



Grandstream Networks, Inc.

Wi-Fi Access Points

GWN76xx – User Manual



OVERVIEW

Grandstream's powerful indoor and outdoor Wi-Fi Access Points (APs) offer high-performance networking and an exceptional Wi-Fi coverage range. The outdoor series offers weatherproof certified casing and supports up to a 750-meter coverage range. They are supported by GWN.Cloud and GWN Manager, Grandstream's cloud and on-premise free management platforms. Each device also includes an embedded controller within the product's web user interface for easy administration of locally deployed Wi-Fi APs. GWN Wi-Fi APs are ideal for any size business or enterprise and can be scaled over time as your business grows.

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

GWN7661 Technical Specifications

| | |
|---------------------------|---|
| Wi-Fi Standards | IEEE 802.11 a/b/g/n/ac/ax |
| Antennas | 4 single band internal antennas. 2.4GHz x 2: gain 3.30dBi, gain 3.51dBi 5GHz x 2: gain 4.79dBi, gain 5.37dBi |
| Wi-Fi Data Rates | 2.4GHz: 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 5GHz: IEEE 802.11ax: 7.3 Mbps to 1201 Mbps 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 <i>*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</i> |
| Frequency Bands | 2.4GHz Radio: 2412 - 2484 MHz 5GHz Radio: 5180 - 5825 MHz <i>*Not all frequency bands can be used in all regions</i> |
| 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) 2×2:2 5GHz (MU-MIMO) |
| Coverage Range | Up to 100 meters <i>*coverage range can vary based on environment</i> |
| Maximum TX Power | 5G: 27dBm 2.4G: 24dBm <i>*Maximum power varies by country, frequency band and MCS rate</i> |
| 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; 802.11ax 20MHz: -60dBm @MCS11; 802.11ax 40MHz: -58dBm @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: -60dBm @MCS11; 802.11ax 40MHz: -58dBm @MCS11; 802.11ax 80MHz: -56dBm @MCS11 |
| SSIDs | 32 SSIDs total , 16 per radio (2.4GHz & 5GHz) |
| Concurrent Clients | Up to 500+ |
| 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 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 | 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); Unit Weight: 185g Entire Package Dimension: 176mm(L)x118.5mm(W)x65mm(H); Entire Package Weight: 400g |
| Package Content | GWN7661 In-Wall Wireless AP 4x Screws(KB 3.5*26) Quick Installation Guide |
| Compliance | FCC, CE, RCM, IC, UKCA |

GWN7661 Technical Specifications

GWN7662 Technical Specifications

| | |
|----------------------------------|--|
| Wi-Fi Standards | IEEE 802.11 a/b/g/n/ac/ax |
| Antennas | 6 single frequency internal antennas 2.4GHz , gain 3.65dBi 5 GHz , gain 5.26dBi |
| 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 <i>*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</i> |
| Frequency Bands | 2.4GHz Radio: 2412 - 2484 MHz 5GHz Radio: 5180 - 5825 MHz <i>*Not all frequency bands can be used in all regions</i> |
| Channel Bandwidth | 2.4G: 20 and 40 MHz 5G: 20, 40 , 80 and 160MHz |
| 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 (MU-MIMO) 4×4:4 5GHz (MU-MIMO) |
| Coverage Range | Up to 175 meters <i>*coverage range can vary based on the environment</i> |
| Maximum TX Power | 5G: 25dBm 2.4G: 27dBm <i>*Maximum power varies by country, frequency band, and MCS rate</i> |
| 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 | 256 |
| Network Interfaces | <ul style="list-style-type: none"> • 1x autosensing 10/100/1000 Base-T Ethernet Port • 1x autosensing 10/100/1000/2500 Base-T Ethernet Port |
| Auxiliary Ports | 1x Reset Pinhole |
| Mounting | Indoor wall mount or ceiling 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 |
| 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 | Supports 802.3az PoE 802.3af/ 802.3at; Maximum Power Consumption: 16W |
| Environmental | Operation:-10°Cto 45°C Storage: -30°C to 60°C Humidity: 5% to 90% Non-condensing |
| Physical | <ul style="list-style-type: none"> • Unit Dimension: 205.3mm(L)x205.3mm(W)x45.9mm(H); Unit Weight: 540g • Entire Package Dimension: 258mm(L)x247mm(W)x86mm(H); Entire Package Weight: 910g |
| Package Content | GWN7664LR 802.11ax Wireless AP, Mounting Kits, Quick Installation Guide |
| Compliance | FCC, CE, RCM, IC, UKCA |

GWN7662 Technical Specifications

GWN7624 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 |

| | |
|----------------------------------|---|
| | <p>IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps</p> <p>5GHz:</p> <p>IEEE 802.11ac: 6.5 Mbps to 1733 Mbps</p> <p>IEEE 802.11n: 6.5Mbps to 600Mbps</p> <p>IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps</p> <p><i>*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</i></p> |
| Frequency Bands | <p>2.4GHz Radio: 2412 - 2484 MHz</p> <p>5GHz Radio: 5180 - 5825 MHz</p> <p><i>*Not all frequency bands can be used in all regions</i></p> |
| Channel Bandwidth | <p>2.4G: 20 and 40 MHz</p> <p>5G: 20, 40 and 80 MHz</p> |
| 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 | <p>2x2:2 2.4GHz (MIMO)</p> <p>4x4:4 5GHz (MU-MIMO)</p> |
| Coverage Range | <p>Up to 100 meters</p> <p><i>*coverage range can vary based on environment</i></p> |
| Maximum TX Power | <p>5G: 25dBm</p> <p>2.4G: 23dBm</p> <p><i>*Maximum power varies by country, frequency band and MCS rate</i></p> |
| Receiver Sensitivity | <p>2.4GHz</p> <p>802.11b: -96dBm@1Mbps, -88dBm@11Mbps;</p> <p>802.11g: -93dBm @6Mbps, -75dBm@54Mbps;</p> <p>802.11n 20MHz: -73dBm @MCS7; 802.11n 40MHz:-70dBm @MCS7 @MCS11</p> <p>5GHz</p> <p>802.11a: -92dBm @6Mbps, -74dBm @54Mbps;</p> <p>802.11n 20MHz: -74dBm @MCS7; 802.11n 40MHz:-71dBm @MCS7</p> <p>802.11ac 20MHz: -67dBm@MCS8; 802.11ac: HT40:- 63dBm @MCS9; 802.11ac 80MHz: -59dBm @MCS9</p> |
| SSIDs | 16 SSIDs total , 8 per radio (2.4GHz & 5GHz) |
| Concurrent Clients | Up to 200 |
| Network Interfaces | <p>1x 10/100/1000M uplink Ethernet port with PoE/PoE+</p> <p>2x 10/100/1000M Ethernet port with PSE</p> <p>1x 10/100/1000M Ethernet port</p> |
| 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°C to 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

GWN7664LR 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 <i>*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</i> |
| Frequency Bands | 2.4GHz Radio: 2412 - 2484 MHz 5GHz Radio: 5180 - 5825 MHz <i>*Not all frequency bands can be used in all regions</i> |
| 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 | 4x4:4 2.4GHz |

| | |
|--|---|
| | 4×4:4 5GHz |
| Coverage Range | Up to 300 meters <i>*coverage range can vary based on environment</i> |
| Maximum TX Power | 5G: 25dBm 2.4G: 26dBm <i>*Maximum power varies by country, frequency band and MCS rate</i> |
| 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°C to 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

GWN7625 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 <i>*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</i> |
| Frequency Bands | 2.4GHz Radio: 2412 - 2484 MHz 5GHz Radio: 5180 - 5825 MHz <i>*Not all frequency bands can be used in all regions</i> |
| 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 <i>*Maximum power varies by country, frequency band and MCS rate</i> |
| 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

GWN7664 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 | <p>5G:</p> <p>IEEE 802.11ax: 8 Mbps to 2402 Mbps</p> <p>IEEE 802.11ac: 6.5 Mbps to 1733 Mbps</p> <p>IEEE 802.11n: 6.5 Mbps to 600 Mbps</p> <p>IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps</p> <p>2.4G:</p> <p>IEEE 802.11ax: 8 Mbps to 1147 Mbps</p> <p>IEEE 802.11n: 6.5 Mbps to 600Mbps</p> <p>IEEE 802.11b: 1, 2, 5.5, 11Mbps</p> <p>IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps</p> <p><i>*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.</i></p> |
| Frequency Bands | <p>2.4GHz Radio: 2412 – 2484 MHz</p> <p>5GHz Radio: 5180 – 5825 MHz</p> <p><i>*Not all frequency bands can be used in all regions</i></p> |
| Channel Bandwidth | <p>2.4G: 20 and 40 MHz (x4)</p> <p>5G: 20, 40 and 80 MHz (x4)</p> |
| Wi-Fi and System Security | <p>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</p> |
| MIMO | <p>4×4:4 2.4GHz</p> <p>4×4:4 5GHz</p> |
| Coverage Range | <p>Up to 175 meters</p> <p><i>*Coverage range can vary based on environment</i></p> |
| Maximum TX Power | <p>5G: 25dBm</p> <p>2.4G: 26dBm</p> <p><i>*Maximum power varies by country, frequency band and MCS rate</i></p> |

| | |
|--|---|
| Receiver Sensitivity | <p>2.4G</p> <p>802.11b: -99dBm@1Mbps, -91dBm@11Mbps;</p> <p>802.11g: -94dBm @6Mbps, -78dBm@54Mbps;</p> <p>802.11n 20MHz: -75dBm @MCS7; 802.11n 40MHz:-71dBm @MCS7;</p> <p>802.11ax 20MHz: -64dBm @ MCS11; 802.11ax 40MHz: -63dBm @MCS11</p> <p>5G</p> <p>802.11a: -95dBm @6Mbps, -77dBm @54Mbps;</p> <p>802.11n 20MHz: -74dBm @MCS7; 802.11n 40MHz:-71dBm @MCS7</p> <p>802.11ac 20MHz: -70dBm@MCS8; 802.11ac: HT40:- 66dBm @MCS9; 802.11ac 80MHz: -62dBm @MCS9;</p> <p>802.11ax 20MHz: -64dBm @ MCS11; 802.11ax 40MHz: -62dBm @MCS11;802.11ax 80MHz: -59dBm @MCS11</p> <p><i>*Receiver sensitivity varies by frequency band, channel width and MCS rate</i></p> |
| 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 | <p>Embedded controller can manage up to 50 local GWN APs</p> <p>GWN.Cloud offers a free cloud management platform for unlimited GWN APs</p> <p>GWN Manager offers premise-based software controller for up to 3,000 GWN APs</p> |
| Auto Power Saving | Self-power adaptation upon auto detection of PoE or PoE+ |
| Power and Green Energy Efficiency | <p>Power over Ethernet 802.3af/802.3at compliant</p> <p>Maximum Power Consumption: 17W.</p> |
| Environmental | <p>Operation: 0°C to 45°C</p> <p>Storage: -10°C to 60°C</p> <p>Humidity: 10% to 90% Non-condensing</p> |
| 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

GWN7660 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 | <p>5G:</p> <p>IEEE 802.11ax: 7.3 Mbps to 1201 Mbps</p> <p>IEEE 802.11ac: 6.5 Mbps to 867 Mbps</p> <p>IEEE 802.11n: 6.5Mbps to 300Mbps</p> <p>IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps</p> <p>2.4G:</p> <p>IEEE 802.11ax: 7.3 Mbps to 573.5 Mbps</p> <p>IEEE 802.11n: 6.5Mbps to 300Mbps</p> <p>IEEE 802.11b: 1, 2, 5.5, 11Mbps</p> <p>IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps</p> <p><i>*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.</i></p> |
| 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) <i>*coverage range can vary based on environment</i> |

| | |
|--|---|
| Maximum TX Power | <p>2.4G: 24 dBm</p> <p>5G: 22 dBm</p> <p><i>*Maximum power varies by country, frequency band and MCS rate</i></p> |
| Receiver Sensitivity | <p>2.4G</p> <p>802.11b: -96dBm@1Mbps, -88dBm@11Mbps; 802.11g: -93dBm @6Mbps, -75dBm@54Mbps;</p> <p>802.11n 20MHz: -73dBm @MCS7; 802.11n 40MHz:-70dBm @MCS7; 802.11ax 20MHz: -60dBm @MCS11; 802.11ax 40MHz: -58dBm @MCS11</p> <p>5G</p> <p>802.11a: -92dBm @6Mbps, -74dBm @54Mbps; 802.11ac 20MHz: -67dBm@MCS8;</p> <p>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 <i>Receiver sensitivity varies by frequency band, channel width and MCS rate</i></p> |
| SSIDs | 32 SSIDs total, 16 per radio (2.4GHz and 5GHz) |
| Concurrent Clients | 500+ |
| 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 | <p>Embedded controller can manage up to 50 local GWN APs</p> <p>GWN.Cloud offers a free cloud management platform for unlimited GWN APs</p> <p>GWN Manager offers premise-based software controller for up to 3,000 GWN APs</p> |
| Auto Power Saving | Self-power adaptation upon auto detection of PoE or PoE+ |
| Power and Green Energy Efficiency | <p>Power over Ethernet 802.3af/802.3at compliant</p> <p>Maximum Power Consumption: 9W.</p> |
| Environmental | <p>Operation: 0°C to 45°C</p> <p>Storage: -10°C to 60°C</p> <p>Humidity: 10% to 90% Non-condensing</p> |

| | |
|------------------------|--|
| 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

GWN7660LR 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 <i>*coverage range can vary based on environment</i> |
| Maximum TX Power | 5G: 26dBm 2.4G: 30dBm *Maximum power varies by country, frequency band, and MCS rate |

| | |
|--|--|
| Receiver Sensitivity | <p>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</p> <p>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</p> |
| SSIDs | 32 SSIDs total, 16 per radio (2.4GHz & 5GHz) |
| Concurrent Clients | 500+ |
| 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 | <p>Embedded controller can manage up to 50 local GWN APs</p> <p>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</p> |
| Power and Green Energy Efficiency | <p>POE 802.3af/ 802.3at;</p> <p>Maximum Power Consumption: 10.16W</p> |
| Environmental | <p>Operation: -30°C to 60°C</p> <p>Storage: -30°C to 70°C</p> <p>Humidity: 5% to 95% Non-condensing</p> |
| Physical | <p>Physical Unit Dimension: 358.3mm(L)*115mm(W)*45.3mm(H); Unit Weight: 500g</p> <p>Entire Package Dimension: 258 × 247× 86mm; Entire Package Weight:655.3g</p> |
| 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 |

| | |
|----------------------------------|---|
| 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 <i>*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.</i> |
| 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) <i>*coverage range can vary based on environment</i> |
| Maximum TX Power | 2.4G: 27 dBm 5G: 25 dBm <i>*Maximum power varies by country, frequency band and MCS rate</i> |
| 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; <i>* Receiver sensitivity varies by frequency band, channel width and MCS rate</i> |

| | |
|--|--|
| 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

GWN7615 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 | <p>IEEE 802.11ac: 6.5 Mbps to 1300Mbps</p> <p>IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps</p> <p>IEEE 802.11n: 6.5 Mbps to 450 Mbps</p> <p>IEEE 802.11b: 1, 2, 5.5, 11Mbps</p> <p>IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps</p> <p><i>*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</i></p> |
| Frequency Bands | <p>2.4 GHz Radio: 2412 – 2484 MHz</p> <p>5 GHz Radio: 5180-5825 MHz</p> |
| Channel Bandwidth | <p>2.4G: 20 and 40MHz</p> <p>5G: 20, 40, and 80MHz</p> |
| 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 | <p>3×3:3 2.4G(MIMO)</p> <p>3×3:3 5G(MU-MIMO)</p> |
| Coverage Range | <p>Up to175 meters</p> <p><i>*coverage range can vary based on environment</i></p> |
| Maximum TX Power | <p>2.4G: 26 dBm</p> <p>5G: 24 dBm</p> |
| Receiver Sensitivity | <p>2.4G</p> <p>802.11b: -96dBm@1Mbps, -88dBm@11Mbps; 802.11g: -93dBm @6Mbps, -75dBm@54Mbps; 802.11n 20MHz: -73dBm @MCS7; 802.11n 40MHz:-70dBm @MCS7</p> <p>5G</p> <p>802.11a: -92dBm @6Mbps, -74dBm @54Mbps; 802.11ac 20MHz: -67dBm@MCS8; 802.11ac: HT40:-63dBm @MCS9; 802.11ac 80MHz: -59dBm @MCS9</p> |
| 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 | <p>≤ 50 APs: Light-weight Master in AP</p> <p>≤ 3000 APs: On-Premises controller</p> <p>≤ +∞ APs: Cloud management</p> |
| Power and Green Energy Efficiency | <p>POE 802.3af/ 802.3at;</p> <p>Max Consumption: 12.5W</p> |
| Environmental | <p>Operation: 0°C to 40°C</p> <p>Storage: -10°C to 60°C</p> <p>Humidity: 10% to 90% Non-condensing</p> |
| Physical | <p>Unit Dimension: 205.4 x 205.4 x 45.9mm; Unit Weight: 500g</p> <p>Entire Package Dimension: 258 x 247 x 86mm; Entire Package Weight: 867.3g</p> |
| Package Content | GWN7615 802.11ac Wireless AP, Mounting Kits, Quick Start Guide |
| Compliance | FCC, CE, RCM, IC |

GWN7615 Technical Specifications

GWN7610 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 | <p>IEEE 802.11ac: 6.5 Mbps to 1300 Mbps</p> <p>IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps</p> <p>IEEE 802.11n: 6.5 Mbps to 450 Mbps</p> <p>IEEE 802.11b: 1, 2, 5.5, 11 Mbps</p> <p>IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps</p> <p><i>*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</i></p> |
| Frequency Bands | <p>2.4GHz radio: 2.400 – 2.4835 GHz</p> <p>5GHz radio: 5.150 – 5.250 GHz, 5.725 – 5.850 GHz (FCC, IC, RCM)</p> |
| Channel Bandwidth | <p>2.4G: 20 and 40 MHz</p> <p>5G: 20,40 and 80 MHz</p> |

| | |
|--|---|
| 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) <i>*coverage range can vary based on environment</i> |
| Maximum TX Power | 5G: 26dBm (FCC) / 20dBm (CE) 2.4G: 26dBm (FCC) / 17dBm (CE) <i>*Maximum power varies by country, frequency band and MCS rate</i> |
| 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 <i>* Receiver sensitivity varies by frequency band, channel width and MCS rate</i> |
| 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

GWN7605 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 <i>*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</i> |
| 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 <i>*coverage range can vary based on environment</i> |
| Maximum TX Power | 5G: 24dBm 2.4G: 22dBm <i>*Maximum power varies by country, frequency band and MCS rate</i> |
| 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 <i>* Receiver sensitivity varies by frequency band, channel width and MCS rate</i> |
| SSIDs | 16 SSIDs total, 8 per radio (2.4GHz and 5GHz) <i>*GWN7605 when deployed as Master can only be added to 8 SSIDs.</i> |
| 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

