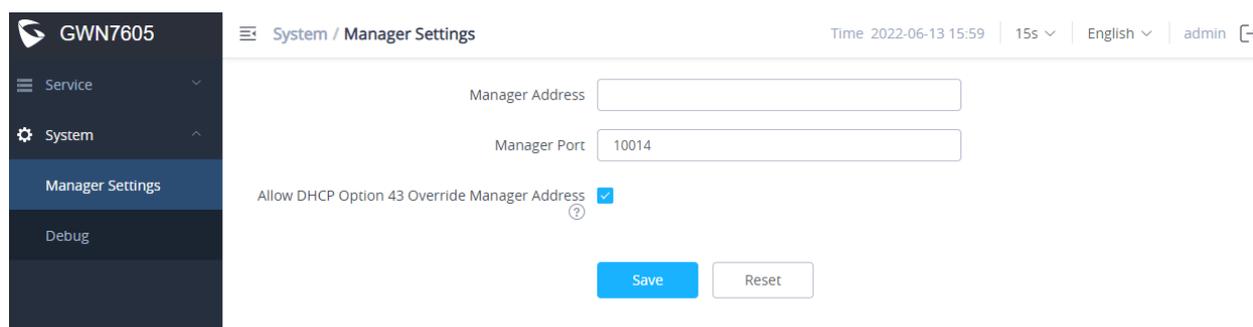
Option 43 Override

After that, the slave AP will be listed on the master AP discovered devices and ready for paring and provisioning process which is described on the next steps.

To Pair a GWN76XX access point connected to the same Network as the GWN76xx follows the below steps:

1. Connect to the GWN76xx Web GUI as Master and go to **Access Points → Configuration.**
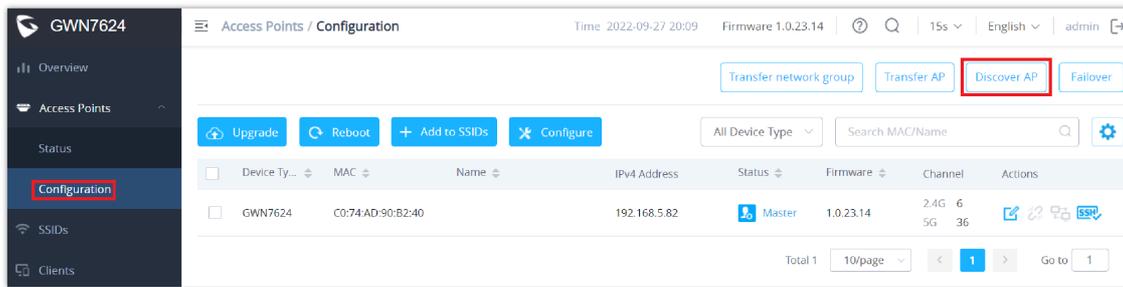
Discover and Pair GWN76XX

2. Click on **Discover AP** to discover access points within GWN76xx Network, the following page will appear.
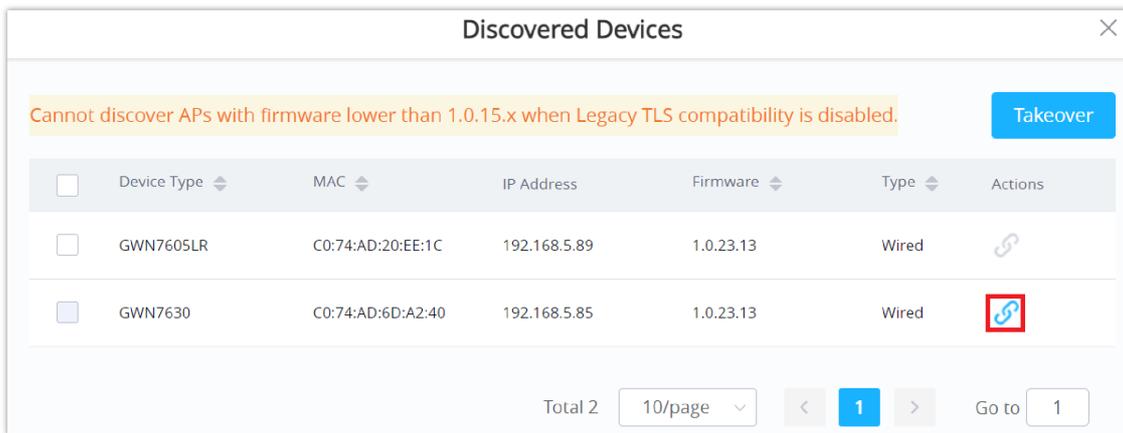
Discovered Devices

3. Click on Pair 🔗 under Actions, to pair the discovered access point as slave with the GWN76xx acting as Master.

The paired GWN76XX access point will appear Online, users can click on 🔗 to unpair it.
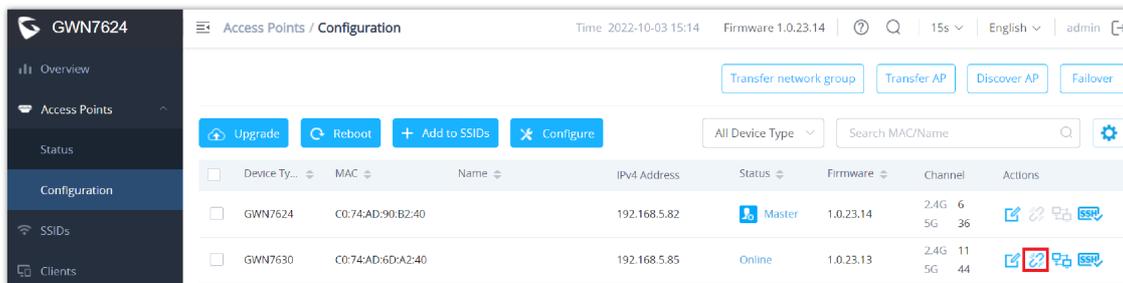
GWN76XX Online

If a GWN76XX is not being discovered or the pair icon is grey color, make sure that it is not being paired with another GWN76XX Access Point acting as Master Controller. If yes, users will need to unpair it first, or reset it to factory default settings in order to make it available for pairing by other GWN76XX Access Point Controller

AP Location

GWN76xx supports a handy feature which allows users to locate other Access points by blinking LED. To use the feature, navigate on the master web GUI under "**Access Points → Status**" page and click on the icon 👤 near the desired AP, and it corresponding unit will start blinking the LEDs.

Transfer AP – Transfer Network Group

Users can easily transfer the AP from local master to the **GWN Cloud** or **GWN Manager** account by clicking on [Transfer AP] When you already have Network/Wi-Fi configurations on your GWN account, using this feature will let you choose existing Network/SSID to adopt your local AP.

Transfer AP

Transferable devices (Online and supported by cloud or GWN Manager):

C0:74:AD:90:B2:40   C0:74:AD:6D:A2:40

Untransferable devices:

There are no untransferable devices.

Transfer To   GWN Cloud

GWN Cloud

GWN Manager

Transfer AP

This feature [Transfer network group] will allow you to transfer your local configurations to your cloud account. For more details, please refer to GWN.Cloud User Guide.

Failover Master

In a Master-Slave architecture, having a backup Master is critical for redundancy and failover function, thus, and in order to avoid a single point of failure in your wireless network, you can specify a slave AP as failover master. Whenever it detects the master is down, it will promote itself as failover master within a time frame of around 20~30 minutes by entering failover mode. After then, if the master AP comes back, failover master will automatically go back to slave mode, or if the master does not come back to alive, Administrator can login using "failover" account to turn the failover master as true master and take over all controls.
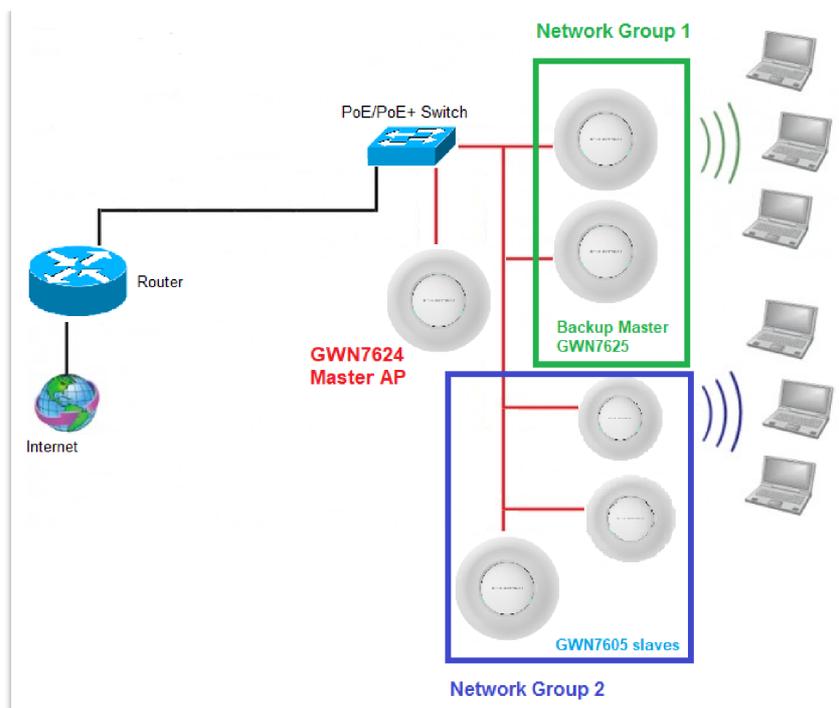
Failover Master

Users could select the Failover Master by following below steps:

Log into Web GUI of the Master access point then navigate to **Access points → Configuration** then click on [Failover] and finally select the candidate access point from the drop-down list to be used as a Failover AP.
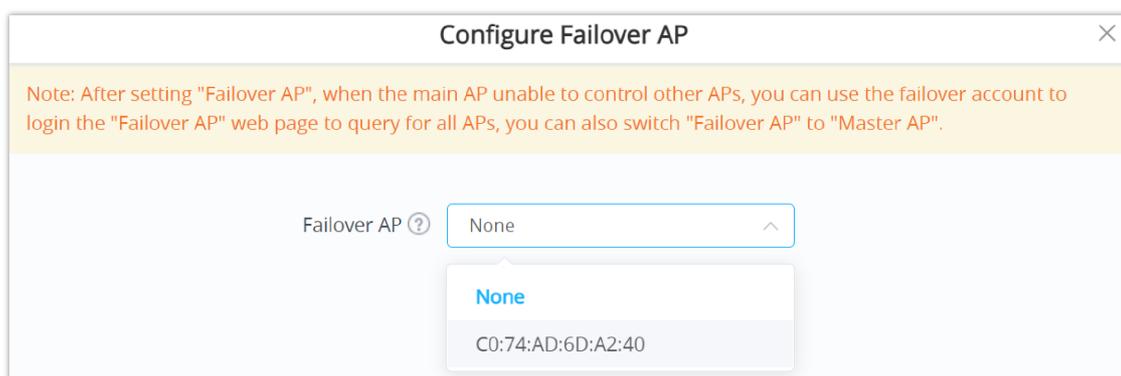
Failover AP

Failover Mode

Once failover slave has been selected, the primary master will send the configuration of the network to the failover slave and the slave will start monitoring the status of the primary master to detect any failure for any reason (network connection loss, power outage).

In case of failure, the failover slave will promote itself to a temporary backup master while waiting for the primary master to come back.

During the failover mode users could access the web GUI of the failover slave using a special failover account with same admin password.

- **Username = failover**
- **Password = admin password**
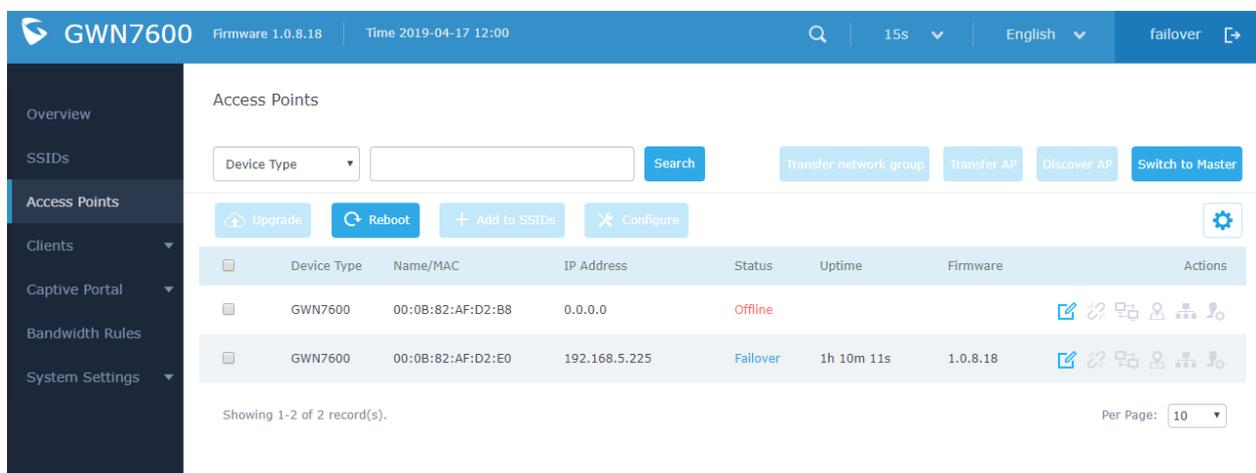
Failover Mode GUI

The failover mode has only read permission on the configuration and limited options, users still can reboot other slave Access points in case it is needed.

Users also can press on **« Switch to Master »** button in order to set the failover slave as the new primary master of the wireless network, once this is done they have full write permission control over the web GUI option as usual. Use that button to switch to master and takeover the rest of the APs.

Important notes

If you click « Switch to Master », this would be become a non-revertible behavior. Failover Slave will become actual master and the prior master cannot take back the control anymore.

When Failover Slave is switched to Master, you will use the Prior Master AP credentials: username: admin, and the admin password.

Otherwise, when original master comes back online, then Failover Slave will become slave again to prior original Master.

Takeover Feature

This feature is used to re-pair the slave APs whose master has gone offline with another master AP in the same subnet. Please follow the steps to takeover slave APs from other master:

Step 1. Login to the Web GUI of Master and click on "Discover APs" in the Access Points Page.
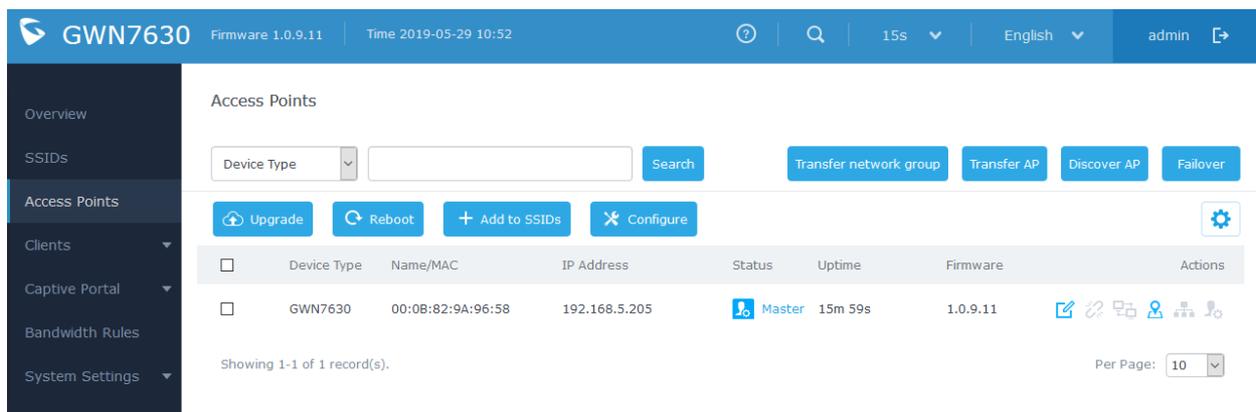
Takeover – Step 1

Step 2. Select the one or multiple APs to be taken over then click on "takeover" button of the target AP.

