Grandstream Networks, Inc.

UCM630x/A

HA User Guide

UCM630x/A HA – User Guide

High Availability feature on Grandstream UCM6300 series/UCM6300 Audio series provides enterprises a reliable solution for PBX redundancy and failover support. In HA setup, there are two UCM with one UCM in the "active" role and the other in the "standby" role. The two UCM must be the same model and use the same firmware version. The data on the active UCM will be synchronized to the standby UCM in a real-time manner and the standby UCM monitors the active UCM's running status regularly. When the active UCM runs into hardware or critical software issues, the standby UCM will take over immediately and become the active server. HA feature supports automatic call recovery for UDP point-to-point calls and conference calls, allowing enterprises to communicate and collaborate without the hassle of service interruption.

TYPICAL NETWORK TOPOLOGY

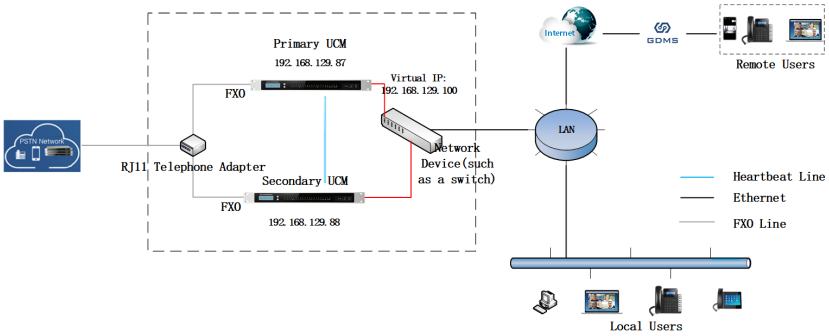

Figure 1: Typical Network Topology

The two UCM in High Availability setup must be deployed in the same location and connected directly to each other via the heartbeat port on each UCM. The primary UCM and secondary UCM can be connected to each other via a straight-through Ethernet cable on the heartbeat port. For each UCM, connect its WAN or LAN port to the uplink network device. For the FXO port, an RJ11 telephone adapter is required to split the PSTN line connection into two ports for each UCM's FXO port to connect to.

HA PREREQUISITES

Prerequisites

The two UCM used for High Availability deployment must be the same model and use the same firmware version to ensure proper sync-up on the configuration and data.

Connecting UCM for HA Setup

The two UCM in High Availability setup must be deployed in the same location and connected directly to each other via the heartbeat port on each UCM.

- Connect a straight-through Ethernet cable between the heartbeat port on the primary UCM and secondary UCM.
- For each UCM, connect its WAN or LAN port to the uplink network device (such as a switch or router).
- For FXO port, an RJ11 telephone adapter is required to split the PSTN line connection into two ports for each UCM's FXO port to connect to. The same FXO port must be used on each UCM when connecting to the adapter.

Network Configuration

Before enabling the High Availability feature on the two UCM, the system admin must configure each UCM with proper network settings.

Notes:

- The network "Method" on the UCM must be set to "Switch".
- The IPv4 address configured on the UCM must be static IP. It can be configured under UCM web UI→Network Settings→Basic Settings.

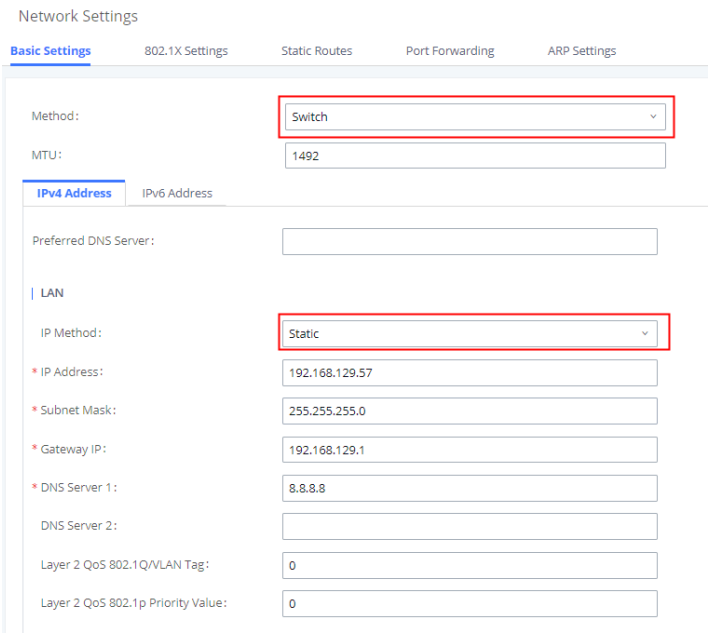

Figure 2: Network Settings

Storage Device

Before enabling High Availability feature on the two UCMs, the system admin must check to ensure both UCM devices have the same storage devices connected and the same storage configuration in place. This is to ensure that the standby UCM device can store the data normally.

For example, if UCM A has one SD card and one USB storage device connected, UCM B must have a SD card and a USB storage device with the same capacity connected as well. If UCM A has configured to use GDMS cloud storage, UCM B must support and use GDMS cloud storage as well. Please note the UCM admin doesn't necessarily need to configure storage path to be the same at this point because the active UCM's configuration will be applied to the standby UCM after HA is enabled.

The UCM storage configuration and status can be found under UCM webUI->System Status->Dashboard:

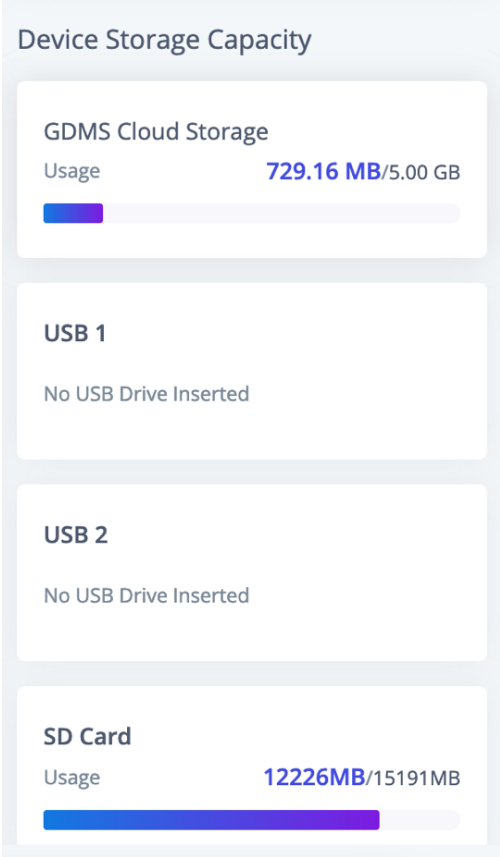

Figure 3: Storage Status Under Dashboard

HA Configurations

For UCM without UCM RemoteConnect Plan

For two new UCM on the factory default setting, the system admin can choose to configure any of them for HA first. However, if one of the UCM is already configured, up and running for PBX service, the system admin should configure this UCM as an HA Primary server and complete all HA settings on it first so it can act as an active role. Assuming no UCMRC (RemoteConnect) service is used on any UCM, please refer to the steps below to configure HA on UCM:

