Grandstream Networks, Inc.

GCC6000 - User Manual - Home

GCC601X(W) series are defined as mid-range all-in-one convergence devices. Integrates VPN Router, NGFW, Switch or Wi-Fi AP, and IP PBX, covering the collaborative office capabilities of data communication and UC audio and video service. Featuring GbE RJ-45 and SFP ports, it enables high-speed multi-WAN port connectivity for enterprises. This series is convenient and fast to deploy and manage through the local simple Web UI, GDMS, mobile APP, or console. Support unified management and centralized control of Grandstream terminal devices including APs, Switches, and UC endpoints. It is also a security firewall that provides excellent performance and defenses against the most advanced network attacks while achieving unified management and consistent security in complex hybrid environments. Ideal for small and medium enterprises, campuses, government, hotels, remote offices/SOHO, etc.

The GCC601x(W) combines the following modules:

- Home
- Networking
- Firewall
- Network Nodes
- PBX
- UC Endpoints

PRODUCT OVERVIEW

Technical Specifications

The following tables resume all the technical specifications including the hardware and the software specifications.

GCC6010 Technical Specifications

Network Ports	2 x 2.5 Gigabit SFP ports and 5 x Gigabit Ethernet ports *All ports are WAN/LAN configurable, max 3 x WAN
Auxiliary Ports	1xMicro-SD, 1xUSB 3.0, 1xReset
Memory	2GB RAM, 32GB eMMC Flash
External Storage	N/A
Router	2.5Gbps
IPsec VPN Throughput	1Gbps
NAT Sessions	160K
IDS/IPS	900Mbps
PBX	12 users and 4 concurrent calls by default. Upgrades available for purchase (See more for PBX capacity upgrade options).
Mounting	Desktop/Wall-mounting
Material	Metal

LEDs	7 x single LEDs and 1 x RGB LED for device tracking and status indication
Connection Type	DHCP, Static IP, PPPoE, PPTP, L2TP
Network Protocols	IPv4, IPv6, IEEE802.1Q,IEEE 802.1p, IEEE802.1x, IEEE802.3, IEEE 802.3u, IEEE 802.3x,IEEE802.3ab
QoS	VLAN, TOS Support multiple traffic classes, filter by port, IP address, DSCP, and policing App QoS: Application/protocol monitoring and traffic statistics VoIP Prioritization
Firewall	DDNS, Port Forwarding, DMZ, UPnP, DoS & Spoofing defense, traffic rules, NAT, ALG DPI, Anti-Virus, IPS/IDS, SSL deep inspection Content Control: DNS Filtering, Web url/class/content filtering, Application identification and control
VPN	• IPsec VPN Client-to-Site / Site-to-Site • IPSec Encryption: 3DES, AES • IPSec Authentication: MD5, SHA-1, SHA2-256 • IPSec Key Exchange: Main/Aggressive Mode, Pre-shared Key, DH Groups 1/2/5/14 • IPSec Protocols: ESP • IPSec NAT Traversal • PPTP VPN Server / Client • PPTP Encrpytion: MPPE 40-bit, 128-bit • PPTP/L2TP Authentication: MS-CHAPv1/2 • L2TP Client-to-Site • OpenVPN® Server / Client • OpenVPN® Encryption: AES, DES • OpenVPN® Authentication: MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512 • OpenVPN® Certificate: RSA • WireGuard®
Network Management	GDMS, Local Web GUI, CLI (Console, Telnet) and SNMP (v1/ v2c/v3)
Max AP/Clients	Up to 150 GWN APs; Up to 500 Clients
Power and Green Energy Efficiency	Universal power adaptor included: Input 100-240VAC 50-60Hz Output: 48VDC 1A (48W); 4 x PoE out ports IEEE802.3af/at Max. PoE Wattage : 36W
Environmental	Operation: 0°C to 45°C Storage: -30°C to 60°C Humidity: 5% to 95% Non-condensing
Physical	**Unit Dimension:** 191x 101 x 29mm **Unit Weight:** 520g **Entire Package Dimension:** 300 x 130 x 53 mm **Entire Package Weight:** 835g
Package Content	GCC6010/GCC6011, Universal Power Supply, Rack mount kit (Only GCC6011), Quick Installation Guide
Compliance	FCC, CE, RCM, IC

GCC6010W Technical Specifications

Wi-Fi Standards	IEEE 802.11 a/b/g/n/ac/ax
Antennas	3 individual internal antennas (2 x dual band + 1 x Single band 5G) 2.4GHz: maximum gain 4.5dBi 5 GHz: maximum gain 5dBi
Wi-Fi Data Rates	**5G:** IEEE 802.11ax: 7.3 Mbps to 3603 Mbps IEEE 802.11ac: 6.5 Mbps to 2600 Mbps IEEE 802.11n: 6.5 Mbps to 450 Mbps 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: 6.5 Mbps to 300 Mbps IEEE 802.11b: 1, 2, 5.5, 11 Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps *Actual throughput may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment and mix of devices in the network
Frequency Bands	2.4GHz radio: 2400 – 2483.5 MHz (2412-2472MHz are channel central frequency range; 2400-2483.5MHz is Frequency band) 5GHz radio: 5150 - 5895 MHz *Not all frequency bands can be used in all regions
Channel Bandwidth	2.4G: 20 and 40 MHz 5G: 20, 40, 80, 160 MHz
Wi-Fi and System Security	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	2x2 2G/3x3 5G
Maximum TX Power	5G: 25.5dBm 2.4G: 24dBm *Maximum power varies by country, frequency band and MCS rate

Receiver Sensitivity	2.4G
	802.11b: -97dBm@1Mbps, -89dBm@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
	5G
	802.11a: -93dBm @6Mbps, -75dBm @54Mbps;
	802.11n: 20MHz: -73dBm @MCS7; 802.11n 40MHz: -70dBm @MCS7
	802.11ac 20MHz: -70dBm@MCS8; 802.11ac: HT40:- 66dBm @MCS9; 802.11ac 80MHz: -62dBm @MCS9;
	802.11ax 20MHz: -64dBm @ MCS11; 802.11ax 40MHz: -61dBm @MCS11;802.11ax 80MHz: -58dBm @MCS11

Network Ports	5 x Gigabit Ethernet ports
	*All ports are WAN/LAN configurable, max 3 x WAN
Auxiliary Ports	1xMicro-SD, 1xUSB 3.0, 1xReset
Memory	2GB RAM, 32GB eMMC Flash

External Storage	N/A
Router	3Gbps
IPsec VPN Throughput	1Gbps
NAT Sessions	160K
IDS/IPS	900Mbps
PBX	12 users and 4 concurrent calls by default Upgrades available for purchase (See more for PBX capacity upgrade options)
Mounting	Desktop
Material	Plastic Mini-Tower
LEDs	9 x LEDs for device tracking and status indication
Connection Type	DHCP, Static IP, PPPoE, PPTP, L2TP
Network Protocols	IPv4, IPv6, IEEE802.1Q,IEEE 802.1p, IEEE802.1x, IEEE802.3, IEEE 802.3u, IEEE 802.3x,IEEE802.3ab
QoS	VLAN, TOS Support multiple traffic classes, filter by port, IP address, DSCP, and policing App QoS: Application/protocol monitoring and traffic statistics VoIP Prioritization
Firewall	DDNS, Port Forwarding, DMZ, UPnP, DoS & Spoofing defense, traffic rules, NAT, ALG DPI, Anti-Virus, IPS/IDS, SSL deep inspection Content Control: DNS Filtering, Web url/class/content filtering, Application identification and control
VPN	IPsec VPN Client-to-Site / Site-to-Site • IPSec Encryption: 3DES, AES • IPSec Authentication: MD5, SHA-1, SHA2-256 • IPSec Key Exchange: Main/Aggressive Mode, Pre-shared Key, DH Groups 1/2/5/14 • IPSec Protocols: ESP • IPSec NAT Traversal • PPTP VPN Server / Client • PPTP Encrpytion: MPPE 40-bit, 128-bit • PPTP/L2TP Authentication: MS-CHAPv1/2 • L2TP Client-to-Site • OpenVPN® Server / Client • OpenVPN® Encryption: AES, DES • OpenVPN® Authentication: MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512 • OpenVPN® Certificate: RSA • WireGuard®
Network Management	GDMS, Local Web GUI, CLI (Console, Telnet) and SNMP (v1/v2c/v3)
Max AP/Clients	Up to 150 GWN APs; Up to 500 Clients
Power and Green Energy Efficiency	Universal power adaptor included: Input 100-240VAC 50-60Hz Output: 48VDC 1A (48W) PoE: N/A

Environmental	Operation: 0°C to 45°C Storage: -30°C to 60°C Humidity: 5% to 95% Non-condensing
Physical	**Unit Dimension:** 95 x 95 x 193 mm **Unit Weight:** 565g **Entire Package Dimension:** 186 x 127 x 105 mm **Entire Package Weight:** 920g
Package Content	GCC6010W, Universal Power Supply, Quick Installation Guide
Compliance	FCC, CE, RCM, IC

GCC6011 Technical Specifications

Network Ports	2 x 2.5 Gigabit SFP port and 10 x Gigabit Ethernet ports *Fixed 3 x WAN
Auxiliary Ports	1xMicro-SD, 1xUSB 3.0, 1xReset
Memory	2GB RAM, 32GB eMMC Flash
External Storage	Optional, up to 1T M.2 SSD
Router	2.5Gbps
IPsec VPN Throughput	1Gbps
NAT Sessions	160K
IDS/IPS	900Mbps
PBX	12 users and 4 concurrent calls by default Upgrades available for purchase (See more for PBX capacity upgrade options)
Mounting	Desktop/Wall/Rack-mounting
Material	Metal
LEDs	12 x single LEDs and 1 x RGB LED for device tracking and status indication
Connection Type	DHCP, Static IP, PPPoE, PPTP, L2TP
Network Protocols	IPv4, IPv6, IEEE802.1Q,IEEE 802.1p, IEEE802.1x, IEEE802.3, IEEE 802.3u, IEEE 802.3x,IEEE802.3ab
QoS	VLAN, TOS Support multiple traffic classes, filter by port, IP address, DSCP, and policing App QoS: Application/protocol monitoring and traffic statistics VoIP Prioritization
Firewall	DDNS, Port Forwarding, DMZ, UPnP, DoS & Spoofing defense, traffic rules, NAT, ALG DPI, Anti-Virus, IPS/IDS, SSL deep inspection Content Control: DNS Filtering, Web url/class/content filtering, Application identification and control

VPN	• IPsec VPN Client-to-Site / Site-to-Site • IPSec Encryption: 3DES, AES • IPSec Authentication: MD5, SHA-1, SHA2-256 • IPSec Key Exchange: Main/Aggressive Mode, Pre-shared Key, DH Groups 1/2/5/14 • IPSec Protocols: ESP • IPSec NAT Traversal • PPTP VPN Server / Client • PPTP Encrpytion: MPPE 40-bit, 128-bit • PPTP/L2TP Authentication: MS-CHAPv1/2 • L2TP Client-to-Site • OpenVPN® Server / Client • OpenVPN® Encryption: AES, DES • OpenVPN® Authentication: MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512 • OpenVPN® Certificate: RSA • WireGuard®
Network Management	GDMS, Local Web GUI, CLI (Console, Telnet) and SNMP (v1/ v2c/v3)
Max AP/Clients	Up to 150 GWN APs; Up to 500 Clients
Power and Green Energy Efficiency	Universal power adaptor included: Input 100-240VAC 50-60Hz Output: 48VDC 1A (48W) 4 x PoE out ports IEEE802.3af/at Max. PoE Wattage : 36W
Environmental	Operation: 0°C to 45°C Storage: -30°C to 60°C Humidity: 5% to 95% Non-condensing
Physical	**Unit Dimension:** 280 x 180 x 44 mm **Unit Weight:** 1200g **Entire Package Dimension:** 366 x 211 x 53 mm **Entire Package Weight:** 1600g
Package Content	GCC6010/GCC6011, Universal Power Supply, Rack mount kit (Only GCC6011), Quick Installation Guide
Compliance	FCC, CE, RCM, IC

INSTALLATION

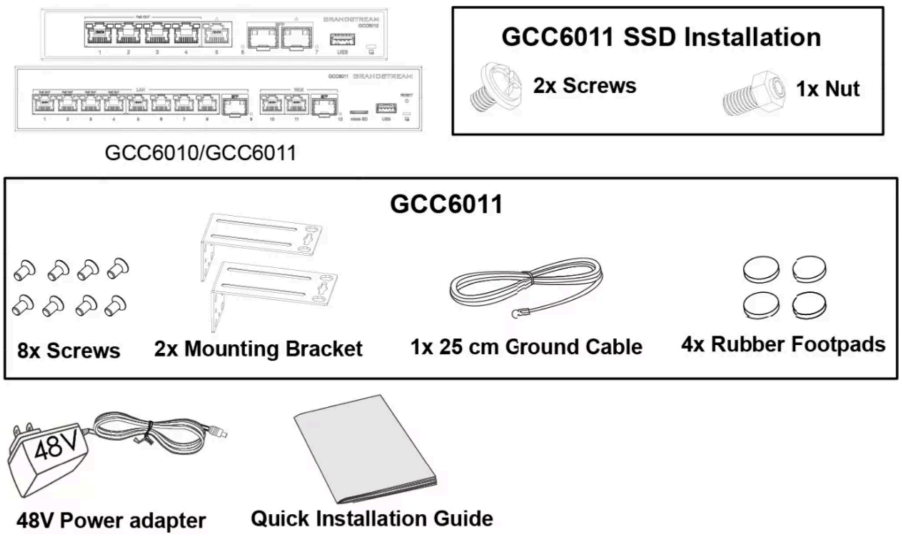
Before deploying and configuring the GCC601X(W) device, the device needs to be properly powered up and connected to the network. This section describes detailed information on the installation, connection, and warranty policy of the GCC601X(W) device.

Package Content

GCC601X(W)	1
Power Adaptor	1
Ethernet Cable	With GCC6010W only.
Rack Mount Kit	with GCC6011 only.

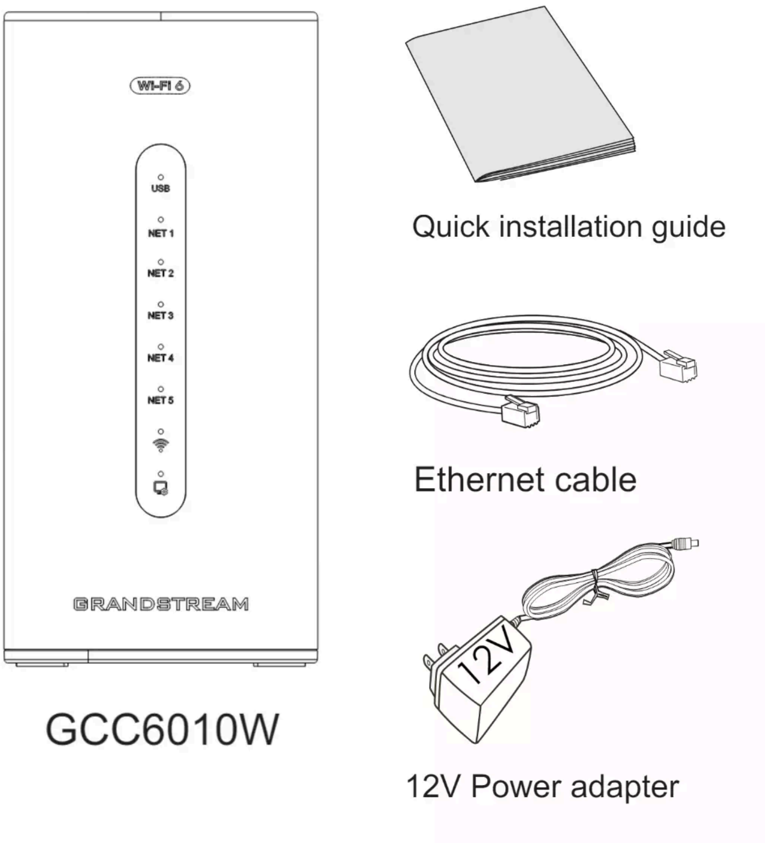
Simplified Quick Installation Guide	1
SSD Installation	2x screws & 1x nut (GCC6011 only).
Ground Cable	with GCC6011 only.
Rubber footpads	with GCC6010/GCC6011 only.

GCC6010/GCC6011 Package Content



GCC6010/GCC6011 Package Content

GCC6010W Package Content



GCC6010W Package Content

Note:

Check the package before installation. If you find anything missing, contact your system administrator.

Connect Your GCC601X(W) Device

Safety Compliances

The GCC601X(W) complies with FCC/CE and various safety standards. The GCC601X(W) power adapter is compliant with the UL standard. Use the universal power adapter provided with the GCC601X(W) package only. The manufacturer's warranty does not cover damages to the device caused by unsupported power adapters.

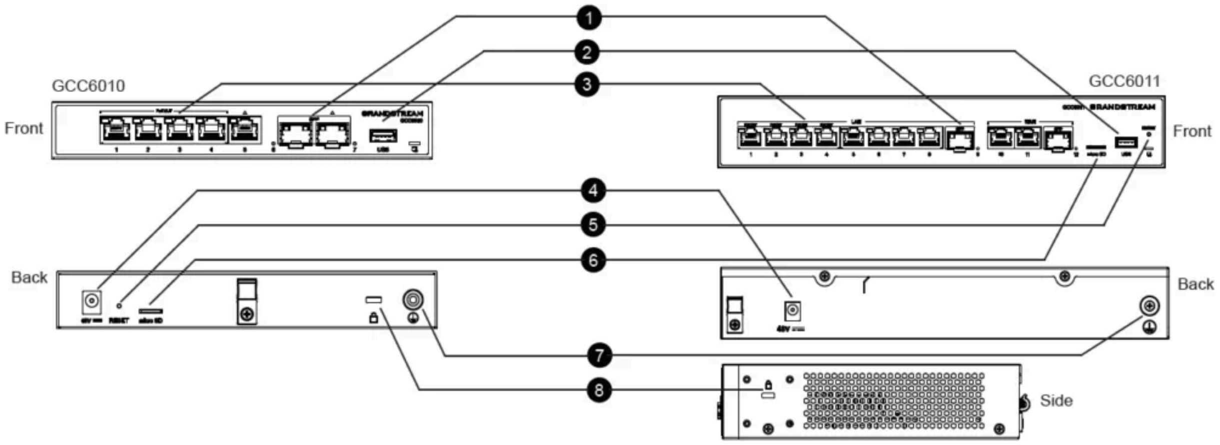
Warranty

If the GCC601X(W) device 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 the warranty policy without prior notification.

Warning

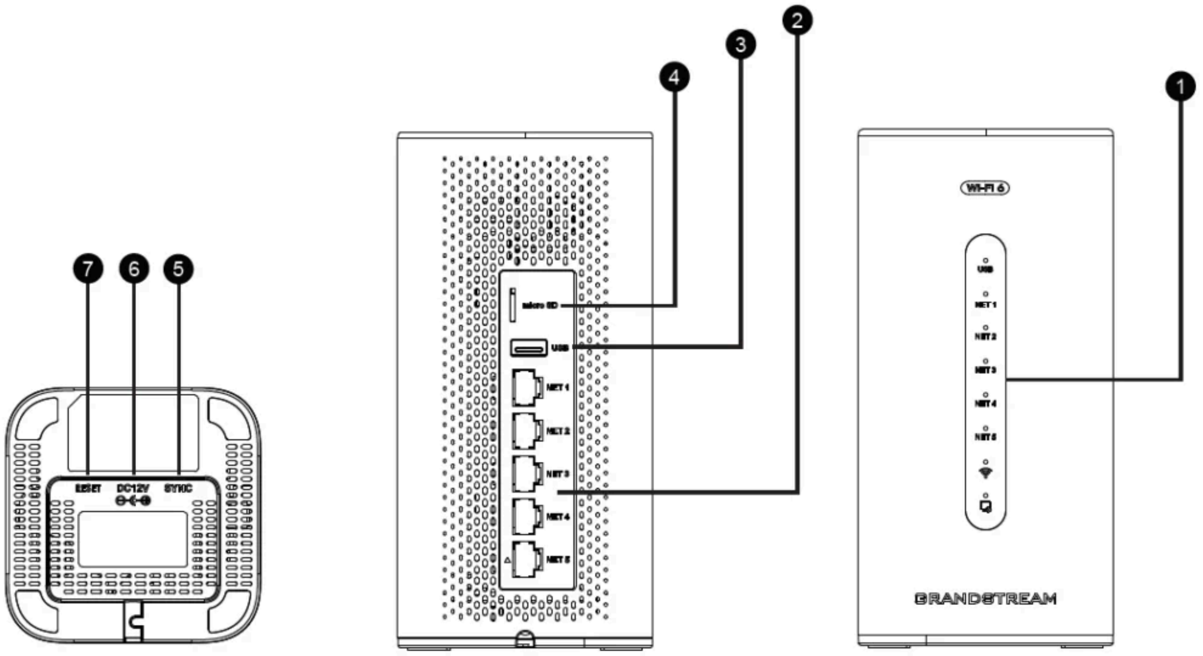
Use the power adapter provided with the GCC601X(W) device. Do not use a different power adapter as this may damage the device. This type of damage is not covered under warranty.