Takeover – Step 2

Step 3. Enter the Takeover key which is the admin password of the previous master AP.
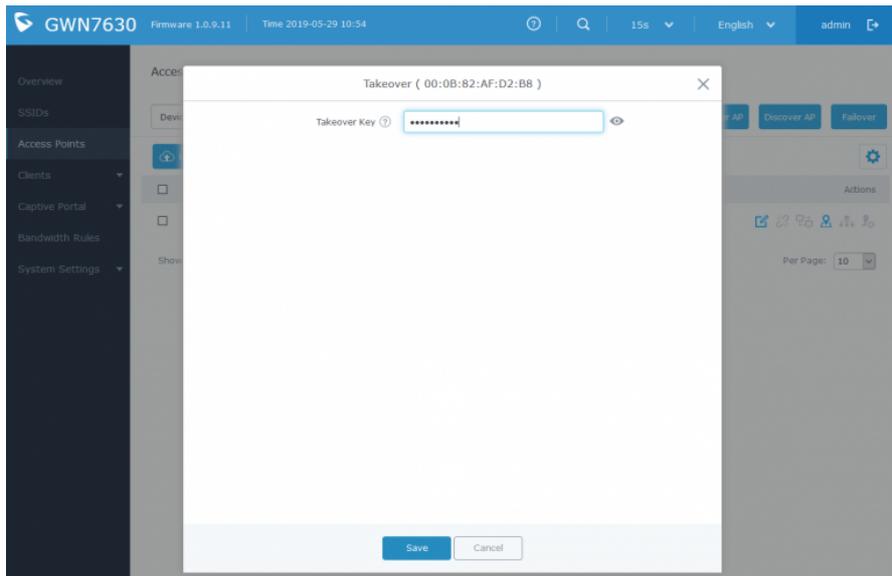
Takeover – Step 3

Transfer to Master

From the Master Access Point, the Administrator do have the capability to assign any Slave Access point to become the new Master to manage all the already paired Access points. Except for GWN7602, it can only be a slave to another GWN76xx access point.
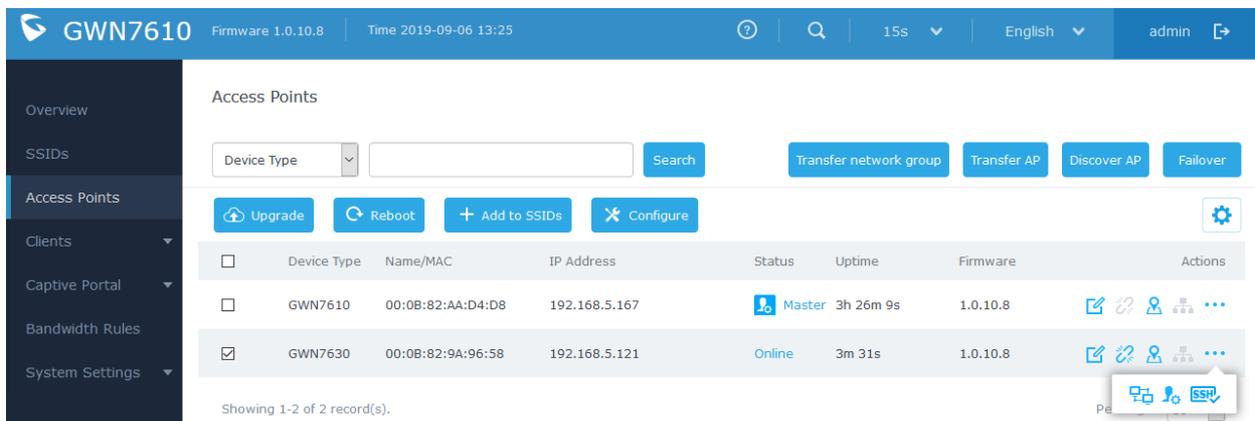
Switch to Master

⋯ After you click on then press the "Switch to Master" button, the following warning message will prompt in order to confirm the procedure:

Transfer Master Role to another device confirmation message

When the process is finished, the original Master will turn to be a slave for the new Assigned Master, and to login to the new Master AP web interface, you will need to use the previous Master Admin password.

Then new assigned Master AP web interface

Note

All the previously existed paired APs will be provisioned with the new Master AP.

The Switch to Master option is unlimited action and does not require any reset for the already paired Aps.

Client Bridge

The Client Bridge feature allows an access point to be configured as a client for bridging wired only clients wirelessly to the network. When an access point is configured in this way, it will share the Wi-Fi connection to the LAN ports transparently. This is not to be confused with a mesh setup. The client will not accept wireless clients in this mode.

··· Once a SSID has the Client Bridge Support enabled, the AP adopted in this SSID can be turned in to Bridge Client mode by click the then the Bridge button ⊞ .

Please be noted that once an AP it turned into Client Bridge mode, it cannot be controlled by a Master anymore, and a factory reset is required to turn it back into normal AP mode.

Client Bridge

Client Bridge

In order to verify, you may access the bridged AP configuration, then under **Status,** the option "Client Bridge Mode" would be set to **Isolated** like shown on the figure down below:

Client Bridge Mode

Important notes

The access point that will be operating on bridge mode, must be set with a fixed IP address before activating the bridge mode on the access point.

Users must enable client bridge support option under SSID or SSID Wi-Fi settings in order to have it fully functional.

The Client Bridge requires the SSID to not have any VLAN ID enabled

USING GWN76xx AS SLAVE ACCESS POINT

Slave Mode allows the users to access to specific service and system settings.

*GWN7624 slave login page*

Notes:

- If the AP is slave to a Master controller, the default username is admin, and the default password is the master AP's password.

- If the AP is paired to the GWN.Cloud the default username is admin, and the default password is the SSH Password (GWN.Cloud→System→Settings).
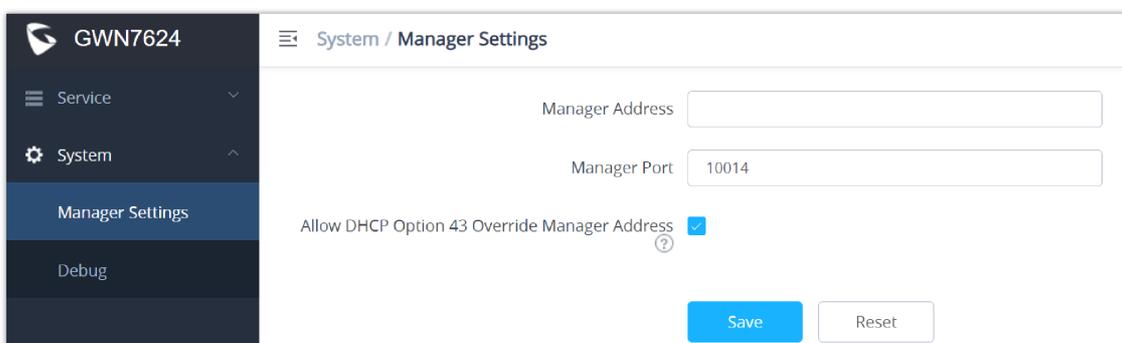
Slave AP Web Interface

Service

The TR-069 interface page allows the settings to enable remote and safe configuration of network devices. Refer to section [TR-069] for details regarding each field.
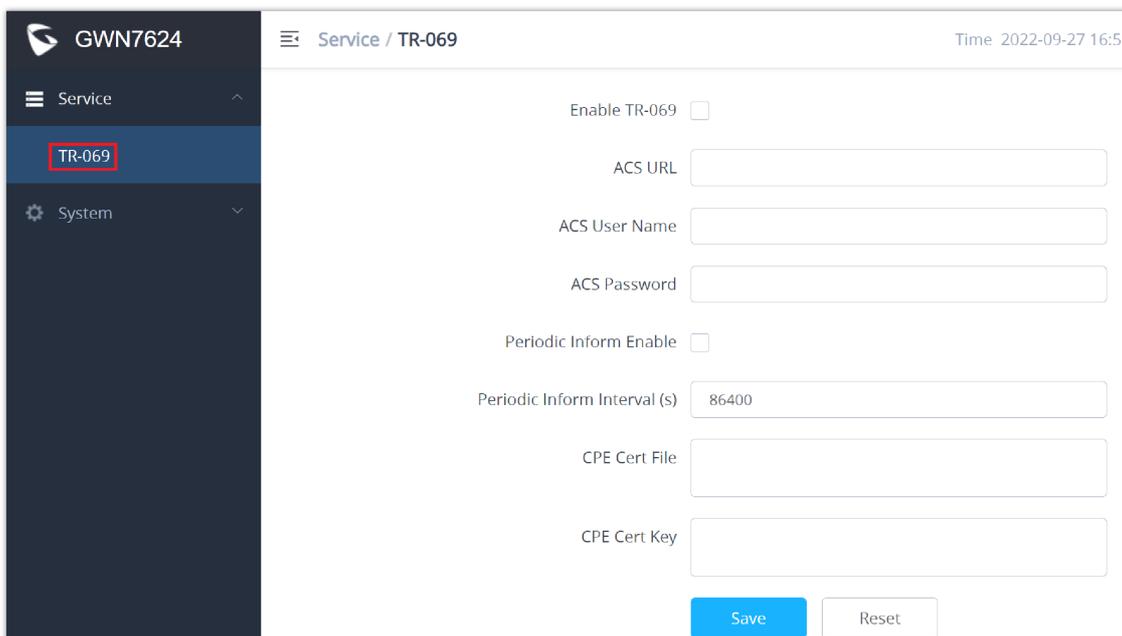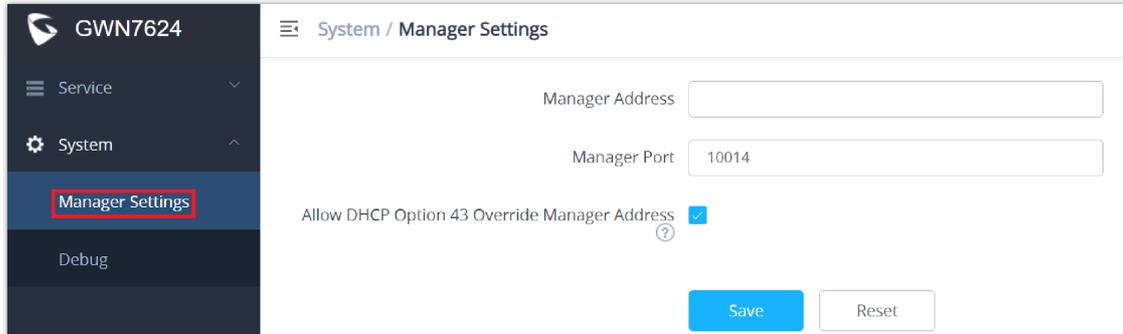

Slave AP Service Settings

System

The system section provides access to the Manager settings and Debug sections.

Manager Settings

The Master (Manager Address) and Port can be found here to GWN7624 be discovered by the Manager.
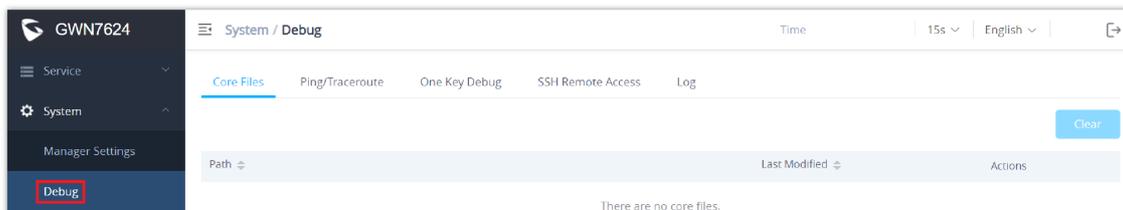

Slave AP manager settings

Manager Address	Enter the IP address of the GWN Manager
Manager Port	Enter the port set for the GWN Manager
Allow DHCP Option 43 Override Manager Address	This configuration will not be effective if AP has been managed by cloud.

Manager settings

Debug

Slave AP debug

Core Files
when a crash event happens on the unit, it will automatically generate a core dump file that can used by engineering team for debugging purposes.

Ping/Traceroute
Allows the users to Ping and traceroute. Input the target's IP address or URL and click on run.

One key Debug
Allows to capture Wireless, Portal or Mesh traffic and logs will be found in Core Files.

SSH Remote Access
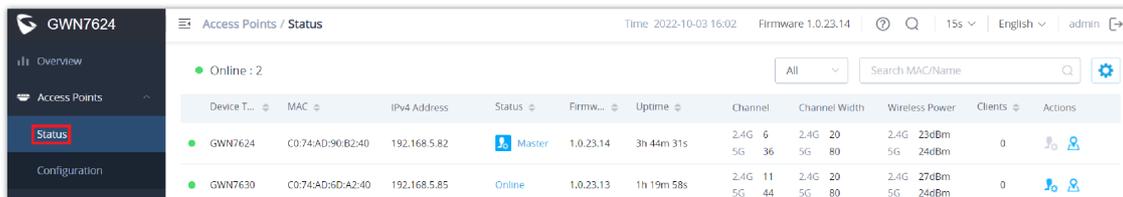Enables the SSH remote access on the slave AP.

Log
Allows the users to retrieve the logs generated for troubleshoot purpose.

ACCESS POINTS

From the access points page, the administrator can monitor different information regarding the access points of the selected network, this section is separated into 2 sub-sections: **Status and Configuration**.

Status

The Status page lists all the access points assigned to the selected network, along with the possibility to perform some basic operations such locating the device (LEDs start blinking in White) or clear the usage data, also users can check more detailed information about each access point and benefit from useful debugging tools which can help diagnose issue when they appear.
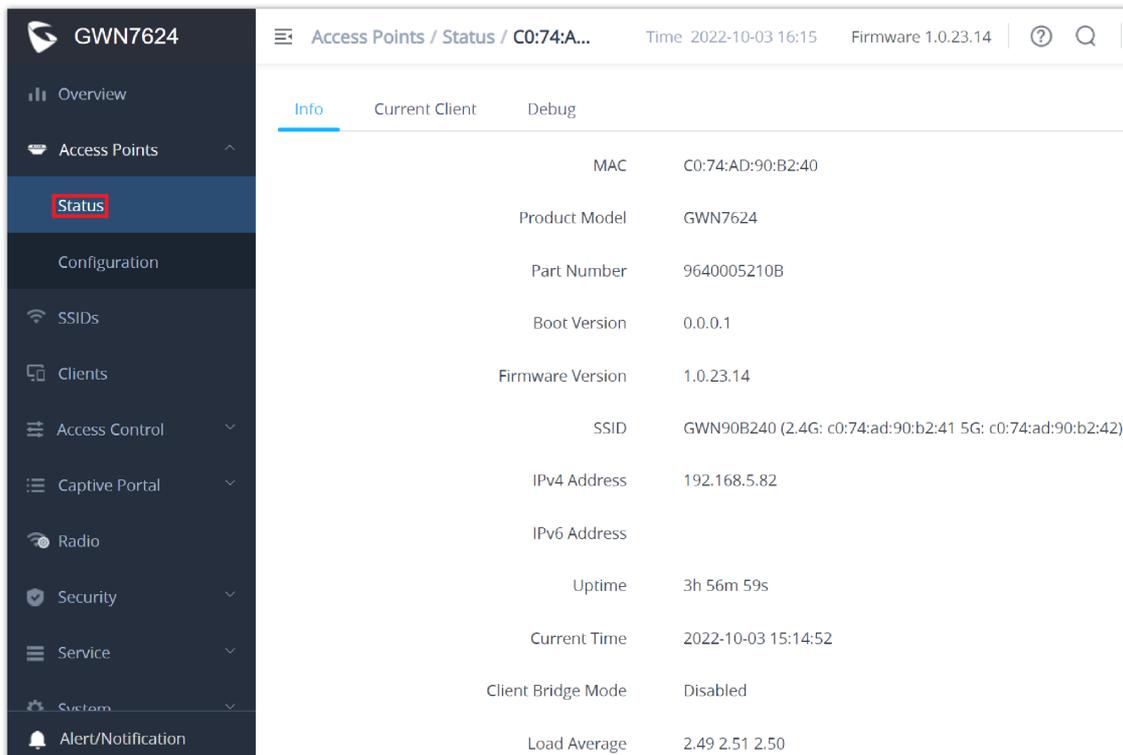

Access Points – Status

To get more detailed information about the status of a specific access point, users can click on the desired AP then a page similar to the following will show up:

AP Info

The first tab "Info" shows general information about the access point such as the firmware version, IP address, Uptime etc. While the second Tab "Current Client" displays the clients connected to this AP and The last Tab is used by administrator for debugging purposes and provides the following tools:

- **Ping/Traceroute** tools, such as the **ping** utility, **traceroute** tool.
- **One Key Debugging,** to capture Wireless, Portal or Mesh traffic and logs will be found in Core Files.
- **Core Files,** when a crash event happens on the unit, it will automatically generate a coredump file that can used by engineering team for debugging purposes.
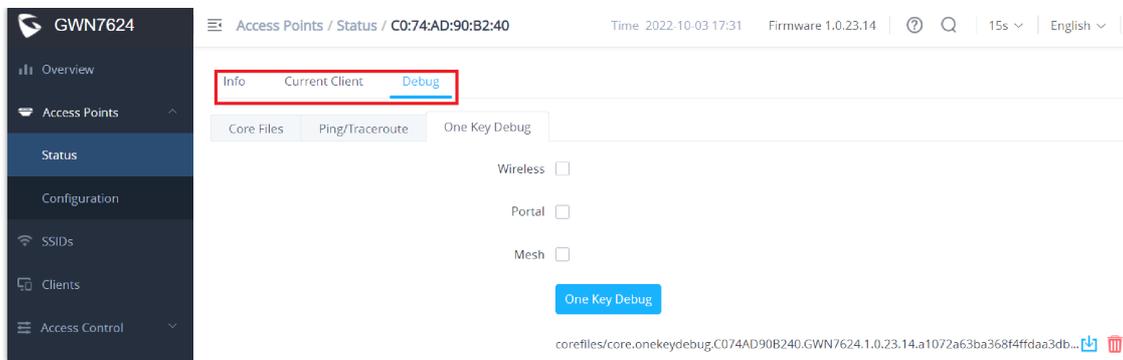
Debug Tool Tab

Configuration

The configuration page allows the administrator to Upgrade, Reboot, Add to SSIDs, Configure, Transfer network group, Transfer AP, Discover AP, Failover.
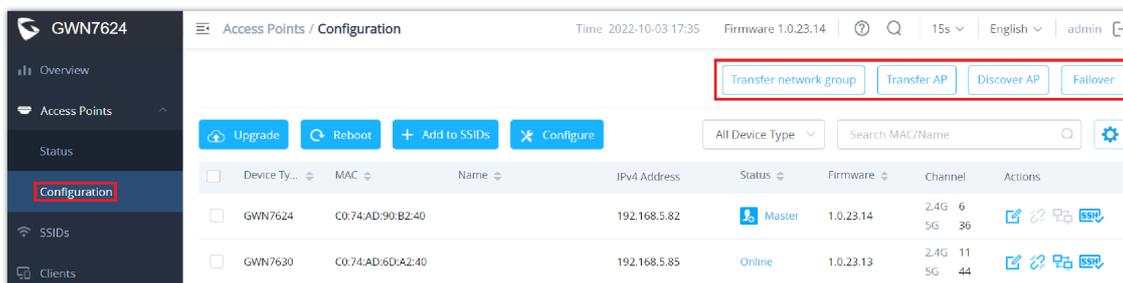
GWN7624 Configuration Page

Upgrade

Select slave AP(s) to upgrade and press [Upgrade] button.