GWN7605LR 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 <i>*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</i> |
| 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 <i>*coverage range can vary based on environment</i> |
| Maximum TX Power | 2.4G: 24 dBm 5G: 22dBm |

| | |
|--|---|
| Receiver Sensitivity | <p>2.4G</p> <p>802.11b: -96dBm@1Mbps, -88dBm@11Mbps; 802.11g: -93dBm @6Mbps, -75dBm@54Mbps; 802.11n 20MHz: -73dBm @MCS7; 802.11n 40MHz:-70dBm @MCS7</p> <p>5G</p> <p>802.11a: -92dBm @6Mbps, -74dBm @54Mbps; 802.11ac 20MHz: -67dBm@MCS8; 802.11ac: HT40:-63dBm @MCS9; 802.11ac 80MHz: -59dBm @MCS9</p> |
| SSIDs | <p>16 SSIDs total, 8 per radio (2.4GHz and 5GHz)</p> <p><i>*GWN7605LR when deployed as Master can only be added to 8 SSIDs.</i></p> |
| 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 | <p>Embedded controller can manage up to 50 local GWN APs</p> <p>GWN.Cloud offers a free cloud management platform for almost unlimited GWN Aps</p> <p>GWN Manager offers premise-based software controller for up to 3,000 GWN APs</p> |
| Power and Green Energy Efficiency | <p>POE 802.3af/ 802.3at;</p> <p>Maximum Power Consumption: 10.16W</p> |
| Environmental | <p>Operation: -30°C to 60°C</p> <p>Storage: -30°C to 70°C</p> <p>Humidity: 10% to 90% Non-condensing</p> |
| Physical | <p>Physical Unit Dimension: 358.3mm(L)*115mm(W)*45.3mm(H); Unit Weight: 500g</p> <p>Entire Package Dimension: 258 × 247× 86mm; Entire Package Weight:655.3g</p> |
| 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

GWN7600 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 | <p>IEEE 802.11ac: 6.5 Mbps to 877 Mbps</p> <p>IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps</p> <p>IEEE 802.11n: 6.5 Mbps to 300 Mbps; 400 Mbps with 256-QAM on 2.4GHz</p> <p>IEEE 802.11b: 1, 2, 5.5, 11 Mbps</p> <p>IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps</p> <p><i>*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.</i></p> |
| Frequency Bands | <p>2.4GHz radio : 2.400 – 2.4835 GHz</p> <p>5GHz radio: 5.150 – 5.250 GHz, 5.725 – 5.850 GHz</p> |
| Channel Bandwidth | <p>2.4G: 20 and 40 MHz</p> <p>5G: 20,40 and 80 MHz</p> |
| 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 | <p>Up to 541ft. (165 meters) for GWN7600.</p> <p><i>*Coverage range can vary based on environment</i></p> |
| Maximum TX Power | <p>5G: 22dBm</p> <p>2.4G: 22dBm</p> <p><i>*Maximum power varies by country, frequency band and MCS rate.</i></p> |
| Receiver Sensitivity | <p>2.4G</p> <p>802.11b:-99dBm @1Mbps,-91dBm @11Mbps;802.11g:-93dBm @6Mbps,-75dBm @54Mbps; 80.11n 20MHz:-72dBm @MCS7;802.11n 40MHz:-69dBm @MCS7</p> <p>5G</p> <p>802.11a:-91dBm @6Mbps,-74dBm @54Mbps;802.11ac 20MHz:-67dBm @MCS8;802.11ac HT40:-63dBm @MCS9;802.11ac 80MHz:-60dBm @MCS9</p> |
| 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

GWN7600LR 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

GWN7630LR 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 | 4x4:4 2.4G (MIMO), 4x4:4 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 | 250+ |
| 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 |

GWN7630LR Technical Specifications

GWN7602 Technical Specifications

| | |
|-----------------------------|--|
| 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 <i>*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</i> |
| Frequency Bands | 2.4GHz Radio: 2412 - 2484 MHz 5GHz Radio: 5150-5250 MHz, 5250-5350 MHz, 5470-5725 MHz, 5725-5850 MHz <i>*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.</i> |
| 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 <i>*coverage range can vary based on environment</i> |
| Maximum TX Power | 5G: 21dBm 2.4G: 21dBm <i>*Maximum power varies by country, frequency band and MCS rate</i> |
| 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°C to 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

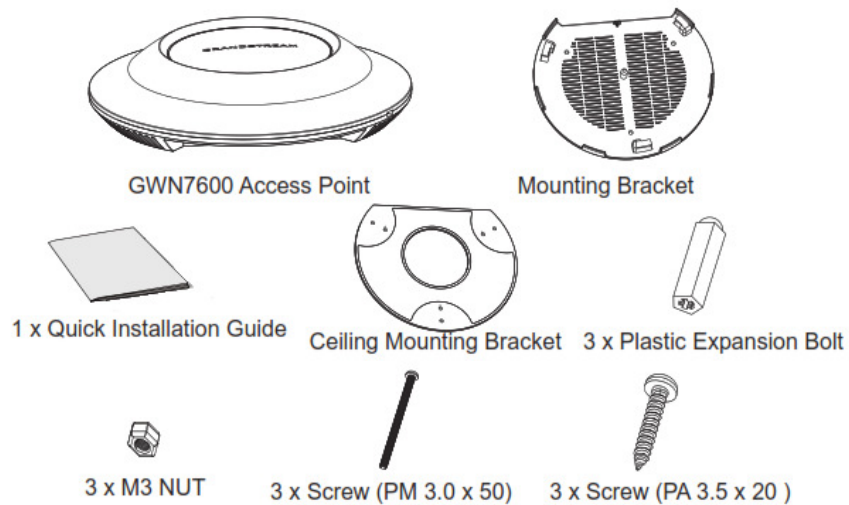
Before deploying and configuring the GWN76XX, the device needs to be properly powered up and connected to the network. This section describes detailed information on installation, connection, and warranty policy of the GWN76XX.

Equipment Packaging

| | |
|--|------------|
| Main Case (GWN7625, GWN7664,GWN7660, GWN7630, GWN7610, GWN7615, GWN7605, GWN7600,GWN7662) | 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

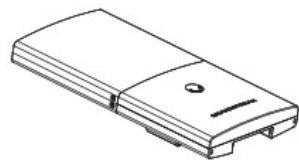


GWN76xx Equipment Packaging

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) |

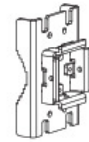
GWN7600LR Equipment Packaging



1 x GWN7600LR Access Point



1 x Cover Bracket



1 x Base Bracket



4 x Screw (PM8 x 115)



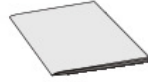
2 x Assembled Screw



4 x Screws and Anchors



4 x Locknut



1 x Quick Installation Guide

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



GWN7603LR
GWN7605LR
GWN7660LR



Antennas



1x Base Bracket



4x Screws
(PM 3.0 x 7)



1x Quick Installation Guide



2x Metal Straps



4x Expansion Screws

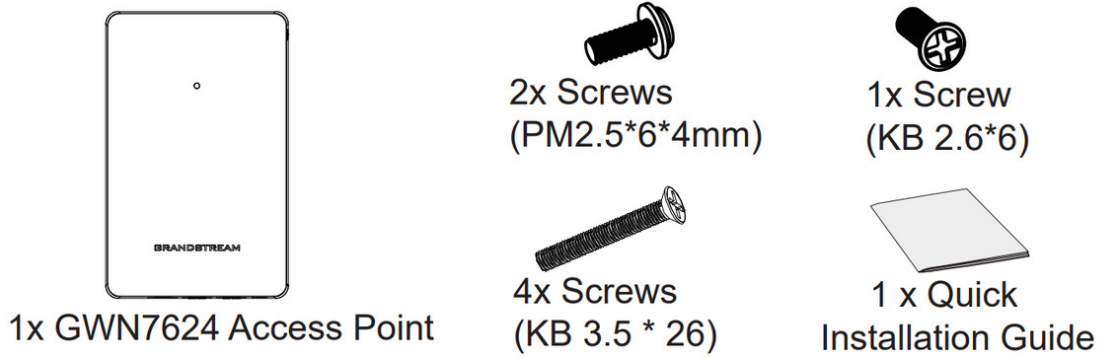
GWN7630LR/GWN7605LR/GWN7660LR /GWN7664LR Equipment Package

Below is the equipment packaging for GWN7624 and GWN7661 models.

| | |
|------------------|---------|
| 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/GWN7661 Equipment Packaging



GWN7624/GWN7661 Equipment Package

The equipment packaging for GWN7602 model.

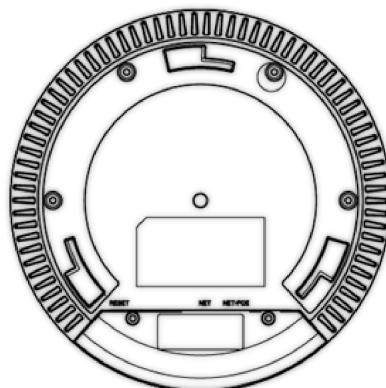
| | |
|--------------------------|---------|
| Main Case | Yes (1) |
| PA3.5*20 Screws | Yes (2) |
| Anchors Screws | Yes (2) |
| Quick Installation Guide | Yes (1) |

GWN7602 Equipment Packaging

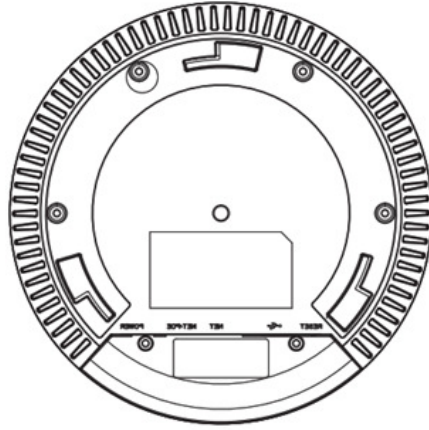


GWN7602 Equipment Package

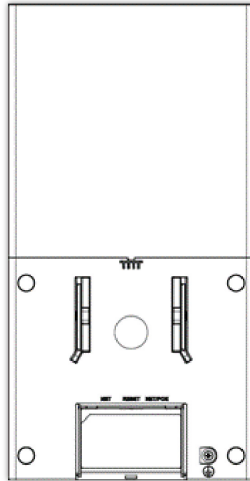
GWN76XX Access Point Ports



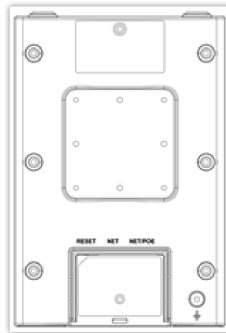
GWN76xx Ports



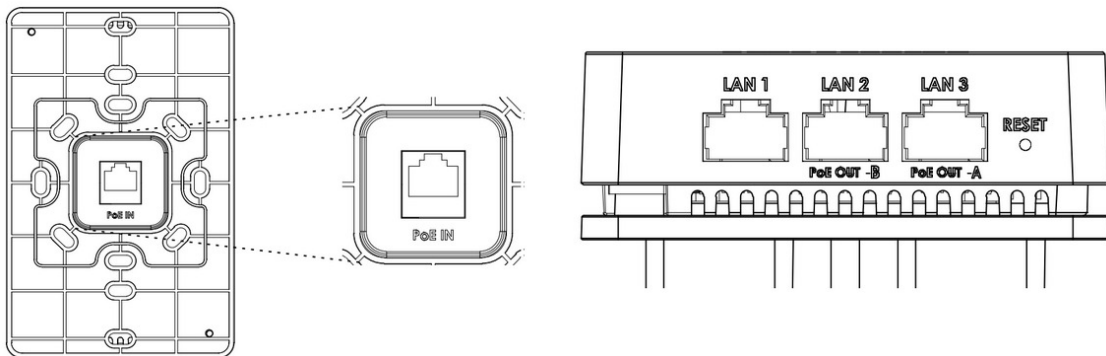
GWN7610/GWN7600 Ports



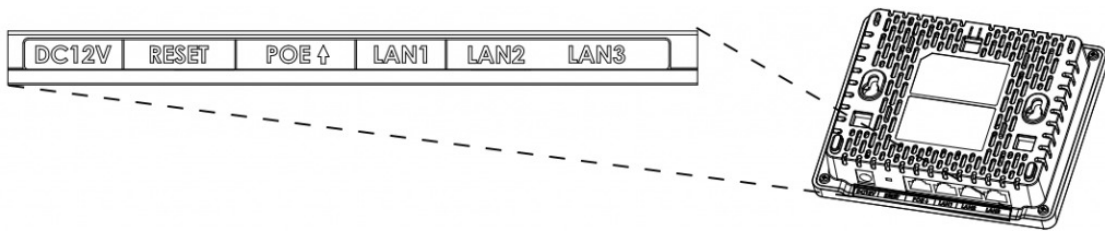
GWN7600LR Ports




GWN7630LR
/GWN7605LR/GWN7660LR/GWN7664LR
Ports



GWN7624/GWN7661 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 and GWN7661 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.

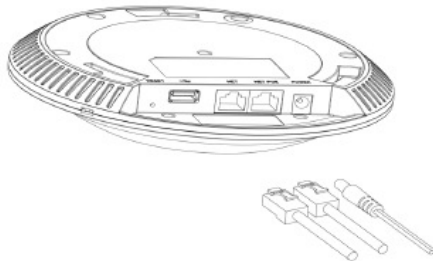
Notes

GWN7624/GWN7625/GWN7664/GWN7660/GWN7662/GWN7661/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.



Connecting 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.

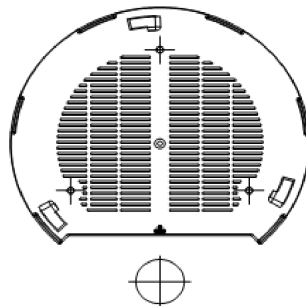
Wall/Ceiling Mount Installation GWN76XX

GWN7625/GWN7664/GWN7660/GWN7630/GWN7610/GWN7615/GWN7600/GWN7605/GWN7662 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

Step 1:

Position the mounting bracket at the desired location on the wall with the arrow pointing up.



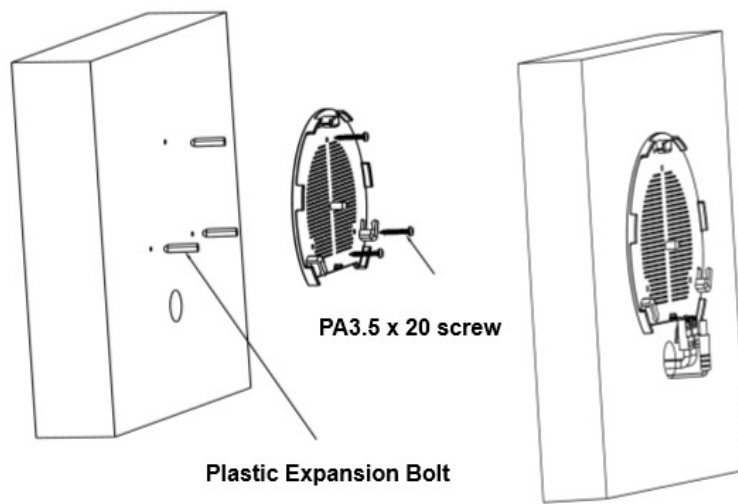
Wall Mount – Steps 1 & 2

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.



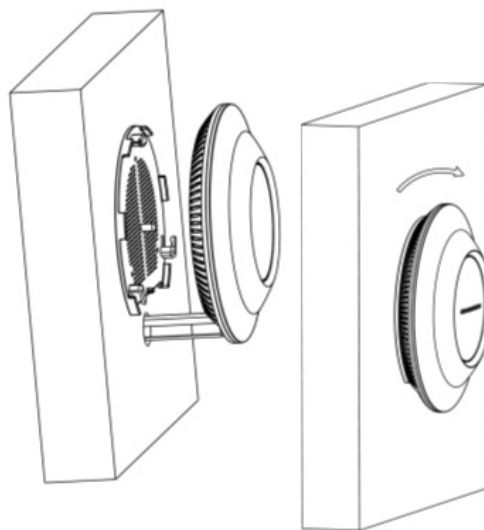
Wall Mount – Steps 3 & 4

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/GWN7662

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

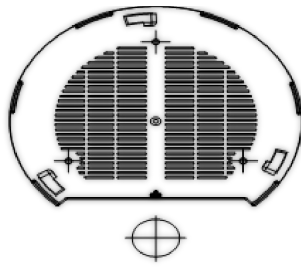
Step 6:

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

Ceiling Mount

Step 1:

Remove the ceiling tile.



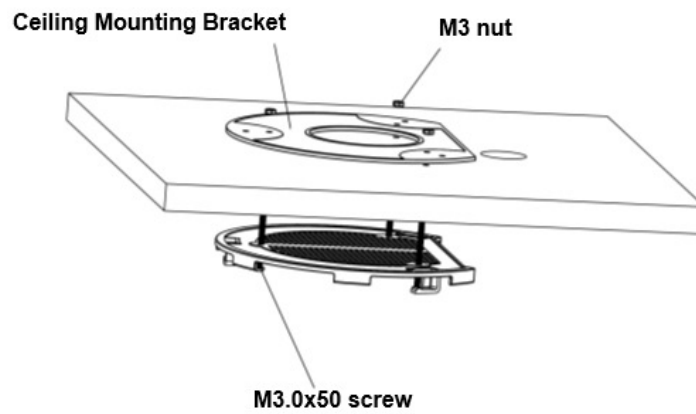
Ceiling Mount – Steps 1 & 2

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:

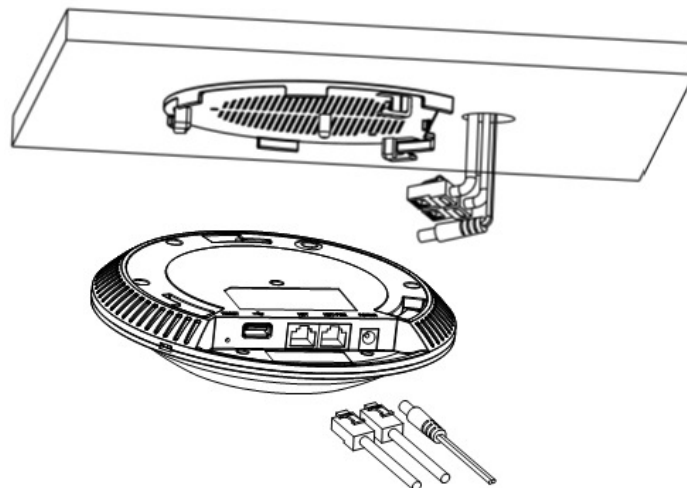
Insert the screws through the mounting bracket.



Ceiling Mount – Step 3

Step 4:

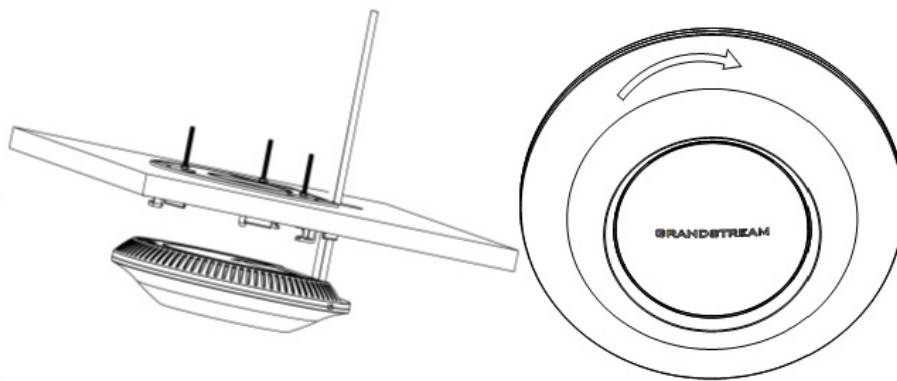
Connect the power cable and the Ethernet cable (RJ45) to the correct ports of your GWN76XX.



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.