Connecting GCC601X



1	2.5G SFP Port
2	USB 3.0
3	Ethernet Port
4	DC48V
5	RESET
6	Micro SD
7	Ground Terminal
8	Kensington Lock

Connecting GCC6010W

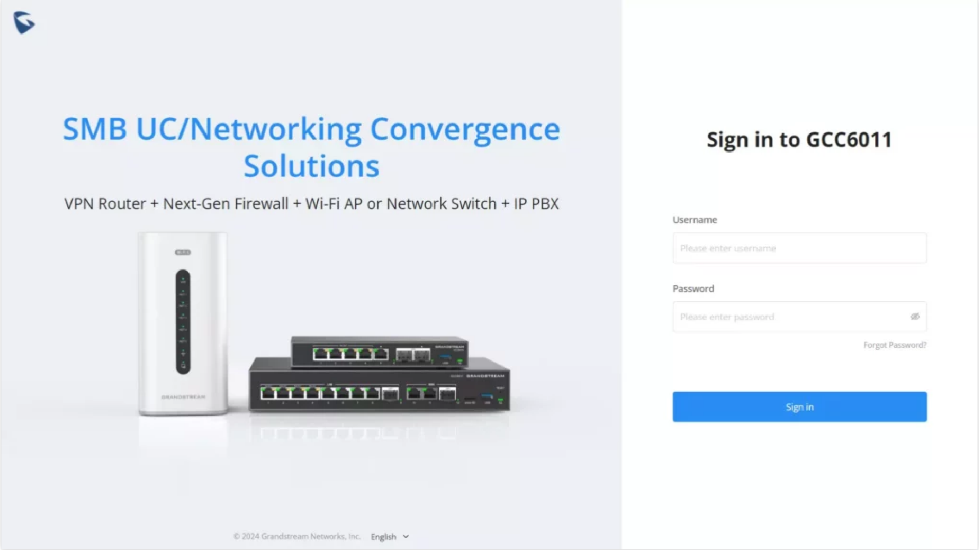


1	LED Indicators
2	NET Ports
3	USB 3.0 Port
4	Micro SD
5	Sync APs Button
6	DC12V
7	RESET Button

1. GCC6010/GCC6011 can be powered on using the right PSU 48VDC 1A (48W) and GCC6010W can be powered by a 12VDC 1.5A power adapter.
2. Connect the WAN port to an optical fiber broadband modem, or ADSL broadband modem.
3. Connect a PC, or laptop to one of the LAN ports for GCC6010 and GCC6011, or connect to SSID (Wi-Fi) only for GCC6010W.

Notes:

- The default password information is printed on the MAC label at the bottom of the unit. The default username is “**admin**”.
- Ports with this symbol △ on GCC6010 are configured to be used as a WAN port by default at the factory.
- The default gateway is 192.168.80.1 (gcc.grandstream.com).

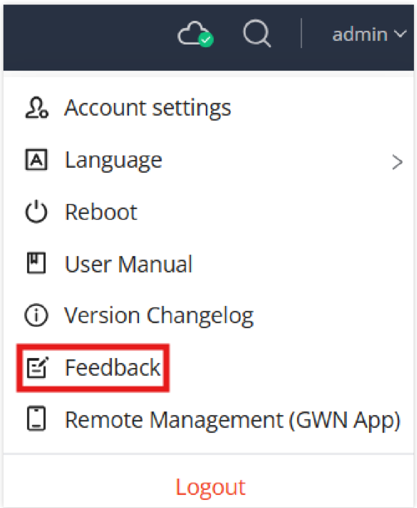

SMB UC/Networking Convergence Solutions
VPN Router + Next-Gen Firewall + Wi-Fi AP or Network Switch + IP PBX
Sign in to GCC6011
Username
Please enter username
Password
Please enter password
Forgot Password?
Sign in
© 2024 Grandstream Networks, Inc.
English

GCC601x(W) login page

Getting Started

Feedback

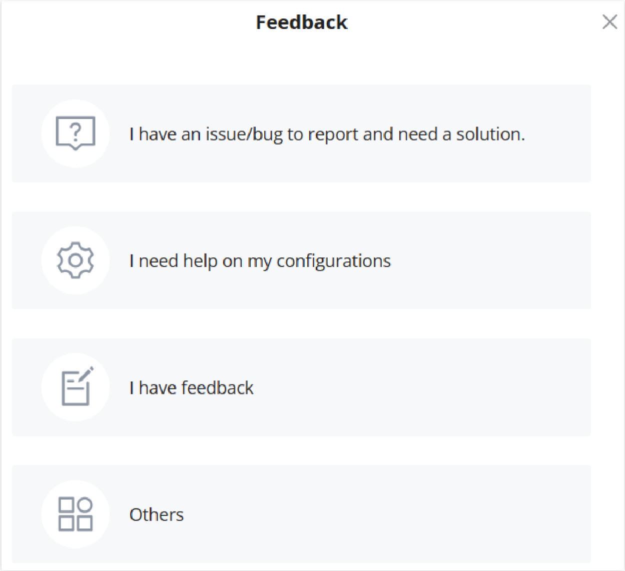
Users can submit feedback directly from the top navigation bar by clicking the **username** in the upper right corner and selecting **Feedback** from the dropdown menu.



Feedback

The feedback system provides four categories to choose from:

- I have an issue/bug to report and need a solution
- I need help on my configurations
- I have feedback
- Others

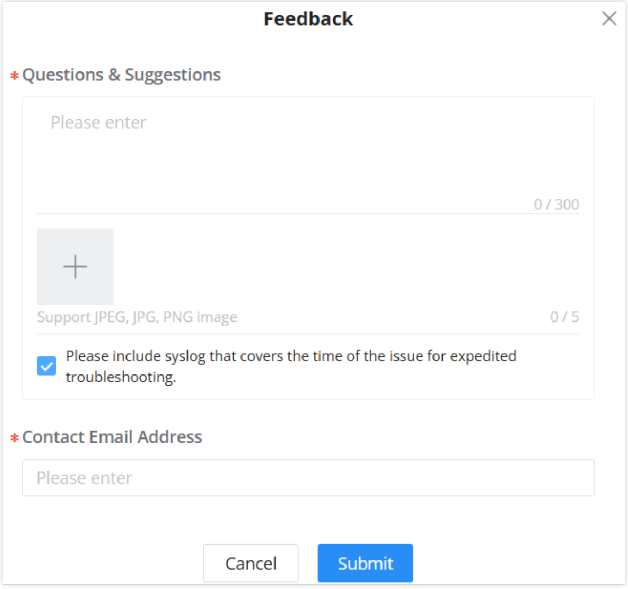


Feedback
I have an issue/bug to report and need a solution.
I need help on my configurations
I have feedback
Others

Feedback

The first two categories will redirect the user to the official help desk support page.

The last two options will open a feedback submission form, allowing users to:



Feedback

* Questions & Suggestions

Please enter

0 / 300

Support JPEG, JPG, PNG image 0 / 5

☑ Please include syslog that covers the time of the issue for expedited troubleshooting.

* Contact Email Address

Please enter

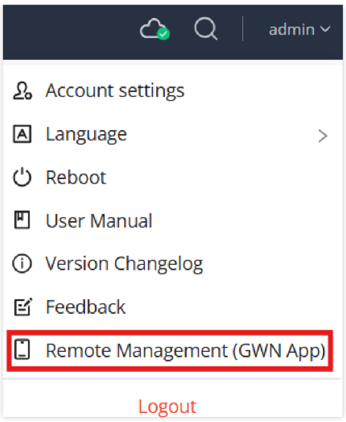
Feedback

- Write a message (up to 300 characters)
- Upload up to 5 images (JPEG, JPG, PNG formats)
- Enter a contact email address
- Optionally include a syslog file to assist with issue diagnosis and troubleshooting

This categorized interface improves the user experience by streamlining support and suggestion handling within the Web UI.

Remote Management (GWN App)

The **Remote Management (GWN App)** option is available from the user menu in the top-right corner of the interface.

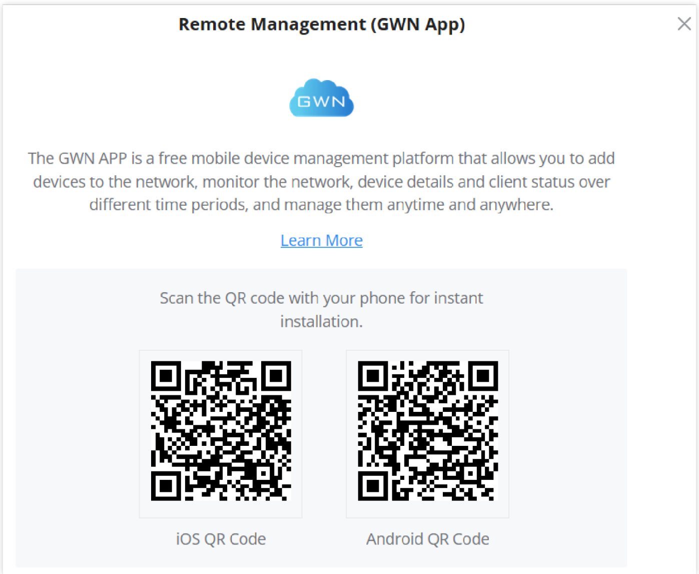


Remote Management (GWN App)

Clicking this option opens a QR code panel for downloading the **GWN mobile app** on iOS or Android.

The GWN App allows users to:

- Remotely manage devices
- Monitor network and device performance
- View client connection history
- Access the network anytime from a mobile device



Remote Management (GWN App)

The GWN APP is a free mobile device management platform that allows you to add devices to the network, monitor the network, device details and client status over different time periods, and manage them anytime and anywhere.

Learn More

Scan the QR code with your phone for instant installation.

Remote Management (GWN App)

HOME

Overview

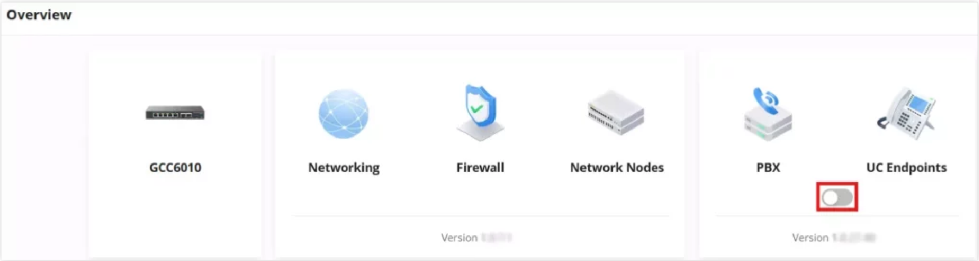
The **Overview** section provides a snapshot of the device’s current operational status and system modules. This includes detailed info such as hardware/software versions, system resource usage, licensing, and session statistics.

Device Modules & Version Panel

The top panel displays the five system modules supported by the GCC6000 series device:

- **Networking**
- **Firewall**
- **Network Nodes**
- **PBX**

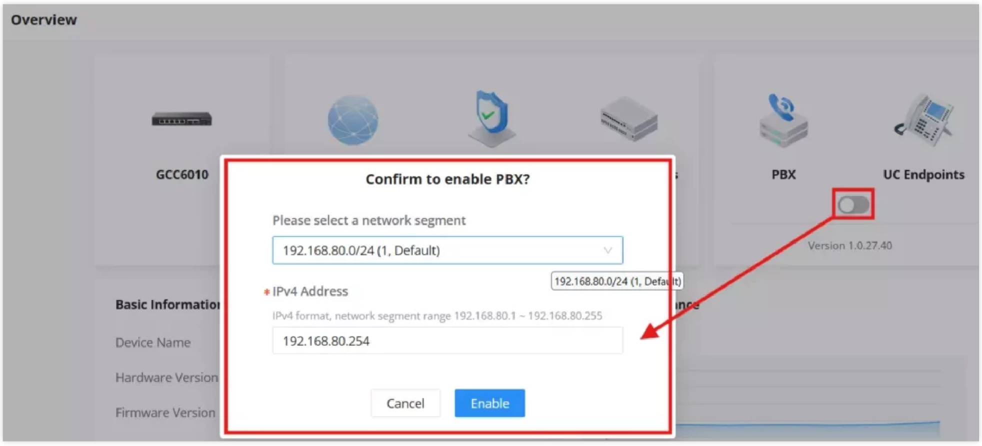
- **UC Endpoints**



Device Modules & Version Panel

PBX and UC Endpoints can be toggled ON/OFF depending on deployment needs. Disabling these modules may help conserve resources for networking functions.

When enabling PBX, users are prompted to assign a **VLAN segment** and specify an **IPv4 address** from the selected range.



Confirm to enable PBX?

Please select a network segment

192.168.80.0/24 (1, Default)

* IPv4 Address

IPv4 format, network segment range 192.168.80.1 ~ 192.168.80.255

192.168.80.254

Device Modules & Version Panel

Device Info & System Performance

This middle panel displays essential system details:

Basic Information

- Device name, MAC, LAN/WAN IP, Part Number, Serial Number
- Uptime and current system time

System Performance

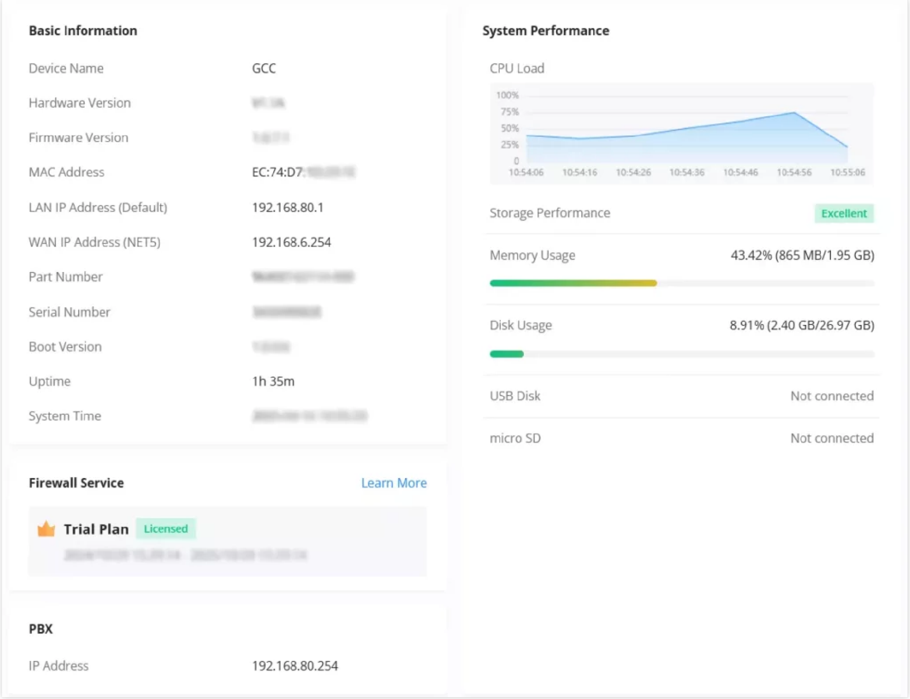
- CPU load graph
- Memory & disk usage
- USB and SD card status

Firewall Service

- Shows current license type and status

PBX

- Displays the current PBX IP address (if enabled)



Basic Information

Device Name	GCC
Hardware Version	[redacted]
Firmware Version	[redacted]
MAC Address	EC:74:D7:[redacted]
LAN IP Address (Default)	192.168.80.1
WAN IP Address (NET5)	192.168.6.254
Part Number	[redacted]
Serial Number	[redacted]
Boot Version	[redacted]
Uptime	1h 35m
System Time	[redacted]

Firewall Service Learn More

Trial Plan Licensed

[redacted]

PBX

IP Address	192.168.80.254

System Performance

CPU Load

Storage Performance	Excellent
Memory Usage	43.42% (865 MB/1.95 GB)
Disk Usage	8.91% (2.40 GB/26.97 GB)
USB Disk	Not connected
micro SD	Not connected

Overview page part 2

Real-Time Session Statistics

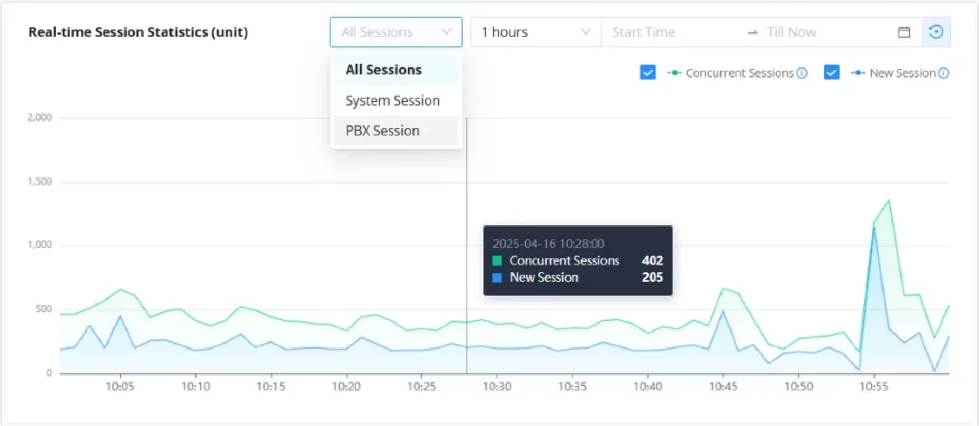
The final section shows a dynamic graph of active sessions in real time.

💡 Features:

- Filter by **All Sessions**, **System Session**, or **PBX Session**
- Choose custom time durations (e.g. 1 hour, 12 hours, etc.)
- View session count by type:
  - **Concurrent Sessions**
  - **New Sessions**
- Hover to reveal stats for any specific timestamp
- Use the ⟳ icon to **reset** the data

Note:

A session refers to a temporary connection or data exchange between devices like loading a webpage, making a call, or streaming data.



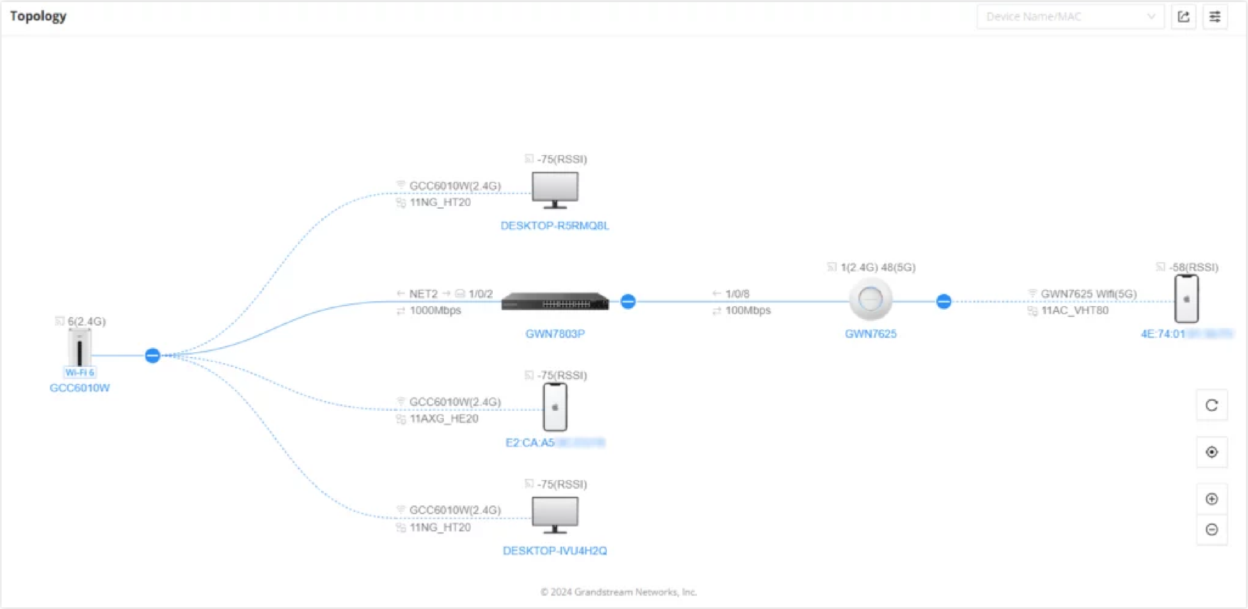
Real-time Session Statistics (unit)

2025-04-16 10:28:00
Concurrent Sessions 402
New Session 205

Overview page part 3

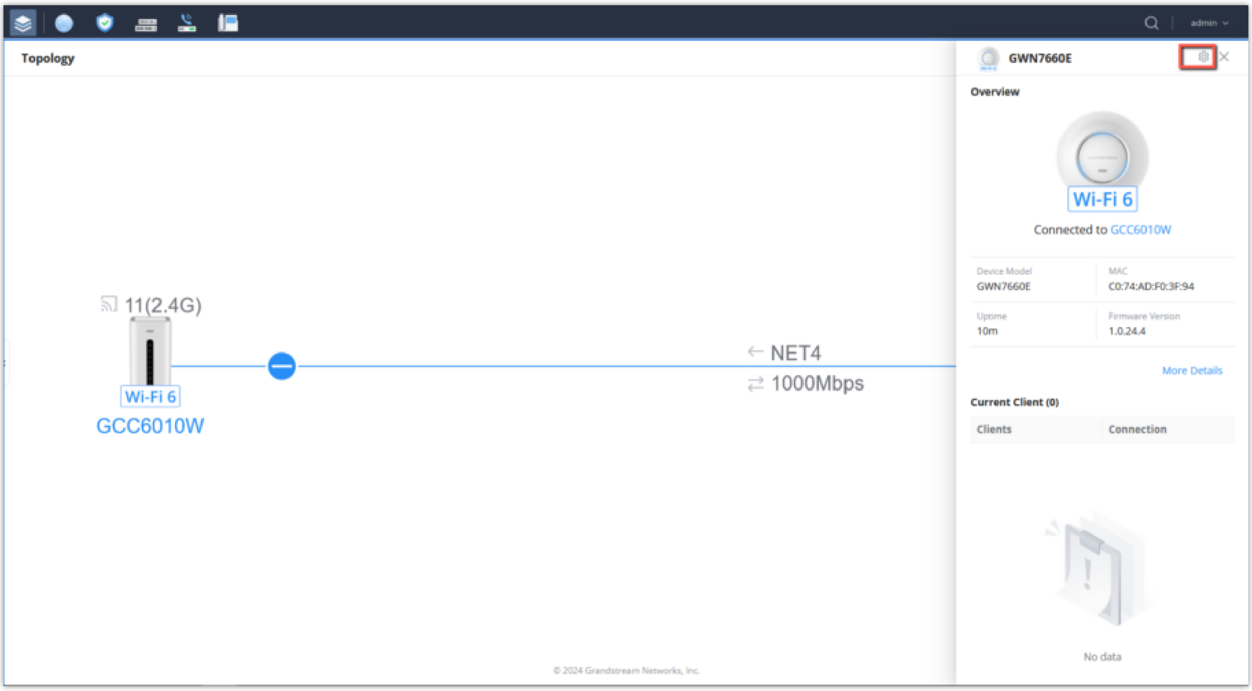
Topology

In this section, the administrator can view the topology of the Grandstream networking device connected to the GCC device.