1. Ensure both UCM have the same model and same firmware version. They have been connected properly at the same location and configured with static IP. The UCM admin also needs to ensure that the same type and amount of storage is connected to each UCM.
2. Select one UCM to be the active device (UCM A). If both UCM are new on factory default settings, select any of them as the active UCM. If one of the UCM is already configured and running, then select this UCM as the active device.
3. If Cloud IM service is needed, please enable Cloud IM on UCM A (active UCM) and ensure Cloud IM is disabled on the other UCM (UCM B).
4. Log in the active UCM (UCM A) web UI and go to System Settings→HA page. Enable HA and configure UCM A as Primary station type. Please refer to HA related parameters in table 2 below and complete other HA related settings. Save the HA settings on UCM A and reboot UCM A. Ensure UCM A boots up normally.

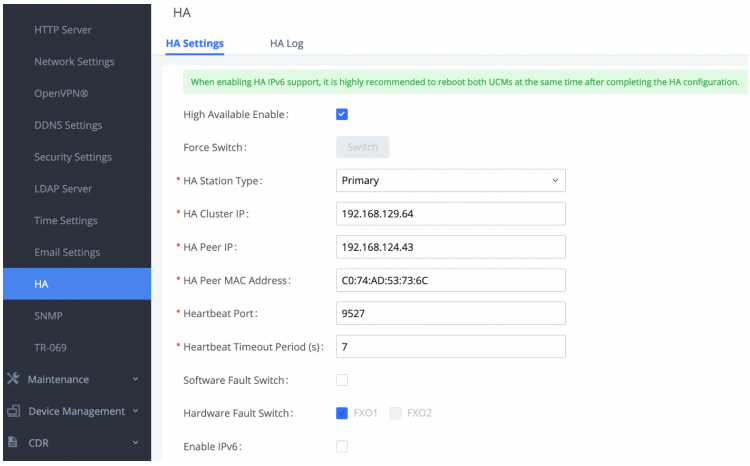

Figure 4: HA Settings on Primary UCM

5. Verify HA status on UCM A. Log in UCM A using its static IP and admin login information. On web UI→System Settings→HA page, ensure HA function is enabled. HA status should display "Active".
6. After ensuring UCM A's HA status as active, configure UCM B as secondary UCM and complete UCM B's HA settings. Log in UCM B's web UI and go to System Settings→HA page, enable HA and set the station type as "Secondary". Please refer to HA related parameters in table 2 below to complete other HA related settings. Save the settings and reboot UCM B.

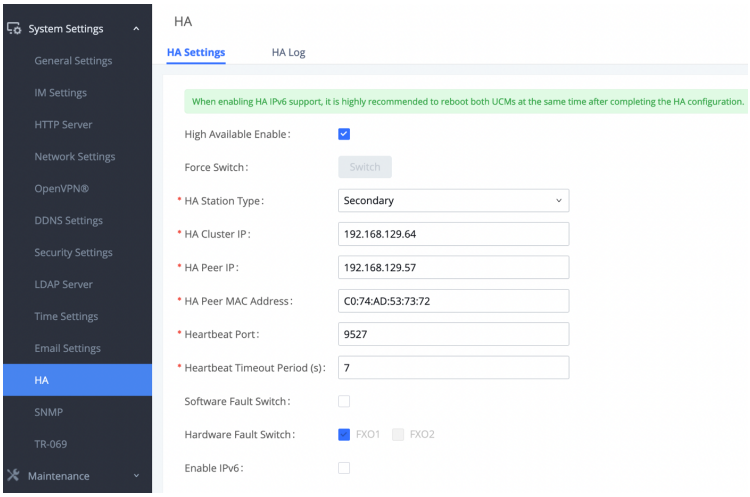

Figure 5: HA Settings on Secondary UCM

7. After UCM B boots up normally, log in UCM B's web UI via its static IP address and admin login information. Go to System Settings→HA page, ensure the HA function is enabled, "Switch" button is grey and only HA peer IP / peer MAC address options are available for configuration. The HA status should display as "Standby".

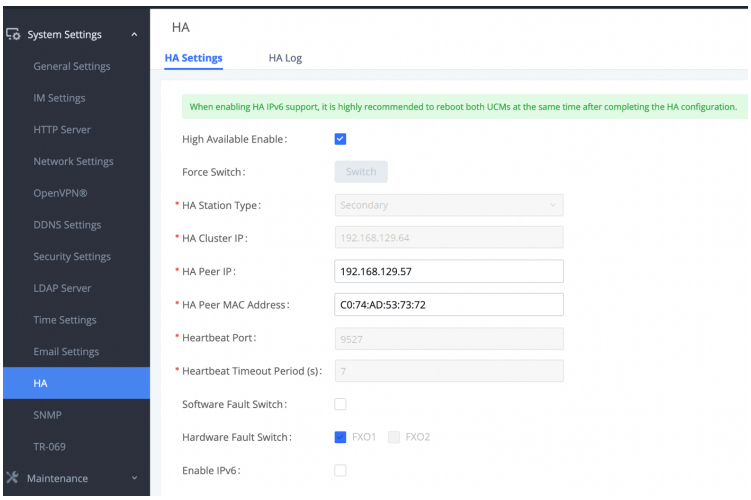

Figure 6: HA Configured on Secondary UCM

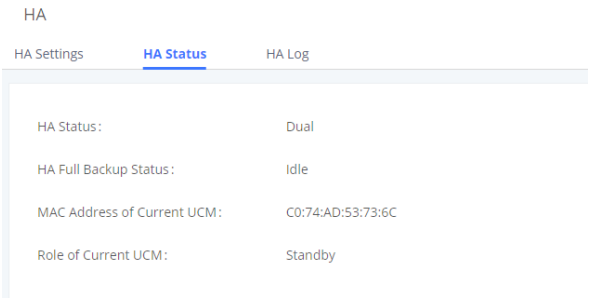

Figure 7: HA Status on Secondary UCM

For UCM with UCM RemoteConnect Plan

Scenario 1: Two new UCMs on factory default settings and both UCM use UCM RemoteConnect service.