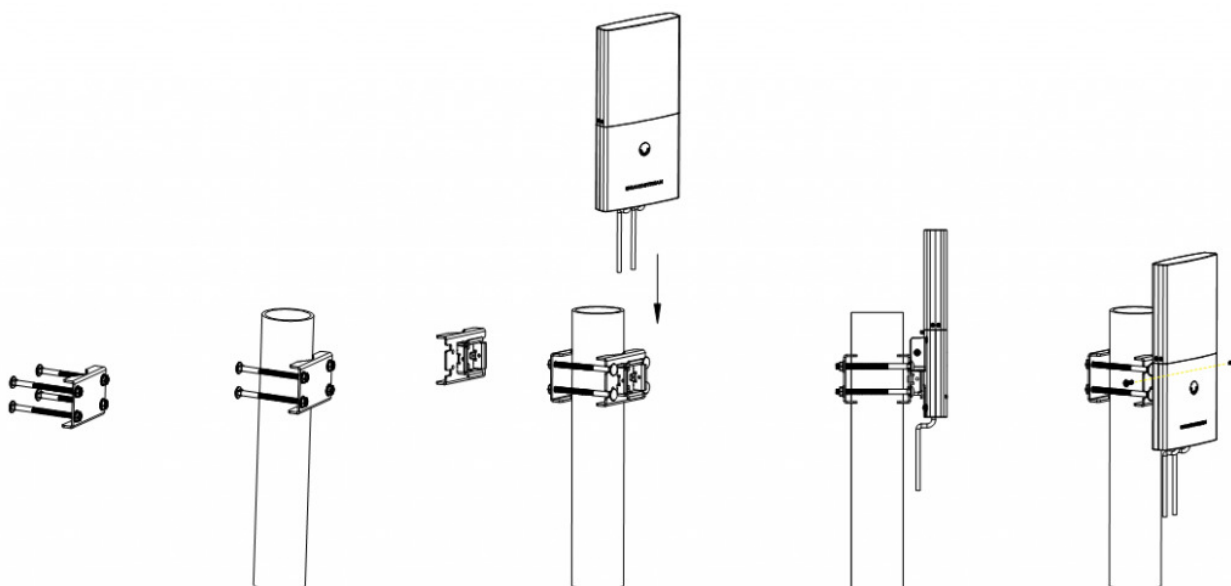
Note

Ceiling mounting is recommended for optimal coverage performance.

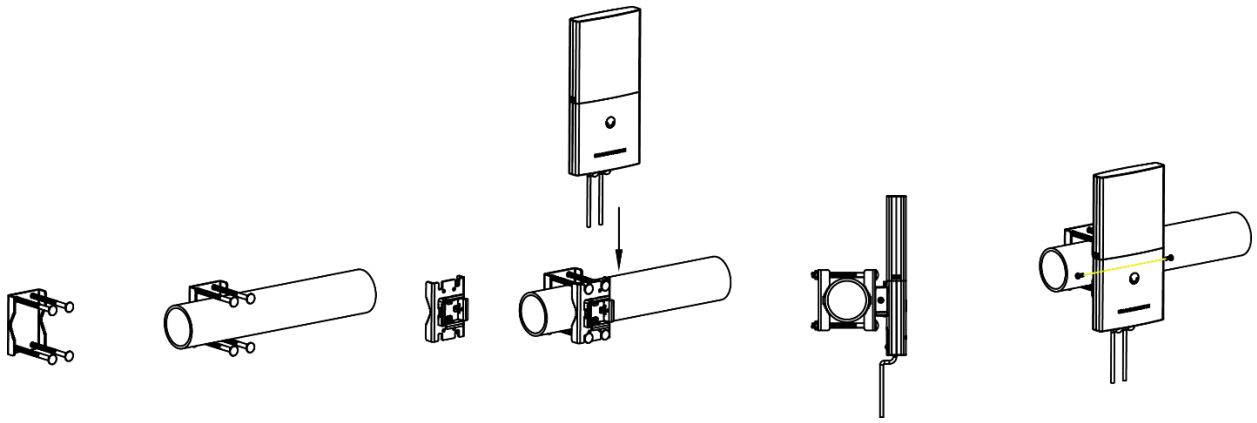
Mounting Instructions for GWN7600LR

Please refer to the following steps to mount 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.



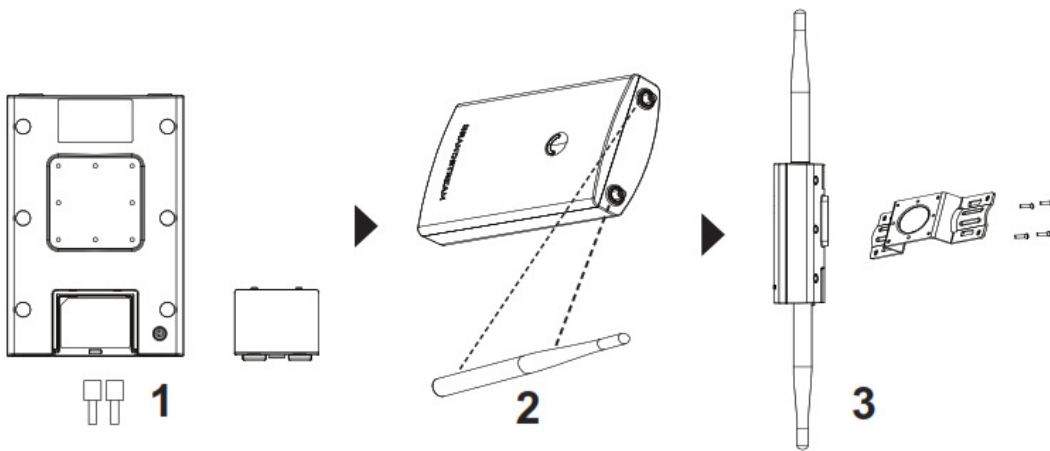
GWN7600LR Vertical Mounting



GWN7600LR Horizontal Mounting

Mounting Instructions for GWN7630LR/GWN7605LR/GWN7660LR/GWN7664LR

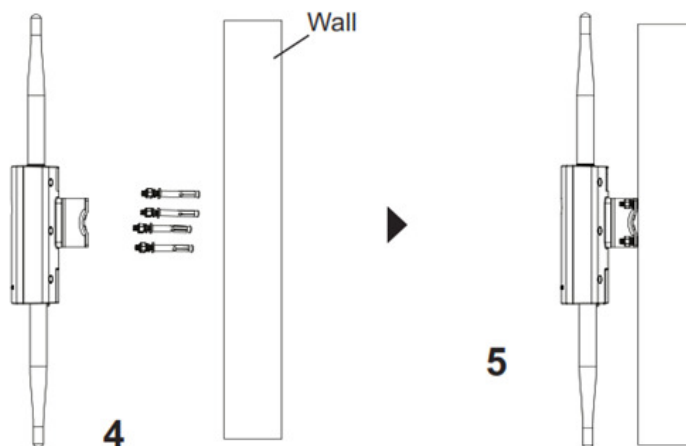
GWN76xxLR can be mounted on the wall or on a metal bar. Please refer to the following steps for the appropriate installation.



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

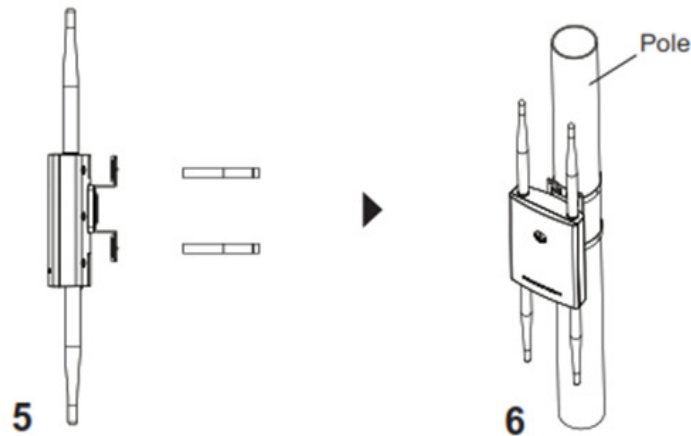


GWN7630LR/GWN7605LR/GWN7660LR Wall Mount

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

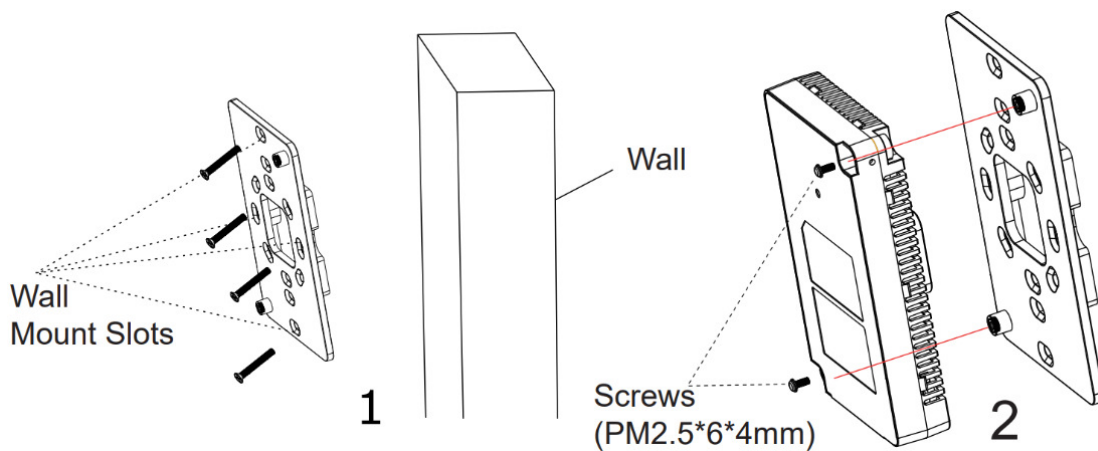
1. Open the metal straps by turning the locking mechanism counter-clockwise. You can loosen it by hand or use a flathead screwdriver.
2. Straighten out the end of the metal straps and slide it through the back of the base bracket.
3. Wrap the metal strap around the pole and use a flathead screwdriver to tighten the locking mechanism by turning it clockwise.

Mounting Instructions for GWN7624/GWN7661

GWN7624/GWN7661 can be mounted on the wall, Please refer to the following steps for the appropriate installation.

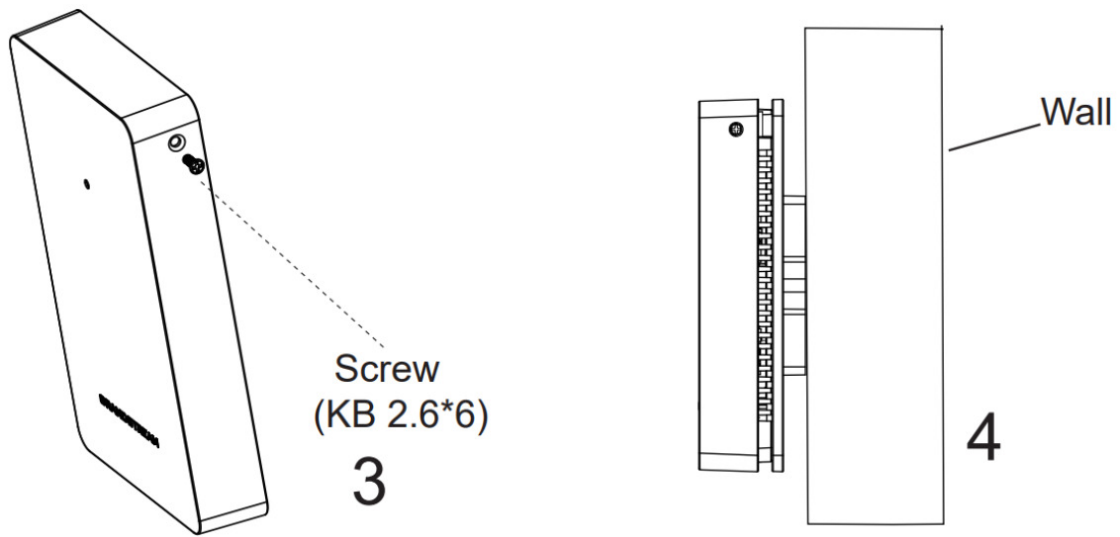
Wall Mount (GWN7624/GWN7661)

1. Use a measuring tape to measure the distance between the four wall mount slots on the back of the AP 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 AP main body on the wall mount after mounting the wall mount on the wall.



Wall Mount

4. Attach the front cover with the AP body and then the grey screw on the side.



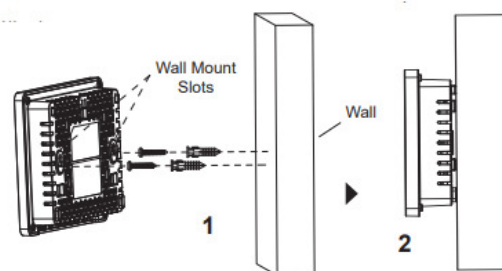
GWN7624/GWN7661 Wall Installation

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 stickers of the unit, which is located on the back 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.

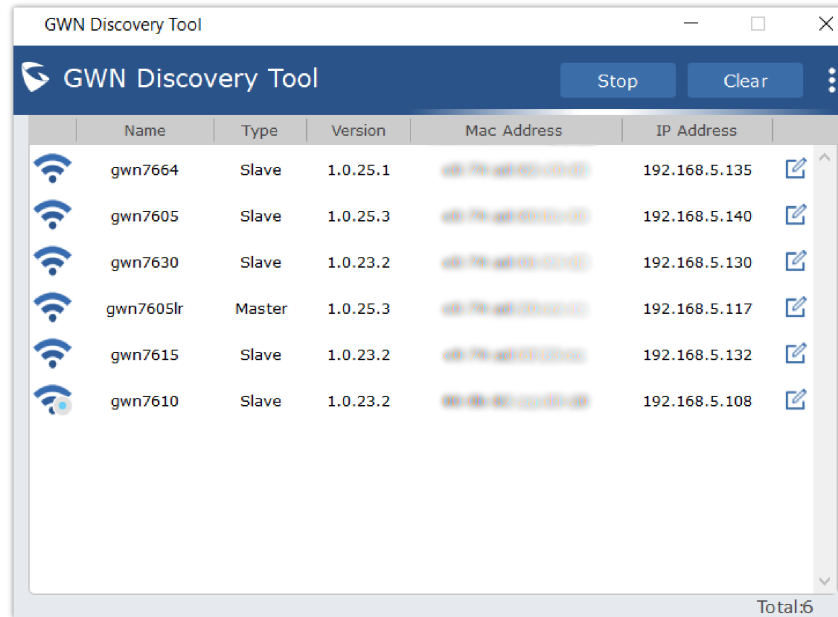


Discover the GWN76XX using its MAC Address

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**.

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



The screenshot shows a window titled "GWN Discovery Tool" with a dark blue header. Below the header is a table with columns: Name, Type, Version, Mac Address, and IP Address. There are six rows of data, each with a Wi-Fi icon to the left of the Name column. The Mac Address column contains blurred text. At the bottom right of the table area, it says "Total:6".

| Name | Type | Version | Mac Address | IP Address |
|-----------|--------|----------|-------------|---------------|
| gwn7664 | Slave | 1.0.25.1 | [blurred] | 192.168.5.135 |
| gwn7605 | Slave | 1.0.25.3 | [blurred] | 192.168.5.140 |
| gwn7630 | Slave | 1.0.23.2 | [blurred] | 192.168.5.130 |
| gwn7605lr | Master | 1.0.25.3 | [blurred] | 192.168.5.117 |
| gwn7615 | Slave | 1.0.23.2 | [blurred] | 192.168.5.132 |
| gwn7610 | Slave | 1.0.23.2 | [blurred] | 192.168.5.108 |

GWN Discovery Tool

Use the Web GUI

Users can access 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.



GWN76XX Web GUI Login Page

To access the Web GUI:

- Make sure to use a computer connected to the same local Network as the GWN76XX.
- Ensure the device is properly powered up.
- 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: **[http\(s\)://IP_Address](https://IP_Address)**
- 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

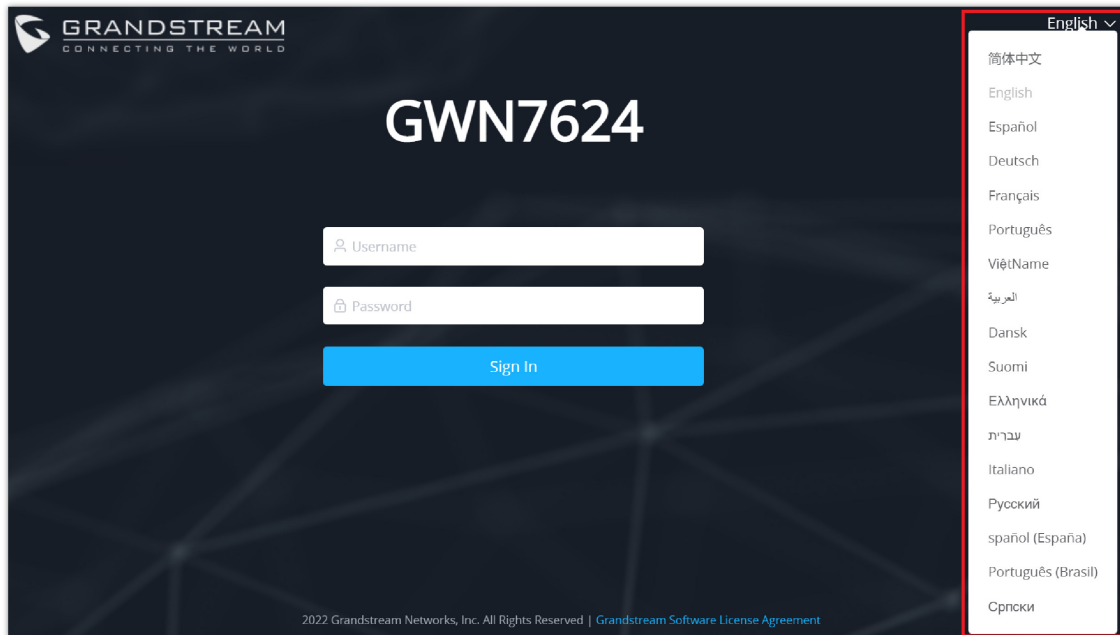
GWN AP's web UI access will be locked for 15 mins after 5 login failures

Note:

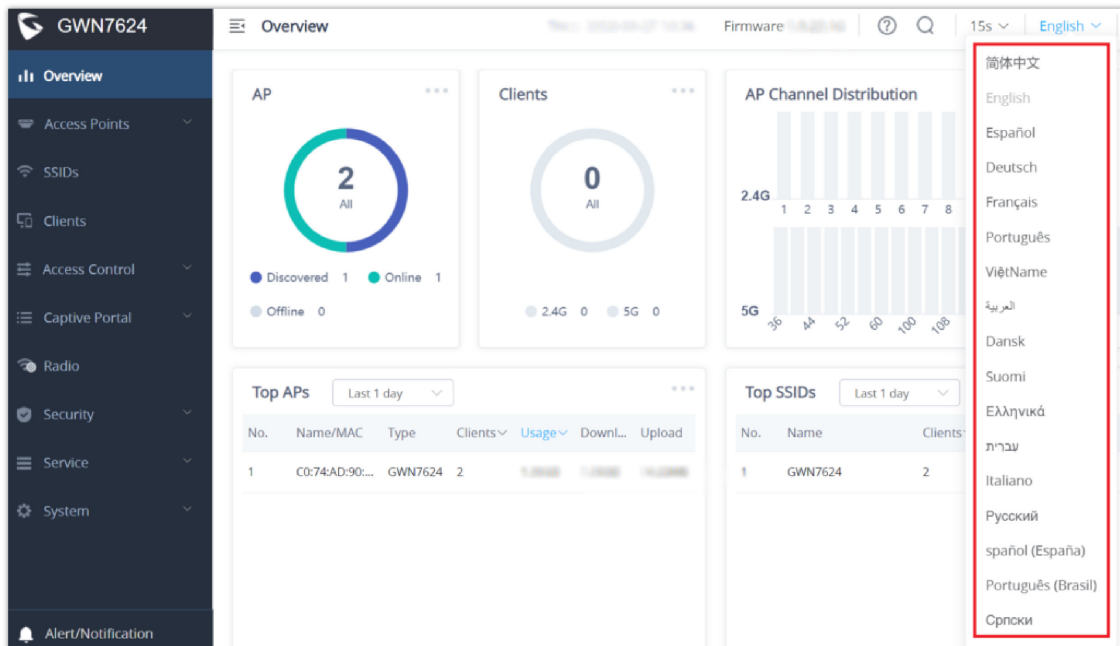
GWN7602 doesn't support embedded Web server, it can only be managed through another GWN access point as a slave, GWN Cloud or GWN Manager.