Topology

When clicking on the highlighted icon below, the user can view the device details and settings



GWN7660E

Overview

Wi-Fi 6

Connected to GCC6010W

Device Model	MAC
GWN7660E	C0:74:AD:F0:3F:94
Uptime	**Firmware Version**
10m	1.0.24.4

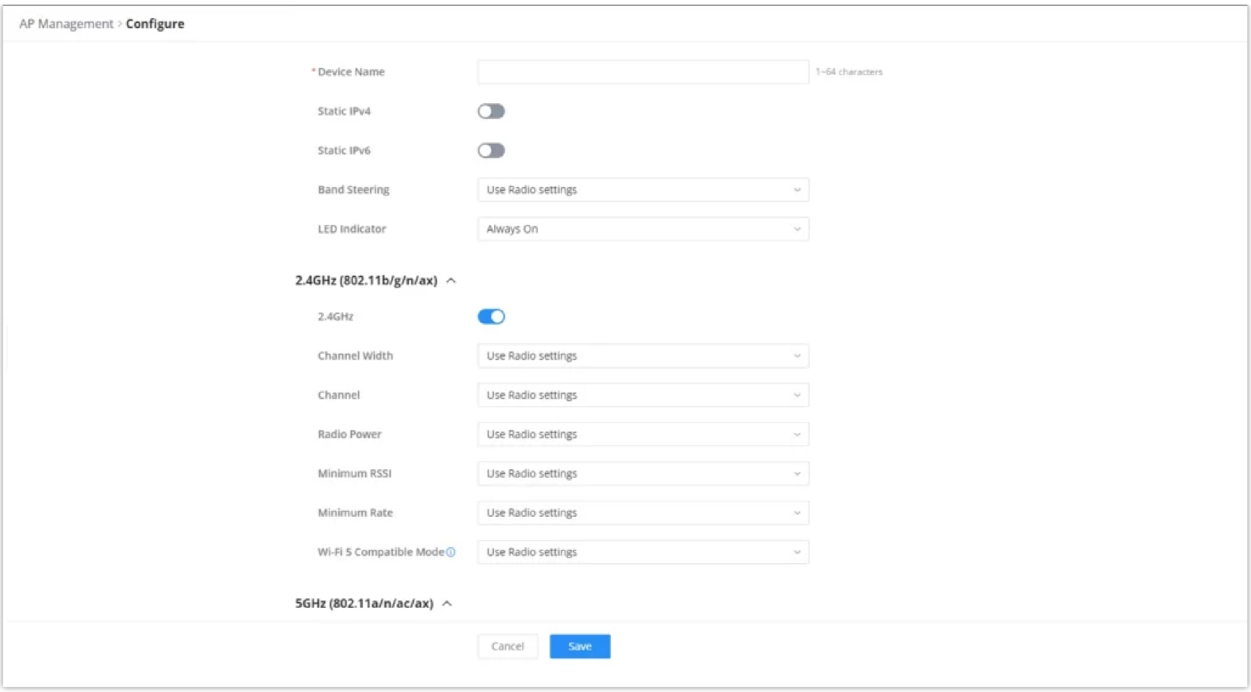
More Details

Current Client (0)

Clients	Connection

No data

Icon View



AP Management › **Configure**

* Device Name	1~64 characters
Static IPv4	○
Static IPv6	○
Band Steering	Use Radio settings
LED Indicator	Always On

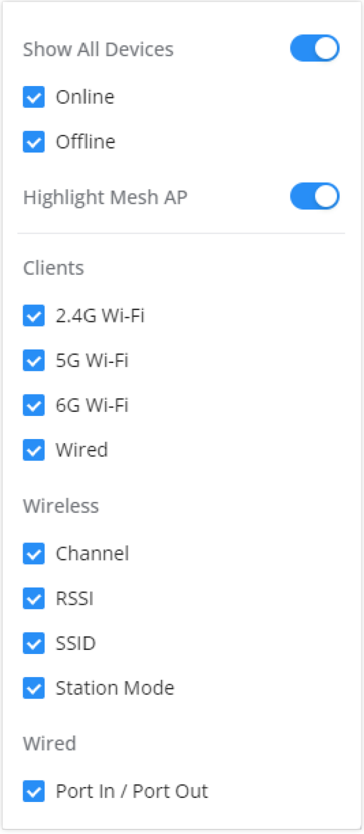
2.4GHz (802.11b/g/n/ax)

2.4GHz	●
Channel Width	Use Radio settings
Channel	Use Radio settings
Radio Power	Use Radio settings
Minimum RSSI	Use Radio settings
Minimum Rate	Use Radio settings
Wi-Fi 5 Compatible Mode	Use Radio settings

5GHz (802.11a/n/ac/ax)

AP Settings

To filter the types of devices that are shown on the topology click on ☰



Show All Devices ●

☑ Online

☑ Offline

Highlight Mesh AP ●

Clients

☑ 2.4G Wi-Fi

☑ 5G Wi-Fi

☑ 6G Wi-Fi

☑ Wired

Wireless

☑ Channel

☑ RSSI

☑ SSID

☑ Station Mode

Wired

☑ Port In / Port Out

Topology Filter

System Settings

In this section, the user can configure settings related to the general operations of the device.

Basic Settings

Basic Settings

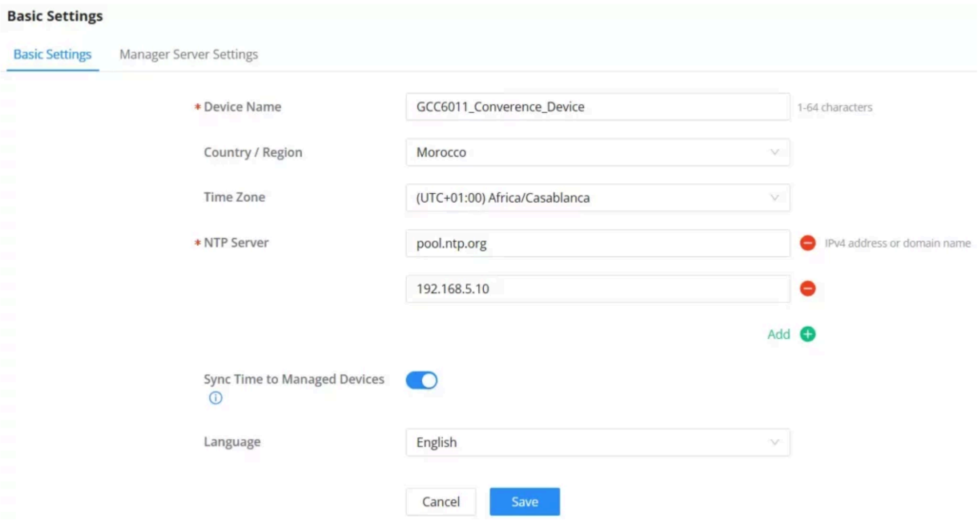
To configure the device's general parameters such as name, time zone, NTP server, and language:

1. Navigate to **System Settings** → **Basic Settings**.
2. Adjust the fields as needed.
3. Click **Save** to apply your changes.

Note:

After a factory reset, the default country is set to Spain and the time zone is set to UTC+00:00 (Etc/Universal).

For more details, refer to the figure and table below.



Basic Settings

Basic Settings | Manager Server Settings

* Device Name: GCC6011_Converence_Device (1-64 characters)

Country / Region: Morocco

Time Zone: (UTC+01:00) Africa/Casablanca

* NTP Server: pool.ntp.org (IPv4 address or domain name)

192.168.5.10

Add

Sync Time to Managed Devices: ●

Language: English

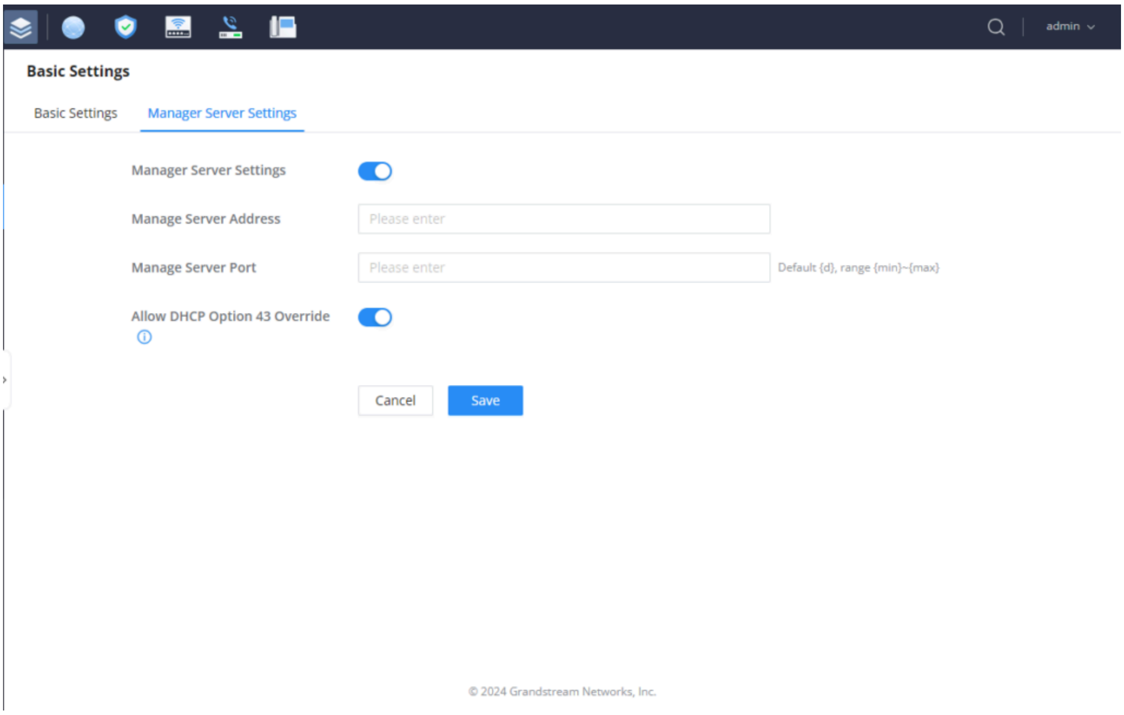
Cancel Save

Basic Settings

Field	Description
Device Name	Sets a unique name to identify the device. Supports 1–64 characters.
Country / Region	Selects the country for localization settings (e.g., default time zones, UI language).
Time Zone	Defines the system time zone. Some locations (e.g., Asuncion, Almaty) use fixed UTC offsets and do not follow DST changes.
NTP Server	Primary server used to synchronize the system time. Enter a domain or IP address.
"+" Add NTP Server	Click the **"+"** icon to add additional NTP servers for redundancy — if one fails, others will be used as backup.
"-"Remove NTP Server	Click the **"-"** icon next to an entry to remove it.
Sync Time to Managed Devices	When enabled, the GCC device will push its NTP-configured time to all managed devices (like APs or switches) for unified time sync.
Language	Sets the web interface display language.

Basic Settings

Manager Server Settings



Basic Settings

Basic Settings | Manager Server Settings

Manager Server Settings: ●

Manage Server Address: Please enter

Manage Server Port: Please enter — Default {d}, range {min}~{max}

Allow DHCP Option 43 Override: ●

Cancel | Save

© 2024 Grandstream Networks, Inc.

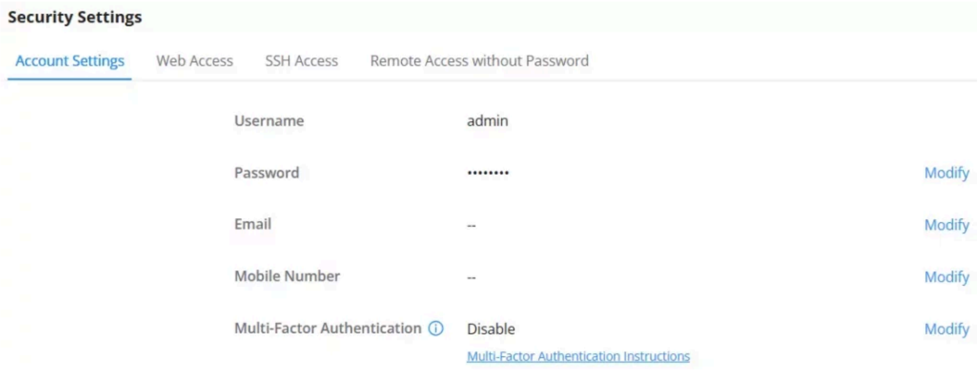
Manager Server Settings

Security Settings

In this section, the user will be able to configure different security-related settings. These settings are mainly related to securing user access to the device either locally or remotely.

Account Settings

This section allows administrators to manage essential login and security details for the web portal access of the GCC device. Users can modify credentials, enable Multi-Factor Authentication (MFA) for enhanced login security, and configure notification details.
For more details, refer to the figure and table below.



Security Settings

Account Settings | Web Access | SSH Access | Remote Access without Password

Username	admin	
Password	••••••••	Modify
Email	--	Modify
Mobile Number	--	Modify
Multi-Factor Authentication	Disable Multi-Factor Authentication Instructions	Modify

Account Settings

Field	**Description**
Username	Displays the default login username (not editable).
Password	Allows updating the administrator login password.
Email	Optional field for system alerts and notifications.
Mobile Number	Optional contact number, used for notifications (where supported).

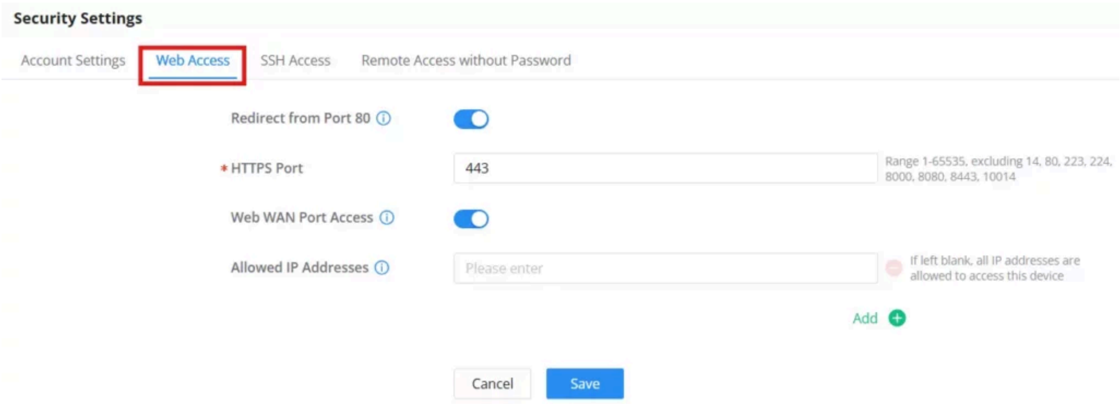
Multi-Factor Authentication	Enables additional login verification using an MFA code. If enabled, users will enter a time-based one-time password (TOTP) after the main login credentials. A setup guide is available through the link shown.
Modify (links)	Use the "Modify" button next to each field to update its value.

Account Settings

Web Access

The **Web Access** tab allows administrators to configure how the GCC6000 device is accessed through the web interface, including WAN accessibility, HTTPS port, and IP restrictions. This helps strengthen remote management security and limit exposure.

For more details, refer to the figure and table below.



Redirect from Port 80 ⓘ

* HTTPS Port: 443

Range 1-65535, excluding 14, 80, 223, 224, 8000, 8080, 8443, 10014

Web WAN Port Access ⓘ

Allowed IP Addresses ⓘ: Please enter

If left blank, all IP addresses are allowed to access this device

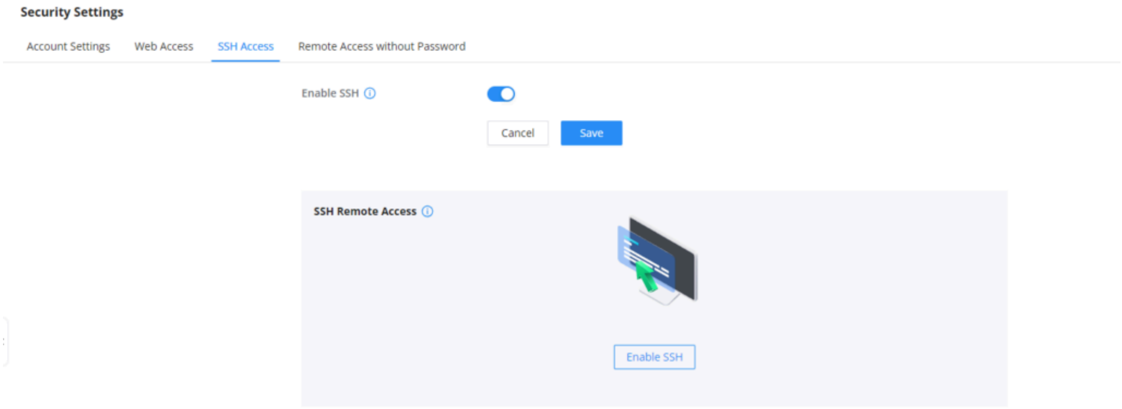
Web Access

Field	**Description**
Redirect from Port 80	Enable or disable redirection from HTTP (port 80) to HTTPS. Disabling this will stop automatic redirect to secure access.
HTTPS Port	Port used for HTTPS web access. Range: 1–65535 (excluding: 14, 80, 223, 224, 8000, 8080, 8443, 10014).
Web WAN Port Access	Allows or restricts web access over the WAN interface.
Allowed IP Addresses	Specify IP addresses allowed to access the web interface via WAN. If left blank, all IP addresses are permitted.

Web Access

SSH Access

In this section, the user can enable SSH remote access to the device, this includes SSH remote access as well.



Security Settings

Account Settings | Web Access | SSH Access | Remote Access without Password

Enable SSH ⓘ ●

Cancel | Save

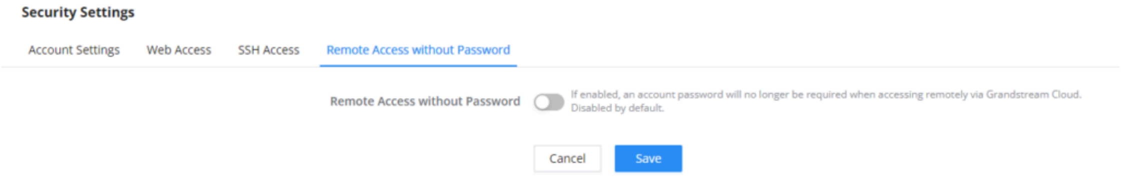
SSH Remote Access ⓘ

Enable SSH

SSH Access

Remote Access without Password

Enabling passwordless remote access allows you to access the device through the GDMS management platform without having to provide a username and password for authentication.



Security Settings

Account Settings | Web Access | SSH Access | Remote Access without Password

Remote Access without Password ○ If enabled, an account password will no longer be required when accessing remotely via Grandstream Cloud. Disabled by default.

