

Grandstream Networks, Inc.

GCC6020 - User Manual - Home



GCC6020 - User Manual - Home

The **GCC6020 Series** is an advanced all-in-one solution that unifies communication, networking, and security capabilities into a single, powerful platform. It integrates the functionality of four distinct systems **VPN router**, **next-generation firewall**, **IPPBX**, and **network switch** to deliver enterprise-grade performance in a compact, centrally managed appliance.

With the GCC6020 and GCC6021 models, businesses can deploy and manage wired, wireless, and VPN networks while benefiting from deep security protections such as DPI, SSL inspection, and IDS/IPS. These devices offer built-in IP PBX functionality for seamless voice and video collaboration, and support for encrypted traffic, secure boot, and high-availability deployment.

The platform supports unified management of Grandstream access points, switches, and UC endpoints through the **Grandstream Device Management System (GDMS)**, **GWN mobile app**, **local web UI**, **SSH**, **SNMP**, and **CLI** making it easy to provision and maintain an integrated network.

Ideal for **small-to-medium sized businesses**, the GCC602x series simplifies deployment and reduces costs by consolidating business data, security, communication, and collaboration into one cohesive system.

The GCC6020 series combines the following modules:

- [Home](#)
- [Networking](#)
- [Firewall](#)
- [Network Nodes](#)
- [PBX](#)
- [UC Endpoints](#)

PRODUCT OVERVIEW

Technical Specifications

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

Field	GCC6020	GCC6021
Network Ports	* 1x 10 Gigabit SFP+ ports* 1x 2.5 Gigabit Ethernet ports* 4x Gigabit Ethernet ports*All ports are WAN/LAN configurable*max 3x WAN	* 4x 10 Gigabit SFP+ ports* 8x 2.5 Gigabit Ethernet ports* 16x Gigabit Ethernet ports*WAN/LAN configurable on Ethernet ports (1-24)*SFP+ : 25-27 configurable ports, 28 fixed WAN port*Max 5x WAN
Auxiliary Ports	* 1x CONSOLE* 1x USB 3.0	* 1x CONSOLE* 1x USB 3.0* 2x HA* 1x MGMT
Memory	4GB RAM, 32GB eMMC	4GB DDR4+256MB DDR3 RAM, 32GB eMMC, 128MB NAND
External Storage	M.2 SSD (Optional)	
Routing	6.5Gbps	10Gbps
IPSec VPN Throughput	1.3Gbps	
NAT Sessions	320K	
Supported number of VLAN	256	
NGFW Throughput (DPI+IPS)	6Gbps	9Gbps
Total No-Blocking Throughput	13Gbps	76Gbps

Total No-Blocking Throughput	Note: Values shown apply when Hardware Acceleration is enabled.	
Switching Capacity	26Gbps	152Gbps
	Note: Values shown apply when Hardware Acceleration is enabled.	
PBX	50 users and 16 concurrent calls by default Upgrades available for purchase: (See more for PBX capacity upgrade options)	
Mounting	Desktop, Wall, and Rack-mountable	Desktop and Rack-mountable
Material	Metal	
LEDs	1x LED for SFP+, 5x LED(G/Y) for Ethernet Ports, 5x LED(Y) for PoE Out, 1x LED(R/G/B) for device tracking and status indication, 1x LED for main power, 1x LED for Redundant Power System	24x LED(G/Y) for Ethernet Ports/PoE Out, 4x LED for SFP+, 2x LED for HA, 1x LED(R/G/B) for device tracking and status indication, 1x LED for main power, 1x LED for Redundant Power System
Connection Type	DHCP, Static IP, PPPoE	
Network Protocols	IPv4, IPv6, IEEE802.1q, IEEE 802.1p, IEEE802.1x, IEEE802.3, IEEE 802.3u, 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* DPI, Anti-Virus, IPS/IDS, SSL Proxy* Content Control: DNS filtering, web url/class/key words filtering, application identification and control* Email Security, Geo-IP filtering	
VPN	IPSec VPN Client-to-Site / Site-to-SiteIPSec Encryption: 3DES, AESIPSec Authentication: MD5, SHA-1, SHA2-256Key Exchange: Main/Aggressive Mode, Pre-shared Key, DH Groups 1/2/5/14IPSec Protocols: ESPIPSec NAT TraversalPPTP VPN Server / ClientPPTP Encryption: MPPE 40-bit, 128-bitPPTP/L2TP Authentication: MS-CHAPv1/2L2TPOpenVPN(R) Server / ClientOpenVPN(R) Encryption: AES, DESOpenVPN(R) Authentication: MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512OpenVPN(R) Certificate: RSAWireGuard(R)	
Network Management	Grandstream Device Management System (GDMS), GWN App, Local Web GUI, SSH, SNMP (v1/v2c/v3) and CLI	
Max AP/Clients	Up to 300 GWN APs; Up to 500 Clients	Up to 300 GWN APs; Up to 1000 Clients
Power and Green Energy Efficiency	Universal power adaptor included: Input 100-240VAC 50-60Hz Output: 54VDC/2.8A (150W); 5x PoE out ports support IEEE802.3af/at, Maximum PoE Wattage: 120W RPS Input: 54VDC/2.8A	Universal power adaptor included: Input 100-240VAC 50-60Hz Output: 54VDC/7.8A (420W); 8x PoE out ports support IEEE802.3 af/at/bt, 16x PoE out ports support IEEE 802.3 af/at, Maximum PoE Wattage: 370W RPS Input: 54VDC/7.8A
Environmental	Operation: 0 degC to 45 degCStorage: -10 degC to 60 degCHumidity: 5% to 95% Non-condensing	
Physical	Unit Dimension: 280 x 185.5 x 44 mmUnit Weight: 1.5KGEntire Package Dimension: 384 x 209.5 x 60 mmEntire Package Weight: 2.1KG	Unit Dimension: 440 x 301.5 x 44mmUnit Weight: 4.2KGEntire Package Dimension: 557 x 413 x 138mmEntire Package Weight: 5.6KG
Package Content	GCC6020/GCC6021, Universal Power Supply, Rack mount kit, Quick Installation Guide	
Compliance	FCC, CE, RCM, IC	

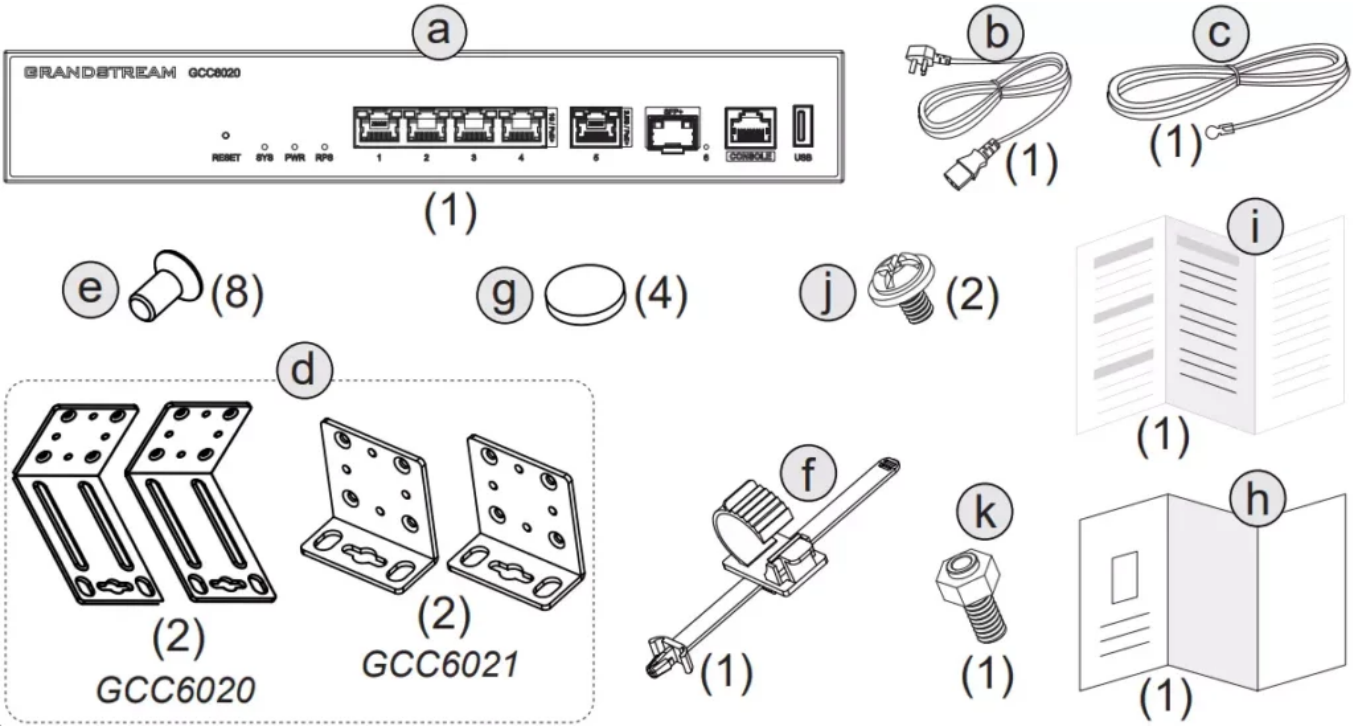
GCC6020 technical specifications

INSTALLATION

Before deploying and configuring the GCC6020 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 GCC6020 device.

Package Contents

The GCC6020/GCC6021 package includes the following components:



Package Contents

Bracket style and screw placement may differ depending on whether the device is GCC6020 or GCC6021.

Label	Quantity	Item
a	1x	Main Unit (GCC6020 or GCC6021)
b	1x	Power Cable
c	1x	Grounding Cable
d	2x	Rack Mount Brackets (model-specific)
e	8x	Rack Mounting Screws
f	1x	Power Cord Anti-Trip
g	4x	Rubber Feet
h	1x	Regulatory Information
i	1x	Quick Installation Guide
j	2x	M.2 SSD Screws (top)
k	1x	M.2 SSD Securing Screw (bottom)

Package Contents

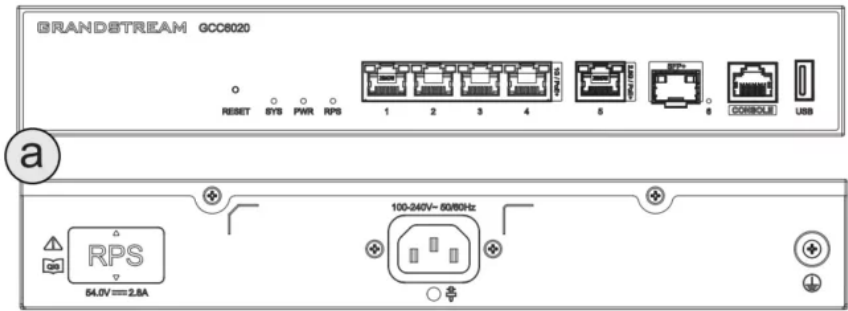
Hardware Overview

The GCC6020 and GCC6021 feature front and rear panels with multiple Ethernet, SFP, USB, and management ports. The exact port layout varies depending on the model.