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.



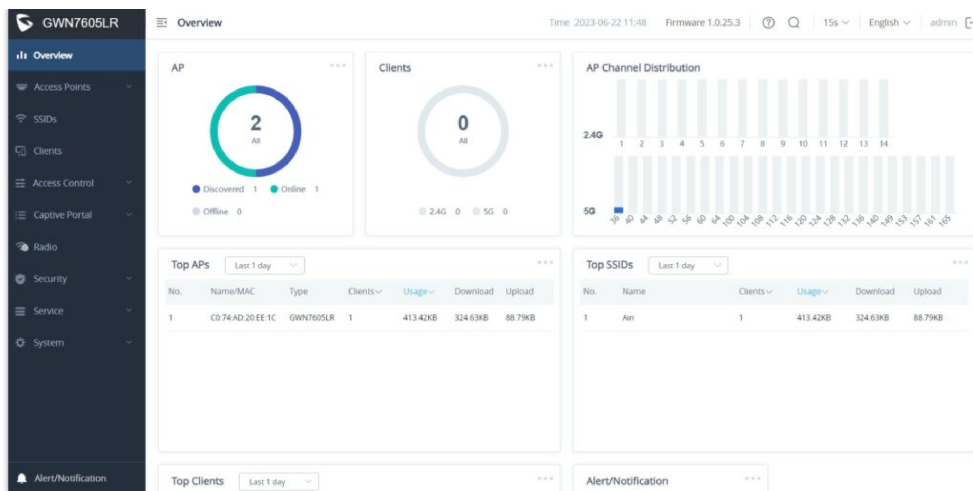
GWN76XX Web GUI Langage (Login page)



GWN76XX Web GUI Language (Web Interface)

Overview Page

Overview is the first page shown after successful login to the GWN76XX's Web Interface. This 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 (GWN7605LR 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 Points that are Discovered, Paired (Online) and Offline. Users may click on to go to the Access Points page for basic and advanced configuration options for the APs. |
| Clients | Shows the total number of connected clients, and a count of connected clients to each Channel. Users may click on to go to the 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 sort the list by number of clients connected to each AP or data usage combining upload and download. Users may click on to go to the Access Points page for basic and advanced configuration options for the APs. |
| Top SSID | Shows the Top SSIDs list, users may sort the list by number of clients connected to each SSID or data usage combining upload and download. Users may click on to go to the SSID page for more options. |
| Top Clients | Shows the Top Clients list, users may sort the list of clients by their upload or download. Users may click on to go to the Clients page for more options. |
| Alert/Notification | Shows 3 types of Alerts/Notifications: Critical, Major and Normal. Users can click to pop up the list of Alert and Notification. |

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 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.

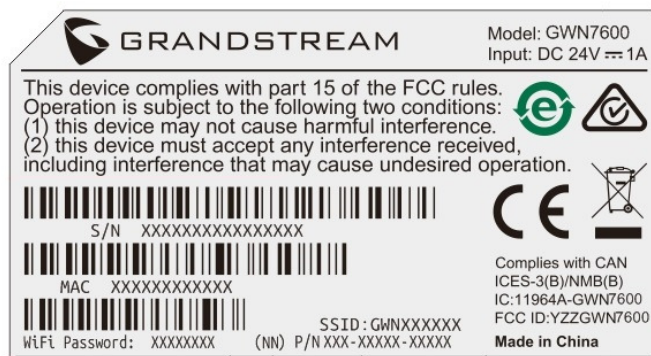
This section will describe how to use and configure the GWN76XX in standalone mode.

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 need more area zones coverage with the same controller.




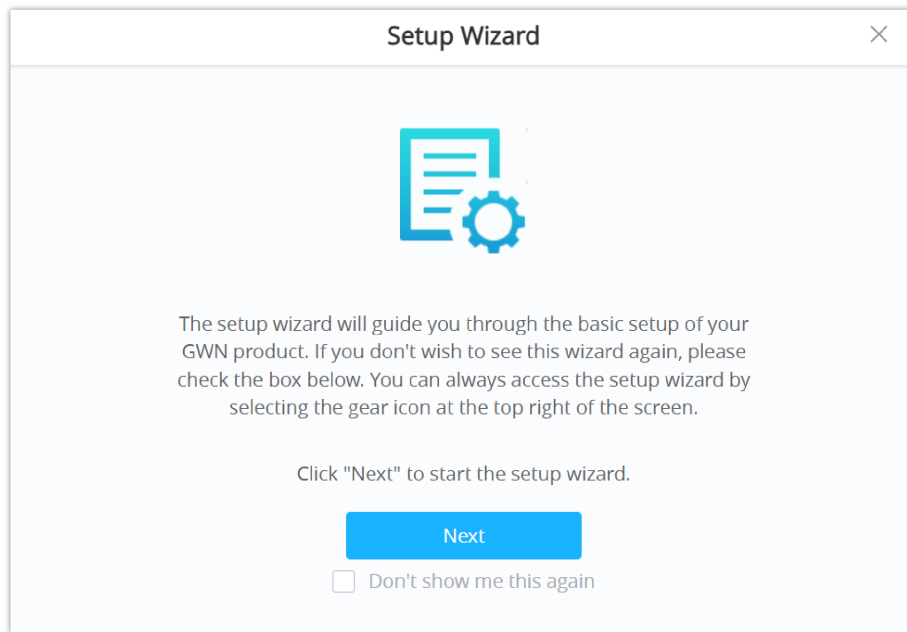
Login Page

Warning

Set unit as Master option will forbid the GWN76XX Access Point from being paired by other Master GWN76XX and can only act as a Master Access point controller. Users will need to perform a factory reset to the GWN76XX, or unpair it from the initial GWN76XX to make it open to Master Access Point mode again.

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

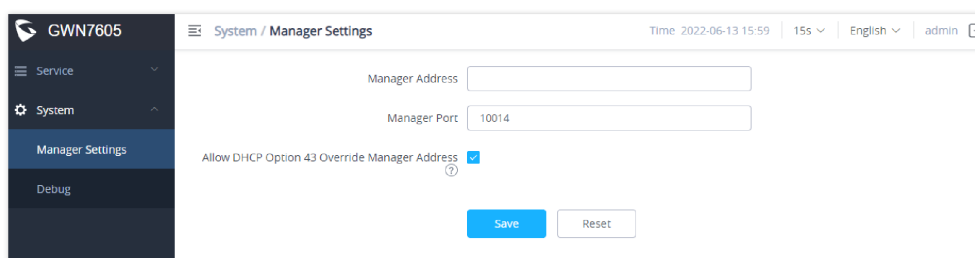
To pair and manage access points located on remote networks, the admin needs to configure the IP address of master AP on DHCP option 43 which will be send to the slave access point during booting stage and allow the save/master connection to be established remotely. GWN76xx accepts option 224 encapsulated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

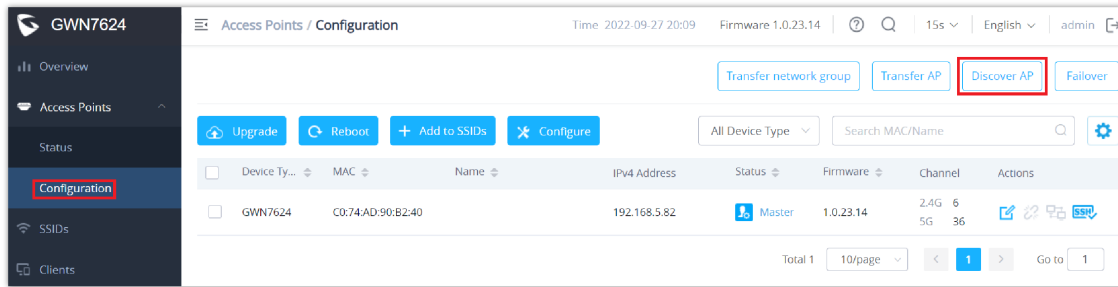


Option 43 Override

After that, the slave AP will be listed on the master AP discovered devices and ready for pairing 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

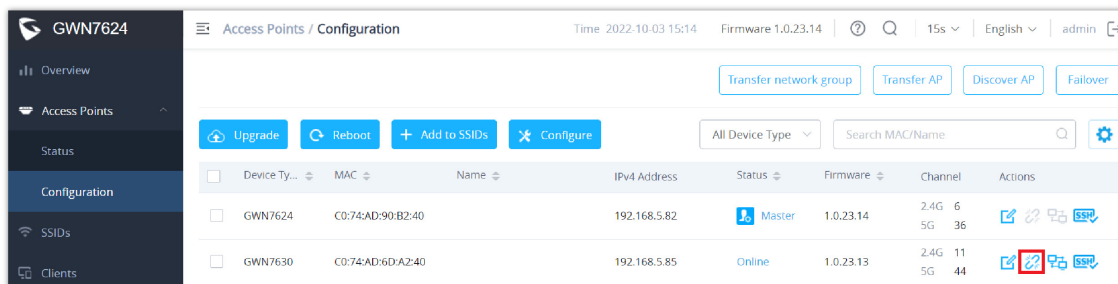
2. Click on **Discover AP** to discover access points within GWN76xx Network, the following page will appear.



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

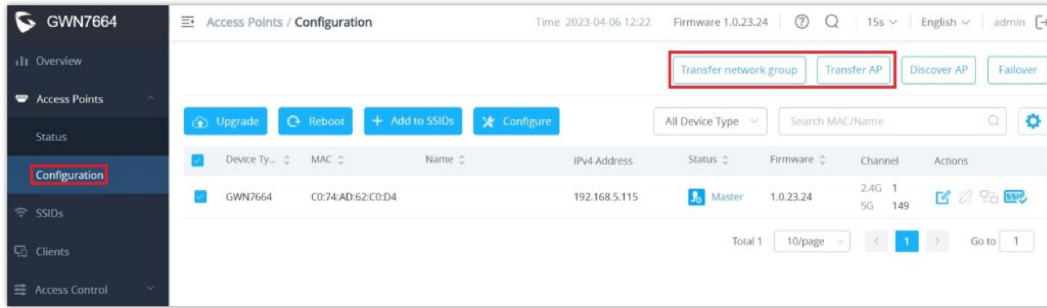
AP Location

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

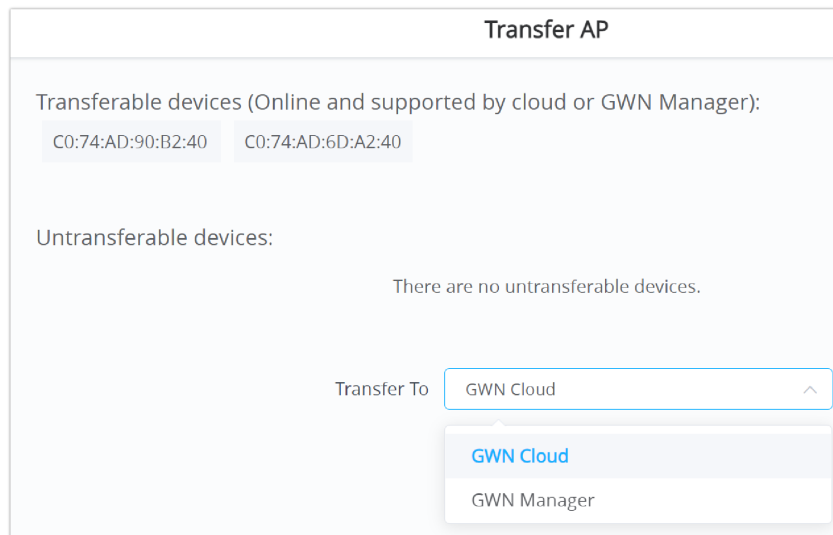
Users can easily transfer the AP from the local master to the **GWN Cloud** or **GWN Manager** account by clicking on **Transfer AP**. When you already have Network/Wi-Fi configurations on your GWN account, using this feature will let you choose existing Network/SSID to adopt your local AP.

Navigate to **AP Web UI** → **Access Points** → **Configuration** page, please refer to the figure below:



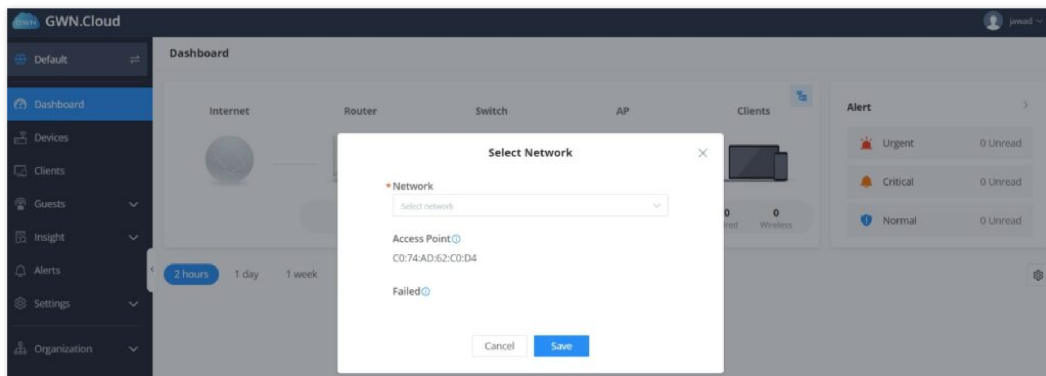
Access points configuration page

Then select where to transfer the select AP, either GWN Cloud or GWN Manager.



Transfer AP

After this step, you will be redirected to GWN Cloud/GWN Manager page, select the network and click on **“Save”** button to complete the transfer.

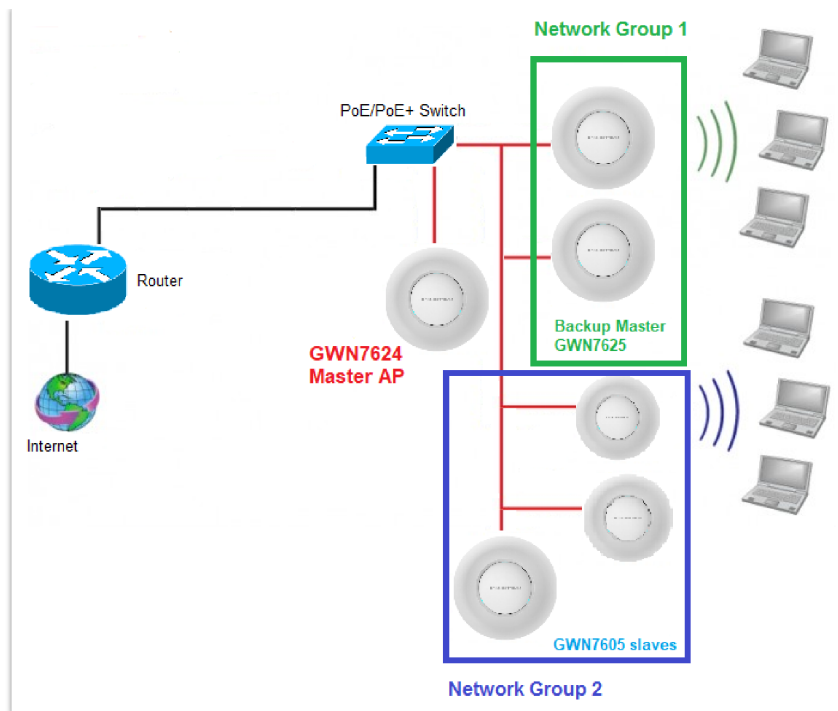


GWN Cloud – Select Network

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

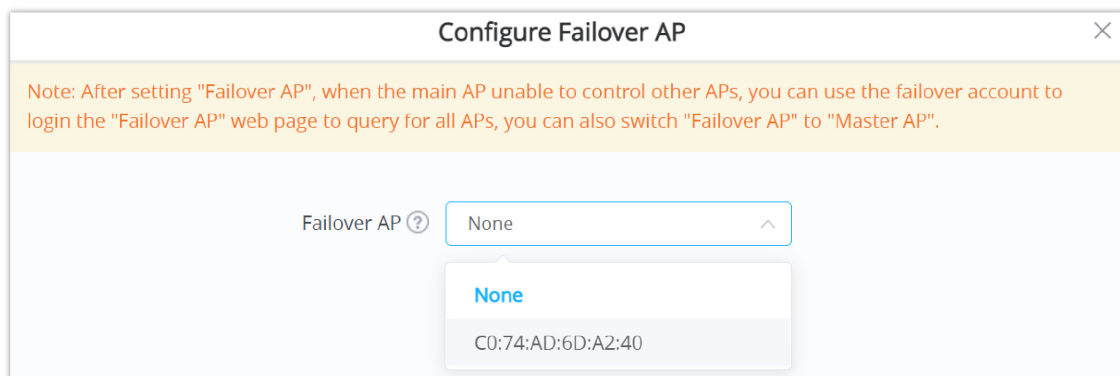
In a Master-Slave architecture, having a backup Master is critical for redundancy and failover function, thus, and in order to avoid a single point of failure in your wireless network, you can specify a slave AP as failover master. Whenever it detects the master is down, it will promote itself as failover 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

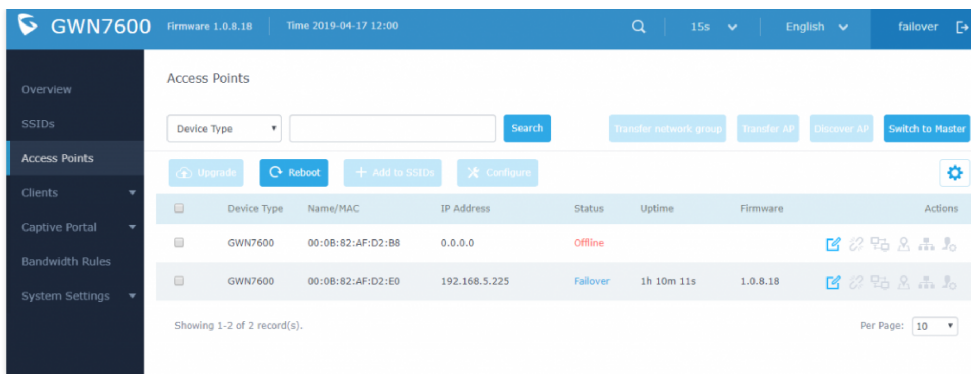
Failover Mode

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.

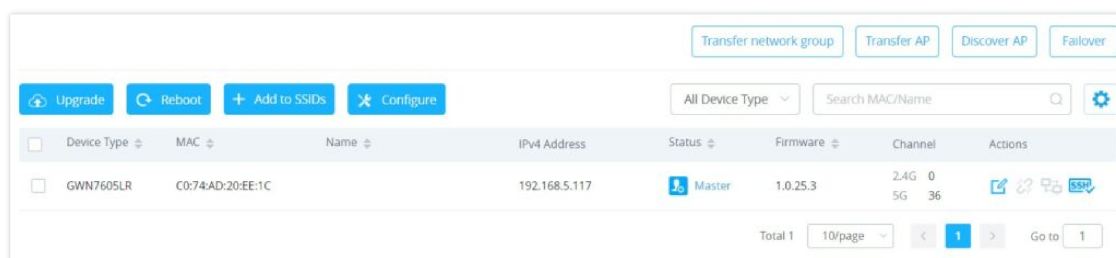
When Failover Slave is switched to Master, you will use the Prior Master AP credentials: username: admin, and the admin password.