Cancel | Save

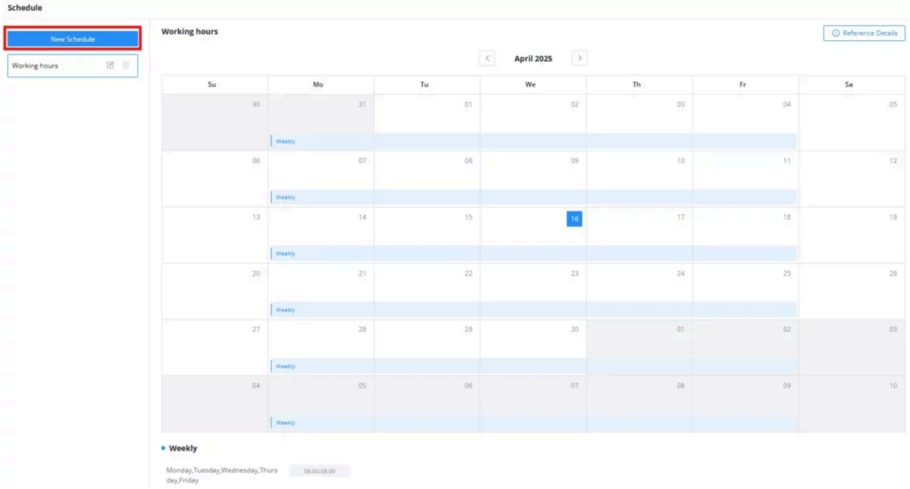
Remote Access without Password

Schedule

The **Schedule** section allows users to create time-based rules that can be applied across various features such as SSID broadcasting, firewall rules, system backups, and more. These schedules help control when specific services or actions should be active.

To configure device schedules, navigate to: **System Settings** → **Schedule**

Click **New Schedule** to begin creating a custom schedule.



Schedule

New Schedule

Working hours

Working hours

ⓘ Reference Details

April 2025

Su	Mo	Tu	We	Th	Fr	Sa
30	31 Weekly	01	02	03	04	05
06	07 Weekly	08	09	10	11	12
13	14 Weekly	15	16	17	18	19
20	21 Weekly	22	23	24	25	26
27	28 Weekly	29	30	01	02	03
04	05 Weekly	06	07	08	09	10

• Weekly

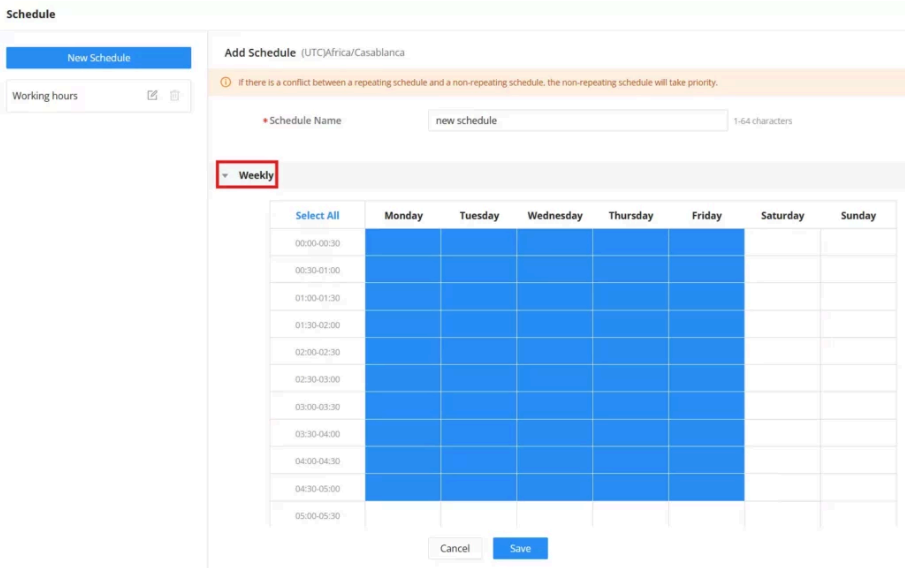
Monday,Tuesday,Wednesday,Thursday,Friday 06:00-08:00

Add a Schedule

When creating a schedule, you can choose between two types:

- **Weekly (repeating)**: Recurs weekly on selected days and times.

- **Absolute (non-repeating)**: Defines one-time actions for specific dates and time slots.



Add Schedule (UTC)Africa/Casablanca

If there is a conflict between a repeating schedule and a non-repeating schedule, the non-repeating schedule will take priority.

*Schedule Name: new schedule — 1-64 characters

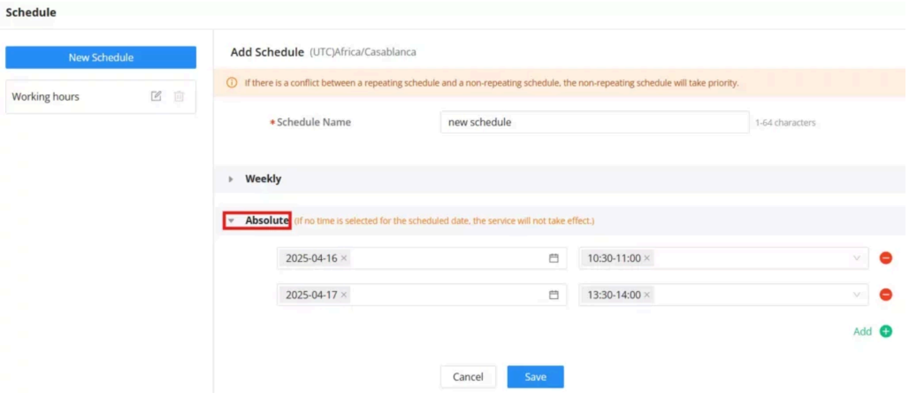
Weekly

Select All	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
00:00-00:30	■	■	■	■	■		
00:30-01:00	■	■	■	■	■		
01:00-01:30	■	■	■	■	■		
01:30-02:00	■	■	■	■	■		
02:00-02:30	■	■	■	■	■		
02:30-03:00	■	■	■	■	■		
03:00-03:30	■	■	■	■	■		
03:30-04:00	■	■	■	■	■		
04:00-04:30	■	■	■	■	■		
04:30-05:00	■	■	■	■	■		
05:00-05:30							

Add a Schedule – Weekly

Note:

- If no time is selected for the scheduled date in an absolute schedule, the service will not take effect
- If both a weekly (repeating) and an absolute (non-repeating) schedule are applied to the same service, the absolute schedule will take priority.



Add Schedule (UTC)Africa/Casablanca

If there is a conflict between a repeating schedule and a non-repeating schedule, the non-repeating schedule will take priority.

*Schedule Name: new schedule — 1-64 characters

Absolute (If no time is selected for the scheduled date, the service will not take effect.)

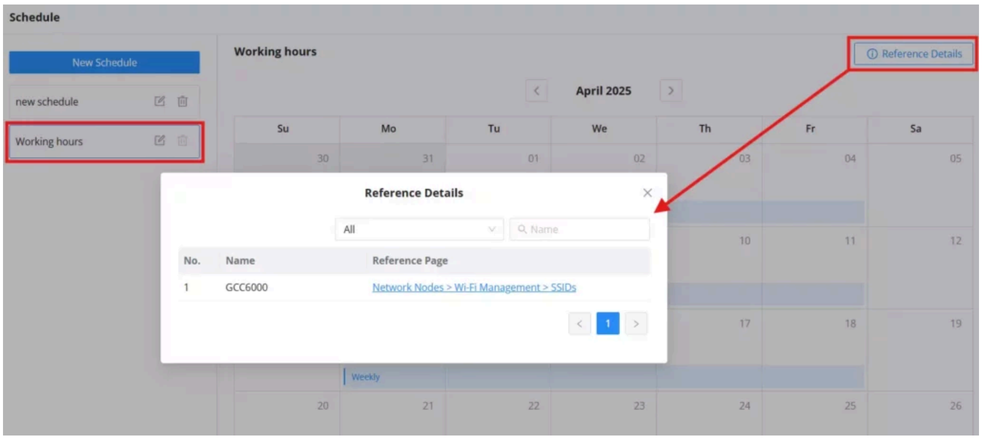
2025-04-16	10:30-11:00
2025-04-17	13:30-14:00

Add a Schedule – Absolute

Users can add time slots per day and save the configuration to make the schedule available for assignment.

Once created, schedules can be applied in various modules. To check where a schedule is currently in use, click **Reference Details**.

The **Reference Details** window shows a list of all modules referencing the selected schedule. This helps prevent accidental deletion of schedules that are actively in use elsewhere.



Reference Details

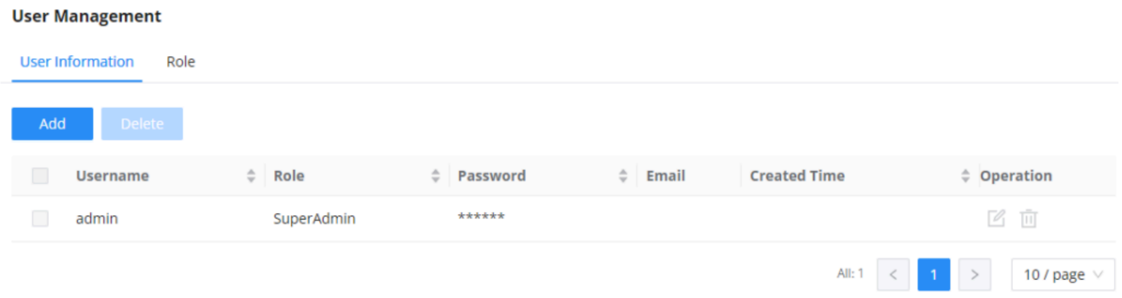
No.	Name	Reference Page
1	GCC6000	Network Nodes > Wi-Fi Management > SSIDs

User Management

User Management allows the user to create users with various roles and privileges.

User Information

In this section, the user can create new users by clicking on the Add button.



User Management

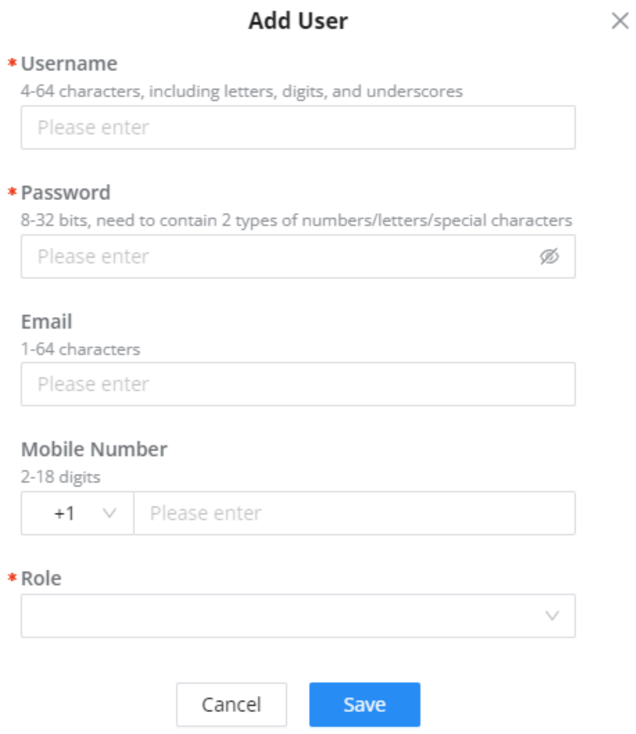
User Information | Role

Add | Delete

☐	Username	Role	Password	Email	Created Time	Operation
☐	admin	SuperAdmin	******			

All: 1 < 1 > 10 / page

User Information



Add User

*Username
4-64 characters, including letters, digits, and underscores
Please enter

*Password
8-32 bits, need to contain 2 types of numbers/letters/special characters
Please enter

Email
1-64 characters
Please enter

Mobile Number
2-18 digits
+1 | Please enter

*Role

Cancel | Save

Add User

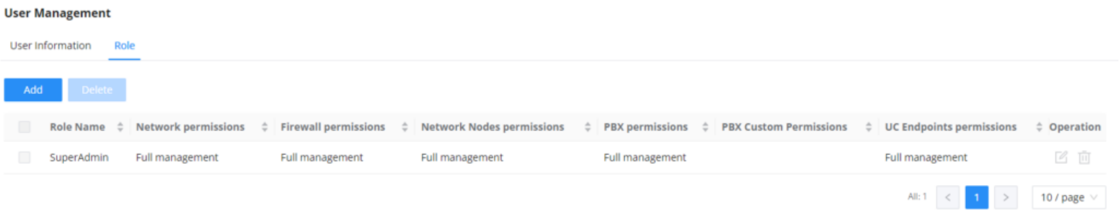
Username	Enter the username. The username can consist of 4-64 characters, including letters, digits, and underscores.
Password	Enter the password. The password can consist of 8-32 characters, need to contain 2 types of numbers/letters/special characters
Email	Enter the email of the user. The email entered should be limited between 1-64 characters
Mobile Number	Enter the mobile number of the user. The phone number is limited between 2-18 digits
Role	Select the role of this user.

	The role must be created first, before it's assigned to the user under

Role

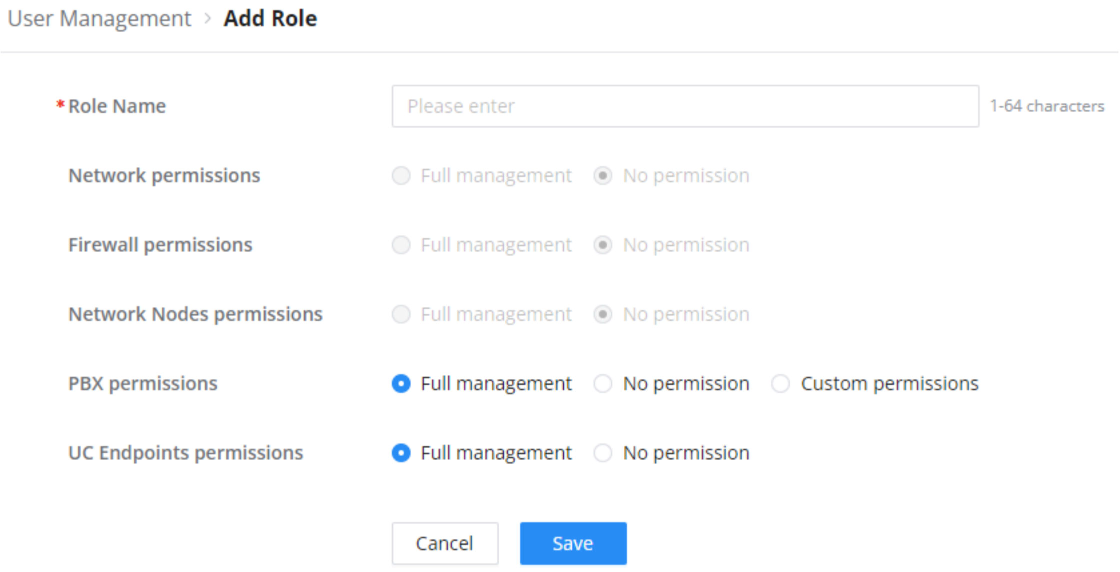
In this section, the user can create roles that can be assigned to different users. By default, the SuperAdmin role is pre-created and assigned to the default administrator account of the device. To create more roles, click on the Add button.

> **Note**
>
> Please note that the SuperAdmin role cannot be assigned to other users. It's an exclusive role for the default user of the device.



□	Role Name	Network permissions	Firewall permissions	Network Nodes permissions	PBX permissions	PBX Custom Permissions	UC Endpoints permissions	Operation
□	SuperAdmin	Full management	Full management	Full management	Full management		Full management	

Role



*Role Name	Please enter	1-64 characters
Network permissions	○ Full management ● No permission	
Firewall permissions	○ Full management ● No permission	
Network Nodes permissions	○ Full management ● No permission	
PBX permissions	● Full management ○ No permission ○ Custom permissions	
UC Endpoints permissions	● Full management ○ No permission	

Add role

Email Settings

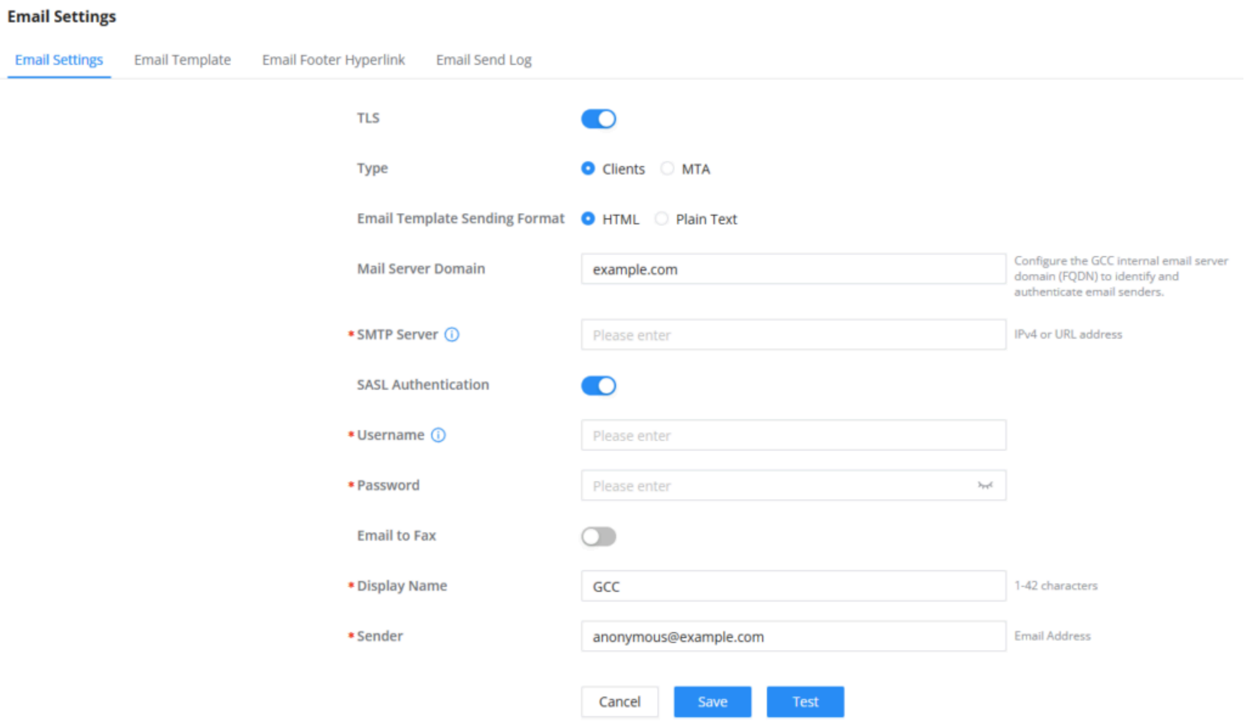
Setting the email client on the GCC60XX device allows the device to send emails directly to users and administrators. For example, when an extension is created on the PBX module and the email is entered in the extension's user information, the user will receive an email stating the information that he/she can use to log into his/her extension.

The email feature is used to send emails for the following types of information:

- **Extension information**
- **Remote registration of an extension**
- **Wave welcome message**
- **Missed calls notifications**
- **Scheduled multimedia meetings**
- **Scheduled meeting reports**
- **Alert events**
- **Emergency calls**
- **Password reset emails**

Email Settings

Configuring email settings on the GCC device allows the sending of notification emails. This deployment of a third-party SMTP server to transfer the emails to the configured email addresses.



TLS: ●

Type: ● Clients ○ MTA

Email Template Sending Format: ● HTML ○ Plain Text

Mail Server Domain: example.com — Configure the GCC internal email server domain (FQDN) to identify and authenticate email senders.