1. Ensure both UCM have the same model and same firmware version. They have been connected properly at the same location and configured with static IP. The UCM admin also needs to ensure that the same type and amount of storage devices are connected to each UCM.
2. Since both UCM are on factory settings, select any of the UCM to be the active UCM (UCM A).
3. If Cloud IM service is needed, please enable Cloud IM on UCM A (active UCM) and ensure Cloud IM is disabled on the other UCM (UCM B). When UCM uses Cloud IM servers from GDMS, please ensure that both UCMs have a UCM RemoteConnect plan with Cloud IM support.
4. Log in the active UCM (UCM A) web UI and go to **System Settings→HA** page. Enable HA and configure UCM A as Primary station type. Please refer to HA related parameters in table 2 below and complete other HA related settings. Save the HA settings on UCM A and reboot UCM A. Ensure UCM A boots up normally.
5. Verify HA status on UCM A. Log in UCM A using its static IP and admin login information. On web **UI→System Settings→HA** page, ensure HA function is enabled. HA status should display as "Active".
6. After ensuring UCM A's HA status is active, now configure UCM B as secondary UCM and complete its HA settings. Log in UCM B's web UI and go to **System Settings→HA** page, enable HA and set the station type as "Secondary". Please refer to HA related parameters in table 2 below to complete other HA related settings. Save the settings and reboot UCM B.
7. Verify UCM B's HA status. UCM B boots up normally, log in UCM B's web UI via the static IP address and admin login information. Go to **System Settings→HA** page, ensure the HA function is enabled, "Switch" button is grey and only HA Peer IP / Peer MAC address options are available for configuration.
8. Purchase UCM RemoteConnect plan for both UCM. Log in UCM web UI and go to **WebUI→RemoteConnect→Plan** page, click on "Learn More". Then follow the page to add the 2 UCM to GDMS and assign UCM RemoteConnect plan for them. It doesn't matter which UCM is assigned with UCM RemoteConnect plan first.
9. For UCM A which has station type "Primary", configure custom domain name. Please refer to "Custom Domain Configuration" section below.

> **Note:**
>
> For UCMRC related settings, please refer to section "UCMRC Configurations".

Scenario 2: 1 UCM is configured and running, and the 2nd UCM needs to be added for HA setup. Both UCMs use UCM RemoteConnect service.

1. Ensure both UCM have the same model and same firmware version. They have been connected properly at the same location and configured with static IP. The UCM admin also needs to ensure that the same type and amount of storage devices are connected to each UCM.
2. Since UCM A is already configured and running, choose this UCM as the active UCM.
3. If Cloud IM service is needed, please enable Cloud IM on UCM A (active UCM) and ensure Cloud IM is disabled on the other UCM (UCM B). When UCM uses Cloud IM servers from GDMS, please ensure that both UCMs have a UCM RemoteConnect plan with Cloud IM support.
4. Log in the active UCM (UCM A) web UI and go to **Web UI→System Settings→HA** page. Enable HA and configure UCM A as Primary station type. Please refer to HA related parameters in table 2 below and complete other HA related settings. Save the HA settings on UCM A and reboot UCM A. Ensure UCM A boots up normally.
5. Verify HA status on UCM A. Log in UCM A using its static IP and admin login information. On web **UI→System Settings→HA** page, ensure HA function is enabled. HA status should display "Active".
6. After ensuring UCM A's HA status as active, now configure UCM B as secondary UCM and complete its HA settings. Log in UCM B's web UI and go to **System Settings→HA** page, enable HA and set the station type as "Secondary". Please refer to HA related parameters in table 2 below to complete other HA related settings. Save the settings and reboot UCM B.
7. Verify UCM B's HA status. UCM B boots up normally, log in UCM B's web UI via the static IP address and admin login information. Go to **System Settings→HA** page, ensure the HA function is enabled, "Switch" button is grey and only HA peer IP/HA MAC address buttons are available for configuration.
8. Purchase UCM RemoteConnect plan for each UCM and ensure the purchased plan for each UCM has the same specification and supports HA. It doesn't matter which UCM is assigned with UCM RemoteConnect plan first.
9. For UCM A which has station type "Primary", configure custom domain name. Please refer to custom domain name configuration section below. If UCM A already has custom domain name, this step can be skipped.

> **Note:**
>
> For UCM RemoteConnect related settings, please refer to section "UCMRC Configurations".

HA CONFIGURATION PARAMETERS

Settings	Description	Value Range	Default Value	Notes
High Available Enable	Enable or disable HA.	Yes/No	No	
Force Switch	Force to switch the roles of active UCM and standby UCM.	NA	NA	Caution: Please do not use this function unless necessary (e.g., it can be used during firmware upgrading).
HA Station Type	Configure the HA station type for the UCM.	Primary Secondary	NA	In HA setup, one UCM must be primary and the other one must be secondary.
HA Cluster IP	This is the IP address for the active UCM in service.	NA	NA	This IP address is shared by the primary and secondary UCM. The UCM in active status providing PBX service will always be using this IP address regardless it's the primary or secondary UCM. This IP address can only be used for the active UCM.
HA Peer IP	This is the IP address of the peer UCM in HA setup.	NA	NA	This is the static IP address of the peer UCM in HA setup connected via heartbeat port.
HA Peer MAC Address	This is the MAC address of the peer UCM in HA setup.	NA	NA	This is the MAC address of the peer UCM in HA setup connected via heartbeat port.
Heartbeat Port	This is the port used for communication between the two UCM via the heartbeat port.	0 – 65535	9527	It is recommended to use default port.
Heartbeat Timeout Period (s)	This is the heartbeat timeout period that active and standby UCM will check with each other for the status (in seconds).	3 – 10	7	If the standby UCM detects the active UCM disconnected when it reaches the timeout, failover will be triggered and the standby UCM will start taking over as active UCM.
Software Fault Switch	Enable failover upon software failure	On/Off	Off	If enabled, when there is critical software failure such as deadlock or system crash detected, it will trigger failover from active UCM to standby UCM. Otherwise, failover will not happen.
Hardware Fault Switch	Enable failover upon hardware failure	On/Off	Off	If enabled, when there is hardware failure such as FXO port no longer working, it will trigger failover from active UCM to standby UCM. Otherwise, failover will not happen.
Enable IPv6	If enabled, HA will support IPv6 while compatible with IPv4.	On/Off	Off	Please enable this option if IPv6 is required for HA deployment. Otherwise, please keep it off. Before enabling this option, please configure both UCMs with static IPv6 address.

Table 1: HA Related Parameters

After enabling the High Availablity feature, please configure the following parameters:

- **Station Type (mandatory):**
  In HA setup, one UCM must be set as primary and the other one must be set as secondary. The two UCMs cannot be configured as the same type. Otherwise, HA function will not work properly. This configuration is to ensure that there is always a UCM on active status and the other one on standby status during negotiation which will automatically determine the active/standby server. When a failure condition happens, it is crucial that the failover mechanism does not end up with two active servers negotiated.