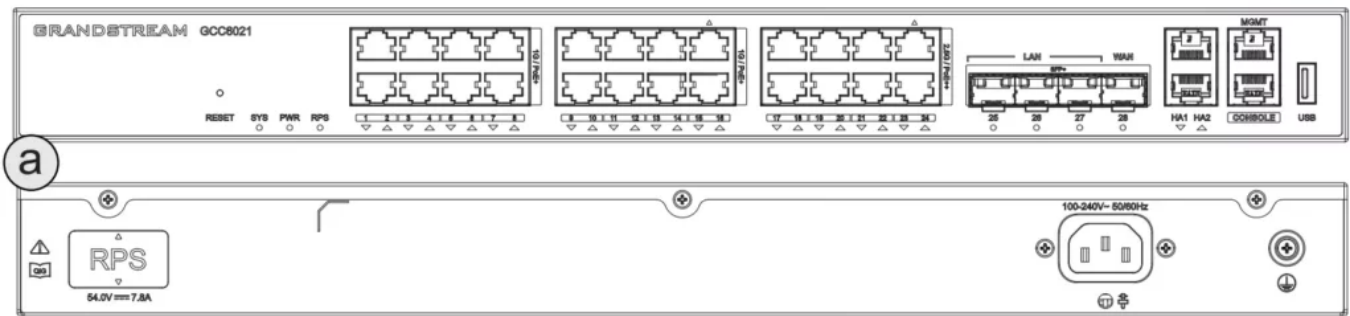
Each unit includes a standard AC power input and a Redundant Power Supply (RPS) port on the back panel. LED indicators on the front help monitor power, connectivity, and system status.

Check the label on your device to identify the exact port configuration.

GCC6020



GCC6021



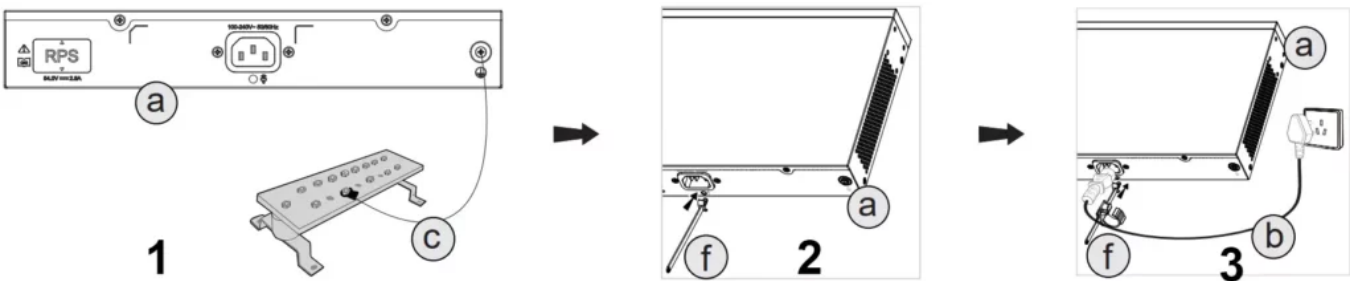
Hardware Overview

Powering the Device

Follow the steps below to properly power the GCC6020/GCC6021:

- 1. Ground the Device**
Attach the grounding cable (c) to the grounding point (a) on the rear panel to prevent electrical surges.
- 2. Secure the Power Cable**
Install the power cord Anti-Trip (f) onto the power socket. This helps prevent accidental unplugging or cable strain.
- 3. Connect the Power Cable**
Plug the power cable (b) into the device, then wrap the Power Cord Anti-Trip (f) around it as shown before connecting to a power outlet.

Optionally, connect a backup power source to the RPS port for redundancy.



Powering the Device

LED Indicators

LED lights	Indication	LED Status	Remarks
LAN/WAN LED	LAN/WAN port connection	Solid Green	

LAN/WAN LED	LAN/WAN port data exchange	Flashing green	The flashing frequency is related to the network transmission rate. The faster the rate, the faster the flashing frequency.
	PoE Out power supply	Solid Orange	Models supporting PoE Out
	No connection	Off	
System LED	Shutdown	Off	
	Normal operation	Solid Blue	
	Firmware Upgrade	Flashing Green -> Solid Green -> Solid Blue	
	Upgrade failed	Solid Red	
	Factory Reset	Red flashes 6 times -> off -> Pink light on for about 3 seconds -> Solid Green -> Solid Pink	
	AP pairing process	Flashing Blue -> Solid Blue	AP System LED Status
	Modify the configuration	Flashing Blue -> Solid Blue	AP System LED Status, If the configuration changes are minor and the update is fast, the indicator light may remain blue.
	Delete pairing	Red flashes 6 times -> off -> Solid Green -> Solid Pink	AP System LED Status
	Mesh	Flashing Yellow -> Solid Blue	AP System LED Status
PWR/RPS power LED	Power supply not in use/failed	Off	
	Power supply in use	Solid Green	
HA (High Availability)	Connected	Solid Green	
	Not connected	Off	

Rack Mount Installation

To mount the device into a standard 19" rack:

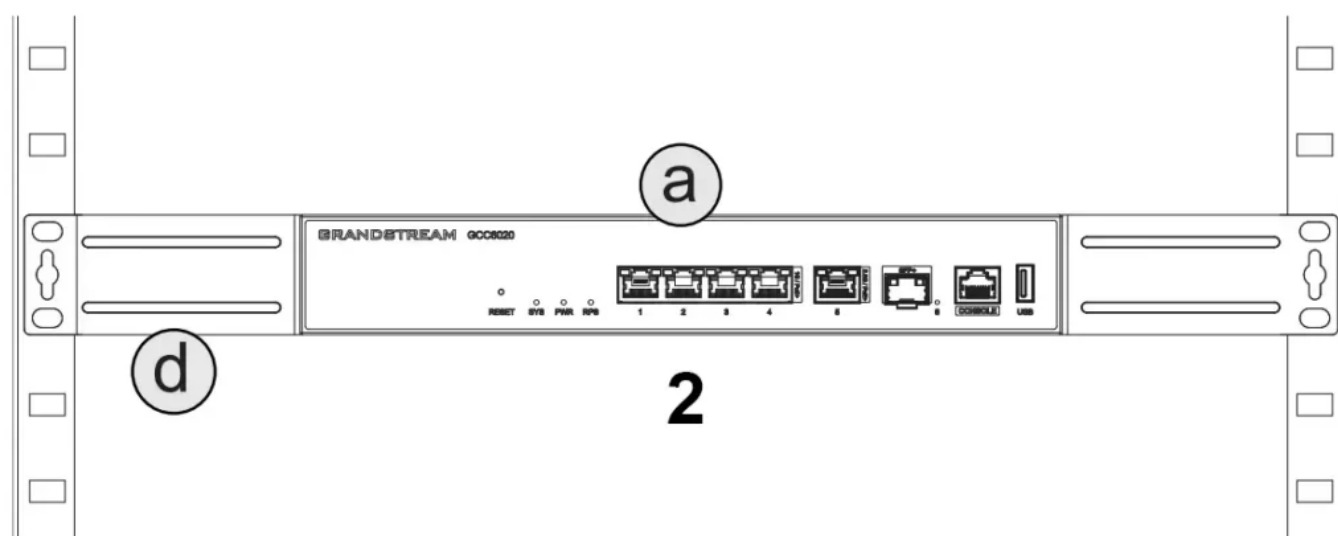
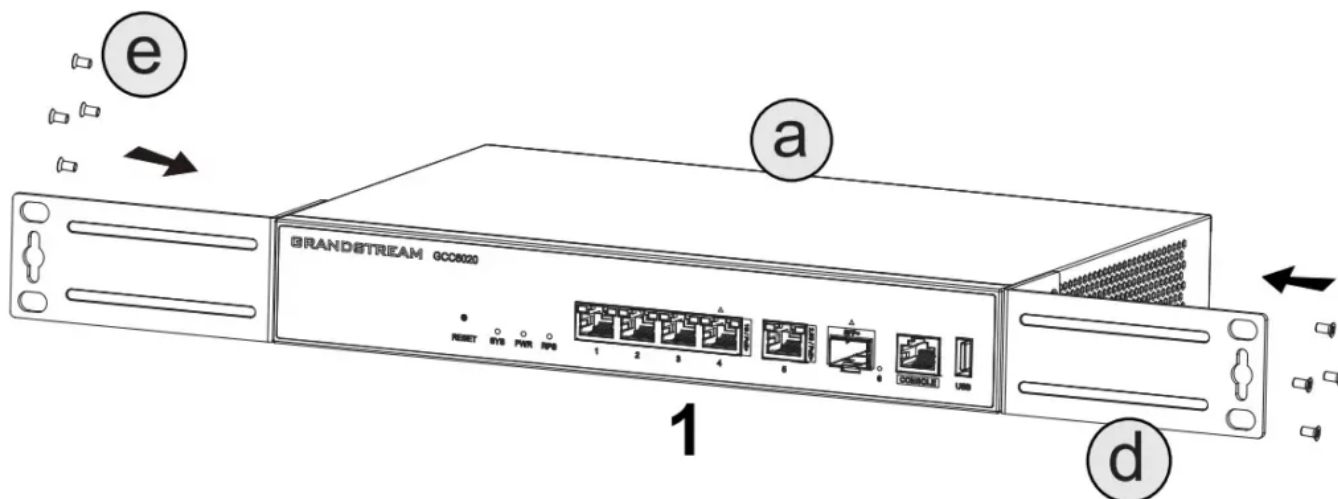
1. Attach the Rack Brackets

Secure the provided rack mount brackets (d) to both sides of the device (a) using the included screws (e).

2. Install the Unit into the Rack

Carefully align and slide the device into the rack, then secure the brackets to the rack frame.

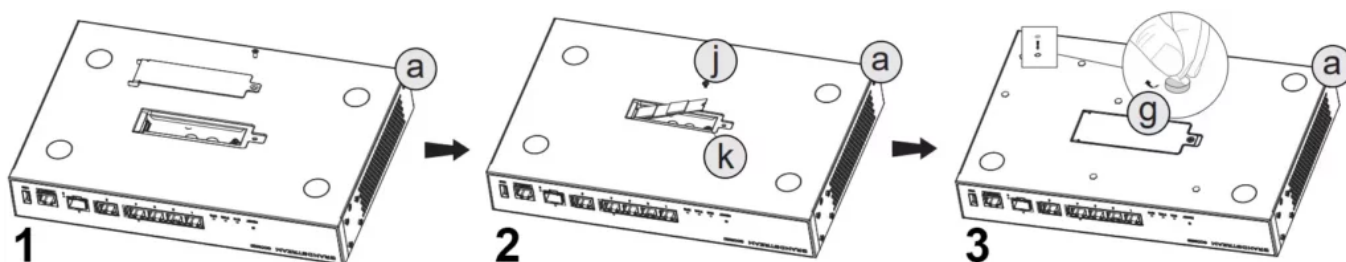
Ensure proper airflow around the device and avoid blocking the ventilation areas on the sides.



Rack Mount Installation

Installing the M.2 SSD

1. **Access the SSD Slot:** Flip the device upside down to locate the SSD compartment (a). Remove the bottom SSD cover by unscrewing the pre-installed screw.
2. **Install the SSD:** Secure the standoff screw (k) in the appropriate mounting position. Insert the M.2 SSD module into the slot at an angle, then press it down flat. Fasten it using the hold-down screw (j) to secure the SSD in place.
3. **Close the SSD Compartment:** Reattach the metal cover and tighten the original screw to finish the installation.