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

Takeover Feature

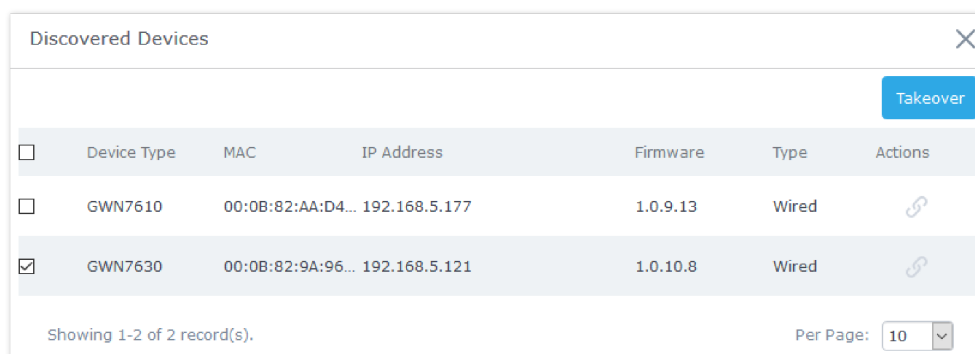
This feature is used to re-pair the slave APs whose master has gone offline with another master AP in the same subnet. Please follow the steps to takeover slave APs from other master:

Step 1. Login to the Web GUI of Master and click on “Discover APs” in the Access Points Page.



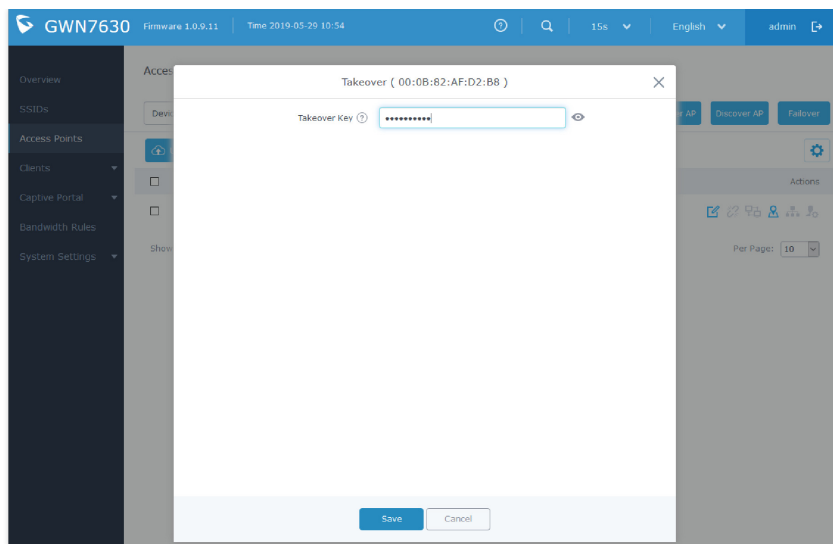
Takeover – Step 1

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

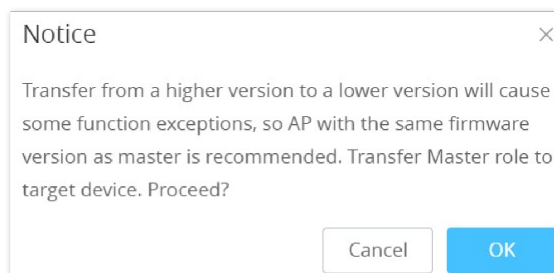
From the Master Access Point, the Administrator do have the capability to assign any Slave Access point to become the new Master to manage all the already paired Access points. Except for GWN7602.

Navigate to **Web UI** → **Access Points** → **Status**, refer to the figure below:

| Device Type | MAC | IPv4 Address | Status | Actions |
|-------------|-----------|--------------|--------|--------------------|
| GWN7605LR | C0:74:AD: | 192.168.5.86 | Master | [Switch to Master] |
| GWN7624 | C0:74:AD: | 192.168.5.94 | Online | [Switch to Master] |

Switch to Master

Click on 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.

| Device Type | MAC | Name | IPv4 Address | Status | Actions |
|-------------|-----------|------|--------------|--------|--------------------|
| GWN7605LR | C0:74:AD: | | 192.168.5.86 | Online | [Switch to Master] |
| GWN7624 | C0:74:AD: | | 192.168.5.94 | Master | [Switch to Master] |


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 act as a wireless bridge and connect the wired only clients to the wireless network. When an access point is configured in this way, it will share the Wi-Fi connection to the LAN ports directly. This is not to be confused with a mesh setup. The configured AP 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.

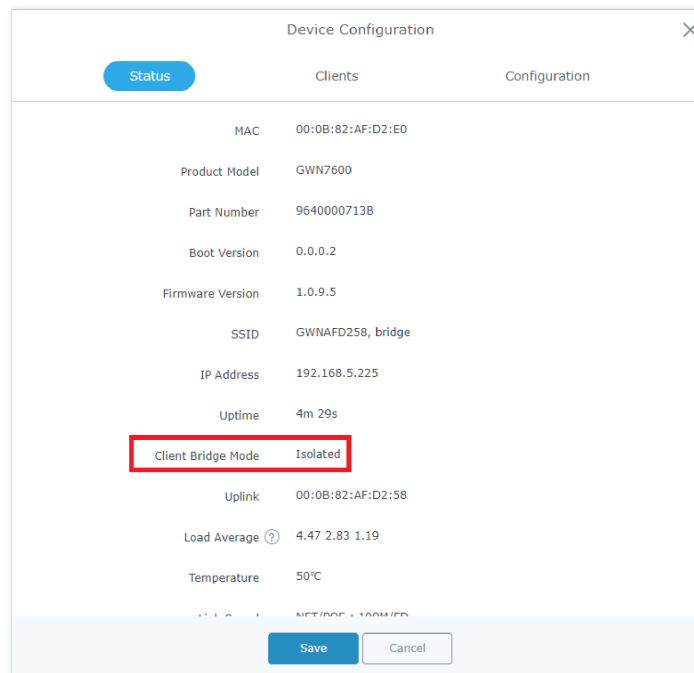


Client Bridge

| Client Bridge | | | | | | | |
|-------------------------------------|-------------|-----------------------------|---------------|------------------|---------|----------|---------|
| | | | | | | | |
| This AP is not a member of any SSID | | | | | | | |
| <input type="checkbox"/> | Device Type | Name/MAC | IP Address | Status | Uptime | Firmware | Actions |
| <input type="checkbox"/> | GWN7600 | 00:0B:82:AF:D2:58 | 192.168.5.100 | Master | 51m 53s | 1.0.9.5 | |
| <input type="checkbox"/> | GWN7600 | bridge 00:0B:82:AF:D2:E0 | 192.168.5.225 | Online Bridge | 2m 49s | 1.0.9.5 | |
| <input type="checkbox"/> | GWN7600 | 00:0B:82:AF:D2:B8 | 192.168.5.226 | Online | 43m 53s | 1.0.9.2 | |

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

GWN access points can be paired as a slave to a master, this master can be another GWN access point, GWN routers or GWN.Cloud/GWN Manager.

If the GWN access point is added to either GWN.Cloud or GWN Manager, the **Speed Test** feature will be available to users. Please for more details check [GWN Management Platforms – User Guide \(Configure a GWN Access Point\)](#).

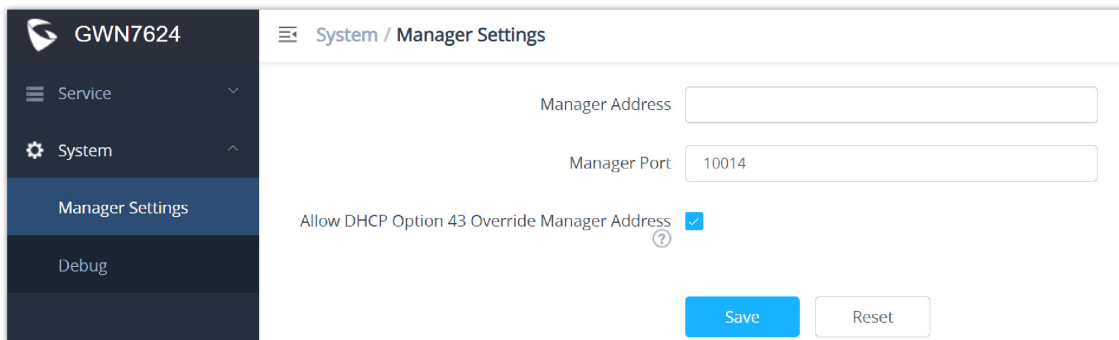
Slave Mode allows the users to access to specific service and system settings.



GWN7624 slave login page

Notes:

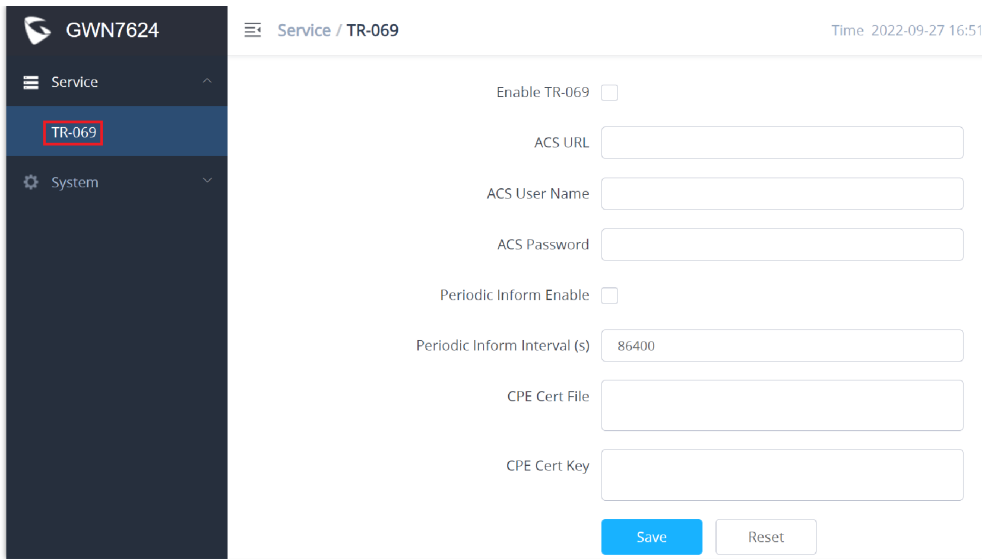
- If the AP is slave to a Master controller, the default username is admin, and the default password is the master AP's password.
- If the AP is paired to the GWN.Cloud the default username is admin, and the default password is the SSH Password (GWN.Cloud → System → Settings).



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.



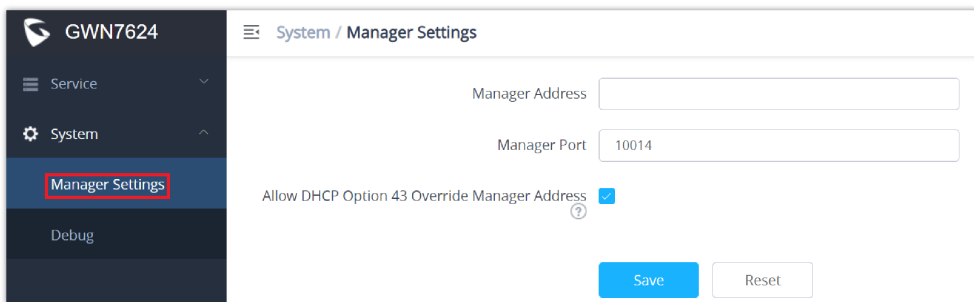
Slave AP Service Settings

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.

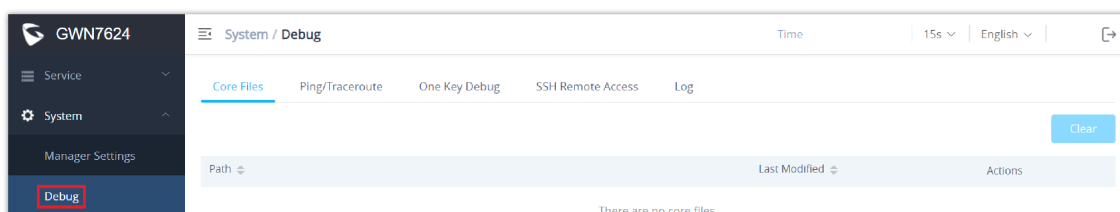


Slave AP manager settings

| | |
|--|---|
| 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 be used by the engineering team for debugging purposes.

Ping/Traceroute

Allows 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 users to retrieve the logs generated for troubleshooting purposes.

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 as 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 issues when they appear.

| Device T... | MAC | IPv4 Address | Status | Firmw... | Uptime | Channel | Channel Width | Wireless Power | Clients | Actions |
|-------------|-------------------|--------------|--------|-----------|------------|------------------|------------------|------------------------|---------|---------|
| GWN7624 | C0:74:AD:90:B2:40 | 192.168.5.82 | Master | 1.0.23.14 | 3h 44m 31s | 2.4G 6 5G 36 | 2.4G 20 5G 80 | 2.4G 230Bm 5G 240Bm | 0 | |
| GWN7630 | C0:74:AD:6D:A2:40 | 192.168.5.85 | Online | 1.0.23.13 | 1h 19m 58s | 2.4G 11 5G 44 | 2.4G 20 5G 80 | 2.4G 270Bm 5G 240Bm | 0 | |

Access Points – Status

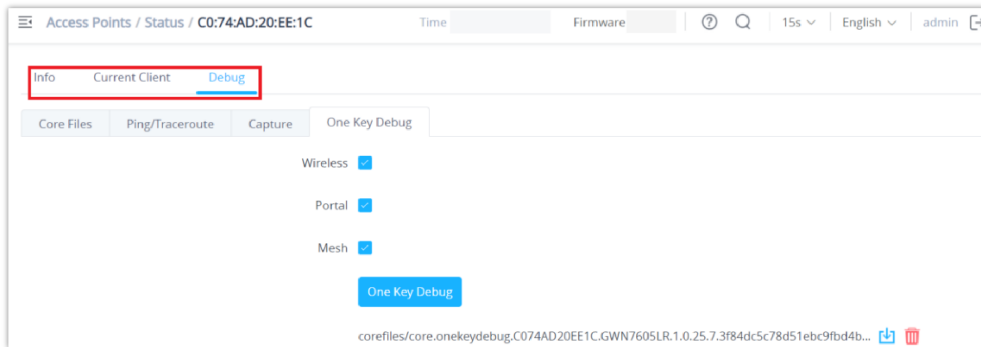
To get more detailed information about the status of a specific access point, users can click on the desired AP. Then a page similar to the following will show up:

| Info | Current Client | Debug |
|--------------------|---|-------|
| MAC | C0:74:AD:90:B2:40 | |
| Product Model | GWN7624 | |
| Part Number | 9640005210B | |
| Boot Version | 0.0.0.1 | |
| Firmware Version | 1.0.23.14 | |
| SSID | GWN90B240 (2.4G: c0:74:ad:90:b2:41 5G: c0:74:ad:90:b2:42) | |
| IPv4 Address | 192.168.5.82 | |
| IPv6 Address | | |
| Uptime | 3h 56m 59s | |
| Current Time | 2022-10-03 15:14:52 | |
| Client Bridge Mode | Disabled | |
| Load Average | 2.49 2.51 2.50 | |

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:

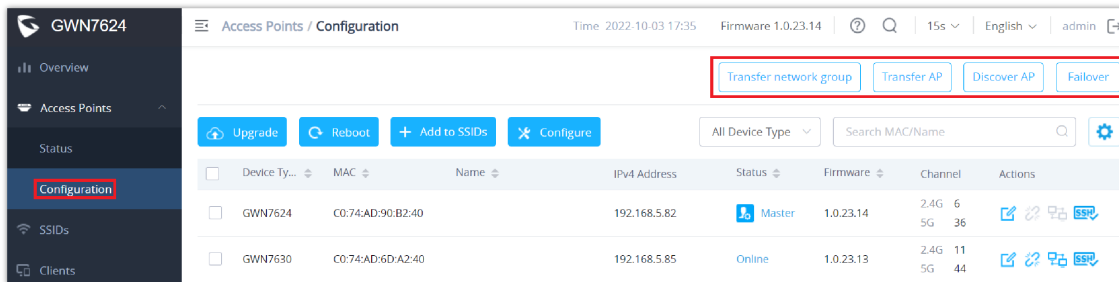
- **Core Files**, when a crash event happens on the unit, it will automatically generate a core dump file that can be used by the engineering team for debugging purposes.
- **Ping/Traceroute** tools, such as the **ping** utility, **traceroute** tool.
- **Capture** helps to capture traffic based on duration, interface, protocol, MAC address, IP address and ports, and there is also the option for custom rules.
- **One Key Debugging**, to capture Wireless, Portal or Mesh traffic and logs will be found in Core Files.



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

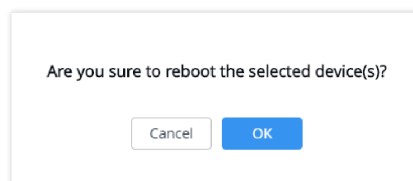
Upgrade

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

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

Reboot slave AP

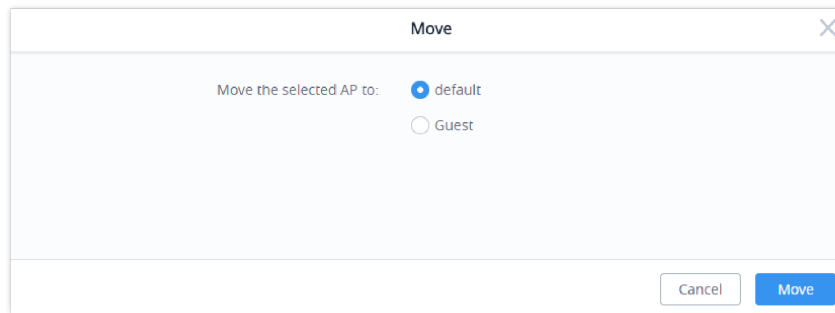
To reboot a slave AP, select it then click on **Reboot** button. the below confirmation message will be displayed:



Reboot Access Point

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.

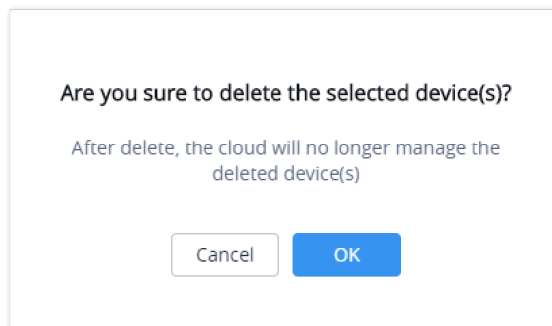


A dialog box titled "Move" with a close button (X) in the top right corner. The main content area contains the text "Move the selected AP to:" followed by two radio button options: "default" (which is selected) and "Guest". At the bottom right of the dialog, there are two buttons: "Cancel" and "Move".

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:

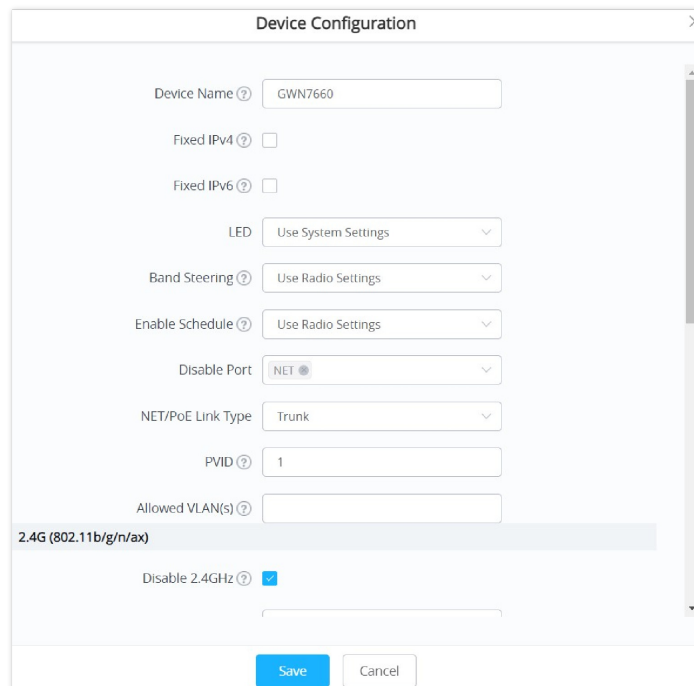


A confirmation dialog box with the title "Are you sure to delete the selected device(s)?" in bold. Below the title, it says "After delete, the cloud will no longer manage the deleted device(s)". At the bottom, there are two buttons: "Cancel" and "OK".