  The active UCM is the PBX providing service and it's not always the primary server configured in HA. The primary/secondary station type is configured but any UCM in HA setup can be the active or standby role when needed. For example, if UCM A is configured as the primary station type and UCM B is configured as the secondary station type, at the beginning UCM A is in an active role and UCM B is in a standby role. After failover happens, UCM A's station type configuration is still primary but it's now in standby role and UCM B is in an active role.

- **HA Cluster IP (mandatory):**
  This is the IP address for the UCM that provides PBX service in HA setup. This IP is always associated with the UCM in active status. For example, when configuring an IP phone to register to UCM, this is the SIP server IP address to be configured on the IP phone. When configuring the SIP peer trunk, this is the SIP server IP address to be configured as the

peer trunk server IP. In the HA setup, the static IP configured for each UCM will not be used for PBX service directly. Normally the cluster IP address is in the same subnet as the static IP address configured on the UCM.

- **HA Peer IP (mandatory):**
  This is the static IP configured on the peer UCM in HA setup. This is used for notifying GDMS when active and standby roles change.

- **Peer MAC Address (optional):**
  This is the MAC address of the peer UCM in HA setup. It is used for UCM with Remote Connect service to configure the MAC address of the peer UCM.

- **Heartbeat Port (mandatory):**
  This is the port used for communication between active and standby UCM for heartbeat negotiation. It is recommended to use the default port number 9527.

- **Heartbeat Timeout Period (mandatory):**
  This is the timeout period for the heartbeat (in seconds). The standby UCM will check regularly whether the active UCM is working normally. If the standby UCM detects that the active UCM has been disconnected for this period, the standby UCM will consider the active UCM in a faulty state and will then automatically take over as active UCM.

- **Software Fault Switch:**
  If enabled, when the active UCM experiences software failure such as a system crash with core dump generated, it will trigger failover automatically and the standby UCM will take over. If disabled, HA alert events will be reported without failover.

- **Hardware Fault Switch:**
  If enabled, when the active UCM has hardware failure such as FXO port no longer working, it will trigger failover automatically and the standby UCM will take over. If disabled, HA alert events will be reported without failover. Please note that plugging or unplugging telephone cable on FXO port is not considered a hardware failure.

- **Force Switch:**
  This will force active and standby UCM to switch roles. It will trigger the standby UCM to take over and switch the active UCM to the standby role. This should be used only when necessary, such as firmware upgrading or if active UCM cannot automatically trigger a switchover.

- **Enable IPv6**:
  If enabled, HA will support IPv6 while compatible with IPv4. Please enable this option if IPv6 is required for HA deployment. Otherwise, please keep it off. Before enabling this option, please configure both UCMs with static IPv6 address.

After the above configurations, click on Save and follow the reboot prompt to reboot the device.

> **Critical Note**
>
> HA configuration requires the UCM to reboot. Please reboot the UCM during non-service hours to avoid service interruption.

UCM RemoteConnect Configurations

UCM RemoteConnect Plan

To ensure that the UCM RemoteConnect plan can be used normally on HA setup, the UCM RemoteConnect plan must be purchased and assigned to both UCM on GDMS. If only one UCM has a UCM RemoteConnect plan, the GDMS operation may fail due to HA backup. If only one UCM has UCM RemoteConnect plan with HA support, HA-related functions will not work in HA deployment.

Log into GDMS web UI and go to UCMRC→UCM Devices. Click to add a new device and enter the UCM information.

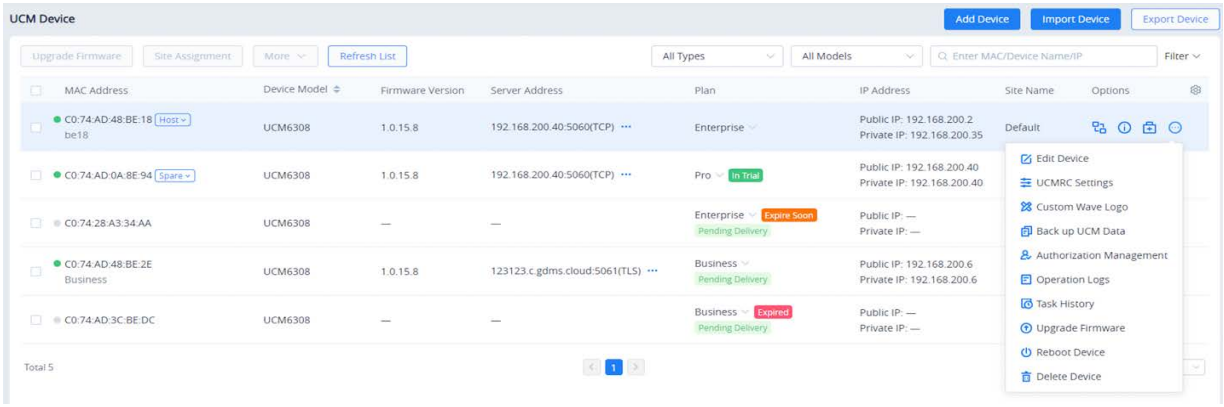

Figure 8: Add UCM to GDMS

Custom Domain Configuration

> **Info**
>
> If you need purchase UCM RemoteConnect plan with custom domain, please use the following link to refer to more details and to purchase the corresponding plan. https://ucmrc.gdms.cloud/plans

For UCM with UCM RemoteConnect service already, configure the custom domain name for the primary UCM (station type "Primary") and ensure this UCM uses a custom domain name.

Custom Domain Name must be set via GDMS. Log in GDMS and go to UCMRC System→UCM Devices, select the UCM and click on "Edit Device" to configure it.