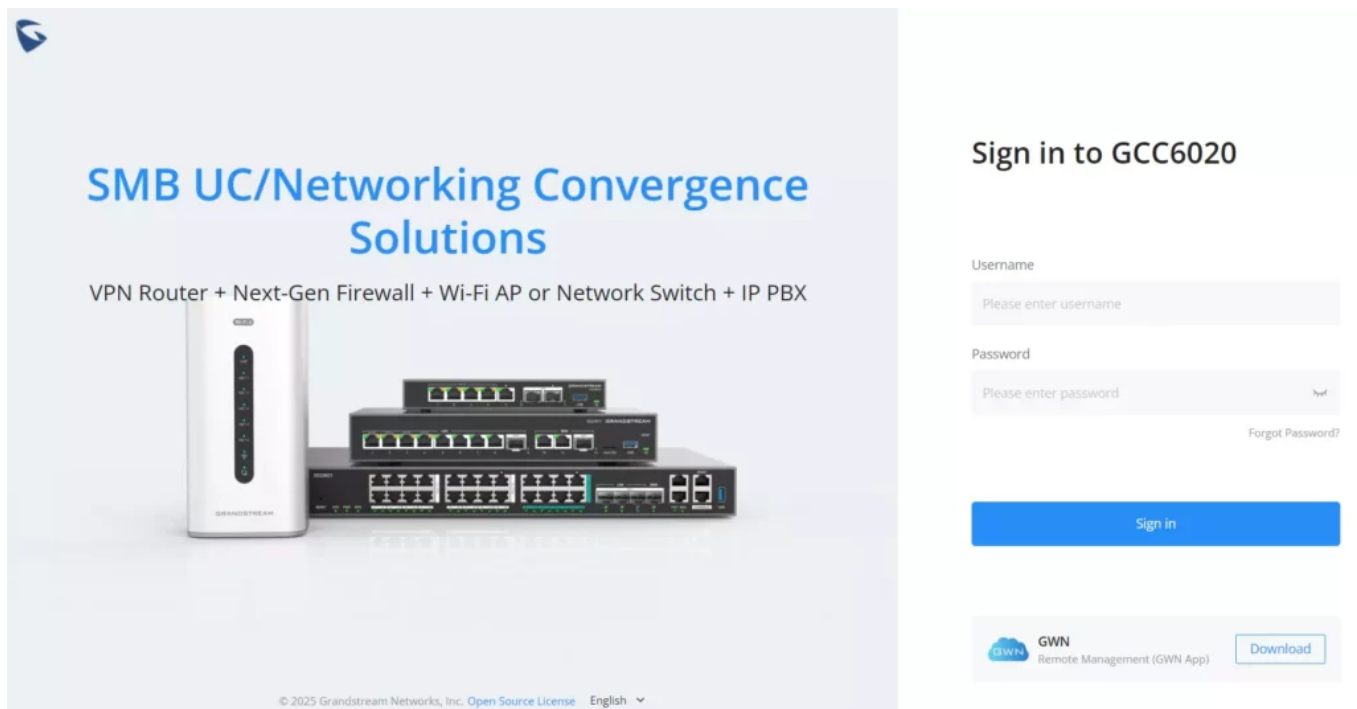
Installing the M2 SSD

Connecting to GCC602x

1. **Connect the WAN port** (marked with ?) to your internet uplink such as an optical modem, router, or ISP-provided gateway.
2. **Connect a PC or laptop** to one of the LAN ports on the GCC602x.
3. Open a web browser and access the default gateway: **http://192.168.80.1** or **gcc.grandstream.com**

- The **default login credentials** are printed on the MAC label on the bottom of the unit. The default username is **admin**.
- LAN ports with a **? symbol** are preconfigured as WAN ports by default.

When powering on the GCC602x device for the first time (or after a factory reset), users will be prompted with the login screen shown below.



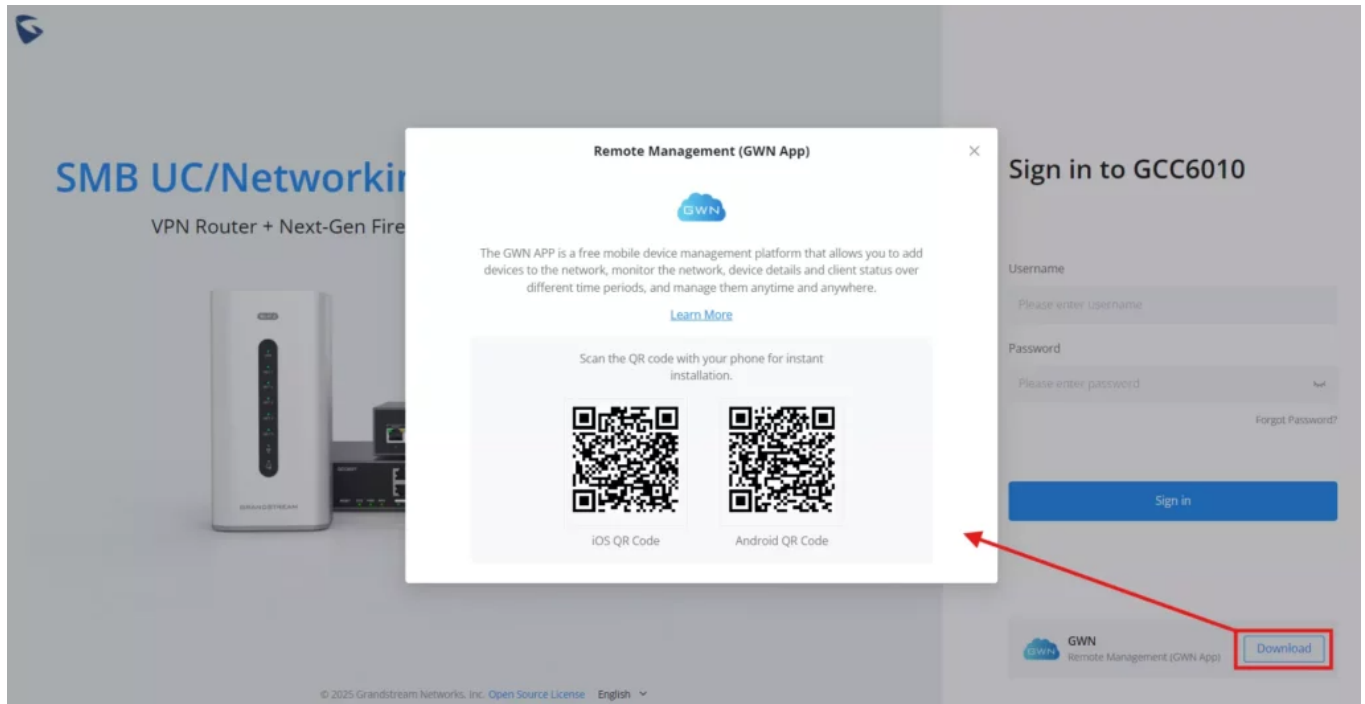
GCC602x Login page

GWN Remote Management App

On the login screen, users will also find an option to download the **GWN App** for remote management. Click the **Download** button under "GWN Remote Management" to view platform-specific QR codes:

- Scan the QR code with your phone to install the app:
- **Left:** iOS (App Store)
- **Right:** Android (Google Play)

For more details, check GWN App for Android - User Manual or GWN App for iOS - User Manual.



GCC601xW login page Download App

Safety and Precautions

- Do not attempt to open, disassemble, or modify the device.
- Do not expose this device to temperatures outside the range of 0 degC to 45 degC for operating and -10 degC to 60 degC for storage.
- Do not expose the device to environments outside of the following humidity range: 5-95% RH (non-condensing).
- Do not power cycle the device during system boot-up or firmware upgrade. You may corrupt firmware images and cause the unit to malfunction.
- Appliance coupler is used as disconnect device, the disconnect device shall remain readily operable.

The GNU GPL license terms are incorporated into the device firmware and can be accessed via the Web user interface of the device at `my_device_ip/gpl_license`. It can also be accessed here:
<https://www.grandstream.com/legal/open-source-software>

To obtain a CD with GPL source code information please submit a written request to info@grandstream.com

The GCC6020 complies with FCC/CE and various safety standards. The GCC6020 power adapter is compliant with the UL standard. Use the universal power adapter provided with the GCC6020 package only. The manufacturer's warranty does not cover damages to the device caused by unsupported power adapters.

If the GCC6020 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.

Use the power adapter provided with the GCC6020 device. Do not use a different power adapter as this may damage the device. This type of damage is not covered under warranty.

Getting Started

Setup Wizard

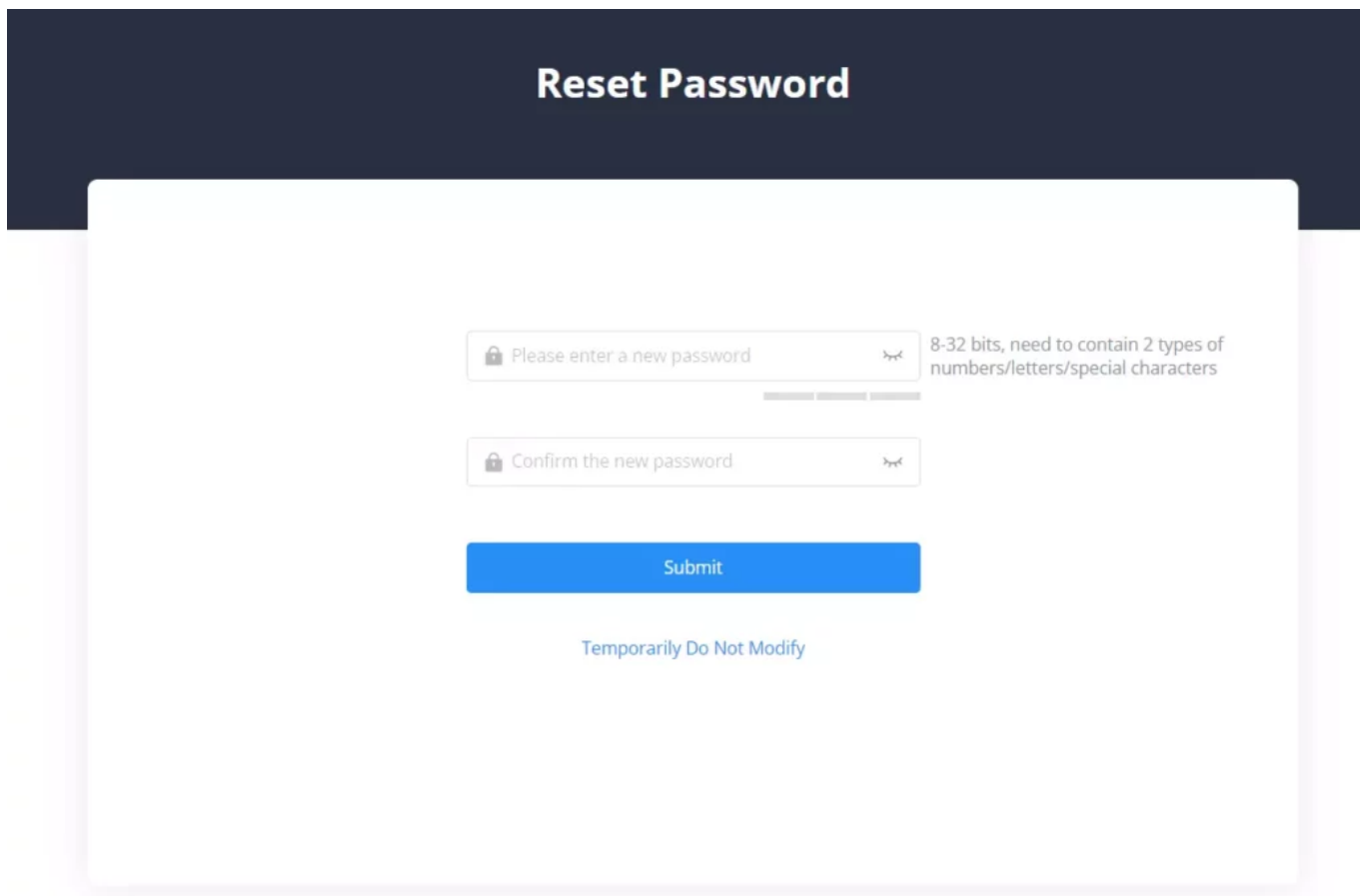
When powering on a brand-new GCC60xx device or after a factory reset, the system will launch the **Initial Setup Wizard** automatically. Follow the steps below to complete the basic configuration.