Delete Access Point

Configure Access Points

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



A "Device Configuration" dialog box with a close button (X) in the top right corner. It contains several configuration fields: "Device Name" (text input with "GWN7660"), "Fixed IPv4" (checkbox), "Fixed IPv6" (checkbox), "LED" (dropdown menu with "Use System Settings"), "Band Steering" (dropdown menu with "Use Radio Settings"), "Enable Schedule" (dropdown menu with "Use Radio Settings"), "Disable Port" (dropdown menu with "NET"), "NET/PoE Link Type" (dropdown menu with "Trunk"), "PVID" (text input with "1"), and "Allowed VLAN(s)" (text input). Below these fields, there is a section for "2.4G (802.11b/g/n/ax)" with a "Disable 2.4GHz" checkbox that is checked. At the bottom, there are "Save" and "Cancel" buttons.

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. |
| LED | Configure the LED: Four options are available: Use System Settings, Always on, Always off, or Schedule. |
| Band Steering | <p>Band Steering will help redirect clients to a radio band 2.4G or 5G, depending on what is supported by the device, to increase efficiency and benefit from the maximum throughput.</p> <p>Four options are allowed by GWN.Cloud:</p> <p>Disable Band steering: This will disable the band steering feature and the access point will accept the band chosen by the client.</p> <p>2G in Priority: 2G Band will be prioritized over 5G Band.</p> <p>5G in Priority: 5G Band will be prioritized over 2G Band</p> <p>Balance: Band Steering will balance between the clients connected to 2G and 5G.</p> <p>Use Radio Settings: GWN will use the value configured under Radio page.</p> |
| Enable Schedule | Configure a schedule for when the Wi-Fi will be ON or Off, by default it is disabled. The user can enable it and select a schedule from the drop-down list or use radio settings. |
| Disable Port | Select "NET" from the drop-down list to disable the Ethernet the NET port. |
| NET/PoE Link Type | If GWN76xx access point is connected to a router or a switch, the NET/PoE port can be configured as a Trunk or Access. |
| PVID | Configures the VLAN ID of the port |
| Allowed VLAN(s) | Configure the VLAN ID(s) allowed to pass through the port. Multiple VLAN IDs can be entered such as 1,2,3,7. Up to 16 VLAN IDs can be configured. If no value is configured, the port allows all VLANs |
| 2.4G/5G (802.11b/g/n/ax) | |
| Disable 2.4GHz/5GHz | This feature allows the user to disable/enable its 2.4GHz/5GHz band on the AP. |
| Channel Width | Choose the Channel Width, note that wide channels will give better speed/throughput, and narrow channel will have less interference. 20Mhz is suggested in a very high-density environment. Default is "Use Radio Settings", the AP then will use the value configured under the 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 the desired cell size to be broadcasted, five options are available: "Low", "Medium", "High", "Custom" and "Use Radio Settings". The default is "Use Radio Settings", the AP then will use the value configured under the Radio page |
| Enable Minimum RSSI | Configure 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 APs. This option can be either Disabled or Enabled and set manually or set to Use Radio Settings. |

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.

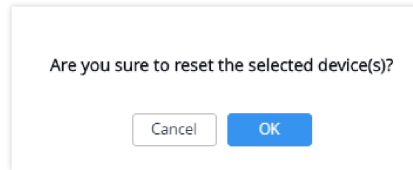
Access Point Configuration Settings

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.

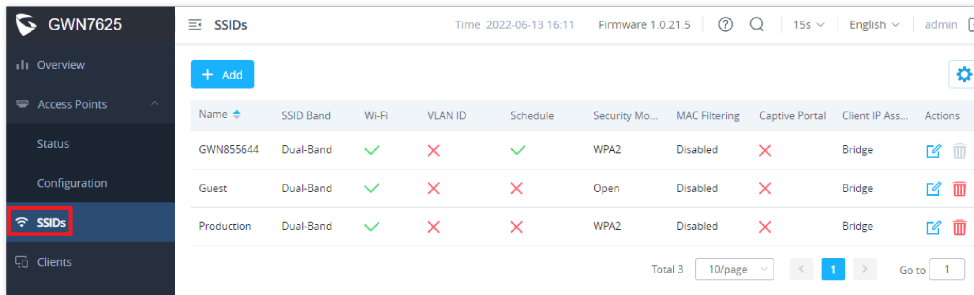


Reset Access Point

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 connected to different APs are isolated from each other. <i>This feature is not supported on GWN7610.</i> |
| 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. <i>This is available when Client IP Assignment is set to Bridge.</i> |

| | |
|-----------------------------|--|
| Security Mode | <p>Set the security mode for encryption, 8 options are available:</p> <ul style="list-style-type: none"> • 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. <p>Note: GWN products support for 802.1x (PEAP-MSCHAPv2 and EAP-TLS) requires external AAA server to permit authentication and centralized access management.</p> |
| WEP Key | <p>Enter the password key for WEP protection mode. <i>This field is available only when "Security Mode" is set to "WEP 64-bit" or "WEP 128-bit".</i></p> |
| WPA Key Mode | <p>Three modes are available:</p> <ul style="list-style-type: none"> • 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. <p>Note: PPSK is available only when "Security Mode" is set to "WPA2".</p> <p>PPSK management is available at Access Control → PPSK.</p> |
| WPA Encryption Type | <p>Two modes are available:</p> <ul style="list-style-type: none"> • 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. <p>Note: This field is available only when "Security Mode" is set to "WPA/WPA2", "WPA2", "WPA2&WPA3", "WPA3" or "WPA3-128".</p> |
| WPA Pre-Shared Key | <p>Set the access key for the clients, and the input range should be: 8-63 ASCII characters or 8-64 hex characters. <i>This field is available only when "Security Mode" is set to "WPA/WPA2", "WPA2", "WPA2/WPA3" or "WPA3".</i></p> |
| 802.11w | <p>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. Users can set this option to Disabled: disable 802.11w; Optional: both the supported and unsupported 802.11w clients may have the network access authority; Required: only the client supported 802.11w have the network access authority.</p> |
| RADIUS Sever Address | <p>Configure RADIUS authentication server address. <i>This field is available only when "WPA Key Mode" is set to "802.1x".</i></p> |

| | |
|---|--|
| RADIUS Server Port | Configure RADIUS Server Listening port. Default is: 1812. <i>This field is available only when "WPA Key Mode" is set to "802.1x".</i> |
| RADIUS Server Secret | Enter the secret password for client authentication with RADIUS server. <i>This field is available only when "WPA Key Mode" is set to "802.1x".</i> |
| Secondary RADIUS Server | <p>Check the box to enable settings a secondary RADIUS server. Then you need to specify below three fields:</p> <ul style="list-style-type: none"> • RADIUS Server Address: Enter the secondary RADIUS server address. • RADIUS Server Port : Enter the secondary RADIUS server port. <i>The default port is 1812 and the range is 1-65535.</i> • RADIUS Server Secret: Enter the secret password for client authentication with the secondary RADIUS server. |
| RADIUS Accounting Server | Configure the address for the RADIUS accounting server. <i>This field is available only when "WPA Key Mode" is set to "802.1x".</i> |
| RADIUS Accounting Server Port | Configure RADIUS accounting server listening port. Default is 1813. <i>This field is available only when "WPA Key Mode" is set to "802.1x".</i> |
| RADIUS Accounting Server Secret | Enter the secret password for client authentication with RADIUS accounting server. <i>This field is available only when "WPA Key Mode" is set to "802.1x".</i> |
| Secondary RADIUS Accounting Server | <p>Check the box to enable settings for a secondary RADIUS accounting server. Then you need to specify below three fields:</p> <ul style="list-style-type: none"> • 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. <i>This field is available only when "WPA Key Mode" is set to "802.1x".</i> |
| Enable Hotspot2.0 | Check to activate Hotspot2.0 in the SSID. <i>This field is available only when "WPA Key Mode" is set to "802.1x".</i> Refer to [Hotspot 2.0] for more details |
| Hotspot2.0 Profile | Select the Hotspot2.0 profile to use in the SSID. <i>This field is available only when "WPA Key Mode" is set to "802.1x".</i> 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 with an 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 | <p>Client isolation feature blocks any TCP/IP connection between connected clients to GWN76XX. Client isolation can be helpful to increase security for Guest networks/Public Wi-Fi. Three modes are available:</p> <ul style="list-style-type: none"> • 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 | Configure 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 the 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 clients. If there is a SSID per-radio on a LAN, each SSID will have the same limit. For example, setting a limit of 50 will limit EACH ssid to 50 users independently. Note: If set to 0, it disables 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 | Configure the Client Bridge Support to allow the access point to be configured as a bridge to connect 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 directly. Once an SSID has Client Bridge Support enabled, the AP adopted in this SSID can be turned into Bridge Client mode by clicking 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 as "Disabled": 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 as "Disabled": none of the multicast package will be converted; When set as "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. When set as "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 | <p>Check to enable/disable Voice Enterprise. The roaming time will be reduced once enabled voice enterprise.</p> <ul style="list-style-type: none"> • 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 faster. 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. <p>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".</p> |
| 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 the 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 |

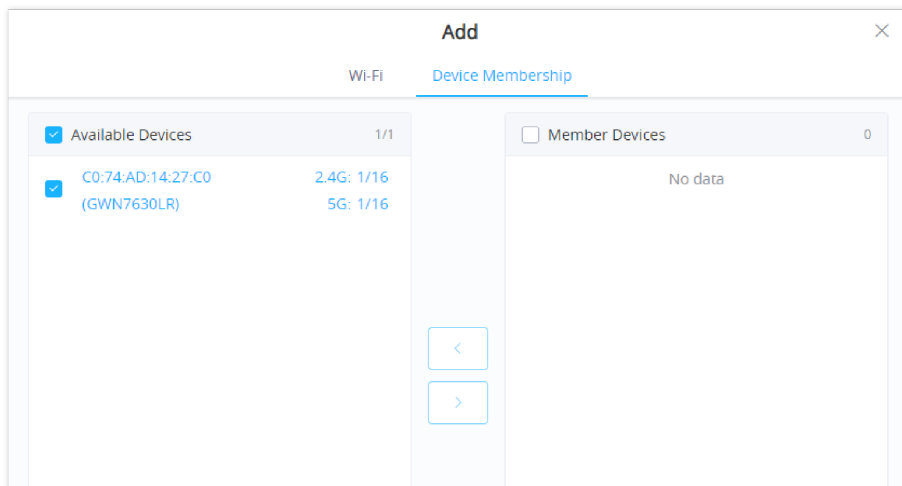
Wi-Fi

- **Device Membership:** Used to add or remove paired access points to the SSID. The MAX SSID number is separately counted for each band (2.4GHz or 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

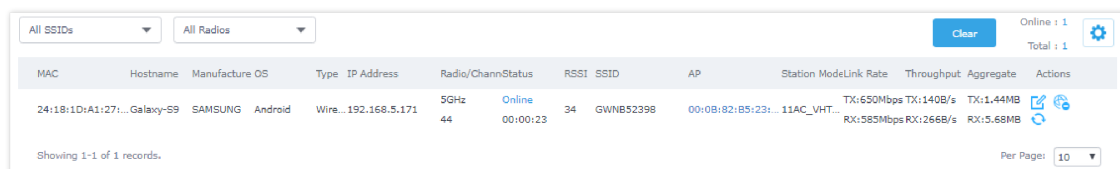


Device Membership

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 as 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
- IPv4 Address
- IPv6 Address
- Radio/Channel
- Status
- RSSI
- SSID
- AP
- Station Mode
- Link Rate
- Throughput
- Aggregate



Default

Clients – Select Items

ACCESS CONTROL

Access List

From this menu, users can manage the blacklist of clients that will be blocked from accessing the Wi-Fi network globally, click on **Client Access** to add/remove MAC addresses of the client to/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

MAC Addresses





[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.

Add

Name

MAC Addresses -
 Add new item +

Enable Schedule

Schedule

Adding Client Access List

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

Access Control / Access List Time 2022-08-17 15:21

+ Add
↑ Import
↓ Export

| Name | MAC Addresses |
|------------------|---------------|
| Global Blacklist | |

Import/Export the client access

Users can check « Enable Schedule » to assign a schedule to the list and set the time it will take effect.

+ Add

| Name | MAC Addresses | Actions |
|------------------|---|-------------------------------------|
| Global Blacklist | | ✎ 🗑 |
| Access List 1 | (3) 48:4B:AA:08:3F:90, 48:4B:AA:08:3F:91, 48:4B:AA:08:3F:92 | ✎ 🗑 |

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.

Edit

Wi-Fi Device Membership

SSID ?

Enable SSID

Client IP Assignment ?

VLAN

SSID Band ?

Access Security

Security Mode

Enable Captive Portal

Use MAC Filtering

Client Isolation Disabled

Advanced

SSID Hidden

Whitelist
Blacklist

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 until the user configurable cool-down period is reached.

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. The administrator can also set the reconnect type and value for the users to reconnect 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 | Set the 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. |

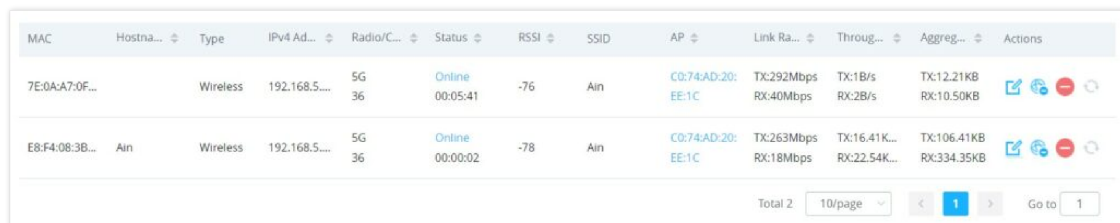
Time Policy Parameters







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

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 .



| MAC | Hostna... | Type | IPv4 Ad... | Radio/C... | Status | RSSI | SSID | AP | Link Ra... | Throug... | Aggreg... | Actions |
|----------------|-----------|----------|--------------|------------|--------------------|------|------|-----------------------|-------------------------|------------------------------|----------------------------|---|
| 7E:0A:A7:0F... | | Wireless | 192.168.5... | 5G 36 | Online 00:05:41 | -76 | Ain | C0:74:AD:20: EE:1C | TX:292Mbps RX:40Mbps | TX:1B/s RX:2B/s | TX:12.21KB RX:10.50KB |    |
| E8:F4:08:3B... | Ain | Wireless | 192.168.5... | 5G 36 | Online 00:00:02 | -78 | Ain | C0:74:AD:20: EE:1C | TX:263Mbps RX:18Mbps | TX:16.41K... RX:22.54K... | TX:106.41KB RX:334.35KB |    |

Total 2 10/page < 1 > Go to 1

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".

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

MAC Address Bandwidth Rule

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 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.

Private Pre-Shared Key (PPSK)

PPSK (Private Pre-Shared Key) is a way of creating Wi-Fi passwords per group of clients instead of using one single password for all clients. It's also possible to assign it for one single device client with a MAC Address.

Note:

- Before adding a PPSK account, first create an SSID with WPA Key Mode set to **"PPSK Without RADIUS or with RADIUS"** under **Web UI → SSIDs**.
- The maximum number of allowed PPSK accounts is 300.

To configure PPSK, **please navigate to Web UI → Access Control → PPSK**, then click on **"Add"** button to add a new PPSK account.

The screenshot shows a modal window titled "Add" with a close button (X) in the top right corner. The form contains the following fields and controls:

- SSID: A dropdown menu with "Guests WiFi" selected.
- Account: A text input field containing "Guests".
- Wi-Fi Key: A text input field with masked characters (dots) and an eye icon to toggle visibility.
- Confirm Wi-Fi Key: A text input field with masked characters (dots) and an eye icon to toggle visibility.
- Maximum Number of Access Clients: A text input field containing "100".
- Upload Limit: A text input field containing "10" and a dropdown menu set to "Mbps".
- Download Limit: A text input field containing "50" and a dropdown menu set to "Mbps".
- VLAN: An empty text input field.
- Description: A text input field containing "PPSK is dedicated to up to 100 Guests".

At the bottom of the form are two buttons: "Save" (highlighted in blue) and "Cancel".

Add a PPSK Profile

In case where the Maximum Number of Access Clients set to 1, then an option to specify a MAC Address is added. Please refer to the figure below:

The screenshot shows a modal window titled "Add" with a close button (X) in the top right corner. The form contains the following fields and controls:

- SSID: A dropdown menu with "Guests WiFi" selected.
- Account: A text input field containing "One Device".
- Wi-Fi Key: A text input field with masked characters (dots) and an eye icon to toggle visibility.
- Confirm Wi-Fi Key: A text input field with masked characters (dots) and an eye icon to toggle visibility.
- Maximum Number of Access Clients: A text input field containing "1", which is highlighted in yellow.
- MAC: A text input field containing "c0:ad:74:11:22:33", which is highlighted in yellow.
- Upload Limit: A text input field containing "10" and a dropdown menu set to "Mbps".
- Download Limit: A text input field containing "50" and a dropdown menu set to "Mbps".
- VLAN: An empty text input field.
- Description: A text input field containing "Dedicated for one single device with a MAC Address".

At the bottom of the form are two buttons: "Save" (highlighted in blue) and "Cancel".

PPSK – Maximum Number of Access Clients

| | |
|---|--|
| SSID | Select the SSID from the drop-down list <i>Note: the SSID WPA Key Mode must be set to "PPSK Without RADIUS or With RADIUS".</i> |
| Account | Set a name for this PPSK profile. |
| Wi-Fi Key | Enter a Wi-Fi key. |
| Confirm Wi-Fi Key | Confirm the Wi-Fi key (must be the same) |
| Maximum Number of Access Clients | Enter the maximum number of access clients (devices) that are allowed to use this key, once the maximum number is reached, the key will not be used to connect to Wi-Fi. |
| MAC | In case the maximum number of access clients is set to 1, then the user can specify the MAC address as well for even more security. |
| Upload Limit | set a max upload limit (Mbps/Kbps) |
| Download Limit | set a max download limit (Mbps/Kbps) |
| VLAN | specify a VLAN or leave it empty (Default VLAN). |
| Description | Enter a description for this PPSK profile. |

PPSK

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.



| MAC Address | Hostname | AP | SSID | IPv4 Address | Authentication St... | Actions |
|--------------|----------------|--------------|---------|----------------|----------------------|---------|
| F4961E89DE84 | | C574AD3E8520 | CPGuest | 192.168.80.223 | Authenticated | ⊘ |
| 88F40E3E42FD | DESKTOP-M3KR86 | C574AD3E8520 | CPGuest | 192.168.80.11 | Authenticated | ⊘ |

Captive Portal – Guest Page

Click on "**Kick out**" button  to kick out connected clients.

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

Select up to 16 items

- MAC Address
- Hostname
- AP
- SSID
- RSSI
- Used Traffic
- Authentication Type
- Login Time
- IPv4 Address
- IPv6 Address
- Name
- Email
- Gender
- Age Range
- Expire Time
- Authentication Status

Default

Captive Portal – Guest Page – Select Items

Policy List

Users can customize a portal policy in this page.

| Name | Authentication Type | Expiration | Portal Page Customization | Actions |
|-------------|---------------------|------------|---------------------------|---------|
| grandstream | Login for free | 86400s | /portal_default.html | |

Captive Portal – Policy List

- Click on to edit the policy.
- Click on to delete the policy.
- Click on 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 can be easily configured as shown in the next section.