* SMTP Server: Please enter — IPv4 or URL address

SASL Authentication: ●

* Username: Please enter

* Password: Please enter

Email to Fax: ○

* Display Name: GCC — 1-42 characters

* Sender: anonymous@example.com — Email Address

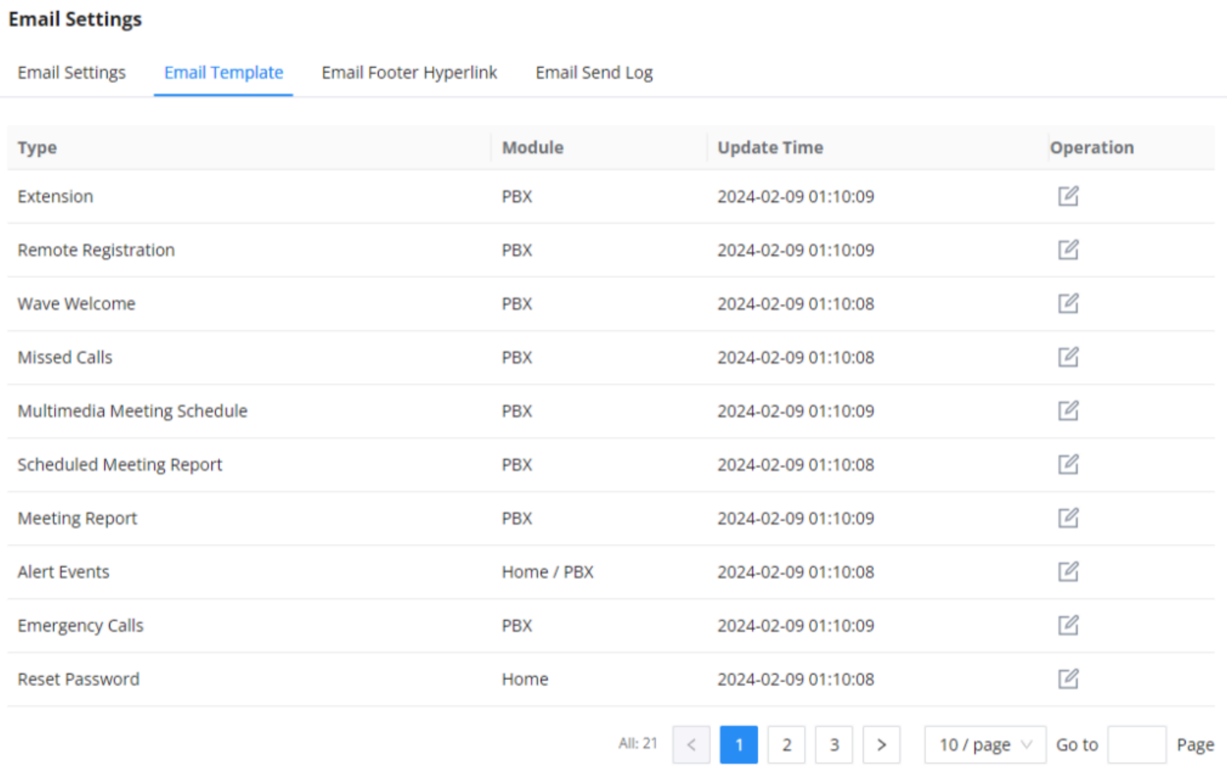
Email Settings

TLS	Enable or disable TLS during transferring/submitting your Email to another SMTP server. The default setting is "Yes".
Type	Select Email Type: ● **MTA**: Mail Transfer Agent. The Email will be sent from the configured domain. When MTA is selected, there is no need to set up SMTP server for it and no user login is required. However, the Emails sent from MTA might be considered as spam by the target SMTP server. ● **Clients:** Submit Emails to the SMTP server. A SMTP server is required, and users need login with correct credentials.
Email Template Sending Format	● **HTML:** The emails will be sent in HTML format. ● **Plain Text:** The emails will be sent as plain text.
Mail Server Domain	Specify the domain name to be used in the Email when using type "MTA".
SMTP Server	Enter the address of the SMTP server when using type "Client". The address can be either an IP address or a FQDN.
SASL Authentication	Enable Simple Authentication and Security Layer. When this option is disabled, the device will not try to use the username and password for mail client authentication. Most of the mail servers require authentication while some other private mail servers allow anonymous login, which requires disabling this option to send email as normal. For Microsoft Exchange Server, please disable this option. **Note:** This option is available when Type is "Clients".
Username	Enter the username created for the SMTP client. **Note:** This option is available when Type is "Clients".

Password	Enter the username created for the SMTP client. **Note:** This option is available when Type is "Clients".
Email To Fax	Monitors the inbox of the configured email address for the specified subject. If enabled, the IPPBX will get a copy of the attachment from the email and send it to the XXX extension by fax. The attachment must be in PDF/TIF/TIFF format. **Note**: This option is available when Type is "Clients".
Email-to-Fax Blocklist/Allowlist	The user can enable the Email-to-Fax Blacklist or Email-to-Fax Whitelist.
Email-to-Fax Subject Format	Select the email subject format to use for emails to fax. ● SendFaxMail To XXX ● XXX XXX refers to the extension that the fax will be sent to. This extension can only contain numbers. **Note**: This option is available when Type is "Clients" and "Email to Fax" is enabled.
Fax Sending Success/Failure Confirmation	Email address blacklist/whitelist for local extensions. **Note**: This option is available when Type is "Clients" and "Email to Fax" is enabled.
POP/POP3 Server Address/Port	Configure the POP/POP3 server address and port for the configured username Example: pop.gmail.com **Note**: This option is available when Type is "Clients" and "Email to Fax" is enabled.
Display Name	Specify the display name in the FROM header in the Email.
Sender	Specify the sender's Email address. For example: pbx@example.mycompany.com.

Email Template

The user can customize the layout of the emails sent by the device to the various users. The device already provides a pre-configured layout that can be modified.



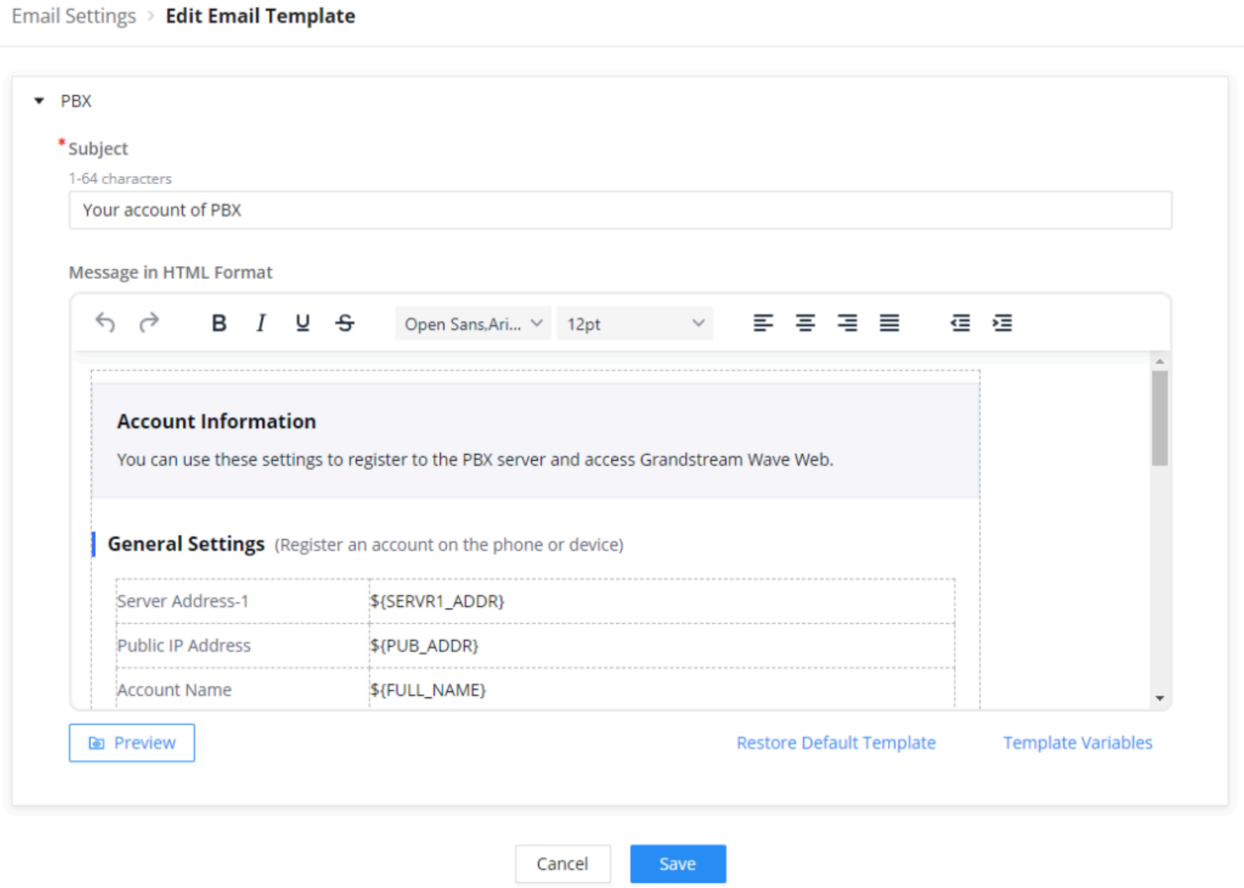
Email Settings

Email Settings | Email Template | Email Footer Hyperlink | Email Send Log

Type	Module	Update Time	Operation
Extension	PBX	2024-02-09 01:10:09	✎
Remote Registration	PBX	2024-02-09 01:10:09	✎
Wave Welcome	PBX	2024-02-09 01:10:08	✎
Missed Calls	PBX	2024-02-09 01:10:08	✎
Multimedia Meeting Schedule	PBX	2024-02-09 01:10:09	✎
Scheduled Meeting Report	PBX	2024-02-09 01:10:08	✎
Meeting Report	PBX	2024-02-09 01:10:09	✎
Alert Events	Home / PBX	2024-02-09 01:10:08	✎
Emergency Calls	PBX	2024-02-09 01:10:09	✎
Reset Password	Home	2024-02-09 01:10:08	✎

Email Template

The user can click on the edit button ✎ to edit a specific template.



Email Settings > **Edit Email Template**

▾ PBX

* Subject

1-64 characters

Your account of PBX

Message in HTML Format

Account Information

You can use these settings to register to the PBX server and access Grandstream Wave Web.

General Settings (Register an account on the phone or device)

Server Address-1	${SERVR1_ADDR}
Public IP Address	${PUB_ADDR}
Account Name	${FULL_NAME}

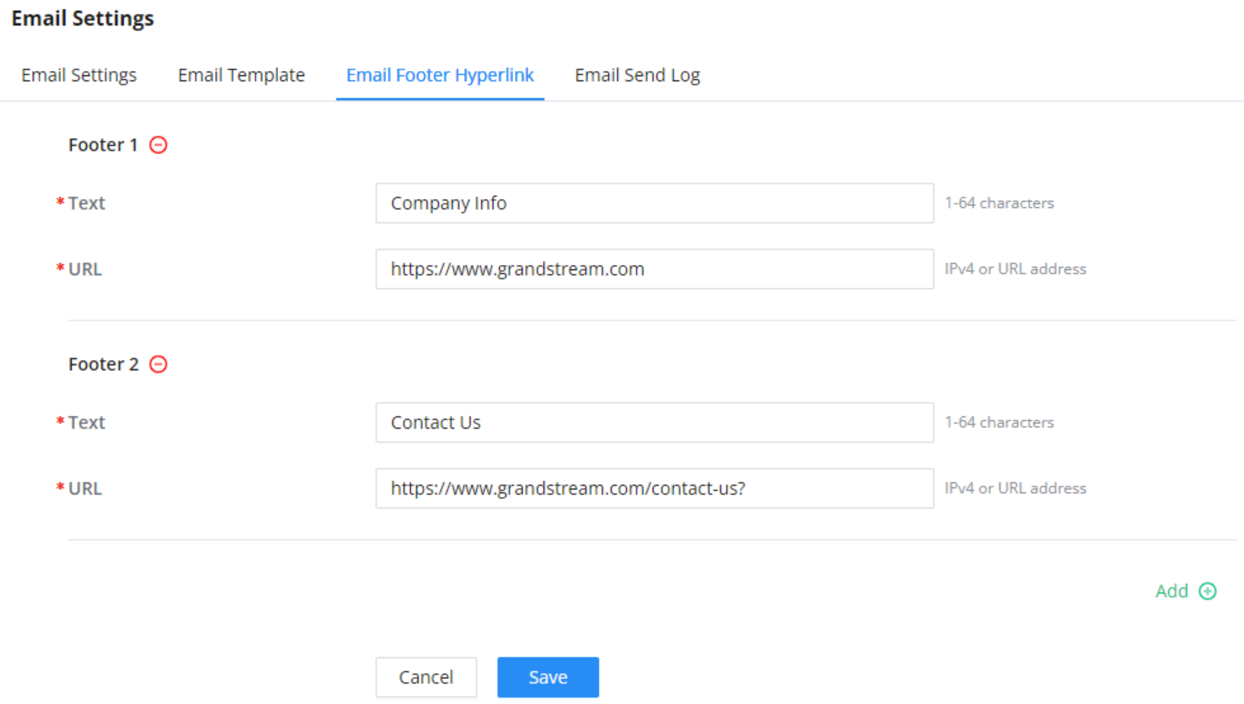
Edit Email Template

The user can use the text editor to change the layout. Once that is done, the user can view the new layout by clicking on Preview.

Email Footer Hyperlink

The customize the links that are included in the footers, please navigate to **System Settings → Email Settings → Email Footer Hyperlink**

On the page, you can edit the text and the URL of each footer. You can add 3 additional footers if needed.



Email Settings

Footer 1 ⊖

* Text: Company Info (1-64 characters)

* URL: https://www.grandstream.com (IPv4 or URL address)

Footer 2 ⊖

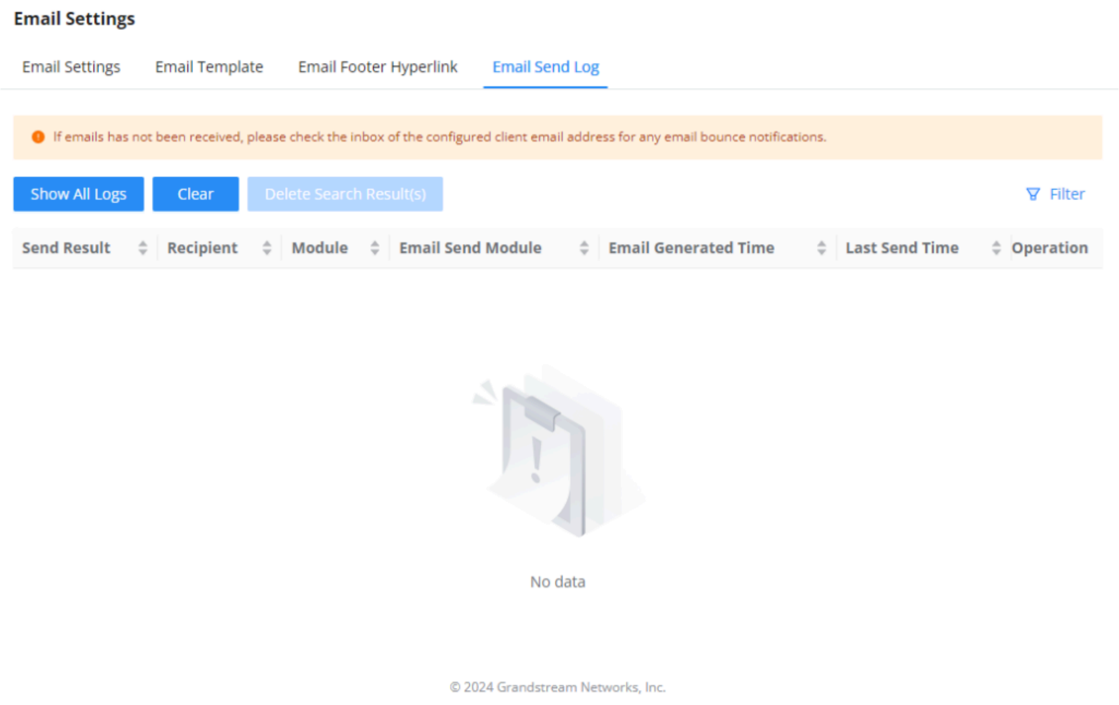
* Text: Contact Us (1-64 characters)

* URL: https://www.grandstream.com/contact-us? (IPv4 or URL address)

Email Footer Hyperlink

Email Send Log

Email send log is used to keep records of all the emails that have been sent from the GCC device.



If emails has not been received, please check the inbox of the configured client email address for any email bounce notifications.

Send Result	Recipient	Module	Email Send Module	Email Generated Time	Last Send Time	Operation

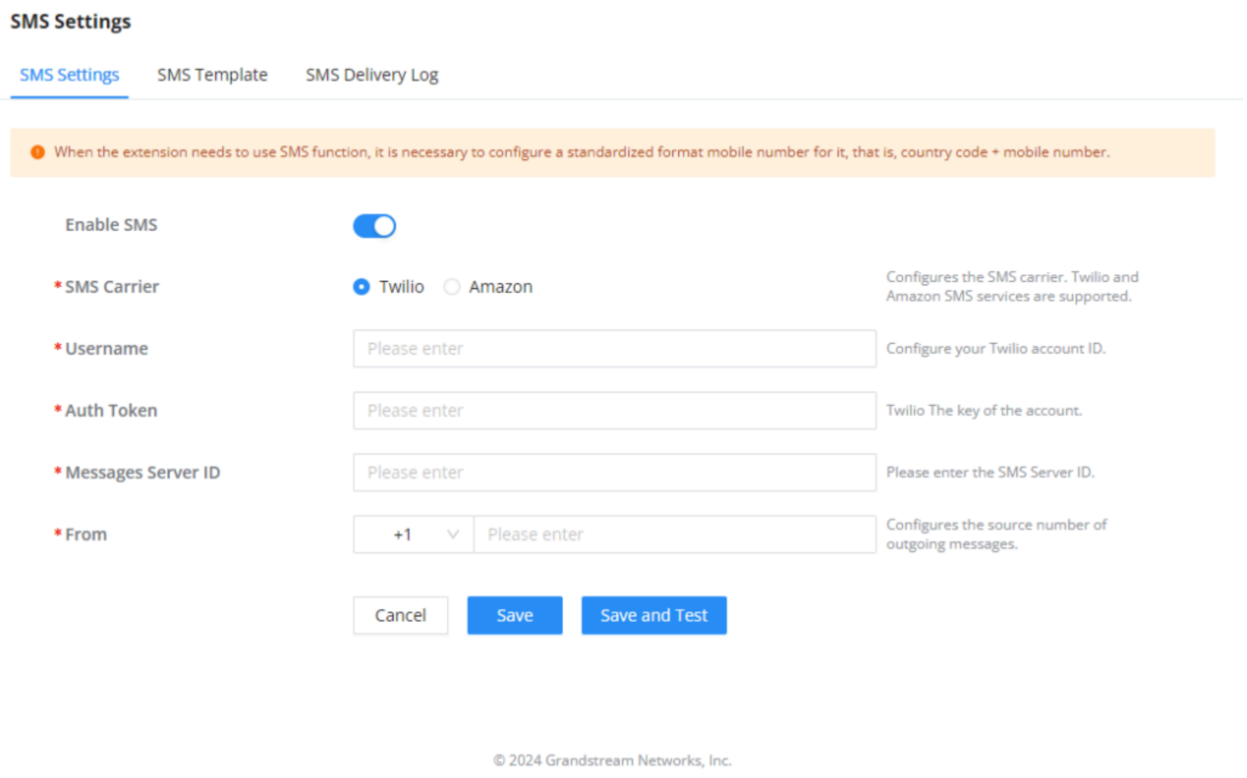
Email Send Log

SMS Settings

The SMS feature allows the user to send information over SMS to mobile numbers. Currently, the information which can be sent over SMS are the following:

- **Profile Code:**
- **Verification Code:**
- **Alarm Notification:**

SMS Settings



SMS Settings

SMS Settings | SMS Template | SMS Delivery Log

When the extension needs to use SMS function, it is necessary to configure a standardized format mobile number for it, that is, country code + mobile number.

Enable SMS	●	
* SMS Carrier	● Twilio ○ Amazon	Configures the SMS carrier. Twilio and Amazon SMS services are supported.
* Username	Please enter	Configure your Twilio account ID.
* Auth Token	Please enter	Twilio The key of the account.
* Messages Server ID	Please enter	Please enter the SMS Server ID.
* From	+1 ⌄ Please enter	Configures the source number of outgoing messages.

SMS Settings

Twilio:

Enable SMS	Toggle the slider to enable/disable SMS service.
SMS Carrier	Select Twilio as the SMS Carrier.
Username	Enter the username of the account of the carrier.
Auth Token	Enter the authentication token generated on the carrier's site.
Message Server ID	Enter the ID of the message server of the carrier.
From	Configure the source number of the outgoing messages.