Step 1: Change Password

After logging in for the first time, you'll be prompted to **reset the default password**. Enter your new password twice and click **Submit**.

Make sure your password is **8-32 characters long** and includes **at least two** of the following: letters, numbers, and special characters.

Alternatively, you may click **Temporarily Do Not Modify** to skip password reset, but this is not recommended for security reasons.



Reset Password

Please enter a new password 8-32 bits, need to contain 2 types of numbers/letters/special characters

Confirm the new password

Submit

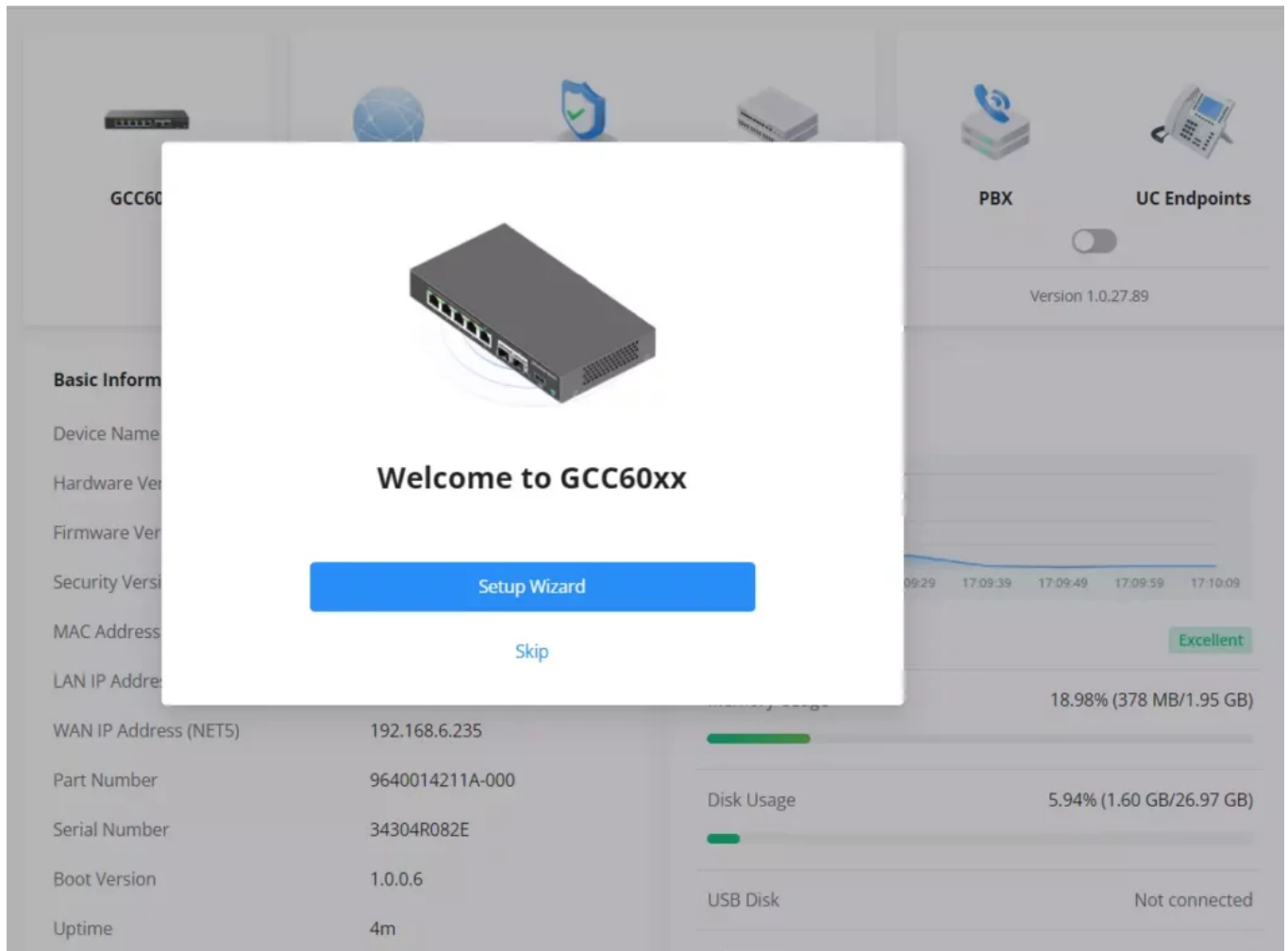
[Temporarily Do Not Modify](#)

GCC Device Setup Wizard part 1

Step 2: Welcome Screen - Launch Setup Wizard

Once the new password is set, the system will log you out. Log in again with your updated credentials. After successful login, the system displays a **welcome prompt** with two options:

- **Setup Wizard:** Starts the initial configuration process.
- **Skip:** Takes you directly to the dashboard (not recommended unless setup was previously completed).



GCC Device Setup Wizard part 2

Step 3: User Settings

After clicking **Setup Wizard**, the configuration will begin with the **User Settings** page.

Fill in the following fields:

- **Username:** Between 4-64 characters (letters, digits, or underscores).
- **Email:** (Optional) Used for alerts and recovery.
- **Mobile Number:** (Optional) For two-factor notifications or alerts.

Use the **blue arrow** at the bottom to continue to the next step.

You may also choose to **Exit Wizard** or **Skip** this step entirely.

Setup Wizard

The setup wizard will guide you through the basic configuration.

1

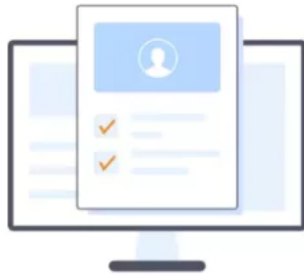
2

3

4

5

User Settings



* Username

4-64 characters, including letters, digits, and underscores

admin

* Email ⓘ

1-64 characters

Please enter

Mobile Number

2-18 digits

+1



Please enter

Exit Wizard



Skip

GCC Device Setup Wizard part 3

Step 4: Email Sending Settings - Part 1

This step configures how the device sends system emails.

- **TLS:** Toggle ON for secure transmission.
- **Type:** Select Clients (recommended) or MTA.
- **Email Format:** Choose HTML or Plain Text
- **SMTP Server:** Enter your outgoing mail server address (IPv4 or hostname).
- **SASL Authentication:** Toggle ON to enter credentials.

Setup Wizard

The setup wizard will guide you through the basic configuration.

1

2

3

4

5

Email sending settings



TLS



Type

☒ Clients ☐ MTA

Email Template Sending Format

☒ HTML ☐ Plain Text

*SMTP Server ⓘ

IPv4 or URL address

Please enter

SASL Authentication



*Username ⓘ

Exit Wizard



Skip

GCC Device Setup Wizard part 4

Step 5: Email Sending Settings - Part 2

Continue email configuration by entering:

- **Username:** Your email address.
- **Password:** Email server password.
- **Display Name:** This name will appear in outgoing emails.
- **Sender Email:** The sender address for system messages.
- Click **Test** to confirm email functionality.

Setup Wizard

The setup wizard will guide you through the basic configuration.

12345



SASL Authentication ☒

*Username ⓘ

Email Address

Please enter

*Password

Please enter

*Display Name

1-42 characters

GCC

*Sender

Email Address

anonymous@example.com

Test

Exit Wizard

<>

Skip

GCC Device Setup Wizard part 5

Step 6: Basic Settings

Define your basic device identity here:

- **Device Name:** A unique name for this GCC6020 unit.
- **Country / Region:** Select your location.
- **Time Zone:** Choose the relevant time zone.

Setup Wizard

The setup wizard will guide you through the basic configuration.

1

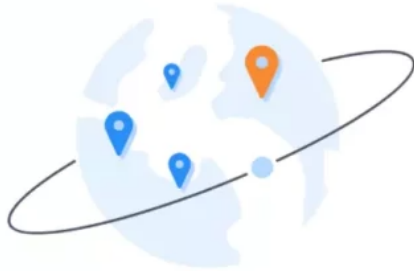
2

3

4

5

Basic Settings



* Device Name

1-64 characters

GCC60xx_device

Country / Region

Morocco

Time Zone

(UTC+01:00) Africa/Casablanca

Exit Wizard



Skip

GCC Device Setup Wizard part 6

Step 7: Internet Settings

Configure how the device connects to the internet.

- **WAN Name:** Label your WAN interface.
- **Port Speed:** Choose between Auto Negotiation, 10/100/1000 Mbps, etc.
- **Connection Type:** Select from DHCP, Static, or PPPoE.
- **DNS Servers:** Enter preferred and alternate DNS servers if necessary.

Setup Wizard

The setup wizard will guide you through the basic configuration.

1

2

3

4

5

Internet Settings



WAN1 (SFP7 | SFP | link down)

*WAN Name

1-64 characters

WAN1

Port Speed

Auto Negotiation

Connection Type

Obtain IP automatically (DHCP)

Preferred DNS Server

Alternative DNS Server

Exit Wizard



Skip

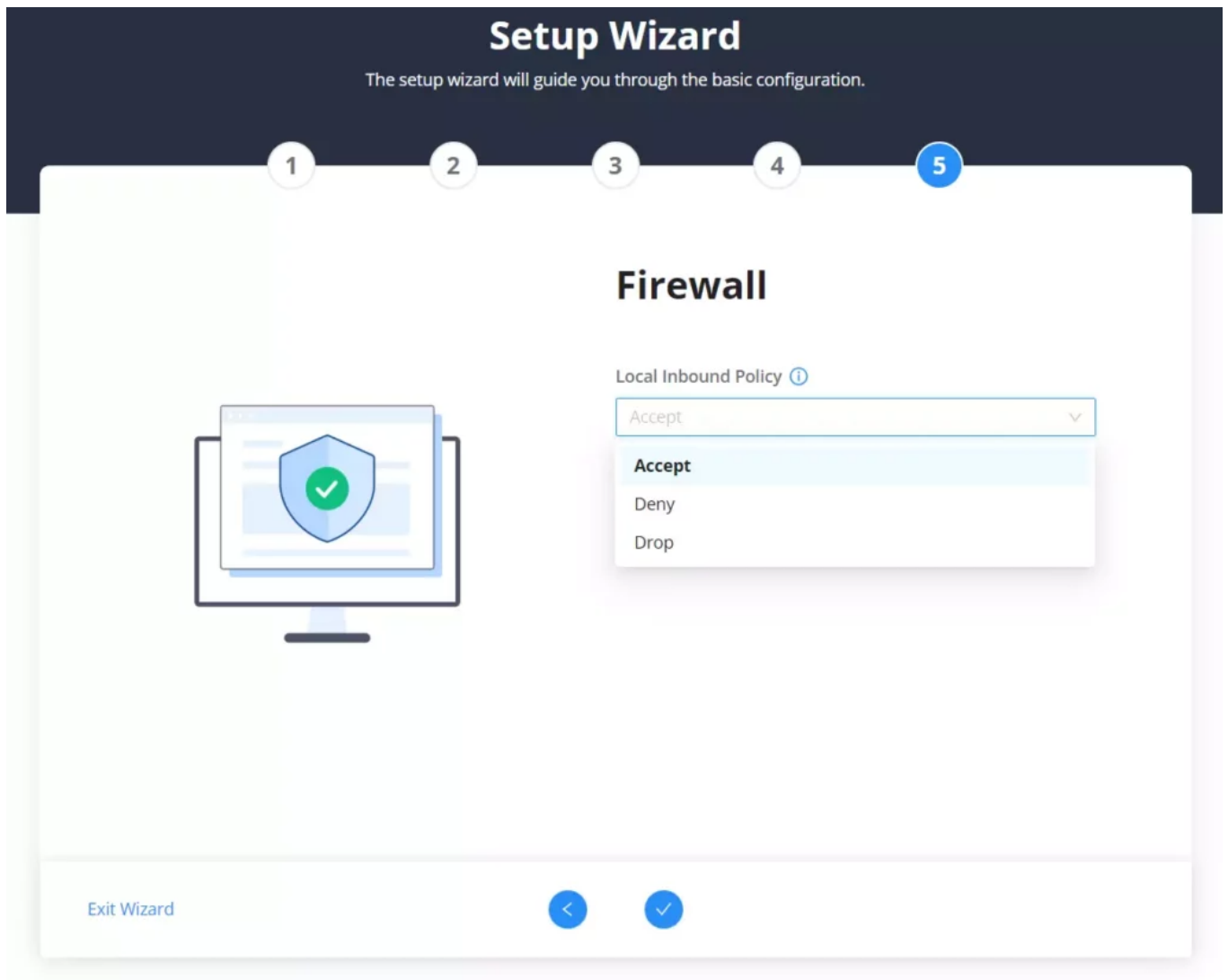
GCC Device Setup Wizard part 7

Step 8: Firewall Policy

Set the **Local Inbound Policy** to control how traffic is handled.