Administrator can use an internal or external splash page.

Add

Basic Auth Rule

Name

Splash Page

Authentication Type

Client Expiration

Client Idle Timeout

Unauthenticated Client Timeout

Use Default Portal Page

Portal Page Customization

Landing Page

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, in this case "Internal" |
| Authentication Type | <p>The following types of authentications are available:</p> <ul style="list-style-type: none"> ● Log in 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 the internet. ● Radius Server: Choosing this option will allow users to set up a RADIUS server to authenticate connecting clients. ● Social Login Authentication: Choosing this option will allow users to enable authentication on 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. ● SAML SSO: Choosing this option will allow users to authenticate clients using SSO Server. ● Active Directory: Choosing this option will allow users to set up an Active Directory server to authenticate connecting clients. |
| Client Expiration | <p>Configure the period of validity, after the valid period, the client will be re-authenticated again.</p> <p><i>Note: the maximum duration is 30 days.</i></p> |
| Client Idle Timeout | <p>Configure the time when the client will automatically deauthenticate when it is idle. This does not apply to Voucher Captive portal mode.</p> <p><i>Note: the maximum duration is 24 hours.</i></p> |
| Unauthenticated Client Timeout | <p>Configure a timeout period, after which unauthenticated client devices will be disconnected, and reconnection is not allowed.</p> <p><i>Note: the maximum duration is 24 hours.</i></p> |
| 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 retries 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 “SAML SSO” | |
| SSO Server URL | Fill in the IP address of the SSO server. |
| Redirect URL | Enter the redirect URL. |
| X.509 Cert SHA1 Fingerprint | enter the X.509 Cert SHA1 Fingerprint |
| 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 from the drop-down list (if “Use Default Portal Page” is unchecked). |
| Landing Page | Choose the landing page, 2 options are available: <ul style="list-style-type: none"> • 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 | <ul style="list-style-type: none"> • Disabled: Non -day access limit. • According to the client limit: After opening, only the Guest is allowed to be connected once a day, and it is not allowed to authenticate again after the network use timeout. • Limit by authentication: The guest is accessed once a day to any authentication method. Refresh the number of times every 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>

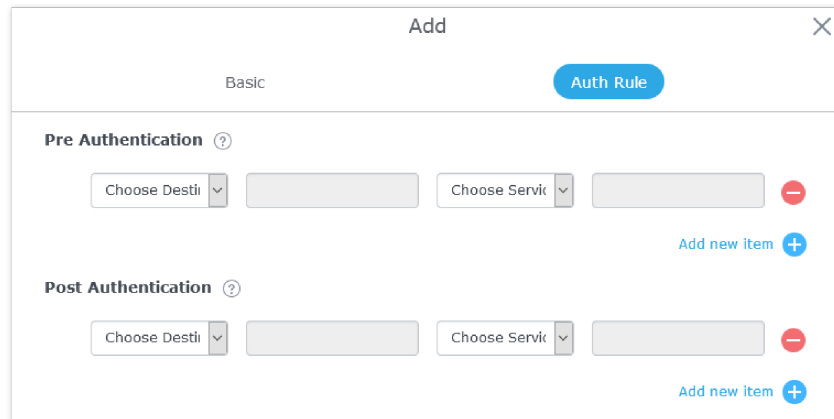
External Splash Page

| Field | Description |
|---------------------------------|---|
| Name | Enter the name of the Captive Portal policy |
| Splash Page | Select Splash Page type, in this case “External” |
| 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. <i>This field appears only when Splash Page is set to "External".</i> |
| 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 media 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

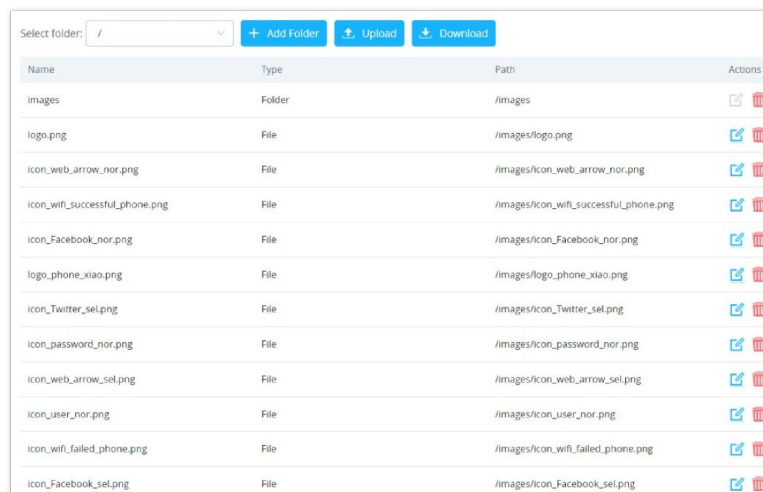
Using this option, users can set rules to match traffic that will be allowed for connected Wi-Fi users before the authentication process. For example, if users need to set up Facebook authentication, some traffic should be allowed to the Facebook server(s) to process the user’s authentication. Or simply 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...).



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

- Click on  to upload a file from local device.
- Click on  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 administrators 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 network 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  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 with the same profile, this way the GWN will generate as many vouchers as needed with the same settings to avoid creating them one by one.
- The administrators 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 with the 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 the internet. Note: in case of multiple users, the duration will start counting after the first user starts using the voucher. |
| Validity Time | Set the validity period of the credentials, limited to 1-365. The unit is day. |
| Download Limit | Set the download bandwidth speed limit (in Kbps or Mbps). |
| Upload Limit | Set the upload bandwidth speed limit (in Kbps or Mbps). |
| Notes | Notes for the administrator when checking the list vouchers list. |

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 to access the internet. More details about captive portal will be covered in the next section, 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

| General | |
|----------------------|--|
| Band Steering | <p>Band Steering will help redirect clients to a radio band 2.4G or 5G, depending on what is supported by the device, for efficient use and to benefit from the maximum throughput.</p> <p>Four options are allowed by GWN.Cloud:</p> <ul style="list-style-type: none"> ● 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 the 5G Band.List Item 2 ● 5G in Priority: 5G Band will be prioritized over the 2G BandList Item 3 |

| | |
|---------------------------------|--|
| | <ul style="list-style-type: none"> ● Balance: GWN will balance between the clients connected to 2G and those connected to 5GHz. |
| Client Steering | <p>This feature will help Wi-Fi clients to roam to other APs within the same Network.</p> <p><i>Note: Once enabled, Band Steering in Access Device → Configuration → Configure cannot be configured. SSID→Wifi Settings→802.11k will be enabled</i></p> |
| RSSI Threshold (dBm) | <p>This option is only available if Client Steering is enabled.</p> <p>Specify the RSSI Threshold before clients get steered away to another AP.</p> <p><i>Note: Must be an integer between -80 and -65.</i></p> |
| Client Access Threshold | <p>This option is only available if Client Steering is enabled.</p> <p>Specify the Client Access Threshold before the AP won't accept clients and they will be steer away to another AP with less connected clients.</p> <p><i>Note: Must be an integer between 10 and 100.</i></p> |
| Airtime Fairness | <p>Allow faster clients to have more airtime than slower clients.</p> |
| Beacon Interval | <p>Configure the beacon period, which decides the frequency the 802.11 beacon management frames AP transmits. Please input integrates from 40 to 500.</p> <ul style="list-style-type: none"> ● When AP enables 0-2 SSIDs, the interval value will be effective are the values from 40 to 500. ● When AP enables 3-8 SSIDs, the interval value will be effective are the values from 100 to 500. ● When AP enables more than 8 SSIDs, the interval value will be effective are the values from 200 to 500. <p>Note: mesh feature will take up a share when it is enabled.</p> |
| Enable Schedule | <p>Configure a schedule for when the Wi-Fi will be ON or Off, by default is disable or the user can enable it and select a shedule form the drop-down list or use radio settings.</p> |
| Country/Region | <p>Display the country/region of the AP.</p> <p><i>Note: To configure the country/Region, Navigate to System → Settings page.</i></p> |
| Scene | <p>Configure whether to disable/enable 5.150–5.350GHz (channels 36-64) for outdoor usage.</p> <p><i>Note: The "Scene" is only effective for the outdoor type of access points.</i></p> |
| 2.4G/5G (802.11b/g/n/ax) | |
| Channel Width | <p>Choose the Channel Width, note that a wider channel will give better speed/throughput, and a narrow channel will have less interference. 20MHz is suggested in a very high-density environment.</p> |
| 40MHz Channel Location | <p>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.</p> |
| Channel | <ul style="list-style-type: none"> ● Auto: the AP selects the channel one time and sticks to it usually after booting up. ● Dynamically Assigned by RRM: the AP dynmically changes the channel accordingly to avoid channels overlapping. <p><i>Default is Auto.</i></p> |
| Custom Channel | <p>Select from the drop-down list the allowed channels either for 2.4GHz or 5GHz. Multiple selections are possible.</p> |
| Radio Power | <p>Set the Radio Power depending on the application and distance, six options are available: "Low", "Medium", "High", "custom", "Dynamically Assigned by RRM" and "Auto".</p> <p>The default is "High".</p> |

| | |
|--------------------------------------|---|
| 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 | Configure 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. |
| Wi-Fi5 Compatible Mode | Some old devices are not fully compatible with Wi-Fi6 and may not be able to scan the signal or have poor connection. After turning on this feature, it will switch to Wi-Fi5 mode to solve the compatibility problem. and turn off Wi-Fi6 related functions.. |

Radio – Global configuration

SECURITY

Rogue AP

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

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.

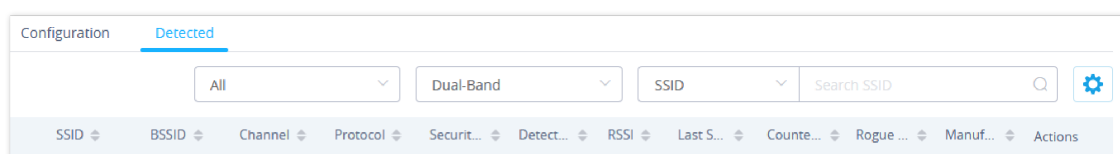
Rogue AP-Configuration

| Field | Description |
|----------------------------------|--|
| Enable Rogue AP Detection | Select to either to enable or disable Rogue AP scan. |

| | |
|-------------------------------------|--|
| Detect range | <p>Specify the rogue AP detect range.</p> <ul style="list-style-type: none"> • 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. <p>Default is Same Channel.</p> |
| Countermeasure Level | <p>Countermeasure level specifies the type of attacks which will be suspected by the AP. Select different levels:</p> <ul style="list-style-type: none"> • 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. <p>Default is Disabled.</p> |
| Containment Range | <p>Specify the containment range:</p> <ul style="list-style-type: none"> • 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. <p>Default is Same Channel.</p> |
| 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

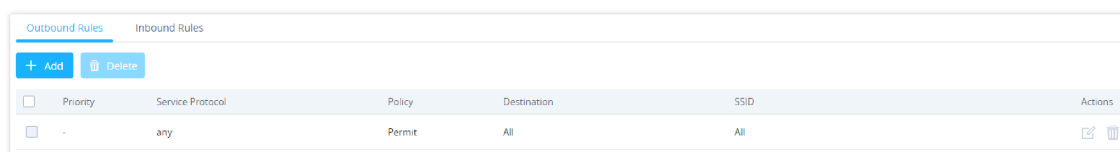
The figure below shows a list of all the detected rogue AP on the network scanned by the GWN access point.



Rogue AP-Detection

Firewall

This section allows users 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.



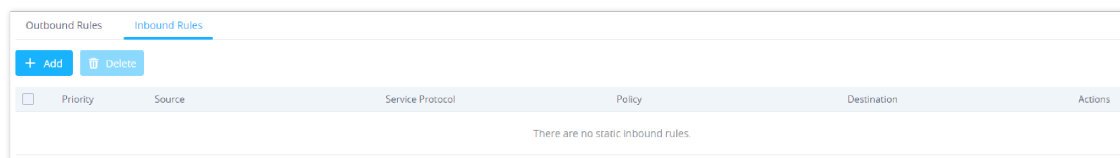
Firewall-Outbound

| 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: <ul style="list-style-type: none"> • Protocol: TCP or UDP • Port: define the port used by this protocol. |
| Policy | Either select to Permit or Deny Outbound traffic. |
| Destination | Select either: <ul style="list-style-type: none"> • 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:



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: <ul style="list-style-type: none"> • Protocol: TCP or UDP • Port: define the port used by this protocol. |
| Policy | Either select to Permit or Deny inbound traffic. |
| Source | Select either: <ul style="list-style-type: none"> • Particular IP: IP address of source. • Particular Network: Network IP address. • All: the rule will apply on all destinations. |
| Destination | Configure the destination address. <ul style="list-style-type: none"> • All • Particular • IP Particular Domain • Particular Network |

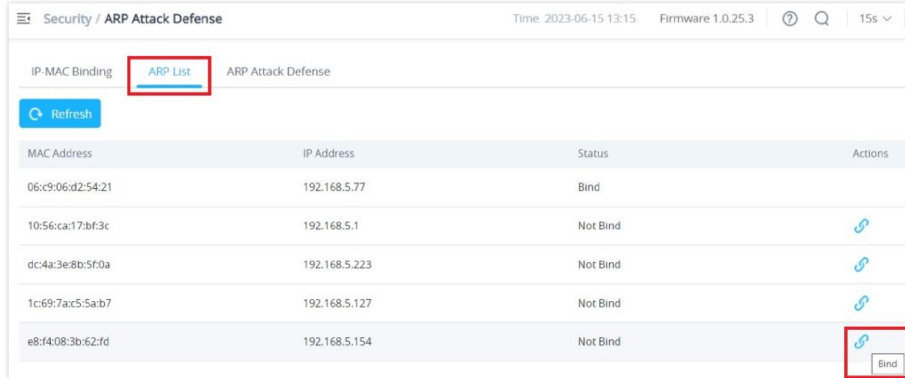
Firewall-Inbound

ARP Attack Defense

GWN Access points also support ARP Attack Defense security feature. This feature protects clients from spoofing MAC addresses by binding the MAC address to an IP address.

ARP List

Navigate to **Web UI** → **Security** → **ARP Attack Defense**, on the ARP list tab, the user can see the current ARP table (MAC address → IP address combination), Click on **"Bind"** icon to bind the MAC address to an IP address.

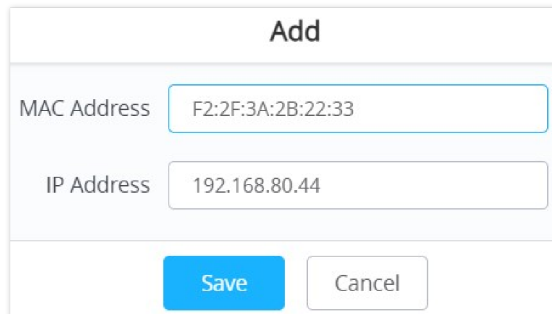


| MAC Address | IP Address | Status | Actions |
|-------------------|---------------|----------|---------|
| 06:c9:06:d2:54:21 | 192.168.5.77 | Bind | |
| 10:56:ca:17:bf:3c | 192.168.5.1 | Not Bind | |
| dc:4a:3e:8b:5f:0a | 192.168.5.223 | Not Bind | |
| 1c:69:7a:c5:5a:b7 | 192.168.5.127 | Not Bind | |
| e8:f4:08:3b:62:fd | 192.168.5.154 | Not Bind | |

ARP Attack Defense – ARP List

IP-MAC Binding

To make an IP-MAC address Binding manually, on the IP-MAC Binding tab, click on **"Add"** button and then enter the IP address and the MAC address then click save.



Add

MAC Address: F2:2F:3A:2B:22:33

IP Address: 192.168.80.44

Save **Cancel**

ARP Attack Defense – IP MAC Binding

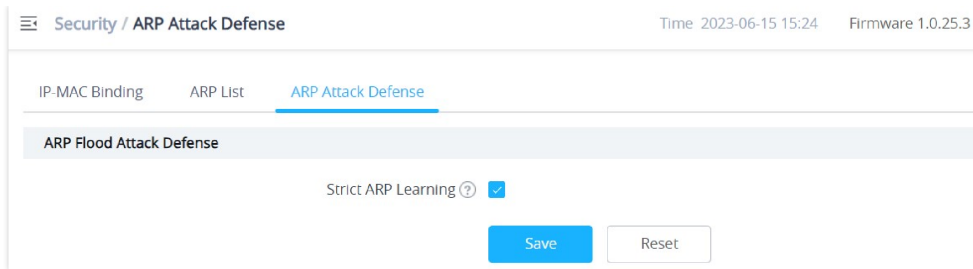
To unbind or edit, click on **"Delete or Edit"** icons under Actions. Please refer to figure below:



| MAC Address | IP Address | Actions |
|-------------------|---------------|---------|
| 1c:69:7a:c5:5a:b7 | 192.168.5.127 | |

ARP Attack Defense

Strict ARP Learning option only learns ARP from the ARP Reply responding to the ARP Request sent by this device.

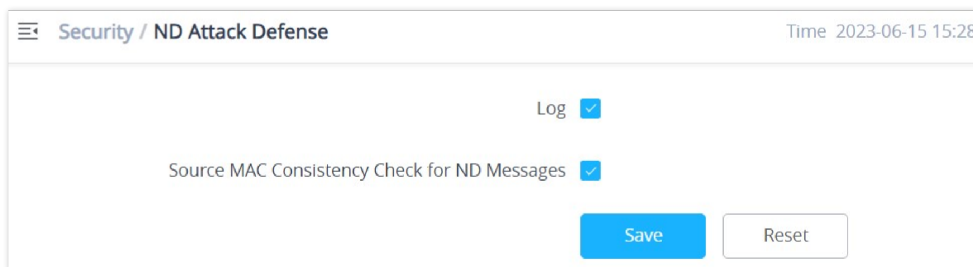


ARP Flood Attack Defense

Neighbor Discovery (ND) Attack Defense

ND Attack Defense is the equivalent of ARP Attack defense but using IPv6 addresses.

Navigate to **Web UI** → **Security** → **ND Attack Defense** page, then you can enable this security feature by clicking on **“Source MAC Consistency Check for ND Messages”**, now the device will check for Source MAC addresses to avoid any spoofing. There is also the option to log these events by checking **“Log”** option.