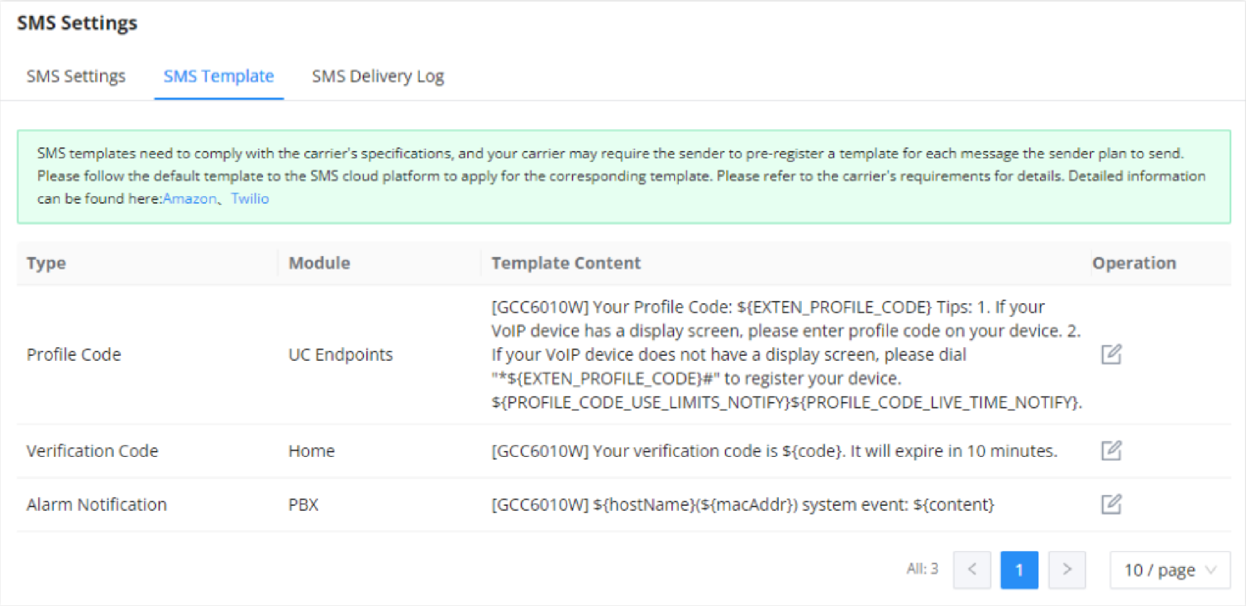
Amazon:

Enable SMS	Toggle the button to enable/disable SMS feature.
SMS Carrier	Choose Amazon as the SMS carrier.
Region	Choose your region. ● US East (N. Virginia) ● US East (Ohio) ● US West (N. California) ● US West (Oregon) ● EU (Ireland) ● EU (London) ● EU (Paris) ● EU (Frankfurt) ● EU (Stockholm) ● EU (Milan) ● Asia Pacific (Hong Kong) ● Asia Pacific (Mumbai)

	- Asia Pacific (Singapore) - Asia Pacific (Sydney) - Asia Pacific (Jakarta) - Asia Pacific (Tokyo) - Asia Pacific (Seoul) - Asia Pacific (Osaka) - South America (Sao Paulo) - China (Beijing) - China (Ningxia) - Canada (Central) - Middle East (Bahrain) - Middle East (UAE) - Africa (Cape Town) - AWS GovCloud (US-West) - AWS GovCloud (US-East) - US ISO East - US ISOB East (Ohio) - US ISO West
Username	Configure your Amazon account ID.
Password	Configure your Amazon account password.

SMS Template

In the “SMS Template” tab, the user can view and edit templates of the SMS messages sent by the GCC device.



SMS Settings

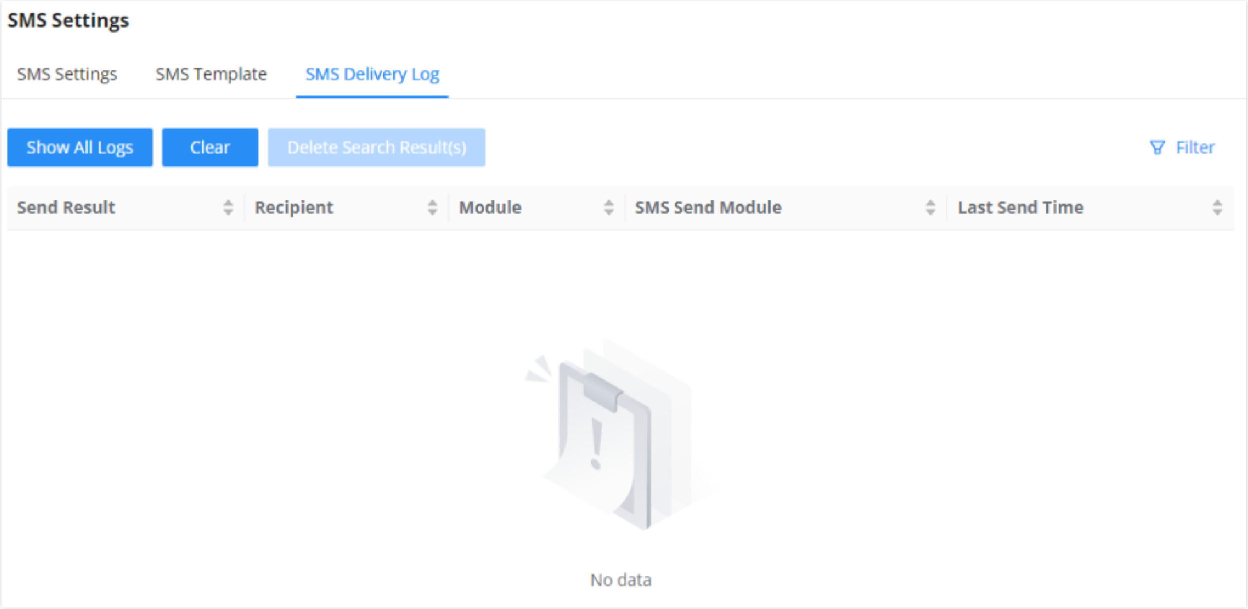
SMS templates need to comply with the carrier's specifications, and your carrier may require the sender to pre-register a template for each message the sender plan to send. Please follow the default template to the SMS cloud platform to apply for the corresponding template. Please refer to the carrier's requirements for details. Detailed information can be found here:Amazon、Twilio

Type	Module	Template Content	Operation
Profile Code	UC Endpoints	[GCC6010W] Your Profile Code: ${EXTEN_PROFILE_CODE} Tips: 1. If your VoIP device has a display screen, please enter profile code on your device. 2. If your VoIP device does not have a display screen, please dial "*${EXTEN_PROFILE_CODE}#" to register your device. ${PROFILE_CODE_USE_LIMITS_NOTIFY}${PROFILE_CODE_LIVE_TIME_NOTIFY}.	✎
Verification Code	Home	[GCC6010W] Your verification code is ${code}. It will expire in 10 minutes.	✎
Alarm Notification	PBX	[GCC6010W] ${hostName}(${macAddr}) system event: ${content}	✎

SMS Template

SMS Delivery Log

The “SMS Delivery Log” tab displays information about all the SMS messages that have originated from the GCC device.



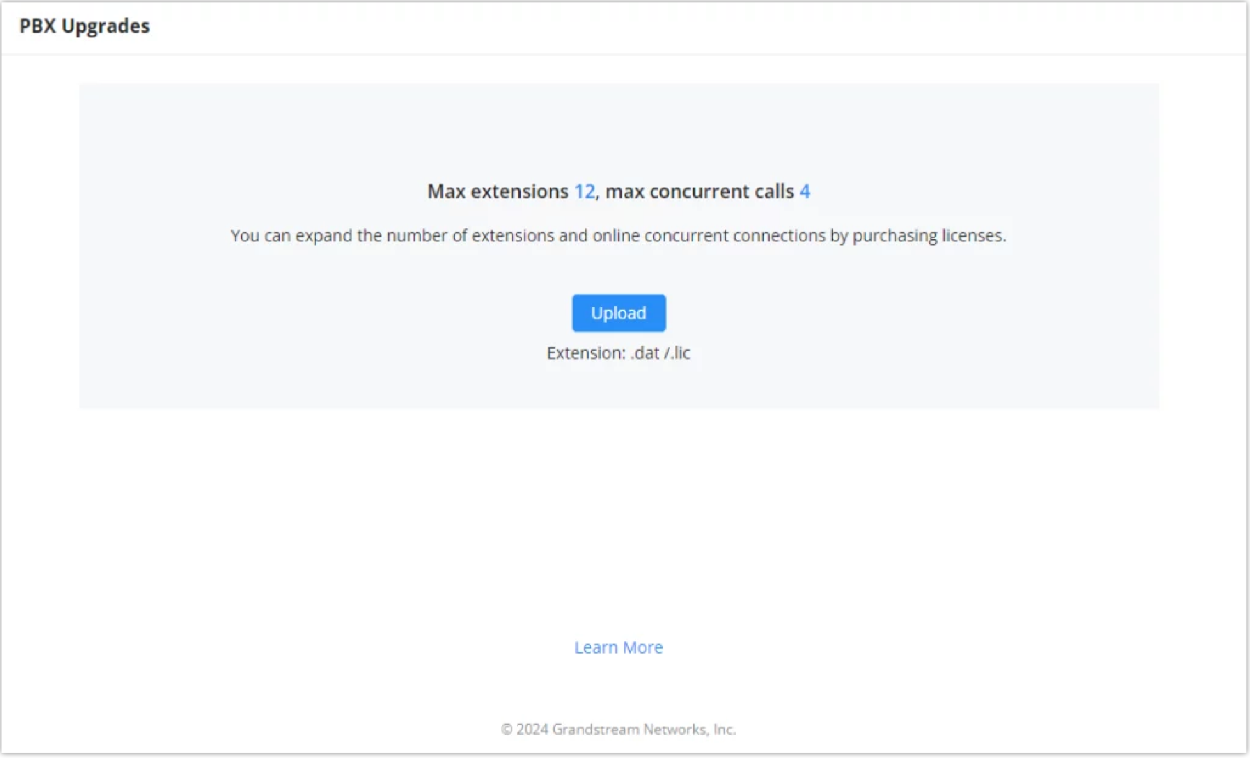
Send Result	Recipient	Module	SMS Send Module	Last Send Time

No data

SMS Delivery Log

PBX Upgrades

On this page, the user can manage the license for upgrading the PBX capabilities of the GCC. When the license file is acquired, the user can upload the license file in this section.



Max extensions 12, max concurrent calls 4

You can expand the number of extensions and online concurrent connections by purchasing licenses.

Extension: .dat /.lic

PBX Upgrades

Note

Please note that only the .dat and .lic files are supported.

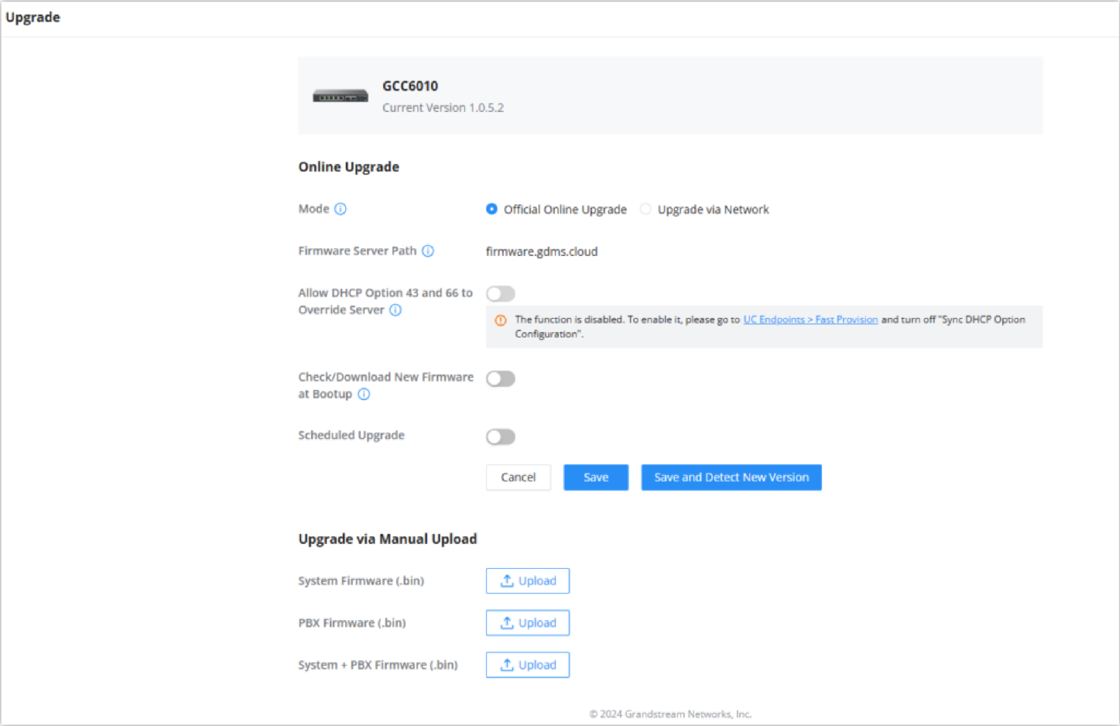
Maintenance

Upgrade

When a new firmware is released for the GCC device, the user can use the “Upgrade” page to update the firmware of the GCC device using different methods of updating the firmware.

There are three methods of upgrading the firmware which are listed below.

- **Official Online Upgrade:** This method allows upgrading directly from the Grandstream firmware server. The administrator can click “Detect New Version” to check for any new firmware releases. When a new firmware version is available, the administrator can proceed with upgrading the device.
- **Allow DHCP Options 43 and 66 to Override Server:** If enabled, DHCP options 66 and 43 will override the upgrade and provisioning settings, if disabled, use the configured server path to request firmware information by default. **Note:** In the official online upgrade mode, “Detect New Version” uses the official default address, and this configuration does not take effect.
- **Check/Download New Firmware at Bootup:** When it is turned on, firmware detection will be performed every time the device is started. If a new firmware version is detected, it will automatically download and upgrade. This option is disabled by default to prevent the device from updating upon booting.
- **Scheduled Upgrade:** Specifies a specific schedule for the device to check for new firmware and install them.
- **Upgrade via Network**: Using this method, the user can choose a specific upgrade method and configure a server address that hosts the firmware files.
- **Upgrade via Manual Upload:** Using this method, the user can upload the firmware file directly on the web UI of the device.



Upgrade

GCC6010
Current Version 1.0.5.2

Online Upgrade

Mode: ● Official Online Upgrade ○ Upgrade via Network

Firmware Server Path: firmware.gdms.cloud

Allow DHCP Option 43 and 66 to Override Server: off

The function is disabled. To enable it, please go to UC Endpoints > Fast Provision and turn off "Sync DHCP Option Configuration".

Check/Download New Firmware at Bootup: off

Scheduled Upgrade: off

Upgrade via Manual Upload

System Firmware (.bin): Upload

PBX Firmware (.bin): Upload

System + PBX Firmware (.bin): Upload

© 2024 Grandstream Networks, Inc.

GCC Upgrade

Important

- When uploading the firmware image to the device, please ensure that you are using the correct firmware image.
- Before upgrading the firmware of the device, please perform a full backup of the configuration of the device to avoid any configuration loss after the upgrade.
- When downgrading to a version that is not compatible with the current system, a factory reset prompt will appear before the process can continue.

Parameter	**Description**
Online Upgrade	
Mode	● **Official Online Upgrade:** Use Grandstream servers to upgrade the device. ● **Upgrade via Network:** Use a specific protocol and server to upgrade the device.

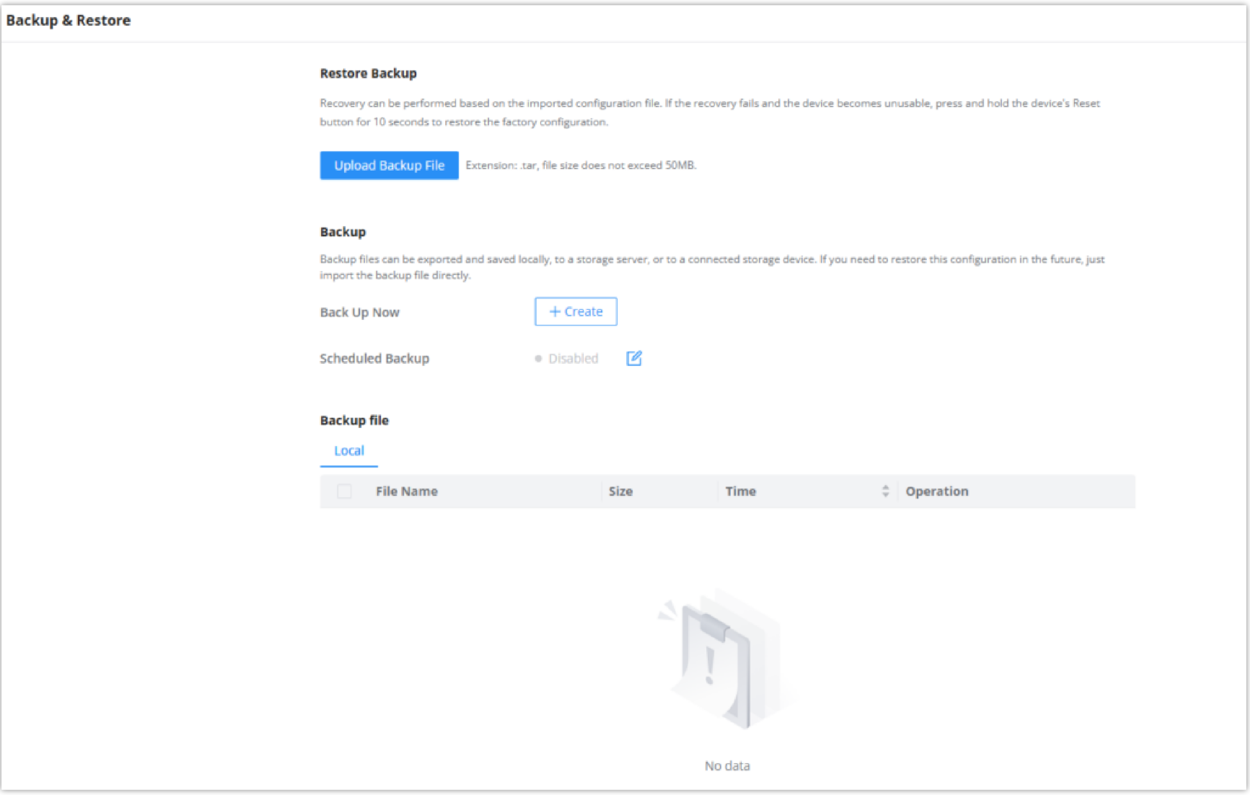
Allow DHCP Option 43 and 66 to Override Server	If enabled, DHCP options 66 and 43 will override the upgrade and provisioning settings. If disabled, use the configured server path to request firmware information by default. **Note:** In the official online upgrade mode, "Detect New Version" uses the official default address, and this configuration does not take effect.
Check/Download New Firmware at Bootup	When it is turned on, firmware detection will be performed every time the device is started. If a new firmware version is detected, it will automatically download and upgrade
Scheduled Upgrade	Enable this option and select the schedule for checking if there is a new firmware version. If a new version is detected, the device will perform the update according to the schedule.
Upgrade via Manual Upload	
System Firmware (.bin)	Upgrade the system's firmware by uploading the firmware image. Only .bin file extensions are allowed.
PBX Firmware (.bin)	Upgrade the PBX's firmware by uploading the firmware image. Only .bin file extensions are allowed.
Firmware (.bin)	Upgrade both the system and PBX firmwares by uploading one firmware file. Only .bin file extensions are allowed.

Backup & Restore

On the “Backup & Restore” page, the user can back up the data of the GCC device manually or using a scheduled backup.

The restore function allows the import of a backup file to restore the GCC.

When backing up the data, the user can choose the data of the GCC modules to be backed up.



Backup & Restore

Restore Backup

Recovery can be performed based on the imported configuration file. If the recovery fails and the device becomes unusable, press and hold the device's Reset button for 10 seconds to restore the factory configuration.

Upload Backup File Extension: .tar, file size does not exceed 50MB.

Backup

Backup files can be exported and saved locally, to a storage server, or to a connected storage device. If you need to restore this configuration in the future, just import the backup file directly.

Back Up Now + Create

Scheduled Backup ● Disabled

Backup file

Local

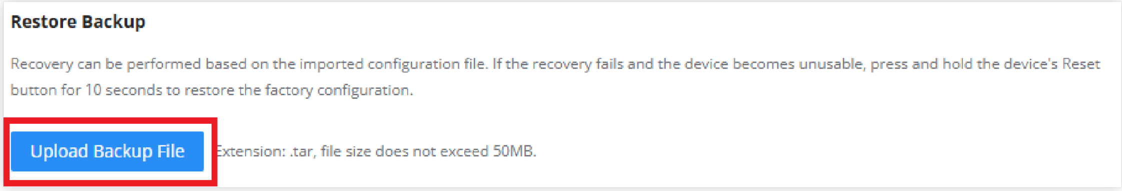
□	File Name	Size	Time	Operation

No data

Backup & Restore

Restore Backup

Press the “Upload Backup File” button to import a previously saved backup file from your computer.



Restore Backup

Recovery can be performed based on the imported configuration file. If the recovery fails and the device becomes unusable, press and hold the device's Reset button for 10 seconds to restore the factory configuration.

Upload Backup File Extension: .tar, file size does not exceed 50MB.

Note:

The backup file should have the extension ".tar" and should not exceed 50 MB.

If the recovery fails and the device becomes unusable, press and hold the device’s Reset button for 10 seconds to restore the factory configuration.