Refer to [Upgrading Slave Access Points] for more details.

Reboot

Select slave AP(s) to reboot and press [Reboot] button.

Reboot Slave

Select slave AP(s) to reboot and press [Reboot] button.

- There are two methods to add new access points, either manually from the master AP or using GWN Cloud App.
- Please refer to [*Adopt GWN76XX to GWN Manager*] section in this manual.

Move Access Points

The administrator can move GWN Access points from one network to another. Click on Move button and the following window will popup, select the network where to move the access point and click on move.
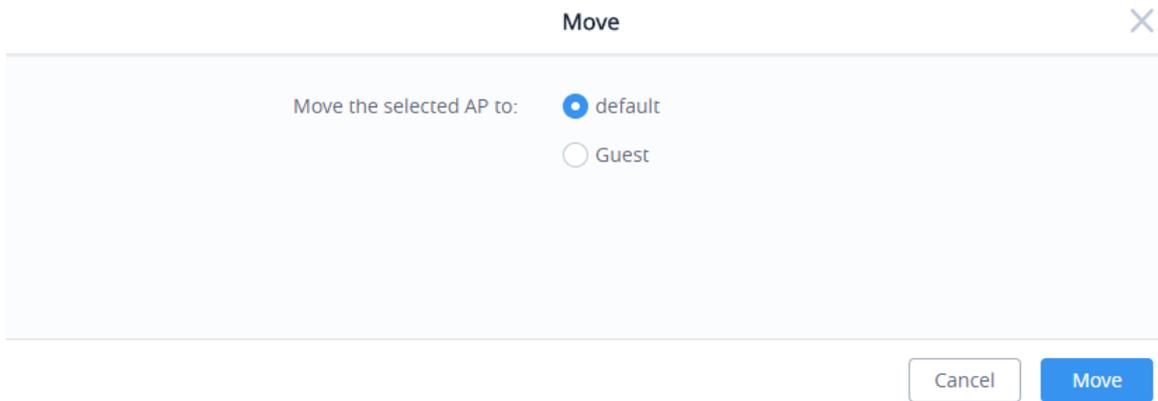
Moving Access Points between Networks

Delete Access Points

To delete an access point, select it, then click on reboot button, the following confirmation message will be displayed:

Delete Access Point
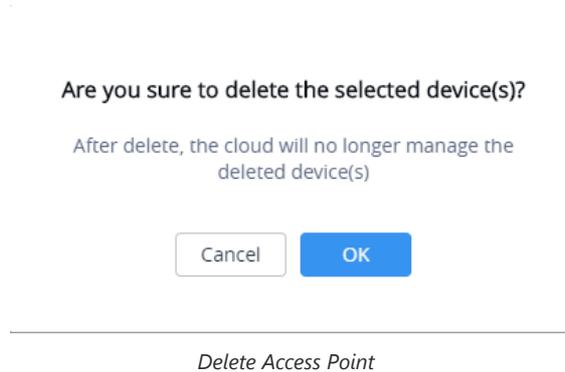
Reboot Access Points

To reboot an Access point, select it then click on Reboot button, the below confirmation message will be displayed:

Reboot Access Point

Configure Access Points

To configure an access point, select and click on Configure button. A new config page will popup:

Access Point Configuration Page

The following settings can be configured from this page:

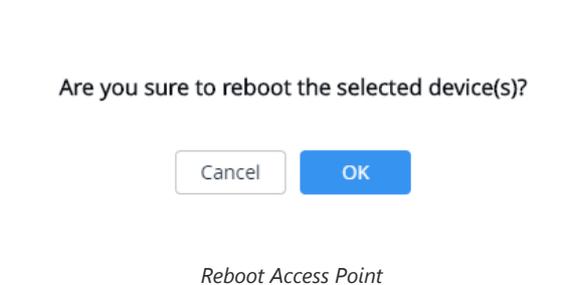| Device Name	Set GWN76xx's name to identify it along with its MAC address.
Fixed IPv4	Check this option to configure the device with a static IP configuration; it must be in the same subnet with the default Network Group; Once enabled, these fields will show up: IPv4 Address/IPv4 Subnet Mask/IPv4 Gateway/Preferred IPv4 DNS/Alternate IPv4 DNS.
Fixed IPv6	Check this option to configure the device with a static IP configuration; it must be in the same subnet with the default Network Group; Once enabled, these fields will show up: IPv6 Address/IPv6 Prefix Length/IPv6 Gateway/Preferred IPv6 DNS/Alternate IPv6 DNS.
Band Steering	Band Steering will help redirecting clients to a radio band 2.4G or 5G, depend on what is supported by the device, for efficient use and to benefit from the maximum throughput. Four options are allowed by GWN.Cloud: **Disable Band steering**: This will disable the band steering feature and the access point will accept the band chosen by the client. **2G in Priority:** 2G Band will be prioritized over 5G Band **5G in Priority:** 5G Band will be prioritized over 2G Band **Balance:** GWN will balance between the clients connected to 2G and those connected to 5G. **Use Radio Settings:** GWN will use the value configured under Radio page.
Net Port Type	You can configure Trunk port or Access port. When it is set to *Access*, you also need to specify the VLAN ID. For example, if you have multiple SSIDs on different VLANs, then the port need to be set to Trunk in order to negotiate trunk with the switch port where the AP is plugged. Otherwise, if there is only one SSID/VLAN the port type is set to Access. *This feature is not supported in GWN7600/7600LR/GWN7610.*
Wi-Fi5 Compatible Mode	Some old devices do not support Wi-Fi6 well and may not be able to scan the signal or connect poorly. After turning on this switch, it will switch to Wi-Fi5 mode to solve the compatibility problem. At the same time, it will turn off Wi-Fi6 related functions. **Note:** Only take effect for GWN766x(LR).
2.4G & 5G	Used for configuring the advanced settings for 2.4G & 5G.
Disable 2.4GHz/5GHz	This feature allows the user to disable/enable its 2.4GHz band on the AP.

Channel Width	Choose the Channel Width, note that wide channel will give better speed/throughput, and narrow channel will have less interference. 20Mhz is suggested in very high-density environment. Default is "Use Radio Settings", the AP then will use the value configured under Radio page.
Channel	Select Use Radio Settings, or a specified channel, default is Auto. Note that the proposed channels depend on Country Settings under System Settings→Maintenance. Default is "Use Radio Settings", the AP then will use the value configured under Radio page.
Radio Power	Set the Radio Power depending on desired cell size to be broadcasted, five options are available: "Low", "Medium", "High", "custom" and "Use Radio Settings". Default is "Use Radio Settings", the AP then will use the value configured under Radio page.
Custom 2.4GHz/5GHz Tx Power (dBm)	When Radio Power is set to "Custom", allow users to set a custom wireless power for both 5GHz/2.4GHz band, the value of this field must be between 1 and 31.
Enable Minimum RSSI	Configures whether to enable/disable Minimum RSSI function. This option can be either Disabled or Enabled and set manually or set to Use Radio Settings.
Minimum Access Rate Limit	Specify whether to limit the minimum access rate for clients. This function may guarantee the connection quality between clients and AP. This option can be either Disabled or Enabled and set manually or set to Use Radio Settings.

Access Point Configuration Settings

Note:

The administrator can filter access points by Model or search by name/MAC of the device. Click on Save Button to save the changes and apply them to the AP.

Reset Access Points

To reset an access point, select and click on Reset button, a confirmation message will be displayed, click on OK to confirm the operation.

Reset Access Point

SSIDs

When using GWN76XX as Master Access Point, users can create different SSIDs and assign GWN76XX Slave Access Points to them.

Log in as Master to the GWN76XX Web GUI and go to **SSIDs.**

SSIDs

All GWN76XX can support up to 32 SSIDs while the GWN7605/GWN7605LR models can support up to 16 SSIDs, and GWN7602 can support up to 8 SSIDs, click on ⊕ Add to add a new SSID.

Add a new SSID

When editing or adding a new SSID, users will have two tabs to configure:

- **Wi-Fi:** Please refer to the below table for Wi-Fi tab options

Field	Description
SSID	Set or modify the SSID name.
Enable SSID	Check to enable Wi-Fi for the SSID.
Client IP Assignment	Set to NAT mode, clients will get the IP addresses from the specified NAT pool. And clients connecting to different APs are isolated from each other. *This feature is not supported in GWN7610.*
SSID Band	Select the Wi-Fi band the GWN will use, three options are available: **Dual-Band 2.4GHz 5Ghz**
VLAN	Enter the VLAN ID corresponding to the SSID. *This is available when Client IP Assignment is set to Bridge.*

Security Mode	Set the security mode for encryption, 8 options are available: • **WEP 64-bit:** Using a static WEP key. The characters can only be 0-9 or A-F with a length of 10, or printable ASCII characters with a length of 5. • **WEP 128-bit:** Using a static WEP key. The characters can only be 0-9 or A-F with a length of 26, or printable ASCII characters with a length of 13. • **WPA/WPA2:** Using "PSK" or "802.1x" as WPA Key Mode, with "AES" or "AES/TKIP" Encryption Type. • **WPA2:** Using "PSK" "PPSK" or "802.1x" as WPA Key Mode, with "AES" or "GCMP-128" Encryption Type. • **WPA2/WPA3:** Using "SAE-PSK" or "802.1x" as WPA Key Mode, with "AES" or "GCMP-128" Encryption Type. • **WPA3:** Using "SAE" or "802.1x" as WPA Key Mode, with "AES" or "AES/TKIP" Encryption Type. • **WPA3-192:** Using "802.1x" as WPA Key Mode, with "GCMP-256" or "CCMP-256" Encryption Type. • **OSEN:** This mode is used with release 2 of Hotspot 2.0 Release 2 OSU (Online Signup Server) for client provisioning. • **Open:** No password is required. Users will be connected without authentication. Not recommended for security reasons. *Note: GWN products support for 802.1x (PEAP-MSCHAPv2 and EAP-TLS) requires external AAA server to permit authentication and centralized access management.*
WEP Key	Enter the password key for WEP protection mode. *This field is available only when "Security Mode" is set to "WEP 64-bit" or "WEP 128-bit".*
WPA Key Mode	Three modes are available: • **PSK:** Use a pre-shared key to authenticate to the Wi-Fi. • **802.1X:** Use a RADIUS server to authenticate to the Wi-Fi. • **PPSK:** allow admin to configure Private Pre-Shared Key as an alternative to 802.1X authentication. *Note: PPSK is available only when "Security Mode" is set to "WPA2". PPSK management is available at Access Control → PPSK. This field is available only when "Security Mode" is set to "WPA/WPA2" , "WPA2", "WPA2/WPA3", "WPA3" or "WPA3-192".*
WPA Encryption Type	Two modes are available: **AES:** This method changes dynamically the encryption keys making them nearly impossible to circumvent. **AES/TKIP:** use both Temporal Key Integrity Protocol and Advanced Encryption Standard for encryption, this provides the most reliable security. *This field is available only when "Security Mode" is set to "WPA/WPA2" , "WPA2", "WPA2&WPA3", "WPA3" or "WPA3-128".*
WPA Pre-Shared Key	Set the access key for the clients, and the input range should be: 8-63 ASCII characters or 8-64 hex characters. *This field is available only when "Security Mode" is set to "WPA/WPA2", "WPA2", "WPA2/WPA3" or "WPA3".*
802.11w	The 802.11w standard is used to prevent certain types of WLAN DoS attacks. 802.11w extends strong cryptographic protection and provides data integrity and replay protection for broadcast/multicast Robust management frames. Set this option to either to Disabled : disable 802.11w; Optional: both of the client supported and unsupported 802.11w may have the network access authority; Required: only the client supported 802.11w have the network access authority.
RADIUS Sever Address	Configures RADIUS authentication server address. *This field is available only when "WPA Key Mode" is set to "802.1x".*

|	
RADIUS Server Port	Configures RADIUS Server Listening port. Default is: 1812. *This field is available only when "WPA Key Mode" is set to "802.1x".*
RADIUS Server Secret	Enter the secret password for client authentication with RADIUS server. *This field is available only when "WPA Key Mode" is set to "802.1x".*
Secondary RADIUS Server	Check the box to enable settings a secondary RADIUS server. Then you need to specify below three fields: • **RADIUS Server Address:** Enter the secondary RADIUS server address. • **RADIUS Server Port** : Enter the secondary RADIUS server port. *The default port is 1812 and the range is 1-65535.* • **RADIUS Server Secret**: Enter the secret password for client authentication with the secondary RADIUS server.
RADIUS Accounting Server	Configures the address for the RADIUS accounting server. *This field is available only when "WPA Key Mode" is set to "802.1x".*
RADIUS Accounting Server Port	Configures RADIUS accounting server listening port. Default is 1813. *This field is available only when "WPA Key Mode" is set to "802.1x".*
RADIUS Accounting Server Secret	Enter the secret password for client authentication with RADIUS accounting server. *This field is available only when "WPA Key Mode" is set to "802.1x".*
Secondary RADIUS Accounting Server	Check the box to enable settings a secondary RADIUS accounting server. Then you need to specify below three fields: • **RADIUS Accounting Server Address:** Enter the secondary Accounting RADIUS server address. • **RADIUS Accounting Server Port:** Configures the secondary RADIUS accounting server listening port. Default is 1813. • **RADIUS Accounting Server Secret:** Enter the secret password for client authentication with the secondary RADIUS accounting server
RADIUS NAS ID	Enter the RADIUS NAS ID. *This field is available only when "WPA Key Mode" is set to "802.1x".*
Enable Hotspot2.0	Check to activate Hotspot2.0 in the SSID. *This field is available only when "WPA Key Mode" is set to "802.1x".* Refer to [Hotspot 2.0] for more details
Hotspot2.0 Profile	Select the Hotspot2.0 profile to use in the SSID. *This field is available only when "WPA Key Mode" is set to "802.1x".* Refer to [Hotspot 2.0] for more details
Enable Captive Portal	Click on the checkbox to enable the captive portal feature.
Use MAC Filtering	Choose Blacklist/Whitelist to specify MAC addresses to be excluded /included from connecting to the zone's Wi-Fi. Default is Disabled.
Enable Dynamic VLAN (beta)	When enabled, clients will be assigned IP address from corresponding VLAN configured on the RADIUS user profile. This field is available only when "WPA Key Mode" is set to "802.1x".
Client Isolation	Client isolation feature blocks any TCP/IP connection between connected clients to GWN76XX's Wi-Fi access point. Client isolation can be helpful to increase security for Guest networks/Public Wi-Fi. Three modes are available: • **Radio:** Wireless clients can access to the internet services, GWN7xxx router and the access points GWN76XX but they cannot communicate with each other. • **Internet:** Wireless clients will be allowed to access only the internet services and they cannot access any of the management services, either on the router nor the access points GWN76XX. • **Gateway MAC:** Wireless client scan only communicate with the gateway, the communication between clients is blocked and they cannot access any of the management services on the GWN76XX access points.
Advanced	
SSID Hidden	Select to hide SSID. SSID will not be visible when scanning for Wi-Fi, to connect a device to hidden SSID, users need to specify SSID name and authentication password manually.