ND Attack Defense

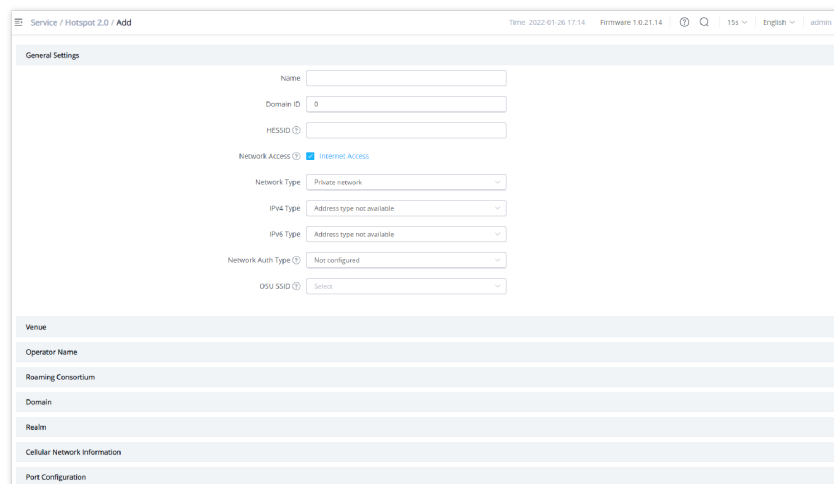
SERVICE

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 to log in to each hotspot. This feature is currently on 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:



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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Acceptance of terms and conditions • On-line enrollment supported • http/https redirection • DNS redirection • Not configured |
| OSU SSID | Configure the Online Sign 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 | <p>When this option is disabled, it means the DGAF is enabled, the AP will forward all downlink broadcast ARP messages and wireless group broadcasts.</p> <p>When this option is enabled, the DGAF function is disabled, the AP will discard all downlink broadcast ARP messages and wireless group broadcasts.</p> <p>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.</p> |

Hotspot 2.0

SNMP

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

SNMPv1, SNMPv2c

Enable

Community String

SNMPv3

Enable

Username

Authentication mode

Authentication password

Privacy mode

Privacy password

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

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 the same ID should be set under the SSID field 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 | Set 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 |

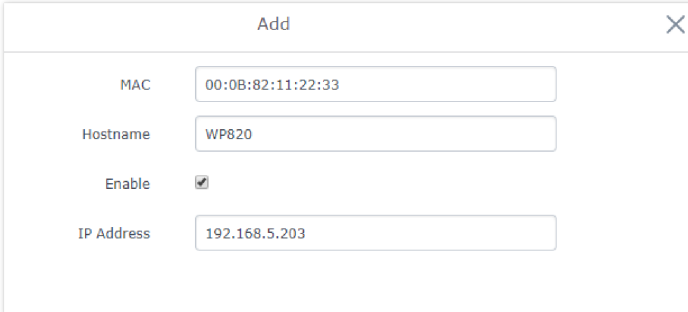
NAT Pool Parameters

Static DHCP

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

To configure Static DHCP, please follow below steps:

1. Click  button to create a new entry.
2. Enter the name of the device, along with its MAC address and IP address



DHCP Binding

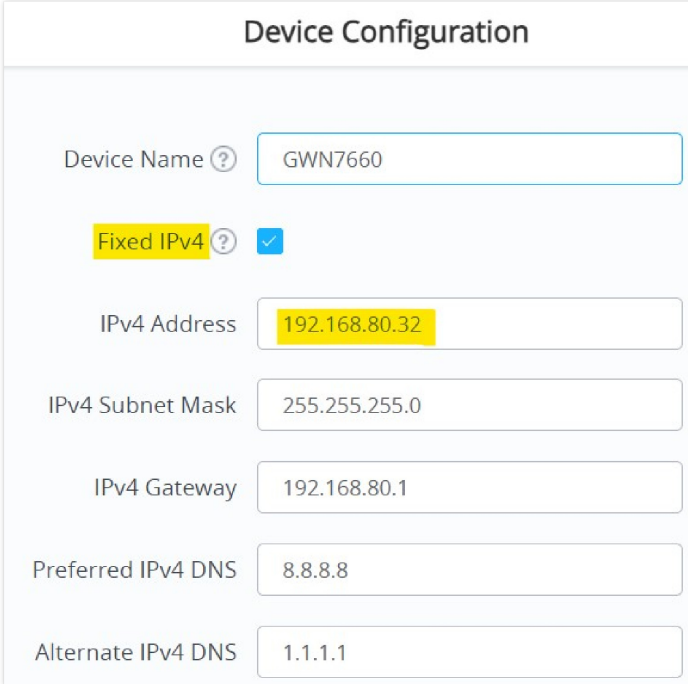
- o Press Save and Apply to submit the changes.

DHCP Relay

DHCP Relay is a network device that forwards IP addresses from the DHCP Server to clients devices, even if the DHCP server is on a different network (ex: VLAN). This way we can have a dedicated DHCP server on many networks. GWN access points can be configured as a DHCP relay agent. Please follow the steps below:

Prerequisite: before configuring DHCP Relay, first we have to assign a static IP address to both devices that will be acting as a DHCP Server and DHCP Relay in our case it's two GWN76xx Access Points.

1. The first step in our example is to make a GWN access point as a DHCP Server, please refer to [DHCP Server](#) configuration.
2. Navigate to **Web UI** → **Access Points** → **Configuration**, click on the access point or click on the "Edit" icon, then the device configuration window will show up. Set a static IP for both access points (one acting as a DHCP Server and the other one as a DHCP Relay), please refer to the figure below.



Device Configuration

Device Name

Fixed IPv4

IPv4 Address

IPv4 Subnet Mask

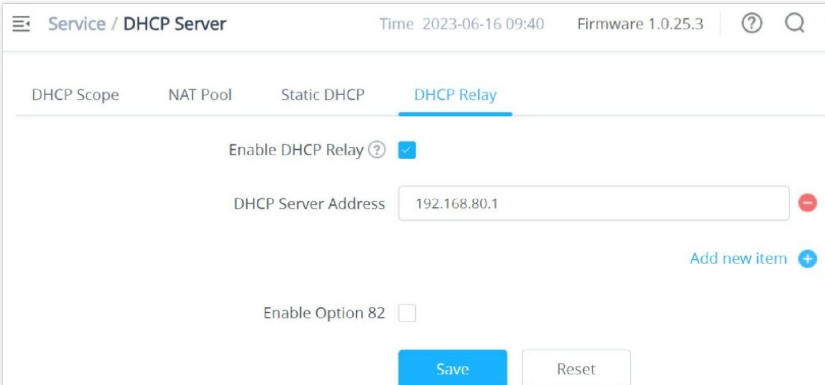
IPv4 Gateway

Preferred IPv4 DNS

Alternate IPv4 DNS

Setting up a static IP

3. To configure DHCP Relay, please navigate to GWN access point **Web UI** → **Service** → **DHCP Server** → **DHCP Relay** tab, Then enable DHCP Relay and then enter the DHCP Server Address (ex: GWN access point).



Service / DHCP Server Time 2023-06-16 09:40 Firmware 1.0.25.3

DHCP Scope NAT Pool Static DHCP **DHCP Relay**

Enable DHCP Relay

DHCP Server Address

Add new item

Enable Option 82

Save Reset

DHCP Relay

Note:

a router side configuration could be required to setup VLANs for both access points to be able to communicate.

TR-069

| | |
|------------------------------|------------------------------------|
| Enable TR-069 | <input type="checkbox"/> |
| ACS URL | <input type="text"/> |
| ACS User Name | <input type="text"/> |
| ACS Password | <input type="text"/> |
| Periodic Inform Enable | <input type="checkbox"/> |
| Periodic Inform Interval (s) | <input type="text" value="86400"/> |
| CPE Cert File | <input type="text"/> |
| CPE Cert Key | <input type="text"/> |

TR-069

| Field | Description |
|-------------------------------------|--|
| Enable TR-069 | Configure 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.

The screenshot shows a web interface with two tabs: 'Basic' (selected) and 'Account'. Below the tabs is a section titled 'LEDs'. In this section, there is a label 'LED' followed by a dropdown menu that is currently set to 'Always on'.

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 to optimizing and reducing energy consumption of the AP. Users 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 a VLAN network. If enabled, APs 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 the deployment type (Indoor or Outdoor) the 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 | 1.0.23.3 1.0.23.3 | Yes Yes | Yes Yes | Yes Yes | Yes | Coming soon |
| GWN7625 | 1.0.23.9 | Yes | Yes | Yes | 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 CAPs access points already deployed (sometimes the CAPs access points can be the master controller of the network).
2. Next, we need to pair the REs 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 administrators 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**.

| Device Type | Name/MAC | IP Address | Status | Uptime | Firmware | Actions |
|-------------|-------------------|---------------|--------------------|---------|----------|---|
| GWN7600 | 00:0B:82:AF:D2:58 | 192.168.5.100 | Master | 31m 50s | 1.0.9.5 |       |
| GWN7600 | 00:0B:82:AF:D2:E0 | 192.168.5.225 | Online Wireless | 17m 33s | 1.0.9.5 |       |
| GWN7600 | 00:0B:82:AF:D2:B8 | 192.168.5.226 | Online | 5m 59s | 1.0.9.2 |       |

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

Enable Mesh ?

Scan Interval(s)

Interface ?

Wireless Cascades ?

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 setting up specific time for Wi-Fi where the service will be active or for LED schedule or bandwidth rules ...etc.

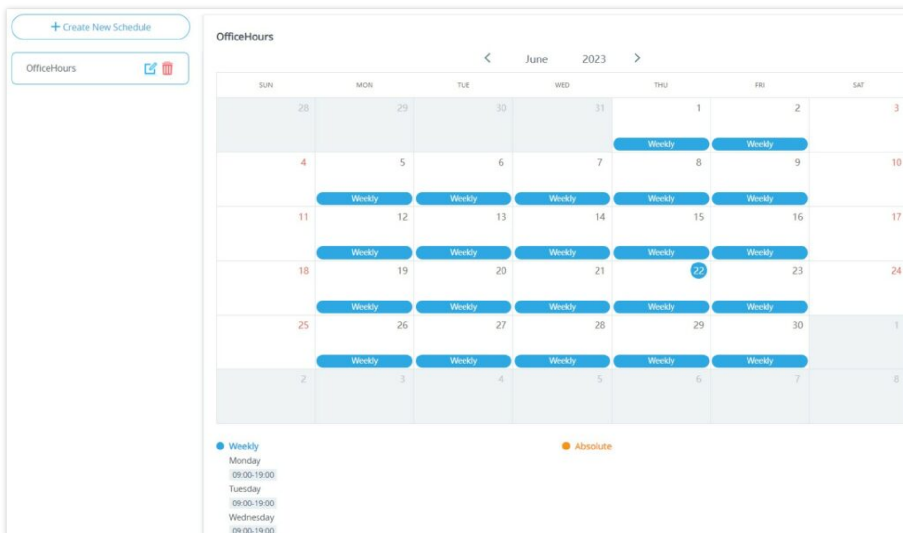
To configure a new schedule, follow below steps:

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.

Upgrade Syslog

General

Upgrade Protocol ? HTTP

Allow DHCP options 66 and 43 override ?

Check/Download New Firmware at Boot ?

Random Upgrade ?

Reboot ?

Factory Reset ?

Firmware

Firmware Server ? fm.grandstream.com/igs

Upgrade Now ?

Automatic Upgrade ? Disabled

Config

Download Configuration ?

Upload Configuration ?

Upgrade

Syslog

On the GWN76XX, users could dump the syslog information to a remote server under **Web GUI** → **System** → **Maintenance** → **Syslog Tab**. 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.

Note:

The device name is added to syslog messages. To configure the device name please navigate to **Web UI** → **Access Points** → **Configuration** select the device and click on **"Configure"** button.

Here is an example of the device name shown in Wireshark capture, please refer to the figure below:

| | | | | | | | | | | | |
|-------|------------|-----------------|----------|--------------|---------------|--------|-----|-------------------|---|----------|--------------------|
| 12692 | 2023-08-01 | 12:28:13.681982 | 0.002866 | 192.168.5.54 | 192.168.5.145 | Syslog | 215 | DAEMON.ERR: Aug | 1 | 11:28:14 | GWN7605LR[c074ad20 |
| 12749 | 2023-08-01 | 12:28:14.042543 | 0.044161 | 192.168.5.54 | 192.168.5.145 | Syslog | 174 | USER.DEBUG: Aug | 1 | 11:28:14 | GWN7605LR[c074ad20 |
| 12822 | 2023-08-01 | 12:28:16.799059 | 0.065550 | 192.168.5.54 | 192.168.5.145 | Syslog | 169 | DAEMON.INFO: Aug | 1 | 11:28:16 | GWN7605LR[c074ad20 |
| 13024 | 2023-08-01 | 12:28:22.111469 | 0.001712 | 192.168.5.54 | 192.168.5.145 | Syslog | 181 | USER.DEBUG: Aug | 1 | 11:28:23 | GWN7605LR[c074ad20 |
| 13025 | 2023-08-01 | 12:28:22.111999 | 0.000530 | 192.168.5.54 | 192.168.5.145 | Syslog | 189 | DAEMON.DEBUG: Aug | 1 | 11:28:23 | GWN7605LR[c074ad |
| 13026 | 2023-08-01 | 12:28:22.112209 | 0.000210 | 192.168.5.54 | 192.168.5.145 | Syslog | 178 | DAEMON.DEBUG: Aug | 1 | 11:28:23 | GWN7605LR[c074ad |
| 13027 | 2023-08-01 | 12:28:22.112311 | 0.000182 | 192.168.5.54 | 192.168.5.145 | Syslog | 178 | DAEMON.DEBUG: Aug | 1 | 11:28:23 | GWN7605LR[c074ad |
| 13028 | 2023-08-01 | 12:28:22.112822 | 0.000511 | 192.168.5.54 | 192.168.5.145 | Syslog | 204 | DAEMON.DEBUG: Aug | 1 | 11:28:23 | GWN7605LR[c074ad |
| 13029 | 2023-08-01 | 12:28:22.112927 | 0.000185 | 192.168.5.54 | 192.168.5.145 | Syslog | 204 | DAEMON.DEBUG: Aug | 1 | 11:28:23 | GWN7605LR[c074ad |
| 13030 | 2023-08-01 | 12:28:22.179520 | 0.057593 | 192.168.5.54 | 192.168.5.145 | Syslog | 168 | DAEMON.DEBUG: Aug | 1 | 11:28:23 | GWN7605LR[c074ad |
| 13176 | 2023-08-01 | 12:28:27.864780 | 0.000380 | 192.168.5.54 | 192.168.5.145 | Syslog | 199 | USER.DEBUG: Aug | 1 | 11:28:28 | GWN7605LR[c074ad20 |

Wireshark – GWN76xx AP

System / Maintenance

Upgrade Syslog

Syslog Server ? 192.168.5.145

Syslog Level ? 7 - Debug

Protocol ? UDP

Log DNS Queries

Client MAC Address ? Select

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. |
| Protocol | The protocol type sent to Syslog Server. |
| Log DNS Queries | Check to log DNS Queries. |
| Client MAC Address | Please configure the client MAC address for the log query. |

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

The screenshot shows the 'Alert Configure' page under the 'Email' section. It contains a list of seven notification settings, each with a question mark icon and a checkbox:

- Memory Usage
- AP Throughput
- SSID Throughput
- Admin password change
- Firmware Upgrade
- Rogue AP
- AP Offline

At the bottom right, there are two buttons: 'Save' (in blue) and 'Reset' (in grey).

Alert Configure

The following table describes the notifications configuration settings:

| Filed | Description |
|-----------------------|--|
| Memory Usage | Configure 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 | Configure whether to send notification on admin password change. |

| | |
|-------------------------|--|
| Firmware upgrade | Configure 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 | Configure 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

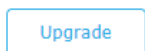
Examples of valid URLs:

firmware.grandstream.com/BETA

192.168.5.87

The upgrading configuration can be accessed via:

Web GUI → System Settings → Maintenance → Upgrade



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**.

| Device Type | MAC | Name | IPv4 Address | Status | Firmware | Channel | Actions |
|-------------|-------------------|------|---------------|--------|----------|-----------------|---|
| GWN7605LR | C0:74:AD:20:EE:1C | | 192.168.5.117 | Online | 1.0.25.3 | 2.4G 0 5G 36 | [Upgrade] [Reboot] [Add to SSIDs] [Configure] |
| GWN7624 | C0:74:AD:90:B2:40 | | 192.168.5.134 | Master | 1.0.25.3 | 2.4G 0 5G 36 | [Upgrade] [Reboot] [Add to SSIDs] [Configure] |

Access Points

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

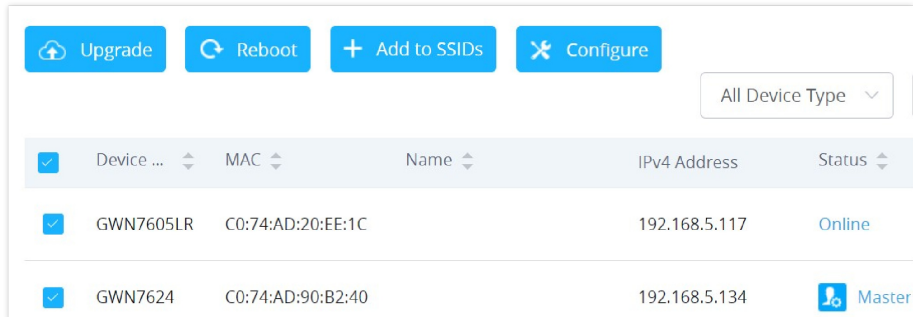


to upgrade the selected paired access points.

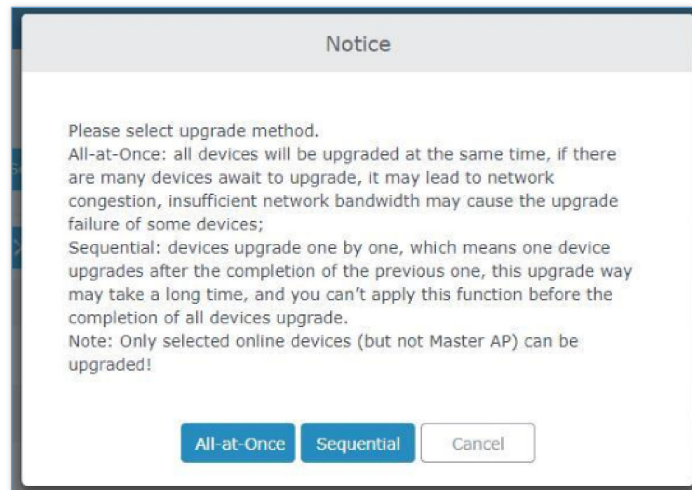
Sequential Upgrade

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:

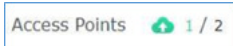
- Avoid entire Wi-Fi service interruption by full system firmware upgrade.
- Reduce network bandwidth consumption caused by firmware downloading.



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  to download the configuration file locally.

Upload Configuration

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



Click on  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 in order for the GWN76XX to be provisioned with that config server file.

Reset and reboot

- Users can reboot the device under **Web GUI→System Settings→Maintenance→Upgrade** by clicking on  button.
- The  button will restore all the GWN76XX options to factory settings.

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 1.0.25.10

Product Name: GWN7600 / GWN7600LR / GWN7602 / GWN7605 / GWN7605LR / GWN7610 / GWN7615 / GWN7624 / GWN7625 / GWN7630 / GWN7630LR / GWN7660 / GWN7660LR / GWN7661 / GWN7662 / GWN7664 / GWN7664LR

- Added support for Speed Test [[GWN AP as a slave](#)]

Firmware Version 1.0.25.9

Product Name: GWN7662

- No major changes

Firmware Version 1.0.25.8

Product Name: GWN7661

- No major changes

Firmware Version 1.0.25.7

Product Name:

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

- Increased PPSK accounts. [[PPSK](#)]

- Increased the client expiration time to 30 days. [[Captive Portal](#)]
- Added device name in Syslog messages. [[Syslog](#)]
- Added support for custom Channel on 2.4G band. [[Radio](#)]

Firmware Version 1.0.25.3

Product Name:

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

- No major changes

Firmware Version 1.0.25.1

Product Name:

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

- Added support of ARP defense [[ARP Attack Defense](#)]
- Added support of IPv6 ND defense [[ND Attack Defense](#)]
- Added support of disabling Ethernet port [[configure access points](#)]
- Added support of DHCP relay and option82 [[DHCP Relay](#)]
- Added support of trunk/access mode for NET/PoE port [[configure access points](#)]
- Added support of External syslog protocol selection [[Syslog](#)]
- Added support of collecting logs by MAC [[Syslog](#)]
- Added support of Captive Portal – Active Directory Auth (LDAP) [[Captive Portal](#)]
- Added support of Captive Portal – kickout timeout unauthenticated clients [[Captive Portal](#)]
- Added support of Captive Portal – Daily access limit by auth method [[Internal Splash page](#)]
- Added support of switching RF timer [[Radio](#)]

Firmware Version 1.0.23.27

Product Name: GWN7662

- This is the initial release of GWN7662

Firmware Version 1.0.23.24

Product Name:

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

- No major changes

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.

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.

ISED 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.

ISED Warning

This equipment complies with ISED 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 ISED 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>