Options:

- **Accept:** Allow incoming traffic.
- **Deny:** Block traffic but respond with rejection.
- **Drop:** Block silently without response.



GCC Device Setup Wizard part 8

Step 9: Setup Complete

Once all steps are completed, a confirmation screen appears.

Click **Go to Overview** to enter the main dashboard and begin using the device. The system will automatically redirect in a few seconds if no action is taken.

Setup Wizard

The setup wizard will guide you through the basic configuration.



Setup is complete, thank you for selecting GCC6010!

The system will automatically switch to the global overview at **2 seconds**.

[Go to Overview](#)

GCC Device Setup Wizard part 9

Interface Language

After logging in for the first time, users can change the Web UI language based on preference.

To do so:

1. Click on your **username** in the top-right corner (default: admin)
2. From the dropdown menu, navigate to **Language**
3. Select your preferred language from the list

Note: The interface will reload automatically in the selected language.



admin ▾

Modify

Modify

Modify

Modify

English

简体中文

正體中文

Español

Français

Português

Русский

Italiano

Polski

Deutsch

Türkçe

Čeština

 Account settings

 Language >

 Reboot

 User Manual

 Version Changelog

 Feedback

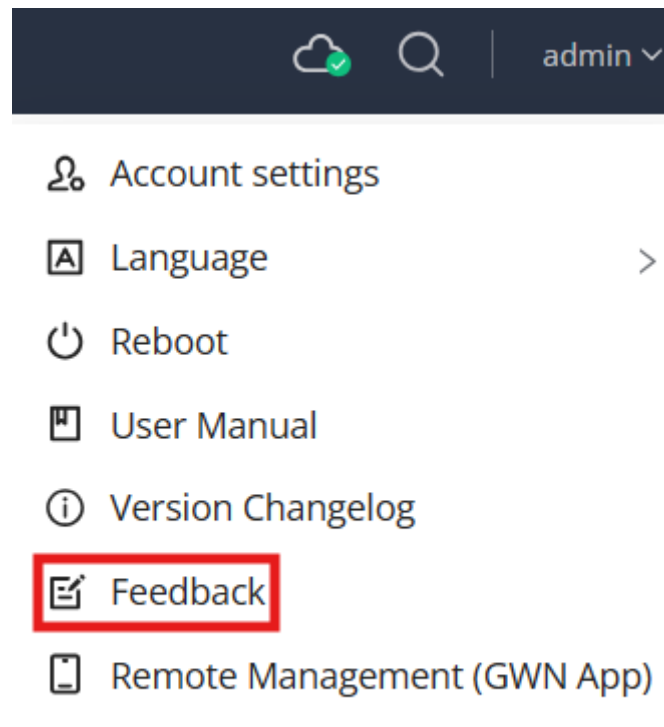
 Remote Management (GWN App)

Logout

Change language

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.



Logout

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

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.

Cancel

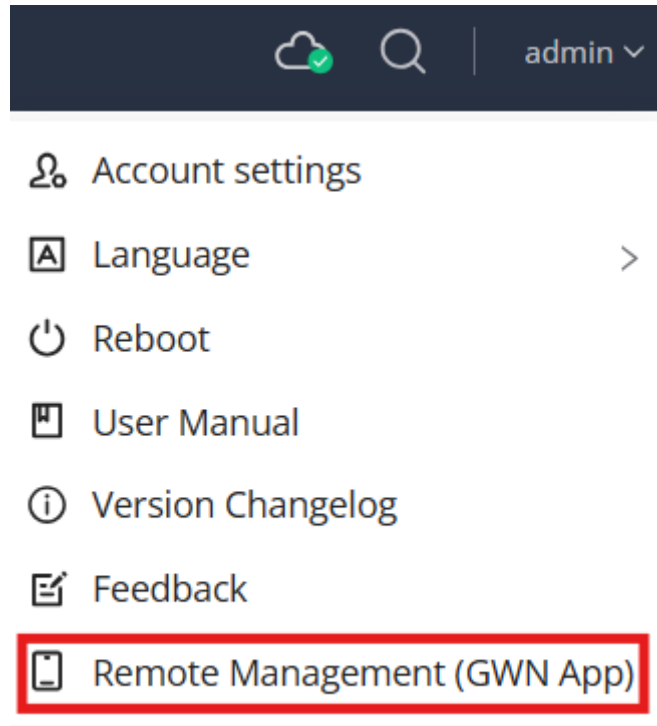
Submit

- 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.



Logout

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



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.



iOS QR Code



Android QR Code

Remote Management GWN App

HOME

Overview

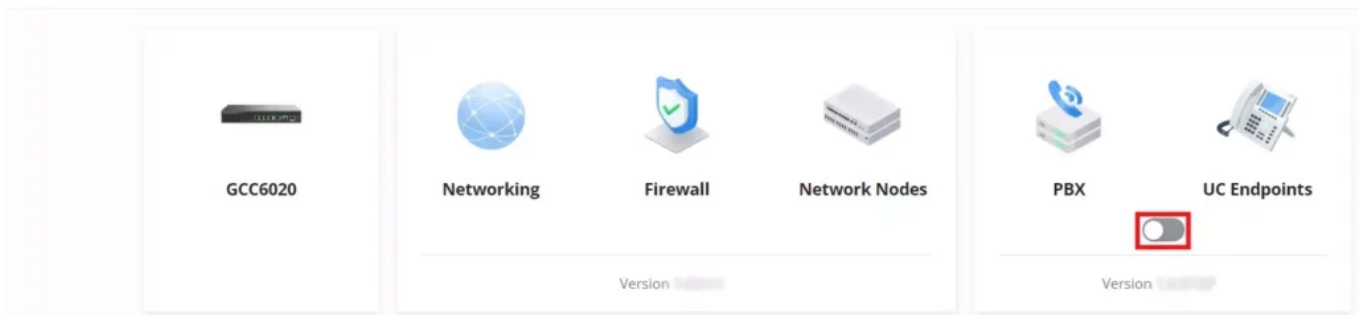
The **Overview** section provides a snapshot of the device's current operational status and system modules. This includes detailed info such as hardware/software versions, system resource usage, licensing, and session statistics.

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**

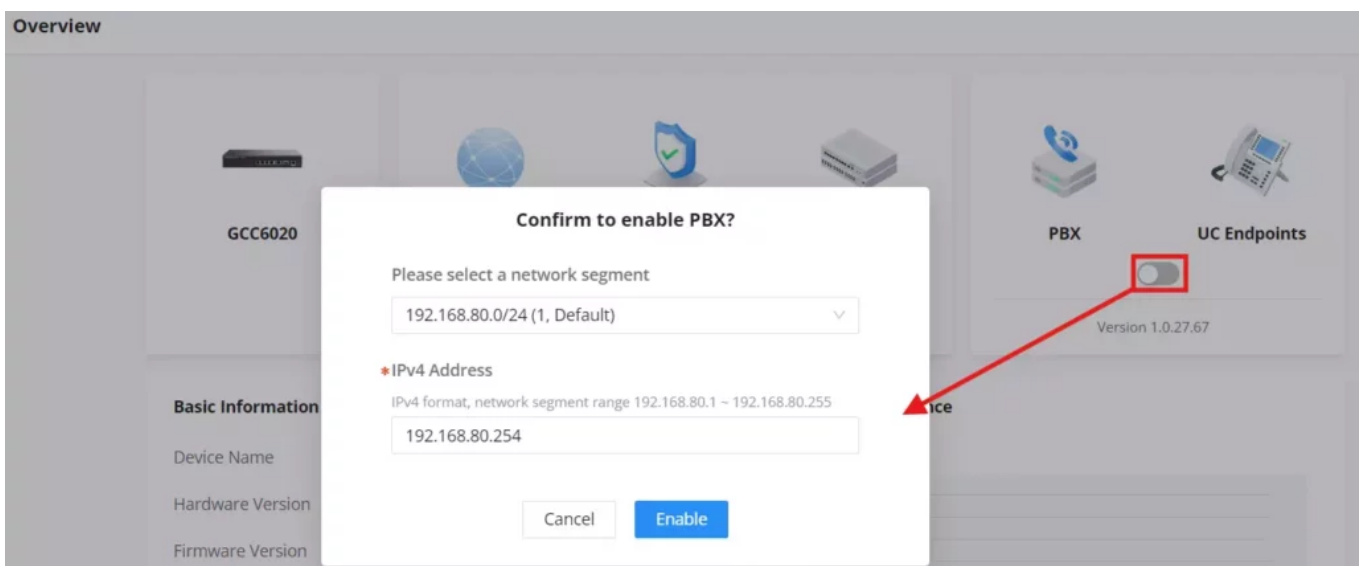
Overview



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.