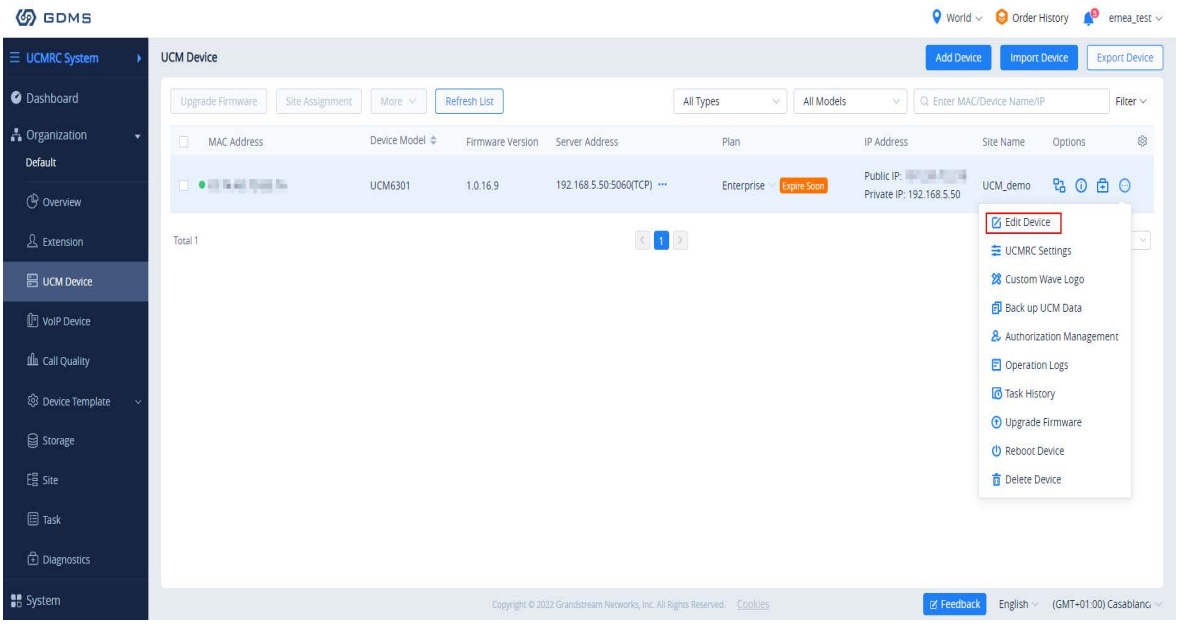

Figure 9: Edit Device

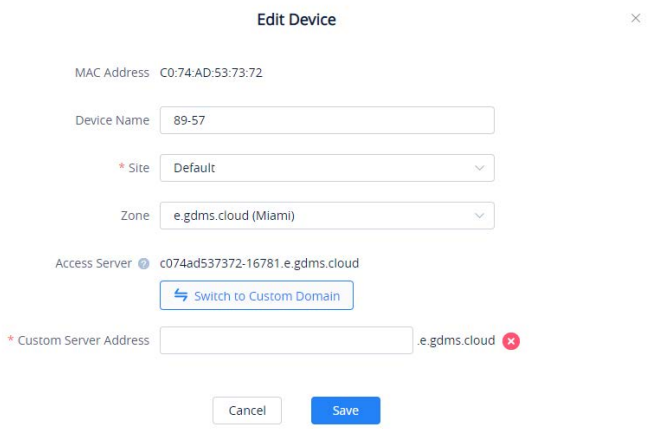

Figure 10: Configure Custom Domain

Click on "Switch to Custom Domain" to edit device custom server access, private secret key and etc. Save the configuration. After changing the custom domain name, please notify UCM users of the new public address for UCM. For more information about configuring a custom domain name on GDMS, please refer to the GDMS user manual.

Verify HA Settings

1. After configuring HA settings on both UCMs, log in the UCM web UI from each UCM's static IP using the active UCM's login information and check HA status. Under HA status page, both UCM should show HA Status as "Dual". One of the UCM should show its role as "Active" and the other one should show "Standby". For "HA Full Backup Status", it will show backup in progress during backup and show as idle during the rest of the time.

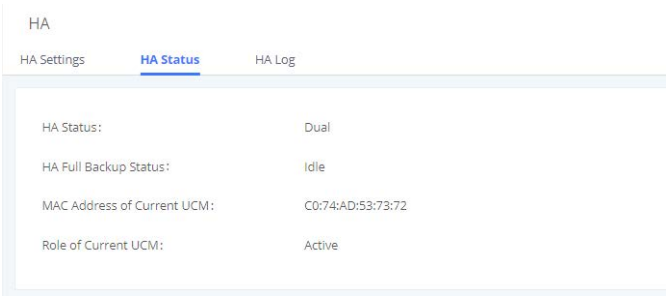

Figure 11: HA Status for Active UCM

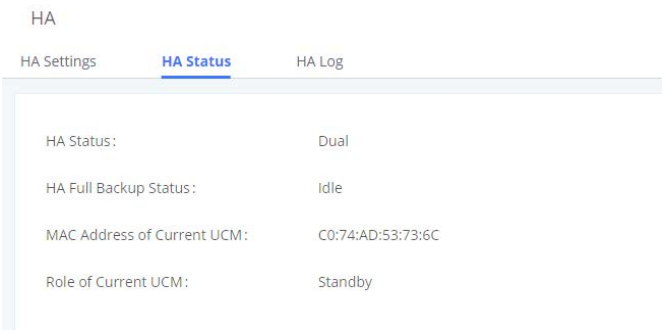

Figure 12: HA Status for Standby UCM

2. Log in the active UCM's web UI and create new SIP extensions. Then log in the standby UCM's web UI to check whether the same extensions created on active UCM are synchronized here. If there are already endpoints registered to UCM, both UCM should show the same extensions and registration status. This indicates that the active UCM's data has been synchronized to the standby UCM.

Verify HA Status via GDMS

GMDS allows the user to verify which UCM is primary and which one is secondary. On the GDMS interface, go to **UCM Device** tab.

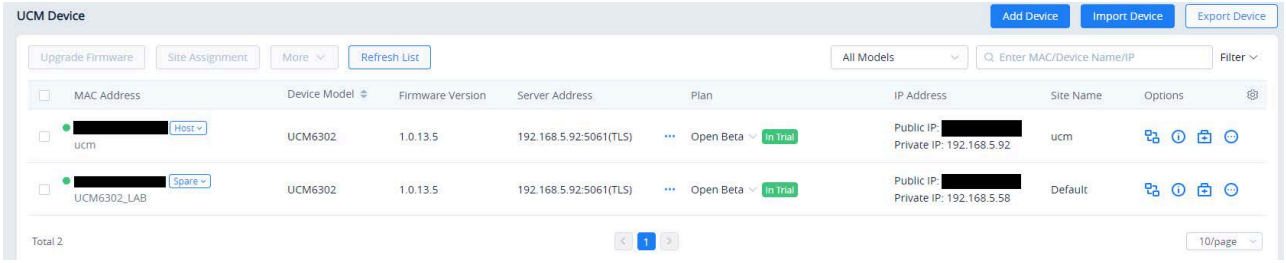

figure 13: UCM Devices

- **Host**: indicates the primary UCM.
- **Spare:** indicates the secondary UCM.

If you want to check which UCM is performing high availability with which UCM, click on "spare" or "host" to verify, as indicated in the screenshots down below.