DTIM Period	Configures the frequency of DTIM (Delivery Traffic Indication Message) transmission per each beacon broadcast. Clients will check the AP for buffered data at every configured DTIM Period. You may set a high value for power saving consideration. Default value is 1, meaning that AP will have DTIM broadcast every beacon. If set to 10, AP will have DTIM broadcast every 10 beacons. Valid range: 1 – 10.
Wireless Client Limit	Configure the limit for wireless client. If there is an SSID per-radio on a LAN, each SSID will have the same limit. So, setting a limit of 50 will limit EACH ssid to 50 users independently. Note: If set to 0, it equals disable the limit.
Client Inactivity Timeout(s)	AP will remove the client's entry if the client generates no traffic at all for the specified time period. The client inactivity timeout is set to 300 seconds by default. Range from 60-3600 seconds.
Client Bridge Support	Configures the client bridge support to allow the access point to be configured as a client for ridging wired only clients wirelessly to the network. When an access point is configured in this way, it will share the Wi-Fi connection to the LAN ports transparently. Once an SSID has Client Bridge Support enabled, the AP adopted in this SSID can be turned in to Bridge Client mode by click the Bridge button. **Note:** This feature is not supported on GWN7602.
Client Time Policy	Select a time policy to be applied to all clients connected to this SSID.
Multicast/Broadcast Suppression	When set to "Disable": all of the broadcast and multicast packages will be forwarded to the wireless interface. When set as "Enabled": all of the broadcast and multicast packages will be discarded except DHCP/ARP/IGMP/ND; When set to "Enable with Proxy ARP enabled": AP will enable the optimization with Proxy ARP enabled in the meantime.
Convert IP multicast to unicast	When set to "Disabled": none of the multicast package will be converted; Passive mode: AP will never initiatively broadcast IGMP queries, and the IGMP snooping item will be aged out 300 seconds after it is registered, which may result in the failure of forwarding multicast data. Active mode: AP will initiatively broadcast IGMP queries to keep updating of the IGMP snooping items.
Enable Schedule	Enable this option to assign a schedule for the bandwidth rule.
Schedule	Within the time of schedule, SSID can be used.
Enable Voice Enterprise	Check to enable/disable Voice Enterprise. The roaming time will be reduced once enable voice enterprise. • The 802.11k standard helps clients to speed up the search for nearby APs that are available as roaming targets by creating an optimized list of channels. • When the signal strength of the current AP weakens, your device will scan for target APs from this list. When your client device roams from one AP to another on the same network, 802.11r uses a feature called Fast Basic Service Set Transition (FT) to authenticate more quickly. FT works with both pre-shared key (PSK) and 802.1X authentication methods. • 802.11v allows client devices to exchange information about the network topology, including information about the RF environment, making each client network aware, facilitating overall improvement of the wireless network. *Note: 11R is required for enterprise audio feature, 11V and 11K are optional. This field is available only when "Security Mode" is set to "WPA/WPA2" or "WPA2".*
Enable 11R	Check to enable 802.11r. *This field is available only when "Security Mode" is set to "WPA/WPA2" or "WPA2".*
Enable 11K	Check to enable 802.11k
Enable 11V	Check to enable 802.11v
ARP Proxy	This option will enable GWN AP to answer the ARP requests from its LAN for its connected Wi-Fi clients. This is mainly to reduce the airtime consumed by ARP Packets
U-APSD	This option will allow the user to enable/disable the Unscheduled Automatic Power Save Delivery feature.
Enable Bonjour Gateway	Once enabled, the client Bonjour on the SSID is forwarded to the VLAN of the Bonjour service (such as Samba). *Supported on GWN7605, GWN7605LR, GWN7615, GWN7630, GWN7630LR, GWN7660, GWN7660LR*

○ **Device Membership**: Used to add or remove paired access points to the SSID. The MAX SSID number is separately counted for each band (2.4GHzor 5Ghz).

The maximum allowed SSID for each band now is as below:

Model	MAX SSID(without Mesh/with Mesh)
GWN7600/7600LR	16/14
GWN7605/7605LR	16/14
GWN7610	16/14
GWN7615	32/14
GWN7630/7630LR	32/14
GWN7660/GWN7660LR	32/14
GWN7664/GWN7664LR	32/14
GWN7624	16/14
GWN7625	16/14
GWN7602	8/6

MAX SSID on each band
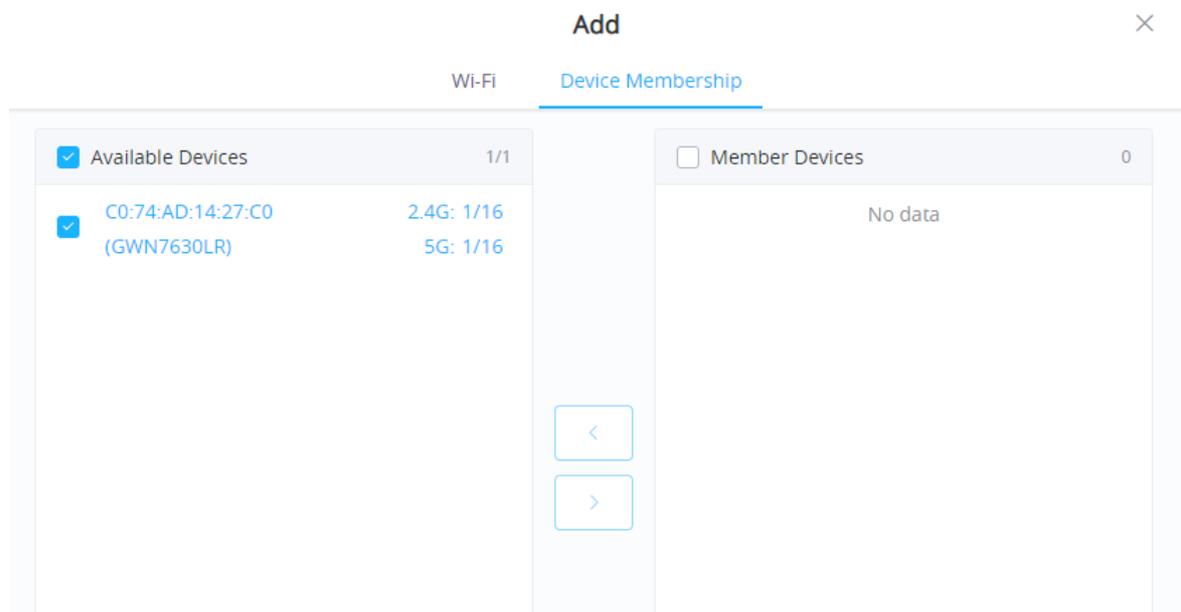
Device Membership

Click on ➡ to add the GWN76XX to the SSID or click on ⬅ to remove it.

CLIENTS

Users can access clients list connected to GWN76XX from **Web GUI → Clients** to perform different actions to wireless clients.

Clients

○ Click on ✎ under Actions to check client's status and modify basic settings such Device's Name.

○ Click on 🚫 to block a client's MAC address from connecting to the zone's SSID.

○ Click on ↻ to release Wi-Fi offline client IP lease.

Users can press ⚙ button to customize items to display on the page. Following items are supported:

Select up to 16 items

☑ MAC

☑ Hostname

☑ Manufacture

☑ OS

☑ Type

☑ IP Address

☑ Radio/Channel

☑ Status

☑ RSSI

☐ Bridge

☑ SSID

☑ AP

☐ Station Mode

☐ Link Rate

☑ Throughput

☑ Aggregate

Default

Clients – Select Items

ACCESS CONTROL

Access List

From this menu, users can manage in global way the blacklist of clients that will be blocked from accessing the Wi-Fi network, click on Client Access to add or remove MAC addresses of client from global blacklist.

Name	MAC Addresses	Actions
Global Blacklist	(2) 48:4B:AA:08:3F:92, 48:4B:AA:08:3F:90	✎ 🗑

Global Blacklist

Edit

Name	Global Blacklist
MAC Addresses	48:4B:AA:08:3F:92 ⊖
	48:4B:AA:08:3F:90 ⊖
	Add new item ⊕

Managing the Global Blacklist

A second option is to add custom access lists that will be used as matching mechanism for MAC address filtering option under SSIDs to allow (whitelist) or disallow (blacklist) clients access to the Wi-Fi network.

Click on **+ Add** in order to create new access list, then fill it with all MAC addresses to be matched.

Adding Client Access List

Users can also Import/Export the client access lists in CSV format as shown below:

Import/Export the client access

Users can check « Enable Schedule » to assign a schedule for the list when it will take effect.

Adding New Access List

Once this is done, this access list can be used under SSID Wi-Fi settings to filter clients either using whitelist or blacklist mode.

Blacklist Access List

Time Policy

The timed client disconnect feature allows the system administrator to set a fixed time for which clients should be allowed to connect to the access point, after which the client will no longer be allowed to connect for a user configurable cool-down period.

The configuration is based on a policy where the administrator can set the amount of time for which clients are allowed to connect to the Wi-Fi and reconnect type and value after which they will be allowed to connect back after they have been disconnected.

To create a new policy, go under **Captive Portal → Time Policy** and add new one.

Then set the following parameters:

Option	Description
Name	Enter the name of the policy
Enabled	Check the box to enable the policy
Limit Client Connection Time	Sets amount of time a client may be connected.
Client Reconnect Timeout Type	Select the method with which we will reset a client's connection timer so they may reconnect again. Options are: Reset Daily. Reset Weekly. Reset Hourly. Timed Reset.
Client Reconnect Timeout	If "Timed Reset" is selected, this is the period for which the client will have to wait before reconnecting.
Day of the Week	If "Reset Weekly" is selected, this is the day when the reset will be applied.
Hour of the Day	If "Reset Weekly" or "Reset Daily" is selected, this is the hour and day when the reset will be applied.

Time Policy Parameters

Note:

Time tracking shall be accounted for on a per-policy basis, such that a client connected to any SSID assigned the time tracking policy will accrue a common counter, regardless of which SSID they are connected to (as long as those SSIDs all share the same time tracking policy).

Banned Clients

Click on Banned Clients menu to view the list of the clients that have been banned after time disconnect feature has taken effect, these clients will not be allowed to connect back until timeout reset or you can unblock a client by clicking on the icon 🌐.

Banned Clients

MAC Addresses	Time Policy	Release Time	Actions
A0:CB:FD:F4:DF:FE	5minute	2017-08-24 11:40:00	🌐
30:75:12:FF:37:89	5minute	2017-08-24 11:40:00	🌐
DC:09:4C:A4:38:BE	5minute	2017-08-24 11:41:00	🌐

Ban/Unban Client

Bandwidth Rules

The bandwidth rule is a GWN76XX feature that allows users to limit bandwidth utilization per SSID or client (MAC address or IP address).

This option can be configured from the GWN76XX WebGUI under "Bandwidth Rules".

Click **+ Add** to add a new rule, the following table provides an explanation about different options for bandwidth rules.

Field	Description
Enabled	Enable/Disable the Bandwidth rule.
SSID	Select which SSID will be affected by the bandwidth rule limitation.
Range Constraint	Choose the type of rule to be applied on bandwidth utilization from the dropdown list, three options are available: **Per-SSID:** Set a bandwidth limitation on the SSID level. **Per-User:** Set a bandwidth limitation per Client. **MAC:** Set a bandwidth limitation per MAC address. **IP Address:** Set a bandwidth limitation per IP address.
MAC	Enter the MAC address of the device to which the limitation will be applied, this option appears only when MAC type is selected.
IP address	Enter the IP address of the device to which the limitation will be applied, this option appears only when IP Address type is selected.
Enable Schedule	Enable this option to assign a schedule for the bandwidth rule.
Upload Limit	Specify the limit for the upload bandwidth using Kbps or Mbps.
Download Limit	Specify the limit for the download bandwidth using Kbps or Mbps.

Bandwidth Rules

The following figure shows an example of MAC address rule limitation.

MAC Address Bandwidth Rule

The following figure shows examples of bandwidth rules:
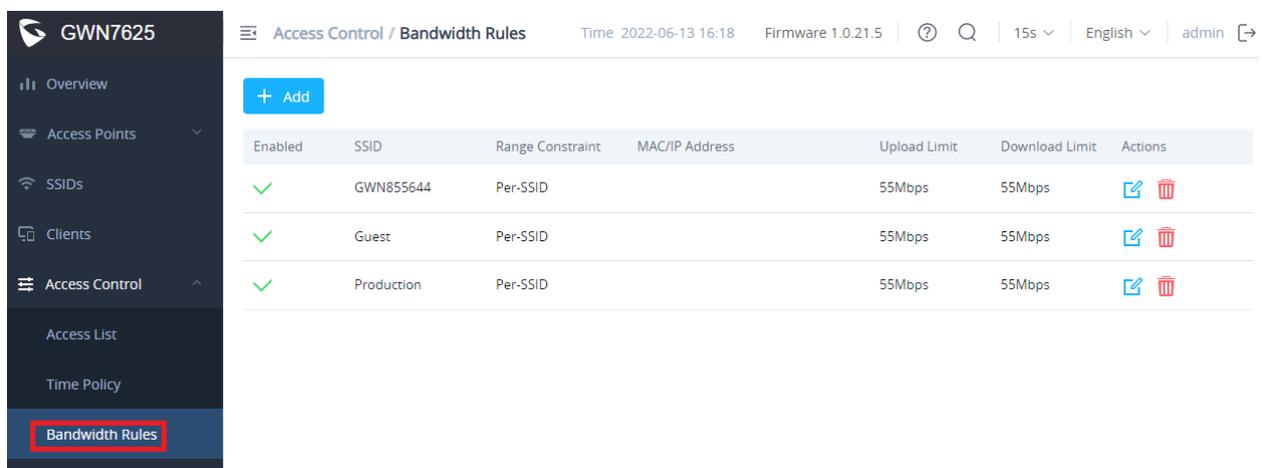
Bandwidth Rules

The same settings for bandwidth management are available from the following menus:

Navigate on the web GUI under "**Clients→Edit→Bandwidth Rules**" where you can set the Upstream and Downstream rate in Mbps

CAPTIVE PORTAL

Captive Portal feature on GWN76XX AP helps to define a Landing Page (Web page) that will be displayed on Wi-Fi clients' browsers when attempting to access Internet. Once connected to a GWN76XX AP, Wi-Fi clients will be forced to view and interact with that landing page before Internet access is granted.

The Captive Portal feature can be configured from the GWN76XX Web page under "Captive Portal".

The page contains following sub-menus: **Guest**, **Policy List**, **Splash Page** and **Vouchers**.

Guest

This section lists the clients connected or trying to connect to Wi-Fi via Captive Portal.
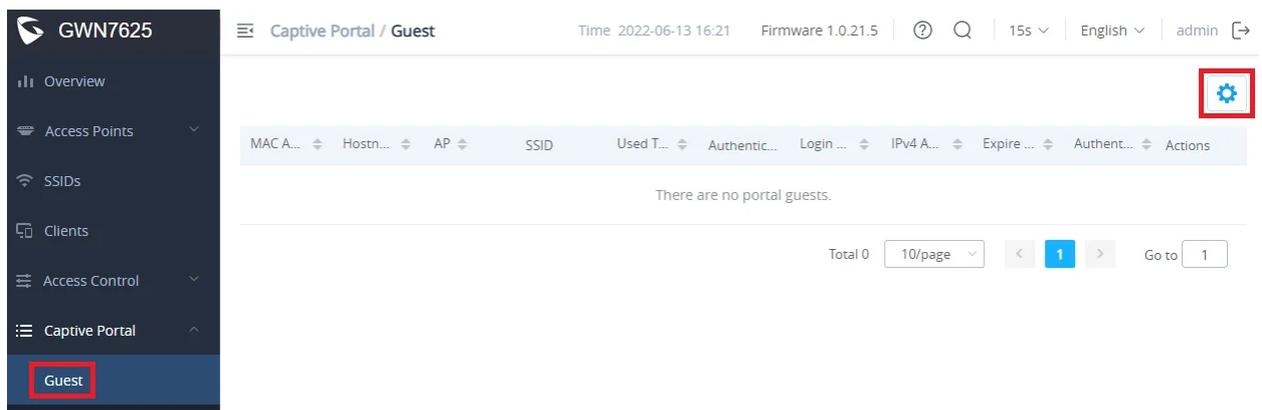
Captive Portal – Guest Page

Users can press   button to customize items to display on the page. Following items are supported:

*Captive Portal – Guest
Page – Select Items*

Policy List

Users can customize a portal policy in this page.

Captive Portal – Policy List

- ○ Click on ☑ to edit the policy.
- ○ Click on 🗑 to delete the policy.
- ○ Click on ➕ Add to add a policy.

The policy configuration page allows adding multiple captive portal policies which will be applied to SSIDs and contains options for different authentication types a splash page that can be easily configured as shown on the next section.

Administrator can use an internal or external splash page.