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

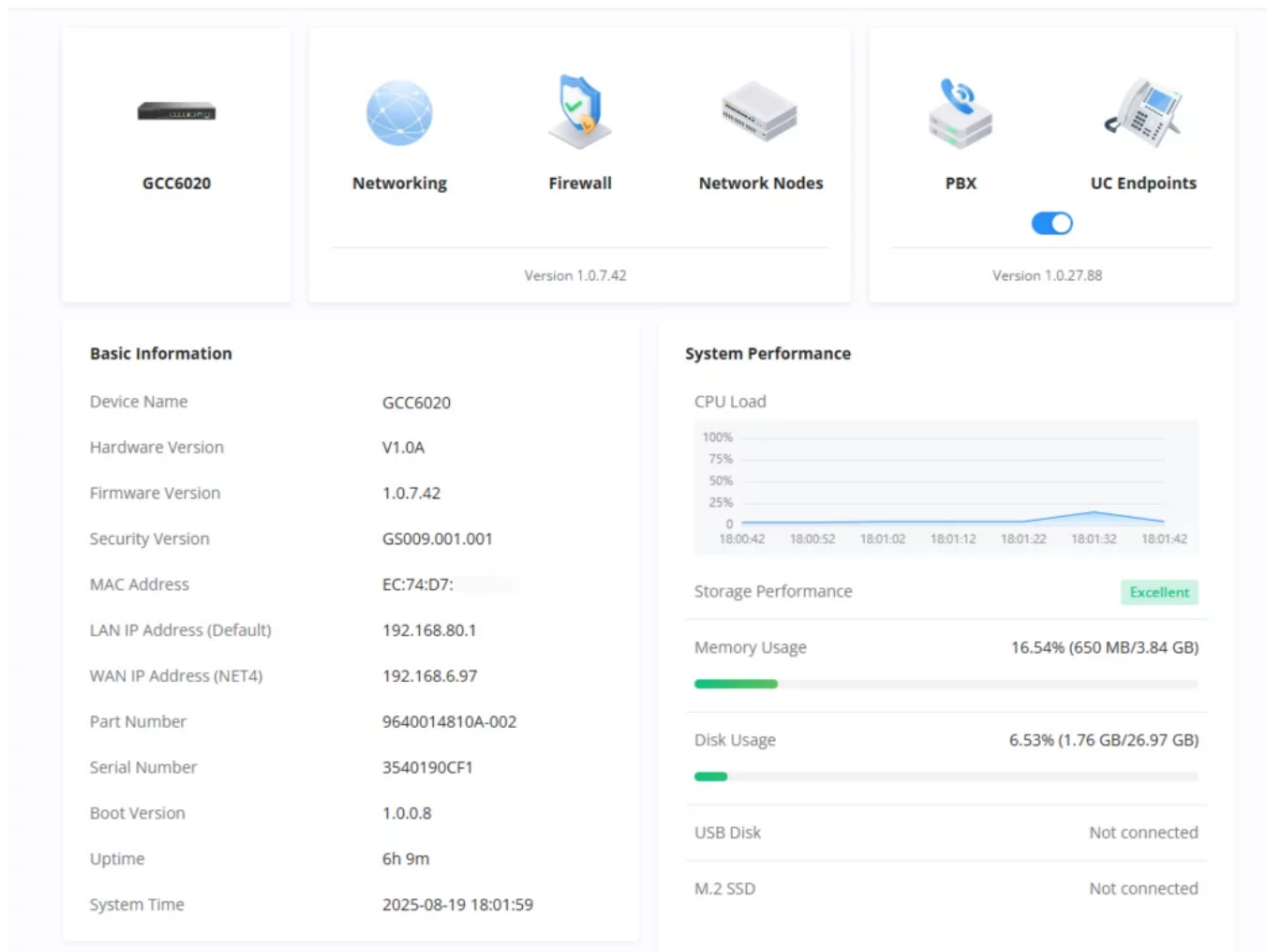
Firewall Service

- Shows current license type and status

PBX

- Displays the current PBX IP address (if enabled)

Overview



Overview page part 2

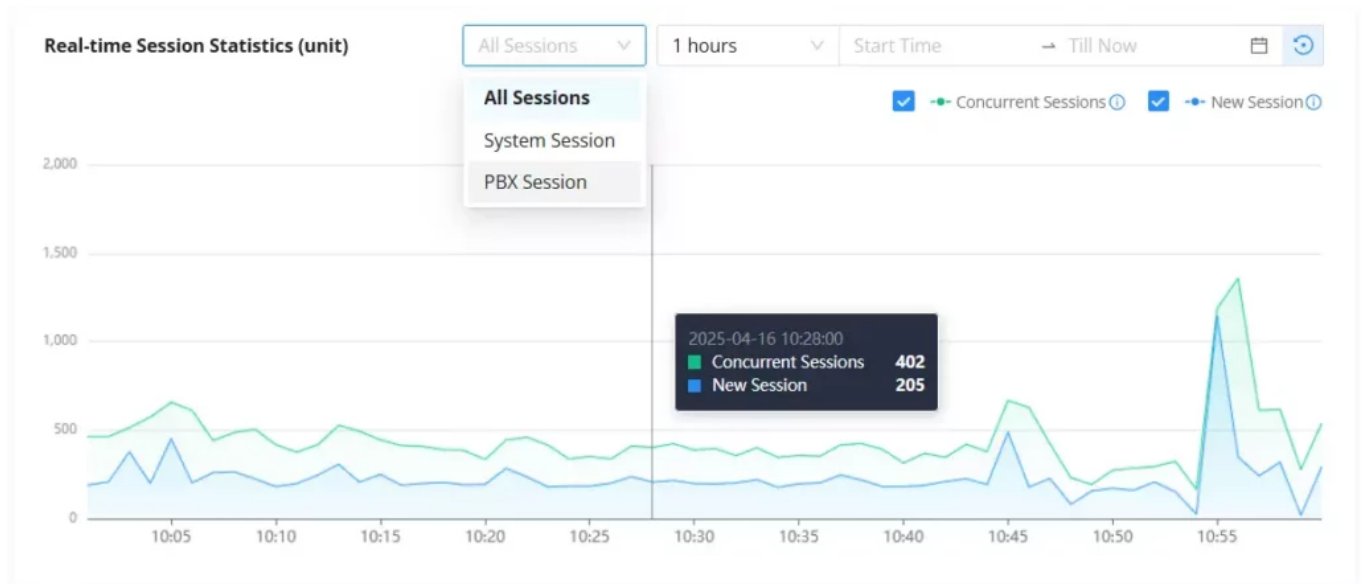
Real-Time Session Statistics

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 duration (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

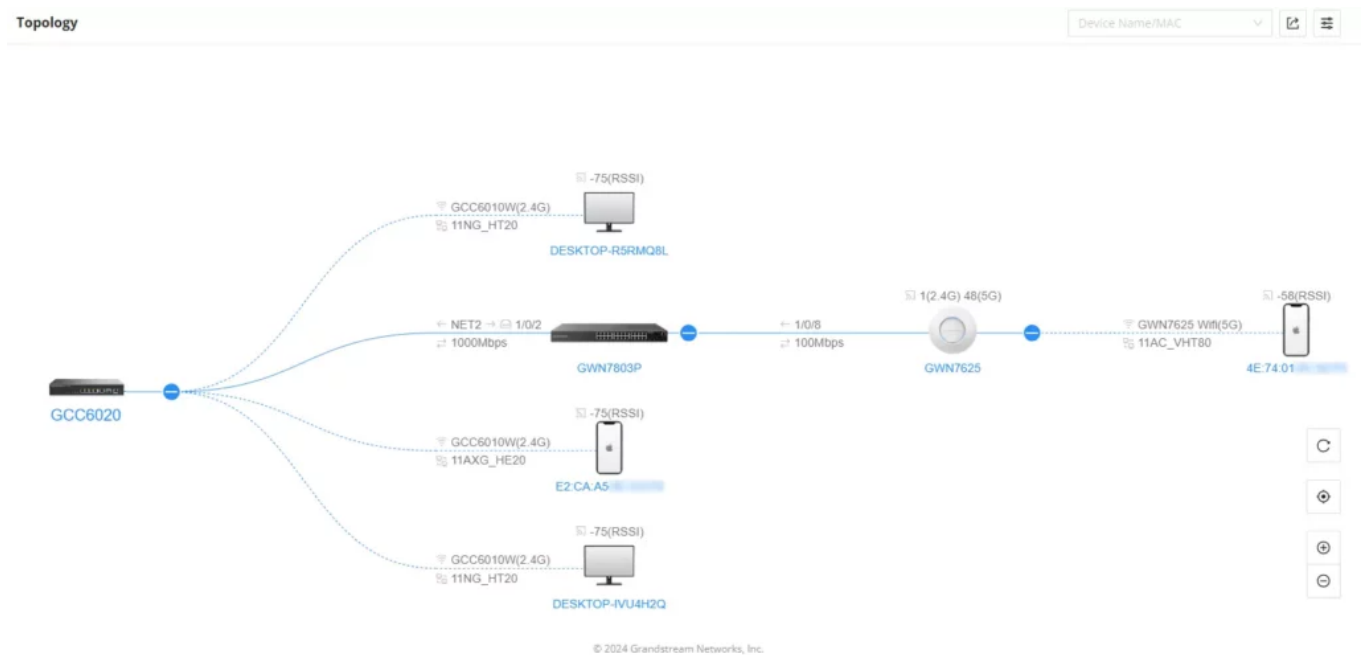
A session refers to a temporary connection or data exchange between devices like loading a webpage, making a call, or streaming data.



Overview page part 3

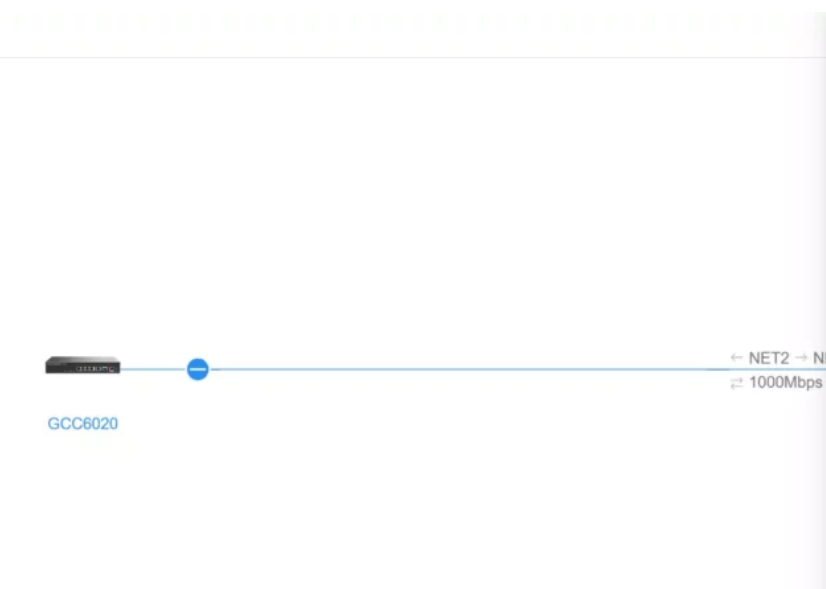
Topology

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



GWN7624

Overview

Connected to [GCC6020](#)

Device Model	MAC
GWN7624	C0:74:AD:88:88:88
Uptime	Firmware Version
3h 55m	1.0.25.34

[More Details](#)

Current Client (0)

Clients	Connection
---------	------------

Icon View

AP Management > **C0:74:AD** [\(GWN7624\)](#)

Details

Client List

Debug

MAC Address	C0:74:AD:88:88:88
Device Model	GWN7624
Part Number	96-4000012-100
Boot Version	0.0.0.1
Firmware Version	1.0.25.34
SSID	GCC6020 (2.4G: c0:74:ad:88:88:88)
IPv4 Address	192.168.80.171
IPv6 Address	-
Gateway IP Address/Mask	-
System Up Time	4h 7min
System Time	2025-05-30 09:13

AP Details

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.

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	GCC6020	1-64 characters
Country / Region	United States	
Time Zone	(UTC-06:00) America/Chicago	
*NTP Server	0.pool.ntp.org	IPv4 address or domain name
	1.pool.ntp.org	
	2.pool.ntp.org	
	3.pool.ntp.org	
	Add	
Sync Time to Managed Devices	☒	
Language	English	
LED Indicator	☒ Always On ☐ Always Off ☐ Enabled based schedule	
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.
LED Indicator	Sets the device's LED behavior. Options include Always On, Always Off, or Enabled based on schedule.

Basic Settings

Manager Server Settings

Basic Settings

Basic Settings

Manager Server Settings

Manager Server Settings



Manage Server Address

Please enter

Manage Server Port

8443

Default 8443, range 1~65535

Allow DHCP Option 43 Override



Cancel

Save

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

[Modify](#)

[Multi-Factor Authentication Instructions](#)

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 GCC6020 device is accessed through the web interface, including WAN accessibility, HTTPS port, IP restrictions, and server certificate settings. This helps strengthen remote management security and limit exposure.