Backup

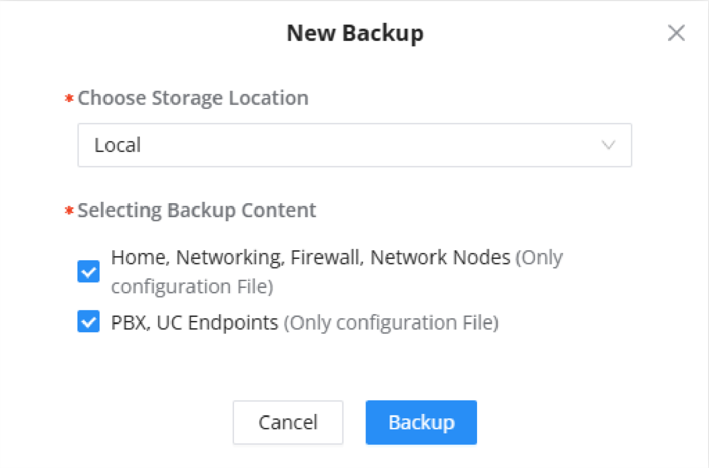
Backup files can be exported and saved locally, to a storage server, or to a connected storage device.

The administration can select the time to back up as follows

Back up Now: Press + Create button to initiate an immediate backup.

1. Choose Storage Location: Local or Storage Server.

- Storage Location: **Local**.



New Backup

* Choose Storage Location: Local

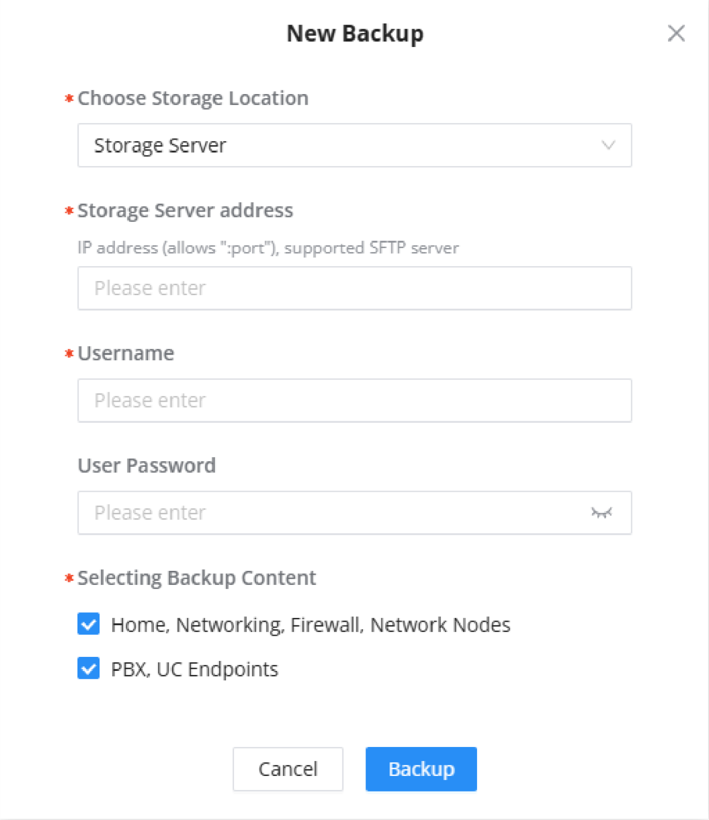
* Selecting Backup Content

☑ Home, Networking, Firewall, Network Nodes (Only configuration File)

☑ PBX, UC Endpoints (Only configuration File)

New Backup – Local

- Storage Location: **Storage Server**.



New Backup

* Choose Storage Location

Storage Server

* Storage Server address

IP address (allows ":port"), supported SFTP server

Please enter

* Username

Please enter

User Password

Please enter

* Selecting Backup Content

☑ Home, Networking, Firewall, Network Nodes

☑ PBX, UC Endpoints

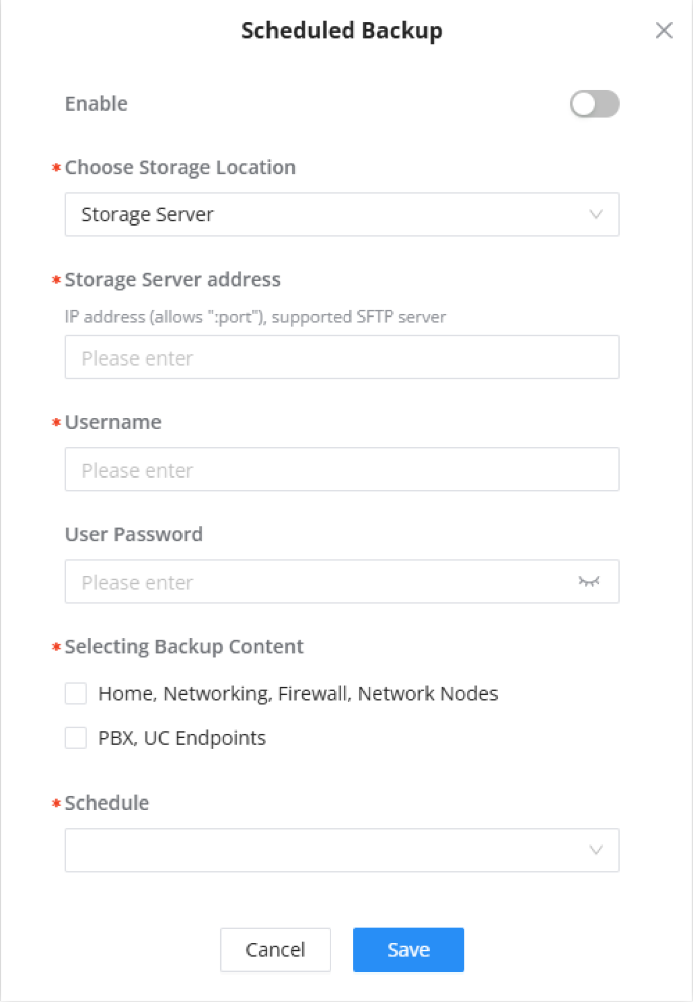
New Backup – Storage Server

Enter the Storage Server Address, Username, and Password.

The storage server must be an SFTP server.

2. Select the backup Content. (Home, Networking, Firewall, Network Node and/or PBX, UC Endpoints).

Scheduled Backup: Press ✎ to create a new backup schedule.



Scheduled Backup

Enable

* Choose Storage Location

Storage Server

* Storage Server address

IP address (allows ":port"), supported SFTP server

* Username

User Password

* Selecting Backup Content

□ Home, Networking, Firewall, Network Nodes

□ PBX, UC Endpoints

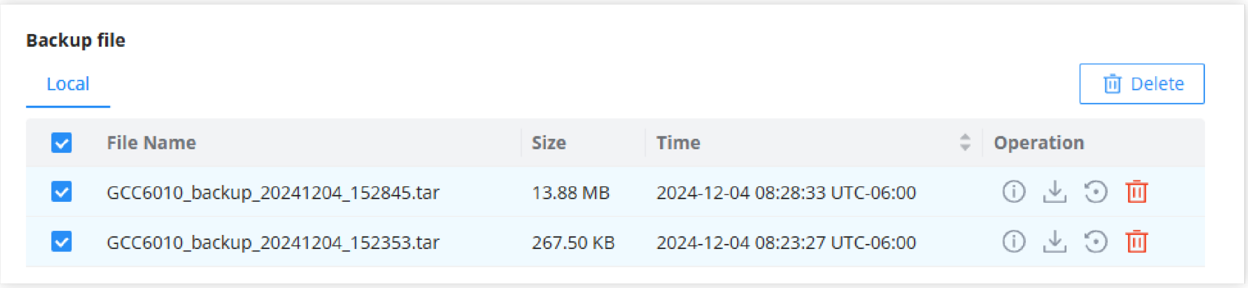
* Schedule

Scheduled Backup

1. Check "Enable" to enable the backup schedule.
2. Choose Storage Location: Storage Server (only)
3. Storage Server Address: Enter the IP address:port of the SFTP server.
4. Username: Enter the SFTP server username.
5. User Password: Enter the SFTP server password.
6. Select the backup content (Home, Networking, Firewall, Network Nodes and/or PBX, UC Endpoints).
7. Schedule: Select a schedule. If no schedule is defined, press the "New Schedule" button to create it.

Only one scheduled backup can be configured.

Backup file: List the local backup files.



Backup file

☑	File Name	Size	Time	Operation
☑	GCC6010_backup_20241204_152845.tar	13.88 MB	2024-12-04 08:28:33 UTC-06:00	ⓘ ⤓ ⟲ 🗑
☑	GCC6010_backup_20241204_152353.tar	267.50 KB	2024-12-04 08:23:27 UTC-06:00	ⓘ ⤓ ⟲ 🗑

Administrators can operate them as follows:

ⓘ: To check the details.

⤓: To download the backup file to a local computer.

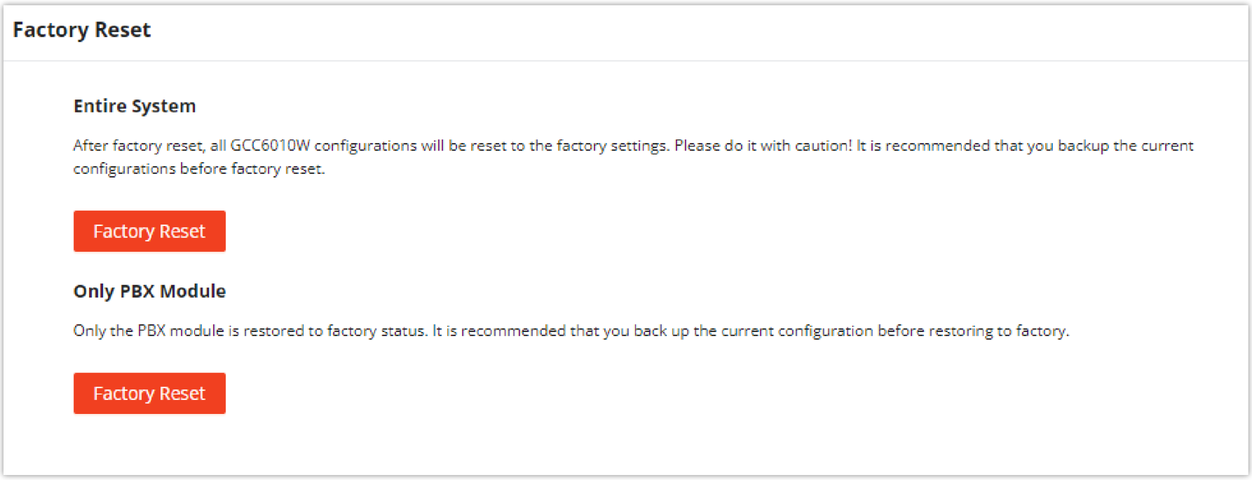
⟲: To restore the local backup file.

🗑: To delete the backup file.

🗑 Delete: Select multiple backup files and batch delete them.

Factory Reset

On this page, the user can perform a factory reset for the entire system. This will delete all the modules' data and configuration which are stored on the local storage of the device. If the user uses the "Factory Reset" button under **Only PBX Module**, only the data and configuration in the PBX module will be deleted. The other modules are not affected by this action.



Factory Reset

Entire System

After factory reset, all GCC6010W configurations will be reset to the factory settings. Please do it with caution! It is recommended that you backup the current configurations before factory reset.

Only PBX Module

Only the PBX module is restored to factory status. It is recommended that you back up the current configuration before restoring to factory.

Factory Reset

Warning

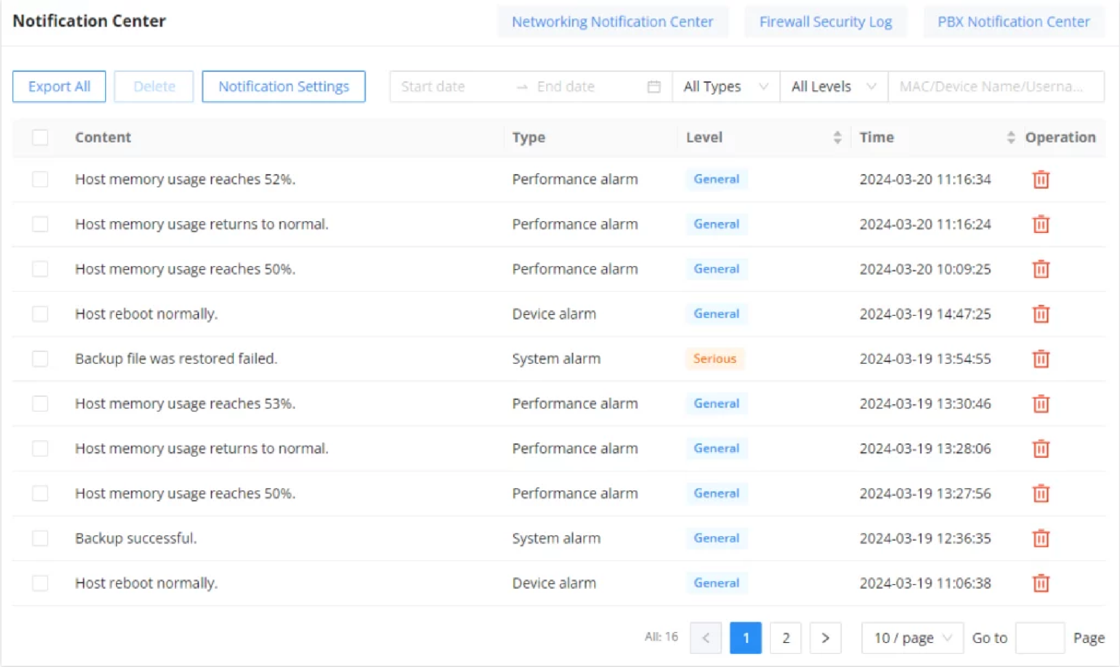
Resetting the device to the factory settings will delete all the data and configuration which are stored on the device. Please proceed with caution as this data cannot be recovered after the factory reset.

Note

Please note that the attached storage such as a USB flash drive or M.2 SSD is not affected when factory-resetting the device.

Notification Center

The Notification Center allows the user to view and configure notifications of the events that occur on the GCC device. To access the notification center, please access the main page of the GCC web UI and then click on the **Notification Center** tab.



Notification Center

Networking Notification Center | Firewall Security Log | PBX Notification Center

Export All | Delete | Notification Settings | Start date → End date | All Types | All Levels | MAC/Device Name/Userna...

□	Content	Type	Level	Time	Operation
□	Host memory usage reaches 52%.	Performance alarm	General	2024-03-20 11:16:34	🗑
□	Host memory usage returns to normal.	Performance alarm	General	2024-03-20 11:16:24	🗑
□	Host memory usage reaches 50%.	Performance alarm	General	2024-03-20 10:09:25	🗑
□	Host reboot normally.	Device alarm	General	2024-03-19 14:47:25	🗑
□	Backup file was restored failed.	System alarm	Serious	2024-03-19 13:54:55	🗑
□	Host memory usage reaches 53%.	Performance alarm	General	2024-03-19 13:30:46	🗑
□	Host memory usage returns to normal.	Performance alarm	General	2024-03-19 13:28:06	🗑
□	Host memory usage reaches 50%.	Performance alarm	General	2024-03-19 13:27:56	🗑
□	Backup successful.	System alarm	General	2024-03-19 12:36:35	🗑
□	Host reboot normally.	Device alarm	General	2024-03-19 11:06:38	🗑

All: 16 < 1 2 > 10 / page Go to Page

Notification Center

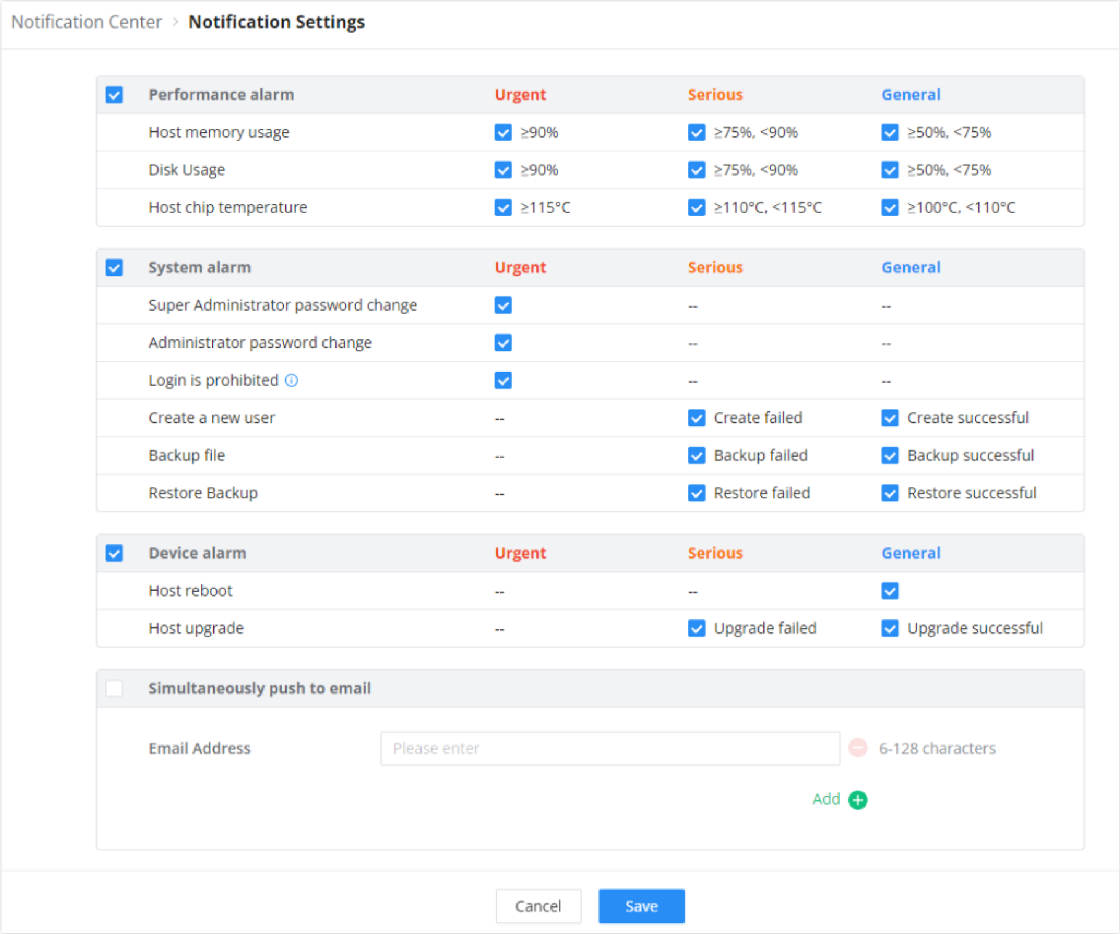
Notification Settings

To set the notifications of the GCC device, click on Notification Settings .

On this page, the user can enable notifications for certain events on the GCC. In addition to generating the notification on the web UI, the user can configure an email address to which email notifications are sent.

Note

To use the email notification feature, please ensure that the Email Settings on the GCC are configured successfully.



Notification Center > **Notification Settings**

☑ Performance alarm	Urgent	Serious	General
Host memory usage	☑ ≥90%	☑ ≥75%, <90%	☑ ≥50%, <75%
Disk Usage	☑ ≥90%	☑ ≥75%, <90%	☑ ≥50%, <75%
Host chip temperature	☑ ≥115°C	☑ ≥110°C, <115°C	☑ ≥100°C, <110°C

☑ System alarm	Urgent	Serious	General
Super Administrator password change	☑	--	--
Administrator password change	☑	--	--
Login is prohibited ⓘ	☑	--	--
Create a new user	--	☑ Create failed	☑ Create successful
Backup file	--	☑ Backup failed	☑ Backup successful
Restore Backup	--	☑ Restore failed	☑ Restore successful

☑ Device alarm	Urgent	Serious	General
Host reboot	--	--	☑
Host upgrade	--	☑ Upgrade failed	☑ Upgrade successful

□ Simultaneously push to email

Email Address: Please enter ⊖ 6-128 characters

Add ⊕

Cancel | Save

Notification Settings

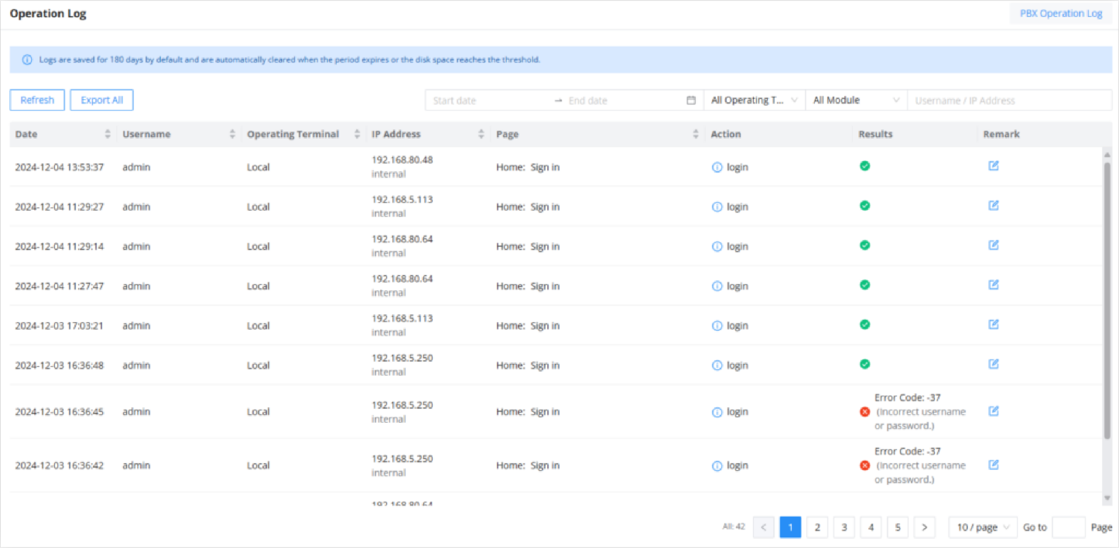
Logs & Diagnostics

Operation Log

The Operation Log page provides administrators with a comprehensive overview of all logged operations, offering detailed information about each activity. This feature ensures transparency and allows administrators to monitor, analyze, and manage system activities effectively.