Edit

Basic   Auth Rule

Name	grandstream
Splash Page	Internal
Authentication Type	Login for free
Client Expiration ❓	86400 Second(s)
Client Idle Timeout ❓	Minute(s)
Use Default Portal Page	☑
Portal Page Customization	/portal_default.html
Landing Page	Redirect to the Original URL
Enable Daily Limit ❓	☐
Enable HTTPS Redirection ❓	☑
Enable Secure Portal ❓	☐

Add a New Policy

Internal Splash Page

Below table lists the items policy add page configures

Name	Enter the name of the Captive Portal policy
Splash Page	Select Splash Page type, Internal or External.
Authentication Type	Following types of authentications are available: • **Login for free:** when choosing this option, the landing page feature will not provide any type of authentication, instead it will prompt users to accept the license agreement to gain access to internet. • **RADIUS Server:** Choosing this option will allow users to set a RADIUS server to authenticate connecting clients. • **Social Login Authentication:** Choosing this option will allow users to enable authentication Facebook, Twitter or Google. • **Vouchers:** Choose this page when using authentication via Vouchers. • **Login with password:** Choose this page when using authentication via a password. • **Active Directory:** Choosing this option will allow users to set a Active Directory server to authenticate connecting clients.
Client Expiration	Configures the period of validity, after the valid period, the client will be re-authenticated again.
Client Idle Timeout	Configure the time when the client will automatically deauthenticate when it is idle. This does not apply to Voucher Captive portal mode.
If Authentication Type is set to RADIUS Authentication	
RADIUS Server Address	Fill in the IP address of the RADIUS server

RADIUS Server Port	Set the RADIUS server port, The default value is 1812.
RADIUS Server Secret	Fill in the key of the RADIUS server.
Radius Authentication Method	Select the RADIUS authentication method, 3 methods are available: **PAP, CHAP and MS-CHAP.**
Radius Retry Timeout(s)	Set the timeout for each authentication request sent to the Radius server. The valid range is 1 to 120 seconds.
Radius Retries	Set the maximum number of retires to send an authentication request for the Radius server. The valid range is 1 to 5.
If Authentication Type is set to "Social Login Authentication"	
Facebook	Check to enable/disable Facebook Authentication
Facebook App ID	Fill in the Facebook App ID.
Facebook APP Secret	Set the key for the portal, once clients want to connect to the Wi-Fi, they should enter this key.
Twitter	Check this box to enable Twitter Authentication.
Force to Follow	If checked, users need to Follow owner before been authenticated.
Consumer Key	Enter the app Key to use Twitter Login API.
Consumer Secret	Enter the app secret to use Twitter Login API.
Google	Check this box to enable Google Authentication.
Google Client ID	Enter the Client Id to use Google Login API.
Google Client Key	Enter the Client Key to use Google Login API.
If Authentication Type is set to "Login with password"	
Login with password	Specify a password for the captive portal.
If Authentication Type is set to "Active Directory"	
AD Server URL	Specify Active Directory URL
Redirect URL	Enter the redirect URL
X.509 Cert SHA1 Fingerprint	enter the X.509 Cert SHA1 Fingerprint
For all Authentication Types	
Use Default Portal Page	• If checked, the users will be redirected to the default portal page once connected to the GWN.• If unchecked, users can manually select which Portal Page to use from Portal Page Customization drop-down list.
Portal Page Customization	Select the customized portal page (if "Use Default Portal Page" is unchecked).• terms_of_use/terms.html • facebook.html • google.html • password_auth.html • portal_default.html • portal_pass.html • portal_tip.html • social_auth.html • status.html • third_auth.html • twitter.html • twitter_website.html • vouchers_auth.html

Landing Page	Choose the landing page, 2 options are available: • Redirect to the Original URL. • Redirect to External Page.
The Redirect External Page URL Address	Once the landing page is set to redirect to external page, user should set the URL address for redirecting.This field appears only when Landing Page is set to "Redirect to an External Page".
Enable Daily Limit	If enabled, captive portal will limit user connection by times of one day.
Enable HTTPS Redirection	Check to enable/disable HTTPS service. If enabled, both HTTP and HTTPS requests sent from stations will be redirected by using HTTPS protocol. And station may receive an invalid certification error while doing HTTPS browsing before authentication. If disabled, only the HTTP request will be redirected.
Enable Secure Portal	Enable Secure Portal: If enabled, unauthorized guests will be redirected to the splash page by using HTTPS protocol. If not, the HTTP protocol will be used.

Captive Portal – Policy List – Splash Page is "Internal"

Notes:

If Facebook authentication is configured, you will need to log in your Facebook account of https://developers.facebook.com/apps , and set the OAuth redirect to : https://cwp.gwn.cloud:8443/GsUserAuth.cgi? GsUserAuthMethod=3

2. If Twitter authentication is configured, you will need to log in your Twitter account of https://apps.twitter.com/app, and set the callback URLs to: http://cwp.gwn.cloud:8080/GsUserAuth.cgi

External Splash Page

Field	Description
Name	Enter the name of the Captive Portal policy
Splash Page	Select to either use **Internal** or **External** Splash Page.
External Splash Page URL	Enter the External Splash Page URL, and make sure to enter the pre-authentication rules request by the external portal platform in the pre-authentication configuration option.
RADIUS Server Address	Fill in the IP address of the RADIUS server.
RADIUS Server Port	Set the RADIUS server port, the default value is 1812.
RADIUS Server Secret	Fill in the key of the RADIUS server.
RADIUS Accounting Server	Configures the address for the RADIUS accounting server address.
RADIUS Accounting Server Port	Configures RADIUS accounting server listening port (default is 1813).
RADIUS Accounting Server Secret	Enter the secret password for client authentication with RADIUS accounting server.
Accounting Update Interval	Enter Update Interval for RADIUS Accounting Server. The interval unit can be set by seconds, minutes, hours, or days.
RADIUS NAS ID	Enter RADIUS NAS ID. *This field appears only when* **Splash Page** *is set to "External".*
Redirect URL	Specify URL where to redirect clients after authentication.

Captive Portal – Policy List – Splash Page is "External"

In case social media authentication is used, the user needs to allow some traffic between the AP and social medial platforms (Facebook API as example) to send authentication credentials and receive reply, this traffic can be allowed using the Authentication rules which are explained below.

Authentication rules

Pre-Authentication Rules

Using this option, users can set rules to match traffic that will be allowed for connected Wi-Fi users before authentication process. This can be needed for example to setup Facebook authentication where some traffic should be allowed to Facebook server(s) to process the user's authentication. Or simply to be used to allow some type of traffic for unauthenticated users.

Post-Authentication Rules

On the other hand, post authentication rules are used to match traffic that will be banned for Wi-Fi clients after authentication. As an example, if you want to disallow connected Wi-Fi clients to issue Telnet or SSH traffic after authentication then you can set post authentication rules to match that traffic and once a connected client passes the authentication process they will be banned from issuing telnet and SSH connections.

Splash Page

Files configuration page allows users to view and upload HTML pages and related files (images…).

Captive Portal – Splash Page

User can add folder in corresponding folder by selecting the folder and click on ⊕ Add Folder .

- Click on **+ Upload** to upload a file from local device.

- Click on **+ Download** to download the files in Captive Portal folder.

- Click on ✎ to edit the corresponding file, in another word, to replace the file with a new one.

- Click on 🗑 to delete the file.

Vouchers

Voucher Feature Description

Voucher feature will allow clients to have internet access for a limited duration using a code that is randomly generated from GWN controller.

Note that multiple users can use a single voucher for connection with expiration duration of the voucher that starts counting after first successful connection from one of the users that are allowed.

Another interesting feature is that the admin can set data bandwidth limitation on each created voucher depending on the current load on the network, users' profile (VIP customers get more speed than regular ones...etc.) and the internet connection available (fiber, DSL, or cable...etc.) to avoid connection congestion and slowness of the service.

Each created voucher can be printed and served to the customers for usage, and the limit is 1000 vouchers.

The usage of voucher feature needs to be combined with captive portal that is explained after this section, in order to have the portal page requesting clients to enter voucher code for authentication.

Voucher Configuration

To configure/create vouchers for clients to use, follow below steps:

1. On controller web GUI, navigate under "**Captive Portal → Vouchers**"

2. Click on **+ Add** button in order to add a new voucher.

3. Enter voucher details which are explained on the next table.

4. Press save to create the voucher(s).

Notes:

- Users can specify how many vouchers to generate which have the same profile, this way the GWN will generate as many vouchers as needed which do have the same settings avoiding creating them one by one.

- The admin can verify the status of each voucher on the list (In use, not used, expired ...etc.).

- Press 🖶 to print the voucher, 🗑 to delete it or 🔄 to renew the voucher.

Add Voucher Sample

The below figure shows the list of the vouchers after GWN randomly generates the code for each one.

Figure 84: Vouchers List

Users can click on buttons 🗑 **Delete** and 🖨 **Print** to delete and print multiple vouchers or click 🖨 **Print All** button to print all vouchers at once.

Also, users can use the drop-down list filter `All Created Time ▼` to filter the vouchers that were created at specific date-time.

The following table summarizes description for voucher configuration parameters:

Field	Description
Create Quantity	Specify how many vouchers to generate which will have same profile/settings (duration, bandwidth, and number of users). Valid range: 1 – 1000.
Max Devices	Specify how many users can use same voucher. Valid range: 1 – 5.
Byte Limit	Specify download byte limit for the voucher. The unit can be either **M** (Megabyte) or **G** (Gigabyte). Valid range: 10 – 1048576 (M) 1 – 1024 (G)
Duration	Specify the duration after which the voucher will expire, and clients will be disconnected from internet. **Note:** in case or multiple users, the duration will start counting after first user starts using the voucher.
Validity Time	Set the validity period of credentials, limited to 1-365 integer. The unit is day.
Download Limit	Set the downstream bandwidth speed limit (in Kbps or Mbps).
Upload Limit	Set the upstream bandwidth speed limit (in Kbps or Mbps).
Notes	Notes for the admin when checking the list of vouchers.

Voucher Parameters

Using Voucher with GWN Captive Portal

In order to successfully use the voucher feature, users will need to create a captive portal in order to request voucher authentication codes from users before allowing them access to internet. More details about captive portal will be covered on next section but for voucher configuration please follow below steps.

1. Go under "**Captive Portal → Policy List**" menu.

2. Press `+ Add` in order to add new captive portal policy.

3. Set the following parameters as shown on the screenshot for basic setup then save and apply.

Captive Portal with Voucher authentication

Then go under your SSID configuration page and enable the generated captive portal under Wi-Fi settings tab.

RADIO

When using GWN76XX as Master Access Point, users can edit the frequency band used by the AP and channel used along with the Transmission power for each band.

Log in as Master to the GWN76XX Web GUI and go to **Radio.**

Radio-General

Field	Description
General	
Band Steering	When Frequency is set to Dual-Band, users can check this option to enable Band Steering on the Access Point, this will help redirecting clients to a radio band accordingly for efficient use and to benefit from the maximum throughput supported by the client.
Client Steering	This feature will help Wi-Fi client to roam to other APs within same Network. Steering happens when clients is inactive or active clients with the standards 802.11K&V support. There are two options for steering. • **Sticky client steer** is based on minimum RSSI once it reaches the RSSI threshold (dBm) it will disconnect and search for another AP. • **Load balance steer** uses the standards 802.11K&V to build a neighborhood table with adjacent APs informations (Channels utilization and Client numbers) and once it reaches full Channel utilization or Client Access Threshold it will switch the client to another AP for better performance. If the client doesn't support the standards 802.11K&V, it will only be deauthenticated with current AP when client is idle. parameters of RSSI Threshold and Client Access Threshold parameters will show up only when Client Steering is enabled. **Note** : *Client Steering works only if Band Steering is enabled.*
Airtime Fairness	Allows faster clients to have more airtime than slower clients.

Beacon Interval	Configures interval between beacon transmissions/broadcasts. The Beacon signals help to keep the network synchronized and provide main information about the network such as SSID, Timestamp... • **Using High Beacon Interval:** AP will be sending beacon broadcast less frequently. This will help to get better throughput, thus better speed/performance. It also helps to save Wi-Fi clients energy consumption. • **Using Low Beacon Interval:** AP will be sending beacon broadcast more frequently. This can help in environments with weak signal areas; sending more frequently beacons will increase chances to be received by Wi-Fi clients with weak signal. **Notes:** When AP enables less than 3 SSIDs, the interval value which will be effective are the values from 40 to 500. When AP enables more than 2 but less than 9 SSIDs, the interval value which will be effective are the values from 100 to 500. When AP enables more than 8 SSIDs, the interval value which will be effective are the values from 200 to 500. Mesh feature will take up a share when it is enabled.
Wi-Fi5 Compatible Mode	Some old devices do not support Wi-Fi6 well and may not be able to scan the signal or connect poorly. After turning on this switch, it will switch to Wi-Fi5 mode to solve the compatibility problem. At the same time, it will turn off Wi-Fi6 related functions. **Note:** Only take effect for GWN766x(LR).
Country/Region	Displays the country/region of the AP.
Scene	Displays the Scene of the AP.

2.4G & 5G Configuration	**Channel Width:** Choose the Channel Width, note that wide channel will give better speed/throughput, and narrow channel will have less interference. 20Mhz is suggested in very high-density environment. • **40MHz Channel Location:** Configure the 40MHz channel location when using 20MHz/40MHz in Channel Width, users can set it to be Secondary below Primary, Primary below Secondary or Auto. • **Channel:** Select Auto, or Dynamically assigned by RRM. **Note** : *Dynamically assigned by RRM activates Dynamic Channel Assignment: Once enabled, AP will try to allocate and move the best channel during operation, unlike Auto Channel Selection (ACS) which scan and assign channel when Wi-Fi interface goes up for one time. This is not supported on GWN7610.* • **Enable DFS Channel:** If enabled, you can use band2 and band3 channels when "Auto" channel is selected. Note: It will not take effect on GWN7600/GWN7602/GWN7610. • **Radio Power:** Set the Radio Power, it can be Low, Medium, or High or Custom or Dynamically assigned by RRM or Auto. **Note** : *Dynamically assigned by RRM activates TPC and CHD:* • *Transmit Power Control: TPC algorithm runs every 10 minutes. AP acquires the RSSI information of the neighbor by wireless scanning and establishes the neighbor table. The algorithm requires that there must be at least 3 neighbor APs with RSSI larger than -70dbm. Otherwise, power will not be adjusted.* • *Coverage Hole Detection: CHD enables AP to decide whether to increase the AP power by the current SNR and SNR threshold of the connected clients.* • **Custom Wireless Power(dBm):** allows users to set a custom wireless power for both 5GHz/2.4GHz band, the value of this field must be between 1 and 31. • **Enable Short Guard Interval:** Check to activate this option to increase throughput. • **Allow Legacy Devices (802.11b):** Check to support 802.11b devices to connect the AP in 802.11n/g mode. (2.4GHz setting) • **Enable Minimum RSSI:** Check to enable RSSI function, this will lead the AP to disconnect users below the configured threshold in Minimum RSSI (dBm). • **Minimum RSSI:** Enter the minimum RSSI value in dBm. If the signal value is lower than the configured minimum value, the client will be disconnected. The input range is from "-94" or "-1". • **Minimum Access Rate Limit:** Specify whether to limit the minimum access rate for clients. When enabled, it will help to eliminate the legacy connection which slow the total performance of the Wi-Fi network. Range from 1 to 54 Mbps.

Radio Settings

SECURITY

Rogue AP

The GWN Access Points offer the ability to prevent malicious intrusion to the network and increases the wireless security access of clients when introducing Rogue AP detection. The detected APs will be listed with all the details under Detected section for further intervention. This feature is not supported in GWN7610.

In the figure below is the configuration page in order to enable the Rogue AP detection and we can set the trusted Aps on the network.

Enable **Rogue** AP Detection ⬤

Detect range ⑦ ● Same channel   ○ All channels

Countermeasure level ⑦ [Disable   ⌄]

Containment Range ⑦ ● Same channel   ○ All channels

Sub-string for Spoofing SSID ⑦ [   ] ⊖

Add new item ⊕

Trusted AP ⑦ [   ] ⊖

Add new item ⊕

Untrusted AP ⑦ [   ] ⊖

Add new item ⊕

[Save]   [Reset]

Rogue AP-Configuration

Field	Description
Enable Rogue AP Detection	Select to either to enable or disable Rogue AP scan.
Detect range	Specify the rogue AP detect range. • **Same channel:** AP will execute simple detection on the APs around, this mode almost has no effects on the wireless network communication. • **All channels:** AP will execute a deep detection every 5 minutes. And the clients connecting to the AP will have few seconds of communication interrupt. Default is Same Channel.
Countermeasure Level	Countermeasures level specifies the type of attacks which will be suspected by the AP. Select different levels: • **High:** Untrusted BSSID, Illegal access without authentication, Illegal access, Spoofing SSID. • **Medium:** Untrusted BSSID, Illegal access without authentication, Illegal access. • **Low:** Untrusted BSSID, Illegal access without authentication. Default is Disabled.
Containment Range	Specify the containment range: • **Same channel:** detect AP will countermeasure the APs in the same channel. • **All channels:** detect AP will countermeasure the APs in all channels at the cost of consuming of much AP performance. Default is Same Channel.
Sub-string for Spoofing SSID	The AP broadcasting SSID with the specified string will be classified as a Spoofing SSID.
Trusted AP	You can specify MAC address of the trusted AP, which should be formatted as XX:XX:XX:XX:XX:XX. If an AP is defined as trusted AP, no countermeasures will be executed on it.

Untrusted AP	You can specify MAC address of the untrusted AP, which should be formatted as XX:XX:XX:XX:XX:XX. If an AP is defined as untrusted AP, countermeasures will be executed on it when countermeasure is enabled.