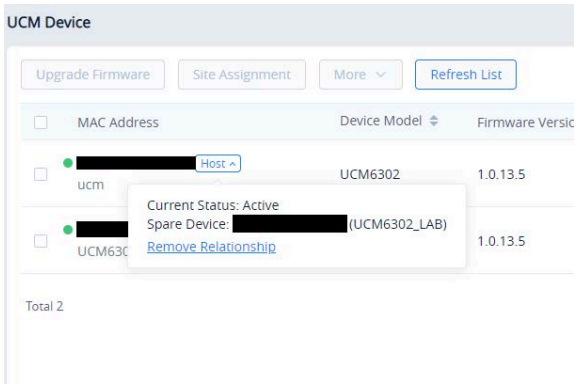

figure 14: Active UCM

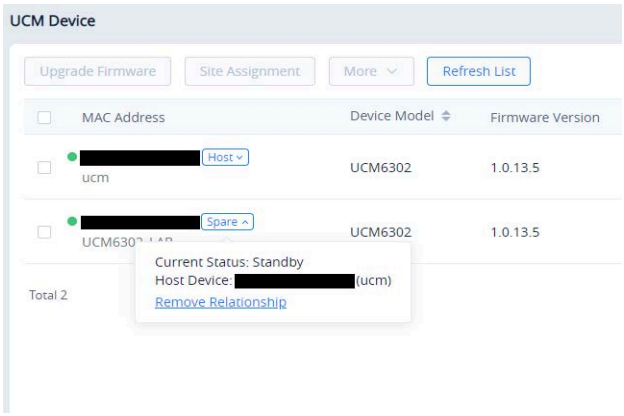

figure 15: Idle UCM

Active/Standby Role in HA

Automatic Failure Detection

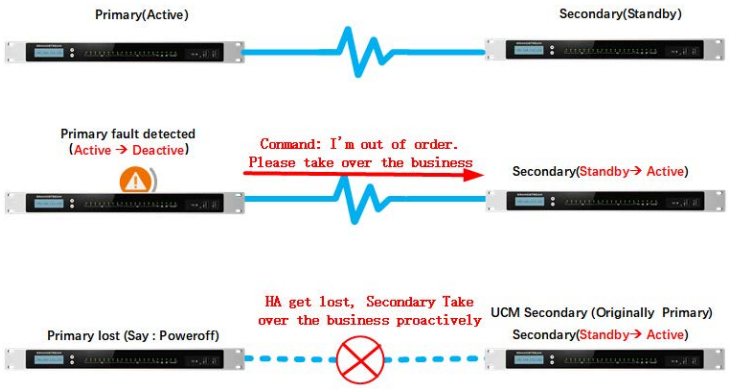

Figure 16: Active and Standby UCM Failover

Important Note

In case of a failure, the user needs to manually unplug the LAN cable from the formerly Active UCM and plug it into the newly Active UCM to fully restore connection with the SIP endpoints.

Active UCM: Self-Failure Detection

The active UCM monitors and regularly checks whether there is any failure on itself. When there is failure detected on itself, it will notify the standby UCM to take over as an active server. Then the original active UCM will reboot automatically and become the standby server. This scenario applies to active UCM which has part of the function or specific service in faulty status, and it can still work partially without shutting down the service completely.

For example, if the active server has a core dump generated for core service, FXO port failure or WAN/LAN port disconnection, with this detection and notification mechanism, the standby UCM can take over immediately without noticeable delay or service interruption.

Standby UCM: Periodic Heartbeat

On HA mode, the standby UCM will check the active UCM's status periodically by sending a heartbeat message to the active UCM. The heartbeat message is sent via the heartbeat port. If the active UCM is under normal working conditions, it will respond to the standby UCM after it receives a heartbeat request from the standby UCM. If the active UCM runs into a faulty situation such as the network chip becomes abnormal or the power adapter no longer works, it will stop responding to heartbeat requests. After the heartbeat period times out, the standby UCM will consider the active UCM as faulty and start taking over as the active server.

The heartbeat timeout period determines how soon the standby UCM can detect an active server's failure and switch over. By default, the heartbeat timeout period is 7 seconds. Users could modify the heartbeat timeout period as preferred, and this will affect the detection/switchover sensitivity.

Force Switch

For the current active UCM, the system admin can click on Force Switch "Switch" button on its web UI HA settings page to force triggering the active/standby role change manually. This operation should be only used during firmware upgrade or the active UCM encounters issue that requires force switchover to be triggered manually.

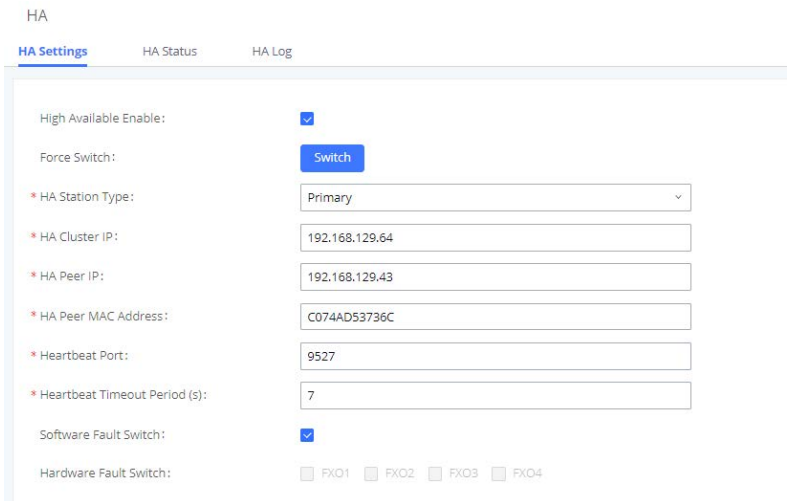

Figure 17: Force Switch

Firmware Upgrade

To ensure that there is no service interruption in HA setup, upgrading UCM requires the user to follow the below steps strictly:

Step 1: Log in the web UI of the standby UCM (A), upload firmware via web UI, and the standby UCM will reboot. Wait for it to boot up.

Step 2: After the standby UCM (A) boots up, log in to the web UI of the active UCM (B) and check the HA web page. The "Force Switch" button on the UCM B's HA web page will be available. Press it to manually trigger a switchover. After switchover, UCM A will become active and UCM B becomes standby.

Step 3: After switchover, log in to UCM B and upload firmware to its web UI. UCM B will reboot and request data from UCM A for a full backup.

In short, when upgrading UCM in HA setup, the standby UCM needs to be upgraded first and becomes active UCM. Then we can upgrade the standby UCM. This will ensure the active UCM is always working and providing PBX functions, so there is no service interruption during upgrading or switchover.

Replacing UCM in HA

HA Setup with UCM RemoteConnect

Assuming 2 UCM (A and B) with UCMRC plan on GDMS have been set up for HA and UCM B becomes defective which requires replacement, please follow the steps below to replace the defective UCM B with UCM C.

Scenario 1: UCM A's station type is "Primary" and it's the active UCM. UCM B's station type is "Secondary" and it's in standby status.