> **Note:**
>
> Logs are saved for 180 days by default and are automatically cleared when the period expires or the disk space reaches the threshold.

From this page, the administrator can monitor system operations, including login actions and their outcomes (success or failure), date/time, IP address, username, and Page. Additionally, the administrator can add remarks for each action by editing the remark column using the provided button ✎.



Operation Log

PBX Operation Log

ⓘ Logs are saved for 180 days by default and are automatically cleared when the period expires or the disk space reaches the threshold.

Date	Username	Operating Terminal	IP Address	Page	Action	Results	Remark
2024-12-04 13:53:37	admin	Local	192.168.80.48 internal	Home: Sign in	ⓘ login	✓	✎
2024-12-04 11:29:27	admin	Local	192.168.5.113 internal	Home: Sign in	ⓘ login	✓	✎
2024-12-04 11:29:14	admin	Local	192.168.80.64 internal	Home: Sign in	ⓘ login	✓	✎
2024-12-04 11:27:47	admin	Local	192.168.80.64 internal	Home: Sign in	ⓘ login	✓	✎
2024-12-03 17:03:21	admin	Local	192.168.5.113 internal	Home: Sign in	ⓘ login	✓	✎
2024-12-03 16:36:48	admin	Local	192.168.5.250 internal	Home: Sign in	ⓘ login	✓	✎
2024-12-03 16:36:45	admin	Local	192.168.5.250 internal	Home: Sign in	ⓘ login	✗ Error Code: -37 (Incorrect username or password.)	✎
2024-12-03 16:36:42	admin	Local	192.168.5.250 internal	Home: Sign in	ⓘ login	✗ Error Code: -37 (Incorrect username or password.)	✎
			192.168.80.64				

Operation Log

The administrator can utilize filters to quickly find the needed information.

The supported filters are:

- Date: Specify a Start date and End date to narrow down results.
- Operation Terminal: Choose from All Operation Terminals, Local, GDMS Networking, Manager, or CLI.
- Module: Filter by specific module such as All Modules, Home, Networking, Firewall, or Network Nodes.
- Username / IP Address: Enter the username or IP address for precise filtering.

> **Notes:**
>
> - The filters can be combined for better results.
> - Click PBX Operation Log on the top right corner to access the PBX Operation Log module.

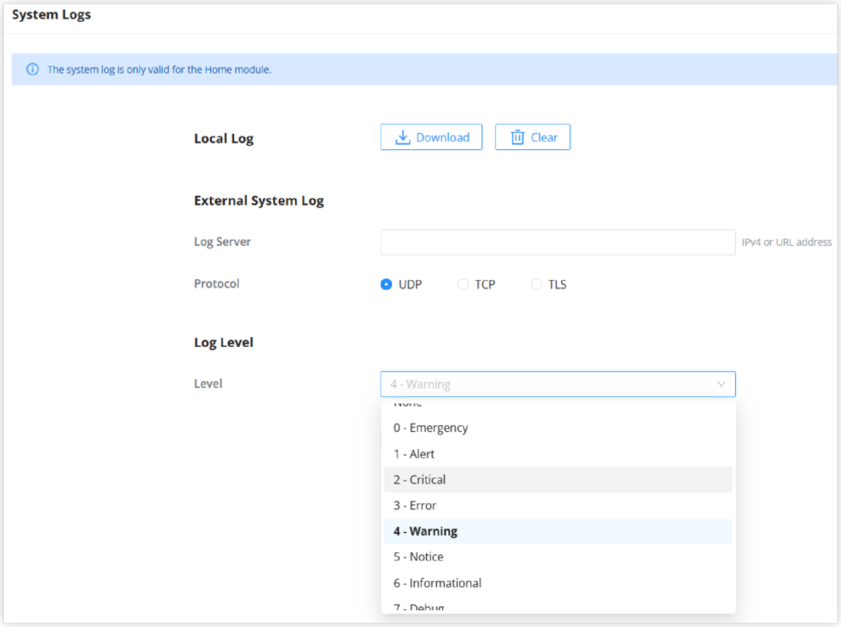
To export the logs, press Export All button. The logs will be saved in a CSV file.

System Logs

The **System Logs** page allows administrators to view, download, and forward system log data to an external server for monitoring and troubleshooting.

> **Note**
>
> This feature is only available when the device is operating in Home mode.

The page is divided into two parts:



System Logs

ⓘ The system log is only valid for the Home module.

Local Log

External System Log

Log Server IPv4 or URL address

Protocol ● UDP ○ TCP ○ TLS

Log Level

Level 4 - Warning

System Logs

- **Local Log**
  Users can download or clear the current system log file directly from the device.
- **External System Log**
  Allows forwarding logs to a remote server. Enter the destination server address and select the desired protocol:
  - **UDP**
  - **TCP**
  - **TLS**

You can also define the **Log Level**, which filters the types of events that are captured and sent. Available log levels are:

- **None**
- **0 – Emergency**
- **1 – Alert**
- **2 – Critical**
- **3 – Error**
- **4 – Warning**
- **5 – Notice**
- **6 – Informational**
- **7 – Debug**

Select the appropriate level based on the desired granularity of system reporting.

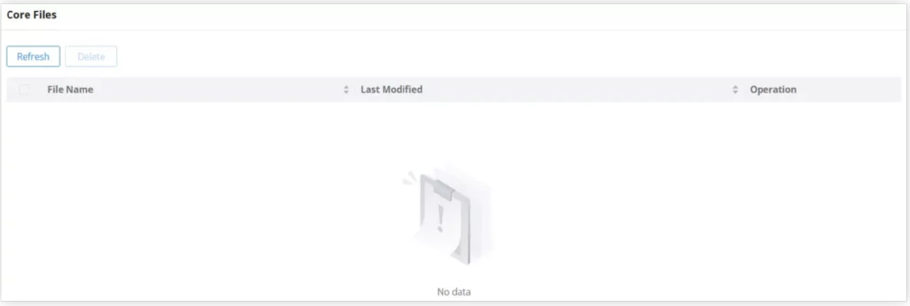
Core Files

The **Core Files** page displays a list of crash dump files generated by the system in the event of a critical failure. These files contain technical information that can help developers or support teams diagnose system issues.

If the device has not experienced any crashes, this page will appear empty.

Users can:

- Click **Refresh** to check for newly generated files.
- Select and **Delete** any stored files if needed.



Core Files

File Name	Last Modified	Operation

No data

Core Files

NETWORKING

The Networking module of GCC601X(W) includes network-related configuration mainly VPN, Multi-WAN, and traffic management. It also allows users to configure all the standard routing configurations such as VLAN, port forwarding, etc.

Click on the icon to access.

FIREWALL

The firewall module of GCC601X(W) is a Next-Generation Firewall (NGFW) that secures users' network environment by providing defense against the most advanced network attacks as it supports anti-virus and intrusion prevention (IDS/IPS) with frequent signature library updates and also supports SSL proxy to filter HTTPS URL.

Click on the icon to access.

NETWORK NODES

Network nodes refer to individual devices or components such as switches and access points that form the interconnected infrastructure of the network. These nodes provide data points for analysis, which helps centralize the monitoring and configuration of the device performance, security, and overall network features. The GCC601X(W) offers an embedded controller for both the wireless access points and the GWN-managed network switches to provide the user with a global overview of his network infrastructure.

Click on the icon to access.

PBX

The integrated IPPBX module in the all-in-one convergence device the GCC601X(W) provides a communication and collaboration solution for enterprises that do not require expanded telephony capabilities. It offers the same features that are provided by Grandstream IPPBX solution, the UCM6300, to ensure cost-effective and efficient collaboration among professionals.

Click on the icon to access.

UC ENDPOINTS

The UC endpoints configuration module contains all the settings and tools to manage and control the unified communication endpoints, including devices ranging from IP phones, Video phones, and Wi-Fi phones, to security facility access devices such as the IP cameras and the door systems. The GCC601X(W) with its VoIP devices and IPC devices management modules offers a centralized way to manage, provision, and control all your on-premise UC endpoint devices.

Click on the icon to access. ☎

CHANGE LOG

This section documents significant changes from previous versions of user manuals for GCC601x. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware version 1.0.7.5 (PBX version 1.0.27.44)

Main:

- Added "Remote Management (GWN App)" to the user menu and optimized the "Feedback" feature. [Feedback] [Remote Management (GWN App)]
- Enhanced "Overview" page with session statistics, firewall info, and PBX VLAN selection. [Overview]
- Improved Basic Settings layout under *System Settings*, supporting multiple NTP servers and managed device time sync. [Basic Settings]
- Added Multi-factor Authentication (MFA). [Security Settings]
- Added "Allowed IP Addresses" control to restrict HTTPS access by IP. [Web Access]
- Added "Reference Details" option to view where a schedule is currently in use. [Schedule]
- Added factory reset prompt when downgrading to an incompatible firmware via manual upload. [Upgrade]
- Added System Logs and Core Files pages under the Logs & Diagnostics section. [System Logs] [Core Files]

Networking Module:

- Added Bridge Mode configuration under Network Settings → WAN to support VLAN-to-port mapping with priority settings for multi-service deployments (e.g., Triple Play). [Bride Mode]
- Optimized Static IP Binding configuration under Network Settings → LAN for a simplified user experience by removing VLAN selection and streamlining the IP assignment process. [Static IP Binding]
- Added VPN Setup Wizard for simplified VPN tunnel configuration. [VPN Setup Wizard]
- Optimized configuration interface and added "User Manual" link for WireGuard®, IPSec, OpenVPN®, PPTP, and L2TP. [VPN]
- Added "Remote Clients" table in WireGuard® configuration. [WireGuard®]
- Added support for domain names in the WireGuard® Endpoint address field. [WireGuard®]
- Added IPSec Encryption option to L2TP server configuration. [L2TP]
- Added support for exporting .ovpn file in OpenVPN® Client configuration. [Remote Users]
- Added Routing Table page. [Routing Table]
- Added OSPF, RIP, and BGP protocols. [Routing]
- Added IP-based traffic statistics. [Traffic Management]
- Added IP Source and Update Interval (Min) settings to DDNS configuration. [DDNS]
- Added Clone feature to Port Forwarding rules for quick duplication. [Port Forwarding]
- Added an input restriction to the TR-069 ACS Username and Password. [TR-069]
- Relocated Ping/Traceroute/NSlookup to Maintenance → Network Tools, and Core File to Home → Logs & Diagnostics. [System Diagnostics]

- Added features of NSlookup and Wake on LAN under [Network Tools]
- Added a feature of Local Logs download under Syslog. [Syslog]
- Added Email Settings page. [System Settings]
- Added Profiles section with support for MAC Group, IP Address Group, FQDN, RADIUS, and Certificates. [Profiles]

Firewall Module:

- Enhanced Firewall Service block to support automatic service activation, manual status refresh, and display of last updated time. [Overview]
- Added "Clone" and "Schedule" options to traffic rule management for Inbound, Outbound, and Forwarding rules. [Rules Policy]
- Enabled rule duplication via the **Clone** button for both **SNAT** and **DNAT** entries in the Advanced NAT section. [Advanced NAT]
- Added support for IP object selection across all firewall exception modules: DoS, IPS, Botnet, Content Control, SSL Proxy, and Geo-IP. [IP Exception]
- Centralized all signature update settings (Virus, IPS, URL, Application) under a unified **Signature Update** section in the Firewall menu. [Signatures Update]
- Added DNS Category Filtering tab under DNS Filtering to simplify domain blocking based on category groups. [DNS Category Filtering]
- In the **URL Category Filtering** tab, the **Search Engine** subcategory has been added under the **Social Activities** category. [URL Category Filtering]
- Optimized the **Application Filtering** → **Application List** interface with enhanced visual charts, batch risk management options, and added new categories. [Application List]
- Added support for customizable intercept pages for blocked access and virus detection events. Applies to Web Filtering and Anti-Virus. [Blocked Web Page]
- Improved **Details** view in **Security Log** → **Log** for "DoS & Spoofing" and "Application Filtering" entries, providing enhanced visibility of logged events. [Log]
- Added **Export All** option in **Security Log** for full log history export. [Log]
- Enhanced **Log Level and Email Notification** to include detailed risk level configuration for DNS Filtering and other security features, allowing granular control over alert triggers. [Log Level and Email Notification]

Networking Nodes Module:

- Added support for VLAN ID assignment in PPSK configuration under Wi-Fi Management. [PPSK]
- Added captive portal support for wired clients under Client Management. [Captive Portal]
- Added Bypass Splash Page option under Captive Portal → Policy, allowing MAC-based exclusion from the captive portal. [Captive Portal]

PBX Module:

- Added support for DDNS configuration.[DDNS Settings]
- Added GCC PBX licence display. [Dashboard]

UC Endpoints Module:

- Added support for monitoring the status of device provisioning and reboot. [Managing Discovered Devices]
- Add upgrade status and ability to download multiple templates in the Model Template Package List. [Model Template Package List]
- Added an option to disable Level-config provisioning. [Follow Device]
- Added support for responding only to provisioning requests with URLs that specify the filename. [Auto-Provisioning Settings]

Firmware Version 1.0.5.11 (PBX version 1.0.27.17)

Main:

- No major changes

PBX:

- No major changes.

Firmware version 1.0.5.6 (PBX version 1.0.27.14)

Main:

- Added Operation Log to the Home module. [Operation Log]
- Added Scheduled Backup support. [Backup & Restore]
- Added support for MTA type for Email settings. [Email Settings]

Networking Module:

- Added support for the Balancing strategy in Policy Routes Settings. [Balancing Strategy]
- Added Support for VRRP protocol. [VRRP]
- Added option to preserve VPN configuration when the VPN is disabled. [VPN]
- Added Speed Test for the GCC from the GDMS Networking. [WAN]
- Set the maximum IPsec tunnels to be created at 64 tunnels. [IPSec]

Firewall Module:

- Added outbound rules. [Outbound Rules]
- Updated IDS/IPS: Removed WAN selector and enabled automatic detection of all WANs by default. [IDS/IPS]
- Added support for detecting SMTP(S) and POP3(S) protocols in Antivirus configuration and SSL basic settings. [Anti-Malware]
- Added import and export lists to DNS Filtering. [DNS Filtering]
- Added import and export lists to Web Filtering. [Web Filtering]
- Added import and export list to SSL Proxy Exemption List. [SSL Proxy]
- Added the option to enable the rule by schedule for DNS Filtering, URL Filtering, Keyword Filtering, and Application Filtering. [DNS Filtering] [URL Filtering] [Keyword Filtering] [Application Filtering]
- Enhanced the function interface and added the application list. [Application Filtering]
- Added Geo-IP Filtering [Geo-IP Filtering]
- Added Domain Name – Wildcard option to SSL Exempted Address. [SSL Proxy]
- Added support for setting log levels for security log and advanced filtering items. [Security Log]
- Added support for SNI and Common Name (CN) in DNS filtering. [DNS Filtering]

Networking Nodes Module:

- Added support for 6G frequency bands. [Radio] [SSID] [MESH]
- Added support for Cloud delivery of PPSK configurations. [PPSK]

PBX Module:

- Added support for high availability [HA]
- Added Account SIP Trunk [VoIP Trunk Configuration]
- Added support for searching CallerID in a third-party MySQL database [Inbound Route: Third-party Database Search]
- Added support for integration with Don’t Call Me database [Don’t Call Me Blacklist Integration]
- Added support for ZRTP on the extensions level [SIP Extension]
- Added support for ZRTP on the trunk level [VoIP Trunk Configuration]
- Added support for enabling multiple Wave sessions on the same platform [SIP Extension]

- Added support for verifying ACS [TR-069]
- Added Task Management feature [Task Management]
- Added support for search function in LDAP server phonebooks [LDAP Phonebook]
- Added support for data encryption on the local storage and attached storage [Data/File Encryption]
- Password Visibility Toggle has been added to the Admin privilege [Super Administrator]
- Added the Merge Same Call Recordings setting [PBX SETTINGS]
- Added support for adding a suffix to the Call Forward Enable/Disable feature [Feature Codes]
- Added icons next to feature codes to indicate whether or not they can be nested by other feature codes [Feature Codes]
- Added support for Time Condition Routing [TIME CONDITION ROUTING]
- Added support for Custom Time Groups [Custom Time Groups]
- Added support for custom announcement for Call Queue [Configure Call Queue]
- Added Reset Agent Call Counter to Call Queue [Configure Call Queue]
- Added number and percentage of transferred calls in the Call Queue Switchboard [Configure Call Queue]
- Added Call Memory in Call Queue [Configure Call Queue]
- Updated Wake-up Service by adding call failure notification [Wakeup Service]
- Room status can now be modified using the API [API CONFIGURATION]
- Odoo CRM integration has been added [Odoo CRM]
- Added custom repeating setting when scheduling meetings [Schedule Meeting]
- Added Extension Login Management module [Extension Login Management]
- Added Wave Administrator privilege [SIP Extension][Custom Privilege]
- Added Download Chat Logs privilege [User Portal/Wave Privileges]
- Added Remote Logout Wave Privilege [User Portal/Wave Privileges]
- Added API support to retrieve recording filename [API CONFIGURATION]
- Added enable/disable setting for Paging/Intercom [Paging/Intercom]
- Added support for configuring custom agent pause reason with a custom prompt [Global Queue Settings]
- Added support for allowing multiple login sessions from the same platform for Wave [SIP Extension]
- Added TLS key download in Ethernet Capture diagnosis tool [Ethernet Capture]
- Increased members notified for Emergency Calls from 10 to 30 [Emergency Calls]
- Added Wave Upgrade page [Wave Upgrade]
- Add support to send a message broadcast using API [API Configuration]

UC Endpoints Module:

- Added Support for LDAP configuration to be pushed through Fast Provisioning. [LDAP Phonebook]

Firmware version 1.0.3.6 (PBX version 1.0.25.41)

- No major changes.

Firmware version 1.0.3.5 (PBX version 1.0.25.40)

Main:

- Added the option to format an unmounted SSD through the overview page. [Overview]
- Added the graphs for the number of sessions established and the total number of concurrent sessions. [Overview]
- Added support for displaying the offline devices on the topology. [Topology]
- Added support for disabling/enabling the redirection from port 80 when accessing the web UI. [Web Access]
- Added support for upgrading all the modules using one firmware file. [Upgrade]
- Added support for factory resetting the PBX data and configuration separately from the other modules. [Factory Reset]

Networking Module:

- Added the option to allow multiple WANs to share the same VLAN ID. [WAN]
- Added the requirement that when **IPv6 is enabled on the WAN**, the minimum **MTU** must be **1280**. [WAN]
- Added WAN port MAC address configuration. [WAN]
- Added the requirement that not all LAN ports can be disabled [Port Configuration]
- Added the assurance that disabling the WAN will not delete dependent configurations. [WAN]
- Added support for exporting .pem format certificates. [Certificates Import and Export]
- Added a black hole option for the outgoing interface. [Static Routes]
- Added PBX service [VoIP Settings]
- Added support for core files batch deletion [Core files]
- Added support for storage options under packet capture [Capture]
- Added alarm Notification Settings and Email Notification Settings for takeover/un-takeover, switch online and offline alarms [Alerts & Notifications]

Firewall Module:

- Updated the firewall package information link [Overview]
- Added ARP Protection – Static ARP List [Static ARP List]
- Added exception IP under content control [IP Exception – Content Control]
- Added search for application filtering rules [App Filtering Rules]

PBX Module:

- Added support for formatting USB flash drives from the web UI. [USB Disk/SD Card File Management]

Firmware version 1.0.1.34 (PBX version 1.0.25.21)

- No major changes.

Firmware version 1.0.1.32 (PBX version 1.0.25.17)

- This is the initial version for GCC6010W and GCC6011.

Firmware version 1.0.1.10 (PBX version 1.0.25.11)

- Disabled Check/Download New Firmware at Boot up by default. [Upgrade]

Firmware version 1.0.1.8 (PBX version 1.0.25.11)

- This is the initial version.

Certification Regulatory Information

- U.S. FCC Part 15 Regulatory Information

This device complies with part 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.

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

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.

- Canada Regulatory Information

CAN ICES-003 (B)/NMB-003(B)
This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.
Le présent produit est conforme aux spécifications techniques applicables d’Innovation, Sciences et Développement économique Canada.