Rogue AP

In the figure below we would have a list showing all the detected rogue AP on the network scanned by the GWN access point.

Configuration	Detected

| | All ⌄ | Dual-Band ⌄ | SSID ⌄ | Search SSID 🔍 | ⚙ |

SSID ⇕	BSSID ⇕	Channel ⇕	Protocol ⇕	Securit... ⇕	Detect... ⇕	RSSI ⇕	Last S... ⇕	Counte... ⇕	Rogue ... ⇕	Manuf... ⇕	Actions
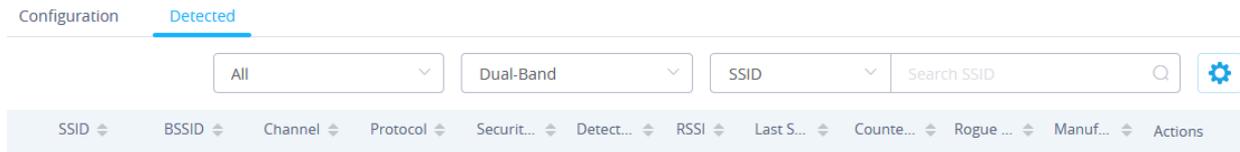
Rogue AP-Detection

Firewall

This section allows user to control the outgoing and incoming traffic from clients by manually setting up.

policies to either deny or permit the traffic based on protocol type and by specifying SSIDs and destinations.

Outbound Rules	Inbound Rules

+ Add   🗑 **Delete**

☐	Priority	Service Protocol	Policy	Destination	SSID	Actions
☐	-	any	Permit	All	All	✎ 🗑

Firewall-Outbound

Field	Description
Service Protocol	Select type of traffic to be affected by the outbound rule like ICMP, HTTP, HTTPS... or you may add another type of traffic when selecting Custom. When set to Custom, user could enter the following: • **Protocol:** TCP or UDP • **Port:** define the port used by this protocol.
Policy	Either select to Permit or Deny Outbound traffic.
Destination	Select either: • **Particular Domain:** enter FQDN of a destination or string: for instance, entering test will block service to any domain name containing string test. • **Particular IP:** IP address of destination. • **Particular Network:** Network IP address. • **All:** the rule will apply on all destinations.
SSID	Select one or multiple SSIDs to apply the rule on.

Firewall- Outbound

User can define outbound and inbound rules on the traffic from the options in figure below:

Outbound Rules	Inbound Rules

+ Add   🗑 **Delete**

☐	Priority	Source	Service Protocol	Policy	Destination	Actions
			There are no static inbound rules.			

Firewall-inbound

Field	Description

Service Protocol	Select type of traffic to be affected by the inbound rule like ICMP, HTTP, HTTPS… or you may add another type of traffic when selecting Custom. When set to Custom, user could enter the following: • **Protocol:** TCP or UDP • **Port:** define the port used by this protocol.
Policy	Either select to Permit or Deny inbound traffic.
Source	Select either: • **Particular IP:** IP address of source. • **Particular Network:** Network IP address. • **All:** the rule will apply on all destinations.
Destination	Configure the destination address. • **All** • **Particular** • **IP Particular Domain** • **Particular Network**

Firewall-Inbound

SERVICE

Hotspot 2.0

This section lists the configuration page to Hotspot 2.0. This is a technology that allows mobile devices to automatically connect to available Passpoint-certified Wi-Fi hotspots. This gives the device liberty to hop from one hotspot on a network to another without the need log in to each hotspot. This feature is currently a beta.

Note: GWN7660, GWN7630, GWN7630LR, GWN7605, GWN7605LR, GWN7615, GWN7625 GWN support Hotspot 2.0 R3beta

To enable this feature, proceed from Access Point's web page → Service → Hotspot 2.0:

Time 2022-01-26 17:14   Firmware 1.0.21.14   15s ∨   English ∨   admin ⤢

General Settings ∨

Name	
Domain ID	0
HESSID ⑦	
Network Access ⑦	☑ Internet Access
Network Type	Private network ∨
IPv4 Type	Address type not available ∨
IPv6 Type	Address type not available ∨
Network Auth Type ⑦	Not configured ∨
OSU SSID ⑦	Select ∨

Venue	›
Operator Name	›
Roaming Consortium	›
Domain	›
Realm	›
Cellular Network Information	›
Port Configuration	›

Hotspot 2.0

General Settings	
Name	Set name of the hotspot.
Domain ID	Set the Domain ID.
HESSID	Configure the Homogenous Extended Service Set Identifier information for Hotspot2.0. This value must be consistent with the BSSID of an AP to identify the AP set that provides the same network access service. The format is H:H:H:H:H:H, where H is a 2-digit hexadecimal number.
Network Access	Enable or disable internet access.
Network Type	Select network type: • Private network • Private network with guest access • Chargeable public network • Free public network • Personal device network • Emergency services only network • Test or experimental • Wildcard
IPv4 Type	Select IPv4 Type: • Address type not available • Public IPv4 address available • Port-restricted IPv4 address available • Single NATed private IPv4 address available • Double NATed private IPv4 address available • Port-restricted IPv4 address and single NATed IPv4 address available • Port-restricted IPv4 address and double NATed IPv4 address available • Availability of the address type not known
IPv6 Type	Select IPv6 Type: • Address type not available • Address type available • Availability of the address type not known

Network Auth Type	Configure the Network authentication type to help users find and select the right network. Select either: • Acceptance of terms and conditions • On-line enrollment supported • http/https redirection • DNS redirection • Not configured
OSU SSID	Configure the Online Sing Up service's SSID. You need to add a SSID with Security Mode is Open or OSEN or WPA2/OSEN.
Venue	
Venue Group	Select the Venue Group type: • Unspecified • Assembly • Business • Educational • Factory • Institutional • Mercantile • Residential • Storage • Utility • Vehicular • Outdoor
Venue Type	Select the Venue type, which will depend on the Venue Group.
Language Code	Select the language.
Venue Name	Set the Venue name.
Operator Name	
Language Code	Select the language.
Operator Name	Set the Operator name.
Roaming Consortium	
Roaming Consortium Name	Configure the Roaming Consortium Name to identify network operators. The format is H-H-H or H-H-H-H-H, where H is a 2-digit hexadecimal number.
Domain	
Domain	Enter the domain name.
Realm	
Realm	Select the EAP Method: EAP-TLS, EAP-SIM, EAP-TTLS, EAP-AKA and EAP-AKA'.
Cellular Network Information	
Cellular Network Information	Enter the Name, Country Code and Network Code.
Port Configuration	
IP Protocol	Configure the protocol type: ICMP, TCP, UDP or ESP.
Port Number	Set the protocol port.
Port Status	Set the port status to either: Open, Close or Unknown.
Terms and Condition	
Filename	Specify the filename.
Timestamp	Select the timestamp
Advice of Charge	

Type	Select the type: • Time-based • Data-volume-based • Time-and-data-volume-based • Unlimited
Realm	Select the Realm.
Language Code	Select the language code.
Currency Code	Select the currency: XSU, BTN, INR, CNY, MOP, HKD, XAF.
XML Content	Upload XML file
Advanced	
WAN Link Status	Set the WAN Link Status to either: Not configured, Link-up, Link-down or Link-test.
WAN Downlink Speed	Set Download speed.
WAN Uplink Speed	Set Upload speed.
GAS Fragmentation Limit	Set GAS fragmentation limit. Default is 1400.
GAS Comeback Delay	Set GAS comeback delay. Default is 0.
Disable Downstream Group-Addressed Forwarding	When this option is disabled, it means the DGAF is enabled, the AP will forward all downlink broadcast ARP messages and wireless group broadcasts. When this option is enabled, the DGAF function is disabled, the AP will discard all downlink broadcast ARP messages and wireless group broadcasts. Disable DGAF function to prevent attackers from using the vulnerability of all clients in the same BSS using the same Group Temporal Key (GTK) to forge Group address frames and then attack the clients.

Hotspot 2.0

SNMP

This section lists the SNMP options available to integrate the GWN76xx with monitoring systems

SNMP

Field	Description
Enable	Enable SNMPv1/SNMPv2c.

Community String	Enter the SNMP Community string.
Enable	Enable SNMPv3.
Username	Enter the SNMPv3 authentication username.
Authentication Mode	Set the authentication mode to: either MD5 or SHA.
Authentication password	Enter the SNMPv3 authentication password.
Privacy Mode	Set the authentication mode to: either AES128 or DES.
Privacy password	Enter the privacy password.

SNMP

DHCP Server

By default, GWN has DHCP relay, but users could create and manage multiple DHCP server pools which will be mapped to the SSID using VLAN tag, for example when creating a DHCP pool under "**System Settings → DHCP Server**" users need to set a VLAN ID and same one should be set under SSID to map the configured DHCP pool with the SSID. This way users could configure multiple SSIDs mapped to multiple VLANs on the network in which case they are isolated by layer 2 switching.

The table below summarizes the configuration parameters for DHCP server.

Field	Description
Name	Set the name of the DHCP Pool.
Enable	Enable/Disable the DHCP pool.
VLAN ID	Set a VLAN ID, same one should be set on SSID settings to map it with the DHCP pool.
DHCP Server Static Address	Configure the static address of the DHCP server (through which GWN Master AP will be accessible).
DHCP Server Subnet Mask	Sets the subnet mask for the DHCP Pool.
DHCP Start Address	Set the start address for DHCP
DHCP End Address	Set the end address for DHCP
DHCP Lease Time	Set the DHCP lease time for the clients (default 12h).
DHCP Options	Add the Option items for DHCP, detailed option contents can be found via: https://wiki.openwrt.org/doc/howto/dhcp.dnsmasq
DHCP Gateway	Set the gateway for DHCP, and it is better to set the gateway, should be different that the static IP of the access point and on the same subnet.
DHCP Preferred DNS	Set the preferred DNS for DHCP
DHCP Alternated DNS	Set the alternated DNS for DHCP

DHCP Server Parameters

NAT Pool

GWN76xx NAT feature defines an address pool from which the Wi-Fi clients will acquire their IP address so that the access point acts as a lightweight home router.

Notes:

1. This option cannot be enabled when Client IP Assignment is set to Bridge mode.

2. This option is not supported in GWN7610

Field	Description
Default Gateway	Set the gateway IP address. **Note:** The gateway address cannot be in the same network segment as the uplink network.

DHCP Server Subnet Mask	Set the gateway mask.
DHCP Lease Time	Set the DHCP Lease time.
DHCP Preferred DNS	Set the preferred DNS for DHCP
DHCP Alternate DNS	Set the alternated DNS for DHCP

NAT Pool Parameters

Static DHCP

Users can use the feature in order to set static DHCP binding to certain clients, to whom you do not want the IP address to change.

To configure Static DHCP, please follow below steps:

1. Click **+ Add** button to create a new entry.

2. Enter the name of the device, along with its MAC address and IP address

Add	✕
MAC	00:0B:82:11:22:33
Hostname	WP820
Enable	☑
IP Address	192.168.5.203

DHCP Binding

○ Press Save and Apply to submit the changes.

TR-069

Enable TR-069	☐
ACS URL	
ACS User Name	
ACS Password	
Periodic Inform Enable	☐
Periodic Inform Interval (s)	86400
CPE Cert File	
CPE Cert Key	

TR-069

Field	Description
Enable TR-069	Configures whether to enable TR-069. **Note:** Once enabled, this device cannot be managed by GWN.Cloud anymore
ACS URL	URL for TR-069 Auto Configuration Server (ACS).
ACS Username	When AP sends a connection request to ACS, the username that ACS authenticates TR-069 client, that is AP, must be consistent with the configuration on the ACS side.
ACS Password	The password of ACS for AP authentication must be consistent with the configuration of ACS side.
Enable Periodic Inform	If enabled, AP will send connection inform packets to ACS regularly.
Periodic Inform Interval (s)	Enter the time interval when AP sends connection Inform packets to ACS regularly
CPE Cert File	Enter the certificate that AP needs to use when connecting to ACS through SSL.
CPE Cert Key	Enter the certificate key that AP needs to use when connecting to ACS through SSL.

TR-069

Notes:

1. Restrictions:

Both Master and Slave (regardless of whether it has been taken over by GWN Cloud/Local Master) support TR-069 function, and you can go to their respective local web terminal to open TR-069 and make related configuration.

If the Slave under the GWN Cloud, it will be disconnected from the Cloud. The AP can still show on the Cloud, but it is not manageable (similar to the AP taken over by the Master can be added to the Cloud); if the Slave is under the Local Master, the connection with the Local Master will be disconnected, and the Master will no longer show this AP.

2. Failover does not support TR-069 function. When multiple slaves are managed under Local Master, set a slave to failover mode. When the Master fails, the slave acts as the Master to manage other slaves. At this time, if you want to migrate to the TR-069 platform, you can only configure TR-069 for each of the other Slaves through their own local web pages. So, they need to be migrated one by one, and APs in Failover mode cannot be migrated. (After failover master get transferred into official master, by admin to login and confirm, there will be no such restriction anymore)

3. Master supports the migration of the whole setup including its slaves to TR-069, and the behavior is irreversible. If the Master turns on TR-069, all online Slave APs it controls will be migrated to the TR-069 platform, and the Master's identity will also be changed to Slave. In this process, you need to ensure the TR-069 configuration information, especially the ACS URL is configured correctly, otherwise the migration will fail, and all AP roles remain unchanged, and the function does not affect the use.

4. If a slave is offline, it will not be migrated to TR-069. After it goes online again, it will not be migrated to the TR-069 platform either. It is still in the state of being taken over by the original Master, but is no longer managed by the Master. It cannot be managed by Cloud, but can only be taken over by other Masters or factory reset.

5. APs managed by TR-069 can be "Take Over" by Local Master. After Taken Over, TR-069 shuts down by itself, and the Local Master issues the configuration to the AP to overwrite the original configuration from TR-069. This process will take a certain amount of time.

6. An AP under TR-069 will be disconnected from TR-069 by itself after the TR-069 function is turned off on the AP's local web UI, but it will not affect its function use and can continue to be taken over by Master/GWN Cloud.

SYSTEM

Settings

Users can access Maintenance page from GWN76XX **WebGUI→System → Settings**.

LEDs

GWN76XX Access Points series also support the LED schedule feature. This feature is used to set the timing when the LEDs are ON and when they will go OFF at customer's convenience.

This can be useful for example when the LEDs become disturbing during some periods of the day, this way with the LED scheduler, you can set the timing so that the LEDs are off at night after specific hours and maintain the Wi-Fi service for other clients without shutting down the AP.

Following options are available:

Field	Description
LEDs Always Off	Configure whether to disable the AP LED dictator
LEDs Always On	Configure whether to enable the AP LED dictator
Schedule	Please choose a schedule to assign to LEDs, users can configure schedules under the menu

LEDs

Following example on the next page sets the LEDs to be turned on from 8am till 8pm every day.

LED Scheduling Sample

Basic

Basic page allows Country and Time configuration.

Field	Description
LED VLAN VLAN ID Allow DHCP Option 43 to Override Management VLAN	This feature is an enhancement in regards of optimizing and reducing energy consumption of the AP. User can select to either **Always on** / **Always off** or to **Schedule** the period where the LEDs can remain on **Management VLAN:** This feature allows GWN AP to be discovered/managed on VLAN network. If enable, AP will get ip from this vlan. Enter VLAN ID Configures AP to get provisioned for management VLAN from DHCP Option 43 in the local server automatically. The default management VLAN will be overridden by the provisioned settings. Note: Once enabled, users cannot manually change the management VLAN.
Rebind Protection	Anti-domain name hijacking protection. If enabled, when the address returned by the superior DNS is a private LAN address, it will be regarded as a domain name hijacking, thus discarding the analytical result. If disabled, the analytical results will not be discarded.
Legacy TLS Compatibility	Due to the security enhancement, unless Legacy TLS Compatibility (only available on 1.0.15.4 or higher version) is enabled, master AP on 1.0.15.4 or higher firmware will not be compatible with slave AP on firmware lower than 1.0.15.4. Master AP on firmware lower than 1.0.15.4 will also not be compatible with slave AP on firmware 1.0.15.4 or higher. Cloud and GWN Manager will still support both firmware. Default is enabled.
Web HTTPS Port	Specifies HTTPS port. By default, is 443.
Country/Region	Select the country from the drop-down list. This can affect the number of channels depending on the country standards.
Scene	Depending on deployment type (Indoor or Outdoor) then additional 5Ghz channels (DFS Channels) will be available to be used. Please refer to table **DFS Channels supported by Model**. Note: This field appears for Country/Region supporting DFS
Time Zone	Configure time zone for the GWN76XX. Make sure to reboot the device to take effect.
NTP Server	Configure the IP address or URL of the NTP server. The device will obtain the date and time from the configured server.
Date Display Format	Change the Date Display Format, three options are possible YYYY/MM/DD, MM/DD/YYYY and DD/MM/YYYY.
Reboot Schedule	Select the time schedule when AP will be rebooted. Refer to [**S**] to define time.