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

Security Settings

Account Settings
Web Access
SSH Access
Remote Access without Password

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

Add

Server Certificate

System Certificate

Cancel

Save

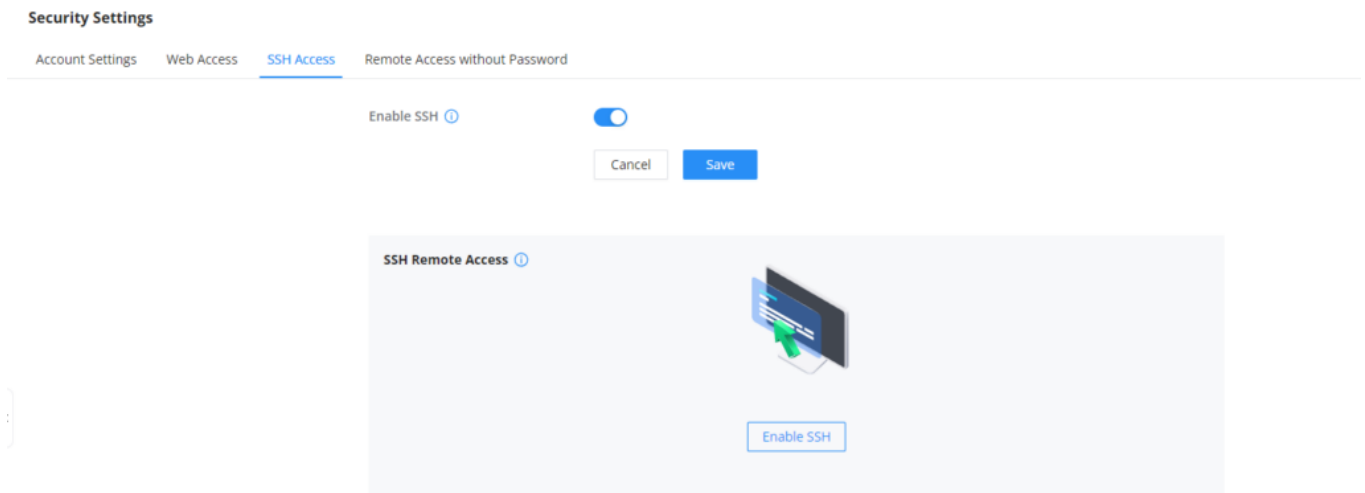
Web Access

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.
Server Certificate	Select the server certificate used for HTTPS access. This certificate is mandatory to be able to access the GCC web GUI using HTTPS. If no valid certificate is configured, then the system will use HTTP instead.

Web Access

SSH Access

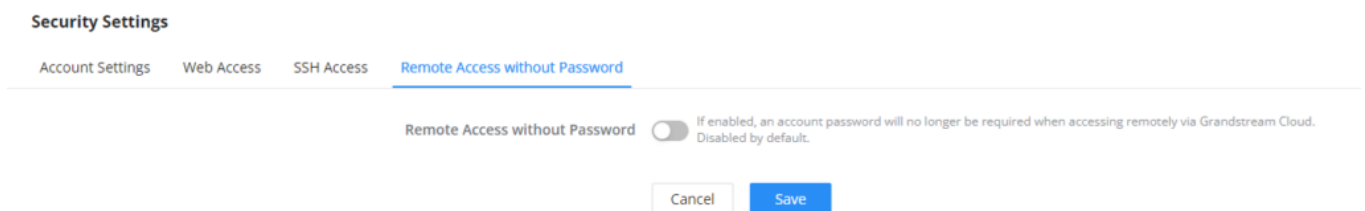
In this section, the user can enable SSH remote access to the device, this includes SSH remote access as well.



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.



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	01	02	03	04	05
Weekly						
06	07	08	09	10	11	12
Weekly						
13	14	15	16	17	18	19
Weekly						
20	21	22	23	24	25	26
Weekly						
27	28	29	30	01	02	03
Weekly						
04	05	06	07	08	09	10
Weekly						

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.

Schedule

New Schedule

Working hours

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							

Cancel

Save

Add a Schedule Weekly

- 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.

Schedule

New Schedule

Working hours

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

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

Cancel

Save

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.

Schedule

New Schedule

new schedule

Working hours

Working hours

April 2025

Su	Mo	Tu	We	Th	Fr	Sa
30	31	01	02	03	04	05
				10	11	12
				17	18	19
				24	25	26

Reference Details

All

Q Name

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

<

1

>

Schedule Reference Details

Administrator

In this page, the administrator can create users with various roles and privileges.

Administrator

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

Administrator

Administrator Role

Add Delete

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

User Information

Add Administrator



***Name**

4-64 characters, including letters, digits, and underscores

***New Password**

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

Confirm the new password

Email

1-64 characters

Mobile Number

2-18 digits

+1

▼

***Role**

***Please enter the current login password**

☐ There will be no more authentication during this login.

Cancel

Save

Add User

Name	Enter the username. The username can consist of 4-64 characters, including letters, digits, and underscores.
New Password	Enter the password. The password can consist of 8-32 characters, need to contain 2 types of numbers/letters/special characters
Confirm the new password	Enter the password again to confirm it.
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
Please enter the current login password	Since only the super administrator is allowed to create other administrators, the super administrator needs to enter their password as a measure of security when creating a new administrator. Enable the option "There will be no more authentication during this login" to disable this measure of security during the configuration session.

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 button.

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

Administrator

Administrator Role

AddDelete

☐	Role Name	Home permissions	Network permissions	Firewall permissions	Network Nodes permissions	PBX permissions	UC Endpoints permissions	Operation
☐	SuperAdmin	Full management	Full management	Full management	Full management	Full management	Full management	

Alt: 2 < 1 > 10 / page

Role

Administrator > Add Role

*Role Name

Please enter

1-64 characters, including letters, digits, and underscores

Home permissions

☐ Full management ☒ Read Only

Network permissions

☒ Full management ☐ No permission ☐ Custom permissions

Firewall permissions

☒ Full management ☐ No permission ☐ Custom permissions

Network Nodes permissions

☒ Full management ☐ No permission ☐ Custom permissions

PBX permissions

☒ Full management ☐ No permission ☐ Custom permissions

UC Endpoints permissions

☒ Full management ☐ No permission

CancelSave

Add role

Email Settings

The Email Settings section allows the GCC6020 device to send notification emails for various system events. When properly configured, the device can deliver emails to specified recipients in response to triggers such as alerts, scheduled meetings, emergency events, and more.

Email notifications can include the following types of information:

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

Email Setting

The configuration interface includes a **Mail Server Providers** option, which defines how email delivery is handled:

- **Common:** Traditional SMTP-based delivery. This mode allows administrators to manually configure all required email settings including SMTP server, authentication, TLS, and sender details.
- **Microsoft:** A streamlined option for Microsoft(R) 365 and Outlook integration. SMTP settings are hidden, and the system requires Microsoft account authorization instead. Only essential delivery fields such as display name and template format are shown.

The interface updates dynamically based on the selected provider to simplify configuration and match the requirements of the chosen email service.

Email Settings

Email Template

Email Footer Hyperlink

Email Send Log

Mail Server Providers

☒ Common
 ☐ Microsoft

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

Cancel

Save

Test

Email Settings Common

Email Settings

[Email Settings](#)[Email Template](#)[Email Footer Hyperlink](#)[Email Send Log](#)

Mail Server Providers

☐ Common☒ Microsoft

Server Authorization

Authentication with Microsoft servers incomplete. Please complete Microsoft authentication first.

[De-authorization >](#)

Email Delivery Settings

Email Template Sending Format ☒ HTML ☐ Plain Text

* Display Name

GCC

1-42 characters

Cancel

Save

Test

Email Settings Microsoft

Mail Server Providers	Select the type of email service provider:Common: Uses standard SMTP configuration.Microsoft(R): Connects to Microsoft(R) 365 or Outlook using account authorization. The available fields will adjust depending on the selected option.
When Mail Server Providers set to Common	
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 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.comNote: 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.
When Mail Server Providers set to Microsoft	
Server Authorization	Displays the Microsoft authorization status. To enable email sending via Microsoft(R) services, users must complete the authentication process. A de-authorization option is available to revoke access.
Email Template Sending Format	Choose whether the email should be sent in HTML or Plain Text format.
Display Name	Specify the display name that will appear in the "From" field of outgoing emails. Maximum 42 characters.

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	
All: 21 < 1 2 3 > 10 / page Go to Page			

Email Template

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

PBX

*

Subject

1-64 characters

Your account of PBX

Message in HTML Format

B

I

U

Open Sans,Ari...

12pt

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

\$(SERVER1_ADDR)

Public IP Address

\$(PUB_ADDR)

Account Name

\$(FULL_NAME)

Preview

Restore Default Template

Template Variables

Cancel

Save

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 .

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

Email Settings Email Template Email Footer Hyperlink Email Send Log

Footer 1

* Text

1-64 characters

* URL

IPv4 or URL address

Footer 2

* Text

1-64 characters

* URL

IPv4 or URL address

Add 

Cancel

Save

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.

Email Settings

Email Settings Email Template Email Footer Hyperlink Email Send Log

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

Show All Logs

Clear

Delete Search Result(s)

 Filter

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



No data

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 SettingsSMS TemplateSMS 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.

Cancel

Save

Save and Test

© 2024 Grandstream Networks, Inc.

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 SettingsSMS TemplateSMS Delivery Log

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 plans 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	[GCC6020] Your Profile Code: \${EXTEN_PROFILE_CODE} Tips: Please enter or use FastProv account to dial the Profile Code on your device to register. \${PROFILE_CODE_USE_LIMITS_NOTIFY}\${PROFILE_CODE_LIVE_TIME_NOTIFY}	
Verification Code	Home	[GCC6020] Your verification code is \${code}. It will expire in 10 minutes.	

SMS Template

SMS Delivery Log

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

SMS SettingsSMS TemplateSMS Delivery Log

Show All LogsClearDelete Search Result(s)

Filter

Send Result	Recipient	Module	SMS Send Module	Last Send Time
-------------	-----------	--------	-----------------	----------------



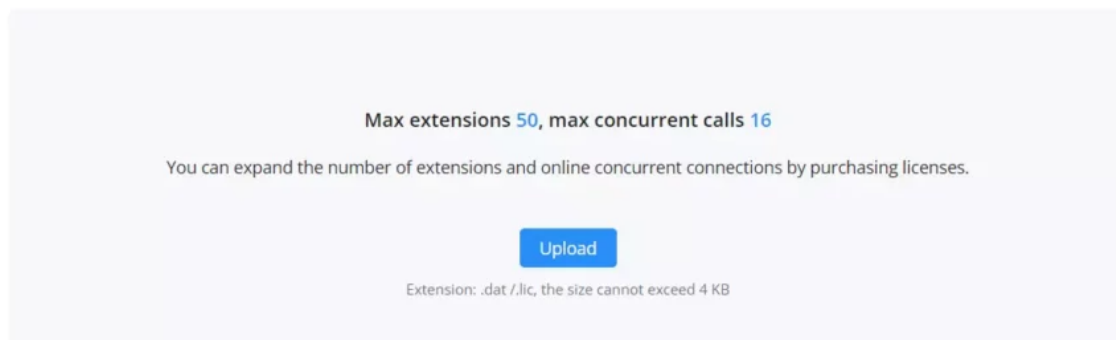
No data

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.