1. Add UCM C to GDMS first. Then assign UCM RemoteConnect plan to UCM C. The UCMRC plan can be a new plan for UCM C or transferred from UCM B.
2. Turn off the power for UCM B.
3. Modify UCM A's HA settings by changing HA Peer MAC address from UCM B to UCM C's MAC address. Save and reboot UCM A.
4. After UCM A boots up, log in UCM A web UI and confirm the HA status to be Active. Connect UCM C to the HA setup using appropriate cables for WAN port, heartbeat port, FXO port and etc.
5. After UCM C boots up, log in UCM C web UI and configure network settings to be the same as UCM B. After configuration, UCM C has the same static IP as UCM B.
6. Check whether UCM C has Cloud IM enabled and ensure it's disabled. Cloud IM must be disabled on UCM C before replacing UCM B.
7. Log in UCM C's web UI, enable HA, configure HA station type and other HA settings to be the same as UCM B. Save and reboot UCM C.
8. After UCM C boots up, check and verify the HA status. UCM A should be active and UCM C should be standby.

Scenario 2: UCM A's station type is "Secondary" and it's the active UCM. UCM B's station type is "Primary" and it's in standby status.

1. On GDMS, delete the custom domain name for UCM B.
2. Add UCM C to GDMS and assign UCMRC plan to UCM C. The UCMRC plan can be a new plan for UCM C or transferred from UCM B. On GDMS, configure the custom domain name for UCM C to be the same as the one for UCM B. Please note UCM C must have custom domain name configured on GDMS.
3. Turn off the power for UCM B.
4. Modify UCM A's HA settings by changing HA Peer MAC address from UCM B to UCM C's MAC address. Save and reboot UCM A.
5. After UCM A boots up, log in UCM A web UI and confirm the HA status to be Active. Connect UCM C to the HA setup using appropriate cables for WAN port, heartbeat port, FXO port and etc.
6. After UCM C boots up, log in UCM C web UI and configure network settings to be the same as UCM B. After configuration, UCM C has the same static IP as UCM B.
7. Check whether UCM C has Cloud IM enabled and ensure it's disabled. Cloud IM must be disabled on UCM C before replacing UCM B.
8. Log in UCM C's web UI, enable HA, configure HA station type and other HA settings to be the same as UCM B. Save and reboot UCM C.
9. After UCM C boots up, check and verify the HA status. UCM A should be active and UCM C should be standby.

HA Setup without UCM RemoteConnect

Assuming 2 UCM (A and B) in HA setup have no UCMRC plan on GDMS, UCM A is in active status and UCM B is in standby status. UCM B becomes defective and requires replacement. Please follow the steps below to replace the defective UCM B with UCM C:

1. Turn off the power for UCM B.
2. Modify UCM A's HA settings by changing HA Peer MAC address from UCM B to UCM C's MAC address. Save and reboot UCM A.
3. After UCM A boots up, log in UCM A web UI and confirm the HA status to be Active. Connect UCM C to the HA setup using appropriate cables for WAN port, heartbeat port, FXO port and etc.
4. After UCM C boots up, log in UCM C web UI and configure network settings to be the same as UCM B. After configuration, UCM C has the same static IP as UCM B.
5. Check whether UCM C has Cloud IM enabled and ensure it's disabled. Cloud IM must be disabled on UCM C before replacing UCM B.
6. Log in UCM C's web UI, enable HA, configure HA station type and other HA settings to be the same as UCM B. Save and reboot UCM C.
7. After UCM C boots up, check and verify the HA status. UCM A should be active and UCM C should be standby.

Critical Note:

HA configuration requires the UCM to reboot. Please reboot the UCM during non-service hour to avoid service interruption.

Disabling HA Setup

If HA setup is no longer required for the UCM, log in to the web UI using the active UCM's IP or the cluster's IP and go to the system settings→HA page to disable HA. Save and reboot the UCM. After both UCM boot up, check the HA status and it should show HA as off.

Cloud IM in HA Setup

Please ensure only one UCM in the HA setup has Cloud IM enabled. If using domain name assigned from GDMS, please ensure both UCM devices have UCM RemoteConnect plan which supports Cloud IM.

After the active UCM A in HA setup enables Cloud IM, the standby UCM B will synchronize from UCM A and obtain Cloud IM service as well. Cloud IM service is always available on the active UCM, and the associated MAC address will change if active/standby UCM changes. Therefore, failover in HA setup does not affect Cloud IM service.

When UCM B becomes defective, if a replacement UCM C has no Cloud IM enabled, and it's used to swap UCM B in HA setup, after replacement, Cloud IM will still work for the UCM in the HA setup, without additional configurations. However, if the replacement UCM C has Cloud IM enabled before swapping, Cloud IM must be turned off on UCM C first. The replacement must be done when there is no previous Cloud IM service on UCM C.

Using UCM RemoteConnect with HA

If the user has purchased a UCM RemoteConnect plan with HA, the GDMS web page can show the UCM with HA status "Host" or "Spare".

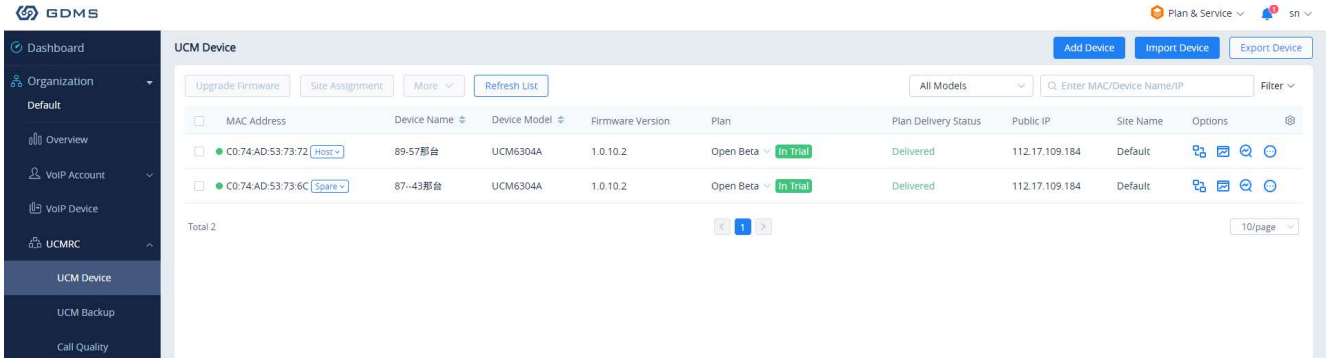

Figure 18: GDMS Display for UCM HA Status

Switching UCM RemoteConnect Role in HA

Prerequisites:

- Both UCM must have UCM RemoteConnect plan with HA feature purchased on GDMS.
- UCMRC service has been successfully delivered to both UCM.

Implementations:

- The call service is provided by GDMS and the active UCM.
- When the active UCM A is faulty condition and has triggered switchover, the standby UCM B will take over and become active. UCM B will send switchover command to GDMS and notify GDMS that call service will be provided by UCM B and GDMS afterwards.