Basic

Device	Firmware	CE	RCM	FCC	IC	ANATEL(Brazil)
GWN7610	1.0.23.3	–	–	–	–	–
GWN7600	1.0.23.3	–	–	–	–	Yes
GWN7600LR	1.0.23.3	Yes	–	–	–	–
GWN7630	1.0.23.9	Yes	Yes	Yes	Yes	Yes
GWN7630LR	1.0.23.9	Yes	Yes	Yes	Yes	–
GWN7602	1.0.23.8	Yes	Yes	Yes	Yes	Yes
GWN7605	1.0.23.9	Yes	Yes	Yes	Yes	–
GWN7605LR	1.0.23.9	Yes	Yes	Yes	Yes	–
GWN7615	1.0.23.9	Yes	Yes	Yes	Yes	–
GWN7660 GWN7660LR	1.0.23.3 1.0.23.3	Yes Yes	Yes Yes	Yes Yes	Yes Yes	–
GWN7664 GWN7664LR GWN7625	1.0.23.3 1.0.23.3 1.0.23.9	Yes Yes Yes	Yes Yes Yes	Yes Yes Yes	Yes Coming soon Yes	–

DFS Channels supported by Model

Account

The Access Web page provide configuration for admin and user password.

Field	Description
Current Administrator Password	Enter the current administrator password
New Administrator Password	Change the current password. This field is case sensitive with a maximum length of 32 characters.
Confirm New Administrator Password	Enter the new administrator password one more time to confirm.
New User Password	Configure the password for user-level Web GUI access. This field is case sensitive with a maximum length of 32 characters.
Confirm New User Password	Enter the new User password again to confirm.

Account

Note: User passwords registered for authentication through the web portal are stored in an encrypted form.

Mesh

In Mesh Network, wireless connection is established between multiple Aps, which is used to pass-through data traffic rather than client association. Each AP will evaluate the performance of wireless channel based on several factors and choose one or multiple appropriate APs to setup connection.

In a mesh network, access points are categorized to two types:

- **CAP (Central Access Point):** this is an access point that has an uplink connection to the wired network.
- **RE (Range Extender):** This is an access point that participate on the mesh network topology and has a wireless uplink connection to the central network.

In order to deploy mesh access points (RE), users/installers can follow below steps:

1. Make sure to have the master and CAP access points already deployed (sometimes the CAP access points can be the master controller of the network).
2. Next, we need to pair the RE access points to the master. This can be done in two ways:
3. Connect all REs to the same wired LAN as the master then perform the normal process of discovery/pairing process, and after successfully pairing the APs they can be deployed on the field.
4. REs can also be discovered wirelessly when powered via PSU or PoE Injector, and admin can configure them after discovery. This requires that the REs must be within the range of the Master or CAP Slave's signals coverage.

Note: If there are other GWN APs broadcasting in the same field with different subnet, RE may be wirelessly connected to those networks and cannot be discovered and paired by your Master. Therefore, it is recommended to use the first method of wired pairing and then deploy those REs.

1. After that all slave access points have been deployed and paired to the master, you can directly manage them to operate the mesh network. Mesh service configuration is the same as transitional GWN WLAN.
2. Log into the master page, and under Access Points page you can see the information, for example the AP in the "**Online Wireless**" state **is the RE** (Range Extender) with a wireless uplink to the CAP. The APs showing "**Online**" state are either a wired **master** or **CAP**.

Access Points Status

For Global mesh network settings, on GWN76XX, navigate to the menu **"System→ Settings → Mesh"**

for setting up the following parameters described below:

Mesh settings for GWN76XX

The following table down below describes the Mesh configuration settings for the GWN76XX:

Filed	Description
Enable Mesh	When checked the Mesh feature will be activated. Default is disabled.
Scan Interval	Interval in seconds to scan for available Mesh neighbors. Must be less than or equal to 300 seconds.
Interface	5GHz band. **Note**: Mesh does not support 2.4GHz, due to the channel interference.
Wireless Cascades	Define how many AP can be cascaded wirelessly with the AP. The minimum value is 1 and maximum value is 3.

Mesh configuration on GWN76XX

For more detailed information about GWN Mesh network feature, you may refer to the following technical document: Mesh Network Guide.

Important notes:

1. The RE should be set with DHCP Mode for a Client device connected to NET PORT to acquire an IP Address.

2. If RE is set with static IP, then using a PoE injector is recommended as any Network activity detected by the AP will cause the Mesh to fail. Otherwise, user will only need to make sure that there is no DHCP Server in the network connected to the AP's Ethernet port.

Schedule

Users can use the schedule configuration menu to set specific schedule for GWN features while giving the flexibility to specify the date and time to turn ON/OFF the selected feature.

The Schedule can be used for settings up specific time for Wi-Fi where the service will be active or for LED schedule or bandwidth rules ...etc.

To configure a new schedule, follow below steps:

1. Go under **System → Schedule** and click on **Create New Schedule**.

Create New Schedule

2. Select the periods on each day that will be included on the schedule and enter a name for the schedule (ex: office hours).

3. Users can choose to set weekly schedule or absolute schedule (for specific days for example), and if both weekly schedule and absolute schedules are configured on the same day then the absolute schedule will take effect and the weekly program will be cancelled for that specific date.

4. Once the schedule periods are selected, click on **Save** to save the schedule.

The list of created schedules will be displayed as shown on the figure below. With the possibility to edit or delete each schedule:

Schedules List

Maintenance

Upgrade

The Upgrade Web page allows upgrade related configuration.

Reboot

Syslog

The syslog Web page provides configuration settings for syslog.

Syslog

Field	Description
Syslog Server	Enter the IP address or URL of Syslog server.
Syslog Level	Select the level of Syslog, 8 levels are available: **Emergency, Alert, Critical, Error, Warning, Notice, Information** and **Debug**
Log DNS Queries	Check to log DNS Queries.

Syslog Parameters

Alert

The Alert page allows the administrator to select a predefined set of system events and to send notifications upon the change of the set events via email.

Email

Field	Description
Enable Email Notification	Set whether to enable Email notification

Email configuration

Alert Configure

Alert Configure

The following table describes the notifications configuration settings:

Filed	Description
Memory Usage	Configures whether to send notification if memory usage is greater than the configured threshold.
AP Throughput	Once enabled, master will generate an Alert when AP throughput reaches the configured threshold.
SSID Throughput	Once enabled, master will generate an Alert when SSID throughput reaches the configured threshold.
Admin Password Change	Configures whether to send notification on admin password change.
Firmware upgrade	Configures whether to send notification on firmware upgrade.
Rogue AP	Once enabled, system will generate an Alert when there is a Rogue AP detected.
AP Offline	Configures whether to send notification when AP going offline.

Email Events

UPGRADING AND PROVISIONING

Upgrading Firmware

The GWN76XX can be upgraded to a new firmware version remotely or locally. This section describes how to upgrade your GWN76XX.

Upgrading via Web GUI

The GWN76XX can be upgraded via TFTP/HTTP/HTTPS by configuring the URL/IP Address for the TFTP/HTTP/HTTPS server and selecting a download method. Configure a valid URL for TFTP, HTTP or HTTPS; the server name can be FQDN or IP address.

Examples of valid URLs:

firmware.grandstream.com/BETA

192.168.5.87

Examples of valid URLs:

firmware.grandstream.com/BETA

192.168.5.87

The upgrading configuration can be accessed via:

Web GUI➔System Settings➔Maintenance➔Upgrade

Upgrade

Network Upgrade Configuration

Upgrading Slave Access Points

When the GWN76XX is being paired as slave using another GWN76XX Access Point acting as Controller, users can upgrade their paired access points from the GWN76XX Master Controller.

To upgrade a slave access point, log in to the GWN76XX acting as Master Controller and go to **Access Points.**
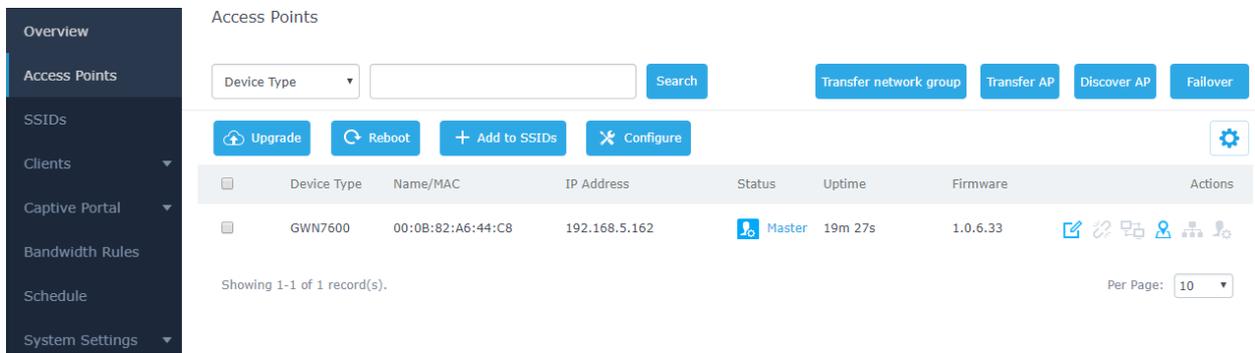
Access Points

Make sure that firmware server path is set correctly under Maintenance, check the desired APs to upgrade, and click on

 to upgrade the selected paired access points.
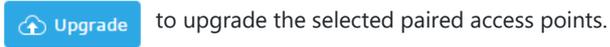
Sequential Upgrade

If you choose multiple slave devices to upgrade their firmware, two options are available: "All-at-Once" and "Sequential". "All-at-Once" will use the default method, all checked slaves will upgrade their firmware at the same time, while using "Sequential" upgrade method, the slaves will upgrade their firmware one by one in order to:

- Avoid entire Wi-Fi service interruption by full system firmware upgrade.
- Reduce network bandwidth consumption caused by firmware downloading.
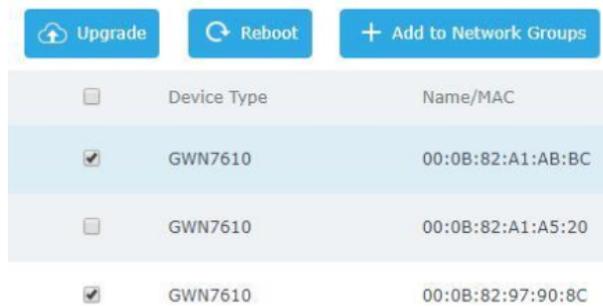
Choosing multiple devices
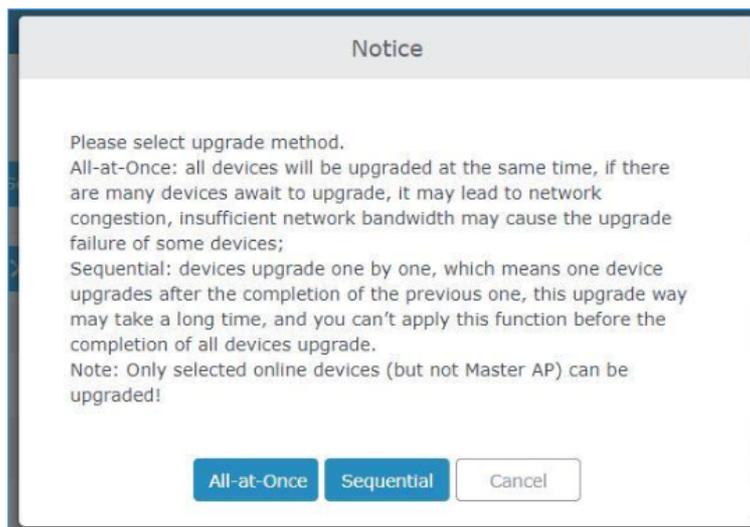
All-at-Once and Sequential Upgrade

Once you choose sequential upgrade, the following icon will update you about the number of upgraded slaves out of the selected slaves.

Provisioning and Backup

The GWN76XX configuration can be backed up locally or via network. The backup file will be used to restore the configuration on GWN76XX when necessary.

Download Configuration

Users can download the GWN76XX configuration for restore purpose under **Web GUI→System Settings→Maintenance→Upgrade**.

Click on [Download] to download locally the configuration file.

Upload Configuration

Users can upload configuration file to the GWN76XX under **Web GUI→System Settings→Maintenance→Upgrade**.

Click on [Upload] to browse for the configuration to upload.

Please note that the GWN76XX will reboot after the configuration file is restored successfully.

Configuration Server

Users can download and provision the GWN76XX by putting the config file on a TFTP/HTTP or HTTPS server and set Config Server to the TFTP/HTTP or HTTPS server used in order for the GWN76XX to be provisioned with that config server file.
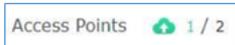
Reset and reboot

- Users could perform a reboot and reset the device to factory functions under **Web GUI→System Settings→Maintenance→Upgrade** by clicking on [Reboot] button.

- [Reset] Will restore all the GWN76XX itself to factory settings.

Syslog

On the GWN76XX, users could dump the syslog information to a remote server under **Web GUI→System Settings→Maintenance**. Enter the syslog server hostname or IP address and select the level for the syslog information. Eight levels of syslog are available: Emergency, Alert, Critical, Error, Warning, Notice, Information and Debug

EXPERIENCING THE GWN76xx Wi-Fi ACCESS POINTS

Please visit our website: https://www.grandstream.com to receive the most up- to-date updates on firmware releases, additional features, FAQs, documentation, and news on new products.

We encourage you to browse our product related documentation, FAQs and User and Developer Forum for answers to your general questions. If you have purchased our products through a Grandstream Certified Partner or Reseller, please contact them directly for immediate support.

Our technical support staff is trained and ready to answer all your questions. Contact a technical support member or submit a trouble ticket online to receive in-depth support.Thank you again for purchasing Grandstream GWN76XX Wi-Fi Access Point, it will be sure to bring convenience and color to both your business and personal life

Thank you again for purchasing Grandstream GWN76XX Wi-Fi Access Point, it will be sure to bring convenience and color to both your business and personal life

CHANGE LOG

This section documents significant changes from previous versions of the GWN76xx user manuals. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware Version 1.0.23.22

Product Name: GWN7610 / GWN7600 / GWN7600LR / GWN7602 / GWN7615 / GWN7605 / GWN7605LR / GWN7630 / GWN7630LR / GWN7624 / GWN7625 / GWN7660 / GWN7660LR / GWN7664 / GWN7664LR

- Added support for GWN Cloud v1.1.23.27 and GWN Manager v1.1.23.27

Firmware Version 1.0.23.11

Product Name: GWN7602

- No major changes

Firmware Version 1.0.23.8

Product Name: GWN7602

- Added support of Import/Export the client access lists in CSV format [Access List]
- Added support of 802.11h
- Added support of PPSK [SSIDs]
- Added support of PassPoint R3 [Hotspot 2.0]
- Added support of Management VLAN [Basic]
- Added support of Active Directory [Internal Splash Page]

Firmware Version 1.0.23.15/1.0.23.7

Version 1.0.23.15

Product Name: GWN7605 / GWN7605LR / GWN7615 / GWN7630 / GWN7630LR / GWN7624 / GWN7625

- No major changes

Version 1.0.23.7

Product Name: GWN7664 / GWN7664LR

- No major changes

Firmware Version 1.0.23.14

Product Name: GWN7615 / GWN7605 / GWN7605LR / GWN7630 / GWN7630LR / GWN7625

- No major changes

Firmware Version 1.0.23.13/1.0.23.6

Version 1.0.23.13

Product Name: GWN7615 / GWN7605 / GWN7605LR / GWN7630 / GWN7630LR

- No major changes

Version 1.0.23.6

Product Name: GWN7600 / GWN7600LR / GWN7610 / GWN7660 / GWN7660LR / GWN7664 / GWN7664LR

- No major changes

Firmware Version 1.0.23.9

Product Name: GWN7605 / GWN7605LR / GWN7615 / GWN7625 / GWN7630 / GWN7630LR

- Added support of more DFS Channels. [Scene]

Firmware Version 1.0.23.7

Product Name: GWN7605 / GWN7605LR / GWN7615 / GWN7625 / GWN7630 / GWN7630LR

- Added support of Import/Export the client access lists in CSV format [Access List]
- Added support of 802.11h
- Added support of PPSK [SSIDs]
- Added support of PassPoint R3 [Hotspot 2.0]
- Added support of 15 languages
- Added support of Management VLAN [Basic]
- Added support of Active Directory [Internal Splash Page]

Firmware Version 1.0.23.3

Product Name: GWN7600 / GWN7600LR / GWN7610 / GWN7660 / GWN7660LR / GWN7664 / GWN7664LR

- Added support of Link aggregation for GWN7664/GWN7664LR

Firmware Version 1.0.19.36

Product Name: GWN7602

- Enabled band 3 and band 4 channels for Israel.
- Added support of SMS authentication. [SMS]

Firmware Version 1.0.21.16

Product Name: GWN7660 / GWN7664

- No major changes.