PBX Upgrades



PBX Upgrades

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

Maintenance

Upgrade

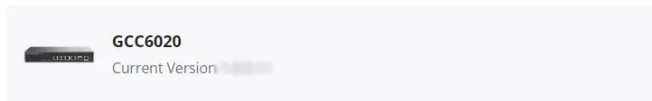
When a new firmware is released for the GCC device, the user can use the "Upgrade" page to update the firmware of the GCC device using different methods of updating the firmware.

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

① To ensure the security of your data, it is recommended that you back up the current configuration information and data before upgrading. [Back Up Now](#)



Online Upgrade

Mode [①](#) ☒ Official Online Upgrade ☐ Upgrade via Network

Firmware Server Path [①](#) firmware.gdms.cloud

Allow DHCP Option 43 and 66 to Override Server [①](#) ☐

Check/Download New Firmware at Bootup [①](#) ☐

Scheduled Upgrade ☐

[Cancel](#) [Save](#) [Save and Check for Updates](#)

Upgrade via Manual Upload

System Firmware (.bin) [Upload](#)

PBX Firmware (.bin) [Upload](#)

System + PBX Firmware (.bin) [Upload](#)

GCC Upgrade

- 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.

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 button to initiate an immediate backup.

1. Choose Storage Location: Local or Storage Server.

- Storage Location: **Local**.

Backup & Restore > **Back Up Now**

*Choose Storage Location

Local (Remaining Capacity: 25.21 GB) ▾

*Selecting Backup Content

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

☐ PBX, UC Endpoints (Only configuration File)

File Name

GCC6020_backup_20250819_180921.tar

[Edit Prefix](#)

Cancel

Backup

New Backup Local

Clicking on "Edit Prefix" allows the user to select the prefixes to include in the name of the backup file for easier identification of the device corresponding to the backup file. The preset prefixes are Device Model, Device Name, and MAC Address. The user can also add a customized prefix.

Backup & Restore > **Back Up Now**

*Choose Storage Location

Local (Remaining Capacity: 25.21 GB) ▾

*Selecting Backup Content

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

☐ PBX, UC Endpoints (Only configuration File)

File Name

GCC6020_EC74D78C9B46_backup_20250819_180921.tar

[Edit Prefix](#)

File Name Prefix Settings

⋮ Device Model

⋮ Device Name

⋮ MAC Address

+ Customize

ⓘ Click to select and drag the icon to adjust the order.

Cancel

Backup

- Storage Location: **Storage Server**.

* Choose Storage Location	Storage Server	
* Storage Server address	Please enter	IP address (allows ":port"), supported SFTP server
* Username	Please enter	
User Password	Please enter	
* Selecting Backup Content	☐ Home, Networking, Firewall, Network Nodes ☐ PBX, UC Endpoints	
File Name	GCC6020_backup_20250819_180921.tar	Edit Prefix
	CancelBackup	

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

Please enter

* Username

Please enter

User Password

Please enter



* Selecting Backup Content

☐ Home, Networking, Firewall, Network Nodes

☐ PBX, UC Endpoints

* Schedule



Cancel

Save

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

Local

Delete

☒	File Name	Size	Time	Operation
☒	GCC6020_backup_20250530_163850.tar	389.50 KB	2025-05-30 10:38:51 UTC-05:00	   
☒	GCC6020_backup_20250530_163827.tar	388.50 KB	2025-05-30 10:38:27 UTC-05:00	   
☒	GCC6020_backup_20250530_163807.tar	388 KB	2025-05-30 10:38:08 UTC-05:00	   

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.
- : 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 GCC6020 configurations will be reset to factory settings. Please proceed with caution! It is recommended to back up the current configurations before factory reset.

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

Factory Reset

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.

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

▼

Keywords

	Content	Type	Level	Time	Operation
☒	Backup successful.	System alarm	General	2025-05-30 10:38:51	
☐	Backup successful.	System alarm	General	2025-05-30 10:38:27	
☐	Backup successful.	System alarm	General	2025-05-30 10:38:08	
☐	Host reboot normally.	Device alarm	General	2025-05-30 02:20:44	
☐	Host reboot normally.	Device alarm	General	2025-05-29 02:07:59	
☐	Host reboot normally.	Device alarm	General	2025-05-28 04:42:46	
☐	PBX module upgraded successfully.	Device alarm	General	2025-05-27 05:02:49	
☐	Host reboot normally.	Device alarm	General	2025-05-27 04:57:59	
☐	Host upgraded successfully.	Device alarm	General	2025-05-27 04:56:41	
☐	Host reboot normally.	Device alarm	General	2025-05-27 02:27:18	

All: 13

<

1

2

>

10 / page

Go to

Page

Notification Center

Notification Settings

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

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.

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

☐ Performance alarm	Urgent	Serious	General
CPU Usage	☒ ≥90%	☒ ≥75%, <90%	☒ ≥50%, <75%
Disk Usage	☒ ≥90%	☒ ≥75%, <90%	☒ ≥50%, <75%
Host average memory 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	☒	--	--
User password change	☒	--	--
Login is prohibited ⓘ	☒	--	--
MFA code verification	--	☒ Verification failed	☒ Verification successful
Create a new user	--	☒ Create failed	☒ Create successful
Backup file	--	☒ Backup failed	☒ Backup successful
Restore Backup	--	☒ Restore failed	☒ Restore successful
Logs kept up to 180 days	--	--	☒ Automatically clean up logs
Disk space reaches 95%	--	--	☒ Automatically clean up logs

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

☐ Simultaneously send email

Email Address 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.

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 .

① Logs are saved for 180 days by default and are automatically cleared when the period expires or the disk space reaches the threshold.

Refresh Export All

Start date → End date All Operating T... All Module Username / IP Address

Date	Username	Operating Terminal	IP Address	Page	Action	Results	Remark
2025-05-30 10:38:51	admin	Local	192.168.5.247 Private IP	Home: Maintenance > Backup & Restore	createBackup	✓	✓
2025-05-30 10:38:35	admin	Local	192.168.5.247 Private IP	Home: Overview	updateComponentSetting	✓	✓
2025-05-30 10:38:27	admin	Local	192.168.5.247 Private IP	Home: Maintenance > Backup & Restore	createBackup	✓	✓
2025-05-30 10:38:08	admin	Local	192.168.5.247 Private IP	Home: Maintenance > Backup & Restore	createBackup	✓	✓
2025-05-30 10:25:34	admin	Local	192.168.5.247 Private IP	Home: System Settings > Schedule	addSchedule	✓	✓
2025-05-30 10:18:47	admin	Local	192.168.5.247 Private IP	Home: Sign in	login	✓	✓
2025-05-30 10:18:44	admin	Local	192.168.5.247 Private IP	Home: Sign in	login	Error Code: -37 (incorrect username or password.)	✓
2025-05-30 09:39:41	admin	Local	192.168.5.247 Private IP	Home: Sign in	login	✓	✓
2025-05-30 09:39:37	admin	Local	192.168.5.247 Private IP	Home: Sign in	login	Error Code: -37 (incorrect username or password.)	✓
2025-05-30 09:24:33	admin	Local	192.168.5.247 Private IP	Home: System Settings > Basic Settings	updateGeneralPrefSettings	✓	✓

All: 55 < 1 2 3 4 5 6 > 10 / page Go to Page

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.

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

To export the logs, press 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.

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

 Download

 Clear

External System Log

Log Server

IPv4 or URL address

Protocol

☒ UDP ☐ TCP ☐ TLS

Log Level

Level

4 - Warning ▼

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

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.

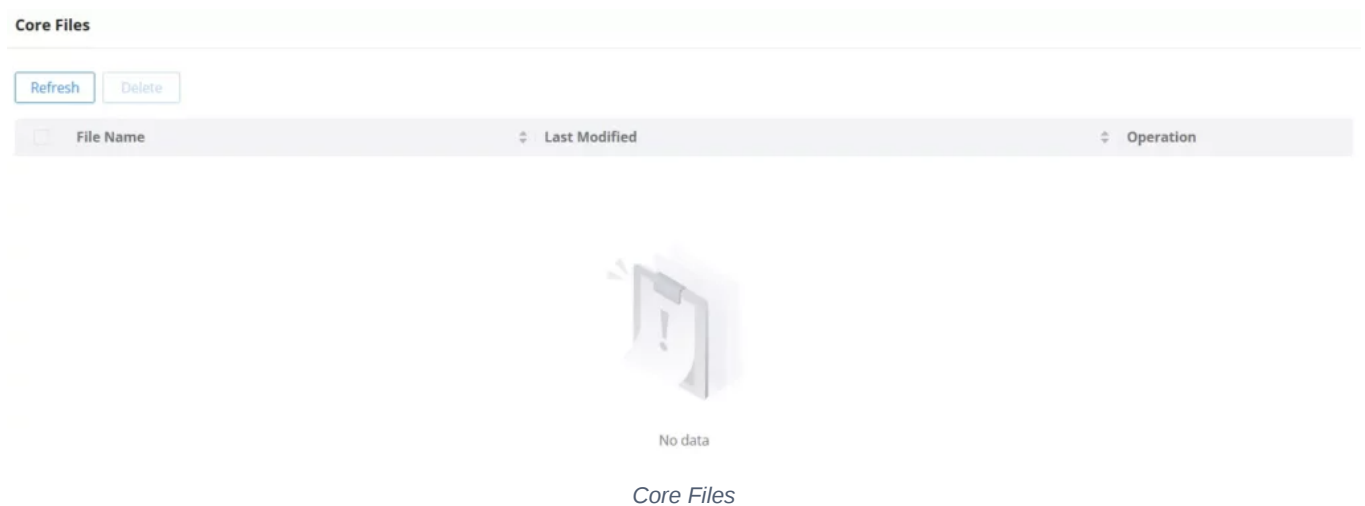
Core Files

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.



NETWORKING

The Networking module of GCC6020 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 GCC device 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 GCC device 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 GCC device 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 GCC device 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 GCC6020. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware version 1.0.7.69 (PBX version 1.0.27.94)

System:

- Ports 25 - 27 can now be configured as WAN ports [[Technical Specifications](#)]
- "User Management" page has been renamed to "Administrator". An additional column "Home Permission" has been added to the "Role" page [[Administrator](#)]

Firewall:

- Added Permission Management section [PERMISSION MANAGEMENT]

Networking:

- Ports 25 - 27 can now be configured as WAN ports [WAN]
- Added Permission Management section [PERMISSION MANAGEMENT]

Network Nodes:

- Added Permission Management section [PERMISSION MANAGEMENT]

Firmware version 1.0.7.59 (PBX version 1.0.27.94)

System:

- Added "Identity Name" information column on the Client page. [Clients]
- Added support for Bridge mode [Bonjour Gateway]

PBX:

- No major changes.

Firmware version 1.0.7.48 (PBX version 1.0.27.90)

System:

- Added support for GDMS new IPsec option "Add Router LAN address", which will allow the router to use its own LAN address to configure local subnet for VPN.

- Added support for [USB 4G/5G dongle].

PBX:

- No major changes.

Firmware version 1.0.7.46 (PBX version 1.0.27.90)

System:

- No major changes.

PBX:

- No major changes.

Firmware version 1.0.7.44 (PBX version 1.0.27.89)

- Security version is now displayed on the Overview page. [[Overview](#)]
- Added prefix configuration for the filename of the backup file. [[Backup](#)]
- Added firewall enabling configuration and local inbound policy configuration to the setup wizard. [[Setup Wizard](#)]

Firmware version 1.0.7.32 (PBX version 1.0.27.70)

System:

- This is the initial version.

PBX:

- This is the initial version.

Microsoft(R) is a registered trademark of Microsoft Corporation in the United States and/or other countries. All other trademarks and registered trademarks are the property of their respective owners.