> **Note**
>
> 1. With UCMRC, after the UCM is configured with HA, UCM will notify its HA role to GDMS. System admin does not need to designate HA role for UCM on GDMS.
> 2. On GDMS, the system admin can still remotely access and operate each UCM in HA. However, the configuration on the standby UCM is limited because it synchronizes data from the active UCM regularly in the HA backup process.
> 3. The PBX providing service is the active UCM. However, GDMS will always assign the domain name for the Remote Connect service based on the primary UCM as configured initially.

Service Status

Active/Standby Status

After the HA setup is completed, the PBX will provide service using the HA cluster IP. During the initial stage, the standby UCM will request and synchronize all data from the active UCM.

The standby UCM monitors and prepares to become active at any time when needed. Manual configuration on standby UCM is restricted because it always synchronizes up data from active UCM. When the active UCM has any hardware or critical software failure, the standby UCM will immediately take over and becomes the active UCM. The previous active UCM will reboot and become the standby UCM. Calls during the role switchover will be recovered after the failover process completes.

Web UI Access for UCM

After HA setup is completed, the system admin can use the cluster IP address to log in to the current active UCM for configurations. The cluster IP address is always bound to the active UCM. For example, assuming HTTP/HTTPS port is 8089, the system admin can access UCM using URL *https://cluster_IP:8089*.

- System admin can log into the current active UCM using https://cluster_IP:8089 or https://activeUCM_IP:8089.
- If the system admin logs into the standby UCM's web UI by using the standby UCM IP https://standbyUCM_IP:8089 and attempts to modify configurations, it will not be allowed. The system will prompt that configuration is restricted on the standby UCM.

> **Critical Note**
>
> HA setup will synchronize up admin login information from the active UCM to the standby UCM. Therefore, when the system admin logs in the UCM web UI using the active UCM IP, standby UCM IP or the cluster IP, the active UCM's login information always needs to be used.

Log in Wave

After HA configuration, the login URL for Wave may be changed. Users can log in to Wave using the following addresses:

1. **Log in via IP.**

Since the UCM providing RemoteConnect service can be the primary or secondary UCM, the user should always use the cluster IP to log in to Wave. For example, https://cluster_IP:8089/gswave#.

1. **Log in via domain name.**

No matter whether failover happens, users could always use the domain name assigned from the GDMS Remote Connect service, which is determined by the initially configured primary UCM.

Failover during Call

When the active server encounters a failure, if there is an ongoing call on the active server, the switchover process will only cause a few seconds of audio cut off and then it will be recovered automatically.

> **Notes**
>
> - Currently, if the call is using UDP as transport method, the call can be recovered after switchover. However, if the call is using TCP as transport method, the call cannot be recovered after switchover.
> - Point-to-point calls such as audio call or audio meeting can be recovered after switchover. However, for calls using ring group, call queue and other call features and services, the call will not be automatically recovered.

Data Sync

HA setup provides data sync mechanism:

1. After UCM boots up, the standby UCM will send requests for all the data on active UCM and perform data sync. Every time when the active UCM has configuration change, it will also synchronize up the data to the standby UCM automatically and immediately.
2. Data sync is triggered in real-time manner. It not only synchronizes up configuration data, but also extensions, voicemail, CDR, etc.
3. Every day at midnight, a full backup will be performed to ensure active and standby UCM always have the same data on daily basis.

Backup and Restore

For backup restore, the admin needs to log in to the active UCM and restore the backup file on the active UCM first. UCM devices will reboot automatically. Once the UCM finishes booting up, the standby UCM will start synchronizing up data from the active UCM to restore the backup as well.

Maintenance

In HA setup, the system admin can check HA-related alerts under UCM web UI's system events page to learn if there is any abnormal event related to HA. According to the alerts, the admin can further diagnose by checking the event time and logs with more details.

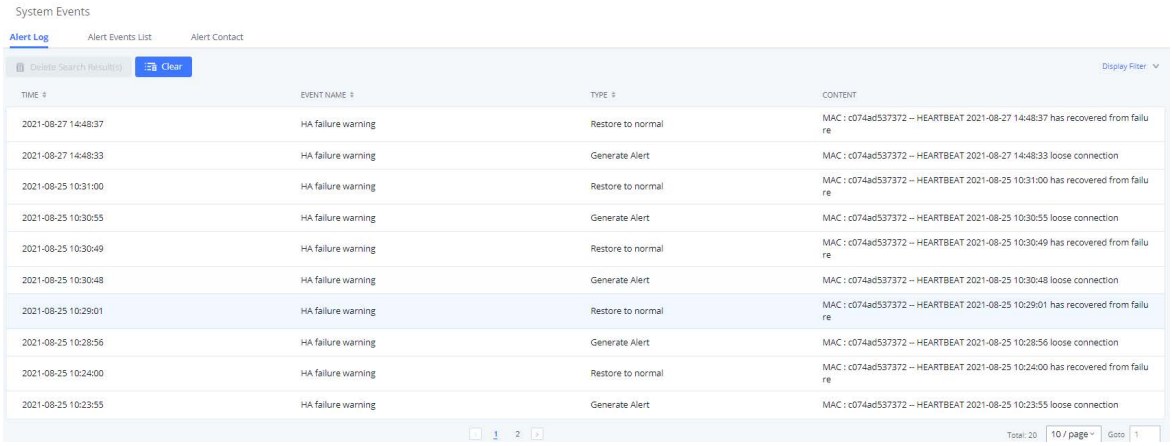

Figure 19: System Alert Events

HA log also shows all HA backup and failover logs.

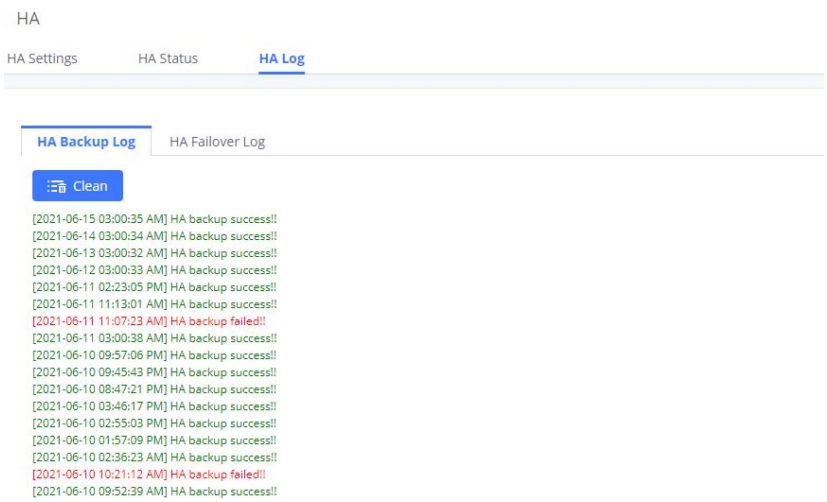

Figure 20: HA Logs