Firmware Version 1.0.21.15

Product Name: GWN7630 / GWN7630LR

- Added support of Hotspot 2.0 R3^{Beta} for GWN7630/GWN7630LR. [Hotspot 2.0]

Firmware Version 1.0.21.14/15

Product Name: GWN7605 / GWN7605LR / GWN7615 / GWN7630 / GWN7630LR / GWN7660 / GWN7664

- Added support of Hotspot 2.0 R3^{Beta} for GWN7660. [Hotspot 2.0]
- Added support of Bonjour Gateway. [Enable Bonjour Gateway]

Firmware Version 1.0.21.7

Product Name: GWN7600 / GWN7600LR / GWN7610 / GWN7660

- Enable FCC DFS channels for GWN7660 [Table 39: DFS Channels supported by Model]

Firmware Version 1.0.21.6

Product Name: GWN7630 / GWN7630LR / GWN7605 / GWN7605LR / GWN7615

- Upgraded the max number of supported SSIDs [Table 22 : MAX SSID on each band]

- Added Option to turn off U-APSD function [Table 21: Wi-Fi]

- Added IPv6 support for internal GWN services [Table 20: Access Point Configuration Settings]

- Added feature to Transfer AP to GWN manager [Transfer AP]

- Added feature to allow Each AP to disable/Enable 2.4GHz or 5GHz independently [Table 20: Access Point Configuration Settings]

- Added feature of TR-069 [TR-069]

- Added feature of Google Authentication [Table 25: Captive Portal – Policy List – Splash Page is "Internal"]

- Added feature to Delete inbound and outbound rules in batches [Firewall]

- Added feature to save network abnormal log to Flash [Debug]

- Added feature of Web lock for failed login [Access Web GUI]

Firmware Version 1.0.19.32

Product Name: GWN7630 / GWN7630LR / GWN7605 / GWN7605LR / GWN7615 / GWN7602 / GWN7600 / GWN7600LR / GWN7610

- No major changes.

Firmware Version 1.0.19.14

Product Name: GWN7660

- This is the initial version for GWN7660

Firmware Version 1.0.19.29

Product Name: GWN7630 / GWN7630LR / GWN7605 / GWN7605LR / GWN7615

- No major changes

Firmware Version 1.0.19.25

Product Name: GWN7630 / GWN7630LR / GWN7605 / GWN7605LR / GWN7615 / GWN7602 / GWN7600 / GWN7600LR / GWN7610

- No major changes

Firmware Version 1.0.19.23

Product Name: GWN7610 / GWN7600 / GWN7600LR

- Added support for Secondary RADIUS Server. [Secondary RADIUS Server]

- Added support for Rogue AP Alert. [Alert Configure]

Firmware Version 1.0.19.22

Product Name: GWN7615 / GWN7602 / GWN7605 / GWN7605LR / GWN7630 / GWN7630LR / GWN7602

- Added support for WPA3 (GWN7602 does NOT support). [Security Mode]

- Added support for Secondary RADIUS Server. [Secondary RADIUS Server]

- Added support for Rogue AP Alert. [Alert Configure]

- Added support of NET port VLAN settings. [Net Port Type]

Firmware Version 1.0.19.15

- No major changes

Firmware Version 1.0.19.9

- Added support of Rogue AP Detection. [Rogue AP]
- Added support of 802.11w. [802.11w]
- Added support of AutoTX Power. [RADIO]
- Added Captive Portal Enhancement. [CAPTIVE PORTAL]
- Added support of SNMP. [SNMP]
- Added support of more DFS Channels. [Scene]
- Added support of NAT. [NAT]
- Added support of Firewall. [Firewall]
- Added support of Hotspot 2.0 Beta. [Hotspot 2.0]
- Added support of Multicast/Broadcast Suppression. [Multicast/Broadcast Suppression]
- Extended support of RRM to GWN Cloud and remaining AP models. [Transmit Power Control][Coverage Hole Detection][Dynamic Channel Assignment]
- Added support of Active IGMP for feature Convert IP multicast to unicast enhancement. [Convert IP multicast to unicast]
- Allow DHCP Option43 to override GWN Manager Address. [Allow DHCP Option 43 to override GWN Manager Address]

Firmware Version 1.0.19.4

Product Name: GWN7602

- Added support of Multicast/Broadcast Suppression. [SSID]
- Added support of RRM. [RADIO]
- Added support of Active IGMP for feature Convert IP multicast to unicast enhancement. [SSID]
- Added support of Rogue AP Detection.[ROGUE AP]
- Added support of 802.11w. [SSID]
- Added support of Auto TX Power. [DEVICE CONFIGURATION]
- Added Captive Portal Enhancement.
- Added support of SNMP. [SNMP]
- Added support of Allow DHCP Option 43 to override GWN Manager Address. [Pairing with Master]
- Added support of NAT. [NAT]
- Added support of Firewall. [FIREWALL]

Firmware Version 1.0.15.20

Product Name: GWN7610 / GWN7600 / GWN7600LR / GWN7630 / GWN7630LR / GWN7602

- Added support for more DFS channels [Scene]

Firmware Version 1.0.15.18

Product Name: GWN7605

- Added support for CE/RCM DFS channels [Scene]

Firmware Version 1.0.15.15

Product Name: GWN7605

- Added yellow LED pattern to indicate Mesh disconnection [LED Status]

Firmware Version 1.0.15.5

Product Name: GWN7605

- This is the initial version for GWN7605

Firmware Version 1.0.15.4

Product Name: GWN7610 / GWN7600 / GWN7600LR/ GWN7630 / GWN7630LR

- Added support of GWM Manager. [GWN Manager]
- Added LED pattern of yellow to indicate Mesh disconnection. [LED Patterns]
- Upgraded TLS to version 1.2

Firmware Version 1.0.15.6

Product Name: GWN7630 / GWN7630LR

- Added support for FCC DFS channels on GWN7630/GWN7630LR. [Scene]

Firmware Version 1.0.11.10

Product Name: GWN7630LR

- This is the initial version for GWN7630LR.

Firmware Version 1.0.11.8

Product Name: GWN7610 / GWN7600 / GWN7600LR / GWN7630

- Added support of DFS channel in EU for GWN7630. [Scene]
- Added support for Client Steering. [Client Steering]
- Added support for Minimum Rate Control. [RADIO]
- Added support for batch operations for Takeover. [Takeover Feature]
- Added support for Client inactivity timeout. [SSID]
- Enhanced Voucher feature by displaying remaining bytes. [Vouchers]
- Changed LED Pattern. [LED Patterns]
- Changed Local Master External Portal Configuration. [External Splash Page]
- Changed default setting of Mesh to OFF. [Mesh]

Firmware Version 1.0.8.18

Product Name: GWN7610 / GWN7600 / GWN7600LR

- Added support of ARP Proxy. [ARP Proxy]
- Enhanced Bandwidth Rules by adding option to limit bandwidth Per-User. [Range Constraint]

Firmware Version 1.0.8.9

Product Name: GWN7610 / GWN7600 / GWN7600LR

- No major changes

Firmware Version 1.0.7.13

Product Name: GWN7610 / GWN7600 / GWN7600LR

- Added support of Radio Resource Management (RRM). [Dynamic Channel Assignment] [Transmit Power Control] [Coverage Hole Detection]

Firmware Version 1.0.4.22

Product Name: GWN7610

- Included patch for WPA2 4-way handshake vulnerability [VU#228519]

Firmware Version 1.0.4.20

Product Name: GWN7610

- Added support for Timed Client Disconnect and Enhanced Client Blocking [CLIENTS]
- Added support for Client Bridge [Client Bridge]
- Added support for Syslog server [Syslog]
- Added support for Configurable Web UI access port. [Web HTTPS Port]
- Added support for E-mail notifications [Email]

Firmware Version 1.0.4.12

Product Name: GWN7600 / GWN7600LR

- Added support for Timed Client Disconnect and Enhanced Client Blocking [CLIENTS]
- Added support for Client Bridge [Client Bridge]
- Added support for Syslog server [Syslog]
- Added support for Configurable Web UI access port. [Web HTTPS Port]
- Included patch for WPA2 4-way handshake vulnerability [VU#228519]

Firmware Version 1.0.3.4

- This is the initial version of GWN7602

Firmware Version 1.0.3.25

Product Name: GWN7600 / GWN7600LR

- No major changes.

Firmware Version 1.0.3.21

Product Name: GWN7610

- No major changes.

Firmware Version 1.0.3.19

Product Name: GWN7610 / GWN7600 / GWN7600LR

- Added support for captive portal [CAPTIVE PORTAL]
- Added support for 802.11k/r/v [Enable Voice Enterprise]
- Added support for failover master [Failover Master]
- Added support for VLAN assignment via RADIUS [SSID][Enable Dynamic VLAN (beta)]
- Added support for Select SSID Band [SSID Band]
- Added support for Exact Radio Power Configuration in dBm [Custom Wireless Power]
- Added support for AP Location [AP Location]
- Added support for Per-Client/Per-SSID bandwidth rules [Bandwidth R]
- Added support for Wi-Fi Schedule [S]
- Added support for LED control [L]
- Added option to enable/disable DHCP option 66 & 43 override [Allow DHCP options 66 and 43 override]

Firmware Version 1.0.2.108

Product Name: GWN7610

- Added Controller protocol security enhancement. [Controller Protocol Security Enhancement]

- Added support for LED control. [L]

- Added support for Captive Portal. [CAPTIVE PORTAL]

- Added support for Wi-Fi schedule. [S]

- Added Client Isolation enhancement. [SSID]

- Added support to store Syslog locally on the unit and display it on Web GUI. [Syslog]

Firmware Version 1.0.2.15

Product Name: GWN7610

- Added New Overview Page.

- Added Web UI enhancement.

- Added support for Password change on first boot.

- Added Country code selection into setup wizard.

Firmware Version 1.0.1.31

Product Name: GWN7600 / GWN7600LR

- This is the initial version.

Firmware Version 1.0.1.27

Product Name: GWN7610

- This is the initial version.

Certificates

COPYRIGHT

©2022 Grandstream Networks, Inc. https://www.grandstream.com
All rights reserved. Information in this document is subject to change without notice. Reproduction or
transmittal of the entire or any part, in any form or by any means, electronic or print, for any purpose
without the express written permission of Grandstream Networks, Inc. is not permitted.
The latest electronic version of this guide is available for download here:
https://www.grandstream.com/support
Grandstream is a registered trademark and Grandstream logo is trademark of Grandstream Networks, Inc. in the United States,
Europe, and other countries

CAUTION

Changes or modifications to this product not expressly approved by Grandstream, or operation of this
product in any way other than as detailed by this guide, could void your manufacturer warranty.

WARNING

Please do not use a different power adapter with devices as it may cause damage to the products and
void the manufacturer warranty.

FCC Caution

Any changes or modifications to this unit not expressly approved by the party responsible for compliance could void the
user's authority to operate the equipment.

This device complies with 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not
cause harmful interference, and (2) this device must accept any interference
received, including interference that may cause undesired operation.

Note:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.
This equipment should be installed and operated with minimum distance 20cm between the radiator&
your body.
This transmitter must not be co-located or operating in conjunction with any other antenna transmitter.

ISEDC Warning

This device complies with Innovation, Science, and Economic Development Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: 1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radio électrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

ISEDC Warning

This equipment complies with ISEDC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. Cet équipement est conforme aux ISEDC RF limites d'exposition aux radiations dans un environnement non contrôlé. Cet émetteur ne doit pas être situé ou opérant en conjonction avec une autre antenne ou émetteur.

CE Authentication

BE	BG	CZ	DK	DE	EE	IE	EL	LI
ES	FR	HR	IT	CY	LV	LT	LU	CH
HU	MT	NL	AT	PL	PT	RO	SI	TR
SK	FI	SE	NO	IS	UK	UK(NI)		

In the UK and EU member states, operation of 5150-5350 MHz is restricted to indoor use only.

EU Regulatory Information

GWN7630	GWN7630LR
TX/RX Frequency	**TX/RX Frequency**
2.4G Wi-Fi: 2412-2472MHz;	**2.4G Wi-Fi:** 2412-2472MHz
5G Wi-Fi: 5150-5250MHz;5250-5350 MHz; 5470-5725 MHz	**5G Wi-Fi:** 5150-5250MHz;5250-5350 MHz; 5470-5725 MHz
Output power	**Output power**

WLAN 2.4G < 20dBm;	WLAN 2.4G < 20dBm
WLAN 5150-5250MHz< 23dBm	WLAN 5150-5250MHz< 23dBm
WLAN 5250-5350 MHz< 20dBm	WLAN 5250-5350 MHz< 20dBm
WLAN 5470-5725 MHz< 27dBm	WLAN 5470-5725 MHz< 27dBm
Modulation	**Modulation**
DSSS, OFDM	DSSS, OFDM

GWN7610	GWN7600
TX/RX Frequency	**TX/RX Frequency**
2.4G Wi-Fi: 2412-2472MHz;	**2.4G Wi-Fi:** 2412-2472MHz
5G Wi-Fi: 5150-5250MHz	**5G Wi-Fi:** 5150-5250MHz
Output power	**Output power**
WLAN 2.4G < 20dBm;	WLAN 2.4G < 20dBm
WLAN 5150-5250MHz< 23dBm	WLAN 5150-5250MHz< 23dBm
Modulation	**Modulation**
DSSS, OFDM	DSSS, OFDM

GWN7615	GWN7600LR
TX/RX Frequency	**TX/RX Frequency**
2.4G Wi-Fi: 2412-2472MHz;	**2.4G Wi-Fi:** 2412-2472MHz
5G Wi-Fi: 5150-5250MHz;5250-5350 MHz; 5470-5725 MHz	**5G Wi-Fi:** 5150-5250MHz;5250-5350 MHz; 5470-5725 MHz; 5725-5850MHz
Output power	**Output power**
WLAN 2.4G < 20dBm;	WLAN 2.4G < 20dBm
WLAN 5150-5250MHz< 23dBm	WLAN 5150-5250MHz< 23dBm
WLAN 5250-5350 MHz< 20dBm	WLAN 5250-5350 MHz< 20dBm
WLAN 5470-5725 MHz< 27dBm	WLAN 5470-5725 MHz< 27dBm
	WLAN 5725-5850 MHz<14dBm

Modulation	**Modulation**
DSSS, OFDM	DSSS, OFDM

GWN7605	GWN7605LR
TX/RX Frequency	**TX/RX Frequency**
2.4G Wi-Fi: 2412-2472MHz;	**2.4G Wi-Fi:** 2412-2472MHz
5G Wi-Fi: 5150-5250MHz;5250-5350 MHz; 5470-5725 MHz	**5G Wi-Fi:** 5150-5250MHz;5250-5350 MHz; 5470-5725 MHz
Output power	**Output power**
WLAN 2.4G < 20dBm;	WLAN 2.4G < 20dBm
WLAN 5150-5250MHz< 23dBm	WLAN 5150-5250MHz< 23dBm
WLAN 5250-5350 MHz< 20dBm	WLAN 5250-5350 MHz< 20dBm
WLAN 5470-5725 MHz< 27dBm	WLAN 5470-5725 MHz< 27dBm
Modulation	**Modulation**
DSSS, OFDM	DSSS, OFDM

GWN7660	GWN7664
TX/RX Frequency	**TX/RX Frequency**
2.4G Wi-Fi: 2412-2472MHz;	**2.4G Wi-Fi:** 2412-2472MHz
5G Wi-Fi: 5150-5250MHz;5250-5350 MHz; 5470-5725 MHz	**5G Wi-Fi:** 5150-5250MHz;5250-5350 MHz; 5470-5725 MHz
Output power	**Output power**
WLAN 2.4G < 20dBm;	WLAN 2.4G < 20dBm
WLAN 5150-5250MHz< 23dBm	WLAN 5150-5250MHz< 23dBm
WLAN 5250-5350 MHz< 20dBm	WLAN 5250-5350 MHz< 20dBm
WLAN 5470-5725 MHz< 27dBm	WLAN 5470-5725 MHz< 27dBm
Modulation	**Modulation**
DSSS, OFDM, OFDMA	DSSS, OFDM, OFDMA

GWN7660LR
TX/RX Frequency
2.4G Wi-Fi: 2412-2484MHz
5G Wi-Fi: 5180-5825MHz
Output power
WLAN 2.4G < 30dBm
WLAN 5G < 26dBm
Modulation
DSSS, OFDM, OFDMA

The simplified EU declaration of conformity referred to in Article 10(9) shall be provided as follows:
Hereby, [Grandstream Networks, Inc.] declares that the radio equipment type
[GWN7664/GWN7660/GWN7630/GWN7630LR/GWN7610/GWN7600/GWN7600LR/GWN7605/GWN7605LR/GWN7615] are in compliance with Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at the following internet address:
https://www.grandstream.com

GNU GPL INFORMATION

GWN76XX firmware contains third-party software licensed under the GNU General Public License (GPL).
Grandstream uses software under the specific terms of the GPL. Please see the GNU General Public License (GPL) for the exact terms and conditions of the license.
Grandstream GNU GPL related source code can be downloaded from Grandstream web site:
https://www.grandstream.com/support/faq/gnu-general-public-license